УДК 340.12
DOI: 10.21564/2663-5704.53.258165

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

КІБЕРПРОСТІР ЯК ПРЕДМЕТ ФІЛОСОФСЬКОГО І ФІЛОСОФСЬКО-ПРАВОВОГО АНАЛІЗУ

Публікацію присвячено огляду наукових публікацій іноземних учених з тематики регулювання існування кіберпростору. Наголошується на зацікавленості іноземної науки цією сферою, з одного боку, та поки на відсутності єдиної стратегії дослідження кіберпростору, з іншого боку. Окремо звернено увагу на право людини на конфіденційність даних у кіберпросторі.

Ключові слова: *кіберпростір, міжнародні договори, права людини, правове регулювання, право на конфіденційність даних.*

Постановка проблеми. Людина продовжує свою експансію кіберпростору, переносячи до нього все більше нових сфер свого життя. Занурення до кіберпростору набуває таких обсягів, що все яскравішою стає проблема прав людини та їхнього захисту. У свою чергу, це ставить питання правового регулювання існування у кіберпросторі та можливостей держави в цьому аспекті. Актуальність, важливість та необхідність такого регулювання також підтверджується простотою вчинення злочинної діяльності та нерозвиненістю механізмів її попередження та придушення. Ускладнює ситуацію неможливість застосування традиційних захисних правових механізмів на теренах Інтернету. Правоохоронна система не врахувала швидкості розвитку кіберпростору та ступеня його впливу на людину. Вагома частина міжнародної правової спільноти сконцентрувалась на осмисленні цієї проблематики. Для України це питання набуває специфічного характеру: з її території поширюється велика кількість злочинів у кіберпросторі, вона знаходиться чи не на перших місцях за кількістю кіберзлочинів. Але варто наголосити на різниці у поглядах на зазначену проблематику вітчизняних та іноземних науковців.

Аналіз останніх досліджень та публікацій. Однією з найпоширеніших та популярних проблем, яка розробляється іноземними науковцями останнім часом, є з'ясування питання належності кіберпростору та, відповідно, способів впливу на нього. Німецький вчений Д. Ламбах [1] ставить питання фраг-

ментації кіберпростору. Він вважає, що фрагментування кіберпростору відбувається на основі традиційних уявлень про територію та державу. Базуючись на географічних знаннях, державні, корпоративні та приватні суб'єкти детериторизують та ретериторизують кіберпростір багатьма способами, що підкреслює актуальність досліджуваної проблеми.

На децентралізованості кіберпростору наголошує і науковець з Греції А. Ліаропулос [2]. Кіберпростір, на його думку, – це унікальна соціально-політична та технологічна галузь з унікальними характеристиками. Це створений людиною домен, що пропонує універсальне охоплення та доступ для своїх користувачів. Його децентралізований характер та той факт, що він переважно належить приватному сектору та керується ним, проблематизує, на думку вченого, питання про межі державного суверенітету та ефективного управління ним.

Відчуття небезпеки фрагментації кіберпростору веде до пропозицій підкорити його дії актів міжнародного права та Статуту ООН. Проблеми узгодженості світової спільноти в цьому питанні вивчає китайський вчений Дж. Дж. Венг [3]. На його переконання, у подальшому сформується система звичаєвого права і практики інтернет-компаній, що поступово набуде обов'язкового характеру.

Окремий наголос зроблено на необхідності визначення прав та обов'язків держави у кіберпросторі як на загальносвітовому, та і на регіональних рівнях. Таку пропозицію висуває македонський вчений М. Хаджи-Джанев [4]. Ця фундаментальна дискусія показує актуальність низки прикладних наукових питань, які будуть розглянуті нище.

У вітчизняній науковій думці ставлення до кіберпростору і до прав людини в кіберпросторі зокрема різниться. З одного боку, можна зустріти спрощені погляди на кіберпростір, де його основне призначення, як зазначає А. Бардінова, – «забезпечення простого, зручного і надійного доступу користувача до розподілених загальномережних ресурсів та організація їх колективного використання, обмін інформацією між усіма комп'ютерами мережі відповідно до їхньої класифікації» [5, с. 8]. Отже, кіберпростір розглядається лише як засіб забезпечення прав людини. Але інший, більш поширений погляд тлумачить кіберпростір як сферу, де людина має специфічні права або традиційні права, що вимагають осучасненого способу захисту. А існування самого кіберпростору необхідно врегулювати. Таку позицію поділяють як науковці, серед яких В. Фарушев [6], Ю. Хоббі [7], так і юристи-практики, наприклад А. Пальонко [8].

Формулювання цілей. Основна мета цієї публікації – показати ставлення до проблематики кіберпростору іноземних науковців та з'ясувати різницю в підходах до його розуміння серед представників вітчизняної науки.

Викладення основного матеріалу. Іноземні публікації з зазначеної тематики є дуже різноманітними за змістом та формою викладення. Переважна більшість апріорі визнає кіберпростір специфічною сферою, де людина є суб'єктом із певним набором прав.

Перехідною можна назвати статтю американського вченого М. Мончіпурі [5]. Автор демонструє, як розвиток кіберпростору, цифрових ідей та бачень впливає на формування політичного та соціального ландшафту на місцевому та глобальному рівнях. Стверджується, що нові технології прискорили соціальні зміни з технологічної та нормативної точок зору, і ці тенденції дуже важливо переосмислити з точки зору їхнього значення для всієї галузі прав людини. На цю ж проблему звертають увагу австралійські вчені М. Поблет та Дж. Коліб [6]. Сучасний кіберпростір, на їхню думку, надає безпрецедентних можливостей для розвитку і процвітання, але також становить низку нових загроз миру, безпеці та правам людини. Суспільство докладає великих зусиль з використання Інтернету в інтересах захисту прав людини. Однак надання інформації в реальному часі не дає захистити права людини, що може поставити під сумнів легітимність усього міжнародного правопорядку. Тому старі проблеми з захисту прав людини потребують інноваційних цифрових інструментів для їхнього вирішення.

Проблему створення системи регулювання кіберпростору порушує грецький вчений А. Ліаропулос [7]. Експерти з інформаційних технологій, юристи, стратеги та державні чиновники, зазначає автор, збагатили дискусію про природу кібербезпеки. Провідна тенденція – незалежно від її теоретичного походження – державоцентрична. Такий підхід правомірний, але одночасно неадекватний. Кібербезпека напряму пов'язана з загрозами критичній національній інфраструктурі, але не повинна обмежуватись традиційною концепцією національної безпеки. Мілітаризація дискурсу кібербезпеки спричинила дилему безпеки, що не враховує потреби людей. Тому проблеми кібербезпеки потрібно розглядати в контексті прав людини. Останніми роками методи інтернет-цензури розвиваються надзвичайно динамічно, що утворює загрозу для свободи, анонімності й захисту. Тому виникає потреба встановити режим управління кіберпростором, що відповідає нормам і стандартам у галузі прав людини.

До регулювання відносин у кіберпросторі звертається російський вчений С. Шахрай [8]. Автор констатує та аналізує проблеми, що пов'язані з невідповідністю швидкостей, за яких формується цифрове суспільство, та створенням ефективних соціальних (передусім правових) регуляторів нової реальності. Така ситуація диктує необхідність якнайшвидшого створення механізмів захисту людини, її прав у цифровому світі. Вчений порушує питання створення цифрового права та цифрової конституції, яка повинна забезпечити необхідну основу соціального порядку в кіберпросторі.

Не створювати спеціальні акти, а поширювати на кіберпростір державний суверенітет пропонує А. Ліаропулос [9]. Кіберпростір, зазначає дослідник, помилково характеризується як домен, що виходить за межі фізичного простору та, отже, виявляється несприйнятливим до державного суверенітету та стійкого міжнародного регулювання. Кіберпростір має свої унікальні особливості, але з іншими сферами (земля, море, повітря, космічний простір) підпадає під державний суверенітет. Хоча він не має кордонів та характеризується анонімністю, нещодавня державна практика доводить, що деякі його компоненти не захищені від суверенітету. Як приклад наводиться використання методів інтернет-фільтрації як авторитарними, так і демократичними режимами. Кіберпростір не має територіальності, але він не є і частиною природи, тобто створений і, відповідно, може бути зруйнований або врегульований людьми. Держави постійно підкреслюють своє право контролювати кіберінфраструктуру, розташовану на їхній території, та захищати її. Останніми роками зростає кількість країн, які оприлюднюють свою національну кіберполітику та створюють власні кіберцентри, метою яких є захист національної кіберструктури та контроль доступу громадян до інформації. Тому проблема суверенітету національного кіберпростору передбачає питання створення міжнародного кіберпорядку. Можливість існування держави, і не тільки, у кіберпросторі підтверджують і американські вчені Дж. Роуленд, М. Райс, С. Чиной [10]. Після Другої світової війни, зазначають дослідники, контроль над землею, морем, повітрям і космосом необхідний для демонстрації національної сили. За останні два десятиліття виникла галузь кіберпростору; це новий засіб для використання чотирьох інструментів влади – дипломатії, інформації, збройних сил та економіки. Поширеність кіберпростору підтримує практично миттєві дії в усіх галузях людської влади. Тому стверджується, що і держави, і недержавні органи можуть існувати, діяти, розвиватися і мати владу в кіберпросторі.

На інший аспект поширення державного суверенітету і прав людини у кіберпросторі звертає увагу ізраїльський вчений А. Беркес [11]. Відсутність контролю територіальної держави над частиною своєї фізичної території тісно пов'язано з порушенням прав людини в мережі, з одного боку, та обмеженим контролем держави над кіберпростором, з іншого боку. Попри відсутність ефективного територіального контролю, держава має право реалізовувати свій суверенітет як над територією, так і над кіберпростором. Автор стверджує, що територіальна держава, не маючи ефективних засобів для повного контролю свого кіберпростору, все одно зберігає свою юрисдикцію і, відповідно, зобов'язання по захисту прав людини в Інтернеті від протиправних дій, що виникають або мають місце у районі, який знаходиться за

межами ефективного контролю держави. Таким чином, наголошується на обов'язку держави в дотриманні прав своїх громадян в Інтернеті навіть на окупованих територіях.

Проблемі юрисдикції в кіберпросторі присвячено статтю італійської науковиці С. Керрі [12]. Авторка намагається витлумачити поняття юрисдикції таким чином, щоб воно охопило зобов'язання держави із захисту прав людини в кіберпросторі. Аналізуючи судову практику та норми міжнародного права, вчена доходить висновку, що гарантувати та забезпечувати права людини в кіберпросторі повинні держава, у якій проживає зацікавлена особа, а також держава, кіберінфраструктура якої використовується при порушенні прав людини. Таким чином, констатується поява багатосуб'єктної юрисдикції держав у галузі захисту прав людини в кіберпросторі.

Цікаву пропозицію подає на розсуд наукової спільноти американський науковець А. Гетенбі [13]. Автор зазначає, що комунікаційні та інформаційні технології створюють нові людські простори, віртуальні місця. Основою таких просторів та місць є не географічна складова, а множинність різних за змістом дискурсів, ідеологій та практик. Закони та правові концепції є центральною частиною цих просторів поряд із комп'ютерами та лініями зв'язку, що перетворює їх на соціальні простори. Соціальні простори – це продукти визначених ідеологій і практик, об'єднаних у динамічних відносинах, що являють собою зростаючу політичну, правову і соціальну владу. Мапу таких соціальних просторів у кіберсередовищі і пропонує створити науковець.

Розглядаючи кіберпростір як сферу, де можуть бути реалізовані, а також порушені права людини, західні науковці пропонують поширити на нього також юрисдикцію певних міжнародних організацій. Так, румунська правкиня А. Понта [14] розглядає можливості залучення кіберпростору до юрисдикції Організації безпеки і співробітництва в Європі (ОБСЄ). Як організація, що просуває права людини та попереджає конфлікти, ОБСЄ може відіграти важливу роль у підтримці введення в дію міжнародного права та його принципів у кіберпросторі. Наявні в кіберпросторі проблеми пропонується вирішувати на міжнародному рівні шляхом дотримання добровільних необов'язкових норм, погоджених країнами. ОБСЄ має за мету забезпечення стабільності та прозорості кіберпростору, зокрема на основі принципу належної обачності та зобов'язань держави в галузі прав людини.

Таким чином, можна побачити, що проблема правового регулювання кіберпростору, його внутрішньої побудови та місця людини як суб'єкта кіберпростору розглядається з різних боків. Але відчувається бажання науковців підлаштувати традиційні правові системи та правові інститути для кіберпростору шляхом розширення тлумачення основних правових категорій.

Другим вагомим напрямом, якому присвячено праці іноземних науковців, є проблеми конфіденційності та недоторканості даних в кіберпросторі. Зацікавленість науковців пояснюється поширеністю порушень цього права. Порушується проблема відповідності та ефективності вже наявних міжнародних стандартів захисту прав людини у кіберпросторі. Про це пише польський учений М. Рожчак [15]. Протягом багатьох років, зауважує дослідник, системи захисту прав людини сприймались як ефективні механізми зміцнення основних прав. Тим не менш у випадку діяльності, яка відбувається в кіберпросторі, захисні стандарти, що випливають з міжнародних договорів, здаються недостатніми. Попри динамічне розширення законодавства в галузі захисту даних, сфера застосування нинішніх стандартів залишається локальною – національною або регіональною, проте не глобальною. Тому необхідно розглянути питання про те, чи потребує досягнення рівного рівня захисту конфіденційності в кіберпросторі і фізичному світі нових правових механізмів, які не тільки долають обмеженість чинних міжнародних угод, але й підвищують довіру до глобального ринку даних, необхідного для розвитку сучасного суспільства. Намагаючись дати відповідь на це питання, автор робить висновок, що це є нагальною сучасною потребою.

На цю проблематику звертає увагу й англійська вчена Е. Ватт [16]. У той час, коли знижується відсоток очного масового стеження за людиною, пише авторка, дедалі більшою стає проблема невизначеності у тлумаченні права на недоторканність людини (відповідно до міжнародних нормативних актів) у контексті кіберпростору. Правники не можуть дійти консенсусу щодо цього. Тому дослідниця намагається зрозуміти право на недоторканність приватного життя в новітній час, а також розглядає численні порушення принципу екстериторіального застосування договорів про права людини, які відбуваються завдяки кібервідстеженням. Е. Ватт підтримує теорію «віртуального контролю», під якою розуміється панування держави та контроль за правами людини попри відсутність фізичного контролю над цією людиною. Учена впевнена: віртуальний контроль, що розуміється як віддалений контроль над правом людини на конфіденційність повідомлень, посприяє усуненню нормативної прогалини, яку дуже часто використовують спецслужби. Свій вихід пропонує американський вчений Дж. Канг [17]. Людина вже реалізує багато соціальних, економічних і політичних операцій через кіберпростір, пише науковець, а разом із покращанням технологій зростатиме їх кількість і якість. Але сама технологія відкриває можливості спостереження за нею. Широкомасштабне спостереження складає серйозну загрозу конфіденційності інформації, особливо персональних даних, які дуже часто використовуються в комерційних цілях. Але дуже часто використання персональної інформації викликає спротив людей. Як вийти

з цієї ситуації? Автор пропонує розглядати таку інформацію як товар, щодо якого зацікавлені сторони мають укласти договір. За відсутності угоди потрібно керуватися принципом «функціональної необхідності», згідно з яким використовується мінімально необхідний для угоди обсяг даних. Такий принцип науковець пропонує закріпити законодавчо.

Висновки. Велика кількість публікацій стосовно кіберпростору, його регулювання, захисту прав людини свідчить про підвищення цінності кіберпростору для людського суспільства. Аналізуючи іноземні публікації, можна відзначити таке:

1. Формуванню ефективних механізмів регулювання кіберпростору заважає швидкість його розвитку. Не маючи інших шляхів, вчені намагаються осучаснити та підлаштувати міжнародні стандарти, зокрема захисту прав людини, під його ознаки.

2. Кіберпростір є сферою, що може спричинити появу нових, раніше невідомих прав людини, що, у свою чергу, розширює галузь філософського та філософсько-правового дослідження цифрової культури.

3. На думку автора, сучасна наука, яка досліджує філософські та філософсько-правові проблеми кіберпростору, перебуває на певному перехресті: поширювати розвиток традиційних систем на кіберпростір чи створювати принципово нові підходи до розгляду.

4. Порівнюючи розробки вітчизняних та іноземних науковців, потрібно сказати наступне. Загалом усі наукові публікації мають теоретико-науковий характер, проте публікації іноземних вчених, як правило, завершуються прикладними рекомендаціями, що наближають до вирішення поставлених питань.

5. Загалом розмаїття наукових публікацій стосовно кіберпростору показує постійне зростання цінності його для людини.

ЛІТЕРАТУРА

1. Lambach D. The Territorialization of Cyberspace. *International studies review.* 2020. № 22 (3). P. 482–506.
2. Liaropoulos A. Exploring the Puzzle of Cyberspace Governance. 15th *European Conference on Cyber Warfare and Security (ECCWS-2016)*. (University of Piraeus, 2016). Piraeus, 2016. P. 198–204.
3. Wang G. G. Are there international rules governing cyberspace? *Journal of international and comparative law.* 2021. № 8 (2). P. 357–383.
4. Hadji-Janev M. Southeast European (SEE) States' International Legal Rights And Obligations In The Cyberspace. Conference on NATO *Advanced Training Course (ATC) on Terrorist Use of the Internet.* Ohrid, Macedonia, 2015. P. 149–160.
5. Бардінова А. Кіберпростір як засіб забезпечення прав людини і формування її самосвідомості. *Витоки педагогічної майстерності*. 2019. № 23. С. 5–9.

6. Фарушев В. М. Кіберпростір і інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності. *Інформація і право.* 2012. № 2 (5). С. 162–175.
7. Хоббі Ю. Право людини на кібербезпеку: проблеми визначення та гарантування. *Юридичний вісник*. 2020. № 2. С. 37–43.
8. Пальонко А. Проблеми захисту прав людини в інформсуспільстві. URL: https://yur-gazeta.com/publications/practice/inshe/problemi-zahistu-prav-lyudini-v-informsuspilstvi.html (дата звернення: 03.02.2022).
9. Monshipouri M. Human Rights in the Digital Age: Opportunities and Constraints. *Public Integrity*. 2017. № 19 (2). P. 123–135.
10. Poblet M., Kolieb J. Responding to human rights abuses in the digital era: new tools, old challenges. *Stanford journal of international law*. 2018. № 54 (2). P. 259–283.
11. Liaropoulos A. Cyber-Security: A Human-Centric Approach. *14th European Conference on Cyber Warfare and Security (ECCWS-2015)*. (University of Piraeus, 2015). Piraeus, 2015. P. 189–194.
12. Shakhrai S. Digital Constitution: Fundamental Rights and Freedoms of an Individual in a Totally Informational Society. *Herald of the Russian academy of sciences*. 2018. № 86 (6). P. 441–447.
13. Liaropoulos A. Exercising State Sovereignty in Cyberspace: An International Cyber-Order Under Construction? *8th International Conference on Information Warfare and Security (ICIW-2013).* (University of Piraeus, 2013). Piraeus, 2013. P. 136–140.
14. Rowland J., Rice M. and Shenoi S. Whither cyberpower? *International journal of critical infrastructure protection.* 2014. № 7 (2). P. 124–137.
15. Berkes A. Human Rights Obligations of the Territorial State in the Cyberspace of Areas Outside Its Effective Control. *Israel law review.* 2019. № 52 (2). P. 197–231.
16. Carrea S. The ECHR in the Cyberspace: Does the Power to Infringe Always Entail the Duty to Protect? *Diritti umani e diritto internazionale*. 2019. № 13 (1). P. 133–153.
17. Gaitenby A. Law's mapping of cyberspace: The shape of new social space. *Technological forecasting and social change.* 1996. № 52 (2-3). P. 135–145.
18. Ponta A. Legal instability in cyberspace and OSCE's mitigation role. *Juridical tribune-tribuna juridica.* 2021. № 11 (3). P. 411–429.
19. Rojszczak M. Does global scope guarantee effectiveness? Searching for a new legal standard for privacy protection in cyberspace. *Information & communications technology law.* 2020. № 29 (1). P. 22–44.
20. Watt E. The Role of International Human Rights Law in the Protection of Online Privacy in the Age of Surveillance. *9th International Conference on Cyber Conflict – Defending the Core (CyCon, 2017).* Tallin, 2017. P. 93–106.
21. Kang J. Information privacy in cyberspace transactions. *Stanford law review*. 1998. № 50 (4). P. 1193–1294.

REFERENCES

1. Lambach, D. (2020). The Territorialization of Cyberspace. *International studies review, 22 (3), 482–506.*

2. Liaropoulos, A. (2016). Exploring the Puzzle of Cyberspace Governance. *Cyber Warfare and Security*: proceeding 15th European Conference (ECCWS-2016). (University of Piraeus, 2016). Piraeus, *2016, 189–194*.
3. Wang, G. G. (2021). Are there international rules governing cyberspace? *Journal of international and comparative law, 8 (2), 357–383*.
4. Hadji-Janev, M. (2015). Southeast European (SEE) States' International Legal Rights And Obligations In The Cyberspace. *Conference on NATO Advanced Training Course (ATC) on Terrorist Use of the Internet:* proceeding Conference, Ohrid, Macedonia, *2015, 149–160*.
5. Bardinova, A. (2019). Kiberprostir yak zasib zabezpechennya prav lyudyny i formuvannya yiyi samosvidomosti. *Vytoky pedahohichnoyi maysternosti – The origins of pedagogical skills*, *23, 5–9* [in Ukrainian].
6. Farushev, V. M. (2012). Kiberprostir i informatsiynyy prostir, kiberbezpeka ta informatsiyna bezpeka: sutnist′, vyznachennya, vidminnosti. *Informatsiya i pravo – Information and law, 2 (5), 162–175* [in Ukrainian].
7. Khobbi, Yu. (2020). Pravo lyudyny na kiberbezpeku: problemy vyznachennya ta harantuvannya. *Yurydychnyy visnyk – Legal Bulletin, 2. 37–43* [in Ukrainian].
8. Pal′onko, A. Problemy zakhystu prav lyudyny v informsuspil′stvi. URL: https://yur-gazeta.com/publications/practice/inshe/problemi-zahistu-prav-lyudini-v-informsuspilstvi.html [in Ukrainian].
9. Monshipouri, M. (2019). Human Rights in the Digital Age: Opportunities and Constraints. *Public Integrity*, *19 (2), 123–135*.
10. Poblet, M., Kolib, Dzh. (2018). Responding to human rights abuses in the digital era: new tools, old challenges. *Stanford journal of international law*, *54 (2), 259–283*.
11. Liaropoulos, A. (2015). Cyber-Security: A Human-Centric Approach. *Cyber Warfare and Security*: proceeding 14th European Conference (ECCWS-2015). (University of Piraeus, 2015). Piraeus, *2015*, *189–194.*
12. Shakhray, S. (2018). Digital Constitution: Fundamental Rights and Freedoms of an Individual in a Totally Informational Society. *Herald of the Russian academy of sciences, 86 (6), 441–447* [in English].
13. Liaropulos, A. (2013). Exercising State Sovereignty in Cyberspace: An International Cyber-Order Under Construction? *Warfare and Security*: proceeding 8th International Conference (ICIW-2013). (University of Piraeus, 2013). Piraeus, *2013, 136–140*.
14. Roulend, Dzh., Rays M. ta Shenoy, S. (2014). Whither cyberpower? *International journal of critical infrastructure protection, 7 (2), 124–137*.
15. Berkes, A. (2019). Human Rights Obligations of the Territorial State in the Cyberspace of Areas Outside Its Effective Control. *Israel law review*, *52 (2), 197–231.*
16. Karrea, S. (2019). Human Rights Obligations of the Territorial State in the Cyberspace of Areas Outside Its Effective Control. *Israel law review*, *13 (1), 133–153.*
17. Gaitenby, A. (1996). Law's mapping of cyberspace: The shape of new social space. *Technological forecasting and social change*, *52 (2-3), 135–145.*
18. Ponta, A. (2021). Legal instability in cyberspace and OSCE's mitigation role. *Juridical tribune-tribuna juridica*, *11 (3), 411–429.*

19. Royshchak, M. (2020). Does global scope guarantee effectiveness? Searching for a new legal standard for privacy protection in cyberspace. *Information & communications technology law, 29 (1), 22–44.*
20. Vatt, E. (2017). The Role of International Human Rights Law in the Protection of Online Privacy in the Age of Surveillance. *Cyber Conflict – Defending the Core*: proceeding 9th International Conference (CyCon, 2017). Tallin, *2017, 93–106.*
21. Kan, Dzh. (1998). Information privacy in cyberspace transactions. *Stanford law review*, *50 (4), 1193–1294.*

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

CYBERSPACE AS A SUBJECT OF PHILOSOPHICAL AND PHILOSOPHICAL AND LEGAL ANALYSIS

The publication is devoted to a review of scientific publications of foreign scientists on the regulation of cyberspace. Emphasis is placed on the interest of foreign science in this field, on the one hand, and the lack of a unified strategy for the study of cyberspace, on the other hand. Special attention is paid to the human right to data confidentiality in cyberspace.

Keywords: *cyberspace, international treaties, human rights, legal regulation, right to data confidentiality.*

Трофименко Владимир Анатольевич, кандидат юридических наук, доцент, доцент кафедры философии Национального юридического университета имени Ярослава Мудрого, г. Харьков, Украина

КИБЕРПРОСТРАНСТВО КАК ПРЕДМЕТ ФИЛОСОФСКОГО И ФИЛОСОФСКО-ПРАВОВОГО АНАЛИЗА

Публикация посвящена обзору научных публикаций иностранных ученых по тематике регулирования существования киберпространства. Отмечается заинтересованность иностранной науки этой сферой, с одной стороны, и пока отсутствие единой стратегии исследования киберпространства, с другой стороны. Отдельно обращается внимание на право человека на конфиденциальность данных в киберпространстве.

Ключевые слова: *киберпространство, международные договоры, права человека, правовое регулирование, право на конфиденциальность данных.*