УДК 340.12
DOI: https://doi.org/10.21564/2663-5704.63.315212

Трофименко Володимир Анатолійович, кандидат юридичних наук, доцент,
доцент кафедри філософії, Національний юридичний університет
імені Ярослава Мудрого, м. Харків, Україна
v.a.trofymenko@nlu.edu.ua
ORCID ID: 0000-0003-2240-3727

КІБЕРПРОСТІР І ДЕРЖАВА: ТОЧКИ ПЕРЕТИНАННЯ

Публікацію присвячено державі в кіберпросторі. Робиться аналіз основних підходів держави до кіберпростору: класичного – з позицій традиційної науки та нового – з позицій тлумачення кіберпростору як особливої сфери регулювання. Виділяються три основних перспективних напрямки взаємодії держави та кіберпростору: технічний, політичний та економічний. При цьому акцентується на тому, що, незважаючи на існуючі нормативні прогалини, лише держава здатна провести певне регулювання існуючих відносин не тільки за наведеними, а і в інших сферах кіберпростору.

Ключові слова: *держава, кіберпростір, інтернет, кіберсуверенітет, цифровий суверенітет, свобода слова, інтернет речей, правове регулювання.*

Постановка проблеми. Наприкінці літа усі відомі світові [1; 2] та вітчизняні [3] засоби масової інформації (ЗМІ) облетіла новина про арешт у Франції Павла Дурова, засновника та власника інтернет-месенджера Telegram. Писалося, що «…правоохоронні органи Франції вважають Telegram розсадником злочинності. Вони незадоволені відмовою Дурова жорстко модерувати контент і співпрацювати з владою для розкриття інформації про користувачів, підозрюваних у поширенні наркотиків, дитячу порнографію та шахрайство» [1]. «Легко побачити, що висунуті обвинувачення можна поділити на три групи. Перша – це недостатньо ретельне адміністрування щодо злочинних груп у Telegram. Друга – це відмова від більш тісної співпраці з силовими структурами Франції, що одночасно трактується як співучасть у злочинній діяльності, яка велася на цій платформі (воно ж – "змова"). Третя – це обвинувачення навколо телеграмівської криптовалюти Toncoin», – писав інший ЗМІ [3]. При цьому варто відмітити, що обвинувачення висувалося особі, яка виконувала адміністративні функції в Telegram, тобто не займалась конкретними технічними питаннями. До речі, Telegram не забарився з відповіддю: «…Telegram випустив офіційну заяву у зв'язку з інформацією про затриман-

ня Дурова. У ній ідеться, що соцмережа "дотримується законів ЄС", а принципи модерації відповідають стандартам індустрії та "постійно покращуються". Голові Telegram Павлу Дурову немає чого приховувати, і він часто подорожує Європою. Абсурдно стверджувати, що на платформі або її власнику лежить відповідальність за зловживання цією платформою», – також заявили в компанії [1]. Історія навколо Павла Дурова не завершена і сьогодні. Вона може слугувати прикладом того, як держава намагається захистити свій кіберпростір від злочинних зазіхань. Проблема врегулювання та захисту кіберпростору набуває все більшого виміру. Незважаючи вже на досить тривалий час його існування, існує велика кількість проблем, які поки не вирішено, а позиція держави поки не набула стабільного статусу. Причому кіберпростір – чи не єдина сфера, у якій держава поки не може стало виділитись серед інших суб'єктів, а іноді навіть і не бажає цього. На це звертає увагу і мексиканський вчений G. Nieto. Він пише, що інтернет – це ресурс, який революціонізував людство. Його наслідки присутні в багатьох вимірах життя людей та іноді породжують негативні наслідки, які рідко помічаються. Право, на думку автора, не звільняється від цих перетворень. Розвиток мережі та її природа маргіналізували її, віддавши перевагу неприборканій дикій силі. Як результат, пише дослідник, – криза законності та національної держави, яка має наслідки для правової сфери індивідів, особливо щодо повного здійснення прав людини, і яка сприяє розміщенню нас у ситуації кібер-анархії, яку на час буття, здається, важко подолати [4]. Тому дискусія про місце та роль держави в кіберпросторі набуває все більшого обговорення в галузі наукових досліджень.

Аналіз останніх досліджень та публікацій. Новою сферою для юридичних досліджень і практики вважають інтернет колумбійські вчені W. Jiménez та O. Quintana. Розвиток інтернету, на їхню думку, є викликом традиційним правовим кордонам, які зміцнюються на понятті суверенітету та просторової локалізації діяльності. Особливості інтернету, такі як його транскордонний характер, географічна незалежність, широке охоплення, анонімність, портативність, легке відтворення, конвергенція, підключення та складність контролю, є новими викликами для нового закону. Тому, вважають науковці, за допомогою якісного та індуктивного методу, використовуючи як первинні, так і вторинні джерела та методи аналізу документів, необхідно представити панорамне уявлення про найважливіші аспекти, пов'язані з інтернетом, а також про найбільш суперечливі чи критичні теми чи сфери. Для науковців, суддів та адвокатів є необхідність ознайомитися з технологічними аспектами віртуального спілкування, щоб зрозуміти, керувати та вирішувати юридичні проблеми, що виникають в інтернеті, роблять висновок колумбійські вчені [5].

На новизну інтернету з точки зору міжнародного звичаєвого права звертає увагу і польський вчений P. Polanski. Міжнародні відносини між країнами,

звертає увагу він, усе частіше відбуваються в кіберпросторі. Від занепокоєння щодо кібербезпеки та стеження в інтернеті до конфіденційності та шкідливих висловлювань – державні та недержавні суб'єкти розробили практики та нормативні концепції, які можна розглядати як міжнародне звичаєве право *in statu nascendi*. Він вважає, що дослідження, які стосуються міжнародного права, повинно бути розширено, щоб охопити кіберпростір. А за відсутності договірного права в цій сфері слід вдаватися до другого джерела міжнародного права, а саме до звичаю [6].

Сучасні дослідники звертаються і до традиційної філософсько-правової проблематики стосовно кіберпростору. Прикладом може слугувати дослідження китайських науковців H. Xu та X. Zhang. Верховенство права, вважають вони, є основною формою національного управління, а модель верховенства права є необхідним напрямком для управління онлайн-суспільством. На їхню думку, інтернет-суспільство, по суті, є новою моделлю соціальних відносин і структурних форм, що містять відносини між громадянами, юридичними особами, організаційними органами тощо, сформованими та об'єднаними на основі інтернет-технологій; а також відображення, розширення та вираження, окремо або в синтезі, різноманітних відносин у сферах реальної економіки, політики, культури, суспільства та навколишнього середовища. Модель верховенства права для управління інтернетом, стверджують китайські дослідники, стосується теорій, систем і практик управління, які використовують концепцію верховенства права та модель верховенства права, щоб перенести елементи, структури, процедури та функції управління інтернетом у сферу верховенства права та його операційний шлях. Розвиток верховенства права в інтернеті в Китаї, узагальнення досвіду побудови верховенства права в інтернеті та міркування про існуючі законодавчі, правоохоронні та судові дилеми дозволять, пишуть автори, побудувати верховенство права системи онлайн-управління з комплексними іменниками, ефективним упровадженням, суворим наглядом і сильними гарантіями. Враховуючи китайські реалії, це забезпечить застосування мислення верховенства права та моделі верховенства права в управлінні, експлуатації, використанні та захисті інтернету, таким чином досягаючи надійного та впорядкованого функціонування та розвитку інтернету на шляху верховенства права та просування модернізації системи управління інтернетом та можливостей управління, завершують свою думку науковці [7].

Усі наведені вище погляди ілюструють бажання науковців екстраполювати досягнення традиційної правової науки на новий для них об'єкт – кіберпростір. Але ще в 1996 р. американські професори D. Johnson та D. Post звернули увагу на інший підхід до нього. Вони стверджували, що кіберпростір потребує системи правил, відмінних від законів, які регулюють фізичні,

географічно визначені території. Кіберпростір ставить під сумнів традиційну залежність закону від територіальних кордонів; це, на їхню думку, «простір», обмежений екранами та паролями, а не фізичними маркерами. Професори твердять, що «серйозне ставлення до кіберпростору» як унікального місця повинно привести до розроблення нових чітких правил для онлайн-трансзакцій і ефективних правових установ [8]. Цю позицію підтримує грецький вчений S. Tzafestas. На його думку, метою закону є підтримка соціального порядку, миру та справедливості в суспільстві, тоді як метою етики є створення кодексів етики та поведінки, які допомагають людям вирішувати, що є неправильним, а також як діяти та поводитися. Закони, продовжує автор, забезпечують мінімальний набір стандартів для досягнення доброї людської поведінки. Етика часто передбачає стандарти, які перевищують законний мінімум. Тому для найкращої поведінки слід поважати як закон, так і етику. Інтернет речей включає велику кількість об'єктів і людей, які підключені через інтернет «у будь-який час» і «в будь-якому місці» для надання однорідних комунікаційних і контекстних послуг. Таким чином, це створює новий соціальний, економічний, політичний та етичний ландшафт, який потребує нових покращених правових та етичних заходів для захисту конфіденційності, безпеки даних, захисту прав власності, покращення довіри та розроблення відповідних стандартів [9].

Таким чином, можна побачити критичне ставлення до кіберпростору з боку науковців. Сьогодні спостерігається намагання розглянути та дослідити його з усіх боків, зважаючи на постійне розширення та зростання впливу на суспільне життя.

Формулювання мети. Мета публікації – показати нестабільність статусу держави в кіберпросторі з причини полісуб'єктності цієї сфери та показати перспективні напрямки його взаємодії з державою.

Викладення основного матеріалу. Сьогодні, незважаючи на інстуціональну розгалуженість, держава не може чітко закріпити свій статус у кіберпросторі. Це пов'язано з тим, що існує велика кількість суб'єктів, що зазіхають на її традиційні владні повноваження, які вона намагається впровадити в кібермережі. На це, наводячи приклад США, звертає увагу група австралійських вчених у складі M. Kelton, M. Sullivan, Z. Rogers, E. Bienvenue, S. Troath. Інфраструктурна потужність у Сполучених Штатах, пишуть вони, тобто здатність видобувати та розгортати соціальні ресурси та ініціювати та використовувати технологічні інновації, все більше створюється приватним інтернет-капіталом і використовується цифровими платформами. Автори стверджують, що, хоча ці приватні актори не мають легітимності, це форма «віртуального суверенітету», яка ускладнює здатність держави США здійснювати інфраструктурну владу. Незважаючи на те, що інтернет-програмне забезпечення було розроб-

лено в основному американськими корпораціями, комерційні користувачі все більше працюють у детериторіальних глобальних просторах, де згода громадян та інтереси штату США не є пріоритетними для бізнесу. Крім того, значна частина апаратного забезпечення інтернету фінансується приватним інтернет-капіталом у глобальних ланцюжках багатства та цифрових просторах, населених американськими та неамериканськими корпораціями. Вони підкреслюють, що цифрові платформи набувають інфраструктурної потужності завдяки накопиченню та комерціалізації великих даних, з яких вони формують індивідуальне мислення та поведінку. Отже, науковці роблять висновок: контроль приватного інтернет-капіталу над величезними соціально-економічними ресурсами зміцнює лідерство цифрових платформ у технологічних інноваціях і кидає виклик монополії суверенної держави на національну безпеку. Автори стверджують, що цифрові платформи в США почали набувати деяких повноважень, якими традиційно володіє держава, створюючи форму «віртуального суверенітету» [10]. Таким чином, вченими фактично ставиться питання віртуального чи цифрового суверенітету держави, і одним із перших є: чи потрібен такий суверенітет самій державі? На це звертають увагу німецькі вчені M. Braun та P. Hummel. Суверенітет є часто використовуваним терміном, коли йдеться про аналіз та формування цифрових процесів і трансформацій. Наприклад, останніми роками цифровий суверенітет став центральною концепцією європейської політики. У своїй публікації автори стверджують, що посилання на цифровий суверенітет здебільшого оперують неправдоподібно одновимірним, надто спрощеним поняттям суверенітету загалом і його застосування до цифрового світу зокрема. Вчені досліджують питання про те, що може містити розмова про суверенітет у контексті даних і цифрового простору. В якості основи для цього дослідження вони виділяють три аспекти концепції суверенітету: 1) суверенітет як абсолютну владу; 2) суверенітет як втілену владу та 3) суверенітет як інституційну владу. Дослідники доходять висновку, що, принаймні в європейських дебатах щодо цифрового суверенітету, два з цих аспектів, що стосуються заплутаних відносин між сувереном і адресатом(ами) претензій на суверенітет, постійно ігноруються. Якщо цифровий суверенітет розуміти як такий, що охоплює три аспекти він міг би, вважають науковці, бути частиною нормативної бази, що нормативно орієнтована на вразливість і свободу, яка залишається відкритою та чутливою до напруженості й амбівалентності та яка постійно приймає їх як відправні точки для нових підходів до управління та регулювання цифрових практик [11]. На думку німецьких вчених, для повної реалізації цифрового суверенітету необхідні всі три наведених ними аспекти. Продовжують проблему проблематичності цифрового суверенітету держави австрійські вчені G. Falkner, S. Heidebrecht, A. Obendiek, T. Seidl. В останні роки мова цифрового

суверенітету стала повсюдною в Європі. Однак, вважають вчені, досі не вистачає системних знань про те, чи супроводжується дискурс про цифровий суверенітет фактичними змінами політики в різних сферах політики ЄС і якою мірою. Незважаючи на те, що автори знаходять зміни в політиці в бік посилення контролю над цифровим світом у всіх розглянутих сферах політики, цей зсув, на їхню думку, лише іноді супроводжується дискурсивними змінами в бік цифрового суверенітету. Це, роблять висновок вчені, є результатом ідейних компромісів, з якими стикаються суб'єкти, коли використовують мову цифрового суверенітету в різних місцях, сферах політики чи країнах [12]. Поряд із подібними дискусіями формулюються і конкретні пропозиції з розуміння цифрового суверенітету. Свою модель пропонує колектив німецьких вчених: I. Fries, M. Greiner, M. Hofmeier, R. Hrestic, U. Lechner, T. Wendeborn. Цифровий суверенітет викликав інтерес у політичному полі та в публічному дискурсі. Автори розглядають «цифровий суверенітет» з різних академічних дисциплін у підході цілісного аналізу: під час обговорення цифрового суверенітету у них виникає питання, чий цифровий суверенітет розглядається, що цифровий суверенітет означає для відповідних суб'єктів, як збільшити цифровий суверенітет і як побудувати цифрове суверенне громадянське суспільство та його критичні інфраструктури. Вчені представляють багатошарову модель для концептуалізації значення цифрового суверенітету на трьох рівнях: 1) держава або наднаціональна установа; 2) організація; 3) особа, а також відносини між трьома рівнями. Запропонована модель, вважають вони, забезпечує керівництво для досліджень і практики, включаючи політику та прийняття рішень, щодо складної теми цифрового суверенітету. Цю живу модель науковці пропонують розширити та адаптувати, оскільки до цього відносно нового поля додається все більше розуміння [13]. У цілому, не закінчуючи дослідження цифрового суверенітету, вчені дійшли згоди про його необхідність та існування, що відкрило можливість розглядати його конкретні аспекти.

Держава може по-різному впливати на громадян-користувачів. Німецький вчений R. Magnus на прикладі Польщі демонструє найбільш м'який спосіб. Поширення інформації про право, зазначає він, є одним із найважливіших аспектів формування оптимального рівня правової безпеки громадян. Це стосується, зокрема, тих етапів розвитку правової системи, на яких відбуваються насильницькі та різнобічні зміни законодавства, що порушують відомі громадськості рішення. Така ситуація склалася в Польщі через політичні зміни, які відбулися останніми роками. За таких умов, вважає автор, ключову роль у поширенні знань про чинне законодавство починають відігравати інструменти поширення інформації про законодавство, а точніше – про зміни в законодавстві. На цьому етапі розвитку, резюмує німецький дослідник, електронні інструменти, у тому числі інструменти соціальної комунікації

в інтернеті, стають основним засобом пізнавальної діяльності, адресованими як усім членам суспільства, які повинні дотримуватися цього закону, так і професіоналам, завдання яких полягає в тому, щоб поставити застосовне право на практиці [14]. Коли подібних механізмів уже недостатньо держава може вдатись до застосування більш серйозних заходів. Так постає проблема регулювання державою доступу до інтернету та його відключення.

Наведеній вище проблемі доступу до інтернету приділяє увагу австралійська вчена L. Cradduck. І вона вважає, що доступом до інтернету держава не може і не повинна зловживати з таких причин. Можливість доступу до вмісту та послуг інтернету, вважає вона, є важливим аспектом нашого життя. Незважаючи на те, що доступ до інтернету використовується багатьма лише як засіб спілкування чи розваги, для людей з обмеженими можливостями чи тих, хто перебуває у віддалених районах, доступ до інтернету може забезпечити такий рівень взаємодії з інформацією, друзями та урядом, який інакше неможливий. Таким чином, звертає увагу авторка, завдяки використанню інтернету реалізуються інші основні права людини. Однак для того, щоб інтернет забезпечував ці інші права, спочатку потрібно ввімкнути доступ до інтернету. Бажано, щоб це відбувалося за допомогою міжнародного визнання доступу до інтернету як основного права людини, яке потім підтримується політикою та законами конкретної юрисдикції. При цьому, резюмує дослідниця, це не сучасні реалії. Але, продовжує вчена, визнання доступу до інтернету як права не втрачається [15]. Відключення інтернету, щоб запобігти зловживанням, повинно бути більш юридично обгрунтованим. На це вказують італієць G. De Gregorio та його колега з Великої Британії N. Stremlau. Відключення інтернету, констатують вони, зростає. За останні кілька років ескалація цієї грубої практики цензури вплинула на різні регіони світу, зокрема на Африку та Азію. Науковці та правозахисники, вважають вони, не запропонували жодних суттєвих рішень для ефективного вирішення проблеми відключення інтернету, а аналіз здебільшого обмежувався вивченням негативних наслідків через дані про їхню частоту, тривалість та економічні витрати. Автори роблять спробу вийти за рамки поляризованої дискусії між «залишити» та «вимкнути», щоб дослідити, як може бути більш прозорим процес прийняття рішень, пов'язаних із відключенням інтернету. Вони обговорюють обмеження законодавства, коли справа доходить до запровадження та здійснення відключень. Вимкнення, як правило, накладаються дещо довільно з невеликим процесом. Повернення юридичних аргументів до дослідження обґрунтувань зупинок може зробити використання зупинок менш частим і більш обмеженим, коли вони трапляються [16]. Але відключення можуть застосовуватись для забезпечення безпеки громадян-користувачів. У цьому аспекті проблеми відключення інтернету (обмеження доступу до кіберпрос-

тору) порушує німецький вчений J. Thumfart. Розглядаючи випадки з Камеруну, Єгипту, Ефіопії, Індії, Індонезії, Ірану, Нігерії, Пакистану, Іспанії, Того, Сполученого Королівства, Сполучених Штатів і Зімбабве, автор розглядає глобальне явище відключення інтернету з нормативної точки зору, справедливої теорії сек'юритизації. Він зосереджується на конфлікті між аргументами, які використовуються для виправдання відключення, і його негативним впливом на фундаментальні права людини. У статті вчений розробляє суворі критерії, коли відключення можуть бути законними як надзвичайні заходи безпеки в надзвичайних ситуаціях. Ці критерії базуються на праві громадян на фізичну цілісність, очікуванні розумного успіху, пропорційності, мінімізації шкоди та конкретності. Німецький дослідник стверджує, що використання відключення інтернету для застосування колективних покарань, превентивної цензури або перешкоджання законним політичним протестам є неправомірним. Також держава зобов'язана десек'юритизувати процедуру відключення після нейтралізації загрози. Як висновок дослідник стверджує, що збалансоване обговорення відключення як виняткового заходу з точки зору безпеки сприяє встановленню традиційного позитивного права людини на цифровий зв'язок у нормальній ситуації [17].

Звертаючись до питання відключення інтернету, слід звернути увагу на те, що воно може мати вигляд репресій уряду проти суспільної думки. Цей аспект розглядає німецький науковець R. Strauch. Відключення інтернету, пише він, стало популярним інструментом для репресивних режимів, щоб змусити замовкнути інакомислення в оцифрованому світі. Незважаючи на те, що влада намагається придушити опонентів, встановлюючи відключення інтернету, мало відомо про те, як громадськість реагує на такі рішучі заходи. Режим може зіткнутися з гнівом і обуренням з боку громадськості як відповідь на позбавлення інтернету. У цій статті автор стверджує, що відключення інтернету знижує оцінку громадськістю політичного керівництва, оскільки громадяни звинувачують уряд у збоях у наданні послуг. Але при цьому громадяни не притягують уряд до відповідальності за збої в інтернеті, що робить його відключення потужним інструментом для автократів, щоб замовчувати незгоду в цифровому режимі [18].

Поряд із проблемою відключення стоїть питання свободи слова в кіберпросторі. Тут дослідники звертають увагу на хиткі позиції традиційного підходу. Розмежуванню свободи слова та цензури приділяють свою увагу іспанські вчені F. Serna та J. Iniesta. З появою інтернету здійснення свободи думки та інформації розширилося до нескінченності, а також з'явилась можливість безкінечних порушень і правопорушень, які є результатом необмеженого використання свободи слова. Зважаючи на ці обставини, відмічають автори, необхідне належне розмежування між використанням свободи слова в інтер-

неті та конфліктами, що виникають. Однак законодавець іноді пропонує суперечливі та неефективні рішення, оскільки вони не пристосовуються чітко до цього нового соціального явища. Нинішньому законодавству, вважають дослідники, доведеться вирішувати серйозні проблеми, особливо пов'язані з питанням визначення відповідальності за викид контенту в мережу, захисту неповнолітніх і регулювання систем участі. Це тим більше важливо тому, що в кількох чинних законодавчих актах свобода слова є правом, яке було зруйновано з моменту появи інтернету. Однак через їхній міжнародний характер і культурні відмінності між країнами такі вказівки не повинні бути єдиними [19]. До права на свободу слова в аспекті мови ворожнечі й ненависті на прикладі своєї країни звертається бразильський науковець F. Pardo. Він також вказує на постійну необхідність оновлення законодавства стосовно інтернету, а саме оновлення теж не повинно запинятись. У публікації автор розглядає мову ненависті в цифровому середовищі за допомогою трансдисциплінарного підходу, заснованого на філософській основі Камю, а також на теорії дискурсу Фуко і Орланді. З огляду на випадки мови ненависті в інтернеті та практики опору його мета – це обговорення тонкої межі між мовою ненависті й свободою слова та вираження поглядів разом із регулюванням інтернету в Бразилії. Гіпотеза науковця полягає в тому, що з появою нових способів соціальних практик в інтернеті, таких як узаємодія в соціальних мережах і виробництво, споживання та обмін інформацією в соціальних мережах, таких як Facebook, WhatsApp і Twitter, було б надзвичайно важливо переглянути законодавство, яке регулює використання інтернету в Бразилії, як це вже відбувається в Європейському Союзі [20].

Менш політизованою, але не менш важливою сферою кіберпростору є так званий інтернет речей. На неї звертає увагу аргентинський вчений A. Porcelli. За останні десятиліття, пише він, інтернет перетворився на щось непередбачуване. Комп'ютерами, принтерами, мобільними телефонами, планшетами, смарт-телевізорами, освітленням, автомобілями, побутовими приладами та навіть дверними замками можна дистанційно керувати для комфорту споживача, але вони також можуть бути засобом для всіх видів злочинів. По суті, необхідно встановити стандарти для забезпечення безпечного використання цих пристроїв, підключених до мережі, констатує проблему вчений [21]. Більш докладно розглядає цю проблему американський вчений A. Tran. інтернет речей, відмічає він, – це інтригуючий цифровий феномен у технологіях, який створює багато юридичних проблем, оскільки світ стає все більш взаємопов'язаним через інтернет. Створюючи підключену систему, інтернет речей пов'язує мережу фізичних об'єктів, таких як споживчі пристрої, і дозволяє цим пристроям спілкуватися та обмінюватися даними. Найближчим часом майже всі споживчі пристрої, від автомобілів до чашки для кави, змо-

жуть підключатися через інтернет. Інтернет речей має неймовірний потенціал для покращення суспільства, надаючи величезну кількість різноманітних сенсорних даних для аналітики та інших цілей. Тим не менш існує також багато прихованих небезпек, які можуть проявлятися в міру його поширення, включаючи порушення конфіденційності та ризики для безпеки.

Юридична наука щодо питань конфіденційності стосовно інтернету речей, продовжує науковець, наразі недостатньо розвинена. Американський дослідник пропонує потенційне рішення, припускаючи, що два правопорушення щодо конфіденційності, публічне розголошення приватних фактів і втручання в ізоляції можуть забезпечити часткові цивільні засоби правового захисту для цих споживачів. Кожне з двох правопорушень конфіденційності еволюціонувало різними шляхами з моменту свого створення, і він досліджує переваги та недоліки обох. Насамкінець автор виступає за розширення використання та активізацію цих порушень конфіденційності через судове застосування у справах інтернету речей як потенційну стратегію його регулювання [22].

Висновок. Підсумовуючи наведене, варто відмітити таке:

1. Незважаючи на доволі тривалий термін наукового дослідження кіберпростору (інтернету), представники наукової спільноти ще не визначились з провідним підходом його вивчення. Якщо перший підхід базується на традиційних філософсько-правових та правових принципах та визначеннях, то другий розглядає кіберпростір як особливу, окрему сферу, що має свою специфіку та вимагає власних наукових принципів. Але при цьому всі науковці визнають наявність кіберпростору і розглядають його як об'єкт наукового осмислення.

2. Класичні державні інститути все більше виявляються неспроможними для врегулювання багатьох питань, що виникають у сфері кіберпростору. Просте перекладання вже існуючих інститутів неможливе тому, що держава не здатна повністю контролювати інтернет. Усі намагання розбиваються через наукові обґрунтування та вимоги необхідного обмеження державної влади, особливо її карної функції. Це влучно відмітили німецькі вчені L. Monsees та D. Lambach. «Цифровий суверенітет» став гарячою темою європейської політики. Але хоча справжній європейський цифровий суверенітет здається недосяжним, аналіз дискурсу цифрового суверенітету все одно корисний, оскільки він багато говорить нам про європейську політику, пишуть вони [23].

3. Можна виділити три перспективних сфери взаємодії держави та користувачів – громадян кіберпростору, які потребують постійного правового втручання. На прикладі відключення інтернету можна виділити технічну сферу, на прикладі свободи слова – політичну, на прикладі інтернету речей – економічну. Користувачі кожної з цих сфер переважно не спроможні врегу-

лювати наявні відносини з урахуванням прав та, особливо, обов'язків усіх учасників. Тому держава фактично є єдиною спроможною надбудовою.

У цілому кіберпростір продовжує свій розвиток і дуже часто без участі держави та її інститутів. Тому потреба в його вивченні стає все більше нагальною. Швидкість та швидкісність розвитку мережевих технологій вимагають від держави постійного різногалузевого реагування. Ефективність цього реагування можлива лише на базі сучасних наукових досліджень.

ЛІТЕРАТУРА

1. «Немає чого приховувати». Що відомо про арешт Дурова і як на нього реагує світ. URL: https://www.bbc.com/ukrainian/articles/c4gqe2qwe82o (дата звернення 18.09.2024).
2. Ордер на арешт Дурова та його брата був виданий ще у березні. *Politico*. URL: https://www.radiosvoboda.org/a/news-durnyy-brat-telehram/33096977.html (дата звернення: 18.09.2024).
3. Арешт Дурова як нагадування про небезпеки, що криються в Telegram. URL: https://www.ukrinform.ua/rubric-world/3899351-arest-durova-ak-nagaduvanna-pro-nebezpeki-so-kriutsa-v-telegram.html (дата звернення: 18.09.2024).
4. Nieto G. The Nature and Development of The Internet: A Crisis for Law. *Ciencia juridica*. 2023. № 12 (24). P. 143–164.
5. Jiménez W., Quintana O. Law and internet: introduction to an emergent field for both legal research and practice. *Prolegomenos-derechos y valores.* 2017. № 20 (40). P. 43–61.
6. Polanski P. Cyberspace: A new branch of international customary law? *Computer law & security review.* 2017. № 33 (3). P. 371–381.
7. Xu H., Zhang X. The Rule of Law Model of Internet Governance. *Social sciences in china*. 2019. № 40 (3). P. 135–151.
8. Johnson D., Post D. Law and borders – The rise of law in Cyberspace. *Stanford law review.* 1996. № 48 (5). P. 1367–1402.
9. Tzafestas S. Ethics and Law in the Internet of Things World. *Smart cities.* 2018. № 1 (1). P. 98–120.
10. Kelton M., Sullivan M., Rogers Z., Bienvenue E., Troath S. Virtual sovereignty? Private internet capital, digital platforms and infrastructural power in the United States. *International affairs.* 2022. № 98 (6). P. 1977–1999.
11. URL: https://academic.oup.com/ia/article/98/6/1977/6783036?login=false.
12. Braun M., Hummel P. Is digital sovereignty normatively desirable? *Information, Communication & Society.* 2024. P. 1–14.
13. URL: https://www.tandfonline.com/doi/epdf/10.1080/1369118X.2024.2332624?needAccess=true.
14. Falkner G., Heidebrecht S., Obendiek A., Seidl T. Digital sovereignty – Rhetoric and reality. *Journal of european public policy.* 2024. № 31 (8). P. 2099–2120.

15. Fries I., Greiner M., Hofmeier M., Hrestic R., Lechner U., Wendeborn T. Towards a Layer Model for Digital Sovereignty: A Holistic Approach. *17th International Conference on Critical Information Infrastructures Security (CRITIS).* Proceedings 17th International Conference on Critical Information Infrastructures Security (CRITIS). Munich. 2022. P. 119–139.
16. Magnus R. Corporate personality rights on the internet and the applicable law. *Rabels zeitschrift fur auslandisches und internationales privatrecht.* 2020. № 84 (1). P. 1–23.
17. Cradduck L. Legislating for Internet «Access» – ability. *Second international handbook of internet research.* New York, 2020. P. 647–668.
18. De Gregorio G., Stremlau N. Internet Shutdowns and the Limits of Law. *International journal of communication.* 2020. № 14. P. 4224–4243.
19. Thumfart J. Digital Rights and the State of Exception. Internet Shutdowns from the Perspective of Just Securitization Theory. *Journal of global security studies*. 2024. № 9 (1). URL: https://academic.oup.com/jogss/article/9/1/ogad024/7515068?login=false
20. Strauch R. Public opinion effects of digital state repression: How internet outages shape government evaluation in Africa. *Journal of information technology & politics*. 2024. № 21. P. 479–492.
21. Serna F., Iniesta J. The delimitation of freedom of speech on the Internet: the confrontation of rights and digital censorship. *Adcaij-advances in distributed computing and artificial intelligence journal*. 2018. № 7 (10). P. 5–12. URL: https://revistas.usal.es/cinco/index.php/2255–2863/article/view/ADCAIJ201871512/19076.
22. Pardo F. Hate speech and freedom of expression in digital environments: social and legal implications. *Soletras*. 2022. № 43. P. 178–196.
23. Porcelli A. (Des)advantages of the first legislation on the internet of things. *En letra.* 2019. № 11/12. P. 139–164.
24. Tran A. The Internet of Things and Potential Remedies in Privacy Tort Law. *Columbia journal of law and social problems.* 2017. № 50 (2). P. 263–298.
25. Monsees L., Lambach D. Digital sovereignty, geopolitical imaginaries, and the reproduction of European identity. *European security*. 2022. № 3. P. 377–394.

REFERENCES

1. “Nemaye choho prykhovuvaty”. Shcho vidomo pro aresht Durova i yak na n′oho reahuye svit. (2024). URL: https://www.bbc.com/ukrainian/articles/c4gqe2qwe82o [in Ukrainian].
2. Order na aresht Durova ta yoho brata buv vydanyy shche u berezni. *Politico* (2024). URL: https://www.radiosvoboda.org/a/news-durnyy-brat-telehram/33096977.html [in Ukrainian].
3. Aresht Durova yak nahaduvannya pro nebezpeky, shcho kryyut′sya v Telegram. (2024). https://www.ukrinform.ua/rubric-world/3899351-arest-durova-ak-nagaduvanna-pro-nebezpeki-so-kriutsa-v-telegram.html [in Ukrainian].
4. Nieto, G. (2023). The Nature and Development of The Internet: A Crisis for Law. *Ciencia juridica*, *12(24), 143–164.*

5. Jiménez, W., Quintana, O. (2017). Law and internet: introduction to an emergent field for both legal research and practice. *Prolegomenos-derechos y valores, 20*(40), *43–61.*
6. Polanski, P. (2017). Cyberspace: A new branch of international customary law? *Computer law & security review, 33(3), 371–381.*
7. Xu, H., Zhang, X. (2019). The Rule of Law Model of Internet Governance. *Social sciences in china*, *40(3), 135–151.*
8. Johnson, D., Post, D. (1996)). Law and borders – The rise of law in Cyberspace. *Stanford law review, 48(5), 1367–1402.*
9. Tzafestas, S. (2018). Ethics and Law in the Internet of Things World. *Smart cities, 1(1), 98–120.*
10. Kelton, M., Sullivan, M., Rogers, Z., Bienvenue, E., Troath, S. (2022). Virtual sovereignty? Private internet capital, digital platforms and infrastructural power in the United States. *International affairs, 98(6), 1977–1999.*
11. URL: https://academic.oup.com/ia/article/98/6/1977/6783036?login=false
12. Braun, M., Hummel, P. (2024). Is digital sovereignty normatively desirable? *Information, Communication & Society, 1–14.*
13. URL: ttps://www.tandfonline.com/doi/epdf/10.1080/1369118X.2024.2332624?needAccess=true
14. Falkner, G., Heidebrecht, S., Obendiek, A., Seidl, T. (2024). Digital sovereignty – Rhetoric and reality. *Journal of european public policy, 31(8), 2099–2120.*
15. Fries, I., Greiner, M., Hofmeier, M., Hrestic, R., Lechner, U., Wendeborn, T. (2022). Towards a Layer Model for Digital Sovereignty: A Holistic Approach. *17th International Conference on Critical Information Infrastructures Security (CRITIS)*: proceedings 17th International Conference on Critical Information Infrastructures Security (CRITIS). Munich, *119–139.*
16. Magnus, R. (2020). Corporate personality rights on the internet and the applicable law. *Rabels zeitschrift fur auslandisches und internationales privatrecht, 84(1), 1–23.*
17. Cradduck, L. (2020). Legislating for Internet «Access» – ability. *Second international handbook of internet research.* New York, *647–668.*
18. De Gregorio, G., Stremlau, N. (2020). Internet Shutdowns and the Limits of Law. *International journal of communication, 14, 4224–4243.*
19. Thumfart, J. (2024). Digital Rights and the State of Exception. Internet Shutdowns from the Perspective of Just Securitization Theory. *Journal of global security studies*, *9(1)*. URL: https://academic.oup.com/jogss/article/9/1/ogad024/7515068?login=false
20. Strauch, R. (2024). Public opinion effects of digital state repression: How internet outages shape government evaluation in Africa. *Journal of information technology & politics*, *21, 479–492.*
21. Serna, F., Iniesta, J. (2018). The delimitation of freedom of speech on the Internet: the confrontation of rights and digital censorship. *Adcaij-advances in distributed computing and artificial intelligence journal*, *7(10), 5–12.* URL: https://revistas.usal.es/cinco/index.php/2255–2863/article/view/ADCAIJ201871512/19076
22. Pardo, F. (2022). Hate speech and freedom of expression in digital environments: social and legal implications. *Soletras*, *43, 178–196.*

23. Porcelli, A. (2019). (Des)advantages of the first legislation on the internet of things. *En letra, 11–12, 139–164.*
24. Tran, A. (2017). The Internet of Things and Potential Remedies in Privacy Tort Law. *Columbia journal of law and social problems, 50(2), 263–298.*
25. Monsees, L., Lambach, D. (2022). Digital sovereignty, geopolitical imaginaries, and the reproduction of European identity. *European security, 3, 377–394.*

Trofymenko Volodymyr Anatolevich, candidate of Legal Sciences, assistant professor, Department of Philosophy, Yaroslav Mudryi National Law University, Kharkiv, Ukraine.

CYBER SPACE AND THE STATE: INTERSECTION POINTS

The publication is dedicated to the state in cyberspace. An analysis is made of the main state approaches to cyberspace: classic – from the standpoint of traditional science and new – from the standpoint of interpreting cyberspace as a special sphere of regulation. There are three main prospective directions of interaction between the state and cyberspace: technical, political and economic. At the same time, attention is focused on the fact that despite existing regulatory gaps, only the state is able to carry out certain regulation of existing relations not only in the above, but also in other areas of cyberspace.

Keywords*: state, cyberspace, Internet, cyber sovereignty, digital sovereignty, freedom of speech, Internet of Things, legal regulation.*