Вісник Львівського університету. Серія філос.-політолог. студії. 2020. Випуск 31, с. 189–195
Visnuk of the Lviv University. Series Philos.-Political Studies. Issue 31, p. 189–195

УДК [323.282+327.88]:004.738.5]:343.301
DOI https://doi.org/10.30970/PPS.2020.31.24

ТРУДНОЩІ ІНСТИТУЦІЙНОГО РЕГУЛЮВАННЯ ЦИФРОВИХ РИЗИКІВ У ТРАНЗИТНОМУ СУСПІЛЬСТВІ

Ольга Свідерська
Національний університет «Львівська політехніка»,
кафедра теоретичної та практичної психології,
вул. Ст. Бандери, 12, 79000, м. Львів, Україна

У статті порушується питання труднощів регулювання цифрових ризиків методами інституційного впливу. Зокрема, ставиться питання аналізу інформаційного простору й ролі у ньому політичних акторів. Доведено, що цифрова епоха зруйнувала раніше збудовану ієрархію, що своєю чергою призвело до нівелювання ролі інститутів, зокрема масової інформації. Визначено, що у сучасному суспільстві ключовою проблемою є ризик, котрий формується за допомогою різноманітних впливів: зовнішнього середовища, економічної ситуації, продукуванням хімічної й біологічної зброї, штучного інтелекту тощо. Окремим питанням, яке заслуговує детального наукового дослідження, є ті ризики, котрі формуються у цифровому форматі задля забезпечення політичного терору як у сфері зовнішньої, так і внутрішньої політики, котру ведуть держави стосовно своїх громадян. Одним із вагомих аспектів соціальних медіа є руйнування ними традиційної ієрархії інформації та медіа, і таким чином детермінування появи нового типу «суперпідсилених індивідуумів» – Homo digitalis. Досліджено, що транзитні суспільства, котрі за своєю суттю характеризуються нестабільністю, непевністю, є особливо вразливими до використання у них соціальних медіа як інструменту структурування політичної реальності. Визначено, що соціальні медіа, сформовані на основі соціальних мереж, мають амбівалентний вплив на політичну реальність, адже дають змогу двом конфліктуючим суб'єктам висвітлювати події таким чином, щоб формувати наратив відповідно до своєї потреби. Таке використання соціальних медіа сприяє викривленню інформаційного потоку, підміні фактів, поширенню дезінформації, що своєю чергою формує постправду. Доведено, що задля інформаційної безпеки громадян суспільства, котре перебуває у процесі демократичного транзиту, необхідно максимально врегулювати положення інтернет-протоколу, що суттєвим чином ускладнить довіру громадян до медіа, створить думку про обмеження прав і свобод, проте в кінцевому варіанті може слугувати засобом безпеки.

Ключові слова: цифрові ризики, транзит, інституційна система, кібервійська, терористичні організації, кіберзлочини.

Постановка проблеми. Труднощі інституційного регулювання небезпек, котрі пов'язані із цифровими ризиками сучасності, великою мірою зумовлені розвитком інформаційного суспільства й формуванням на його основі новітніх медіа. Розвиток соціальних мереж змушує переглянути особливості не тільки сучасного потоку інформації, але й врахувати ті важелі впливу на інформаційні наративи, котрі суттєвим чином формують судження звичайних громадян стосовно політичних реалій. Нині ні для кого не є секретом, що звичайна людина, котра вміло користується новітніми технологіями, може створити конкуренцію у політичних наративах проти своєї держави, адже кожен член суспільства – швидший, креативніший і позбавлений зайвої бюрократичної тяганини. За допомогою соціальних мереж створюється нова реальність, не обмежена горизонтом сприйняття, яка показує цілому світу позицію щодо того чи іншого політичного питання [11, с. 21].

Сучасне розуміння держави відкритого доступу формується внаслідок другої суспільної революції, в тому числі й використання технологій. Перехід між цими двома порядками передбачає цілу низку змін, у результаті яких політична система розширює участь громадян у політичному житті й гарантує їм безособові політичні права, створює прозоріші інститути, відповідальні за ухвалення рішень, і забезпечує законодавчу базу для широкого спектра організаційних форм від політичних партій до економічних організацій [8, с. 22]. Проте справедливості заради варто наголосити на тому, що постійний розвиток соціальних медіа й, відповідно, щоденне збільшення активних користувачів не лише сприяють відкритості суспільства: розквіт дестабілізуючих соціальних медіа збігається у часі із кризою Заходу, який починаючи з 2000-х років переживає системну дискредитацію великих інституцій [9, с. 28], але й зумовлюють процес використання від ліберально-демократичних до авторитарних держав тих самих методів, що й звичайні громадяни. Під керівництвом державних інститутів створюють акаунти у соціальних мережах, наймають на роботу блогерів чи армії кібертролів задля поширення того чи іншого наративу у маси, підтримання свого авторитету чи перемоги над суперником. Сучасність народжує новий тип людини – Homo digitalis, котрий може бути ефективнішим у інформаційній війні проти цілої держави, а його єдиною зброєю буде справна камера у сучасному ґаджеті і вільний доступ до Інтернету.

Особливо небезпечним Homo digitalis, вважає Д. Патрикаракос, є для авторитарних держав, які навіть більше ніж ліберальні демократії покладаються на контроль інформаційних потоків: «Не маючи монополії на ці потоки, держави вже не можуть демонструвати владу (особливо у ситуації війни або протесту) так, як це було можливе раніше» [9, с. 24]. І оскільки ці нові форуми соціальних медіа структурно більш рівноправні, багато хто захоплюється образом Інтернету як досконалого інструменту проти тиранів, проте, з іншого боку, цими методами досить часто користуються й терористичні угруповання чи держави-агресори задля перемоги в інформаційній війні. Окрім того, нині у групі ризику опиняються й транзитні суспільства, адже їх можна розглядати як етап політичного розвитку, в межах якого відбуваються якісні зміни, докорінні трансформації політичного режиму з метою консолідації демократії із дуже складним і часто непередбачуваним і непевним шляхом. Відповідно, у транзитному середовищі ми можемо спостерігати певний вакуум ідентичності, зумовлений передовсім кризою інституційної, ціннісної й ідеологічної систем та непевністю їхнього розвитку. Не складно собі уявити, яку суміш можуть створювати деструктивні використання новітніх медіа у транзитних суспільствах і з якими труднощами зіштовхується і без цього хитка інституційна система. Саме це зумовило формулювання мети нашого дослідження, а саме аналізу основних труднощів регуляції цифрових ризиків у сучасному суспільстві, зокрема транзитному.

Тематика цифрових ризиків починає активно розглядатись у науковому колі приблизно на рубежі XX–XXI століть, у час, коли починають активно використовувати інформаційний простір у віртуалізації політичних реалій. Ідеться як про організацію терористичних організацій, атак, кібервійськ, тролів, так і про активне використання державними інститутами соціальних мереж з метою формування того чи іншого електорального поля, проведення астротерфінгових операцій тощо. Основні напрацювання з цієї тематики відображено у наукових розвідках Норта, У. Бека, Е. Гіденса, Д. Гудмена, Р. Водак, серед українських учених її досліджували Т. Кремінь, Л. Дорош, Г. Почепцов, Ю. Горбань та ін.

Виклад основного матеріалу. Перебуваючи у процесі переходу від одного типу політичного режиму до іншого, транзитні суспільства постають перед проблемою подолання непевності суспільного розвитку й усвідомленого вибрання напряму руху. Вони

можуть досягнути бажаної демократії через інституалізацію непевності або ж потрапити у тривалий перехідний період та гібридизацію режиму, що характеризуються циклічними «відкочуваннями» від демократії через економічну неефективність, поширення популістських ідеологій, загострення безпекових проблем чи труднощі інституційного регулювання ризиків цифрового формату [13, с. 234]. Так, В. Банс акцентує на «подвійній непевності» перехідних суспільств – поєднання непевності результатів та непевності процедур [1, с. 47]. Такі суспільства самі по собі здатні формувати середовище трансформацій, в якому «події раптові, актори нетипові, ідентичності нестійкі, інститути не функціонують, підтримку неможливо прорахувати, вибір поспішний, а ризики неминучі і від них неможливо застрахуватися» [6, с. 10–11].

До слова, під інститутами розуміємо «правила гри», моделі взаємодії, які регулюють і обмежують відносини між індивідами: офіційні правила, формальні соціальні традиції, неформальні норми поведінки та спільні уявлення про світ, а також засоби впровадження того всього у життя [8, с. 35]. Та попри те, що для звичайної людини інститути можуть асоціюватися із обмеженнями поведінки, великою мірою вони дозволяють наперед визначати, як саме буде поводитися індивід у тій чи іншій ситуації. Можливість доступу до інформації активістами, незалежно від фінансових та інституційних можливостей, знижує залежність політичної активності від стабільних публічних інституцій. Ця ситуація може призводити до зростання нестабільності й непередбачуваності політичного процесу. Вочевидь, нові можливості та проблеми, породжені інформаційно-комунікативною революцією і сучасними технологіями Інтернету, будуть привертати увагу і цікавість наукової, політичної та економічної спільноти, а також широкої громадськості. Віртуальна реальність щодалі тим більше набуває масовості й бюджетності, за її допомогою ми маємо змогу не просто перебувати у кількох країнах одночасно, але й досить часто наше перебування засвідчене у середовищах, надто ризикованих для реальної фізичної присутності, на зразок зон бойових дій чи терористичних актів [7, с. 227].

Ризик, котрий щодня збільшується за рахунок накопичення різних видів: ядерного, екологічного, фінансового, воєнного, терористичного, біохімічного чи, зрештою – інформаційного, набув провідного фактору подальшого розвитку глобалізованого світу [2]. Згідно із переконаннями одного із провідних дослідників ризику У. Бека, будучи центральним у наукових розвідках сучасності, ризик може викликати у людей здебільшого три типи реакції: заперечення, притаманне культурі модерну, котра заперечує політичні ризики; апатію, котра формує лінію нігілізму, притаманну постмодерну, й, врешті – трансформацію, що фіксує проблему світового суспільства ризику шляхом усвідомлення насамперед відповідальності людства за варіативність свого майбутнього. Оцінка ймовірності того чи іншого ризику, на думку вченого, впливає на формування картини світу, що проявляється не лише у створенні нових форм і способів комунікації між людьми, а й у формуванні принципово нової стадії розвитку масової свідомості, умови життя й функціонування інститутів у сучасному суспільстві [2]. Посткласична парадигма політичного світу поставила вагоме питання про зняття самої категорії політичного простору в рамках класичного уявлення про національність держав, паралельно забезпечивши трансляцію національних символів і брендів у віртуальне поле у вигляді символічного та міфологічного капіталу національної культури.

Нині інтернет-технології є одним із потужних інструментів мобілізаційного потенціалу, котрий використовують транснаціональні терористичні організації, мирні жителі у спробі мобілізувати суспільство на допомогу один одному й інститути задля підтримки інституційного наративу серед мас. Прикладів цього є дуже багато: використання Twitter

у боротьбі ХАМАС та Ізраїлю, формування волонтерської допомоги під час російсько-української війни, котра почалась у 2014 і триває досі, спроба Ізраїлю протидіяти військовим наративам і т. д. Перш за все «використання Інтернету» в цьому разі означає не тільки використання комп'ютерів, підключених до глобальної мережі, а й використання нових засобів масової інформації (новітніх медіа). З одного боку, нові інтернет-медіа – інструмент, який підвищує ефективність традиційних способів дії як, наприклад, додатковий канал зв'язку (відкритий для збільшення масштабів діяльності або для більш ефективної координації масових дій). З іншого боку, йдеться про дії, що відбуваються лише в Інтернеті, наприклад, хакерство, поширення пропаганди, дезінформація, інформаційна війна. Власне, до діапазону фігурантів, відповідальних за кіберзлочини, належать: суверенні держави, місцеві хулігани, транснаціональні організовані злочинні угруповання, іноземні служби розвідки, хактивісти, військовослужбовці, кібервійська, проксі-бійці, які фінансуються державою, хакери-дилетанти, звичайні хакери, фрікери, кардери, крекери, незадоволені інсайдери, промислові шпигуни тощо [4, с. 37]. Як нами уже було раніше зазначено, використання інтернет-технологій є могутньою зброєю у руках держав-агресорів (яскравим прикладом цього є Росія) з метою формування військового наративу, впливу в інформаційній війні, маніпулювання свідомістю як власних громадян, так і тих, проти кого ведеться ця війна [10, с. 50].

На прикладі України можна виділити досить різноманітні кібератаки: кібершпигунство – викрадення документів задля надання їм розголосу й кібердиверсії проти об'єктів критичної інфраструктури (у 2015 році атакували Прикарпаттяобленерго, у 2016 році – Держказначейство та Мінфін, а у 2018 році вирував вірус Не Пєтя). Проте, як зауважують дослідники, основною метою таких дій у кіберпросторі є створення соціально-політичного хаосу: викликати паніку, створити умови для подальшої дезінформації [5, с. 19]. Звідси можемо акцентувати: децентралізовані технології дають змогу розпалити цикл насильства кому завгодно. На наш погляд, однією із причин труднощів інституційного регулювання таких цифрових небезпек є те, що доступ до віртуального середовища має занадто широка аудиторія користувачів. Тому практично кожен, хто має смартфон, справну камеру і є учасником соціальної спільноти здатен сам боротись проти інституцій, терору чи політичного насильства.

Однією з причин кризи демократичних інститутів і посилення авторитарних тенденцій у сучасному світі є вплив інформаційно-маніпулятивних технологій. Р. Водак пояснює ці процеси «розмиванням меж в політиці: для інтернет-користувача створюється реальність, яка йому видається впорядкованою і керованою, проте насправді – це оманлива проста ілюзія, котра підміняє собою реально складну й плюралістичну систему сучасних суспільств [3, с. 46]. Ці тенденції, які нерідко дестабілізують суспільні процеси у «нових» демократіях, привертають увагу до переосмислення проблем формування чи трансформації інституційного порядку в мінливому світі в межах транзитних процесів, з'ясування причин неефективності демократичних інституцій їх нездатності підтримувати згоду та діалог в інформаційному суспільстві, забезпечувати функціонування суспільної системи загалом [13, с. 235]. На думку Д. Патрикаракоса, Web 2.0 зумів наділити людей двома визначальними можливостями підриву урядової влади: по-перше, вони самі можуть активно створювати контент на платформах соціальних медіа, і по-друге, вони можуть формувати транснаціональні мережі [9, с. 21]. Згідно з класичним розумінням держави, вона має монополію на легітимне застосування насильства і, зрозуміло, контролю інформації, тому привілеї Web 2.0 дають можливість звичайному користувачу нівелювати цю функцію держави, виконувати самому роль регулювання наративу, котрий поширюється інфор-

маційним простором. Рівень небезпеки від такої перспективи не зменшується, а навпаки, посилюється ще більше.

Свого часу У. Ліппман, критикуючи технологічний оптимізм «епохи радіо», зазначав, що ідея поінформованих громадян, які відіграють роль колективних лідерів громадських думок, є утопією. Адже така ідея передбачає існування «надкомпетентних» індивідів, спонукає інформаційні й комунікативні медіа до виконання найскладніших функцій держави і громадянського суспільства. За У. Ліппманом, інформаційні медіа не спроможні «транслювати весь обсяг суспільного життя людства так, аби кожен індивід міг висловити компетентну думку з кожного питання» [12, с. 362]. Дещо схоже зустрічаємо у розвідках британського журналіста Д. Патрикаракоса, який стверджує, що соціальні медіа допомогли зруйнувати традиційну ієрархію інформації та медіа і таким чином спричинили появу нового типу «суперпідсилених індивідуумів» – Homo digitalis, унікального за своєю суттю явища XXI століття [9, с. 21]. Довіра людей до інституцій, котрі раніше були авторитетними, з активним використанням соціальних мереж та включеністю в інформаційні потоки поступово ще більше починає падати. Досить показовим це було під час формування волонтерських рухів для допомоги армії під час російсько-української війни. Втративши довіру до держави, люди намагались допомогти один одному, мобілізувавшись у соціальних мережах та створюючи волонтерські центри. Довіра до волонтерів була набагато вищою ніж до органів влади, адже все, на що витрачались гроші, мало строгу звітність, підтверджену численними дописами, відео та фотоповідомленнями у соціальних мережах.

Це була надзвичайно потужна лінія допомоги військовим, котра, звісно, сприяла державному регулюванню небезпеки, проте децентралізованою, позбавленою бюрократії, тому швидшою і мобільнішою. Йдеться не просто про купівлю харчів чи одягу, йдеться про купівлю автомобілів, у тому числі реанімаційних, комплектуючих для військової техніки тощо. Іншою лінією була онлайн-боротьба численної кількості інтернет-юзерів із проросійськими наративами, котрі поширювали антиукраїнські настрої, тому проводилась робота із відслідковування фейкових новин, їхнього спростування й знаходження правдивої інформації. Це триває й досі, проте усупереч об'єктивним намаганням тримати оборону російській пропаганді, таких користувачів у соціальних мережах досить часто називають «порохоботами». Ця боротьба є досить складною, з огляду на те, що агресор, котрий веде з Україною інформаційну війну, має надзвичайно потужні ресурси, спеціальні «ботоферми», котрі працюють над проєктами щодо дестабілізації політичної ситуації в Україні. А тому дає змогу говорити про негативний бік соціальних мереж, коли державні інститути, політичні партії використовують соціальні медіа задля поширення політичної пропаганди, забруднюючи тим самим цифрову інформаційну екосистему, пригнічуючи свободу слова як професійної преси, так і вчених чи науковців. Нині ми маємо інформаційне середовище, котре не є здоровим: «Ми живемо у світі, де факти менш важливі ніж наративи, де політики швидше заграють з емоціями свого електорату, ніж ведуть дебати, і де різного роду коди й алгоритми формують наш світогляд [9, с. 345]. Віртуальна реальність змінює саме значення правди у сучасній політиці, небезпечне воно передусім тим, що торкається дуже часто військових конфліктів. Відкритість доступу до Інтернету дає змогу традиційним організованим злочинним угрупованням перенаправляти зусилля й ресурси у віртуальний простір задля можливості отримати легкі прибутки, збільшити анонімність й обмежити інституційне втручання у їхню діяльність.

Нині ми маємо чимало доказів вербування до терористичних організацій шляхом комунікації через соціальні мережі. Справа дійшла до того, що експерти із досліджень тероризму [4, с. 43] почали трактувати Інтернет як «Університет терористів» – місце,

де є змога освоїти нові методи і навички задля збільшення ефективності у здійсненні терористичних атак, щоб досягати більшої ефективності в своїх атаках, збільшення фінансування, пропаганди своєї організації й розширення власного соціального капіталу. Окрім того, ще однією небезпекою є можливість для терористичних угруповань отримати доступ до Big Data. Поступово все наше життя перетворюється на систему знаків, кодів та шифрів. Втомлюючись щоразу вигадувати нові і нову паролі, ми починаємо використовувати один і той самий пароль на кількох серверах чи банківських картках, не задумуючись, що таким чином даємо шанс кіберзлочинцям відстежувати наші персональні дані. Цифрові ризики, пов'язані із всеосяжністю Інтернету та хмари, в якій він мешкає: величезна кількість пристроїв, підключених до Інтернету, створена для того, щоб збирати, передавати дані потоком, й зберігати їх у хмарі. Усе, що має стосунок до хмари і може бути вистеженим, рано чи пізно буде таким. Ми навіть не замислюємось над тим, наскільки пристрої, котрими ми користуємось щодня: електронна скринька, оплата комунальних послуг, місцезнаходження й реєстр дзвінків мобільного телефону, публічні камери, онлайн-магазини, кредитні картки, розпізнавання обличь на фото, соцмережі, пошукові браузери, трекери для фітнесу можуть сприяти розвитку терористичних організацій [7, с. 251].

Отже, попри те, що у глобалізованому світі, політична система здатна великою мірою розширювати політичну участь громадян, гарантуючи їм безособові права, створюючи прозоріші інститути, соціальні медіа є водночас платформою й інструментом як боротьби із цифровими й реальними ризиками, тоталітаризмом, політичним насиллям, так і розвитку численних терористичних угруповань шляхом формування відповідних наративів, вербування нових членів до терористичних організацій. Однією із нагальних потреб вважаємо необхідність інституційного врегулювання інформаційної політики соціальних мереж: створення відповідного протоколу, який би відповідав за інформаційну безпеку громадян. Для того потрібно поступово відновлювати довіру до інститутів, зміцнювати їхню позицію, змінювати постулати бюрократії і т. д. Проте варто й пам'ятати про те, що інколи зміцнення інститутів не є достатнім, адже проведення «демократичних» виборів не є ознакою, що у країні працюють демократичні інституції, а для того, щоб налагодилась ефективна співпраця між державою й громадянами, потрібне двостороннє дотримання правил, норм та законів.

Список використаної літератури

1. Банс В. Элементы неопределенности в переходный период. *Полис*. 1993. № 1. С. 44–51.
2. Бек У. Жизнь в обществе глобального риска – как с этим справиться: космополитический поворот. URL: https://www.gorby.ru/userfiles/lekciya_.
3. Водак Р. Политика страха. Что значит дискурс правых популистов? Харьков : изд-во «Гуманитарный Центр», 2018. 404 с.
4. Гудмен М. Злочини майбутнього. Харків : «Фабула», 2019. 592 с.
5. Деструктивні впливи та негативні наративи: інструменти виявлення та протидії: методичні матеріали / Д.В. Дубов, А.В. Баровська, Ю.К. Каздобіна. Київ : УФБС, 2020. 60 с.
6. Карл Т. Демократизация: концепты, постулаты, гипотезы. Размышления по поводу применимости транзитологической парадигмы при изучении посткоммунистических трансформаций. *Полис*, 2004. № 4. С. 10–11.
7. Келлі К. Невідворотне: 12 технологій, що формують наше майбутнє. Київ : «Наш формат», 2018. 340 с.
8. Норт Д., Волліс Дж., Вайнгест Б. Насильство та суспільні порядки. Основні чинники, які вплинули на хід історії. Київ : Наш формат, 2017. 352 с.

9. Патрикаракос Д. Війна у 140 знаках. Як соціальні медіа змінюють конфлікти у XXI столітті. Київ : Yakaboo Publishing, 2019. 352 с.
10. Свідерська О. Симулятивна компонента віртуальної масової політичної поведінки у суспільстві ризику. *Вісник Харківського національного університету імені В.Н. Каразіна. Сер.: Питання політології*. 2020. Вип. 37. С. 46–53. DOI: 10.26565/2220-8089-2020-37-07.
11. Сінгер П. Війна лайків. Зброя в руках соціальних мереж. Харків : Клуб Сімейного Дозвілля, 2019. 320 с.
12. Lippmann W. Public Opinion. NewYork. 1934. 362 p.
13. Sviderska O., Uhryn L. Institutional and socio-cultural of post-communist transformations. Research, challenges and development prospects in the area of social sciences : collective monograph. Riga : Izdevniecība "Baltija Publishing", 2020. 348 p. Pp. 234–252. DOI: https://doi.org/10.36059/978-9934-588-42-6/234-252.

DIFFICULTIES OF INSTITUTIONAL REGULATION OF DIGITAL RISKS IN THE TRANSIT SOCIETY

Olha Sviderska
Lviv Polytechnic National University,
Department of Theoretical and Practical Psychology
Stepana Bandera str., 12, 79000, Lviv, Ukraine

The article raises the issue of difficulties in regulating digital risks by methods of institutional influence. In particular, the issue of analysis of the information space and the role of political actors in it is raised. It is proved that the digital age destroyed the previously built hierarchy, which in turn led to the leveling of the role of institutions, including the media. It is noted that in modern society the key problem is the risk that is formed by various influences: the external environment, the economic situation, the production of chemical and biological weapons, artificial intelligence, etc. A separate issue that deserves detailed research is the risks that are formed in digital format to ensure political terror in both foreign and domestic policy pursued by states against their citizens. One of the important aspects of social media is the destruction of the traditional hierarchy of information and media, and thus the determination of the emergence of a new type of "super-enhanced individuals" – Homo digitalis. It has been studied that transit societies, which are inherently characterized by instability and uncertainty, are particularly vulnerable to the use of social media as a tool for structuring political reality. It was determined that social media is formed based on social networks are ambivalent impact on political reality, after allowing two conflicting entities cover events so as to form a narrative according to their needs. Such use of social media contributes to the distortion of information flow, substitution of facts, dissemination of misinformation, which in turn creates a post-truth. It is proved that for the information security of the citizens of the society, which is in the process of democratic transit, it is necessary to regulate the provisions of the Internet protocol, which will significantly complicate citizens' trust in the media, create an idea of restriction of rights and freedoms.

Key words: digital risks, transit, institutional system, cyber military, terrorist organizations, cybercrimes.