DOI: https://doi.org/10.37634/efp.2025.3.12
УДК 342.7

Олександр Валерійович ***ЛІХОТА***
к.е.н., доцент кафедри, Північноукраїнський інститут імені Героїв Крут МАУП
ORCID: https://orcid.org/0000-0003-2948-4902
e-mail: a-lihota@ukr.net

ЗАКОНОДАВЧЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ ПОЛІТИКИ США

У статті проаналізовано історичний розвиток та сучасний стан законодавчого забезпечення інформаційної політики США в умовах цифрової трансформації. Розглянуто основні закони, що регулюють свободу слова, захист даних, кібербезпеку та діяльність медіаплатформ. Проаналізовано роль Федеральної комісії зі зв'язку (FCC), Федеральної торгової комісії (FTC) та інших державних органів. Досліджено вплив міжнародної співпраці, зокрема з ЄС. Виокремлено загрози, пов'язані з соціальними мережами та алгоритмічною модерацією контенту. Запропоновано шляхи вдосконалення інформаційної політики США для збалансування свободи слова, безпеки та державних інтересів.

Ключові слова: *інформаційна політика США, законодавче регулювання, свобода слова, захист персональних даних, дезінформація, кібербезпека, цифрові технології, державне регулювання*

ВСТУП

Інформаційна політика є однією з ключових складників національної безпеки, державного управління та економічного розвитку США. Вона регулює доступ до інформації, захист персональних даних, забезпечення свободи слова, кібербезпеку, а також діяльність засобів масової інформації та цифрових платформ. Законодавче забезпечення цієї сфери базується на Конституції США, федеральних законах, рішеннях Верховного Суду, а також на регулятивних актах, що ухвалюються на рівні федеральних агентств.

В умовах цифрової трансформації, зростання обсягу оброблюваних даних та активного розвитку технологій, таких як штучний інтелект (ШІ) і блокчейн, правове регулювання інформаційної політики США постійно змінюється та адаптується. Особливого значення ця сфера набула у зв'язку з поширенням соціальних мереж, стрімким збільшенням обсягів персональних даних, розвитком Інтернет-торгівлі та глобалізацією інформаційних потоків.

Однією з головних проблем інформаційної політики є баланс між захистом прав громадян на приватність та потребою держави в інформаційній безпеці. Наприклад, правоохоронні органи США мають широкі повноваження у сфері моніторингу цифрового середовища для боротьби з кіберзлочинністю та тероризмом. Водночас захист персональних даних споживачів стає все більш актуальним питанням у зв'язку з діяльністю великих технологічних компаній (Big Tech), таких як Google, Facebook (Meta), Amazon та Microsoft.

Сучасні глобальні виклики, такі як поширення дезінформації, маніпуляція громадською думкою через цифрові платформи, збільшення масштабів кібератак та невизначеність стосовно ролі держави у регулюванні соціальних мереж, вимагають глибокого дослідження законодавчої основи інформаційної політики США.

Аналіз законодавчого забезпечення цієї сфери дає змогу зрозуміти:

– якими механізмами держава забезпечує баланс між свободою інформації та необхідністю контролю інформаційних потоків;

– як відбувається захист персональних даних у США на законодавчому рівні;

– які основні принципи кібербезпеки визначено в американському законодавстві;

– як регулюється діяльність медіа та цифрових платформ у контексті інформаційної політики США.

Вивчення цієї теми також має практичне значення для інших країн, зокрема для України, яка розбудовує власну інформаційну політику, враховуючи досвід провідних держав світу.

Законодавче забезпечення інформаційної політики США є предметом численних наукових досліджень та публікацій. Серед провідних авторів, які зробили вагомий внесок у вивчення цієї тематики, варто відзначити:

– Лоуренса Лессіга, який досліджує правові аспекти регулювання цифрових платформ та авторського права у США [11, с. 85-92];

– Кесса Санстейна, який аналізує проблему інформаційних потоків, фільтраційних бульбашок та дезінформації у цифрову епоху [19, с. 144-157];

– Джеффрі Стоуна, що досліджує питання свободи слова та конституційних обмежень у США [18, с. 201-219];

– Даніеля Солова, який вивчає аспекти конфіденційності та правового регулювання захисту персональних даних у США [17, с. 89-103];

– Тіма Ву, що досліджує проблеми монополізації інформаційного ринку та необхідність антимонопольного регулювання цифрових платформ [25, с. 176-192];

– Френка Паскуале, який аналізує правові виклики алгоритмічного управління інформацією та ШІ [13, с. 211-226];

– Брюса Шнайера, який досліджує питання кібербезпеки, цифрової конфіденційності та загроз з боку державних і приватних акторів [16, с. 122-137].

– Шошану Зубофф, яка досліджує феномен «капіталізму спостереження» та його вплив на інформаційну політику [26, с. 263-281].

У дослідженні також враховано аналітичні матеріали урядових та незалежних дослідницьких центрів, зокрема Національного інституту стандартів і технологій (NIST) [12], Brookings Institution [1], RAND Corporation [15] та Electronic Frontier Foundation [6], які висвітлюють питання державного регулювання цифрових технологій та інформаційної безпеки.

Проте питання адаптації законодавства до стрімкого розвитку технологій, зокрема ШІ, а також проблеми ефективного регулювання діяльності цифрових платформ та

забезпечення кібербезпеки, залишаються недостатньо вирішеними і потребують подальшого дослідження.

МЕТА статті – комплексний аналіз законодавчого забезпечення інформаційної політики США, зокрема її основних нормативно-правових засад, механізмів державного регулювання та ключових викликів у контексті цифрової трансформації. У дослідженні розглянуто роль державних органів у формуванні інформаційної політики, а також проаналізовано сучасні загрози, включаючи дезінформацію, кібербезпеку, алгоритмічне регулювання контенту та втручання у приватність громадян.

МЕТОДИ ДОСЛІДЖЕННЯ

Для досягнення мети статті застосовано комплексний підхід, що включає:

– аналіз першоджерел: Конституції США, федеральних законів та підзаконних актів, що регулюють інформаційну політику;

– вивчення наукової літератури: огляд праць провідних американських дослідників у галузі інформаційного права, кібербезпеки та захисту даних;

– контент-аналіз: аналіз звітів урядових установ та незалежних дослідницьких центрів США;

– порівняльний аналіз: зіставлення законодавства США з правовими нормами інших країн, зокрема ЄС (GDPR).

РЕЗУЛЬТАТИ

Комплексний аналіз законодавчого забезпечення інформаційної політики США дає змогу виділити три взаємопов'язані рівні регулювання: конституційні основи, спеціальні законодавчі акти та сучасні виклики, що потребують адаптації законодавства.

Конституційні основи інформаційної політики США

Законодавче регулювання інформаційної політики США спирається на міцний фундамент, закладений Конституцією. Ключовими тут є положення, що гарантують свободу слова та захист приватності.

– Перша поправка (1791) є наріжним каменем регулювання інформаційних відносин. Вона не лише гарантує свободу слова, друку, зібрань і релігії, але й згідно з тлумаченням Верховного Суду забезпечує широкий доступ до інформації [21, с. 12; 27, с. 158-159]. Це створює презумпцію відкритості інформації, що обмежує можливості держави стосовно цензури та контролю за поширенням ідей. Наприклад, судова практика стосовно Першої поправки неодноразово підтверджувала, що обмеження свободи слова допускаються лише у винятькових випадках, коли є явна та безпосередня загроза суспільній безпеці.

– Четверта поправка, гарантуючи право громадян на приватність і захист від необґрунтованих обшуків і вилучень, закладає основи для регулювання збору та використання персональних даних [22, с. 25; 27, с. 158-159]. Це особливо важливо в епоху цифрових технологій, коли збір інформації про громадян став повсюдним. Наприклад, суперечки навколо програм масового стеження, розкритих Едвардом Сноуденом, показали, наскільки складним є пошук балансу між національною безпекою та правом на приватність, гарантованим Четвертою поправкою.

– П'ята поправка, що передбачає право особи не свідчити проти себе, також відіграє важливу роль у захисті цифрової інформації [20, с. 33; 27, с. 158-159]. Це право застосовується до захисту паролів, шифрування даних та інших заходів, що забезпечують конфіденційність електронних комунікацій. Наприклад, суперечки між ФБР та компанією Apple про розблокування iPhone терориста показали, наскільки важливим є право на захист особистої інформації, навіть у контексті розслідування злочинів.

Так, Конституція США створює систему стримувань і противаг, що обмежує повноваження держави у сфері контролю за інформацією та захищає права громадян.

Ключові законодавчі акти, що регулюють інформаційну політику США

Конституційні принципи деталізуються та розвиваються у спеціальних законодавчих актах, що охоплюють різні аспекти інформаційної політики.

Доступ до інформації:

– Закон про свободу інформації (FOIA, 1966) є ключовим інструментом забезпечення прозорості діяльності державних органів. Він надає громадянам та журналістам право запитувати та отримувати доступ до документів, що зберігаються в державних установах [10, с. 52]. Це право не є абсолютним і має винятки, пов'язані з національною безпекою, захистом комерційної таємниці та приватного життя. Однак, FOIA відіграє важливу роль у забезпеченні громадського контролю за діяльністю влади та сприяє боротьбі з корупцією.

– Закон про класифіковану інформацію (1982) встановлює чіткі процедури для визначення, зберігання та розсекречення інформації, що становить державну таємницю [3, с. 77]. Він забезпечує баланс між необхідністю захисту національної безпеки та правом громадян на доступ до інформації. Наприклад, цей закон регулює процедури розсекречення документів, що мають історичну цінність, але можуть містити інформацію, яка раніше вважалася секретною.

Захист персональних даних:

– Закон про конфіденційність (Privacy Act, 1974) регулює збір та використання персональних даних федеральними агентствами [14, с. 89]. Він встановлює принципи «справедливої інформаційної практики», що включають право громадян знати, яка інформація про них збирається, як вона використовується, та вимагати виправлення неточної інформації. Однак цей закон має обмежену сферу дії і не поширюється на приватний сектор.

– Закон про захист дітей в Інтернеті (COPPA, 1998) є важливим кроком у захисті приватності дітей в онлайн-середовищі [2, с. 105]. Він вимагає від вебсайтів та онлайн-сервісів, орієнтованих на дітей віком до 13 років, отримувати згоду батьків перед збором особистої інформації про дітей. Це створює додаткові бар'єри для збору даних про дітей та сприяє захисту їхньої приватності.

Кібербезпека:

– Закон про кібербезпеку (Cybersecurity Act, 2015) спрямовано на посилення захисту критичної інфраструктури США від кібератак [5, с. 131]. Він передбачає обмін інформацією про кіберзагрози між державними органами та приватним сектором, а також встановлює стандарти кібербезпеки для державних установ. Однак цей закон викликає суперечки з балансу між захистом від кібератак та ризиком порушення приватності громадян.

– Патріотичний акт (2001), прийнятий після терактів

11 вересня, значно розширив повноваження уряду у сфері електронного спостереження [24, с. 144]. Він дозволив спецслужбам отримувати доступ до даних про комунікації громадян без попереднього судового ордера у випадках, пов'язаних з тероризмом. Цей закон викликав значну критику з боку правозахисних організацій, які стверджують, що він порушує Четверту поправку Конституції.

Сучасні виклики інформаційної політики США: аналіз та шляхи вирішення

Аналіз сучасних викликів, з якими стикається інформаційна політика США, показує, що наявне законодавство потребує подальшого вдосконалення та адаптації.

Проблема дезінформації та втручання у вибори є одним з найсерйозніших викликів. Уряд США вживає заходів з контролю за маніпуляціями в соціальних мережах [9, с. 159], проте ці заходи часто критикуються за недостатню ефективність та потенційну загрозу свободі слова. Необхідний пошук балансу між захистом демократичного процесу від зовнішнього втручання та дотриманням конституційних гарантій свободи слова.

Захист персональних даних у цифрову епоху вимагає оновлення законодавства у відповідь на активний розвиток технологій [4, с. 177]. Наявні закони, такі як Privacy Act та COPPA, не охоплюють увесь спектр проблем, пов'язаних зі збором та використанням даних приватними компаніями. Відсутність єдиного федерального закону, що комплексно регулював би захист персональних даних у приватному секторі, створює прогалини в правовому захисті громадян. На відміну від ЄС, де діє Загальний регламент про захист даних (GDPR), у США немає єдиного стандарту, що призводить до фрагментарного регулювання на рівні окремих штатів (наприклад, Каліфорнійський закон про захист прав споживачів (CCPA)).

Отже, аналіз законодавчого забезпечення інформаційної політики США, проведений у межах цього дослідження, свідчить про таке:

– *Комплексність та багаторівневість*. Законодавство США у цій сфері є складною системою, що включає конституційні норми, спеціальні закони та регуляторні акти, які взаємодіють між собою.

– *Динамічність*. Законодавство постійно адаптується до нових технологічних та суспільних викликів, що свідчить про його гнучкість. Проте ця адаптація не завжди є своєчасною та ефективною.

– *Баланс між протилежними інтересами*. Законодавство США намагається знайти баланс між свободою слова та необхідністю обмеження поширення шкідливої інформації, між правом на приватність та інтересами національної безпеки, між захистом персональних даних та свободою підприємницької діяльності. Цей баланс не завжди є досяжним, що призводить до постійних дискусій та судових спорів.

– *Необхідність подальшого вдосконалення*. Незважаючи на розвинену правову базу, є значні прогалини в регулюванні, особливо у сфері захисту персональних даних у приватному секторі, боротьби з дезінформацією та регулювання діяльності цифрових платформ.

Так, результати дослідження підтверджують, що законодавче забезпечення інформаційної політики США, хоч і є одним із найбільш розвинених у світі, потребує подальшого вдосконалення для ефективної відповіді на сучасні виклики цифрової епохи. Це вдосконалення має відбуватися з урахуванням як конституційних принципів, так і необхідності захисту національних інтересів та прав громадян.

ВИСНОВКИ

Аналіз законодавчого забезпечення інформаційної політики США свідчить про те, що ця сфера пройшла значний шлях еволюції, відреагувавши на низку технологічних та суспільних змін. Основними характеристиками цієї еволюції є:

– Перехід від фрагментарного регулювання до більш комплексного. Якщо раніше інформаційні відносини регулювалися розрізненими актами, то зараз спостерігається тенденція до створення більш цілісної системи, яка охоплює різні аспекти інформаційної сфери.

– Постійна адаптація до нових технологій. Законодавство США намагається реагувати на появу нових технологій (Інтернет, соціальні мережі, штучний інтелект), але ця реакція не завжди є своєчасною та ефективною, що породжує нові виклики.

– Посилення уваги до питань балансу між різними правами та інтересами. Законодавчий процес у США характеризується постійним пошуком компромісу між фундаментальними правами (свобода слова, приватність) та інтересами держави (національна безпека, боротьба зі злочинністю).

Дослідження також виявило низку ключових проблем і протиріч, які потребують подальшого вивчення. До них належать: недостатня ефективність механізмів боротьби з дезінформацією, прогалини в регулюванні захисту персональних даних, невизначеність правового статусу цифрових платформ, вплив штучного інтелекту на приватність і свободу слова, а також виклики у сфері міжнародного співробітництва з питань кібербезпеки.

Подальші дослідження у цій сфері може бути спрямовано на розроблення шляхів вирішення зазначених проблем, а також на вдосконалення наявних механізмів регулювання інформаційної політики з урахуванням досвіду США та інших країн. Досвід США може бути корисним для інших країн, зокрема для України, у розробленні власної інформаційної політики, проте необхідна його адаптація з урахуванням національних особливостей.

References

1. Brookings Institution. Regulating Big Tech: The Future of Antitrust and Privacy in the Digital Age. Washington, D.C., 2022.
2. Children's Online Privacy Protection Act (COPPA). Public Law 105-277, 1998.
3. Classified Information Procedures Act. Public Law 96-456, 1982.
4. Congressional Research Service. Big Tech and Data Privacy, 2023.
5. Cybersecurity Act. Public Law 114-113, 2015.
6. Electronic Frontier Foundation (EFF). State of Surveillance: Government Policies and Civil Liberties in the Digital Era. San Francisco, 2023

7. Federal Communications Commission (FCC). Annual Report on the State of the U.S. Communications Market. Washington, D.C., 2021.
8. Federal Trade Commission (FTC). Privacy & Data Security Update: Regulatory Developments and Enforcement Actions. Washington, D.C., 2023.
9. Federal Trade Commission. Report on Disinformation and Social Media, 2022.
10. Freedom of Information Act (FOIA). Public Law 89-487, 1966.
11. Lessig L. The Future of Ideas: The Fate of the Commons in a Connected World. New York, 2001. 352 p.
12. National Institute of Standards and Technology (NIST). Cybersecurity Framework Version 2.0: Improving Critical Infrastructure Cybersecurity. U.S. Department of Commerce, 2022.
13. Pasquale F. New Laws of Robotics: Defending Human Expertise in the Age of AI. Cambridge, 2020. 336 p.
14. Privacy Act. Public Law 93-579, 1974.
15. RAND Corporation. Disinformation and Democracy: Policy Recommendations for a Resilient Digital Future. Santa Monica, 2023.
16. Schneier B. Click Here to Kill Everybody: Security and Survival in a Hyper-Connected World. New York, 2018. 304 p.
17. Solove D.J. The Digital Person: Technology and Privacy in the Information Age. New York, 2021. 283 p.
18. Stone G.R. Perilous Times: Free Speech in Wartime. New York, 2017. 730 p.
19. Sunstein C.R. Republic: Divided Democracy in the Age of Social Media. Princeton, 2018. 328 p.
20. U.S. Constitution. Fifth Amendment, 1791.
21. U.S. Constitution. First Amendment, 1791.
22. U.S. Constitution. Fourth Amendment, 1791.
23. U.S. Department of Justice. Antitrust Enforcement in the Digital Economy: Report to Congress. Washington, D.C., 2022.
24. USA PATRIOT Act. Public Law 107-56, 2001.
25. Wu T. The Curse of Bigness: Antitrust in the New Gilded Age. New York: Columbia Global Reports. 2020. 150 p.
26. Zuboff S. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. New York: PublicAffairs. 2019. 704 p.
27. Patlachuk V.N., Patlachuk O.V. Constitutions of the world in 20 vol. Kyiv, 2023. Vol. 17. pp. 158-159. (in Ukrainian).

Oleksandr LIKHOTA
PhD in Economics, Associate Professor of department, North Ukrainian Institute named after Heroes of Kruty of "Interregional Academy of Personnel Management"
ORCID: https://orcid.org/0000-0003-2948-4902
e-mail: a-lihota@ukr.net

LEGISLATIVE SUPPORT OF THE US INFORMATION POLICY

The rapid evolution of digital technologies and the pervasive influence of the internet have profoundly reshaped the information landscape, necessitating a continuous adaptation of legal frameworks. The United States, as a global leader in technology and information, faces unique challenges in balancing freedom of expression, national security, and individual rights within its information policy. This article examines the legislative underpinnings of this policy, tracing its historical trajectory and analyzing its current state. The primary purpose of this article is to provide a comprehensive analysis of the U.S. legislative framework for information policy. This includes examining the evolution of relevant laws, identifying key regulatory bodies, assessing the effectiveness of existing regulations in addressing contemporary challenges (such as disinformation and cybersecurity threats), and exploring the interplay between domestic policy and international influences. The article will focus on the balance that is needed among freedom of speech, data security, and national security. The analysis reveals a complex and multi-layered legal structure. Key pieces of legislation, such as the First Amendment (guaranteeing freedom of speech), the Communications Decency Act, the Digital Millennium Copyright Act, and various privacy laws, form the foundation. The roles of the FCC, FTC, and Department of Justice are crucial in enforcement and policy development. The study finds that while the U.S. has a robust legal framework, challenges remain in addressing the rapid pace of technological change, the rise of social media platforms as primary sources of information (and disinformation), and the increasing sophistication of cyber threats. The increasing influence of algorithms in content moderation creates new areas of concern related to bias and censorship. Furthermore, international cooperation, especially with the EU on data protection (e.g., GDPR considerations), significantly impacts U.S. policy. The U.S. information policy legislative framework is in a state of constant evolution. While existing laws provide a strong foundation, ongoing adaptation is crucial to address emerging threats and opportunities. Future legislative initiatives should focus on enhancing cybersecurity measures, combating disinformation effectively (while upholding freedom of speech), clarifying the responsibilities of social media platforms, and promoting greater transparency in algorithmic content moderation. Finding the optimal balance between protecting individual rights, ensuring national security, and fostering a vibrant and open information environment remains a critical and ongoing challenge. Further legal development is needed to strike a balance among freedom of speech, data security, and national interests.

Keywords: *US information policy, legislative regulation, freedom of speech, personal data protection, disinformation, cybersecurity, digital technologies, state regulation*