2. Бориславська О.М. Конституційна юрисдикція в умовах європейської моделі конституціоналізму. *Право України*. 2018. № 4. С. 93–107.

3. Бориславська О.М. Роль органу конституційної юрисдикції у формуванні в Україні системи конституціоналізму європейського зразка: до постановки проблеми. *Вісник Конституційного Суду України*. 2014. № 3. С. 62–71.

4. Речицький В. Конституціоналізм. Коротка версія: (читанка з конституціоналізму для зацікавлених). Харків: Права людини, 2014. 262 с.

5. Савчин М.В. Конституціоналізм і природа конституції: монографія. Ужгород: Поліграфцентр «Ліра», 2009. 372 с.

6. Lehideux and Isorni v. France, № (55/1997/839/1045, ECHR, URL: https://www.legal-tools.org/doc/2fed5c/pdf/

DOI https://doi.org/10.30525/978-9934-588-92-1-27

ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ ПРАВ ЛЮДИНИ І НАЦІОНАЛЬНОЇ БЕЗПЕКИ В УМОВАХ ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА

Роскошний І. В.
аспірант
Харківського національного університету імені В. Н. Каразіна
м. Харків, Україна

Бенджамін Франклін, один із батьків-засновників Сполучених Штатів Америки, одного разу заявив на Асамблеї штату Пенсільванія, що «ті, хто готовий пожертвувати наявною свободою заради малої частки тимчасової безпеки, не гідні ні свободи, ні безпеки» [1]. Це твердження зберігає свою істинність та актуальність і дотепер, оскільки основні права і свободи кожної людини мають бути захищені незалежно від часу, місця чи обставин. У XXI ст. загрози національній безпеці набувають якісно нових форм, відповідно розвиваються і загрози правам людини. Система захисту національних інтересів від небезпек змушена адаптуватися до нових викликів, тому на благо нації й з метою захисту її від загроз, як внутрішніх, так і міжнародних, держави змушені вдаватись до відповідних заходів. Цілком зрозуміло, що деякі з них мають правообмежувальний характер або, принаймні,

становлять потенційну загрозу основним правам таі свободам людини і громадянина. Тому треба завжди пам'ятати про ціну та ефективність таких дій. Саме в такий спосіб необхідно перевіряти вищезгадану тезу Франкліна і ставити найважливіше питання: яку ціну ми готові заплатити за нашу безпеку?

Інформаційне суспільство, або суспільство знань, котре прийшло на зміну індустріальному наприкінці XX століття, являє собою таке суспільство, в якому створення, використання і поширення інформації є найбільш важливою економічною, політичною, соціальною та культурною діяльністю. Економічну основу даного суспільства складають чотири взаємозалежні та взаємопов'язані елементи: 1) виробництво нових знань (здебільшого шляхом наукових досліджень); 2) передача нових знань через освіту і виховання; 3) поширення нових знань через інформаційно-комунікаційні технології (ІКТ); 4) використання нових знань в технологічних інноваціях для нових промислових процесів та послуг [2, с. 1].

Серед позитивних сторін інформаційного суспільства традиційно називають: універсальний доступ до інформації для всіх, прозорість та відкритість державної діяльності, електронну демократію, вдосконалення освіти та професійної підготовки, покращення рівня зайнятості, підтримку ринкової економіки, різні юридичні та соціальні вигоди і, нарешті, вдосконалення наукових досліджень і розробок. Втім, як слушно зауважує С. Петріна, «є спокусливим позиціонувати інформаційно-комунікаційні технології як творчий інструмент для вирішення криз у галузі прав людини в глобальній економіці, але здебільшого «права людини в глобальному інформаційному суспільстві» являють собою значно більш тверезий портрет» [3, с. 148]. Зокрема, прихильність до інформаційного суспільства – вимога, що отримала закріплення в Женевській декларації принципів 2003 р. [4] і стала основним принципом Декларації тисячоліття ООН [5], – загострила проблему державної та індивідуальної безпеки, оскільки вона протиставила її вимогам захисту прав людини активніше, ніж будь-коли.

Найбільш страшним породженням інформаційного суспільства стала поява кіберзлочинності. У Повідомленні Європейської комісії «На шляху до спільної політики по боротьбі з кіберзлочинністю» 2007 р. кіберзлочинність визначається як комплексне поняття, що охоплює три категорії кримінальних дій: 1) традиційні види злочинів (шахрайство, підробка документів тощо), котрі вчиняються з використанням електронних комунікаційних мереж та інформаційних систем; 2) розміщення незаконного контенту в електронних медіа; 3) атаки проти інформаційних систем, блокування програмного

забезпечення сайтів і хакерство [6]. Наведений перелік навряд чи можна назвати повним, але й він переконливо демонструє, наскільки загрозливим можуть бути здобутки інформаційного суспільства для основоположних прав і свобод людини і громадянина без надійних гарантій з боку національних держав і світової спільноти в цілому.

На жаль, важливі питання виміру безпеки – такі як секюритизація громадського порядку, забезпечення інтелектуальної власності в кіберпросторі та захист персональних даних – стали каменем спотикання для держав та їхніх правоохоронних і судових систем. З іншого боку, акти про свободу слова та право на інформацію доволі часто вступають у суперечність із вимогами інших правових актів, зокрема у сфері громадської безпеки, призводячи до зловживань, залежно від обставин, як з боку правоохоронних органів, так і з боку інституцій громадянського суспільства. Такі порушення виявляються або в надмірних заходах щодо охорони громадського порядку, котрі самі по собі можуть інтерпретуватися по-різному, або в недотриманні соціальної відповідальності з боку громадських активістів.

Названа проблематика суттєво ускладнюється з поширенням електронних соціальних мереж, використання яких передбачає наявність складних технологій, котрі дозволяють уникати суворого юридичного контролю як з боку держави, так і з боку громадянського суспільства. Серед основних ризиків інформаційного суспільства дослідники називають також: повсюдний вплив ІКТ на такі аспекти повсякденного життя людей, як виконання трудових обов'язків, побут і дозвілля; розшарування суспільства на нові класи – тих, хто багатий на інформацію, і тих, у кого інформації бракує; посилення контролю з боку правоохоронних органів за приватним життям людей; зростання кількості витончених злочинців, які можуть вкрасти персональні дані й величезні суми грошей за допомогою кіберзлочинів.

Тектонічні за своїми масштабами і руйнівні за своїми наслідками для прав і свобод громадян стали терористичні атаки в Нью-Йорку 11 вересня 2001 р.; вони радикально вплинули на життя та суспільство не тільки Сполучених Штатів, але й інших країн світу. Подальша реакція урядів на теракти призвела до прийняття законодавства та формування правоохоронних структур, які суттєво обмежували права людини в інформаційній сфері, включаючи право на недоторканність приватного життя, свободу слова та доступ до інформації. У міру того, як уряди рухались до захисту громадян від терористичних загроз та посилення національної й глобальної безпеки, баланс між безпекою і правами людини за багатьма аспектами змінився, причому не на користь останніх. Ці зміни, передусім, виявились у посиленні контролю за реалізацією громадянських свобод з точки зору забезпечення

національної безпеки. Інформація почала сприйматися в іншому світлі (принаймні в очах громадськості); стало зрозуміло, що інформацію можна прирівняти до зброї, яка може завдати шкоди будь-якій вільній, відкритій та демократичній державі. То ж не дивно, що широка громадськість почала охоче відмовлятися від деяких громадянських свобод в обмін на заходи національної безпеки.

При цьому слід наголосити, що режим обмежень і заборон, запроваджений у зв'язку з посиленням терористичних загроз, передусім з боку Аль-Каїди та її сателітів, не був скасований навіть після ліквідації Усами бен Ладена та звільнення території Сирії та Іраку від угруповань ІДІЛ. Зокрема, глобальних масштабів набуло відеоспостереження в публічних місцях, профілювання користувачів Інтернету, відстеження трафіку та місцезнаходження користувачів стільникового зв'язку (особливо в умовах пандемії COVID-19), блокування доступу користувачів до певного контенту, який вважається владою небезпечним, тощо.

Виправлення наявної ситуації та збалансування інтересів національної безпеки і прав людини вбачається у наступному:

1. Заходи, що запроваджуються в рамках забезпечення національної безпеки і становлять потенційну загрозу основним правам і свободам громадян, мають запроваджуватись тільки законом, бути прийнятними для демократичного суспільства і співмірними (адекватними) тим цілям, заради яких вводяться, і не знівельовувати сутність відповідних прав і свобод.

2. В умовах інформаційного суспільства перелік основних прав і свобод, що визнаються світовим співтовариством, має бути доповнений інформаційно-комунікаційними правами і свободами, серед яких право на інформацію, свобода доступу до мережі Інтернет, свобода інтернет-серфінгу та ін. Ці права мають отримати об'єктивацію (закріплення) як в національному праві (передусім, на рівні національних конституцій), так і в праві міжнародному (у вигляді окремого Пакту на зразок пактів 1966 р. чи принаймні Декларації інформаційно-комунікаційних прав).

3. Мають бути переглянуті принципові підходи до побудови систем забезпечення безпеки як на національному, так і на міжнародному рівнях: вони повинні стати «людиноцентричними», коли головним критерієм безпеки є забезпечення основних прав і свобод людини і громадянина. Національна безпека має починатись із безпеки людини, адже безпека людини можлива тільки за відсутності перешкод в реалізації її прав і свобод.

4. Зміцнення безпеки не може забезпечуватись за рахунок прав і свобод людини і громадянина. В іншому випадку політика конституційної держави втрачає ціннісні орієнтири, а відтак і втрачає сенс як така.

Література:

1. Votes and Proceedings of the House of Representatives, 1755-1756 (Philadelphia, 1756). P. 19–21. URL: http://franklinpapers.org/franklin/ framedVolumes.jsp?vol=6& page=238a .
2. Ziya Aktaş A. Information/Knowledge Society And Europe. *Proceedings of World Academy of Science, Engineering and Technology.* 2005. Vol. 8. P. 1–6.
3. Petrina S. Technology and (Human) Rights: A Review of Human Rights in the Global Information Society. *Workplace*. 2010. № 17. P. 147–149.
4. Построение информационного общества – глобальная задача в новом тысячелетии. Декларация принципов. Женева, 2003 год. URL: http://www.itu.int/net/wsis/outcome/ booklet/declaration_Bru.html.
5. Декларация тысячелетия Организации Объединенных Наций, утв. резолюцией 55/2 Генеральной Ассамблеи от 08.09.2000. URL: https://zakon.rada.gov.ua/laws/show/ 995_621#Text.
6. Communication from the Commission to the European Parliament, the Council and the Committee of the Regions of 22 May 2007 «Towards a general policy on the fight against cyber crime». Brussels, 22.5.2007. COM(2007) 267 final.

DOI https://doi.org/10.30525/978-9934-588-92-1-28

ДЕЦЕНТРАЛІЗАЦІЯ ПУБЛІЧНОЇ ВЛАДИ: ПОНЯТТЯ, ЗМІСТ, ОСНОВНІ ТЕНДЕНЦІЇ

Серьогін В. О.
доктор юридичних наук, професор,
професор кафедри конституційного і муніципального права
Харківського національного університету імені В. Н. Каразіна
м. Харків, Україна

Децентралізація означає передачу повноважень та відповідальності з центрального рівня врядування до виборних органів влади на субнаціональному рівні (регіональним органам, муніципалітетам тощо), котрі мають певний ступінь автономії. Децентралізація полягає також у переформатуванні (зміні конфігурації) відносин між центральним урядом та органами влади субнаціонального рівня у бік більш координаційної та стратегічної ролі національних урядів. Вона є