МЕХАНІЗМ ПУБЛІЧНОГО УПРАВЛІННЯ БЕЗПЕКОЮ ОСОБИСТОСТІ: ЯКІСНО-НОВИЙ ВИМІР У СИСТЕМІ ЦИФРОВИХ ТЕХНОЛОГІЙ ТА ІННОВАЦІЙ

THE MECHANISM OF PUBLIC PERSONAL SECURITY MANAGEMENT: A QUALITATIVELY NEW DIMENSION IN THE SYSTEM OF DIGITAL TECHNOLOGIES AND INNOVATIONS

УДК 351
DOI https://doi.org/10.32843/pma2663-5240-2022.30.15

Цимбал Б. М.
докторант навчально-науково-виробничого центру
Національний університет цивільного захисту України

У статті здійснено комплексне наукове обґрунтування та дослідження проблематики визначення сутності та особливостей механізму публічного управління безпекою особистості крізь призму якісно-нового виміру у системі цифрових технологій та інновацій.
Акцентовано увагу на тому, що право на безпеку особистості та виокремлення відповідних механізмів управління в умовах цифрової епохи може досліджуватися у двох парадигмах: «безпеки цифровізації» та «безпеки від цифровізації». Ці парадигми тісно пов'язані, оскільки ряд загроз і викликів збігаються або не можуть бути усунені без вирішення одного з цих завдань, однак штучне стимулювання цифровізації збільшує ризики. Як приклад можуть служити системи біометричної ідентифікації з імплантацією. Необхідно розробити основні параметри права людини на безцифрове довкілля, передбачити можливість зберегти традиційний, безцифровий спосіб життя. Цілком ймовірним є те, що існуюча система доктринально-інформаційного наповнення діючих механізмів публічного управління потребує перегляду та впровадження окремої доктрини цифрової безпеки, яка зафіксує загрози та ризики цифровізації суспільних відносин, допоможе визначити основні напрями державної політики у сфері забезпечення безпеки особистості, суспільства та держави в умовах цифровізації державного управління, економіки та права. Вона має координувати діяльність органів державної влади, місцевого самоврядування, інститутів громадянського суспільства, суб'єктів цифрового бізнесу, інформаційного середовища щодо створення системи гарантій безпеки в умовах цифровізації суспільних відносин, прогнозувати ризики та виклики, визначити поняття та механізми забезпечення цифрової безпеки, особливо щодо людини, сформулювати принципи застосування цифрових технологій у житті держави та суспільства. Обмеження та заборони необхідні для забезпечення безпеки особистості, суспільства, держави в умовах загальної цифровізації, що загрожує національному суверенітету, культурній ідентичності національної держави, демократії, так як, держава не повинна перетворюватися на «цифровий концтабір», суспільство – на «цифрову колонію», а людина – на «цифрову особистість». Ці обмеження мають бути закріплені законом, а також стати найбільш значущим та важливим розділом майбутнього розвитку нашої державності.

Ключові слова: *публічне управління, механізми публічного управління, людський фактор, безпека людини, управління безпекою людини.*

In the article, a comprehensive scientific substantiation and study of the issues of determining the essence and features of the mechanism of public management of personal safety is carried out through the prism of a qualitatively new dimension in the system of digital technologies and innovations.
Attention is focused on the fact that the right to personal security and the separation of appropriate management mechanisms in the conditions of the digital era can be studied in two paradigms: "security of digitalization" and "security from digitalization". These paradigms are closely related, as a number of threats and challenges overlap or cannot be eliminated without solving one of these tasks, but the artificial stimulation of digitalization increases the risks. As an example, biometric identification systems with implantation can serve. It is necessary to develop the basic parameters of the human right to a non-digital environment, to provide for the possibility of preserving a traditional, non-digital way of life. It is quite likely that the existing system of doctrinal and informational filling of existing mechanisms of public administration needs revision and implementation of a separate doctrine of digital security, which will record the threats and risks of digitalization of social relations, will help determine the main directions of state policy in the sphere of ensuring the security of the individual, society and the state in conditions of digitization of public administration, economy and law. It should coordinate the activities of state authorities, local governments, civil society institutions, digital business entities, the information environment regarding the creation of a system of security guarantees in the conditions of digitalization of social relations, forecast risks and challenges, define concepts and mechanisms for ensuring digital security, especially in relation to people , to formulate the principles of using digital technologies in the life of the state and society. Restrictions and prohibitions are necessary to ensure the safety of the individual, society, and the state in the conditions of general digitalization, which threatens national sovereignty, the cultural identity of the national state, democracy, since the state should not turn into a "digital concentration camp", society into a "digital colony", and a person – on "digital identity". These restrictions should be established by law, and also become the most significant and important part of the future development of our statehood.

Key words: *public administration, mechanisms of public administration, human factor, human security, human security management.*

Постановка проблеми у загальному вигляді. Ризики та виклики національної безпеки в епоху цифрового світу стають особливо явними в контексті цифрової глобалізації, під якою слід розуміти формування нового світового порядку, що конструюється та керується за допомогою цифрових технологій у єдності мережевої, комунікаційної та світоглядно-смислової структури. Видається правильним говорити в такому разі про цифрову безпеку як найважливіший елемент національної безпеки, але не в сенсі технологічного захисту інформації. Поняття «цифрова безпека» значно ширше, ніж його часто розуміють технічні фахівці, визначаючи її як комплекс заходів, спрямованих на захист конфіденційності, цілісності та доступності інформації від вірусних атак та несанкціонованого втручання, адже представляється, що такий підхід не враховує зміну парадигм суспільно-політичного розвитку України та світу загалом.

Вже в найближчому майбутньому поняття «цифрова безпека» ототожнюватиметься за смисловим обсягом із поняттям «національна безпека» – у цьому слід бачити наслідки цифрової глобалізації, цифрової революції, зміни технологічних вимірів. Національна держава поступово перестає сприйматися як основний гарант безпеки людини, більшу частину свого життя, що проводить у цифровій реальності, позбавленої звичних культурних і територіальних кордонів, тоді як саме безпека була ідейно-смисловим фундаментом концептуального оформлення буржуазної держави у вигляді доктрини правової держави та суспільного договору, що укладається з метою забезпечення безпеки кожної людини. Відтак, публічне управління безпекою особистості набуває особливого значення в контексті розвитку та провадження цифрових технологій та інновацій.

Аналіз останніх досліджень і публікацій. Теоретико-прикладні аспекти дослідження людського фактору в системі публічного управління знайшли своє відображення у наукових працях багатьох вчених, зокрема таких як: О. Бородіна, Н. Голікова, Е. Денісон, С. Кузнець, Р. Лукас, Р. Сміт, Р. Солоу, Л. Туроу, І. Фішер, А. Чухно, Т. Шульц. Водночас, питання пов'язані із комплексним науковим обґрунтуванням та дослідження сутності й особливостей механізму публічного управління безпекою особистості крізь призму якісно-нового виміру у системі цифрових технологій та інновацій ще не отримали належного теоретико-прикладного обґрунтування та аналізу.

Внаслідок чого **метою** даної статті є наукове обґрунтування та дослідження проблематики механізму публічного управління безпекою особистості крізь призму якісно-нового виміру у системі цифрових технологій та інновацій.

Виклад основного матеріалу. У сучасній науковій літературі більш звичним при обговоренні проблем безпеки людини, суспільства та держави у контексті цифровізації є термін «інформаційна безпека», однак його виникнення та використання не асоціюється з формуванням абсолютно нового цифрового світу та нової людини, не пов'язане з новим світоглядом. Інформаційна безпека – це стан захищеності особистості, суспільства та держави від внутрішніх та зовнішніх інформаційних загроз, при якому забезпечуються реалізація конституційних прав і свобод людини та громадянина, гідна якість та рівень життя громадян, суверенітет, територіальна цілісність та стійкий соціально-економічний розвиток, оборона та безпека держави [1, с. 105–106].

В той же час, термін «цифрова безпека» вже прокладає собі дорогу у вітчизняній науці у зв'язку з дослідженням раніше невідомих науці цифрових об'єктів. У зарубіжній науковій літературі термін «цифрова безпека» давно використовується для позначення різноманітних аспектів захищеності у цифровому середовищі особистості та державних інститутів. Цифрова безпека є режимом захищеності людини та суспільства, а також держави від загроз, що виникають в умовах нового цифрового технологічного устрою, у тому числі викликаних використанням цифрових технологій у державному управлінні, цифровізацією економіки, освіти, медицини та інших сфер освіти й приватного життя [2, с. 14]. Цифрові технології – це не лише мережеві технології передачі інформації, а й розвиток штучного інтелекту, цифрової електроніки, біометрії, стільникового зв'язку, телемедицини, смартміст, навігації, робототехніки та багато іншого. Все перераховане робить поняття цифрової безпеки більш об'ємним та універсально-конотативним: термін «інформаційна безпека» звично асоціюється з кібертероризмом, вірусами, екстремізмом [3, с. 60].

В той же час, варто звернути увагу на те, які ризики для національної безпеки несе цифровізування в умовах тренду світового розвитку, що зберігається, на глобалізацію. Здається, мову слід вести вже не просто про глобалізацію, оскільки спроби глобалізувати світ давно реалізуються під різними ідейними обґрунтуваннями (наприклад, імперська ідея Стародавнього Риму), а про цифрову глобалізацію, оскільки в умовах цифровізації суспільства і держави слід сказати про зовсім нове в історії людства явище. Ще десять років тому

цифрові потоки не мали істотного впливу на зростання ВВП, тоді як сьогодні вони впливають на нього більше, ніж багатовікова торгівля товарами. Глобалізоване цифрове суспільство породжує інноваційні стратегії управління, сфери та тенденції розвитку культури, економіки, права, торгівлі і навіть мислення. І не завжди ці стратегії призводитимуть до позитивних для людини та держави результатів. Національна держава певною мірою базується на цінностях традиційної національної культури, національно-культурної ідентичності, тому сучасні вітчизняні вчені та публіцисти так стурбовані, відсутністю національної ідеї та державної ідеології. У світоглядному сенсі цифрова глобалізація несе загрозу для держави втрати традиційних моральних цінностей, тому що формальний раціоналізм в умовах цифрового суспільства стає основним інструментом і критерієм правильності прийнятих рішень, тоді як традиційні цінності мають раціональний характер, що базуються на вірі в Бога, жертовності людини особистими інтересами в ім'я інтересів суспільства тощо [4, с. 296].

Як відомо, сьогодні ідентифікація особи здійснюється або за біометричними ознаками людини, або за допомогою спеціальних пристроїв, у тому числі імплантованих. Загальний та обов'язковий для всіх збір біометричних параметрів людини для зберігання та ідентифікації неприпустимий з точки зору прав людини на приватне життя: принцип добровільності, точніше принцип «недоторканності приватного життя, неприпустимість збору, зберігання користування та розповсюдження інформації про приватне життя особи без її згоди», закріплений у діючому законодавстві України, який в умовах цифрового суспільства та держави стає основоположним з погляду перешкоджання цифровим формам тотальної диктатури [5, с. 31].

Слід звернути увагу на загрози безпеці людини, дегуманізації та технократизації правозастосування, що виникають у зв'язку з впровадженням штучного інтелекту у правозастосовчу діяльність. Цей шлях розвитку права та правосуддя лише посилюватиме недоліки явно помилкового, позитивістського сприйняття права, формально-догматичного праворозуміння. І річ тут не в тому, що з погляду штучного інтелекту норми права в тоталітарній державі нічим не відрізняються від норм, закріплених у сучасних соціальних державах, наприклад, Данії чи Фінляндії [6, с. 36].

Ще в середині XX ст. вчені фіксували кризу права: юридичний формалізм став панувати над змістовною гранню права. Задовго до цифровізації представники західної інтелектуальної еліти фіксували наростаючу кризу європейської традиції права, викликаний надмірною формальною раціональністю, механістичним світосприйняттям права та правосуддя, домінуванням формальної законності над справедливістю.

Відомий історик права Г. Дж. Берман зазначає, що людина перебуває у гущі безпрецедентної кризи правових цінностей та правового мислення, так як право сприймається все більше як «каша з миттєвих рішень і норм, що суперечать один одному, поєднаних тільки загальними прийомами та юридичною технікою. Розквіт і панування юридичного формалізму слід розглядати як процес відчуження людини від права. Його також можна вважати «переродженням формальної раціональності»: формально-раціональний початок, зобов'язаний своєю появою проблемі пошуку справедливості «незважаючи на особу» в рамках «здорового» формалізму, покликаного як засіб забезпечити справедливість на початках рівності, обернувся і зайняв місце мети, тобто досягнення цієї справедливості [7, с. 144].

Об'єктивність у правозастосуванні за допомогою штучного інтелекту досягти неможливо і не потрібно, оскільки система правових норм є перш за все системою цінностей, захищених цими нормами. До того ж ця система має ієрархічний характер, що передбачає постійне зіставлення засобів і цілей, тобто цілепокладання, оцінку, суб'єктивність [8, с. 128]. Саме досягнення об'єктивності передбачається використанням штучного інтелекту у правозастосовчому процесі. Але річ у тому, що можливість використання штучного інтелекту на сучасному етапі його проектування, точніше сказати, обґрунтування цієї можливості та межі його використання мають бути пов'язані з вивченням етимологічних характеристик правового мислення, логічних аспектів правозастосовної діяльності з логічним аналізом правового мислення, правозастосовного пізнання [9, с. 94]. Таким чином, практично завжди правозастосування супроводжується неусвідомленим, не видно поверхневим поглядом, неявним правотворчістю, якого штучний інтелект здійснювати не може. Неявна правотворчість потрібна під час осмислення норми права у зв'язку з конкретною ситуацією. У даному процесі відбувається конкретизація норми, яка є народженням у правосвідомості правозастосовника норми, що конкретизує норму вищого порядку, яка має загальний характер до повністю тотожних та ідентичних даному конкретному випадку ситуацій [10, с. 390]. Доки люди не перетворяться на повністю ідентичні, однакові «біороботи», зберігатиметься

колізія між абстрактною нормою та конкретними життєвими обставинами, між типовістю та індивідуальністю [11, с. 299].

Висновки. Таким чином, можна зробити висновок, що право на безпеку особистості та виокремлення відповідних механізмів управління в умовах цифрової епохи може досліджуватися у двох парадигмах: «безпеки цифровізації» та «безпеки від цифровізації». Ці парадигми тісно пов'язані, оскільки ряд загроз і викликів збігаються або не можуть бути усунені без вирішення одного з цих завдань, однак штучне стимулювання цифровізації збільшує ризики. Як приклад можуть служити системи біометричної ідентифікації з імплантацією. Необхідно розробити основні параметри права людини на безцифрове довкілля, передбачити можливість зберегти традиційний, безцифровий спосіб життя. Цілком ймовірним є те, що існуюча система доктринально-інформаційного наповнення діючих механізмів публічного управління потребує перегляду та впровадження окремої доктрини цифрової безпеки, яка зафіксує загрози та ризики цифровізації суспільних відносин, допоможе визначити основні напрями державної політики у сфері забезпечення безпеки особистості, суспільства та держави в умовах цифровізації державного управління, економіки та права. Вона має координувати діяльність органів державної влади, місцевого самоврядування, інститутів громадянського суспільства, суб'єктів цифрового бізнесу, інформаційного середовища щодо створення системи гарантій безпеки в умовах цифровізації суспільних відносин, прогнозувати ризики та виклики, визначити поняття та механізми забезпечення цифрової безпеки, особливо щодо людини, сформулювати принципи застосування цифрових технологій у житті держави та суспільства. Обмеження та заборони необхідні для забезпечення безпеки особистості, суспільства, держави в умовах загальної цифровізації, що загрожує національному суверенітету, культурній ідентичності національної держави, демократії, так як, держава не повинна перетворюватися на «цифровий концтабір», суспільство – на «цифрову колонію», а людина – на «цифрову особистість». Ці обмеження мають бути закріплені законом, а також стати найбільш значущим та важливим розділом майбутнього розвитку нашої державності.

ЛІТЕРАТУРА:

1. Ковальчук К. Ф. Інноваційно-інвестиційна політика сталого розвитку регіонів України: від теорії до практики. Донецьк : ІМА-прес, 2012. 214 с.

2. Бакуменко В. Д. Теоретичні та організаційні засади державного управління. Київ : Видавництво НАДУ, 2003. 210 с.

3. Грабар Н. С., Хмиров І. М. Становлення та трансформація механізмів державного управління (на прикладі управління інтелектуально-інноваційними ресурсами економіки в Україні). *Вісник НУЦЗУ. Серія : Державне управління.* 2021. Вип. 1(14). С. 58–65.

4. Грішнова О. А. Людський розвиток : навч. посіб. Київ : КНЕУ, 2006. 308 с.

5. Ларіна Я., Брацлавська О. Розвиток людського капіталу в умовах глобалізації. Київ : ВЦ «Академія», 2012. 248 с.

6. Ковальчук В. Інвестування в людський капітал як фактор інноваційного розвитку економіки України. *Соціально-економічні проблеми і держава*. 2016. Вип. 2(15). С. 33–40.

7. Надобко С. В. Інтелектуальна власність як об'єкт адміністративно-правової охорони. *Експерт: парадигми юридичних наук і державного управління.* 2020. № 3(9). С. 141–149. URL: https://doi.org/10.32689/2617-9660-2020-3(9)-141-149

8. Смелянцев А. П. Сутність феномену загроз інтересам безпеки України. *Наук. записки Харків. військового ун-ту. Соціальна філософія, педагогіка, психологія*. Харків : ХВУ, 2000. Вип. VIII. С. 127–130.

9. Гошовська В. А. Соціальна домінанта національної безпеки. *Стратегічна панорама*. 2003. № 2. С. 94–99.

10. Janeček V. Ownership of personal data in the Internet of Things. *Computer Law & Security Review*. 2018. Vol. 34. Iss. 5. URL: https://doi.org/10.1016/j.clsr.2018.04.007

11. Kadar M., Moise I. A., Colomba C. Innovation Management in the Globalized Digital Society. *Procedia − Social and Behavioral Sciences*. 2014. Vol.143.https://doi.org/10.1016/j.sbspro.2014.07.560