

ДЕРЖАВНИЙ ТОРГОВЕЛЬНО-ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

*Кваліфікаційна наукова
праця на правах рукопису*

ЩЕРБАК ГЕННАДІЙ РОСТИСЛАВОВИЧ

УДК 341.171

ДИСЕРТАЦІЯ

САМОРЕГУЛЮВАННЯ ОНЛАЙН-ПЛАТФОРМ У ПРАВІ ЄС

Спеціальність 293 «Міжнародне право»

Галузь знань 29 «Міжнародні відносини»

Подається на здобуття ступеня доктора філософії

Дисертація містить результати власних досліджень. Використання ідей результатів і текстів інших авторів мають посилання на відповідне джерело

_____ **Г. Р. Щербак**

Науковий керівник: **Мазаракі Наталія Анатоліївна**, доктор юридичних наук, професор, заслужений юрист України

Київ – 2026

ЗМІСТ

АНОТАЦІЯ.....	4
ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ.....	11
ВСТУП.....	12
РОЗДІЛ 1. ДОКТРИНАЛЬНІ ПІДХОДИ ДО РОЗУМІННЯ САМОРЕГУЛЮВАННЯ.....	24
1.1. Онлайн-платформи як особливий об'єкт регулювання.....	24
1.2. Саморегулювання як модель регуляторного управління.....	45
Висновки до розділу 1.....	63
РОЗДІЛ 2. ОСНОВНІ ПІДХОДИ ДО РЕГУЛЮВАННЯ ОНЛАЙН-ПЛАТФОРМ.....	65
2.1. Американський підхід до регулювання онлайн-платформ.....	65
2.2. Китайський підхід до регулювання онлайн-платформ.....	84
2.3 Європейський підхід до регулювання онлайн-платформ.....	99
Висновки до розділу 2.....	112
РОЗДІЛ 3. РЕАЛІЗАЦІЯ МОДЕЛІ РЕГУЛЬОВАНОГО САМОРЕГУЛЮВАННЯ У DIGITAL SERVICES ACT	115
3.1. Базовий процедурний рівень платформного саморегулювання.....	116
3.2. Посилений ризик-орієнтований рівень регульованого саморегулювання для VLOPs/VLOSEs.....	134
3.3. Співрегуляторний рівень колективних інструментів DSA.....	148
Висновки до розділу 3.....	157

ВИСНОВКИ.....	161
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	168

АНОТАЦІЯ

Дисертація є одним із перших у вітчизняній юридичній науці комплексних монографічних досліджень правового регулювання саморегулювання онлайн-платформ у праві Європейського Союзу, у межах якого здійснено системний аналіз теоретико-правових засад платформного саморегулювання, досліджено правову природу онлайн-платформ, визначено особливості інституційних та нормативних механізмів саморегулювання цифрового середовища.

Обґрунтовано актуальність формування ефективної моделі саморегулювання онлайн-платформ у праві Європейського Союзу в умовах стрімкого розвитку цифрової економіки, зростання ролі платформних сервісів у суспільних відносинах та необхідності забезпечення балансу між державним регулюванням і автономією цифрових суб'єктів. Встановлено, що традиційні механізми правового саморегулювання не завжди здатні оперативно реагувати на динамічні зміни цифрового середовища, що зумовлює підвищення значення регульованих саморегуляторних інструментів як складової сучасної регуляторної політики Європейського Союзу.

У дисертації здійснено комплексний доктринальний аналіз поняття саморегулювання, його правової природи, функцій, принципів та видів. Доведено, що саморегулювання у сфері діяльності онлайн-платформ являє собою форму регульованого саморегулювання, за якої приватна нормотворчість і приватне правозастосування платформ зберігаються, але підпорядковуються юридично обов'язковим вимогам прозорості, належної процедури, пропорційності, підзвітності та зовнішнього контролю. Аргументовано, що саморегулювання не є альтернативою державному регулюванню, а виступає його важливим доповненням, спрямованим на підвищення ефективності регуляторного впливу.

Запропоновано авторський підхід до розуміння поняття онлайн-платформи як цифрової системи, що забезпечує взаємодію між користувачами або між користувачем та цифровим середовищем з метою обміну інформацією, товарами, послугами чи контентом. На основі аналізу доктринальних підходів та положень

законодавства Європейського Союзу досліджено особливості правового статусу онлайн-платформ, їх місце у системі цифрових послуг та класифікацію за функціональним призначенням.

У межах дослідження здійснено аналіз нормативно-правової бази Європейського Союзу у сфері діяльності онлайн-платформ, зокрема положень Акту про цифрові послуги, актів у сфері електронної комерції, захисту прав споживачів, конкуренції та цифрового ринку. Обґрунтовано, що сучасна модель регулювання онлайн-платформ у Європейському Союзі поступово трансформується від переважно державного регулювання до поєднання нормативних та саморегуляторних механізмів, заснованих на співпраці між державними інституціями, платформами та іншими заінтересованими сторонами.

Особливу увагу приділено дослідженню кодексів поведінки, галузевих стандартів та практик належного врядування як основних інструментів саморегулювання онлайн-платформ. Доведено, що кодекси поведінки виконують не лише регулятивну, а й превентивну, контрольну та координаційну функції, сприяючи підвищенню рівня прозорості, підзвітності та відповідальності цифрових платформ перед користувачами й суспільством.

Здійснено системний аналіз інституційного механізму саморегулювання онлайн-платформ у Європейському Союзі. Визначено роль Європейської комісії, громадянського суспільства, наукових та платформних спільнот у процесах формування та реалізації правил поведінки у цифровому середовищі. Встановлено, що ефективність саморегулювання значною мірою залежить від рівня представництва учасників цифрового ринку, прозорості процедур прийняття рішень та наявності механізмів контролю за виконанням встановлених стандартів.

На основі порівняльно-правового аналізу досліджено особливості європейського, американського та китайського підходів до саморегулювання онлайн-платформ. Встановлено, що європейська модель характеризується прагненням до поєднання ринкової автономії з високими стандартами захисту прав людини, забезпеченням прозорості діяльності платформ та посиленням наглядом за виконанням добровільно прийнятих зобов'язань. Водночас американський підхід

орієнтується на ринкову свободу та мінімальне державне втручання, тоді як китайська модель передбачає тісну інтеграцію саморегуляторних механізмів із системою державного контролю та встановленням режиму цензури.

З'ясовано сучасні тенденції розвитку саморегулювання онлайн-платформ у праві Європейського Союзу. Аргументовано, що подальша еволюція регулювання цифрових платформ буде пов'язана з розширенням використання механізмів співрегулювання, посиленням ролі кодексів поведінки, впровадженням стандартів належної цифрової практики та розвитком процедур незалежного моніторингу виконання саморегуляторних зобов'язань.

Ключові слова: Саморегулювання, захист фундаментальних прав, цифрові послуги, кодекси поведінки, електронна комерція, регулювання онлайн-платформ, право ЄС, європеїзація, Угода про асоціацію між Україною та ЄС, Акт про цифрові послуги.

SUMMARY

The dissertation is one of the first in domestic legal science of comprehensive monographic studies of the legal regulation of self-regulation of online platforms in the law of the European Union, within which a systematic analysis of the theoretical and legal foundations of platform self-regulation was carried out, the legal nature of online platforms was investigated, and the features of institutional and regulatory mechanisms for self-regulation of the digital environment were identified.

The relevance of forming an effective model of self-regulation of online platforms in the law of the European Union in the conditions of the rapid development of the digital economy, the growing role of platform services in public relations and the need to ensure a balance between state regulation and the autonomy of digital entities is substantiated. It is established that traditional mechanisms of legal self-regulation are not always able to respond promptly to dynamic changes in the digital environment, which leads to an increase in the importance of regulated self-regulatory instruments as a component of the modern regulatory policy of the European Union.

The dissertation provides a comprehensive doctrinal analysis of the concept of self-regulation, its legal nature, functions, principles and types. It is proven that self-regulation in the field of online platforms is a form of regulated self-regulation, in which private rule-making and private law enforcement of platforms are preserved, but are subject to legally binding requirements of transparency, due process, proportionality, accountability and external control. It is argued that self-regulation is not an alternative to state regulation, but is an important complement to it, aimed at increasing the effectiveness of regulatory influence.

The author's approach to understanding the concept of an online platform as a digital system that ensures interaction between users or between a user and a digital environment for the purpose of exchanging information, goods, services or content is proposed. Based on the analysis of doctrinal approaches and provisions of European Union legislation, the features of the legal status of online platforms, their place in the system of digital services and classification by functional purpose are investigated.

The study analyzes the regulatory framework of the European Union in the field of online platforms, in particular the provisions of the Digital Services Act, acts in the field of e-commerce, consumer protection, competition and the digital market. It is substantiated that the modern model of regulation of online platforms in the European Union is gradually transforming from predominantly state regulation to a combination of regulatory and self-regulatory mechanisms based on cooperation between state institutions, platforms and other stakeholders.

Particular attention is paid to the study of codes of conduct, industry standards and good governance practices as the main tools for self-regulation of online platforms. It is proven that codes of conduct perform not only regulatory, but also preventive, control and coordination functions, contributing to increasing the level of transparency, accountability and responsibility of digital platforms to users and society.

A systematic analysis of the institutional mechanism for self-regulation of online platforms in the European Union is carried out. The role of the European Commission, civil society, scientific and platform communities in the processes of forming and implementing rules of conduct in the digital environment is determined. It is established

that the effectiveness of self-regulation largely depends on the level of representation of digital market participants, the transparency of decision-making procedures and the availability of mechanisms for monitoring the implementation of established standards.

Based on a comparative legal analysis, the features of the European, American and Chinese approaches to self-regulation of online platforms are investigated. It is established that the European model is characterized by the desire to combine market autonomy with high standards of human rights protection, ensuring transparency of platform activities and enhanced supervision over the implementation of voluntarily accepted obligations. At the same time, the American approach is focused on market freedom and minimal state intervention, while the Chinese model involves close integration of self-regulatory mechanisms with the system of state control and the establishment of a censorship regime.

The current trends in the development of self-regulation of online platforms in European Union law are clarified. It is argued that the further evolution of digital platform regulation will be associated with the expansion of the use of co-regulatory mechanisms, the strengthening of the role of codes of conduct, the introduction of standards of good digital practice, and the development of procedures for independent monitoring of the implementation of self-regulatory obligations.

Keywords: Self-regulation, protection of fundamental rights, digital services, codes of conduct, e-commerce, regulation of online platforms, EU law, Europeanization, EU-Ukraine Association Agreement, Digital Services Act.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ, в яких опубліковані основні наукові результати дисертації:

1. Щербак, Г. 2022. Інтеграційна модель АСЕАН. *Ius Modernum*. 124, 5 (Жов 2022), 52–65.
2. Щербак, Г. 2024. Регулювання онлайн-платформ у праві КНР. *Ius Modernum*. 137, 6 (Груд 2024), 111–129.

3. Щербак, Г. 2025. Регулювання онлайн-платформ у праві США. *Ius Modernum*. 139, 2 (Чер 2025), 36–49.

4. Щербак Г.Р. Регулювання саморегулювання: Кодекси поведінки у системі цифрового врядування ЄС. *Наука і техніка сьогодні СЕРІЯ «Право»*. № 3(57). 2026, 417-437.

5. Щербак Г.Р. Стан правового регулювання онлайн-платформ для електронної комерції в державах-членах АСЕАН. *Юридичні науки: проблеми та перспективи : матеріали міжнародної науково-практичної конференції, м. Запоріжжя, 24–25 лютого 2023 р.* – Львів – Торунь : Liha-Pres, 2023 – 292-295

6. Shcherbak, H. R. (2023). Legal Regulation of Online Platforms in Ukraine and EU Experience. *In: Proceedings of the International Scientific Conference*. Częstochowa, Republic of Poland, 215-218.

7. Щербак Г.Р. Імплементация Акту про цифрові послуги в Україні. *Юридична осінь 2023 року: зб. Тез доповідей та наук. Повідомл. Учасників міжнар. Наук.-практ. Конф. Молодих учених та студентів (Харків, 17 листоп. 2023 р.) / за заг. Ред. Д.В. Лученка.* – Х.: Нац. Юрид. Ун-т імені Ярослава Мудрого, 2023. – 195-198

8. Щербак Г.Р. Регулювання онлайн платформ у Китайській Народній Республіці. *Правове регулювання цифрової економіки: правові інструменти, можливості та виклики [Електронне видання]: Матеріали круглого столу (21 листопада 2023 року) / відп. Ред. Н.А. Мазаракі.* – Київ: Держ. Торг.-екон. Ун-т, 2023. 153-156.

9. Shcherbak H.R. Regulation of online gambling platforms in EU legislation. *International scientific conference «New approaches and current legal research» : conference proceedings (November 3–4, 2022. Riga, the Republic of Latvia)*. Riga, Latvia : “Baltija Publishing”, 2022. 204-207.

10.Щербак Г.Р. Стан захисту персональних даних споживачів комерційних онлайн платформ в праві ЄС: правове регулювання та судовий захист. *Євроінтеграційні процеси в Україні: історичні, культурні, політико-правові та психологічні аспекти : матеріали Міжнародної науково-практичної*

конференції, 12–13 квітня 2023 р., м. Київ. – Львів – Торунь : Liha-Pres, 2023. 206-209.

11. Щербак Г.Р. Правове регулювання використання штучного інтелекту в комерційних онлайн платформах: європейський, американський та китайський підходи. *Становлення та розвиток правової держави: проблеми теорії та практики: Матеріали XVI міжнародної науково-практичної конференції, м. Миколаїв, 21 грудня 2023 р. Львів – Торунь : Liha-Pres, 2023. – 268-271.*

12. Щербак Г.Р. Можливості використання напрацювань поведінкової економіки у сфері регулювання комерційних онлайн-платформ. *Фундаментальні та прикладні проблеми суспільства: історія, сьогодення, майбутнє [Електронний ресурс] : тези доп. Міжнар. Наук.-практ. Конф. (Київ, 11 квіт. 2024 р.) / відп. Ред. А. Кравченко. – Київ : Держ. Торг.-екон. Ун-т, 2024. – 313 с. – Укр. Та інозем. Мовами.*

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ЄК	- Європейська комісія	
ЄС	- Європейський Союз	
ІВ	- Інтелектуальна власність	
ODS	- Органи позасудового вирішення спорів	- out-of-court dispute settlement
ІІІ	- Штучний інтелект	
CAC	- Cyberspace Administration of China	- Адміністрація кіберпростору Китаю
DMA	- Акт про цифрові ринки	- Digital Markets Act
DSA	- Акт про цифрові послуги	- Digital Services Act
FTC	- Федеральна торгова комісія	- Federal Trade Commission
GDPR	- Загальний регламент про захист даних	- General data protection regulation
VLOP	- дуже великі онлайн- платформи	- Very Large Online Platforms
VLOSE	- дуже великі онлайн- пошукові системи	- Very Large Online Search Engines

ВСТУП

Ухвалення Регламенту (ЄС) 2022/2065 про єдиний ринок цифрових послуг започаткувало концептуально новий етап у регулюванні діяльності онлайн-платформ у праві Європейського Союзу. На відміну від підходу, сформованого Директивою 2000/31/ЄС про електронну комерцію, який залишав цифровим посередникам значний простір для приватної автономії, DSA виходить із необхідності системного публічного впливу на платформне середовище.

Поява такого підходу була зумовлена зростанням ролі онлайн-платформ у здійсненні основоположних прав, функціонуванні демократичних процесів, поширенні інформації, формуванні суспільної думки та організації економічної взаємодії. Платформи перестали виконувати лише технічну посередницьку функцію. Їхні правила, алгоритмічні системи, політики модерації та внутрішні процедури почали безпосередньо впливати на доступ користувачів до інформації, свободу вираження поглядів, участь у публічній дискусії та інші суспільно значущі процеси. Представники громадянського суспільства та організації із захисту прав споживачів неодноразово звертали увагу на ризики концентрації регуляторних повноважень у руках приватних суб'єктів. Основні застереження стосувалися недостатньої прозорості та підзвітності платформ, які могли встановлювати і застосовувати власні правила без належного залучення користувачів, громадянського суспільства та регуляторних органів¹.

Відповіддю Європейського Союзу стало формування складної регуляторної моделі, у якій поєднуються імперативні правові вимоги, приватна нормотворчість платформ, механізми саморегулювання, співрегулювання, управління ризиками, зовнішній аудит, прозорість і публічний нагляд. Саме таке поєднання різних регуляторних механізмів стало однією з найбільш характерних рис DSA.

¹ Access Now, Protecting Free Expression in the Era of Online Content Moderation: Preliminary Recommendations on Content Moderation and Facebook's Planned Oversight Board (Access Now 2019); ARTICLE 19, 'The Santa Clara Principles and the Push for Transparency' (8 December 2021); BEUC, The Digital Services Act Proposal: BEUC Position Paper (BEUC-X-2021-032, 9 April 2021); The Santa Clara Principles on Transparency and Accountability in Content Moderation (2nd edn, 2021).

На ранньому етапі розвитку Інтернету європейське регулювання цифрового середовища мало переважно ринково орієнтований характер і залишало значний простір для приватної автономії постачальників цифрових послуг. Такий підхід, близький до сформованої у США моделі обмеженого державного втручання, знайшов відображення у Директиві про електронну комерцію², яка закріпила режим обмеженої відповідальності посередників і заборону покладення на них загального обов'язку моніторингу інформації. Водночас вона не виключала державного нагляду, застосування судових приписів і розвитку кодексів поведінки.

Подальше накопичення ризиків, пов'язаних із діяльністю онлайн-платформ, показало обмеженість такого підходу. До них належать поширення незаконного контенту та дезінформації, непрозорість модерації і алгоритмічних систем, використання маніпулятивних практик, інформаційна асиметрія, а також концентрація економічної та інформаційної влади найбільшими платформами. За цих умов виключно добровільні механізми вже не могли забезпечити належний рівень прозорості, підзвітності та захисту прав користувачів.

Еволюцію підходів до регулювання онлайн-платформ можна узагальнено описати через три моделі³. Американська модель традиційно надає особливого значення свободі вираження поглядів, інноваціям і обмеженню відповідальності цифрових посередників. Китайська модель ґрунтується на пріоритеті державного суверенітету, національної та інформаційної безпеки й передбачає значний централізований контроль над платформами та інформаційним простором.

Європейський Союз поступово сформував відмінний підхід, у центрі якого перебуває забезпечення справедливого балансу між свободою вираження поглядів, іншими основоположними правами, безпекою користувачів та економічною свободою платформ. Цей підхід не зводиться ані до повної автономії платформ, ані до безпосереднього державного контролю над цифровим середовищем. Натомість

² Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market [2000] OJ L178/1.

³ Anu Bradford, *Digital Empires: The Global Battle to Regulate Technology* (Oxford University Press 2023).

він поєднує публічно-правове регулювання із збереженням приватної нормотворчості платформ, підпорядковуючи їхнє саморегулювання обов'язковим вимогам щодо прозорості, процедурної справедливості, управління ризиками, зовнішнього контролю та підзвітності.

Із різноманіття новел DSA мій науковий інтерес сфокусувався на механізмах саморегулювання та співрегулювання. Це не було випадковим, адже на той час на кафедрі тематика саморегулювання досліджувалася моїми колегами Оленою Гончаренко⁴ та Гаяне Бабаджанян⁵, їхні публікації стимулювали інтерес до проявів саморегулювання в онлайн-середовищі.

На момент обрання теми дисертації у 2022 році в науковій літературі вже був сформований розвинений комплекс теоретичних підходів до пояснення взаємодії державного регулювання та приватної самоорганізації. Концепція реагувального регулювання Ієна Ейрса і Джона Брейтуейта⁶ обґрунтувала залежність інтенсивності регуляторного втручання від поведінки регульованого суб'єкта та ефективності добровільного виконання ним установлених вимог. У німецькій правовій доктрині Вольфганг Шульц і Торстен Гельд⁷ розробили концепцію регульованого саморегулювання як форми сучасного управління, у межах якої приватна самоорганізація поєднується з визначеними державою цілями, процедурами та механізмами контролю. Бернгард Керн⁸ застосував відповідні підходи безпосередньо до інтернет-середовища, дослідивши співвідношення державного регулювання, автономного саморегулювання та їх гібридних форм. Історичні та інституційні передумови саморегулювання були розкриті також у

⁴ Гончаренко О. М. Теоретико-правові засади саморегулювання господарської діяльності : дис. ... д-ра юрид. наук : 12.00.04. Київ, 2020.

⁵ Бабаджанян Г. Б. Правове забезпечення саморегулювання господарсько-торговельної діяльності : дис. ... д-ра філософії : 081 Право. Київ : Державний торговельно-економічний університет, 2024. 230 с.

⁶ Ian Ayres and John Braithwaite, *Responsive Regulation: Transcending the Deregulation Debate* (OUP 1992).

⁷ Wolfgang Schulz and Thorsten Held, *Regulierte Selbstregulierung als Form modernen Regierens* (Arbeitspapiere des Hans-Bredow-Instituts No 10, Verlag Hans-Bredow-Institut 2002).

⁸ Bernhard Georg Kern, *Das Internet zwischen Regulierung und Selbstregulierung* (doctoral dissertation, Humboldt-Universität zu Berlin 2009).

колективній праці за редакцією Петера Колліна та інших авторів⁹, а дослідження Еви Томанн¹⁰ систематизувало розуміння регулювання як державного втручання, форми управління та сукупності державних і недержавних механізмів соціального контролю. Сукупність цих праць дала теоретичні підстави розглядати саморегулювання як складову ширшої регуляторної системи, у якій взаємодіють публічні та приватні суб'єкти, імперативні норми, добровільні правила, процедури контролю і механізми примусу.

Безпосереднім імпульсом для зосередження дослідження на DSA стала колективна монографія *To Break Up or Regulate Big Tech? Avenues to Constrain Private Power in the DSA/DMA Package*, підготовлена за участю дослідників Інституту Макса Планка у 2021 році¹¹. Її автори аналізували ще проєкти DSA і DMA та порушували питання про правову природу запропонованих ними механізмів, способи обмеження приватної влади технологічних компаній, співвідношення публічного і приватного правозастосування, а також роль процедурних, конкурентних і регуляторних інструментів у новій цифровій архітектурі Європейського Союзу. Ця праця допомогла конкретизувати науковий інтерес до внутрішньої логіки DSA та до місця саморегулювання онлайн-платформ у сформованій ним системі. Особливе значення для формування наукового задуму дослідження мали також праці Мартіна Кречмера¹², у яких порушувалося питання трансформації приватної влади великих цифрових платформ та необхідності пошуку нових моделей її правового обмеження. Саме вони стали одним із перших інтелектуальних імпульсів до дослідження правової природи механізмів DSA та місця саморегулювання в новій системі платформного регулювання.

⁹ Peter Collin, Gerd Bender, Stefan Ruppert, Margrit Seckelmann and Michael Stolleis (eds), *Selbstregulierung im 19. Jahrhundert: Zwischen Autonomie und staatlichen Steuerungsansprüchen* (Vittorio Klostermann 2011).

¹⁰ Eva Thomann, 'The Notions of Regulation and Self-Regulation in Political Science' (2017) 3 *Journal of Self-Regulation and Regulation* 55.

¹¹ Heiko Richter, Marlene Straub and Erik Tuchtfield (eds), *To Break Up or Regulate Big Tech? Avenues to Constrain Private Power in the DSA/DMA Package* (Max Planck Institute for Innovation and Competition Research Paper No 21-25, 2021).

¹² Martin Kretschmer, 'Platforms and Digital Regulation' (Weizenbaum Journal of the Digital Society, 2021).

Відповідно, **метою** дисертаційного дослідження було визначено обґрунтування цілісної теоретико-правової концепції саморегулювання онлайн-платформ у праві Європейського Союзу.

Об'єктом дисертаційного дослідження є суспільні відносини, що виникають у процесі саморегулювання діяльності онлайн-платформ та його взаємодії з механізмами публічного регулювання у праві Європейського Союзу.

Предметом дисертаційного дослідження є теоретико-правові засади, нормативна модель, механізми, форми та інструменти саморегулювання онлайн-платформ, закріплені правом Європейського Союзу, насамперед Регламентом (ЄС) 2022/2065 (Digital Services Act), а також практика їх реалізації.

Для досягнення поставленої мети визначено такі **завдання**:

з'ясувати правову, економічну та соціальну природу онлайн-платформ як особливого об'єкта правового регулювання;

визначити ознаки онлайн-платформи як приватного регулятора, що здійснює нормотворчі, правозастосовні та контрольні функції у цифровому середовищі;

розкрити поняття саморегулювання онлайн-платформ та відмежувати його від державного регулювання, співрегулювання, метарегулювання та інших суміжних регуляторних моделей;

систематизувати основні теоретичні концепції саморегулювання, а також визначити їх придатність для аналізу DSA;

виявити межі автономного саморегулювання онлайн-платформ, зумовлені конфліктом приватних і публічних інтересів, інформаційною асиметрією, масштабом платформного впливу та дефіцитом процедурної підзвітності;

дослідити основні моделі регулювання онлайн-платформ, що сформувалися у США, Китаї та Європейському Союзі, та визначити особливості європейського підходу;

систематизувати нормативні елементи саморегулювання онлайн-платформ у DSA та визначити їх рівні, зміст і функціональне призначення;

проаналізувати механізми внутрішньої нормотворчості, модерації контенту, обґрунтування рішень, розгляду скарг і позасудового вирішення спорів як прояви процедурного саморегулювання платформ;

дослідити ризик-орієнтовані механізми DSA, включаючи оцінку і мінімізацію системних ризиків, комплаєнс, аудит, звітність і доступ дослідників до даних, як прояви метарегуляторного впливу;

визначити правову природу кодексів поведінки, стандартів і кризових протоколів як інструментів співрегулювання у системі DSA;

оцінити роль публічного нагляду, зовнішньої верифікації та механізмів відповідальності у забезпеченні ефективності платформного саморегулювання;

сформулювати цілісну теоретико-правову концепцію саморегулювання онлайн-платформ у праві Європейського Союзу та визначити її основні ознаки, структуру, межі й механізми функціонування.

Зв'язок роботи з науковими програмами, планами, темами. Обраний напрям дослідження узгоджується з положеннями [Загальнодержавної програми адаптації законодавства України до законодавства ЄС](#), а також зі стратегічними нормативними актами, що визначають пріоритети цифрової трансформації та правової модернізації України. Зокрема, дослідження корелює із [Цілями сталого розвитку України на період до 2030 року](#) та [Стратегією цифрового розвитку інноваційної діяльності України на період до 2030 року](#). Дисертаційна робота виконана в межах тем науково-дослідних робіт кафедри міжнародного, цивільного та комерційного права Державного торговельно-економічного університету «Україна в координатах перебудови міжнародного права і європейської інтеграції».

Після обрання теми дослідження у 2022 році академічна дискусія щодо правової природи механізмів DSA істотно активізувалася. Під час підготовки дисертації було враховано праці Ану Бредфорд про американську, китайську та європейську моделі цифрового регулювання¹³; Роберта Горви про політичні

¹³ Anu Bradford, *Digital Empires: The Global Battle to Regulate Technology* (Oxford University Press 2023); Anu Bradford, 'The False Choice Between Digital Regulation and Innovation' (2024) 118 *Northwestern University Law Review* 377.

стратегії держав у сфері платформного регулювання¹⁴; Сімуза Сімпсона про перехід ЄС від саморегуляторної моделі Директиви про електронну комерцію до публічно орієнтованої мережевої моделі управління DSA¹⁵; Ребекки Гзенгер та співавторів про платформне управління в умовах DSA¹⁶; Ніколауса фон Бернута про саморегулювання, забезпечене державним примусом та залежність ефективності DSA від добросовісності платформ¹⁷; Крістіана Олліга про конституціоналізацію цифрових комунікаційних просторів і вплив ст. 14(4) DSA на приватні правила платформ¹⁸; Тіма Шпренгера про процедурні засади платформного правозастосування¹⁹ та ін.

У вітчизняній доктрині дискусія розвивалася з урахуванням праць Наталії Філатової-Білоус²⁰ та досліджень моїх колег із кафедри міжнародного, цивільного та комерційного права ДТЕУ²¹. Ці публікації дозволили вести академічну дискусію

¹⁴ Robert Gorwa, *The Politics of Platform Regulation: How Governments Shape Online Content Moderation* (Oxford University Press 2024).

¹⁵ Seamus Simpson, 'The Limits of Internet Self-Regulation: The EU's Policy for Digital Internet Intermediaries' (2024) 9 *Frontiers in Communication*

¹⁶ Rita Gsenger and others, 'Platform Governance under the Digital Services Act' (2025) *Information, Communication & Society* <https://doi.org/10.1080/1369118X.2025.2590561>.

¹⁷ Nikolaus von Bernuth, 'The Premise of Good Faith in Platform Regulation: On the Changing Conditions of the Digital Services Act's Regulatory Approach' (Verfassungsblog, 14 April 2025) <https://doi.org/10.59704/5494324c1cc2203d>.

¹⁸ Christian Ollig, *Europäische Plattformverfassungen: Die Konstitutionalisierung digitaler Kommunikationsräume durch Art 14 Abs 4 Digital Services Act* (Mohr Siebeck 2025) <https://doi.org/10.1628/978-3-16-164538-9>

¹⁹ Tim Sprenger, *Das Plattformverfahren: Ausbalancierte Rechtsdurchsetzung mittels Verfahrensgrundsätzen* (Weizenbaum Institute 2024)

²⁰ Наталія Філатова-Білоус, 'Саморегулівні організації: юридичні особи на межі приватного і публічного права' (2024) 2 *Цивілістична платформа* 58 <https://doi.org/10.69724/2786-8834-2024-2-2-58-82>; Філатова Н Ю, *Саморегулівні організації як суб'єкти цивільного права* (дис канд юрид наук, Національний юридичний університет імені Ярослава Мудрого, 2014).

²¹ Olena Honcharenko, Mariia Pozhydaieva, Larysa Neskorozhena and Oleksandra Kolohoida, 'Self-Regulatory Practices of Electronic Trade and Transnational Public Order in the Context of Ensuring the Economic Security of the State' (2024) 36 *Revista Juridica Portucalense* 106 [https://doi.org/10.34625/issn.2183-2705\(36\)2024.ic-5](https://doi.org/10.34625/issn.2183-2705(36)2024.ic-5).Примак В Д, Нескороджена Л Л, 'Основоположні права у цифровому середовищі: практика Суду Європейського Союзу' (2025) 11 *Юридичний науковий електронний журнал* 97 <https://doi.org/10.32782/2524-0374/2025-11/19>;; Наталія Мазаракі, Володимир Примак 'Механізм вирішення спорів між користувачами та онлайн-платформами в Акті ЄС про цифрові послуги' (2026) 19 *Український політико-правовий дискурс* <https://doi.org/10.5281/zenodo.18662891>; Мазаракі Н, Жибак А, 'Зобов'язання гейткіперів, закріплені в Акті про цифрові ринки' (2024) 137(6) *Ius Modernum* 4 [https://doi.org/10.31617/3.2024\(137\)01](https://doi.org/10.31617/3.2024(137)01); Gerasymenko, A., Mazaraki, N. (2023). The "New Normal" in Competition—Filling the Gaps of Ukrainian Competition Law in the Digital Economy Age. In: Richter,

одночасно щодо меж приватної автономії платформ, гарантій прав користувачів, процесуального становища платформ, економічних передумов їхньої влади та співвідношення приватноправових і публічно-правових засад саморегулювання.

Методи дослідження. Методологічну основу дисертації становить сукупність філософських, загальнонаукових та спеціально-юридичних методів, вибір яких зумовлений метою, завданнями та предметом дослідження.

Філософську основу роботи становить діалектичний метод, який дав змогу розглянути саморегулювання онлайн-платформ у розвитку та внутрішній суперечливості — як явище, що еволюціонує від автономної приватної нормотворчості до юридично впорядкованої моделі під впливом суперечності між приватною автономією платформ і публічними інтересами (розділи 1, 3).

Серед загальнонаукових методів визначальну роль відіграли системно-структурний і функціональний. Системно-структурний метод застосовано для розгляду положень DSA як взаємопов'язаних елементів єдиної регуляторної архітектури та для обґрунтування трирівневої моделі регульованого саморегулювання і співрегулювання (підрозділи 3.1–3.3). Функціональний метод використано у двох вимірах: для з'ясування поняття онлайн-платформи через виконувану посередницьку функцію, незалежно від технологічної форми (підрозділ 1.1), та для з'ясування ролі кожної норми DSA в механізмі саморегулювання — впорядкування нормотворчості, процедуризація правозастосування, внутрішній контроль, зовнішня верифікація чи колективне вироблення стандартів (розділ 3). Методи аналізу і синтезу, індукції та дедукції, абстрагування й узагальнення застосовувалися наскрізно.

Основу спеціально-юридичного інструментарію становить формально-юридичний (догматичний) метод, за допомогою якого проаналізовано зміст положень Регламенту 2022/2065 у їх системному зв'язку з преамбулою, підготовчими матеріалами, делегованими актами Комісії та суміжними актами

Н. (eds) Competition and Intellectual Property Law in Ukraine. MPI Studies on Intellectual Property and Competition Law, vol 31. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-66101-7_7;

права ЄС, визначено адресатів, обсяг обов'язків і правові наслідки відповідних норм (розділ 3). Догматичний аналіз доповнено телеологічним тлумаченням, спрямованим на з'ясування регуляторної мети окремих механізмів, зокрема на основі пояснювального меморандуму до пропозиції COM(2020) 825 final та оцінок впливу Комісії.

Порівняльно-правовий метод застосовано у двох формах: для зіставлення американської, китайської та європейської моделей регулювання онлайн-платформ за критеріями джерела нормотворчості, механізму підзвітності та захисту фундаментальних прав (розділ 2), а також для виявлення нормативних прототипів механізмів DSA у попередніх актах права ЄС — праві захисту прав споживачів, праві захисту даних та ін. (розділ 3). Історико-правовий метод дав змогу простежити генезу правового регулювання відносин в інтернеті та еволюцію добровільних інструментів, що передували DSA (підрозділи 1.2, 3.3).

Емпіричну складову методології становить метод аналізу правозастосовної практики: досліджено першу практику Європейської Комісії та координаторів цифрових послуг щодо VLOPs/VLOSEs, рішення про визначення VLOPs/VLOSEs, звіти платформ про оцінку системних ризиків, аудиторські звіти першого циклу та звіт Європейської ради з цифрових послуг за ст. 35(2) DSA (розділ 3).

Наукова новизна отриманих результатів. Дисертація є науковим дослідженням, у якому запропоновано цілісну концепцію регульованого саморегулювання онлайн-платформ у праві ЄС як моделі, за якої приватна нормотворчість і приватне правозастосування платформ зберігаються, але підпорядковуються юридично обов'язковим вимогам прозорості, належної процедури, пропорційності, підзвітності та зовнішнього контролю. Конкретними результатами наукового дослідження, що містять наукову новизну, слід визнати такі:

Уперше:

обґрунтовано трирівневу модель регульованого саморегулювання та співрегулювання онлайн-платформ у DSA, яка охоплює: базовий процедурний рівень платформного саморегулювання (ст. 14, 16, 17, 20, 21), посилений ризик-

орієнтований рівень для VLOPs/VLOSEs, що поєднує метарегулювання внутрішніх систем управління (ст. 34, 35, 41) із зовнішньою верифікацією та підзвітністю (ст. 37, 40, 42), і власне співрегуляторний рівень колективних інструментів (ст. 45–48);

– сформульовано критерій розмежування регульованого саморегулювання та співрегулювання за походженням і функцією приватних правил: у співрегулюванні приватне нормотворення слугує засобом реалізації публічно визначених цілей, тоді як у регульованому саморегулюванні право впорядковує та обмежує самостійно сформовану приватну нормотворчість, не делегуючи повноваження на її створення.

Удосконалено:

— поняття саморегулювання онлайн-платформ з урахуванням його структурної специфіки, яка полягає в тому, що, на відміну від класичного галузевого саморегулювання, платформи регулюють переважно поведінку третіх осіб — користувачів, рекламодавців і бізнес-користувачів, що зближує платформну нормотворчість із приватним управлінням та загострює проблему її легітимності;

— наукові підходи до визначення правової природи умов користування онлайн-платформами як актів подвійної природи: договірної за формою та регуляторної за функцією, що обґрунтовує поширення на них не лише механізмів договірного права, а й публічно-правових вимог щодо прозорості, пропорційності, недискримінаційності, процедурної справедливості та підзвітності;

— характеристику добровільності співрегуляторних інструментів DSA як відносної та функціонально обмеженої: обґрунтовано, що їхній зв'язок із заходами мінімізації системних ризиків за ст. 35(1)(h) DSA, положеннями преамбули 104 та можливістю аудиторської перевірки відповідних зобов'язань за ст. 37 DSA робить межу між добровільним співрегулюванням і фактично обов'язковою регуляторною поведінкою рухливою та залежною від практики Європейської Комісії.

Набули подальшого розвитку:

— доктринальні положення щодо застосування теорій реагувального регулювання, метарегулювання та децентрованого регулювання до платформного середовища шляхом розмежування їхньої природи та функцій: реагувального регулювання — як стратегії диференційованого правозастосування,

метарегулювання — як способу правового впливу на внутрішні системи управління регульованого суб'єкта, децентрованого регулювання — як моделі розподілу регуляторних функцій між публічними та приватними акторами;

— наукові уявлення про генезу регуляторної моделі DSA: обґрунтовано, що регульоване саморегулювання не є новоствореною конструкцією Регламенту, а розвиває усталені техніки права Європейського Союзу, апробовані у праві захисту прав споживачів, праві захисту персональних даних і регулюванні медіа, а також кодифікує окремі стандарти прозорості, добросовісності, пропорційності та процедурної справедливості, які раніше формувалися у національній судовій практиці засобами договірного права;

— положення щодо порівняльно-правової характеристики американської, китайської та європейської моделей регулювання онлайн-платформ, що дало змогу визначити модель DSA як самостійну регуляторну конструкцію, яка займає проміжне місце між широкою автономією платформного саморегулювання та державно-центричним імперативним контролем і поєднує приватну нормотворчість із публічно-правовими вимогами, зовнішнім наглядом та механізмами відповідальності.

Особистий внесок здобувача. Дисертаційне дослідження виконано здобувачем самостійно, усі сформульовані в ньому положення та висновки обґрунтовано на основі власних досліджень автора. Нові наукові результати дисертації отримані дисертантом особисто.

Апробація результатів дисертаційного дослідження. Основні положення дисертації оприлюднено на восьми міжнародних та всеукраїнських науково-практичних конференціях і круглих столах: міжнародна наукова конференція «Нові підходи та сучасні правові дослідження» (м. Рига, Латвійська Республіка, 3–4 листопада 2022 р.); науково-практична конференція «Юридичні науки: проблеми та перспективи» (м. Запоріжжя, 24–25 лютого 2023 р.); міжнародна науково-практична конференція «Євроінтеграційні процеси в Україні: історичні, культурні, політико-правові та психологічні аспекти» (м. Київ, 12–13 квітня 2023 року); міжнародна наукова конференція «Тенденції розвитку юридичної науки та

освіти України в контексті європейської інтеграції»: матеріали конференції (м. Ченстохова, Республіка Польща 1–2 листопада 2023 р.); міжнародна науково-практична конференція молодих учених та студентів «Юридична осінь 2023» (м. Харків, 17 листопада 2023 р.); круглий стіл «Правове регулювання цифрової економіки: правові інструменти, можливості та виклики» (м. Київ, 21 листопада 2023 року); міжнародна науково-практична конференція «Становлення та розвиток правової держави: проблеми теорії та практики» (м. Миколаїв, 21 грудня 2023 р.); міжнародна науково-практична конференція «Фундаментальні та прикладні проблеми суспільства: історія, сьогодення, майбутнє» (м. Київ, 11 квіт. 2024 р.).

Публікації. Основні положення та висновки дослідження відображені у 12 одноосібних наукових працях, з них: 4 наукові статті – у виданнях, включених МОН України до переліку наукових фахових видань з юридичних наук, зареєстрованих та проіндексованих у міжнародних наукометричних базах даних (Index Copernicus); 8 тез доповідей, опублікованих у збірниках матеріалів науково-практичних міжнародних, всеукраїнських конференцій і круглих столів.

Структура та обсяг дисертації. Робота складається зі вступу, трьох розділів, що містять вісім підрозділів, висновків, списку використаних джерел, а також додатків. Загальний обсяг дисертації становить 181 сторінку, з яких основний текст займає 144 сторінки. Список використаних джерел складається з 201 найменування і займає 14 сторінок.

РОЗДІЛ 1. ДОКТРИНАЛЬНІ ПІДХОДИ ДО РОЗУМІННЯ САМОРЕГУЛЮВАННЯ

1.1. Онлайн-платформи як особливий об'єкт регулювання

Дослідження регуляторних механізмів, запроваджених Digital Services Act, неможливе без попереднього з'ясування природи об'єкта, на який вони спрямовані. Онлайн-платформи є не просто технологічними інструментами або суб'єктами господарювання у традиційному розумінні — вони являють собою якісно новий тип соціального інституту, що поєднує ознаки ринкового посередника, інфраструктури публічної комунікації та приватного регулятора. Саме ця гібридна природа робить платформи особливим об'єктом правового регулювання і зумовлює недостатність традиційних регуляторних підходів.

Метою цього підрозділу є встановлення правової та економічної природи онлайн-платформ як передумова для подальшого аналізу регуляторних моделей. Послідовно розкриваються чотири взаємопов'язані аспекти: по-перше, понятійний апарат і типологія платформ у доктрині та позитивному праві ЄС; по-друге, економічна логіка платформних ринків, що породжує структурну асиметрію між платформою і користувачем; по-третє, трансформація платформ від приватних сервісів до інфраструктури публічної комунікації; по-четверте, нормотворчі та виконавчі функції платформ, що надають їм ознак приватного регулятора. Завершальний параграф систематизує регуляторні виклики, специфічні для платформного середовища, і тим самим створює аналітичне підґрунтя для наступного підрозділу, присвяченого концепціям саморегулювання як первинної відповіді на ці виклики. З методологічної точки зору підрозділ поєднує догматичний аналіз нормативних визначень із доктринальним синтезом економічної та правової літератури. Для з'ясування поняття платформи використовується функціональний підхід, що дозволяє уникнути прив'язки до конкретних технологічних рішень. Там, де правова природа платформ є дискусійною в доктрині, застосовується порівняльний аналіз позицій з метою

вироблення авторської концептуалізації, релевантної для цілей дисертаційного дослідження.

1.1.1. Поняття та типологія онлайн-платформ

Термін «платформа» у його сучасному технологічному значенні почав використовуватися у 1990-х роках у середовищі розробників програмного забезпечення для позначення не окремої програми, а гнучкої обчислювальної основи, на якій могли створюватися та функціонувати інші програмні рішення. Широкого поширення це поняття набуло на початку 2000-х років у контексті Web 2.0 та розвитку контенту, створюваного користувачами. У цьому розумінні визначальною ознакою платформи є її програмованість: як зазначав Марк Андріссен, платформа становить систему, яку зовнішні розробники або користувачі можуть перепрограмувати й адаптувати до потреб, не передбачених її первинними розробниками²².

Попри центральну роль онлайн-платформ у сучасній цифровій економіці та суспільному житті, їх правова дефініція тривалий час залишалася предметом доктринальної дискусії, не отримуючи уніфікованого закріплення ні в праві ЄС, ні в національних правових системах держав-членів. Ця понятійна невизначеність не була випадковою: вона відображала принципову складність феномену, що поєднує технологічні, економічні та соціальні виміри, жоден з яких не є достатнім для вичерпної правової характеристики.

У доктрині сформувалися три основні підходи до визначення онлайн-платформ. Функціональний підхід акцентує на ролі платформи як посередника між двома або більше групами користувачів, що взаємодіють через спільний технологічний інтерфейс. У межах цього підходу визначальною ознакою платформи є не характер контенту чи послуги, а організація взаємодії між сторонами, які без платформи не вступили б у контакт або зробили б це зі значно

²² Robert Gorwa, *The Politics of Platform Regulation: How Governments Shape Online Content Moderation* (Oxford University Press 2024) 13–14, який цитував Ian Bogost and Nick Montfort, 'Platform Studies: Frequently Questioned Answers' (Digital Arts and Culture 2009 Conference, 2009) 4, and Marc Andreessen, 'The Three Kinds of Platforms You Meet on the Internet' (16 September 2007) https://pmarchive.com/three_kinds_of_platforms_you_meet_on_the_internet.html

вищими транзакційними витратами. Перевагою функціонального підходу є його технологічна нейтральність: він охоплює якісно різні суб'єкти — від соціальних мереж до маркетплейсів — не прив'язуючись до конкретного технологічного рішення. Саме цей підхід імпліцитно покладений в основу регуляторної концепції DSA²³.

Економічний підхід, що спирається на теорію багатосторонніх ринків, визначає платформу через структуру її ринкової взаємодії: платформа обслуговує щонайменше дві відмінні групи користувачів, між якими існують непрямі мережеві ефекти, тобто цінність послуги для однієї групи залежить від кількості або поведінки іншої. Цей підхід є аналітично потужним для розуміння ринкової влади платформ і їх схильності до природної монополізації, проте має обмежену нормативну цінність: він описує економічну логіку, але не визначає правових наслідків²⁴.

Технологічний підхід зосереджується на алгоритмічному управлінні як конститутивній ознаці платформи: саме алгоритми ранжування, рекомендацій і таргетування відрізняють сучасну платформу від пасивного технічного каналу передачі інформації. Цей підхід набуває особливої регуляторної релевантності в контексті DSA, який приділяє значну увагу рекомендаційним системам (ст. 27, 38 DSA) та алгоритмічній прозорості саме тому, що алгоритмічне управління

²³ Miriam C Buiten, 'The Digital Services Act: From Intermediary Liability to Platform Regulation' (2021) 12(3) JIPITEC 361; Christoph Busch and Vanessa Mak, 'Putting the Digital Services Act in Context: Bridging the Gap between EU Consumer Law and Platform Regulation' (2021) 10 Journal of European Consumer and Market Law 109; Christoph Busch, 'Regulating the Expanding Content Moderation Universe: A European Perspective on Infrastructure Moderation' (2022) 27 UCLA Journal of Law & Technology 32; Thomas Poell, David Nieborg and José van Dijck, 'Platformisation' (2019) 8(4) Internet Policy Review 1.

²⁴ Jean-Charles Rochet and Jean Tirole, 'Platform Competition in Two-Sided Markets' (2003) 1 Journal of the European Economic Association 990; Mark Armstrong, 'Competition in Two-Sided Markets' (2006) 37 RAND Journal of Economics 6684 David S Evans, 'The Antitrust Economics of Multi-Sided Platform Markets' (2003) 20 Yale Journal on Regulation 325; David S Evans and Richard Schmalensee, 'The Industrial Organization of Markets with Two-Sided Platforms' (2007) 3 Competition Policy International 151; Bernard Caillaud and Bruno Jullien, 'Chicken & Egg: Competition among Intermediation Service Providers' (2003) 34 RAND Journal of Economics 309.

перетворює платформу на активного формувача інформаційного середовища користувача²⁵.

Жоден із зазначених підходів окремо не є достатнім для цілей правового регулювання. Функціональний підхід надто широкий і охоплює суб'єктів із принципово різним соціальним впливом; економічний підхід ігнорує публічно-правовий вимір платформної діяльності; технологічний підхід ризикує швидко застаріти в умовах технологічних змін. Тому сучасна доктрина тяжіє до інтегративних визначень, що поєднують елементи всіх трьох підходів.

На рівні позитивного права ЄС одне із перших законодавчих визначень «онлайн-платформи» закріплено у ст. 3(i) DSA: це «постачальник послуги хостингу, який на прохання отримувача послуги зберігає та поширює інформацію серед громадськості, якщо така діяльність не є незначною функцією іншої послуги». Це визначення є функціональним за своєю природою і свідомо широким: воно охоплює якісно різні суб'єкти, диференціація між якими здійснюється не через дефініцію, а через диференційовані рівні зобов'язань залежно від розміру та впливу платформи. Європейська Комісія (далі – ЄК) виходила з інформаційно-посередницької, а не суто економічної логіки визначення онлайн-платформи. Онлайн-платформа розглядалася як підвид хостингової послуги, який не лише зберігає інформацію на запит користувача, а й поширює її для публіки. Така дефініція дозволяла побудувати градуйовану систему обов'язків: від загальних правил для всіх посередницьких послуг до спеціальних обов'язків для платформ і посилених обов'язків для дуже великих платформ. Водночас Комісія прагнула уникнути надмірно широкого охоплення, тому виключила випадки, коли публічне

²⁵ Julie E Cohen, 'Law for the Platform Economy' (2017) 51 UC Davis Law Review 133; Karen Yeung, 'Hypertext: Big Data as a Mode of Regulation through the Design of Choice Architecture' (2017) 20(1) Information, Communication & Society 118; Fabiana Di Porto and Marialuisa Zuppetta, 'Co-regulating Algorithmic Disclosure for Digital Platforms' (2021) 40(2) Policy and Society 272

поширення інформації є лише незначною і суто допоміжною функцією іншої основної послуги²⁶.

DSA не подає вичерпного переліку видів онлайн-платформ, але його визначення дозволяє віднести до цієї категорії різні цифрові сервіси, якщо вони на запит користувача зберігають і поширюють інформацію для публіки. До таких сервісів можуть належати соціальні мережі, платформи для обміну відеоконтентом, онлайн-маркетплейси, магазини застосунків, платформи для бронювання подорожей і розміщення, а також інші сервіси з подібною інформаційно-посередницькою функцією. Водночас пошукові системи в DSA становлять окрему категорію посередницьких послуг і не ототожнюються з онлайн-платформами у вузькому значенні. Регуляторна специфіка відповідних сервісів визначається виконуваною функцією, характером користувацької взаємодії, способом поширення інформації, роллю алгоритмічного ранжування та масштабом потенційного впливу на публічну комунікацію, споживчі відносини й суспільні ризики.

Масштаб онлайн-платформи є самостійною ознакою її регуляторної класифікації у DSA. Регламент виходить із того, що не всі платформи створюють однаковий рівень суспільних ризиків: чим більшою є кількість користувачів, тим вищою є здатність платформи впливати на поширення інформації, споживчу поведінку, публічну комунікацію та демократичні процеси. Саме тому DSA виокремлює категорію дуже великих онлайн-платформ та дуже великих онлайн-пошукових систем, які охоплюють щонайменше 45 млн середньомісячних активних отримувачів послуги в ЄС. Такий кількісний критерій має не лише технічне, а й регуляторне значення: він слугує підставою для покладення на найбільші платформи посилених обов'язків щодо оцінки і мінімізації системних ризиків, незалежного аудиту, прозорості алгоритмічних систем, доступу

²⁶ Commission, 'Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC' COM (2020) 825 final.

дослідників до даних та посиленого публічного нагляду. Отже, у DSA масштаб платформи виступає індикатором її потенційної суспільної влади та обґрунтовує диференційований регуляторний вплив.

Таким чином, поняття онлайн-платформи у праві ЄС є результатом свідомого регуляторного вибору на користь функціонального підходу з елементами технологічного, що забезпечує достатню широту охоплення при збереженні регуляторної гнучкості. Типологія платформ, закріплена у практиці Комісії з призначення VLOP, демонструє, що законодавець усвідомлює якісні відмінності між різними типами платформ, хоча формально не кодифікує цю типологію у тексті Регламенту.

Водночас онлайн-платформу як цифровий сервіс необхідно відмежовувати від юридичної особи, яка забезпечує його функціонування. Назва платформи, відома користувачам, часто є лише комерційним позначенням окремого сервісу, тоді як його власником, оператором або постачальником може виступати одна з юридичних осіб складної корпоративної групи. DSA не пов'язує статус постачальника онлайн-платформи з конкретною організаційно-правовою формою, державою реєстрації чи структурою власності. Адресатом установлених Регламентом обов'язків є саме «постачальник посередницької послуги» — фізична або юридична особа, яка надає відповідну послугу, а не бренд, вебсайт, застосунок чи корпоративна група загалом. Тому для визначення суб'єкта прав та обов'язків у кожному конкретному випадку необхідно встановити, яка юридична особа фактично і юридично надає сервіс користувачам, визначає умови користування, організовує модерацію контенту та вступає з ними у договірні відносини. Такий підхід чітко простежується у рішеннях Європейської Комісії про визначення дуже великих онлайн-платформ²⁷: статус VLOP надається певному сервісу, однак відповідне рішення адресується конкретному його постачальнику, наприклад Meta Platforms Ireland Limited щодо Facebook та Instagram, Google Ireland Limited щодо низки сервісів Google або Amazon EU S.à r.l. щодо Amazon Store. При цьому, одна

²⁷ European Commission, 'Supervision of the Designated Very Large Online Platforms and Search Engines under DSA'

корпоративна група може надавати кілька окремих платформних послуг, кожна з яких кваліфікується самостійно: так, рішеннями Комісії про десигнацію VLOPs Facebook та Instagram визначені як окремі дуже великі онлайн-платформи, хоча обидві послуги надає той самий провайдер — Meta Platforms Ireland Limited²⁸. Пороги (зокрема 45 млн активних отримувачів для VLOP/VLOSE) також обчислюються за кожною послугою окремо. Отже, у правовому значенні платформа є функціонально визначеним цифровим сервісом, тоді як носієм пов'язаних із ним юридичних обов'язків виступає конкретний постачальник цього сервісу.

Територіальна дія DSA також не залежить від організаційно-правової форми або місця реєстрації постачальника. Регламент застосовується до посередницьких послуг, що пропонуються отримувачам, які перебувають або засновані в ЄС, незалежно від місця заснування самого постачальника. Якщо постачальник не має установи в ЄС, він зобов'язаний призначити в одній із держав-членів фізичну або юридичну особу своїм законним представником. Такий представник є адресатом комунікацій і рішень органів нагляду та за певних умов може нести відповідальність за невиконання вимог DSA, однак його призначення не змінює того, що первинним адресатом матеріальних обов'язків залишається постачальник послуги, і саме по собі не створює установи постачальника в ЄС.

1.1.2 Економічна природа платформ

Розуміння правової природи онлайн-платформ як особливого об'єкта регулювання неможливе без аналізу їхньої економічної логіки. Економічні характеристики платформних ринків — зокрема мережеві ефекти, ефекти масштабу, накопичення даних, інформаційна асиметрія та залежність користувачів від доступу до платформної інфраструктури — зумовлюють регуляторні виклики, які не можуть бути повністю охоплені традиційними правовими інструментами,

²⁸ Commission Decisions of 25 April 2023 designating Facebook and Instagram as very large online platforms pursuant to Article 33(4) of Regulation (EU) 2022/2065; тексти рішень: Commission, 'Designation Decisions for the First Set of Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs)' (20 December 2023) <https://digital-strategy.ec.europa.eu/en/library/designation-decisions-first-set-very-large-online-platforms-vlops-and-very-large-online-search>

розробленими для лінійних ринкових відносин індустріальної економіки. Вони також пояснюють, чому автономне саморегулювання платформ не може вважатися достатнім механізмом гарантування справедливості та захисту публічних інтересів: платформи мають власні комерційні стимули щодо організації видимості контенту, модерації, ранжування, реклами та взаємодії користувачів. Саме тому право ЄС переходить від довіри до автономного саморегулювання платформ до моделі встановлення правових меж їхньої регуляторної влади, що у DSA проявляється через обов'язки прозорості, процедурні гарантії, оцінку системних ризиків, незалежний аудит і публічний нагляд.

Онлайн-платформи функціонують як організатори багатосторонніх ринків — особливого типу економічних структур, у межах яких посередник забезпечує взаємодію між двома або більше відмінними групами користувачів, пов'язаними непрямыми мережевими ефектами. Концептуальні засади теорії багатосторонніх ринків були сформульовані у працях J.-C. Rochet і J. Tirole²⁹, які показали, що ціноутворення в таких структурах принципово відрізняється від традиційних односторонніх ринків: платформа може субсидіювати одну сторону ринку за рахунок іншої, оскільки її метою є максимізація загальної цінності мережевої взаємодії. Саме тому пошукові системи та соціальні мережі часто надають послуги кінцевим користувачам без грошової оплати, фінансуючи свою діяльність за рахунок рекламодавців, яким забезпечується доступ до сформованої аудиторії.

Така асиметрія ціноутворення не є ринковою аномалією, а становить структурну ознаку платформної економіки. Вона має істотні правові наслідки, оскільки формальна «безкоштовність» послуги для користувача не означає відсутності економічного обміну. Натомість вона ускладнює застосування традиційних споживчо-правових і конкурентно-правових категорій, побудованих навколо ціни, прямої оплати та лінійних відносин між продавцем і споживачем. У платформному середовищі економічна цінність формується через дані, увагу користувачів, мережеві ефекти, алгоритмічне ранжування та доступ до аудиторії.

²⁹ Jean-Charles Rochet and Jean Tirole, 'Platform Competition in Two-Sided Markets' (2003) 1 Journal of the European Economic Association 990

Саме ці характеристики пояснюють, чому платформи набувають не лише ринкової, а й регуляторної влади над умовами цифрової взаємодії, що, у свою чергу, обґрунтовує необхідність їх правового впорядкування у межах DSA.

Визначальною економічною рисою платформних ринків є мережеві ефекти — механізм, за якого цінність послуги для окремого користувача зростає зі збільшенням кількості інших учасників мережі. Прямі мережеві ефекти виникають усередині однієї групи користувачів, наприклад коли більша кількість учасників соціальної мережі підвищує її цінність для кожного з них. Непрямі мережеві ефекти виникають між різними групами користувачів, наприклад коли збільшення аудиторії соціальної мережі підвищує її привабливість для рекламодавців. Взаємодія прямих і непрямих мережевих ефектів створює тенденцію до концентрації, оскільки велика платформа здатна накопичувати аудиторію, дані, рекламні доходи та технологічні ресурси, які посилюють її конкурентну позицію. У таких умовах ринки можуть тяжіти до структури “winner takes most”, коли домінуюча платформа отримує самопідтримувальну перевагу, а вхід нових учасників ускладнюється через високі бар’єри доступу до користувачів, даних і рекламної інфраструктури³⁰. У праві ЄС ця економічна особливість відображена у диференційованому підході до найбільших цифрових посередників: DSA встановлює посилені обов’язки для дуже великих онлайн-платформ і пошукових систем, що охоплюють понад 45 млн середньомісячних активних отримувачів у ЄС, тоді як DMA окремо регулює “gatekeepers” як найбільші платформи, що є важливими шлюзами між бізнес-користувачами та кінцевими користувачами.

Значна частина великих онлайн-платформ, передусім соціальні мережі, відеоплатформи та пошукові системи, функціонує в межах економіки уваги, у якій ключовим ресурсом є увага користувача, а одним із головних джерел доходу —

³⁰ Michael L Katz and Carl Shapiro, ‘Network Externalities, Competition, and Compatibility’ (1985) 75 American Economic Review 424; Jean-Charles Rochet and Jean Tirole, ‘Platform Competition in Two-Sided Markets’ (2003) 1 Journal of the European Economic Association 990

надання рекламодавцям доступу до цієї уваги. Така модель створює структурне напруження для саморегулювання: платформа комерційно зацікавлена у збільшенні часу перебування користувача на сервісі, інтенсивності взаємодії та обсягу зібраних поведінкових даних. Це може стимулювати алгоритмічне просування контенту, який викликає високу емоційну залученість, навіть якщо такий контент є маніпулятивним, поляризуючим або соціально шкідливим. У концепції “surveillance capitalism” Shoshana Zuboff описує поведінкові дані користувачів як сировину для прогнозування й комерціалізації майбутньої поведінки. У такому контексті добровільне саморегулювання платформ має внутрішні обмеження, оскільки належна модерація, обмеження шкідливого контенту, прозорість алгоритмічного ранжування та мінімізація маніпулятивних практик можуть не збігатися з короткостроковими комерційними стимулами платформи³¹. Саме це пояснює потребу у зовнішніх правових вимогах до прозорості, оцінки системних ризиків, підзвітності та публічного нагляду, які в DSA покликані компенсувати структурні дефіцити автономного платформного саморегулювання.

Окрім мережевих ефектів, ринкову владу онлайн-платформ посилюють ефекти блокування користувачів та переваги, пов’язані з накопиченням даних. Ефекти блокування виникають тоді, коли перехід користувача до альтернативної платформи пов’язаний не лише з технічною зміною сервісу, а й із втратою накопичених соціальних зв’язків, контенту, історії взаємодій, репутації, відгуків, налаштувань або доступу до сформованої аудиторії. Такі витрати переходу знижують інтенсивність конкурентного тиску навіть за наявності функціонально подібних або якісніших альтернатив. Додатковим джерелом стійкості платформної влади є залежність від даних: великі платформи акумулюють значні масиви поведінкових даних, які використовуються для вдосконалення алгоритмічного ранжування, персоналізації, таргетованої реклами, рекомендаційних систем і

³¹ Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (PublicAffairs 2019); Tim Wu, *The Attention Merchants: The Epic Scramble to Get Inside Our Heads* (Knopf 2016)

модерації контенту. За певних умов така перевага даних набуває самопідтримувального характеру: більша кількість користувачів генерує більше даних, більше даних підвищує якість сервісу, а вища якість сервісу, своєю чергою, приваблює нових користувачів. У такий спосіб дані стають не лише ресурсом конкуренції, а й додатковим бар'єром входу, який виходить за межі традиційного розуміння економії на масштабі³².

Описана економічна логіка платформних ринків має безпосередні правові наслідки, що визначають специфіку їх регулювання. По-перше, асиметрія переговорної сили між платформою і користувачем є настільки значною, що ставить під сумнів ефективність суто договірних механізмів захисту прав користувачів: Terms of Service, формально прийняті на добровільних засадах, фактично функціонують як договори приєднання з обмеженою можливістю індивідуального погодження або реальної альтернативи. По-друге, тенденція платформних ринків до концентрації зумовлює системний характер ризиків, пов'язаних із діяльністю найбільших платформ: недоліки модерації, алгоритмічного ранжування або управління контентом на одній великій платформі можуть одночасно впливати на мільйони користувачів і на якість публічної комунікації загалом. По-третє, конфлікт інтересів, властивий економіці уваги, обмежує можливість покладатися на добровільне саморегулювання як достатній механізм захисту суспільних інтересів.

Таким чином, економічна природа онлайн-платформ безпосередньо впливає на підходи до їх регулювання. Розуміння мережеских ефектів, структури багатосторонніх ринків, ефектів блокування, залежності від даних і конфлікту інтересів в економіці уваги є необхідною передумовою для пояснення того, чому DSA не покладається виключно на ринкові механізми або добровільні кодекси поведінки, а встановлює багаторівневу систему правових обов'язків для онлайн-платформ, особливо для дуже великих онлайн-платформ і пошукових систем.

1.1.3. Онлайн-платформи як інфраструктура публічної комунікації

³² John M Newman, 'Attention Capitalism: The Law and Political Economy of Attention Markets' (2026) 78 Stanford Law Review 415

Економічна логіка платформних ринків є необхідною, але недостатньою передумовою для розуміння онлайн-платформ як особливого об'єкта правового регулювання. Поряд з економічним виміром онлайн-платформи набули якісно нової соціальної функції: вони стали однією з ключових інфраструктур публічної комунікації сучасного суспільства. Через соціальні мережі, відеоплатформи, пошукові системи, маркетплейси та інші цифрові посередницькі сервіси користувачі отримують доступ до інформації, беруть участь у публічному дискурсі, поширюють власні погляди, здійснюють економічну діяльність і взаємодіють з іншими особами. Саме ця трансформація — від приватних цифрових сервісів до інфраструктур, що організовують значну частину цифрової комунікації, — пояснює, чому питання платформного саморегулювання набуває не лише приватноправового, а й публічно-правового та конституційно значущого виміру.

Цей процес у сучасній доктрині часто описується через поняття «платформізації» (platformisation)³³. Йдеться про поступове проникнення платформної логіки у різні сфери соціального, культурного, економічного і політичного життя. Платформи не лише надають технічний інтерфейс для взаємодії користувачів, а й встановлюють порядок та умови цієї взаємодії: визначають правила доступу до сервісу, умови видимості контенту, механізми ранжування, способи монетизації, процедури модерації та санкції за порушення правил.

Близькою до цього є концепція «інфраструктуризації платформ»³⁴. Вона підкреслює, що великі онлайн-платформи поступово набувають ознак інфраструктури: вони стають вбудованими у повсякденні соціальні практики, забезпечують доступ до аудиторії, створюють умови для професійної, політичної, культурної та економічної активності, а їхня відсутність або обмеження доступу до них може істотно впливати на можливості користувачів діяти у цифровому середовищі. Водночас ця аналогія з класичними інфраструктурами не означає автоматичного перенесення на платформи режимів, характерних для залізниць,

³³ Thomas Poell, David Nieborg and José van Dijck, 'Platformisation' (2019) 8(4) *Internet Policy Review* DOI: 10.14763/2019.4.1425

³⁴ Jean-Christophe Plantin, Carl Lagoze, Paul N Edwards and Christian Sandvig, 'Infrastructure Studies Meet Platform Studies in the Age of Google and Facebook' (2018) 20(1) *New Media & Society* 293

електромереж чи телекомунікаційних систем. Її значення полягає радше в тому, що суспільна значущість платформ обґрунтовує посилення публічно-правових вимог до прозорості, підзвітності та недискримінаційності їхньої діяльності.

Особливе значення онлайн-платформи мають для публічного дискурсу. Соціальні мережі, пошукові системи та платформи для обміну контентом стали важливими середовищами, у яких формується суспільна думка, здійснюється політична комунікація, організовується громадянська активність³⁵ і реалізується свобода вираження поглядів. Однак платформи не є нейтральними провідниками комунікації. Через дизайн інтерфейсу, алгоритмічне ранжування, рекомендаційні системи, правила модерації та комерційні стимули вони впливають на те, який контент стає видимим, який маргіналізується, який видаляється, а який отримує алгоритмічне поширення. Отже, платформи не лише відображають публічну сферу, а й активно структурують її.

Саме тут виникає центральна правова проблема. З формально-правового погляду платформи залишаються приватними суб'єктами, що діють у межах свободи підприємництва, договірної автономії та права власності на цифрову інфраструктуру. Водночас їхні рішення щодо модерації контенту, блокування акаунтів, демонетизації, алгоритмічного ранжування або обмеження видимості мають наслідки для реалізації фундаментальних прав користувачів, зокрема свободи вираження поглядів, доступу до інформації, недискримінації, захисту персональних даних, свободи підприємницької діяльності та участі у демократичному процесі. Через це платформні правила не можуть розглядатися виключно як приватні умови користування, що мають значення лише для договірних відносин між платформою і користувачем.

³⁵ Саме у цьому контексті показовим є початок Євромайдану. 21 листопада 2013 р. журналіст Мустафа Найєм опублікував у Facebook заклик вийти о 22:30 до монумента Незалежності в Києві, додавши: «Одягайтеся тепло, беріть парасолі, чай, каву, гарний настрій і друзів». Цей допис, поширений через соціальну мережу, став одним із символічних прикладів того, як онлайн-платформа може виконувати функцію не лише каналу інформування, а й інструменту політичної мобілізації та організації громадянської дії.

У доктрині ця проблема часто описується як приватизація публічного простору або приватне управління публічним дискурсом³⁶. Йдеться про ситуацію, коли простори, у яких фактично реалізуються публічні права та свободи, перебувають під контролем приватних суб'єктів, що керуються власними комерційними інтересами і не є державними органами. Така ситуація не означає, що платформи слід повністю прирівнювати до держави або автоматично покладати на них ті самі конституційні обов'язки, які мають публічні органи. Однак вона ставить питання про необхідність правових механізмів, які б обмежували приватну регуляторну владу платформ і забезпечували мінімальні гарантії прозорості, належної процедури, оскарження та врахування фундаментальних прав користувачів.

Порівняння онлайн-платформ із традиційними засобами масової інформації також має обмежене пояснювальне значення. Традиційні медіа здебільшого діють як редактори контенту і несуть відповідальність за власні редакційні рішення. Онлайн-платформи, натомість, організовують інфраструктуру, через яку у великому масштабі циркулює контент третіх осіб. Вони не створюють основний масив цього контенту, але визначають умови його видимості, поширення, обмеження або видалення. Крім того, контентні рішення платформ часто приймаються не лише людьми, а й автоматизованими системами, що здійснюють ранжування, рекомендацію, фільтрацію або попередню модерацію мільярдів одиниць контенту. Саме тому регулювання платформ не може бути простим продовженням класичного медіарегулювання³⁷.

Саме тому поріг у 45 мільйонів середньомісячних активних отримувачів послуги в ЄС має не лише кількісне, а й регуляторне значення. Він ідентифікує сервіси, чий масштаб створює потенційно системний вплив на публічну

³⁶ Kate Klonick, 'The New Governors: The People, Rules, and Processes Governing Online Speech' (2018) 131 *Harvard Law Review* 1598; Hannah Bloch-Wehba, 'Global Platform Governance: Private Power in the Shadow of the State' (2019) 72 *SMU Law Review* 27

³⁷ Natali Helberger, 'The Political Power of Platforms: How Current Attempts to Regulate Misinformation Amplify Opinion Power' (2020) 8(6) *Digital Journalism* 84; Damian Tambini (ed), *Regulating Big Tech: Policy Responses to Digital Dominance* (Oxford University Press 2021)

комунікацію, споживчі відносини, виборчі процеси, захист неповнолітніх, громадську безпеку та фундаментальні права. Саме тому такі сервіси підпадають під найбільш інтенсивний режим нагляду і додаткові обов'язки щодо оцінки та мінімізації системних ризиків.

Отже, трансформація онлайн-платформ із приватних цифрових сервісів у ключові інфраструктури публічної комунікації є одним із головних чинників, що пояснює необхідність їхнього публічно-правового регулювання. Якщо економічний аналіз платформ показує структурну асиметрію влади, мережеві ефекти, концентрацію та конфлікт інтересів, то аналіз платформ як комунікаційної інфраструктури додає конституційно значущий вимір. Платформи організовують доступ до аудиторії, структурують видимість інформації, встановлюють правила допустимої поведінки та застосовують санкції до користувачів. Тому їхнє саморегулювання не може залишатися повністю автономним. У DSA ця логіка втілена у моделі регульованого саморегулювання, що поєднує приватні правила платформ із публічно-правовими вимогами прозорості, належної процедури, підзвітності, оцінки системних ризиків і врахування фундаментальних прав користувачів.

1.1.4 Онлайн-платформа як регулятор

Попередні параграфи показали економічну природу онлайн-платформ та їхню роль як інфраструктури публічної комунікації. У сукупності ці характеристики дозволяють сформулювати ключовий висновок для подальшого дослідження: онлайн-платформи є не лише об'єктами правового регулювання, а й приватними регуляторами, які самостійно встановлюють правила поведінки, організовують їх застосування та застосовують санкції до користувачів. Саме ця подвійна природа платформ — одночасно як адресатів правових вимог і як суб'єктів приватного регулювання цифрового середовища — визначає складність регуляторної архітектури DSA. Відповідно, аналіз DSA має враховувати не лише те, як право ЄС регулює платформи, а й те, як самі платформи регулюють поведінку користувачів і умови публічної комунікації.

Найбільш очевидним проявом регуляторної функції платформ є їхня нормотворча діяльність через умови користування, стандарти спільноти, політики модерації, рекламні правила, правила монетизації та інші внутрішні документи. За формально-правовою природою такі документи здебільшого є умовами договору приєднання. Однак за функціональним змістом вони виходять за межі звичайного приватноправового договору, оскільки встановлюють правила поведінки для великих груп користувачів і визначають умови доступу до цифрової комунікаційної інфраструктури. Вони окреслюють допустимі та недопустимі форми висловлювання, регулюють порядок публікації контенту, встановлюють процедури подання скарг і оскарження рішень, визначають правила щодо інтелектуальної власності, персональних даних, реклами, політичного контенту, монетизації та санкцій за порушення правил³⁸.

У цьому сенсі умови користування та стандарти спільноти можуть розглядатися як форми приватного нормотворення, або *lex privata*³⁹. Їхня особливість полягає в тому, що вони створюються односторонньо, змінюються за ініціативою платформи, застосовуються до дуже широкої аудиторії та фактично визначають межі участі користувача у цифровому середовищі. Користувач формально погоджується з такими правилами, але на практиці часто не має можливості вести переговори щодо їх змісту або обрати функціонально рівноцінну альтернативу, особливо якщо йдеться про великі платформи, що забезпечують доступ до значної аудиторії. Саме тому платформні правила не можна розглядати лише як приватну договірну конструкцію: вони мають публічно значущі наслідки

³⁸ Meta, 'Terms of Service' <https://www.facebook.com/terms/>; Meta, 'Facebook Community Standards' <https://transparency.meta.com/policies/community-standards/>; Instagram, 'Terms of Use' <https://help.instagram.com/termsfuse>; Instagram, 'Community Guidelines' <https://help.instagram.com/477434105621119>; Google, 'YouTube Terms of Service' <https://www.youtube.com/t/terms>; YouTube, 'Community Guidelines' <https://www.youtube.com/howyoutubeworks/policies/community-guidelines/>

³⁹ Joel R Reidenberg, 'Lex Informatica: The Formulation of Information Policy Rules through Technology' (1998) 76 *Texas Law Review* 55;

для свободи вираження поглядів, доступу до інформації, підприємницької активності та участі у публічному дискурсі.

Поряд із нормотворчою функцією платформи здійснюють функцію застосування власних правил через системи контентної модерації. Модерація охоплює виявлення потенційних порушень, оцінку відповідності контенту правилам платформи, прийняття рішення про видалення, обмеження видимості, маркування, демонетизацію, тимчасове призупинення або блокування акаунту, а також розгляд скарг користувачів на такі рішення. Ця діяльність має квазіадміністративний характер, оскільки платформа одночасно встановлює правила, застосовує їх до конкретних ситуацій і організовує внутрішні процедури перегляду власних рішень. Водночас її не слід прямо ототожнювати з судовою діяльністю: платформи не вирішують спір від імені держави, але їхні рішення можуть мати для користувача наслідки, співмірні з обмеженням доступу до важливого комунікаційного простору.

Контентна модерація не є нейтральним технічним процесом. Кожне рішення про видалення, залишення, маркування або зниження видимості контенту передбачає нормативну оцінку того, які форми висловлювання, поведінки або взаємодії є допустимими в межах певної цифрової спільноти. Навіть тоді, коли рішення приймається автоматизованими засобами, воно спирається на попередньо закладені критерії, класифікації ризиків і ціннісні припущення щодо меж прийнятної комунікації. Тому модерація є не лише технічним інструментом управління контентом, а й формою приватного правозастосування у цифровому середовищі.

Окремим виміром приватної регуляторної влади платформ є алгоритмічне управління. На відміну від явної модерації, яка проявляється у видаленні або блокуванні контенту, алгоритмічне ранжування, рекомендаційні системи, персоналізація та таргетування впливають на видимість інформації менш помітно, але не менш суттєво. Вони визначають, який контент користувач побачить першим, які повідомлення отримають ширше поширення, які теми стануть більш помітними, а які залишаться маргінальними. Саме тому алгоритмічне управління

можна описати як форму “невидимого регулювання”: воно не забороняє певну поведінку прямо, але структурує інформаційне середовище через дизайн, пріоритети видимості.

Правове значення алгоритмічного управління полягає в тому, що воно впливає на реалізацію свободи вираження поглядів, доступу до інформації, політичної комунікації та економічної активності без класичних формального рішення чи відкритої санкції. У цьому аспекті актуальною є теза Lessig про те, що “code is law”⁴⁰: технологічна архітектура може виконувати регуляторну функцію не менш ефективно, ніж юридична заборона. Для платформ це означає, що їхній вплив на публічний дискурс здійснюється не лише через правила і модерацію, а й через саму технічну організацію цифрового простору. Саме тому DSA приділяє увагу прозорості рекомендаційних систем, параметрам ранжування та додатковим обов’язкам дуже великих онлайн-платформ щодо надання користувачам альтернативних систем рекомендацій.

У доктрині ця регуляторна роль платформ описується через різні концепції: “new governors”⁴¹, “private governance”⁴², “custodians of the internet”⁴³, “platform governance”⁴⁴, “private ordering of public discourse”⁴⁵ або “platform constitutionalism”⁴⁶. Спільною для цих підходів є думка, що великі платформи не є нейтральними посередниками, а здійснюють власну владу щодо організації

⁴⁰ Lawrence Lessig, *Code: Version 2.0* (Basic Books 2006)

⁴¹ Kate Klonick, 'The New Governors: The People, Rules, and Processes Governing Online Speech' (2018) 131 *Harvard Law Review* 1598

⁴² Hannah Bloch-Wehba, 'Global Platform Governance: Private Power in the Shadow of the State' (2019) 72 *SMU Law Review* 27; Jack M Balkin, 'Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation' (2018) 51 *UC Davis Law Review* 1149

⁴³ Tarleton Gillespie, *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media* (Yale University Press 2018)

⁴⁴ Robert Gorwa, 'What Is Platform Governance?' (2019) 22(6) *Information, Communication & Society* 854

⁴⁵ Evelyn Douek, 'Governing Online Speech: From "Posts-As-Trumps" to Proportionality and Probability' (2021) 121 *Columbia Law Review* 759; Nicolas Suzor, *Lawless: The Secret Rules That Govern Our Digital Lives* (Cambridge University Press 2019).

⁴⁶ Edoardo Celeste, 'Digital Constitutionalism: A New Systematic Theorisation' (2019) 33(1) *International Review of Law, Computers & Technology* 76; Giovanni De Gregorio, 'The Rise of Digital Constitutionalism in the European Union' (2021) 19(1) *International Journal of Constitutional Law* 41; Christian Ollig, *Hybrid Speech Governance: Plattformregulierung zwischen privater Autonomie und öffentlicher Verantwortung* (Mohr Siebeck 2025)

цифрового середовища. Вони формують правила доступу, видимості, комунікації та санкціонування, а тому їхня діяльність має оцінюватися не лише в категоріях договору чи свободи підприємництва, а й крізь призму підзвітності, процедурної справедливості та захисту фундаментальних прав.

Водночас визнання платформ приватними регуляторами не означає їх повного прирівнювання до державних органів. Платформи залишаються приватними суб'єктами, що діють у межах власної комерційної логіки, технологічних можливостей і договірних відносин з користувачами. Проте масштаб їхнього впливу на публічну комунікацію та фундаментальні права користувачів обґрунтовує необхідність спеціального правового режиму. Його завдання полягає не в тому, щоб усунути платформне саморегулювання, а в тому, щоб встановити його правові межі, забезпечити прозорість правил, обмежити свавільність їх застосування і створити механізми оскарження рішень платформ.

Саме в цій логіці слід розглядати DSA. Регламент не замінює приватні правила платформ публічно-правовими правилами. Натомість він юридично впорядковує приватну регуляторну владу платформ через обов'язки щодо прозорості умов користування, обґрунтування рішень про модерацію, внутрішнього розгляду скарг, позасудового вирішення спорів, звітності, аудиту, оцінки системних ризиків і врахування фундаментальних прав користувачів. Особливе значення має ст. 14(4) DSA, яка вимагає від платформ застосовувати свої обмеження сумлінно, об'єктивно і пропорційно, з належним урахуванням прав та законних інтересів усіх залучених сторін.

Отже, онлайн-платформи виступають не лише об'єктами, а й суб'єктами регулювання у сфері цифрової публічної комунікації. Вони створюють приватні правила, застосовують їх до користувачів, організовують процедури перегляду власних рішень і через алгоритмічні системи структурують видимість інформації. Ця приватна регуляторна влада не може залишатися повністю автономною, оскільки її здійснення впливає на фундаментальні права користувачів і функціонування публічного дискурсу. DSA відповідає на цю проблему шляхом переходу від довіри до автономного саморегулювання платформ до моделі

регульованого саморегулювання, у якій приватні правила платформ підпорядковуються вимогам прозорості, належної процедури, підзвітності, пропорційності та публічного нагляду.

1.1.5. Регуляторні виклики, специфічні для онлайн-платформ

Аналіз поняття, економічної природи, інфраструктурної ролі та приватнорегуляторних функцій онлайн-платформ дозволяє систематизувати ті регуляторні виклики, які відрізняють платформи від традиційних об'єктів правового регулювання. Ці виклики не є випадковими або суто технологічними. Вони випливають із самої організації платформного середовища: концентрації аудиторії, алгоритмічного управління інформаційними потоками, транскордонності цифрових послуг, асиметрії інформації між платформами, користувачами і регуляторами, а також із поєднання приватної комерційної логіки з публічно значущими наслідками платформної діяльності. Саме ця сукупність факторів пояснює, чому традиційні інструменти регулювання онлайн-посередників виявилися недостатніми і чому DSA запроваджує більш складну систему обов'язків належної обачності, прозорості, оцінки ризиків і публічного нагляду.

Першим регуляторним викликом є асиметрія інформації між платформами, користувачами, дослідниками та органами нагляду. Платформи мають значно ширший доступ до інформації про функціонування власних алгоритмічних систем, критерії ранжування, результати модераційних рішень, практики таргетування реклами, поведінкові патерни користувачів і наслідки власних управлінських рішень. Натомість зовнішні актори часто можуть спостерігати лише результати функціонування платформи, але не внутрішню логіку відповідних процесів. Алгоритмічні системи, моделі виявлення порушень, рекомендаційні механізми і рекламні технології є технічно складними, динамічними та значною мірою закритими для зовнішньої перевірки. Саме тому DSA намагається зменшити цю асиметрію через вимоги до прозорості, звітності, оцінки системних ризиків, незалежного аудиту та доступу дослідників до даних.

Другим викликом є транскордонний характер платформної діяльності. Онлайн-платформи можуть надавати послуги користувачам у багатьох державах одночасно, незалежно від місця розташування їхньої головної компанії, серверної інфраструктури або основних активів. Це ускладнює застосування традиційних територіальних механізмів правового регулювання. Виникають питання юрисдикції, координації між національними органами, виконання рішень, уникнення фрагментації правового режиму та запобігання регуляторному арбітражу. DSA відповідає на цей виклик через поширення свого режиму на посередницькі послуги, що пропонуються отримувачам у ЄС, незалежно від місця заснування постачальника, а також через інституційну систему співпраці між цифровими координаторами послуг і ЄК.

Третім викликом є масштаб і швидкість платформної діяльності. Найбільші онлайн-платформи оперують із мільйонами або мільярдами користувачів, величезними масивами контенту, великою кількістю автоматизованих рішень і швидкими змінами технічної архітектури сервісів. У таких умовах класичний індивідуалізований контроль кожного рішення щодо контенту, реклами чи ранжування є практично неможливим. Проблема посилюється тим, що технологічні практики платформ розвиваються швидше, ніж звичайні законодавчі цикли. Саме тому DSA не намагається детально врегулювати кожне технологічне рішення, а використовує ризик-орієнтований підхід: він встановлює процедурні й організаційні обов'язки, які мають застосовуватися незалежно від конкретної технологічної моделі платформи.

Четвертим викликом є можливий, цілком реальний конфлікт між комерційними інтересами платформ і публічними цінностями. Частина великих платформ функціонує в умовах економіки уваги, де комерційний інтерес пов'язаний із залученням користувача, тривалістю його перебування на сервісі, інтенсивністю взаємодії та обсягом зібраних даних. Це може створювати стимули до просування контенту, який викликає сильну емоційну реакцію, поляризує аудиторію або максимізує взаємодію, навіть якщо такий контент породжує

суспільні ризики. Водночас це не означає, що платформи взагалі не мають стимулів до модерації або підтримання безпечного середовища. Проблема полягає радше в тому, що приватні стимули платформ не завжди збігаються з публічними інтересами, пов'язаними із захистом фундаментальних прав, демократичного дискурсу, споживачів, неповнолітніх і суспільної безпеки. Тому добровільне саморегулювання не може розглядатися як достатній механізм гарантування цих інтересів⁴⁷.

П'ятим викликом є дефіцит підзвітності у системах приватного платформного управління. Платформи встановлюють правила, застосовують їх до користувачів, організовують модераційні процедури, визначають умови видимості інформації і застосовують санкції у вигляді видалення контенту, обмеження доступу, демонетизації або блокування акаунтів. Проте ці рішення ухвалюються в межах приватних організаційних структур, які не підпадають під ті самі механізми демократичної, адміністративної або судової підзвітності, що й публічні органи. Це створює розрив між публічно значущими наслідками платформних рішень і приватноправовою формою їх ухвалення⁴⁸. DSA намагається зменшити цей розрив через вимоги до мотивування рішень, внутрішнього розгляду скарг, позасудового вирішення спорів, прозорості умов користування, звітності, аудиту та зовнішнього нагляду⁴⁹.

1.2. Саморегулювання як модель регуляторного управління

Встановлення природи онлайн-платформ як особливого об'єкта правового регулювання дозволило ідентифікувати структурні виклики, що ускладнюють застосування до платформного середовища традиційних правових інструментів.

⁴⁷ Christoph Busch, 'Regulating the Expanding Content Moderation Universe: A European Perspective on Infrastructure Moderation' (2022) 27 *UCLA Journal of Law & Technology* 32

⁴⁸ Natali Helberger, Jo Pierson and Thomas Poell, 'Governing Online Platforms: From Contested to Cooperative Responsibility' (2018) 34(1) *The Information Society* 1.

⁴⁹ Miriam C Buiten, 'The Digital Services Act: From Intermediary Liability to Platform Regulation' (2021) 12(3) *JIPITEC* 361.

Однак з'ясування цих викликів не є достатньою без визначення того, які регуляторні моделі можуть бути використані для відповіді на них. На ранніх етапах розвитку платформного середовища регулятори здебільшого не мали готової відповіді на нові виклики, тому фактично толерували широку автономію платформ у виробленні власних правил, процедур модерації та добровільних стандартів поведінки. Це не завжди було результатом свідомого нормативного вибору на користь саморегулювання - радше йшлося про поєднання технологічної новизни, швидкого розвитку платформ, обмежених знань регуляторів, прагнення не стримувати інновації та відсутності усталеної правової моделі для втручання у приватне управління цифровими комунікаційними просторами.

У цьому підрозділі буде з'ясовано, що означає саморегулювання як модель регуляторного управління, які його основні види виокремлюються у доктрині, за яких умов воно може бути ефективним і чому автономне саморегулювання онлайн-платформ виявляється недостатнім. На цій основі буде обґрунтовано, що DSA не відмовляється від саморегулювання платформ, а трансформує його у модель регульованого саморегулювання, поєднуючи приватні правила платформ із юридично обов'язковими вимогами прозорості, підзвітності, належної процедури та публічного нагляду.

Підрозділ структурований як послідовний рух від абстрактного до конкретного. Спочатку встановлюється поняття саморегулювання та його відмежування від суміжних регуляторних категорій. Далі розглядаються основні теоретичні моделі саморегулювання. Третій параграф вводить концепцію децентрованого регулювання та поєднання різних регуляторних інструментів. Четвертий параграф аналізує межі саморегулювання у платформному середовищі як пояснення того, чому структурні характеристики платформ роблять автономне саморегулювання системно недостатнім механізмом захисту публічних інтересів.

Методологічно цей підрозділ спирається на доктринальний аналіз регуляторних теорій, сформованих у правовій, політико-правовій та соціально-економічній літературі. Оскільки більшість класичних моделей саморегулювання розроблялася щодо традиційних регульованих секторів, їх застосування до онлайн-

платформ потребує критичної адаптації. Тому відповідні теорії використовуються як аналітичні інструменти для пояснення того, яка модель саморегулювання притаманна DSA.

1.2.1. Поняття саморегулювання та його відмежування від державного регулювання і співрегулювання

Поняття саморегулювання належить до найбільш дискусійних у регуляторній доктрині: воно широко використовується як у правовій науці, так і в політичній практиці, однак не має уніфікованого визначення. Ця понятійна невизначеність є не лише термінологічною проблемою. Вона відображає глибші розбіжності щодо природи регулювання, ролі держави у регуляторному процесі та меж легітимності приватного нормотворення. Для цілей цього дослідження встановлення операційного визначення саморегулювання є необхідною передумовою аналізу трансформації платформного управління у DSA

У найбільш загальному значенні саморегулювання описує ситуацію, у якій недержавні актори самостійно виробляють, застосовують і контролюють виконання правил, що регулюють їхню власну діяльність або діяльність відповідної професійної, економічної чи соціальної спільноти. Baldwin, Cave та Lodge розглядають саморегулювання як регулювання певної групи її власними членами, тим самим підкреслюючи, що джерело правил, механізми їх застосування та контроль за їх дотриманням переміщуються від держави до самих регульованих суб'єктів⁵⁰. Тезаурус EUROVOC на сайті Верховної Ради України подає “саморегулювання” як термін у сфері права, пов’язаний із “добровільним регулюванням”, “м’яким правом” і “спільним регулюванням”⁵¹.

У цьому сенсі саморегулювання охоплює три взаємопов’язані елементи: нормотворчий, оскільки приватні актори формують правила поведінки; виконавчий, оскільки вони організовують застосування цих правил; і контрольний,

⁵⁰ Robert Baldwin, Martin Cave and Martin Lodge, *Understanding Regulation: Theory, Strategy, and Practice* (2nd edn, OUP 2012) ch 8.

⁵¹ Тезаурус EUROVOC, ‘Саморегулювання’ (Законодавство України, Верховна Рада України) <<https://zakon.rada.gov.ua/laws/euro/6367>>

оскільки вони створюють механізми перевірки дотримання правил та реагування на їх порушення⁵².

Водночас застосування цього поняття до онлайн-платформ потребує суттєвого уточнення. Класична доктрина розглядає саморегулювання як регулювання групою власних членів: професійна спільнота чи галузева асоціація встановлює правила для самих себе. Натомість онлайн-платформи через умови користування та політики модерації регулюють насамперед поведінку третіх осіб — користувачів, рекламодавців, продавців, — а не власну діяльність у вузькому сенсі. Тому платформне "саморегулювання" є структурно ближчим до приватного управління (*private governance*), у якому окрема компанія здійснює квазірегуляторні функції щодо інших суб'єктів. У цьому дослідженні термін "саморегулювання онлайн-платформ" використовується з урахуванням цієї специфіки: він охоплює самостійне вироблення платформою правил функціонування власного сервісу, невід'ємною частиною якого є впорядкування поведінки його користувачів. Саме ця подвійна природа — самоорганізація сервісу, що водночас є регулюванням інших, — пояснює, чому автономність платформних правил породжує проблему легітимності, гострішу за класичне галузеве саморегулювання, і чому вона потребує публічно-правового впорядкування⁵³.

Для платформного середовища таке розуміння є особливо важливим. Онлайн-платформи не лише підпорядковуються зовнішнім правовим вимогам, а й самі створюють внутрішні нормативні порядки через умови користування, стандарти спільноти, політики модерації, рекламні правила, системи скарг, процедури перегляду рішень і алгоритмічні механізми управління видимістю інформації. З позиції Black, сучасне регулювання дедалі менше може розумітися як ієрархічний процес, у якому держава є єдиним центром регуляторної влади;

⁵² Robert Baldwin, Martin Cave and Martin Lodge, *Understanding Regulation: Theory, Strategy, and Practice* (2nd edn, OUP 2012) ch 8

⁵³ Klonick, "The New Governors", *Harvard Law Review* 2018

натомість воно формується у децентрованому регуляторному просторі, де регуляторні функції розподілені між державними і недержавними акторами⁵⁴.

Саме тому платформне саморегулювання має аналізуватися не як виняток із правового регулювання, а як один із його фактичних елементів, який потребує юридичного впорядкування.

Саморегулювання слід відмежовувати від класичної моделі імперативного державного регулювання, у межах якої держава самостійно встановлює обов'язкові правила поведінки, контролює їх виконання та застосовує юридичні санкції у разі порушення. Натомість у саморегулюванні правила формуються самими приватними акторами, застосовуються ними ж і забезпечуються переважно внутрішніми або приватноправовими механізмами. У випадку онлайн-платформ такими механізмами можуть бути видалення контенту, обмеження видимості, демонетизація, тимчасове призупинення або блокування акаунту. Принципова відмінність між цими моделями полягає не лише у суб'єкті нормотворення, а й у джерелах легітимності: державне регулювання спирається на публічний мандат, демократичні процедури та конституційні обмеження влади, тоді як саморегулювання зазвичай обґрунтовується договірною згодою, професійним досвідом, ринковими стимулами або здатністю приватних акторів ефективніше реагувати на складність відповідної сфери.

Окремо необхідно відмежовувати саморегулювання від співрегулювання. У праві ЄС поняття співрегулювання отримало нормативне закріплення у Міжінституційній угоді про краще законотворення 2003 р., яка визначає його як механізм, за якого законодавчий акт ЄС доручає досягнення визначених законодавцем цілей визнаним учасникам відповідної сфери, зокрема економічним операторам, соціальним партнерам, неурядовим організаціям або асоціаціям.⁵⁵

⁵⁴ Julia Black, 'Decentring Regulation: Understanding the Role of Regulation and Self-Regulation in a "Post-Regulatory" World' (2001) 54 Current Legal Problems 103.

⁵⁵ Interinstitutional Agreement on Better Law-Making [2003] OJ C321/1, paras 18–22.

На відміну від автономного саморегулювання, співрегулювання передбачає активну роль публічної влади: вона визначає цілі, межі, базові стандарти або механізми контролю, тоді як приватні чи суспільні актори беруть участь у конкретизації або реалізації цих цілей. Отже, співрегулювання не є повною передачею регуляторної влади приватним суб'єктам; радше воно є гібридною моделлю, у якій приватна експертиза та організаційна спроможність поєднуються з публічним мандатом і зовнішнім контролем⁵⁶.

Водночас співрегулювання слід відрізнити і від регульованого саморегулювання, центрального для цього дослідження. Критерієм розмежування є походження та функція приватних правил. У співрегулюванні законодавець визначає власні регуляторні цілі і доручає їх досягнення приватним акторам: приватне нормотворення тут є інструментом реалізації публічного мандата (у DSA — кодекси поведінки, кризові протоколи). У регульованому саморегулюванні, навпаки, приватні правила виникають і існують самостійно, з власних комерційних та організаційних потреб платформи, а право не делегує їх створення, а дисциплінує вже наявну приватну нормотворчість — встановлює вимоги до її прозорості, процедур і зовнішньої перевірки⁵⁷. Отже, співрегулювання — це публічні цілі, реалізовані приватними засобами; регульоване саморегулювання — приватні правила, підпорядковані публічним стандартам.

У доктрині саморегулювання зазвичай класифікують залежно від того, якою мірою держава бере участь у його виникненні, змістовному наповненні, контролі та забезпеченні виконання. За цим критерієм можна виокремити щонайменше три

⁵⁶ Christopher T Marsden, *Internet Co-Regulation: European Law, Regulatory Governance and Legitimacy in Cyberspace* (CUP 2011) 46–52

⁵⁷ Wolfgang Schulz and Thorsten Held, *Regulated Self-Regulation as a Form of Modern Government: An Analysis of Case Studies from Media and Telecommunications Law* (University of Luton Press 2004); Christopher T Marsden, *Internet Co-Regulation: European Law, Regulatory Governance and Legitimacy in Cyberspace* (CUP 2011) 46–52.

основні форми: добровільне саморегулювання, мандатне саморегулювання та саморегулювання, забезпечене державним примусом⁵⁸.

Добровільне саморегулювання виникає з ініціативи самих приватних або професійних акторів без прямого законодавчого обов'язку створити відповідну систему правил. Його типовими проявами є галузеві кодекси поведінки, етичні стандарти, професійні правила, внутрішні політики компаній або стандарти добросовісної практики, що приймаються самими учасниками відповідної сфери. У цій моделі держава або взагалі не бере участі у формуванні правил, або лише опосередковано стимулює їх появу через політичні очікування, репутаційний тиск чи загальну загрозу майбутнього втручання. Перевагою добровільного саморегулювання є його гнучкість і близькість до практичних потреб відповідної сфери; водночас його слабким місцем є відсутність зовнішнього контролю, ризик конфлікту інтересів і залежність ефективності від доброї волі самих регульованих суб'єктів.

Мандатне саморегулювання відрізняється тим, що його виникнення ініціюється або прямо вимагається державою чи іншим публічним актором. У такій моделі публічна влада встановлює обов'язок певної галузі, професійної спільноти або категорії суб'єктів створити механізм саморегулювання, але залишає їм простір для визначення конкретного змісту правил, процедур і організаційних форм.

Прикладами такої моделі можуть бути випадки, коли закон зобов'язує професійну спільноту або галузь створити власні стандарти поведінки, кодекси етики, дисциплінарні процедури чи органи внутрішнього контролю. Зокрема, у регульованих професіях держава може вимагати існування професійного самоврядування, але залишати самій професійній спільноті повноваження щодо деталізації правил професійної етики, стандартів належної практики або

⁵⁸ Cary Coglianese and Evan Mendelson, 'Meta-Regulation and Self-Regulation' in Robert Baldwin, Martin Cave and Martin Lodge (eds), *The Oxford Handbook of Regulation* (OUP 2010) 146, 151–53; Ian Ayres and John Braithwaite, *Responsive Regulation: Transcending the Deregulation Debate* (OUP 1992) ch 4.

дисциплінарної відповідальності. Подібна логіка може проявлятися і у фінансовому секторі, коли учасники ринку зобов'язані діяти через саморегулівні організації або дотримуватися галузевих правил, розроблених такими організаціями в межах публічно визначеної рамки⁵⁹. Хоча таким організаціям держава делегує публічно-владні повноваження в правотворчій галузі, що може викликати невизначеність щодо розуміння їхнього правового статусу, це не прирівнює їх за статусом до органів державної влади або юридичних осіб публічного права⁶⁰.

Інакше кажучи, держава не детально регламентує поведінку кожного учасника, але вимагає, щоб самі учасники відповідної сфери розробили власну систему правил і контролю. Така модель є проміжною між повністю добровільним саморегулюванням і класичним державним регулюванням: приватні актори зберігають нормотворчу автономію, однак сама поява системи саморегулювання вже не є суто добровільною.

Найінтенсивнішою формою є саморегулювання, забезпечене державним примусом. У концепції Ayres і Braithwaite така модель передбачає, що регульовані суб'єкти самостійно розробляють правила відповідності, але ці правила підлягають зовнішньому схваленню, контролю або примусовому забезпеченню з боку державного регулятора.⁶¹

Її логіка полягає в тому, що приватні актори краще знають технічні й організаційні особливості власної діяльності, тому можуть ефективніше сформулювати конкретні правила поведінки. Водночас держава не відмовляється від регуляторної відповідальності: вона контролює якість таких правил, перевіряє

⁵⁹ Подібний тип саморегулювання передбачений, зокрема, законодавством України про ринки капіталу та організовані товарні ринки, яке регламентує статус і діяльність саморегулівних організацій професійних учасників ринків капіталу. Див.: Закон України «Про ринки капіталу та організовані товарні ринки» від 23 лютого 2006 р. № 3480-IV, ст. 143–144 <<https://zakon.rada.gov.ua/go/3480-15>>

⁶⁰ Філатова-Білоус Н. Саморегулівні організації: юридичні особи на межі приватного і публічного права. Цивілістична платформа. 2024. № 2. С. 58-82. <https://doi.org/10.69724/2786-8834-2024-2-2-58-82> С. 76

⁶¹ Ian Ayres and John Braithwaite, *Responsive Regulation: Transcending the Deregulation Debate* (OUP 1992) ch 4.

їх виконання і може застосувати санкції у разі невідповідності або порушення. Отже, у цій моделі приватна експертиза поєднується з публічним примусом.

Ця типологія має значення для подальшого аналізу, оскільки DSA не може бути адекватно описаний як приклад лише однієї з наведених форм. Він очевидно не відтворює модель повністю добровільного саморегулювання, оскільки встановлює юридично обов'язкові вимоги щодо умов користування, прозорості модерації, мотивування рішень, розгляду скарг, оцінки системних ризиків, аудиту та публічного нагляду. Водночас він не є і класичною моделлю імперативного державного регулювання, оскільки не замінює платформні правила детальним публічно-правовим кодексом допустимого і недопустимого контенту. Ця проміжна позиція DSA потребує точнішого теоретичного інструментарію, який буде розгорнуто у наступних параграфах.

Для цілей цього дослідження саморегулювання онлайн-платформ визначається як сукупність правил, процедур і механізмів застосування, що виробляються, впроваджуються і контролюються самими платформами щодо контенту, поведінки користувачів, видимості інформації та функціонування власних сервісів. Регульоване саморегулювання онлайн-платформ, своєю чергою, означає модель, за якої ці приватні правила і процедури зберігаються, але підпорядковуються обов'язковим публічно-правовим вимогам прозорості, належної процедури, пропорційності, підзвітності та зовнішнього контролю. Обґрунтування того, що саме ця модель притаманна DSA, є завданням наступних параграфів.

1.2.2. Основні теоретичні моделі саморегулювання

Типологія добровільного, мандатного та забезпеченого державним примусом саморегулювання описує різні ступені участі держави у приватному нормотворенні. Однак для аналізу DSA цього недостатньо, оскільки Регламент поєднує кілька регуляторних логік одночасно: він зберігає приватні правила платформ, встановлює публічно-правові вимоги до процедур їх застосування, запроваджує ризик-орієнтований нагляд і створює умови для співрегуляторних інструментів, зокрема кодексів поведінки. Наведена типологія відповідає лише на

питання, хто ініціює і забезпечує саморегулювання; вона не пояснює, як саме право може управляти приватними регуляторними системами, не замінюючи їх. Для цього необхідно звернутися до теоретичних конструкцій іншого рівня. При цьому важливо розрізняти їхню природу: одні з них описують стратегію публічного правозастосування (реагувальне регулювання)⁶², інші — предмет правового впливу (метарегулювання)⁶³, треті — модель співвідношення приватного і публічного нормотворення (регульоване саморегулювання)⁶⁴.

Реагувальне регулювання, запропоноване Ayres і Braithwaite як альтернатива протиставленню дерегуляції та жорсткого державного контролю, є теорією стратегії правозастосування. Її логіка полягає в тому, що інтенсивність державного втручання має змінюватися залежно від поведінки регульованого суб'єкта: держава починає з м'яких форм стимулювання, діалогу і саморегулювання, але зберігає можливість поступового переходу до жорсткіших заходів у разі недобросовісності, неефективності або повторних порушень. Складовою цієї теорії є розглянута вище модель саморегулювання, забезпеченого державним примусом. У DSA логіка реагувальності проявляється у диференціації обов'язків залежно від типу посередника, масштабу платформи та рівня системних ризиків, а також у посиленому нагляді за дуже великими онлайн-платформами і пошуковими системами.

Метарегулювання, на відміну від класичного регулювання поведінки, визначає особливий предмет правового впливу: внутрішні системи управління самого регульованого суб'єкта. Держава не встановлює детальний зміст кожного правила, але визначає, як має бути організована система управління ризиками, комплаєнсу, контролю, звітності та внутрішньої перевірки. Право регулює не лише

⁶² Ian Ayres and John Braithwaite, *Responsive Regulation: Transcending the Deregulation Debate* (OUP 1992); Robert Baldwin and Julia Black, 'Really Responsive Regulation' (2008) 71 MLR 59; Christine Parker, *The Open Corporation: Effective Self-Regulation and Democracy* (CUP 2002)

⁶³ Cary Coglianese and Evan Mendelson, 'Meta-Regulation and Self-Regulation' in Robert Baldwin, Martin Cave and Martin Lodge (eds), *The Oxford Handbook of Regulation* (OUP 2010) 146

⁶⁴ Wolfgang Schulz and Thorsten Held, *Regulated Self-Regulation as a Form of Modern Government* (University of Luton Press 2004); Christopher T Marsden, *Internet Co-Regulation: European Law, Regulatory Governance and Legitimacy in Cyberspace* (CUP 2011)

окремі рішення платформи, а й архітектуру прийняття таких рішень. Ця модель особливо важлива для аналізу DSA, оскільки значна частина його обов'язків стосується не конкретного контенту як такого, а системних процесів: оцінки і мінімізації ризиків, незалежного аудиту, прозорості рекомендаційних систем, доступу дослідників до даних і звітності. Право ЄС втручається не шляхом заміни приватних правил державними, а шляхом встановлення вимог до того, як платформи мають організовувати, пояснювати, перевіряти і коригувати власне саморегулювання.

Центральною для цього дослідження є модель регульованого саморегулювання. Її концептуальне походження пов'язане з німецькою публічно-правовою доктриною (*regulierte Selbstregulierung*)⁶⁵, яка розробила цю категорію насамперед на матеріалі медійного і телекомунікаційного права як форму сучасного управління, за якої приватне нормотворення зберігається, але вбудовується у публічно-правову рамку. Регульоване саморегулювання охоплює ситуації, у яких приватні актори зберігають власні правила, процедури та організаційні механізми, однак ці правила функціонують у межах публічно встановлених стандартів. У сфері онлайн-платформ це означає, що умови користування, стандарти спільноти, політики модерації, системи скарг і алгоритмічні механізми не зникають і не замінюються державними правилами, але більше не можуть розглядатися як суто приватна справа платформи: право встановлює вимоги до їх прозорості, зрозумілості, пропорційності, недискримінаційності, належної процедури та зовнішньої перевірки. На відміну від співрегулювання, яке передбачає реалізацію публічно визначених цілей приватними засобами, регульоване саморегулювання дисциплінує вже наявну, самотійно сформовану приватну нормотворчість.

У вітчизняній доктрині класифікаційні підходи до саморегулювання розроблялися переважно щодо господарської діяльності. Так, О. М. Гончаренко за

⁶⁵ Wolfgang Hoffmann-Riem, 'Medienregulierung als regulierte Selbstregulierung' in *Regulierte Selbstregulierung als Steuerungskonzept des Gewährleistungsstaates* (Duncker & Humblot 2001); Wolfgang Schulz and Thorsten Held, *Regulated Self-Regulation as a Form of Modern Government* (University of Luton Press 2004).

критерієм засобу здійснення саморегулювання виокремлює договірне, корпоративне та інституційне саморегулювання. Ця класифікація частково застосовна до платформного середовища: правила онлайн-платформ за своєю формою найближчі до корпоративного саморегулювання, оскільки ґрунтуються на односторонніх корпоративних актах. Водночас вона не охоплює специфіки платформ: договірний та інституційний види передбачають колективну координацію учасників ринку, тоді як кожна платформа здійснює нормотворення одноосібно, і його адресатами є не сама компанія чи професійна спільнота, а треті особи — користувачі сервісу. Тому для аналізу DSA ця класифікація може використовуватися лише як допоміжна⁶⁶.

Отже, DSA не слід описувати одним поняттям. Теоретично точніше говорити, що він реалізує модель регульованого саморегулювання, використовуючи при цьому метарегулювання як техніку впливу на внутрішні системи платформ, реагувальну та ризик-орієнтовану логіку як стратегію диференціації обов'язків і нагляду, а також окремі елементи співрегулювання (кодекси поведінки, кризові протоколи). Сучасне платформне регулювання не повертається до моделі державного командного контролю, але й не залишає платформам автономну регуляторну владу: воно створює проміжну конструкцію, у якій приватна нормотворчість платформ визнається фактично неминучою, проте юридично впорядковується через процедурні, інституційні та наглядові вимоги..

1.2.3. Децентроване регулювання

Класичні теорії регулювання часто виходили з припущення, що держава є центральним і привілейованим суб'єктом регуляторної влади. Однак розвиток складних технологічних, фінансових і інформаційних систем показав обмеженість такого уявлення. Julia Black запропонувала концепцію децентрованого регулювання, яка виходить із того, що регуляторні функції у сучасному суспільстві розподілені між множиною акторів: державними органами, приватними компаніями, професійними асоціаціями, технічними організаціями, громадянським

⁶⁶ Гончаренко О. Види саморегулювання господарської діяльності. Підприємництво, господарство і право. 2016. № 11. С. 68–72. URL: <http://pgp-journal.kiev.ua/archive/2016/11/15.pdf>

суспільством і самими користувачами⁶⁷. У такому підході держава залишається важливим, але не єдиним центром регулювання.

Для онлайн-платформ ця концепція має особливе значення. Платформи не є лише адресатами правових норм. Вони самі формують правила доступу до цифрової інфраструктури, визначають допустимі і недопустимі форми поведінки, організовують видимість інформації, встановлюють процедури модерації та фактично здійснюють первинний контроль за значною частиною цифрової комунікації. Водночас на них впливають законодавці, регулятори, суди, рекламодавці, громадські організації, медіа, дослідники, користувачі і конкуренти. Регуляторний простір платформ тому є не ієрархічним, а розподіленим.

Якщо регуляторна влада розподілена, то ефективне регулювання не може спиратися на один інструмент. У доктрині *smart regulation* це отримало назву регуляторної суміші (*regulatory mix*)⁶⁸ — свідомого поєднання різних регуляторних інструментів і акторів для досягнення регуляторної мети. У платформному середовищі одночасно діють норми публічного права, договірні умови платформ, стандарти спільноти, технічні протоколи, алгоритмічні системи, рекомендації регуляторів, кодекси поведінки та ін. Особливе місце серед цих інструментів посідає технічна архітектура: як показав Lessig⁶⁹, у цифровому середовищі програмний код виконує регуляторну функцію нарівні з правом, соціальними нормами і ринком, оскільки безпосередньо визначає, які дії користувача є можливими, а які — ні. Кожен із цих елементів окремо не пояснює реальний режим управління платформами, але разом вони формують складну систему багаторівневого регулювання. Кожен із цих елементів окремо не пояснює повністю реальний режим управління платформами, але разом вони формують складну систему багаторівневого регулювання.

⁶⁷ Julia Black, 'Decentring Regulation: Understanding the Role of Regulation and Self-Regulation in a "Post-Regulatory" World' (2001) 54 *Current Legal Problems* 103.

⁶⁸ Neil Gunningham and Peter Grabosky, *Smart Regulation: Designing Environmental Policy* (OUP 1998)

⁶⁹ Lawrence Lessig, *Code: Version 2.0* (Basic Books 2006)

DSA є прикладом саме такої регуляторної суміші. З одного боку, він є обов'язковим актом права ЄС і встановлює юридично зобов'язувальні вимоги до посередницьких сервісів. З іншого боку, він не усуває приватні правила платформ і не замінює їх детальним кодексом поведінки. Натомість DSA інтегрує платформні правила у публічно-правові вимоги: умови користування мають бути зрозумілими і прозорими; рішення про модерацію мають супроводжуватися поясненням; користувачі мають отримати можливість скарги; найбільші платформи мають оцінювати системні ризики і проходити аудит; дослідники за певних умов отримують доступ до даних.

Концепція децентрованого регулювання, таким чином, пояснює не лише те, що робить DSA, а й те, чому він обрав саме такий спосіб впливу. У децентрованому регуляторному просторі законодавець не може ані повністю витіснити приватну нормотворчість платформ, ані покластися на неї: перше є технічно й організаційно нездійсненним, друге — несумісним із захистом публічних інтересів. Тому право ЄС впливає на платформи переважно процедурно та інституційно — через вимоги до того, як приватні правила створюються, пояснюються, застосовуються і перевіряються. Саме ця логіка підводить до аналізу меж автономного саморегулювання у наступному параграфі.

1.2.4. Межі автономного саморегулювання у платформному середовищі

Автономне саморегулювання може бути ефективним за наявності певних умов: відносно збалансованих інтересів учасників, професійної культури дотримання правил, репутаційних стимулів, можливості зовнішньої перевірки та відсутності значного конфлікту між приватною вигодою і публічним інтересом⁷⁰. У платформному середовищі ці умови виконуються лише частково. Саме тому саморегулювання онлайн-платформ не може бути повністю відкинута, але й не може залишатися автономним.

⁷⁰ Anthony Ogus, *Regulation: Legal Form and Economic Theory* (Hart Publishing 2004); Robert Baldwin, Martin Cave and Martin Lodge, *Understanding Regulation: Theory, Strategy, and Practice* (2nd edn, OUP 2012) ch 8.

Першою межею є конфлікт інтересів. Платформи зацікавлені у підтриманні безпечного і передбачуваного середовища, оскільки це впливає на довіру користувачів, рекламодавців і регуляторів. Водночас їхні комерційні стимули не завжди збігаються з публічними інтересами у захисті фундаментальних прав, якості публічної комунікації, недискримінаційності, безпеці користувачів або мінімізації маніпулятивних практик. Особливо це помітно там, де бізнес-модель залежить від уваги користувачів, персоналізації, залучення до контенту і рекламної монетизації⁷¹.

Другою межею є інформаційна асиметрія. Платформи володіють значно більшим обсягом інформації про власні алгоритмічні системи, модераційні практики, рекламні механізми, дані користувачів і внутрішню логіку прийняття рішень, ніж користувачі, дослідники або регулятори⁷². Ця асиметрія робить просту довіру до добровільних заяв платформ недостатньою: зовнішні суб'єкти позбавлені навіть фактичної можливості оцінити, чи відповідає платформне саморегулювання заявленим стандартам.

Третьою межею є дефіцит процедурної підзвітності. Платформи приймають рішення, які можуть істотно впливати на свободу вираження поглядів, доступ до інформації, економічну діяльність, репутацію та участь у публічному дискурсі. Однак традиційно такі рішення приймалися в межах приватних процедур, без достатнього пояснення, без ефективної можливості оскарження і без незалежної зовнішньої перевірки⁷³. Це створює ситуацію, у якій приватна компанія здійснює функції, подібні до регуляторних, але не несе порівнюваного рівня публічної відповідальності.

⁷¹ Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (PublicAffairs 2019); Tim Wu, *The Attention Merchants: The Epic Scramble to Get Inside Our Heads* (Knopf 2016) Мазаракі - Примак

⁷² Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harvard University Press 2015). Анжеліка Герасименко

⁷³ Мазаракі Примак Kate Klonick, 'The New Governors: The People, Rules, and Processes Governing Online Speech' (2018) 131 Harvard Law Review 1598; Nicolas Suzor, *Lawless: The Secret Rules That Govern Our Digital Lives* (CUP 2019)

Четвертою межею є масштаб платформного впливу. Помилка або системний переки́с у правилах модерації, рекомендаційних алгоритмах чи рекламних системах великої платформи може одночасно вплинути на мільйони користувачів і на умови публічної комунікації загалом. Тому автономне саморегулювання, прийнятне для невеликих професійних спільнот або локальних галузевих стандартів, стає недостатнім у середовищі, де приватні правила мають масовий суспільний ефект.

П'ятою межею є інституційна слабкість зовнішньої верифікації. Якщо інформаційна асиметрія стосується доступу до відомостей, то ця межа стосується відсутності суб'єкта та процедури перевірки: до DSA не існувало інституції, уповноваженої систематично перевіряти, як платформи застосовують власні правила, навіть якщо відповідна інформація ставала доступною. Перевірку додатково ускладнювали технічна складність алгоритмічних систем, комерційна таємниця та транскордонний характер сервісів.

Обмеженість автономного саморегулювання підтвердив і практичний досвід ЄС. Добровільні інструменти, що передували DSA, — зокрема Кодекс практики щодо дезінформації 2018 р. та Кодекс поведінки щодо протидії незаконним висловлюванням ненависті 2016 р. — за оцінками Європейської Комісії, продемонстрували обмежену ефективність через відсутність санкцій, вибірковість участі та неможливість незалежної перевірки заявлених результатів⁷⁴. Саме цей досвід став одним з емпіричних аргументів на користь юридично обов'язкових вимог.

Отже, проблема платформного саморегулювання полягає не в самому факті приватного нормотворення — без участі платформ регулювання цифрового середовища було б технічно й організаційно неможливим. Проблема в тому, що автономне саморегулювання не забезпечує достатніх гарантій прозорості, підзвітності, пропорційності та захисту фундаментальних прав. Саме ця обставина пояснює перехід DSA до моделі регульованого саморегулювання, яка аналізується у наступному параграфі.

⁷⁴ Commission, 'Assessment of the Code of Practice on Disinformation – Achievements and Areas for Further Improvement' (Staff Working Document) SWD (2020) 180 final, 10 September 2020

1.2.5. DSA як модель регульованого саморегулювання

DSA не заперечує саморегулювання онлайн-платформ. Навпаки, він виходить із того, що платформи й надалі залишаються первинними суб'єктами організації власного інформаційного середовища: вони формують умови користування, визначають стандарти спільноти, застосовують політики модерації, організовують рекомендаційні системи, рекламні інструменти, процедури скарг і внутрішні механізми контролю. Однак DSA змінює правовий статус цієї автономії: вона перестає бути суто приватною та вбудовується у систему публічно-правових вимог. Нижче ця трансформація розкривається через п'ять вимірів, які в сукупності відповідають ознакам регульованого саморегулювання, обґрунтованим у попередніх параграфах.

Перший вимір цієї трансформації стосується умов користування. Стаття 14 DSA вимагає, щоб провайдери посередницьких послуг викладали у своїх умовах користування інформацію про будь-які обмеження, які вони накладають на використання сервісу, включно з політиками, процедурами, заходами та інструментами модерації контенту. Особливе значення має ст. 14(4) DSA, яка вимагає, щоб платформи застосовували такі обмеження сумлінно, об'єктивно і пропорційно, з належним урахуванням прав і законних інтересів усіх залучених сторін, включно з фундаментальними правами користувачів. Саме ця норма є одним із ключових прикладів юридичного впорядкування приватної нормотворчої влади платформ.

Другий вимір полягає у процедуризації модерації контенту. DSA не встановлює матеріального переліку дозволеного і забороненого контенту; натомість він створює процедури, через які платформні рішення стають прозорими, мотивованими та оскаржуваними: механізми повідомлення і дії (ст. 16), виклад підстав (ст. 17), внутрішня система розгляду скарг (ст. 20) та позасудове вирішення спорів (ст. 21). Приватна модерація не зникає, але набуває рис належної процедури. Водночас слід зауважити, що процедурний характер DSA стосується саме контенту. Регламент містить і прямі матеріальні заборони — маніпулятивних

інтерфейсів (ст. 25), реклами на основі профілювання з використанням чутливих даних (ст. 26(3)) та таргетованої реклами щодо неповнолітніх (ст. 28(2)).

Третій вимір стосується системних ризиків. Для дуже великих онлайн-платформ і дуже великих онлайн-пошукових систем DSA встановлює обов'язки щодо оцінки і мінімізації системних ризиків, пов'язаних із поширенням незаконного контенту, впливом на фундаментальні права, громадянський дискурс, виборчі процеси, громадську безпеку, гендерно зумовлене насильство, захист неповнолітніх, психічне і фізичне благополуччя користувачів. Тут найповніше проявляється метарегуляторна техніка: право регулює не окремі рішення, а здатність платформи виявляти, пояснювати і зменшувати ризики, що виникають з архітектури її сервісу.

Четвертий вимір полягає у зовнішній верифікації платформного саморегулювання. DSA передбачає незалежний аудит, звітність, доступ дослідників до даних, повноваження координаторів цифрових послуг і ЄК щодо нагляду за найбільшими платформами. Це переводить платформне саморегулювання з площини приватних декларацій у площину інституційної підзвітності. Платформа не лише встановлює власні правила, а й повинна пояснити, як вони працюють, які ризики створюють, які заходи мінімізації застосовуються і як ці заходи перевіряються зовні.

П'ятий вимір становлять елементи співрегулювання. DSA передбачає можливість розроблення кодексів поведінки, кодексів щодо онлайн-реклами і кризових протоколів. За критерієм, сформульованим у 1.2.1, ці інструменти є саме співрегулюванням — реалізацією публічно визначених цілей приватними засобами, — на відміну від перших чотирьох вимірів, які визначають характер самостійно сформованих приватних пнорм. Формально такі інструменти залишаються *soft law* і ґрунтуються на участі приватних акторів, однак у контексті DSA вони набувають більшої регуляторної ваги, оскільки можуть бути пов'язані з виконанням обов'язків щодо мінімізації ризиків, прозорості і відповідальності найбільших платформ.

Отже, DSA реалізує модель регульованого саморегулювання, змістом якої є інституціоналізація підзвітності платформ. Підзвітність тут — не окрема регуляторна модель, а юридичний механізм, через який приватна нормотворчість підпорядковується публічним стандартам: вимогам прозорості, належної процедури, оцінки ризиків, аудиту, доступу до даних і публічного нагляду. Платформи продовжують здійснювати нормотворчі й виконавчі функції, але вже не як автономні приватні суверени цифрового середовища, а як суб'єкти, чия регуляторна влада має бути прозорою, пропорційною, обґрунтованою і підзвітною. Ця модель становить теоретичну основу для аналізу конкретних механізмів DSA у наступних розділах дисертації.

Висновки до розділу 1

Проведений аналіз дозволяє зробити висновок, що онлайн-платформи є особливим об'єктом правового регулювання, оскільки поєднують ознаки технологічного посередника, суб'єкта багатостороннього ринку, інфраструктури публічної комунікації та приватного регулятора. Їх правова природа не може бути зведена лише до договірних відносин між платформою і користувачем, адже платформи організовують доступ до інформації, визначають умови її видимості, встановлюють правила поведінки та застосовують санкції за їх порушення. Фактично це означає, що правила поведінки, які формуються онлайн-платформами, виходять за межі класичних цивільно-правових відносин.

Економічна логіка платформних ринків посилює цю специфіку. Мережеві ефекти, накопичення даних, ефекти блокування користувачів, інформаційна асиметрія та контроль над доступом до аудиторії створюють структурну нерівність між платформою і користувачем. Окрім того необхідність посилення публічно-правового регулювання пояснюється низкою системних факторів, як-от: транскордонний характер діяльності онлайн-платформ, глобальний масштаб поширення інформації та потенційний конфлікт між комерційними інтересами платформ і публічними інтересами держав. За таких обставин діяльність онлайн-платформ перестає виключно визначатися як питання реалізації свободи договору

між приватними суб'єктами, а набуває публічно-правового значення. Тому автономне саморегулювання платформ не може розглядатися як достатній механізм захисту користувачів і публічних інтересів, особливо коли комерційні стимули платформи можуть не збігатися з вимогами прозорості, недискримінації та захисту фундаментальних прав.

Саме тому DSA відображає перехід від довіри до автономного саморегулювання до моделі регульованого саморегулювання. У цій моделі приватні правила платформ не усуваються, але підпорядковуються публічно-правовим вимогам прозорості, належної процедури, обґрунтування рішень, оскарження, оцінки системних ризиків, аудиту та публічного нагляду. Отже, подальший аналіз концепцій саморегулювання має виходити з того, що в сучасному праві ЄС саморегулювання платформ зберігається, але юридично впорядковується та обмежується з метою захисту фундаментальних прав користувачів, забезпечення балансу між свободою здійснення підприємницької діяльності платформ та публічним інтересом, що також проявляється в гарантуванні відкритості інформаційного середовища та забезпеченні належного функціонування демократичних процесів у цифровому просторі.

РОЗДІЛ 2. ОСНОВНІ ПІДХОДИ ДО РЕГУЛЮВАННЯ ОНЛАЙН-ПЛАТФОРМ

2.1 Американський підхід до регулювання онлайн-платформ

Після з'ясування правової природи онлайн-платформ, причин трансформації платформ із суто приватних сервісів у такі, що мають публічно-правове значення, оскільки впливають на реалізацію фундаментальних прав користувачів та функціонування демократичних інститутів, закономірно постає питання щодо концепцій та підходів до їхнього регулювання. У результаті в сучасній правовій практиці сформувалося кілька концептуально відмінних моделей регулювання онлайн-платформ, кожна з яких відображає певний набір суспільних цінностей, що домінують у тій чи іншій правовій системі; власне бачення співвідношення свободи підприємницької діяльності та публічного інтересу, саморегулювання та державного контролю.

Метою цього підрозділу є дослідження основних підходів до правового регулювання онлайн-платформ, що сформувалися у найбільш впливових правових системах світу, а також встановлення передумов для формування європейської концепції регульованого або контрольованого саморегулювання, що було відображено в DSA. Для досягнення цієї мети послідовно аналізуються три найбільш впливові підходи до регулювання цифрового середовища загалом, онлайн-платформ та захисту прав користувачів у цифровому середовищі. Спочатку розглядається американська модель, яка історично ґрунтується на мінімальному втручанні держави у сферу регулювання цифрового середовища та широкому застосуванні механізмів саморегулювання онлайн-платформ, що є реалізацією принципу пріоритету свободи вираження поглядів, який домінує в американському правовому просторі. Далі розглядається китайська модель, для якої стало характерним домінування державного контролю над цифровим

простором, абсолютний пріоритет публічних інтересів над приватними, широкі адміністративні повноваження державних органів щодо втручання в діяльність онлайн-платформ, що можна пояснити авторитарним характером китайської влади, ціллю якої є унеможливлення зміни політичного режиму держави. Завершальна частина присвячена європейській моделі регулювання, яка сформувалася як окрема та самостійна концепція між попередніми крайніми підходами та базується на поєднанні елементів цих двох концепцій, як-от: приватного саморегулювання із системою обов'язкових публічно-правових вимог, спрямованих на забезпечення прозорості діяльності онлайн-платформ та захисту фундаментальних прав користувачів платформ.

З методологічної точки зору дослідження ґрунтується на поєднанні порівняльно-правового, історико-правового та догматичного методів. Порівняльно-правовий метод застосовується для виявлення спільних рис та принципових відмінностей зазначених концепцій; історико-правовий метод був використаний для аналізу еволюції відповідних моделей регулювання; догматичний – для аналізу нормативно-правових актів, які визначають правовий режим діяльності онлайн-платформ, прав користувачів тощо. Загалом цей підхід дозволяє простежити закономірності розвитку відповідних концепцій правового регулювання платформ та обґрунтувати місце відповідної моделі серед них.

Історія розвитку Інтернету та його регулювання на території КНР є досить складною та довгою. Вперше доступ до всесвітньої мережі в країні з'явився у 1987 році, але його використання було обмежено державними органами та науково-дослідними установами. З 1995 року Інтернет стає доступним в Китаї вже для широкого загалу, а також з метою комерційного використання. Як наслідок кількість користувачів почала стрімко зростати: протягом 1995 року їхня кількість зросла від 3000 до 40000 осіб. Також протягом наступних років були засновані

нинішні китайські ІТ гіганти, так як NetEase (1997 року), Tencent (лютий 1999 року), Alibaba (квітень 1999 року), Baidu (січень 2000 року) тощо⁷⁵.

Поява Інтернету в Китаї відбулася в період економічної та часткової політичної лібералізації, який розпочався в КНР після смерті Мао Цзедуна в 1976 році та закінчення руйнівної двадцятирічної культурної революції та часткової міжнародної ізоляції, яка нанесла країні значні економічні збитки. З приходом до влади Дена Сяопіна КНР почала реалізовувати політику покращення зіпсованих дипломатичних відносин з країнами Заходу та Сполученими Штатами зокрема та політику інтеграції КНР в міжнародну спільноту та систему міжнародної торгівлі. Так зокрема КНР розпочала процес вступу до Світової організації торгівлі та вступила до неї у 2001 році⁷⁶.

Вочевидь причина початку цієї епохи лібералізації була досить прагматичною: культурна революція замість «великого скачка» так і залишила КНР відсталою та закритою аграрною державою, яка не могла конкурувати з індустріальними гігантами Заходу, більше того бідність та розруха могли стати приводом для масових соціальних заворушень, які могли поставити під сумнів легітимність правлячого авторитарного режиму КПК (Комуністична партія Китаю)⁷⁷.

В той же час країни Заходу позитивно зустріли початок епохи лібералізації та зокрема поширення на території Китаю доступу до Інтернету, оскільки були переконані, що це призведе до ще більшої перебудови всередині КНР та перетворить її в демократичну країну. Так, наприклад, Білл Клінтон у своїй промові у 2000 році зазначив: «Ми знаємо, наскільки Інтернет змінив Америку, і ми вже є

⁷⁵ Webster, G. (2019). A brief history of the Chinese Internet. <https://logicmag.io/china/a-brief-history-of-the-chinese-internet/>

⁷⁶ Sapir, A., & Mavroidis, P. C. (2021, April 29). China and the WTO: An uneasy relationship. <https://cepr.org/voxeu/columns/china-and-wto-uneasy-relationship>

⁷⁷ Webster, G. (2019). A brief history of the Chinese Internet. <https://logicmag.io/china/a-brief-history-of-the-chinese-internet/>

відкритим суспільством.... Уявіть, наскільки це може змінити Китай (примітка – переклад автора)»⁷⁸.

Влада КНР не збиралася будувати відкрите суспільство в країні, оскільки в майбутньому це могло зруйнувати побудований авторитарний режим, а тому вона готувалася адаптувати Інтернет до китайського культурно-правового простору, а саме встановлення політичної цензури та обмеження свободи висловлення. В Китаї вже існувала система політичної цензури та обмежень свобода висловлення в межах традиційних ЗМІ, які належали державі: газети, журнали, радіо та телебачення. У китайського керівництва для цього були всі можливості, оскільки створення інтернет-інфраструктури в Китаї здійснювалося державою, інтернет-провайдери повинні мати ліцензію для здійснення своєї діяльності та хоча б на 51% належати державним компаніям⁷⁹. Таким чином, китайська влада могла досить легко реалізувати впровадження обмежень до свого інтернет-простору. З цього приводу Ану Бредфорд влучно зазначила, що «Китайський уряд перетворив Інтернет з засобу просування демократії на інструмент, що слугує автократії ... Це показує, що свобода не є невід'ємною рисою інтернету, а скоріше об'єктом політичного вибору тих, хто має владу дозволяти або подавляти цю свободу (примітка – переклад автора)»⁸⁰.

Структура державних органів для контролю за інтернет-простором в Китаї протягом 2000-х років була досить розгалуженою. Інституційно ця система складалася з різних органів партійно-урядового апарату: з двох керівних груп Центрального комітету КПК, які займалися широким колом питань, Центрального відділу пропаганди КПК, який відповідав за щоденне управління пропагандою, Інформаційного бюро Державної ради, яке стежило за новинами, та ряду органів на

⁷⁸ Sanger, D. E. (2000, March 9). Clinton sends to a wary Congress a long-delayed China trade bill. The New York Times. <https://www.nytimes.com/2000/03/09/world/clinton-sends-to-a-wary-congress-a-long-delayed-china-trade-bill.html>

⁷⁹ Weber Digital. (2023). What is an ICP license? Types & requirements. <https://service.weber.digital/index.php?/en/Knowledgebase/Article/View/what-is-an-icp-license-types--requirements>

⁸⁰ Bradford, A. (2023). Digital empires: The Global Battle to Regulate Technology. Oxford University Press. C. 103

рівні міністерства, які здійснювали нагляд за державними ЗМІ⁸¹. Разом з тим в 1996 році Державною Радою КНР були видані Тимчасові положення, що регулюють управління комп'ютерними інформаційними мережами, які вперше визначили перелік забороненої для передачі в інтернет-просторі інформації: інформації щодо національної безпеки, державної таємниці, інформації, яка порушує соціальну стабільність та матеріали сексуального характеру. А в 2000 році цей перелік був розширений у новому документі - Міри з управління інформаційними інтернет-службами, де було додано інформацію, що підриває національну єдність, соціальний порядок, поширення чуток, інформацію, яка зачіпає честь та інтереси держави, інформацію, яка суперечить базовим принципам конституції або порушує закони та інші адміністративні регулювання. Також в 2003 році для посилення політичної цензури в Китаї також була впроваджена фільтраційна система «Золотий щит», яка обмежувала користувачам доступ до інформації, яка містить заборонені слова⁸².

Таким чином, можна сказати, що вже на ранньому етапі існування Інтернету в Китаї влада КНР швидкими темпами сформувала систему політичної цензури для своїх користувачів, фактично перенісши її з сфери традиційних китайських ЗМІ. Діяльність китайської влади протягом цього періоду була сфокусована на виключно на обмеженнях користувачів. Що ж стосується інтернет-провайдерів та онлайн-платформ, то Китай не поспішав створювати комплексне регулювання для них.

Китайська влада вочевидь була зацікавлена у формуванні власних ІТ гігантів, які б по-перше, могли стимулювати технологічний прогрес в сфері китайських цифрових технологій, а по-друге, щоб конкурувати з американськими ІТ гігантами як на території Китаю, так і за його межами. А це дало б можливість убезпечити китайських користувачів від американського впливу, який розповсюджували

⁸¹ Creemers, R. (2017). Cyber China: Upgrading propaganda, public opinion work and social management for the twenty-first century. *Journal of Contemporary China*, 26(103), 85–100. с. 89

⁸² Zheng, H. (2013). Regulating the Internet: China's Law and Practice. *Beijing Law review*, 4(1), 37–41. <http://dx.doi.org/10.4236/blr.2013.41005> с. 38

американські корпорації, та мати можливість здійснювати свій вплив на третій країни.

Зміни в напрямку регулювання онлайн-платформ розпочалися з обранням Сі Цзіньпіна головою КНР у 2013 році. Секретне комюніке Центрального комітету КПК було розповсюджено серед вищих посадовців. У цьому документі було визначено сім категорій потенційного ідеологічного ризику та зазначено, що Інтернет, зокрема, є каналом для «помилкових тенденцій мислення» для проникнення в основний дискурс. Це супроводжувалося медійною кампанією, у ході якої центральні партійні ЗМІ опублікували серію статей із закликами до ідеологічної чесності та пильності щодо проникнення та втрати контролю, зокрема в Інтернеті⁸³.

Можна виділити наступні підстави для впровадження комплексного регулювання онлайн-платформ:

- Занепокоєння китайської влади щодо використання соціальних мереж для координації протестів та інших соціальних заворушень на прикладі Арабської весни⁸⁴;
- Оприлюднення Едвардом Сноуденом секретних документів, які розкривають можливості американської розвідки по спостереженню за іноземними чиновниками⁸⁵.
- Китайські ІТ гіганти майже повністю забезпечували китайських користувачів власними цифровими сервісами.

2. Ключові нормативно-правові акти КНР для регулювання інтернет-простору

⁸³ Creemers, R. (2017). Cyber China: Upgrading propaganda, public opinion work and social management for the twenty-first century. *Journal of Contemporary China*, 26(103), 85–100. С. 91

⁸⁴ Fontaine, R., & Rogers, W. (2011, October). China's Arab Spring cyber lessons. *The Diplomat*. <https://thediplomat.com/2011/10/chinas-arab-spring-cyber-lessons>

⁸⁵ Strittmatter, K. (2013, July 3). Why China's internet censors can't get enough of Edward Snowden. <https://worldcrunch.com/world-affairs/why-china039s-internet-censors-can039t-get-enough-of-edward-snowden>

Протягом наступних років в Китаї були прийняті чотири ключові закони, які стали основою державного регулювання інтернет-простору в країні, а саме:

- 1) Закон про кібербезпеку 2016 року;
- 2) Закон про електронну комерцію 2018 року;
- 3) Закон про захист персональної інформації 2021 року;
- 4) Закон про охорону даних 2021 року.

Закон про кібербезпеку КНР був прийнятий в 2016 році. Як зазначається в самому законі його ціллю є захист китайського кіберпростору, державних та приватних інтересів в цій сфері тощо. Серед термінів закон визначає поняття «кібербезпеки», під чим розуміється здатність запобігати мережевим атакам, вторгненням, перешкодам, пошкодженню, незаконному використанню та нещасним випадкам, робити мережі стабільними та надійними, а також забезпечувати цілісність, конфіденційність і доступність мережових даних, а також поняття «оператора мережі», що охоплює власників мереж, адміністраторів та постачальників мережових послуг.

Від операторів мереж, організацій, пов'язаних з інтернет-індустрією, вимагається:

1. дотримання положень законів та регулювань, «поважати соціальну мораль, дотримуватись ділової етики, діяти сумлінно, виконувати свої зобов'язання щодо захисту кібербезпеки, приймати нагляд з боку уряду та громадськості та брати на себе соціальну відповідальність», а також «покращити галузеву самодисципліну, сформулювати кодекси поведінки щодо кібербезпеки, навчити своїх членів посилювати заходи кібербезпеки, покращити можливості кібербезпеки та сприяти здоровому розвитку галузі»;

2. створення багаторівневої системи захисту кібербезпеки для запобігання несанкціонованим втручанням та захисту персональних даних користувачів (створення правил внутрішньої безпеки, технічних мір по запобігання зараженню комп'ютерними вірусами, боротьбі з кібератаками, технічних мір по спостереженню за статусом операцій в мережі та їх запису, такі

міри, як класифікація даних, резервне копіювання важливих даних і шифрування даних тощо). У випадку виявлення вразливості в системі безпеки оператори окрім вживання необхідних заходів мають також повідомити про інцидент державні органи; при зборі персональних даних чітко зазначати про це та здійснювати збір тільки у випадку їхньої згоди;

3. при реєстрації користувачів мають вимагати від них надання відомостей, які підтверджують їхню особу. Без цього реєстрація не дозволяється; мають надавати технічну підтримку та допомогу відповідним органам державної влади за їхнім запитом. Зокрема в сфері сприяння розслідуванню кримінальних правопорушень;

4. Провайдери інтернет-послуг, які збирають персональні дані китайських користувачів, мають зберігати на серверах в межах материкового Китаю. Для отримання дозволу на передачу даних за межі Китаю має бути проведене безпекова оцінка;

5. Принаймні один раз на рік оператори критичної інформаційної інфраструктури повинні проводити оцінку потенційних ризиків мережевої безпеки особисто або довіривши це постачальнику послуг кібербезпеки. Результати цієї оцінки та заходи щодо покращення мають бути представлені відповідному відділу, відповідальному за безпеку критичної інформаційної інфраструктури;

6. Провайдери інтернет-послуг, які збирають персональні дані користувачів, мають зберігати конфіденційність цих даних, не повинні збиратися дані не пов'язані з діяльністю платформи, персональні дані не повинні розкриватися, зазнавати шкоди або передаватися третім сторонам без згоди користувача.

Від будь-якої фізичної або юридичної особи вимагається:

1. дотримуватися в інтернет-просторі соціального порядку, поважати соціальну мораль, не брати участь в діяльності, яка загрожує національній безпеці та інтересам, не закликати до повалення соціалістичного режиму, терористичних або екстремістських актів, розпалювати сепаратистські настрої, не пропагувати

дискримінацію чи етнічну ворожнечу, поширювати неправдиву інформацію, жорстокий або порнографічний контент, порушувати авторські або інші права інших осіб тощо. Будь-яка особа чи організація має право повідомляти про поведінку, яка загрожує кібербезпеці, органам влади в кіберпросторі, органам телекомунікацій, органам громадської безпеки чи іншим відповідним органам;

2. не повинні створювати веб-сайти чи групи спілкування з метою вчинення шахрайства, поширення злочинної діяльності, виробництва чи продажу заборонених або контрольованих товарів або участі в іншій незаконній та злочинній діяльності;

3. У випадку порушення провайдером відповідних вимог щодо збору та обробки персональних даних користувач має право вимагати видалення відповідних даних;

4. надіслана електронна інформація чи прикладне програмне забезпечення, надане будь-якою особою чи організацією, не повинно встановлювати зловмисне програмне забезпечення або містити інформацію, публікацію чи передачу якої заборонено законами та адміністративними правилами.

Закон наділяє державу повноваженнями зокрема:

1. по формуванню стратегій, регламентів та вимог у сфері кібербезпеки, а також приймати міри для попередження та боротьби з кібербезпековими ризиками, захищати критичну інформаційну структуру тощо. Безпосередньо відповідальним за реалізацію цих повноважень є Адміністрація з кіберпростору (далі – САС), а також відділи Державної Ради.

2. Національні органи кіберпростору та відповідні департаменти несуть відповідальність за моніторинг та управління безпекою онлайн-контенту. Якщо вони виявляють публікацію або передачу інформації, яка заборонена законами чи адміністративними правилами, вони вимагають, щоб оператори мереж припинили передачу такої інформації та вжили заходів для видалення, таких як видалення.

3. Департаменти та їхній персонал, який відповідає за нагляд та адміністрування кібербезпеки, повинні зберігати особисту інформацію, приватну інформацію та комерційну таємницю, отриману під час виконання своїх обов'язків, у суворій конфіденційності та не повинні розголошувати, продавати чи незаконно надавати таку інформацію іншим особам.

Законом передбачаються покарання у вигляді штрафів. До найсерйозніших видів порушень можна віднести: по-перше, участь у діяльності, яка спрямована на загрозу кібербезпеці, технічній підтримці тощо або створення інструментів та програм для цього і якщо це не становить склад злочину, то може застосовуватися штраф від 50000 до 500000 юанів з конфіскацією незаконного прибутку та арештом до 5 діб, а серйозних випадках штраф зростає до 100000 юанів та арешту до 15 діб; по-друге, у випадку створення веб-сайтів для здійснення незаконної або злочинної діяльності в серйозних випадках може каратися штрафом в 50000-500000 юанів та арештом від 5 до 15 діб; по-третє, оператор критичної інформаційної інфраструктури не справляється зі своїми основними зобов'язаннями в сфері кібербезпеки, за що йому може загрожувати штраф від 100000 до 1000000 юанів⁸⁶.

Отже, закон про кібербезпеку є основою нового режиму комплексного регулювання інтернет-простору в Китаї. З одного боку, закон спрямований на формування безпечного для користувачів інтернет-простору, зобов'язує інтернет-провайдерів та онлайн-платформи проводити регулярні оцінки ризиків в їхніх системах. З іншого ж боку, закон встановлює перелік видів забороненої інформації з дуже широкими можливостями щодо трактування (поширення неправдивої інформації, посягання на суспільну мораль), що вочевидь обмежує свободу висловлення користувачів. Також закон закріплює повноваження державних органів по спостереженню за діяльністю онлайн-платформ та зобов'язує платформи надавати технічну допомогу на вимогу державних органів, за

⁸⁶ DigiChina. (2017). Translation: Cybersecurity law of the People's Republic of China.<https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/>

діяльністю користувачів на платформах і у разі виявлення незаконного контенту надсилати платформі вимогу про його видалення.

Закон про електронну комерцію КНР було прийнято в 2018 році. Під «електронною комерцією» розуміється комерційна діяльність з продажу товарів або надання послуг через Інтернет або будь-яку іншу інформаційну мережу. Однак існує ряд винятків: фінансові продукти та послуги, інформація про новини, аудіо- та відеопрограми, публікації, культурні продукти та інші контент-послуги, що надаються через інформаційні мережі.

Виділяється такі категорії суб'єктів як:

«бізнес електронної комерції», що означає фізичних осіб або юридичних осіб, які займаються підприємницькою діяльністю з продажу товарів або надання послуг через Інтернет або будь-яку іншу інформаційну мережу, включаючи підприємства платформи електронної комерції, компанії, що працюють на платформі, і компанії електронної комерції, які продають товари або надають послуги за допомогою самостійно створеного веб-сайту або будь-яких інших мережевих послуг;

«бізнес платформи електронної комерції», що означає юридичну особу або організацію без статусу юридичної особи, яка надає такі послуги, як онлайн-площадки для бізнесу, пошук партнерів і оприлюднення інформації, щоб вони могли самостійно вести торгову діяльність;

«бізнес на платформі» означає бізнес електронної комерції, який продає товари або надає послуги через платформу.

Значна частина положень стосується зобов'язань комерційних онлайн-платформ, серед яких можна виділити наступні ключові моменти:

1. На бізнеси електронної комерції покладаються наступні зобов'язання: при продажі товарів або надаванні послуг дотримуючись вимог гарантії особистої та майнової безпеки тощо, гарантувати користувачам право вибору шляхом повного та точного розкриття інформації про товари та послуги, які надаються;

повинен гарантувати користувачам право на виправлення та видалення особистої інформації; гарантувати користувачам можливість відмовитися від таргетованої реклами, повинні надавати на вимогу державних органів відповідні дані та інформацію, пов'язані з електронною комерцією;

2. Від бізнес платформ електронної комерції вимагається: при реєстрації бізнесів на своїй платформі вимагати від них вказати особисті дані, адресу тощо; в разі виявлення порушень, які були здійснені бізнесами на платформі, мають повідомити про це відповідні органи; приймати міри по запобіганню кіберзлочинів та іншої незаконної діяльності у себе на платформі; записувати та зберігати інформацію про товари та сервіси на платформі, а також про транзакції.

3. Відповідно до Закону про електронну комерцію, якщо власник прав інтелектуальної власності (далі - ІВ) вважає, що оператор платформи порушив його права ІВ, власник прав ІВ може повідомити оператора платформи та вимагати від останнього вжити необхідних попередніх заходів, таких як видалення або перегляд інформації про ймовірне порушення, відключення відповідних веб-сторінок або припинення транзакції чи послуги. Якщо оператор платформи не зміг негайно вжити необхідних попередніх заходів після отримання повідомлення, він несе солідарну відповідальність за додаткові збитки разом з оператором платформи⁸⁷.

Загалом закон про електронну комерцію встановлює різні зобов'язання для комерційних онлайн-платформ та права для користувачів для запобігання зловживань з боку платформ. Законом встановлюється досить зручний та зрозумілий поділ на бізнеси електронної комерції, які надають свої послуги та товари за допомогою одного сайту, бізнес платформи електронної комерції, які окрім вище зазначеної діяльності можуть надавати майданчик для суб'єктів підприємницької діяльності, бізнеси на платформі, які є фізичними або

⁸⁷ Library of Congress. (2018, November 21). China: E-commerce law passed. Global Legal Monitor. <https://www.loc.gov/item/global-legal-monitor/2018-11-21/china-e-commerce-law-passed>

юридичними особами, які здійснюють свою діяльність на майданчику комерційної онлайн-платформи⁸⁸.

Закон про захист персональних даних та Закон про охорону даних були прийняті в 2021 році. Відповідно до закону під особистими даними розуміються різні види інформації, пов'язаної з ідентифікованими фізичними особами, записаної електронними або іншими засобами, за винятком інформації, яка обробляється анонімно. Також окремо виділяється поняття чутливої інформації, до якої відноситься інформація, яка пов'язана з особистою гідністю, майновою та особистою безпекою. Вона охоплює біометричні дані, релігійні вірування, медичні дані, фінансові рахунки, місце проживання, а також будь-які особисті дані осіб до 14 років. Персональні дані осіб мають збиратися та оброблятися тільки за виправданої та визначеної мети цього процесу і за згоди особи. Однак закон встановлює ряд винятків, де згоди особи не потрібна, а саме: у випадку загрози життю чи здоров'ю особи, коли дані використовуються в змi і це виправдано суспільним інтересом та в розумних межах, коли інформація розкрита самою особою, коли це необхідно для виконання статутних зобов'язань, тощо.

Цікавим є положення, що обладнання для зйомки зображень та ідентифікації особи, встановлене в громадських місцях, є необхідним для забезпечення громадської безпеки, дотримання законів держави. Особисті зображення та зібрану особисту інформацію можна використовувати лише з метою підтримки громадської безпеки та не використовувати для інших цілей, якщо не отримано згоду особи. Так само як в законі про кібербезпеку в цьому законі вказується вимога зберігання персональних даних користувачів на серверах виключно на території КНР. Серед зобов'язань, які накладаються на суб'єктів обробки персональних даних, варто зазначити проведення регулярних аудитів, а також оцінку впливу на захист персональних даних різних обставин (обробка чутливої інформації,

⁸⁸ Ministry of Commerce of the People's Republic of China. (2019). E-commerce law of the People's Republic of China. <http://mg.mofcom.gov.cn/article/policy/201912/20191202923971.shtml>

передача персональних даних за кордон тощо). Оцінка впливу охоплює визначення чи обробка має виправдану та законну мету, вплив на права та інтереси осіб тощо.

Також закон окремо виділяє категорію «обробників персональної інформації, які надають важливі послуги інтернет-платформи для великої кількості користувачів і складних типів бізнесу», що можна порівняти зі поняттями «дуже великі онлайн-платформи» та «дуже великі пошукові онлайн-системи» з Акту про цифрові послуги ЄС. До них застосовуються наступні зобов'язання:

1. створити та вдосконалити систему відповідності для захисту персональної інформації відповідно до державних норм, а також створити незалежну організацію, що складається переважно із зовнішніх членів для захисту особистої інформації
2. Припинити надавати послуги продукту або постачальникам послуг на платформі, які серйозно порушують закони та адміністративні правила щодо обробки особистої інформації
3. Регулярний випуск звіту про соціальну відповідальність щодо захисту персональної інформації та підлягає громадському контролю.

Від іноземних провайдерів інформаційних послуг, які займаються обробкою персональних даних, вимагається створити на території КНР представництво для того, щоб мати можливість займатися цією діяльністю. У випадку якщо іноземні суб'єкти обробки персональних даних своєю діяльністю порушують права осіб, загрожують національній безпеці тощо, то в такому випадку ці суб'єкти вносяться до переліку організацій, яким забороняється здійснювати обробку персональних даних осіб.

Законом передбачаються такі права осіб щодо персональних даних: приймати рішення щодо обробки персональних даних та відмовлятися давати згоду на обробку, отримувати копію даних, які обробляються, вимагати усунути помилку в особистих даних, вимагати видалення персональних даних, вимагати пояснити правила обробки персональних даних. Правами щодо персональних даних особи у випадку її смерті можуть користуватися її рідні.

Закон про захист персональних даних як і закон про кібербезпеку також передбачає повноваження САС, саме: створювати стандарти захисту персональних даних, наглядати за обробкою персональних даних державними органами, приймати скарги (зокрема і анонімні) щодо порушень в сфері обробки персональних даних тощо. Також цим законом передбачається відповідальність за порушення зобов'язань в сфері захисту персональних даних. У випадку відмови усунути порушення може бути накладено штраф розміром до 1000000 юанів, а у серйозних випадках – до 50000000 юанів або 5% від річного обороту. По відношенню до іноземних провайдерів також може бути застосована така міра як заморожування їх фінансових активів на території Китаю або накладені інші види санкцій⁸⁹.

Закон про охорону персональних даних був прийнятий в 2021 році. Ціллю регулювання цього документу є стандартизація діяльності з обробки даних, забезпечення безпеки даних, сприяння розвитку та використанню даних. Значна частина положень стосуються зобов'язань держави по створенню стандартів захисту даних, відповідної інфраструктури тощо. Також держава повинна встановити систему захисту даних за категоріями та ступенями, впроваджуючи захист даних за категоріями та ступенями відповідно до ступеня важливості даних для економічного та соціального розвитку, а також ступеня небезпеки для національної безпеки, суспільних інтересів або законні права та інтереси окремих осіб або організацій, які виникають у разі їх зміни, знищення, витоку або незаконного отримання чи використання.

Що ж до зобов'язань передбачених для надавачів інформаційних послуг, то на них покладається наступне:

1. Проведення діяльності з обробки даних повинно здійснюватися відповідно до положень законів та адміністративних правил, створення та

⁸⁹ China Briefing. (2021). The PRC Personal Information Protection Law (Final): A full translation.<https://www.china-briefing.com/news/the-prc-personal-information-protection-law-final-a-full-translation/>

завершення системи управління безпекою даних для всього робочого процесу, організації та проведення навчання та навчання з безпеки даних, а також прийняття відповідних технічних заходів та інших необхідних заходів для забезпечення безпеки даних.

2. Проведення діяльності з обробки даних повинно посилити моніторинг ризиків, і коли виявлено недоліки безпеки даних, витоки чи інші подібні ризики, необхідно негайно вжити заходів для їх усунення; у разі виникнення інцидентів із безпекою даних слід негайно вживати методи їх усунення, негайно сповіщаючи користувачів і повідомляючи відповідним відповідальним відділам, як це передбачено.

3. Особи, які обробляють важливі дані, повинні періодично проводити оцінку ризиків такої діяльності з обробки даних, як це передбачено, і подавати звіти про оцінку ризиків відповідним відповідальним департаментам. Звіти про оцінку ризиків повинні включати тип і обсяг важливих даних, що обробляються, обставини діяльності з обробки даних, ризики безпеки даних, з якими зіткнулися, та заходи щодо їх вирішення тощо.

За порушення цих положень провайдери отримують попередження та вимогу усунути порушення, а також можливе накладення штрафу від 50000 до 500000 юанів, а у випадку неусунення порушення може бути накладено штраф розміром в 500000-2000000 юанів. У разі порушення основних національних систем управління даними, що ставить під загрозу національний суверенітет, безпеку чи інтереси розвитку, відповідні відповідальні департаменти мають накласти штраф у розмірі від 2 000 000 до 10 000 000 юанів⁹⁰.

Отже, закон про захист персональних даних та закон про охорону даних встановлюють комплексну систему як особистих даних, так і будь-яких інших важливих даних, а також гарантують користувачам права щодо своїх персональних даних, зокрема конфіденційність. Положення щодо оцінки ризиків, які мають

⁹⁰ China Briefing. (2021). The PRC Personal Information Protection Law (Final): A full translation.<https://www.china-briefing.com/news/the-prc-personal-information-protection-law-final-a-full-translation/>

проводитися інтернет-провайдерами та онлайн-платформами дещо повторюють положення із закону про кібербезпеку. З іншого боку, хоч і гарантується, що обробка персональних даних може проводитися лише за згоди особи, деякі з винятків, при яких згода не вимагається, можуть трактуватися досить широко, що знову ж дозволятиме державі втручатися в особисте життя користувачів. Також цими законами значно ускладнюється діяльність іноземних суб'єктів в сфері обробки даних, оскільки за загальним правилом дані китайських користувачів можуть зберігатися тільки на серверах на території Китаю. І хоча закон дозволяє передачу даних за кордон, однак це сильно ускладнюється необхідністю отримати відповідні дозволи. Таким чином, ці два закони спрямовані і на обмеження впливу іноземних ІТ гігантів (в першу чергу американських). Окрім того, законами закріплюється можливість заборони діяльності іноземних суб'єктів як покарання за порушення положень цих законів.

Особливо важливим елементом в китайській системі регулювання онлайн-платформ є політична цензура. Загалом поняття «незаконний контент» в КНР включає в себе три категорії: політично шкідливий або чутливий контент, вульгарний контент та контент, пов'язаний з неполітичною дезінформацією та чутками⁹¹. Питання забороненої інформації детально висвітлено в Положеннях про управління екосистемою інформаційного контенту онлайн, виданих САС. До цього переліку входять такі види інформації як: інформація, що суперечить основним принципам, викладеним у Конституції Китаю, законах чи постановах; інформація, яка загрожує державній безпеці, підризу державної влади; інформація, яка шкодить національній честі та національним інтересам Китаю; інформація, яка розпалює етнічну ворожнечу, расову дискримінацію або порушує етнічної єдності; інформація, яка заподіює шкоду національній релігійній політиці та поширює феодальних забобонів; інформація, що поширює чутки, порушує суспільний порядок та стабільність; інформація, що підбурює до незаконних зборів,

⁹¹ Wang, J. (2020). Regulation of digital media platforms: The case of China. Oxford: The Foundation for Law, Justice and Society

демонстрацій, протестів, порушення громадського порядку тощо⁹². Вочевидь даний перелік забороненої інформації написано максимально розпливчасто, що дозволяє відносити будь-який контент, який не подобається китайській владі.

Також варто додати, що для виробництва новин в інтернет-просторі онлайн-платформ та новинним сайтам необхідно отримати ліцензію від САС. Згідно з Положеннями про управління інформаційних служб новин в Інтернеті до новин відносяться саме висвітлення або повідомлення про публічні події або шокуючі соціальні інциденти, в той час як, наприклад, новини про спортивні події або в розважальній сфері цим документом не регулюються⁹³. Ці положення зокрема можуть стосуватися і користувачів онлайн-платформ, які в своїх дописах можуть повідомляти власну інформацію про певні публічні події, а не просто поширювати дані, взяті з офіційних джерел. Однак в адміністрації китайських онлайн-платформ часто виникають труднощі з визначенням, що входить до поняття «новини» згідно з вище згаданими положеннями, а тому можуть надавати можливість певним користувачам публікувати новини, які суперечать офіційним китайським ЗМІ. Окрім того, Положення забороняють іноземному капіталу отримати відповідну ліцензію, навіть у партнерстві з китайським капіталом⁹⁴.

Прикладами реалізації політичної цензури можуть послугувати наступні випадки, які сталися з китайськими ІТ гігантами. Наприклад, Китайська САС змусила ряд популярних китайських онлайн-платформ (WeChat, Weibo та Tieba) видалити майже 60 популярних аккаунтів, які розповсюджували контент, в якому китайська влада вбачала «вульгарне та сенсаційне висвітлення скандалів зі знаменитостями та показного способу життя»⁹⁵. Далі САС у серпні 2017 року

⁹² China Law Translate. (2019). Provisions on the governance of the online information content ecosystem. <https://www.chinalawtranslate.com/en/provisions-on-the-governance-of-the-online-information-content-ecosystem/>

⁹³ China Law Translate. (2016). Provisions on Management of Internet News Services. <https://www.chinalawtranslate.com/en/provisions-on-internet-news-information-management/>

⁹⁴ Wang, J. (2022). Platform responsibility with Chinese characteristics. Defeating Disinformation. https://digitalplanet.tufts.edu/wp-content/uploads/2023/02/DD-Report_1-Jufang-Wang-11.30.22.pdf

⁹⁵ Reuters. (2017). China closes 60 celebrity gossip social media accounts. <https://www.reuters.com/article/us-china-internet-censorship-idUSKBN18Z0J3/>

наклала штрафи (на 500000 юанів) на трійку провідних китайських інтернет-гігантів (Tencent, Baidu і Sina) через те, що користувачі онлайн-платформ, що належали цим корпораціям, поширювали «інформацію про насильство та терор, неправдиві чутки, порнографію та іншу інформацію, яка ставить під загрозу національну безпеку, громадську безпеку та суспільний порядок».

Також варто зазначити, що КНР реалізує свою регуляторну політику щодо онлайн-платформ шляхом ініціативи «Частка для спеціального управління». Вона передбачає, що китайський уряд купує у компаній, що є власниками невеликих онлайн-платформ невелику частку акцій (1-2%). Завдяки цьому китайський уряд має можливість призначити свого представника до ради директорів компанії-власника онлайн-платформи, що дає можливість отримання додаткового редакторського контролю над відповідною онлайн-платформою⁹⁶.

Висновки. Можна підсумувати, що за майже 25 років Китай зумів успішно побудувати власну систему регулювання онлайн-платформ та контролю за власним сегментом інтернет-простору. З однієї сторони КНР змогли створити комплексну правову систему захисту своїх інтернет-користувачів від свавілля та порушень з боку онлайн-платформ, яка є схожою на європейську систему регулювання онлайн-платформ. З іншого ж боку ця система забезпечує тотальний контроль з боку з держави над інформацією, яка рухається по китайському інтернет-сегменту, тобто створюється система політичної цензури.

Таким чином, можна виділити наступні ключові особливості китайського підходу до регулювання онлайн-платформ:

- Створення спеціального державного-партійного органу для контролю за онлайн-платформами та китайським сегментом інтернет-простору – Китайської адміністрації з кіберпростору (яка очолюється головою КНР Сі Цзіньпінем, що підкреслює важливість для китайської влади контролю за цією сферою);

⁹⁶ Gao, C. (2017, September). China fines its top 3 internet giants for violating cybersecurity law. The Diplomat. <https://thediplomat.com/2017/09/china-fines-its-top-3-internet-giants-for-violating-cybersecurity-law/>

- Створення комплексної системи захисту особистих даних користувачів від порушень та свавілля онлайн-платформ на основі європейського досвіду;
- Впровадження моніторингу з боку китайської влади за діяльністю на онлайн-платформах та вимога до адміністрацій онлайн-платформ здійснювати власний моніторинг та виявлення незаконного контенту;
- Забезпечення деанонізації інтернет-користувачів шляхом впровадження вимоги надання паспортних даних при реєстрації на будь-якій онлайн-платформі;
- Створення системи політичної цензури за допомогою визначення широкого переліку забороненої інформації з розпливчатим трактуванням, що дозволяє забороняти будь-який контент, який не подобається китайській владі.

2.2 Китайський підхід до регулювання онлайн-платформ

Марк Цукерберг, власник та виконавчий директор корпорації Meta, 7 січня 2025 року виклав відеозвернення на своїй сторінці у Facebook, в якому зазначив, що компанія збирається переглянути політику модерації у власних соціальних мережах (Facebook, Instagram, Threads), зменшивши цензурування, та відмовитися від «фактчекерів», які були залучені корпорацією у 2016, і замінити їх на «нотатки від спільноти», що застосовуються, наприклад, в соцмережі «X». Цукерберг пояснив дане рішення тим, що «фактчекери стали занадто політично упередженими та руйнували довіру більше, ніж її створювали»⁹⁷. Заміна незалежних «фактчекерів» на «нотатки від спільноти» може бути корисною для створення більш прозорої системи перевірки інформації, а також може зменшити звинувачення у цензурі з боку консервативних чи інших груп, які раніше критикували Meta. Проте спільнота може не завжди ефективно протидіяти

⁹⁷ Booth, R. (2025). Meta to get rid of factcheckers and recommend more political content. The Guardian. <https://www.theguardian.com/technology/2025/jan/07/meta-facebook-instagram-threads-mark-zuckerberg-remove-fact-checkers-recommend-political-content>

фейковим новинам через брак експертності, що може призвести до зниження якості інформаційного середовища, посилює ризик використання платформ для політичної пропаганди та поляризації суспільства. Дану ж ситуацію можна назвати проявом принципу саморегулювання, що є одним з характерних аспектів американського підходу до регулювання онлайн-платформ.

Вище згаданий американський підхід, який виник першим, став ґрунтуватися на невтручанні держави в діяльність онлайн-платформ, щоб не заважати прискоренню інновацій в цифровій сфері, а тому його коливання зрушено в бік приватного інтересу. Фактично китайський та європейський підходи стали зворотною реакцією та відповіддю на американський підхід та його фокус на мінімальному втручанні. Так європейський підхід переважно був сфокусований на захист фундаментальних прав користувачів онлайн-платформ, а тому при ньому відбувається балансування між вимушеним державним контролем та регулюванням задля забезпечення фундаментальних прав і приватними інтересами онлайн-платформ, а китайський підхід своєю чергою розглядає регулювання онлайн-платформ як один з інструментів контролю держави за громадянами та забезпечення існування правлячого політично-правового режиму, а тому в цьому випадку коливання сильно зрушено в напрямку публічного або державного інтересу.

Причинами ранньої успішності американського підходу можна вважати стрімкий розвиток цифрових технологій та інновацій, оскільки це було достатнім для американської влади аргументом, що мінімальна роль держави у регулюванні онлайн-платформ є вірним варіантом; з поширенням доступу до Інтернету по світу американські онлайн-платформи були ефективним способом поширення американських цінностей в інші країни світу. Однак, протягом часу стали як і очевидні недоліки даного підходу до регулювання, так і відмінність у пріоритетах регулювання (в ЄС – пріоритет захисту прав людини, в КНР – пріоритет забезпечення існування правлячого режиму), які зокрема і спричинили виникнення європейського та китайського підходів. Так даний підхід призвів до того, що без втручання держави, за відсутності федеральних законів про захист даних

користувачів, а також бездіяльності з боку антимонопольних органів власники онлайн-платформ отримали значну владу над своїми користувачами та їхніми особистими даними, що створювало передумови для вчинення онлайн-платформами різноманітних зловживань⁹⁸.

А проте в останні роки американська федеральна влада почала робити перші кроки з внесення змін до даного підходу, а на рівні штатів почали прийматися перші закони, що врегульовують певні аспекти діяльності онлайн-платформ.

1. Регулювання онлайн-платформ на федеральному рівні до 2016 року

Хоча Сполучені Штати і є одним з найперших та найбільшим осередком онлайн-платформ у світі держава майже не намагається їх контролювати. З моменту масового розповсюдження інтернету та створення перших онлайн-платформ на території США майже зразу сформувалася ідея того, що інтернет-простір має бути вільним від впливу реального світу, що виражалася в недопущенні того, що держава може регулювати та контролювати інтернет-спільноти. Навпаки вони повинні бути саморегульованими. Ці ідеї просувалися візіонерами та відповідно творцями перших онлайн-платформ, а згодом вони знайшли відгук і серед представників американської влади як в Конгресі, так і в тодішній адміністрації президента Клінтона⁹⁹. Таким чином, процес створення законодавчої бази для регулювання онлайн-платформ був повністю загальмований. Як зазначила виконавча директорка Silicon Flatirons Center Емі Степановіч: «Історично в США є купа розрізнених федеральних законів [вони] або направлені на конкретні типи даних, як-от кредитні дані чи інформацію про здоров'я або направлені на конкретні групи населення, як на дітей, і регулюють ці сфери»¹⁰⁰.

⁹⁸ Bradford, A. (2024). The false choice between digital regulation and innovation. *Northwestern University Law Review*, 118(2), 377–454. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4753107 с. 379

⁹⁹ Bradford, A. (2023). *Digital empires: The Global Battle to Regulate Technology*. Oxford University Press.

¹⁰⁰ Klosowski, T. (2021). The State of Consumer Data Privacy Laws in the US (And Why It Matters). *Wirecutter*. <https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/>

Американська законодавча база щодо захисту даних на федеральному охоплює такі закони¹⁰¹:

Акт про приватність 1974 року

Акт стосується виключно діяльності федеральних агенцій по збору та обробці персональних даних громадян. Документ гарантує право на отримання копії даних, які обробляються, право вимагати внести зміни у випадку неточності даних. Акт забороняє розкриття даних без письмової згоди особи, а також невинуватене втручання в особисте життя¹⁰².

Акт про мобільність та підзвітність медичного страхування 1996 року

Цей акт регулює діяльність зі збору обробки персональних медичних даних надавачам медичних послуг. Акт так само гарантує право користувача отримати копію своїх даних та право на виправлення неточності в персональних медичних даних, а також забороняє розкривати їх без наданої письмової згоди¹⁰³.

Акт про фінансову модернізацію або Акт Гремма-Ліча-Блайлі 1998 року

Даний документ стосується діяльності фінансових установ по збору та обробці персональних даних. Цей акт зобов'язує фінансові установи створювати політики по захисту даних користувачів, пояснювати як відбувається обробка персональних даних та забороняє передавати дані третім особам без згоди осіб¹⁰⁴.

Акт про захист конфіденційності дітей онлайн 2000 року

Акт стосується збору та обробки персональних даних дітей віком до 13 років, що може здійснюватися будь-якою приватною компанією або вебсайтом. Акт зобов'язує їх отримати дозвіл батьків або опікунів на обробку персональних даних дітей. Окрім того, батьки або опікуни дітей мають право отримати доступ до

¹⁰¹ Boyne, S. M. (2018). Data Protection in the United States. The American Journal of Comparative Law, (66), Supplement 1, 299–343. <https://www.scilit.com/publications/9cc47792af226bef0c996c5c21aec052> с. 318-321

¹⁰² Privacy Act of 1974, 5 U.S.C. § 552a (1974). <https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1279>

¹⁰³ Health Insurance Portability and Accountability Act of 1996 (1996). <https://aspe.hhs.gov/reports/health-insurance-portability-accountability-act-1996>

¹⁰⁴ Financial Services Modernization Act of 1999 (1999). <https://fraser.stlouisfed.org/title/financial-services-modernization-act-1999-gramm-leach-bliley-act-1050/fulltext>

оброблюваних даних та перевіряти їх, на видалення даних та не давати компанії надалі збирати персональні дані дітей¹⁰⁵.

Розділ 230 Акту про комунікації

На початку 1990-х років ряд онлайн-платформ почали створювати перші правила модерації контенту задля формування середовища, яке було б безпечним для сімейного перегляду. З цією метою адміністрації платформ видаляли незаконний або вульгарний контент (наприклад, порнографічні матеріали). Але цим вони наразили себе на небезпеку: в ряді судових позовів американські суди прирівняли діяльність адміністрацій цих платформ до кураторської відповідальності, яку, виявляють видавці чи дистриб'ютори, що фактично дозволяло притягати платформи до відповідальності за контент, створений користувачами.

В 1996 році до Акту про комунікації Конгресом було внесено правки, які були об'єднані під заголовком «Захист для «добро-самаритянського» блокування та перевірки образливих матеріалів» або «Розділ 230 Акту про комунікації»¹⁰⁶. Цей розділ знімав відповідальність з онлайн-платформ за контент, який публікували користувачі; за видалення контенту, який вважається непристойним, образливим, насильницьким тощо¹⁰⁷.

Акт про авторське право в цифрову епоху 1998

Даний акт містив положення щодо умовного імунітету онлайн-платформ у сфері авторського права, а саме: онлайн-сервіси, що надають доступ до захищеного авторським правом вмісту, мають «безпечну гавань», але з умовами впровадження функціональних процесів для отримання та виконання скарг від власників авторських прав.

¹⁰⁵ Children's Online Privacy Protection Act of 1998 (COPPA) (1998). <https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa>

¹⁰⁶ 47 U.S. Code § 230 – Protection for private blocking and screening of offensive material (1996). <https://www.law.cornell.edu/uscode/text/47/230>

¹⁰⁷ Balendra, S. (2024). Free Speech in the Puzzle of Content Regulation: Insights from the West and the Global South. Springer Nature Switzerland. C. 109

Також варто зазначити, що в Сполучених Штатах вже давно було розроблене комплексне антимонопольне законодавство (Акт Шермана 1890 року, Акт Клеймана 1914 року та Акт про створення Федеральної торгової комісії 1914 року). Однак через обраний американською владою підхід на невтручання та саморегулювання онлайн-платформ Федеральна торгова комісія, (далі - FTC) головним завданням якої є сприяння захисту прав споживачів та усунення і запобігання антиділових практик, таких як примусова монополія, не втручалася у сферу онлайн-платформ. Хоча FTC в 1990 році подала судовий позов проти корпорації Microsoft, звинувативши компанію в монополізації ринку веббраузерів¹⁰⁸.

Таким чином, в Сполучених штатах на федеральному рівні практично відсутня законодавча система для регулювання онлайн-платформ¹⁰⁹. Єдине, що стосувалося безпосередньо цієї сфери, це Розділ 230 Акту про комунікації, який наділяв онлайн-платформи як проміжні сервіси імунітетом від відповідальності за публікації користувачів, та Акт про захист конфіденційності дітей онлайн, який стосується зобов'язань онлайн-платформ у досить вузькій сфері.

2. Зміни у відношенні до регулювання онлайн-платформ після 2016 року

Протягом 2000-х років онлайн-платформи продовжували користуватися лояльністю американської влади. Під час президентства Джорджа Буша Молодшого при його адміністрації була створена Консультативна рада з інформаційних технологій, куди увійшли представники великих фірм, що займаються програмним забезпеченням і обладнанням. При президентстві Барака Обами Державний департамент та його держсекретарка Хіллари Клінтон активно просували «свободу в інтернеті» на міжнародній арені та повістку «Державного управління двадцять першого століття», яка закликала до збільшення глобального доступу не тільки до інтернету загалом, а й до пошукових двигунів, соціальних

¹⁰⁸ Gorwa, R. (2024). The Politics of Platform Regulation: How Governments Shape Online Content Moderation. Oxford University Press. C. 32

¹⁰⁹ Jamison, S. G. (2019). Creating a National Data Privacy Law for the United States. Intellectual Property Law Review, 10(1). <https://open.mitchellhamline.edu/cgi/viewcontent.cgi?article=1089&context=cybaris> C. 3

мереж тощо, розроблених американськими ІТ корпораціями. Також компанії власники онлайн-платформ були залучені в розробку цієї повістки та інших політик Державного департаменту в цій сфері¹¹⁰.

Переломним моментом у зміні відношення до регулювання онлайн-платформ американською владою можна вважати період президентства республіканця Дональда Трампа (2017-2021). Трамп є активним користувачем соціальних мереж (зокрема Twitter/X), які дозволяли досягати своєї аудиторії. Його початкова позиція до онлайн-платформ була лояльною, що можна було помітити у випадку, коли французький президент Макрон пропонував ввести податок на цифрові сервіси на території ЄС. Дональд Трамп погрожував введенням високих мит на французькі предмети розкоші¹¹¹. Однак під кінець президентства його позиція (а також консервативно-республіканських правих сил) змінилася на ворожу щодо платформ, оскільки, на його думку, вони почали заважати йому досягати своєї аудиторії. Яскравим прикладом буде ситуація, коли в травні 2020 року під виборчої кампанії Твіттер почав маркувати пости Трампа, в яких він зазначав, що під голосування поштою мала місце фальсифікація голосів, приписами, що звинувачення є не обґрунтованими¹¹². Після цього президент Трамп видав указ «Щодо запобігання онлайн цензури», де вказувалося, що онлайн-платформи перешкоджають реалізації права на свободу вираження¹¹³. Наказ був спрямований на звуження застосування Розділу 230: в указі зазначалося, що соціальні мережі використовують цю поправку як засіб боротьби з думками та позиціями, з якими вони не згодні, а тому вони не мають права користуватися захистом, передбаченим Розділом 230. Для реалізації указу Національна адміністрація з телекомунікацій та інформації мала подати

¹¹⁰ Gorwa, R. (2024). The Politics of Platform Regulation: How Governments Shape Online Content Moderation. Oxford University Press. С.116

¹¹¹ BBC. (2019). Trump threatens tariffs against "foolish" Macron. <https://www.bbc.com/news/world-us-canada-49131301>

¹¹² BBC. (2020). Twitter tags Trump tweet with fact-checking warning. <https://www.bbc.com/news/technology-52815552>

¹¹³ The White House Archives. (2020). Executive Order on Preventing Online Censorship. <https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-preventing-online-censorship/>

петицію Федеральній комісії з комунікацій з вимогою розтлумачити положення Розділу 230.

Іншою підставою обурення для правих сил було блокування акаунту Дональда Трампа в соціальних мережах Twitter та Facebook у зв'язку з захопленням Капітолія прихильниками Трампа в січні 2021 року. В цей час Дональд Трамп виклав відео в цих соціальних мережах, де виправдовував дії своїх прихильників (захоплення відбулося через переконання, що президентські вибори в США 2020 року були сфальсифіковані). Twitter та Facebook спочатку додали примітки до постів Трампа, а згодом видали їх та призупинили дію його акаунтів¹¹⁴.

З іншого боку, були підстави для обурення діяльністю онлайн-платформ у прихильників Демократичної партії. Але якщо республіканці дотримувалися думки, що онлайн-платформи своєю модерацією та боротьбою з дезінформацією посягають на свободу вираження думок, то демократи вважали, що адміністрації онлайн-платформ навпаки прикладали недостатньо зусиль для запобігання дезінформації на власних платформах. Оскільки вони вважали, що завдяки дезінформації американських виборців Дональд Трамп зумів перемогти на президентських виборах 2016 року, до цього не маючи значного досвіду у великій політиці та не займаючи жодної державної посади.

Для боротьби з онлайн-платформами й республіканець Дональд Трамп, і наступний президент-демократ Джо Байден вирішили залучити Федеральну торгову комісію (далі - FTC), яка до цього ігнорувала сферу онлайн-платформ. Під кінець президентства Трампа керівник комісії Джо Сіммонс зайнявся формуванням технологічного відділу комісії, який би займався питаннями технічної політики. В кінці 2020 року FTC оголосила про подання судового позову проти компанії Facebook, вимагаючи диверсифікації активів, зокрема Whatsapp та Instagram, припинити накладати антиконкурентні умови на виробників програмного забезпечення тощо¹¹⁵. Наступний президент Джо Байден призначив на посаду

¹¹⁴ Al Jazeera. (2021). Which online platforms banned Trump over Capitol riot? <https://www.aljazeera.com/news/2021/1/14/which-online-platforms-banned-trump-over-capitol-riot>

¹¹⁵ FTC. (2024a). Facebook, Inc., FTC v. <https://www.ftc.gov/legal-library/browse/cases-proceedings/191-0134-facebook-inc-ftc-v>

комісії Ліну Хан, яка мала намір продовжити боротьбу з монополіями у сфері онлайн-платформ. Так у 2022 році комісія подала позов проти корпорації Microsoft, щоб заблокувати придбання нею ігрового видавця, корпорації Activision Blizzard¹¹⁶. У 2023 році FTC подала судовий позов проти корпорації Amazon, звинувативши її в незаконній монополізації сфери онлайн роздрібної торгівлі¹¹⁷.

3. Спроби законодавчого врегулювання діяльності онлайн-платформ на рівні штатів

На рівні штатів ситуація відрізняється. У 2018 році в Каліфорнії був прийнятий Акт про приватність споживачів¹¹⁸, який у 2020 році був доповнений Актом про права приватності. Оскільки цей не належить до федерального законодавства, а є складовою частиною каліфорнійської законодавчої бази, то він застосовується до бізнесів, під чим розуміється будь-яка фізична особа підприємець, або юридична особа, яка працює з метою отримання прибутку чи фінансової вигоди та яка збирає особисту інформацію споживачів і здійснює свою підприємницьку діяльність в штаті Каліфорнія. Відповідно «споживачем» у розумінні даного закону будуть вважатися виключно фізичні особи, які мають місце проживання в штаті Каліфорнія. Акт застосовується як до діяльності офлайн, так і онлайн.

Варто зазначити, що даний документ не застосовується до будь-якого бізнесу, а лише до тих, які відповідають одному або декільком критеріям, а саме:

1. Річний дохід становить 25000000 доларів США;
2. Щорічно продає, купує або ділиться особистими даними більше ніж 100000 споживачів або домашніх господарств;

¹¹⁶ FTC. (2024b). Microsoft/Activision Blizzard, In the Matter of. <https://www.ftc.gov/legal-library/browse/cases-proceedings/2210077-microsoftactivision-blizzard-matter>

¹¹⁷ FTC. (2023). FTC Sues Amazon for Illegally Maintaining Monopoly Power. <https://www.ftc.gov/news-events/news/press-releases/2023/09/ftc-sues-amazon-illegally-maintaining-monopoly-power>

¹¹⁸ California Consumer Privacy Act of 2018. (2018). https://cpra.ca.gov/regulations/pdf/ccpa_statute.pdf

3. Як мінімум 50% щорічного доходу походить від продажу або поширення особистих даних.

Хоча акт також допускає, що будь-яка особа, яка займається підприємницькою діяльністю в Каліфорнії може добровільно підтвердити свою відповідність цьому акту.

Загалом, можна підсумувати, що акт застосовується до будь-якого бізнесу, який здійснює свою діяльність (офлайн або онлайн) на території штату Каліфорнія, є прибутковою організацією, збирає особисті дані споживачів і також відповідає хоча б одному з трьох вище зазначених критеріїв. Таким чином, можна сказати, що цей акт зокрема спрямований на регулювання великих комерційних та інших онлайн-платформ.

Що ж до обсягу персональної інформації, яка захищається актом, то до неї відноситься:

- Інформація, яка ідентифікує особу (справжнє ім'я, поштова адреса, ідентифікаційний код, номер водійського посвідчення, номер соціального страхування, адреса електронної пошти, номер банківського рахунку тощо);
- Біометричні дані особи;
- Комерційна інформація (дані про власність особи, про придбані товари та послуги тощо);
- Інформація про активності в інтернеті або інших цифрових мережах (історія пошуку в браузері, історія взаємодії з цифровими застосунками та рекламою тощо);
- Геолокаційні дані;
- Інформація пов'язана з працевлаштуванням, з освітою;
- Чутлива особиста інформація;
- Висновки, зроблені на основі будь-якої вище вказаної інформації, що дозволяють визначити профіль споживача, який відображає його вподобання, психологічні характеристики, схильності, поведінку, соціальні відносини, розумові здібності тощо.

На суб'єктів акт покладає такі основні зобов'язання:

- Необхідність інформувати споживачів про те, які категорії даних з них збираються, використовуються або продаються та з якою ціллю і метою;
- Забороняється збирати додаткові категорії інформації, що не виправдовується ціллю та метою збору;
- Необхідність інформувати про період часу протягом якого будуть використовуватися дані споживачів;
- Збір, використання та продаж особистих даних споживачів мають бути обґрунтовано необхідними та виправданими для досягнення мети.

Акт про приватність споживачів гарантує споживачам наступні права стосовно своїх персональних даних:

- Право на видалення зібраної платформою особистої інформації споживача за його запитом;
- Право на виправлення особистої інформації у випадку виявлення неточностей та помилок;
- Право знати яку персональну інформацію платформа збирає та право мати доступ до персональної інформації, яку збирила платформа;
- Право знати яку персональну інформацію платформа продає або ділиться та з ким;
- Право не допускати продаж або передачу персональної інформації платформою третій стороні за запитом;
- Право на обмеження використання чутливої особистої інформації за запитом;
- Право на недопущення дискримінації;

Споживач не повинен зазнавати дискримінації з боку суб'єкта у випадку застосування ним одного з вище зазначених прав, що може проявлятися в: ненаданні товарів чи послуг, в стягненні відмінної від вказаної плати за товари або послуги, в гіршому рівні якості товарів тощо.

Актом також передбачається створення органу контролю – Агентства з захисту приватності Каліфорнії (California Privacy Protection Agency), діяльність якого спрямована на застосування та контроль за виконанням положень Акту про приватність, захистом та просуванням права на приватність фізичних осіб та інших похідних прав, які зазначені в цьому акті. На Агентство покладаються такі обов'язки як:

- Проведення консультацій з суб'єктами, які підпадають під дію цього акту, для роз'яснення їх обов'язків та відповідальності у сфері захисту персональних даних;
- Проведення консультацій з каліфорнійськими споживачами для роз'яснення їхніх прав, гарантованих цим актом;
- Надання технічної та консультаційної допомоги законодавчим органам штату за запитом стосовно законодавства, пов'язаного з захистом персональних даних;
- Співробітництво з іншими агентствами та органами, чия діяльність пов'язана із захистом приватності або обробкою персональних даних у Каліфорнії, інших штатах, на федеральному рівні.

Агентство наділяється повноваженнями з розслідування можливих випадків порушення положень акту, вчинених вище вказаними суб'єктами. Розслідування може розпочиналися як за власною ініціативою органу, так і за скаргами фізичних осіб. Агентство може припинити розслідування, якщо було доведено відсутність доказів існування порушення або якщо суб'єкт добровільно повідомляє про факт порушення та вчиняє дії по його припиненню. В такому випадку воно може дати суб'єкту час на ліквідацію порушення та його наслідків. Також, до того як зробити будь-які висновки стосовно існування факту порушення Агентство має повідомити суб'єкта за допомогою електронного листа про розслідування та надати докази існування порушення, якими воно володіє, і запросити надати Агентству свою позицію та можливі докази щодо відсутності порушення. В процесі розслідування Агентство може допитувати свідків. Далі Агентство проводить слухання з представниками суб'єкту, який підозрюється у вчиненні порушення, за

результатами якого Агентство може визнати факт відсутності порушення або визнати суб'єкта винним та накласти на нього штраф.

Для фізичних осіб цей спосіб захисту своїх прав не є єдиним. Акт також гарантує можливість звернення до суду з цивільним позовом до суб'єкта, який порушив права особи у сфері захисту персональних даних.

Окрім того, для каліфорнійських споживачів передбачається інший механізм захисту порушених прав. Якщо до персональних даних споживачів здійснюється несанкціонований доступ, що стався внаслідок незабезпечення суб'єктом належного рівня захисту та безпеки, споживач може звернутися з цивільним позовом проти цього суб'єкта. Споживачі можуть стягнути збитки, якщо вони є більшими ніж 100 доларів США, але не перевищують 750 доларів США на споживача; вимагати судову заборону або декларативне рішення; інші вимоги, які буду визнані судом відповідними.

Що ж до відповідальності, то Актом передбачається накладення адміністративного штрафу розміром до 2500 доларів США за ненавмисне порушення, що стосується персональних даних неповнолітніх осіб та до 7500 доларів США за вмисне порушення в цій сфері.

Окрім вище згаданих штатів подібні закони про захист приватності споживачів вступили в дію у Вірджинії - 1 січня 2023 року; у Колорадо - 1 липня 2023 року; в Юті - 31 березня 2023 року; Коннектикуті - 1 липня 2023 року, в Орегоні, Техасі, Флориді - 1 липня 2024 року; в Монтані – 1 жовтня 2024 року; в Айові, Делавері, Небрасці, Нью Гемпширі - 1 січня 2025 року; у Нью-Джерсі – 15 січня 2025 року. Також такі закони були прийняті, але ще не набрали чинності, в Індіані, Монтані, Теннессі, Кентуккі, Мериленді, Міннесоті, Небрасці, Род Айленді. Отже, можна підсумувати, що приблизно третина американських штатів прийняла власні закони для захисту приватності споживачів, зокрема у цифровій сфері¹¹⁹.

¹¹⁹ Bloomberg Law. (2024). Which States Have Consumer Data Privacy Laws? <https://pro.bloomberglaw.com/insights/privacy/state-privacy-legislation-tracker/#map-of-state-privacy-laws>

Також варто згадати спроби губернаторів штатів Флорида та Техас, які були представниками республіканської партії, внести в парламенти штатів законопроекти про заборону цензури на онлайн-платформах. У Флориді законопроект містив положення про обов'язок онлайн-платформ за 30 днів повідомляти про зміни до правил користування платформою, користувацької угоди тощо, а також заборонялося видаляти облікові записи або займатися «деплатформуванням» кандидатів на політичні посади. Схожі положення містилися і в законопроекті, запропонованим губернатором Техасу, а саме «Інтерактивна комп'ютерна служба не може цензурувати користувача, висловлювання користувача або здатність користувача сприймати вирази іншої особи на основі: (1) погляду користувача або іншої особи; [або] (2) погляду, представленої у висловлюванні користувача або висловлюванні іншої особи»¹²⁰.

Висновки. Отже, можна підсумувати, що в США з 2016 року почав відбуватися період переосмислення наявного ліберального підходу до регулювання онлайн-платформ, що виразився як в прийнятті нових законів щодо регулювання онлайн-платформ, так і наділенні відповідних федеральних урядових агентств повноваженнями розслідувати порушення, які були скоєні адміністраціями або власниками онлайн-платформ. Хоча на федеральному рівні законодавчий процес загальмований через суперечності між демократами та республіканцями, але на рівні окремих штатів законодавчі органи змогли частково подолати проблему відсутності комплексного федерального законодавства у сфері регулювання онлайн-платформ, приймаючи власні закони у сфері регулювання онлайн-платформ, однак цей підхід має суттєвий недолік – відсутність уніфікації: всі зазначені штати приймали закони, які за своєю сутністю та структурою є схожими до акту, прийнятого в Каліфорнії (який, своєю чергою, орієнтується на Загальний регламент про захист даних ЄС (General Data Protection Regulation, GDPR)), але кожен з них містить різні критерії до визначення суб'єктів регулювання, відмінності у визначенні поняття «споживач», різний зміст і перелік прав

¹²⁰ Gorwa, R. (2024). The Politics of Platform Regulation: How Governments Shape Online Content Moderation. Oxford University Press.

споживачів, а також різні механізми притягнення до відповідальності. Таким чином, все це ускладнює можливості онлайн-платформ дотримуватися законодавства про приватність і підвищує витрати на юридичне забезпечення їхньої діяльності.

З іншого боку, за відсутності відповідного закону на федеральному рівні, прийняття та введення в дію закону про приватність даних є єдиним способом на цей момент гарантувати захист прав осіб щодо їхніх даних, які обробляються онлайн-платформами або іншими суб'єктами, які підпадають під дію таких законів. Крім того, зі зростанням кількості штатів, які приймають закони про приватність даних, виникає ймовірність, що це спонукатиме федеральних законодавців до створення єдиного закону на федеральному рівні з метою уніфікації законодавства. Також варто зазначити, що важливим кроком є активізація американської адміністрації, зокрема FTC, у розслідуванні порушень антимонопольного законодавства з боку великих ІТ-компаній.

Однак прийняття законів на рівні штатів, заснованих на GDPR, не є достатнім. Для забезпечення комплексного регулювання та для подолання проблем американського підходу необхідним є залучення найкращих практик європейського та китайського досвіду: зокрема, на федеральному рівні мають бути прийняті закони, подібні, наприклад, до європейських Акту про цифрові ринки (Digital Markets Act) та Акту про цифрові послуги (Digital Services Act). Ці закони мають встановлювати для онлайн-платформ вимоги як у сфері антимонопольного регулювання, так і в питаннях боротьби з незаконним контентом. Серед таких вимог: забезпечення можливості користувачам оскаржувати рішення платформ щодо них, створення механізмів оцінки ризиків, проведення регулярних перевірок, складання звітів та впровадження додаткових заходів для підвищення прозорості та відповідальності платформ. Це дозволить забезпечити більш ефективний захист інтересів користувачів і справедливу конкуренцію на ринку цифрових послуг.

Дана проблематика продовжуватиме бути актуальною через зростаючу роль онлайн-платформ в суспільних відносинах, монополізацію ринку цифрових платформ, проблеми захисту приватності та даних користувачів, боротьбу з

дезінформацією тощо, а тому потребує подальших досліджень, зокрема в таких напрямках як порівняльний аналіз ефективності різних моделей регулювання онлайн-платформ (США, КНР, ЄС тощо), роль антимонопольного регулювання в діяльності онлайн-платформ, розвиток законодавства у сфері приватності даних, протистояння саморегулювання та державного втручання, моделі вирішення конфліктів між керівництвами онлайн-платформ та урядами держав тощо.

2.3 Європейський підхід до регулювання онлайн-платформ

Зі створенням Інтернету та формуванням перших онлайн платформ на території Сполучених Штатів сформувалася і перша доктрина щодо підходу до регулювання інтернет середовища та онлайн платформ, що виражалася у запереченні права держави регулювати діяльність онлайн платформи та інтернет середовище взагалі, підтримці абсолютної свободи слова та саморегулюванні онлайн платформ. Ця доктрина просувалася візіонерами Інтернету, які розглядали його як альтернативу реальному світу, вільну від регуляторного впливу держав, де повинна домінувати свобода слова та вираження думок. Що ж до онлайн платформ, то необхідність відсутності регулювання їхньої діяльності пояснювалася тим, що наявність державного регулювання негативно вплинуло б на розвиток інновацій в цій сфері. Згодом ця позиція отримала підтримку і від американської влади, таким чином закріпивши цю доктрину невтручання на державному рівні.

Згодом американський підхід до регулювання онлайн платформ поширився і на територію Європейського союзу, де вплинув на положення Директиви про електронну комерцію, яка готувалася. Підхід, якого дотримувалася Європейська Комісія був гнучким. Пояснення цьому подвійне: по-перше, зважаючи на ранню стадію розвитку, було б нерозумно обтяжувати Інтернет громіздким

законодавством. По-друге, було важливо регулювати лише те, що дійсно необхідно в інтересах Єдиного ринку, поважаючи суверенітет держав-членів¹²¹.

Директива про електронну комерцію встановлює ряд важливих положень¹²²:

1) Забезпечення державою-членом відповідності положенням національного законодавства інформаційних послуг, які надаються постачальниками інформаційних послуг.

2) Держави-члени не повинні обмежувати надання інформаційних послуг постачальниками з інших держав-членів за винятком якщо це необхідно для запобігання, розслідування, затримання та переслідування злочинців; захисту здоров'я громадян; державної безпеки, в тому числі забезпечення національної безпеки та оборони тощо.

3) Зобов'язання для постачальників послуг надавати загальну інформацію про себе (ім'я постачальника послуг, його географічна адреса, електронна пошта тощо).

4) Комерційні повідомлення та рекламні оголошення мають бути чітко ідентифіковані як такі, однозначними та чіткими; фізична або юридична особа, яка його замовила, має бути чітко ідентифікована.

5) Вимога до правових систем держав-членів передбачити створення правового режиму регулювання укладання контрактів за допомогою електронних засобів.

6) Постачальники інформаційних послуг звільнюються від відповідальності за передачу інформації в рамках мережі зв'язку за умов, що вони не є ініціаторами передачі, не обирають одержувача передачі та не змінюють інформацію, яка міститься в передачі.

¹²¹ Fratangelo, Pierpaolo, 2001. "The E-Commerce Directive: first evaluations," MPRA Paper 5543, University Library of Munich, Germany. С. 3

¹²² Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'). <https://eur-lex.europa.eu/eli/dir/2000/31/oj/eng>

7) Постачальники інформаційних послуг, які надають послуги «кешування», які охоплюють не тільки передачу інформації, але і її тимчасове проміжне зберігання, звільняються від відповідальності за умов, що вони не змінюють відповідну інформацію, задовольняють умови щодо доступу до інформації та правила щодо оновлення інформації не перешкоджають законному використанню технологій, при отриманні даних про використання інформації тощо.

8) Постачальники інформаційних послуг, які надають послуги «хостингу», які включають в себе і зберігання інформації, що передається, звільняються від відповідальності за умов якщо постачальники не знають про незаконний характер відповідної інформації або у випадку обізнаності вдається до швидких дій щодо обмеження доступу до відповідної інформації одержувачем послуг.

9) Директива не встановлює загального обов'язку для постачальників інформаційних послуг займатися моніторингом інформації, яку вони передають, та займатися пошуком фактів незаконної діяльності. Лише за запитом компетентних національних органів.

10) Заохочення створеннями об'єднаннями постачальниками інформаційних послуг кодексів поведінки.

11) Забезпечення вирішення спорів між постачальниками та одержувачами інформаційних послуг як судовим шляхом, так і позасудовими способами.

Таким чином, Директива про електронну комерцію, хоч і мала певні положення, що стосувалися онлайн платформ, однак більшість з них стосувалася виключно забезпечення звільнення платформ від відповідальності щодо незаконних дій їхніх користувачів, а також гарантувалося саморегулювання онлайн платформ.

З подальшим розвитком Інтернету, розвитком самих онлайн платформ та збільшенням кількості інтернет користувачів і як наслідок зростанням кількості

злочинів в цифровому середовищі стало зрозуміло американська доктрина потребує вдосконалення. Таким чином певні питання щодо окремих аспектів регулювання онлайн платформ та захисту прав інтернет користувачів були висвітлені в положення ряду нормативно-правових актів ЄС, а саме:

- Директива 2011/92/ЄС про боротьбу з сексуальним насильством і сексуальною експлуатацією дітей та дитячою порнографією
- Директива 2017/541 про боротьбу з тероризмом
- Директива 2018/1808 про аудіовізуальні медіа сервіси
- Загального регламенту про захист персональних даних

Директива 2011/92/ЄС про боротьбу з сексуальним насильством і сексуальною експлуатацією дітей та дитячою порнографією встановлює певні зобов'язання на веб-сайти. Згідно зі статтею 25 держави-члени зобов'язані приймати міри по видаленню веб-сторінок, на яких міститься або поширюється дитяча порнографія, які знаходяться як на території держав-членів, так і за їх межами. В якості альтернативи можливе блокування доступу до цих веб-сторінок для власних інтернет користувачів¹²³.

Директива 2017/541 про боротьбу з тероризмом встановлює, що держави-члени повинні приймати міри по притягненню до кримінальної відповідальності за поширення онлайн або офлайн публічних повідомлень, в яких присутня глорифікація тероризму, виправдання терористичних актів тощо. Згідно зі статтею 21 держави-члени зобов'язані приймати міри по видаленню онлайн контенту, в якому присутні заклики до вчинення терористичних актів, який знаходиться на їхній території, та в якості альтернативи блокувати доступ до цього контенту для інтернет користувачів на своїй території¹²⁴.

¹²³ Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on the assessment of the effects of certain public and private projects on the environment (codification). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32011L0092>

¹²⁴ Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA <https://eur-lex.europa.eu/eli/dir/2017/541/oj/eng>

Директива 2018/1808 про аудіовізуальні медіа сервіси встановлює вимоги до контенту аудіовізуальних медіа сервісів, а саме аудіовізуальні комерційні повідомлення на цих платформах повинні бути чітко зрозумілими, забороняється використання сублімативних технік, не допускається присутність елементів, які містять зневагу до людської гідності, спонукають до поведінки, яка загрожує здоров'ю та безпеці, навколишньому середовищу, рекламу сигарет, інших тютюнових виробів та електронних сигарет, реклама алкогольних напоїв не має бути спрямована на неповнолітніх, не мають спричиняти фізичної, психічної або моральної шкоди, не мають містити заклики до дискримінації расової, етнічної, релігійної, на основі інвалідності тощо¹²⁵.

Загальний регламент про захист персональних даних є ключовим щодо захисту персональних даних користувачів онлайн платформ на території ЄС¹²⁶. Під поняття «персональні дані» згідно з цим регламентом відносяться будь-які дані за допомогою яких можна ідентифікувати особу, а саме виділяються такі категорії як: ім'я особи, ідентифікаційний номер та онлайн ідентифікатор, інформація про психічний та фізичний стан особи, економічне та соціальне становище тощо. Також регламентом окреслюється поняття обробки персональних даних, під що підпадають такі процеси як збір, записування, зберігання, змінення, розкриття, а також видалення оброблюваних персональних даних. Положення Загального регламенту про захист персональних даних спрямовані на захист прав користувачів від свавілля онлайн платформ при обробці їхніх персональних даних.

Регламентом визначаються дві основні категорії суб'єктів, які залучені до діяльності з обробки персональних даних користувачів, в саме контролери та

¹²⁵ Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities. <https://eur-lex.europa.eu/eli/dir/2018/1808/oj/eng>

¹²⁶ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng>

процесори (обробники). Перша категорія відповідальна за визначення мети обробки персональних даних користувачів та засобів за допомогою яких, вона буде здійснюватися. Обробники ж безпосередньо здійснюють обробку персональних даних користувачів згідно з вимогами, встановленими контролерами.

Ключовою вимогою до законності обробки персональних даних є необхідність отримання згоди на обробку персональних даних від їхнього власника, яка має бути чіткою та зрозумілою. Для дітей віком до 16 років обробка персональних даних допускається лише випадку надання згоди з боку їхніх законних представників (батьків або опікунів). Також згода на обробку персональних даних може не вимагатися, якщо контролер доведе, що оброблювані не дозволяють ідентифікувати особу, якій вони належать.

Регламент гарантує наступні права користувачів:

- 1) Право користувача на доступ, яке передбачає, що онлайн платформа має підтвердити факт обробки персональних даних за запитом користувача та надати копію оброблюваних даних;
- 2) Право на виправлення, яке надає користувачу можливість виправити неточності в персональних даних, які були передані онлайн платформі;
- 3) Право на забуття, яке дозволяє користувачу вимагати від онлайн платформи стерти персональні дані, а також якщо немає більше потреби в опрацюванні даних чи користувач відкликав згоду на обробку персональних даних;
- 4) Право на обмеження, яке дозволяє користувачу обмежити обробку персональних даних у випадку, якщо користувач оспорує точність персональних даних, обробка є незаконною тощо;
- 5) Право на мобільність даних, яке дає можливість користувачу отримати від онлайн платформи персональні дані в структурованому, загальноприйнятому форматі, які користувач може передати іншій онлайн платформі;

6) Право на заперечення, яке передбачає, що користувач має право заперечити проти обробки персональних даних з боку онлайн платформи з певних підстав.

Також регламентом встановлюється ряд вимог щодо забезпечення безпеки персональних даних користувачів, а саме:

Під час обробки персональних даних повинна забезпечуватися їхня псевдонімізація та шифрування; відновлення даних у випадку технічної несправності або знищення даних

У випадку взлому особистих даних обробник має повідомити контролера про інцидент, в контролер у свою чергу зобов'язаний повідомити про це власника персональних даних;

Необхідність проводити систематичні перевірки з оцінки захисту персональних даних користувачів;

Регламент Р2В регулює відносини між комерційними онлайн платформами та бізнес користувачами. Для позначення комерційних онлайн платформ у даному регламенті використовується термін «сервіс онлайн-посередництва», під яким розуміється онлайн платформи, яка надає можливість бізнес користувачам пропонувати товари або послуги споживачам та сприяє здійсненню транзакцій між споживачами та бізнес користувачами¹²⁷.

Для даних онлайн платформ регламент встановлює наступні зобов'язання, а саме:

У випадку коли платформа збирається припинити або призупинити дію аккаунту бізнес користувача через продаж певних товарів або послуг, то попередньо вона має повідомити причину цього рішення.

На платформі повинна існувати система ранжування товарів та послуг

¹²⁷ Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services. <https://eur-lex.europa.eu/eli/reg/2019/1150/oj/eng>

У користувацькій угоді мають бути чітко вказані випадки, коли до певних товарів або послуг застосовується відношення ніж до більшості товарів та послуг

Створення системи подачі скарг

Створення системи медіації для вирішення спорів між бізнес користувачами

Однак згодом стало зрозуміло, що цифрова сфера потребує більш комплексного регулювання. Серед підстав можна виділити ситуацію, яка склалася навколо Facebook, а саме через підозри, що соціальна мережа використовувалася для виборчих маніпуляцій під кампанії Брекситу у Великій Британії 2016 року, кампанії по дезінформації перед президентськими виборами у Франції 2017 року, а також для поширення мови ненависті по відношенню до біженців у Німеччині¹²⁸.

У грудні 2019 року з'явилася інформація, що ЄК вважає Директиву про електронну комерцію «застарілою» і її потрібно замінити більш повним комплексом правил для цифрових послуг¹²⁹.

16 грудня 2020 року ЄК був запропонований Пакет Акту про цифрові послуги, який включав дві пропозиції: Акт про цифрові послуги (DSA) і Акт про цифрові ринки (DMA). За даними ЄК, ці законодавчі пропозиції мають дві цілі: просування основних прав у цифрових послугах та сприяння технологічним інноваціям шляхом встановлення загальних правил для постачальників цифрових послуг на єдиному європейському ринку та за його межами¹³⁰.

19 жовтня 2022 року було прийнято Акт про цифрові послуги (DSA)¹³¹. Положення Акту про цифрові послуги зосереджені на просуванні прозорого та безпечного онлайн-середовища та встановлюють підзвітність усіх постачальників

¹²⁸ Heldt, Amélie P. (2020) "Merging the Social and the Public: How Social Media Platforms Could Be a New Public Forum," Mitchell Hamline Law Review: Vol. 46: Iss. 5, Article 1. C. 1026

¹²⁹ Fanta A., Rudl T. (2019). Leaked document: EU Commission mulls new law to regulate online platform. <https://netzpolitik.org/2019/leaked-document-eu-commission-mulls-new-law-to-regulate-online-platforms/>

¹³⁰ CAUFFMAN C, GOANTA C. A New Order: The Digital Services Act and Consumer Protection. European Journal of Risk Regulation. 2021;12(4):758-774. doi:10.1017/err.2021.8 C. 1

¹³¹ Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) <https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng>

цифрових послуг¹³². Загалом Акт про цифрові послуги покладає зобов'язання на проміжні сервіси, яке є аналогом поняття постачальників інформаційних послуг з Директиви про електронну комерцію. Це поняття охоплює такі види: сервіси простої передачі даних, сервіси кешування та сервіси хостингу.

Під онлайн платформою розуміється сервіс хостингу, який за запитом одержувача послуги зберігає та поширює інформацію для громадськості; поняття пошукової онлайн системи, яке означає проміжний сервіс, який дозволяє користувачам вводити запити для виконання пошуку на всіх веб-сайтах або на всіх веб-сайтах певною мовою на основі запиту на будь-яку тему у формі ключове слово, голосовий запит, фразу чи інший вхід, і повертає результати в будь-якому форматі, у якому можна знайти інформацію, пов'язану із запитуваним вмістом.

Загалом зобов'язання, які Акт покладає на онлайн платформ можна розділити на чотири частини:

- зобов'язання, які стосуються всіх проміжних сервісів;
- зобов'язання, які стосуються сервісів хостингу;
- зобов'язання, які стосуються онлайн платформ;
- зобов'язання, які стосуються виключно дуже великих онлайн платформ та пошукових систем.

Одним з основних зобов'язань, яке стосується усіх проміжних сервісів є видалення незаконного контенту за наказом Координатора цифрових послуг. Також проміжний сервіс має проінформувати користувача про видалення та його причини. Питанням же виявлення незаконного контенту займаються відповідні державні органи, Акт не зобов'язує проміжні сервіси самостійно цим займатися. Наступним основним зобов'язанням є вимога надати конкретну інформацію про одного або кількох конкретних одержувачів послуги за наказом, виданим

¹³² Decarolis, Francesco and Li, Muxin, Regulating online search in the EU: From the android case to the digital markets act and digital services act (July 6, 2023). Available at SSRN: <https://ssrn.com/abstract=4660372> or <http://dx.doi.org/10.2139/ssrn.4660372> C. 5

відповідними національними судовими чи адміністративними органами на основі застосовного права Союзу або національного законодавства.

Також усі проміжні сервіси повинні включати інформацію про будь-які обмеження, які вони встановлюють щодо використання їхніх послуг, до своїх умов користування. Ця інформація включатиме інформацію про будь-які політики, процедури, заходи та інструменти, що використовуються з метою модерації вмісту. Інформація повинна бути однозначною та зрозумілою і при будь-яких істотних змінах умов провайдери проміжних сервісів мусять повідомляти користувачів про це. Це зобов'язання є вкрай важливими, оскільки воно спрямоване на боротьбу з тіньовим баном. Цей термін стосувався оманливого призупинення облікового запису на веб-форумах: для заблокованого користувача створювалося враження, що він усе ще може публікувати повідомлення, тоді як насправді його вміст більше не бачили інші користувачі. Також під тіньовим баном розуміється альтернативні засоби правового захисту, особливо засобів видимості, таких як видалення зі списку та пониження рейтингу. Ці засоби правового захисту не повністю припиняють доступ до вмісту, а натомість роблять цей вміст менш видимим за допомогою функцій виявлення, таких як пошук і рекомендації¹³³.

Наступна категорія стосується сервісів хостингу. Щодо них варто наступні зобов'язання:

1. по-перше, від них вимагається запровадити механізми зворотнього зв'язку, які дозволять будь-якому користувачу повідомляти платформі про наявність у їхній системі інформації, які користувачі вважають незаконним вмістом;
2. по-друге, коли провайдери сервісів хостингу застосовують обмеження по відношенню до користувачів на підставі того, що інформація, яка передавалася користувачем, є незаконним вмістом або порушує

¹³³ Leerssen P (2023) An end to shadow banning? Transparency rights in the digital services act between content moderation and curation. *Computer Law & Security Review* 48: 105790. <https://www.sciencedirect.com/science/article/pii/S0267364923000018#section-cited-by> C. 2

положення та правила платформи, повинні надати чітке та конкретне пояснення даного обмеження;

3. по-третє, якщо провайдеру сервісу хостингу стає відома будь-яка інформація про кримінальне правопорушення, пов'язане із загрозою життю або безпеці особи або осіб, він мусить негайно повідомити правоохоронні органи та надати всю доступну інформацію.

Наступна категорія зобов'язань стосуються онлайн платформ. Онлайн-платформам забороняється створювати та управляти своїми онлайн-інтерфейсами таким чином, щоб вводити в оману користувачів або іншим чином негативно впливати на здатність прийняття рішень. Онлайн-платформи, які розміщують рекламу, повинні забезпечити можливість, щоб щодо будь-якого рекламного повідомлення користувачі могли ідентифікувати в чіткій формі, що ця інформація є носить рекламний характер, фізичну або юридичну особу, яка замовила та оплатила рекламне повідомлення, а також інформацію щодо параметрів яким чином визначається коло осіб, яким пропонується це рекламне повідомлення. Також онлайн-платформи, доступні для неповнолітніх, повинні запровадити заходи для забезпечення високого рівня конфіденційності та безпеки неповнолітніх у своїх послугах.

Остання категорія зобов'язань стосуються дуже великих онлайн-платформ та дуже великих пошукових онлайн-систем. Дуже великі онлайн-платформи (VLOP), є ті онлайн платформи, якими користуються понад 10% із 450 мільйонів споживачів у ЄС, до яких відносяться соціальні мережі, інтернет ринки, онлайн магазини додатків тощо; і до дуже великих онлайн-пошукових систем (VLOSE) відносяться ті, якими користуються понад 10% із 450 мільйонів споживачів у ЄС¹³⁴.

На дуже великі онлайн-платформи і дуже великі онлайн-пошукові системи покладаються найбільш серйозні зобов'язання. По-перше, вони повинні ретельно

¹³⁴ Наталія Мазаракі, Володимир Примаєк 'Механізм вирішення спорів між користувачами та онлайн-платформами в Акті ЄС про цифрові послуги' (2026) 19 Український політико-правовий дискурс <https://doi.org/10.5281/zenodo.18662891>

виявляти, аналізувати та оцінювати будь-які системні ризики, до яких відносяться: поширення незаконного контенту, будь-який фактичний або передбачуваний негативний вплив на громадський дискурс і виборчі процеси, а також громадську безпеку тощо, що впливають із дизайну чи функціонування їхнього сервісу та пов'язаних із ним систем. По-друге, провайдери дуже великих онлайн-платформ і дуже великих онлайн-пошукових систем підлягають, за власний рахунок і принаймні раз на рік, незалежному аудиту для оцінки відповідності. Також провайдери дуже великих онлайн-платформ або дуже великих онлайн-пошукових систем створюють незалежну службу з відповідності, яка повинна мати достатні повноваження для моніторингу дотримання провайдером Акту.

Також Актом про цифрові послуги надає певні можливості щодо саморегулювання в сфері онлайн платформ. По-перше, Єврокомісія заохочує та сприяє складанню добровільних кодексів поведінки на рівні Союзу для сприяння належному застосуванню цього Акту, беручи до уваги, зокрема, конкретні проблеми боротьби з різними типами незаконного контенту та системними ризиками, у відповідності до законодавства Союзу, зокрема щодо конкуренції та захисту персональних даних. Далі Комісія може запросити відповідних провайдерів дуже великих онлайн-платформ або дуже великих онлайн-пошукових систем, а також відповідні компетентні органи, організації громадянського суспільства та інші відповідні зацікавлені сторони брати участь у складанні кодексів поведінки щодо вжиття конкретних заходів із зменшення ризиків, а також системи регулярного звітування про будь-які вжиті заходи та їх результати.

Також разом з Актом про цифрові послуги було прийнято Акт про цифрові ринки¹³⁵, який спрямований на боротьбу з монополіями в цифровому секторі економіки ЄС та захист економічних прав користувачів. Акт визначає поняття «гейткіперів», під яким розуміються великі онлайн платформи, які мають значний вплив на цифровий ринок. Для гейткіперів встановлюються різні зобов'язань по

¹³⁵ Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) <https://eur-lex.europa.eu/eli/reg/2022/1925/oj/eng>

відношенню до своїх звичайних та бізнес користувачів. Акт забороняє онлайн платформам краще просувати свої продукти по відношенню до продуктів своїх бізнес користувачів, не надавати доступ до даних, які були створені при користуванні платформою, а також не дозволяти їм просувати свої продукти та заключати договори за межами платформи. Також встановлюються зобов'язання і щодо звичайних користувачів: відслідковувати користувачів за межами платформи для цільової реклами, використовувати особисті дані користувачів для цільової реклами без згоди, а також встановлювати користувачам програмне забезпечення без їх згоди та перешкоджати його видаленню.

Акт про цифрові послуги та Акт про цифрові ринки задля забезпечення дотримання онлайн платформами своїх положень встановлюють відповідальність у виді накладення штрафів. DSA передбачає стягнення грошової суми до 6% від світового річного обороту платформи у випадку недотримання зобов'язань. DMA в свою чергу передбачає стягнення грошової суми до 10% від світового річного обороту платформи, а випадку повторного порушення зобов'язань – до 20%.

Також в ЄС було прийнято комплексний акт з регулювання ШІ¹³⁶, який набрав сили 1 серпня 2024 року. Акт містить приклади моделей, які становлять неприйнятний ризик. Моделі, що підпадають під цю категорію, заборонені. Приклади включають використання віддаленої біометричної ідентифікації в режимі реального часу в громадських місцях або системи оцінювання соціальних балів, а також використання підсвідомих методів впливу, які використовують вразливі місця певних груп¹³⁷.

Моделі високого ризику дозволені, але вони повинні відповідати багатьом вимогам і пройти оцінку відповідності. Цю оцінку потрібно завершити до виходу

¹³⁶ What is the Artificial Intelligence Act of the European Union (EU AI Act)? <https://www.ibm.com/think/topics/eu-ai-act>

¹³⁷ Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng>

моделі на ринок. Ці моделі також мають бути зареєстровані в базі даних ЄС, яка буде створена. Експлуатація моделей штучного інтелекту з високим ступенем ризику вимагає відповідної системи управління ризиками, можливостей ведення журналів і людського нагляду відповідно до власності. До даних, які використовуються для навчання, тестування та перевірки, а також засобів контролю, що забезпечують кібербезпеку, надійність і справедливість моделі, має бути належне управління даними.

Прикладами систем високого ризику є моделі, пов'язані з функціонуванням критичної інфраструктури, системи, що використовуються в процесах найму чи рейтингу працівників, системи оцінки кредитоспроможності, автоматизована обробка страхових вимог або встановлення премій за ризик для клієнтів.

Решта моделей вважаються обмеженими або мінімальним ризиком. Для них потрібна прозорість, тобто користувач має бути проінформований про те, з чим він взаємодіє, створене ШІ. Приклади включають чат-ботів або діпфейки, які не вважаються високими ризиками, але для яких необхідно, щоб користувачі знали про те, що за цим стоїть ШІ.

Висновки до розділу 2

Отже можна підсумувати, що європейська правова система пройшла певний шлях від сприйняття та застосування американського підходу до регулювання онлайн платформ до формування власного підходу, який можна описати як правозахисний. На території Китаю так само як і в ЄС також спочатку сприйняли американську доктрину, але згодом теж від неї відійшли до повноцінного регулювання цифрової сфери. Однак в основі китайської доктрини стояла політична цензура з метою недопущення поширення ідей та думок, які суперечать офіційній ідеології Китайської комуністичної партії. В ЄС же були спроби досягти балансу між саморегулюванням та свободою слова з американської доктрини та державного контролю та цензури з китайської доктрини. Державний контроль також вбачався вимушеною мірою для забезпечення прав та свобод користувачів, які могли бути порушені онлайн платформами.

Таким чином, можна сформувати наступну періодизацію розвитку регулювання онлайн платформ у праві ЄС:

1) перший етап – етап повного саморегулювання. На цьому етапі правова система ЄС схилилася до американської доктрини регулювання онлайн платформ, яка спиралася на домінування свободи слова над іншими правами людини, невтручання у діяльність онлайн платформ та саморегулювання. Директива про електронну комерцію, хоч і мала певні положення, що стосувалися онлайн платформ, однак більшість з них стосувалася виключно забезпечення звільнення платформ від відповідальності щодо незаконних дій їхніх користувачів, а також гарантувалося саморегулювання онлайн платформ.

2) Другий етап – перехідний етап. На цьому етапі відбуваються перші кроки по відході від американської доктрини регулювання онлайн платформ та формуванню власного підходу до питання регулювання онлайн платформ, який був би спрямований головним на захисті прав користувачів платформ. Приймаються Директива 2011/92/ЄС про боротьбу з сексуальним насильством і сексуальною експлуатацією дітей та дитячою порнографією, Директива 2017/541 про боротьбу з тероризмом, Директива 2018/1808 про аудіовізуальні медіа сервіси. Ці нормативно-правові документи хоч і безпосередньо не стосувалися регулювання онлайн платформ, однак встановлювали певні вимоги до діяльності онлайн платформ, зокрема стосовно попередження злочинів та виявлення незаконного контенту. Також серед положень Загального регламенту про захист персональних даних були визначені права користувачів по використанню персональних прав, які мають гарантуватися онлайн платформами.

3) Третій етап – етап становлення європейської системи регулювання онлайн платформ. З прийняттям Пакету про цифрові послуги (Директиви про цифрові послуги та Директиви про цифрові ринки) було остаточно сформовано вигляд європейської правозахисної доктрини щодо

регулювання онлайн платформ. DSA зобов'язує надавачів цифрових послуг забезпечувати існування механізмів зворотнього зв'язку задля можливості оскарження рішень по обмеженню доступу користувача; вимагає чітко та зрозуміло прописувати в правилах платформи підстави обмеження доступу; забороняється застосування інтерфесів платформ, які можуть вводити користувачів в оману тощо. Від великих онлайн платформ вимагається проводити регулярні перевірки на виявлення системних ризиків. DMA в свою чергу зобов'язує забезпечувати справедливі умови для своїх бізнес користувачів (наприклад, не просувати краще свої продукти по відношенню до продуктів своїх бізнес користувачів), забороняється використовувати особисті дані користувачів для цільової реклами без їхньої згоди тощо.

РОЗДІЛ 3. РЕАЛІЗАЦІЯ МОДЕЛІ РЕГУЛЬОВАНОГО САМОРЕГУЛЮВАННЯ У DIGITAL SERVICES ACT

Метою цього розділу є визначення внутрішньої структури механізму регульованого саморегулювання та співрегулювання онлайн-платформ, закріпленого в DSA, а також оцінка його ефективності. Попередні частини дослідження з'ясували теоретико-правову природу саморегулювання онлайн-платформ та місце європейської моделі у порівняльній перспективі; цей розділ має прикладне нормативно-аналітичне значення: він показує, яким чином абстрактна ідея саморегулювання трансформується в конкретну систему правових обов'язків, процедур, інституційних зв'язків та механізмів контролю. DSA зберігає автономію онлайн-платформ у формуванні власних правил поведінки, модерації контенту, організації внутрішніх процедур та управлінні ризиками, водночас юридично впорядковуючи цю автономію — вбудовуючи її у багаторівневу систему публічно-правових вимог, процедурних гарантій, зовнішньої верифікації та колективних співрегуляторних інструментів. Тому DSA доцільно розглядати як складну конструкцію регульованого саморегулювання, у якій приватна нормотворчість і приватне правозастосування платформ поєднуються з публічним контролем, прозорістю, підзвітністю та врахуванням фундаментальних прав користувачів.

Методологічно розділ побудовано на поєднанні нормативно-догматичного, системно-структурного та функціонального підходів. Нормативно-догматичний підхід застосовується для аналізу змісту окремих статей DSA — їхніх адресатів, обсягу обов'язків, процедурних вимог та правових наслідків. Системно-структурний підхід дозволяє розглядати ці положення як взаємопов'язані елементи єдиної регуляторної архітектури. Функціональний підхід з'ясовує роль кожної статті в механізмі саморегулювання чи співрегулювання: юридичне впорядкування платформної нормотворчості, процедуризація приватного правозастосування, внутрішній самоконтроль, зовнішня верифікація, ризик-менеджмент або колективне вироблення стандартів. Оцінка ефективності механізмів здійснюється на основі першої правозастосовної практики ЄК та координаторів цифрових

послуг, аудиторських звітів і звітів про системні ризики, а також їхнього аналізу в доктрині.

Аналіз здійснюється за єдиною логікою: для кожної статті визначається її регуляторна функція та проблема, на вирішення якої вона спрямована; розкривається її зміст і механізм дії; враховуються релевантна судова практика, доктринальні підходи, матеріали ЄК, аудиторські та прозорісні звіти платформ; насамкінець визначається, який елемент регульованого саморегулювання або співрегулювання відповідна стаття втілює в загальній архітектурі DSA.

У межах розділу обґрунтовується триступенева модель. Перший рівень становить базовий процедурний рівень платформного саморегулювання, юридично впорядкований статтями 14, 16, 17, 20 і 21 DSA. Другий рівень охоплює посилений ризик-орієнтований режим для VLOPs/VLOSEs: статті 34, 35 і 41 як форма метарегулювання внутрішніх систем управління та статті 37, 40 і 42 як механізм зовнішньої верифікації та підзвітності. Третій рівень становлять співрегуляторні колективні інструменти, передбачені статтями 45–48 DSA. Окреме місце посідає стаття 22 щодо *trusted flaggers*, яка має проміжний характер, оскільки поєднує платформний механізм *notice-and-action* із залученням до платформного правозастосування зовнішніх суб'єктів, сертифікованих координатором цифрових послуг.

Завданням розділу, таким чином, є виявлення системного значення положень DSA для трансформації приватної автономії онлайн-платформ у юридично впорядковану, процедурно контрольовану та інституційно верифіковану модель регулювання цифрового середовища, а також встановлення проблем правозастосування та перспектив її розвитку у взаємодії із суміжними актами цифрового права ЄС.

3.1 Базовий процедурний рівень платформного саморегулювання

До базового процедурного рівня в цьому дослідженні віднесено статті 14, 16, 17, 20 і 21 DSA за трьома спільними ознаками. По-перше, за їхнім місцем у системі

Регламенту: ці положення не належать до спеціального посиленого режиму VLOPs/VLOSEs, а формують загальну процедурну основу належної поведінки провайдерів посередницьких послуг, хостинг-провайдерів та онлайн-платформ залежно від сфери застосування відповідної статті. Саме тому цей рівень є базовим, оскільки встановлює мінімальний стандарт юридичного впорядкування платформного саморегулювання.

По-друге, за предметом регуляторного впливу: ці статті не визначають наперед змісту платформних правил і не встановлюють загального переліку допустимого чи недопустимого контенту. Натомість вони впорядковують форму приватної нормотворчості платформи, насамперед через вимоги до умов користування за статтею 14, а також процедуру застосування цих правил — від отримання повідомлення про потенційно незаконний контент і прийняття рішення до його мотивування, внутрішнього оскарження та зовнішнього позасудового перегляду відповідно до статей 16, 17, 20 і 21 DSA. Саме тому цей рівень має процедурний характер.

По-третє, за функцією в моделі регульованого саморегулювання: у сукупності ці статті відтворюють повний цикл саморегулятивної діяльності онлайн-платформи, що охоплює нормотворчість, застосування правил і контроль за їх застосуванням. Водночас кожен із цих елементів підпорядковується публічно-правовим стандартам прозорості, передбачуваності, обґрунтованості, пропорційності та процедурної оскаржуваності.

3.1.1. Стаття 14 DSA: умови користування як приватна нормотворчість під публічним контролем

Регуляторна функція та передумови. Стаття 14 спрямована на вирішення проблеми непрозорості та непередбачуваної приватної нормотворчості платформ. Умови користування за юридичною формою є договорами приєднання: вони розробляються платформою односторонньо, пропонуються у стандартизованому вигляді й не підлягають індивідуальному узгодженню, а вибір користувача зводиться до прийняття умов у цілому або відмови від сервісу. Водночас суто

договірна кваліфікація не відображає фактичної функції цих актів: умови користування великих платформ адресовані сотням мільйонів осіб, визначають межі допустимої публічної комунікації, встановлюють санкції та процедури їх застосування, тобто виконують функцію, у матеріальному сенсі подібну до нормативного регулювання. У доктрині цей феномен описано як здійснення платформами де-факто врядувальних повноважень щодо онлайн-висловлювань: Klonick характеризує платформи як «нових управителів» публічного дискурсу, а Suzor підкреслює, що правила, за якими платформи здійснюють цю владу, тривалий час формувалися і застосовувалися поза будь-якими вимогами верховенства права¹³⁸.

До ухвалення DSA дефіцит прозорості платформних правил був предметом системної критики. Спеціальний доповідач ООН з питань свободи вираження поглядів констатував, що контентні стандарти платформ сформульовані настільки широко, що залишають компаніям недостатньо пояснену дискрецію, а користувачі, публічна влада і громадянське суспільство послідовно висловлюють незадоволення непередбачуваністю застосування умов користування¹³⁹. Класичний договірно-правовий захист виявився структурно неадекватним цій проблемі: судові оскарження умов вимагає послідовного вирішення питань вибору суду, застосовного права, тлумачення договору та його зіставлення з імперативними нормами, кожне з яких у транскордонному контексті пов'язане зі значною невизначеністю, а успішне рішення має силу лише *inter partes* і не змінює практики платформи¹⁴⁰. Під час публічних консультацій щодо DSA прозорість модерації була визнана пріоритетом практично всіма групами стейкхолдерів, а Комісія в

¹³⁸Kate Klonick, 'The New Governors: The People, Rules, and Processes Governing Online Speech' (2018) 131 Harvard Law Review 1598; Nicolas Suzor, *Lawless: The Secret Rules That Govern Our Digital Lives* (CUP 2019).

¹³⁹UNHRC, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression' (6 April 2018) UN Doc A/HRC/38/35, paras 24–27.

¹⁴⁰Milos Novovic, *The EU Digital Services Act (DSA): A Commentary* (Kluwer Law International 2024), commentary to art 14.

оцінці впливу кваліфікувала посилені вимоги прозорості як передумову ефективного засобу правового захисту¹⁴¹. Стаття 14 відповідає на цю проблему характерним для регульованого саморегулювання способом: вона зберігає договірний режим, накладаючи на нього публічно-правові вимоги до форми і застосування приватних правил. Свобода договору провайдерів при цьому в принципі поважається: саме провайдер визначає обсяг сервісу, категорії заборонених матеріалів і доступні користувачам засоби реагування¹⁴².

Зміст і механізм дії. Стаття 14 встановлює два рівні вимог. Перший — інформаційно-формальний (ст. 14(1)–(3), (5)–(6)): провайдери зобов'язані включати до умов користування відомості про будь-які обмеження щодо інформації, наданої користувачами, зокрема про політики, процедури, заходи та інструменти модерації контенту, включно з алгоритмічним ухваленням рішень і людською перевіркою, а також про правила внутрішньої системи розгляду скарг. Ця інформація має бути викладена чіткою, простою, зрозумілою, дружньою до користувача й однозначною мовою та бути публічно доступною в машиночитаному форматі. Провайдер повідомляє користувачів про будь-які суттєві зміни умов; якщо сервіс переважно спрямований на неповнолітніх або переважно використовується ними, умови мають бути пояснені у спосіб, зрозумілий неповнолітнім. Для дуже великих онлайн-платформ і пошукових систем встановлено посилений режим: стислий машиночитаний виклад умов та їх публікація офіційними мовами всіх держав-членів, у яких надається сервіс.

Другий рівень — стандарт застосування (ст. 14(4)): провайдери зобов'язані діяти сумлінно, об'єктивно і пропорційно при застосуванні та забезпеченні виконання встановлених ними обмежень, з належним урахуванням прав і законних інтересів усіх залучених сторін, включно з фундаментальними правами

¹⁴¹Commission, 'Impact Assessment Report Accompanying the Proposal for a Regulation on a Single Market for Digital Services' SWD(2020) 348 final.

¹⁴²Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services (Digital Services Act) [2022] OJ L277/1, recital 45.

користувачів, закріпленими Хартією. Якщо вимоги прозорості дисциплінують форму приватних правил, то ст. 14(4) дисциплінує їх застосування: платформа залишається вільною у визначенні змісту власних правил, однак втрачає свободу довільного їх застосування. Преамбула конкретизує стандарт: правила мають застосовуватися в однаковий, прозорий і передбачуваний спосіб, із надійними гарантіями прав та законних інтересів усіх зачеплених сторін¹⁴³.

Таким чином, ст. 14 виконує подвійну функцію: по-перше, вона юридично формалізує приватну нормотворчість платформи, вимагаючи зробити її правила видимими, зрозумілими й доступними; по-друге, вона встановлює стандарт правомірного застосування цих правил. Саме ця подвійність дозволяє розглядати ст. 14 як вихідний елемент базового процедурного рівня DSA: без прозорих умов користування неможливими стають ані ефективний notice-and-action за ст. 16, ані мотивування рішень за ст. 17, ані внутрішнє чи зовнішнє оскарження за статтями 20 і 21.

Судова практика, доктрина, практика застосування. Мовно-інформаційні вимоги ст. 14 продовжують усталені підходи права ЄС. Вимога простої і зрозумілої мови закріплена ще у ст. 5 Директиви 93/13/ЄЕС; Суд ЄС тлумачить її суворо: у справі *RWE Vertrieb* підкреслено фундаментальне значення переддоговірного інформування для здатності споживача передбачати наслідки договору¹⁴⁴, а у справі *Kásler* — що зрозумілість вимагає не лише граматичної доступності, а й деталізації, яка дозволяє на основі чітких критеріїв оцінити конкретні наслідки умови¹⁴⁵. Аналогічний стандарт закріплено у ст. 12(1) GDPR та розвинуто в настановах щодо прозорості Групи ст. 29¹⁴⁶. Отже, ст. 14 переносить

¹⁴³DSA, recital 52.

¹⁴⁴Case C-92/11 *RWE Vertrieb AG v Verbraucherzentrale Nordrhein-Westfalen eV* EU:C:2013:180, paras 44, 53.

¹⁴⁵Case C-26/13 *Kásler and Káslerné Rábai v OTP Jelzálogbank Zrt* EU:C:2014:282, para 75.

¹⁴⁶Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts [1993] OJ L95/29, art 5; Regulation (EU) 2016/679 (GDPR) [2016] OJ L119/1, art 12(1); Article 29 Working Party, 'Guidelines on Transparency under Regulation 2016/679' WP260 rev.01 (11 April 2018).

на платформні правила техніку, вже випробувану правом захисту споживачів і правом захисту даних, — що підтверджує тезу першого розділу: регульоване саморегулювання є усталеною технікою права ЄС, яку Регламент вперше системно поширив на платформне середовище.

Щодо змісту стандарту ст. 14(4) у доктрині запропоновано орієнтуватися на фігуру дбайливого економічного оператора: провайдер має діяти з рівнем обачності, який дозволяє ухвалити недовільне рішення без складного правового розслідування, зважуючи характер сервісу, тяжкість порушення та інтереси користувача і суспільства, й обирати захід, пропорційний значущості порушення¹⁴⁷. Проти такої конструкції висувається заперечення з позицій свободи підприємницької діяльності (ст. 16 Хартії): визначення того, як сторона здійснює свої договірні права, є втручанням у свободу надання послуг. Це заперечення непереконливе: обов'язок добросовісного поведіння зі структурно слабшою стороною давно відомий праву захисту споживачів, конкурентному праву і праву захисту даних, і ст. 14(4) залишається в межах цієї логіки¹⁴⁸. Глибшим є питання горизонтальної дії фундаментальних прав: ст. 14(4) зобов'язує платформу враховувати Хартію при застосуванні власного договору, і від того, чи визнає практика за цією нормою джерело суб'єктивного права користувача, залежить її реальна сила.

Показово, що до аналогічної конструкції національне право дійшло ще до DSA засобами договірної права. У рішеннях від 29 липня 2021 р. Федеральний верховний суд Німеччини, здійснюючи контроль умов користування Facebook за § 307 BGB, визнав: платформа має право встановлювати контентні стандарти, суворіші за законодавчі, однак її умови недійсні в частині, що не передбачає процедурних гарантій — повідомлення користувача про видалення контенту та можливості висловитися при блокуванні акаунта¹⁴⁹. Логіка цих рішень —

¹⁴⁷Novovic (n 3).

¹⁴⁸ibid.

¹⁴⁹BGH, Urteile vom 29.7.2021 – III ZR 179/20 und III ZR 192/20.

збереження приватної нормотворчості за одночасного процедурного її дисциплінування — структурно є прообразом ст. 14(4) і може розглядатися як національна прото-модель регульованого саморегулювання.

Отже, значення ст. 14 DSA полягає в тому, що вона змінює правову природу платформних умов користування: із формально договірний документ вони перетворюються на юридично контрольований інструмент приватної нормотворчості. Платформа зберігає автономію у формуванні власних правил, але їх зміст, спосіб подання та практика застосування підпорядковуються публічно-правовим стандартам прозорості, передбачуваності, об'єктивності, пропорційності та поваги до фундаментальних прав.

3.1.2. Стаття 16 DSA: механізм повідомлення та дії як процедуризація первинного платформного правозастосування

Регуляторна функція та передумови. Стаття 16 зобов'язує кожного провайдера хостингових послуг запровадити механізм, через який будь-яка особа може повідомити про наявність на сервісі інформації, яку вона вважає незаконною. Механізми повідомлення та дії (notice-and-action) становлять основу сучасної системи відповідальності посередників: вони є компромісом між покладенням на посередника відповідальності за кожну одиницю оброблюваної інформації та неконтрольованим поширенням незаконного контенту. У цьому сенсі ст. 16 не є новелою — такі механізми були поширені й до DSA¹⁵⁰. Її регуляторне значення полягає в іншому: по-перше, механізм стає юридично обов'язковим для провайдерів послуг хостингу; по-друге, DSA вперше встановлює мінімальні змістовні вимоги до функціональності й доступності таких механізмів. Водночас в академічних джерелах підкреслюються структурні ризики такого механізму¹⁵¹:

¹⁵⁰ Насамперед як наслідок ст. 14 Директиви 2000/31/ЄС про електронну комерцію, яка ставила імунітет хостинг-провайдера в залежність від оперативного видалення контенту після отримання фактичного знання і тим самим стимулювала створення систем нотифікації, не регламентуючи їх; формалізовані механізми існували також у національному праві (зокрема, німецький NetzDG 2017 р.) та у ст. 17(4) Директиви (ЄС) 2019/790.

¹⁵¹ Jennifer M Urban, Joe Karaganis and Brianna L Schofield, Notice and Takedown in Everyday Practice (UC Berkeley Public Law Research Paper No 2755628, 2017); Aleksandra Kuczerawy,

повідомлення про конкретний контент не запобігає його повторній появі, а стимулює уникнути відповідальності схиляє провайдерів до видалення будь-якого повідомленого контенту, що створює загрозу надмірної модерації та свободі вираження поглядів. Саме на врівноваження цих ризиків спрямована процедурна конструкція статті.

Слід зазначити, що адресатом ст. 16 є ширше коло суб'єктів, ніж онлайн-платформи, — усі провайдери хостингу. Для цього дослідження стаття значуща тим, що вона процедуризує первинну ланку приватного нормозастосування: момент, у якому зовнішній сигнал перетворюється на модераційне рішення платформи.

Зміст і механізм дії. Механізм має бути легкодоступним, зручним і дозволяти подання повідомлень виключно електронними засобами. Повідомлення має бути достатньо точним і належно обґрунтованим: містити пояснення причин, з яких особа вважає інформацію незаконною, чітко зазначення точного електронного розташування інформації (зокрема URL), ім'я та електронну адресу повідомника (крім повідомлень щодо окремих злочинів проти статевої свободи), а також підтвердження добросовісності — заяву про точність і повноту повідомлення. Обидві кваліфікаційні вимоги мають функціональне навантаження. Вимога точності запобігає перетворенню повідомлення на підставу загального моніторингу, забороненого ст. 8 DSA. Вимога обґрунтованості дає провайдеру фактичну основу для ухвалення поінформованого і зваженого рішення — не лише щодо незаконності, а й щодо фундаментальних прав інших осіб. Ключовим правовим наслідком є зв'язок із режимом відповідальності: за ст. 16(3) належно обґрунтоване повідомлення, яке дозволяє дбайливому провайдеру без детального правового дослідження встановити очевидну незаконність контенту, породжує фактичне знання у розумінні ст. 6 — і, відповідно, втрату імунітету в разі бездіяльності.

'Intermediary Liability & Freedom of Expression: Recent Developments in the EU Notice & Action Initiative' (2015) 31 Computer Law & Security Review 46.

Отримавши повідомлення, провайдер зобов'язаний своєчасно підтвердити його отримання (якщо надані контактні дані), ухвалити рішення своєчасно, дбайливо, об'єктивно і повідомити про нього повідомника із зазначенням доступних засобів захисту. Якщо для обробки повідомлень використовуються автоматизовані засоби, це має бути розкрито.

Судова практика, доктрина, практика застосування. Кваліфікаційні вимоги до механізму ст. 16 DSA кодифікують практику Суду ЄС. Заборону широких превентивних заходів сформульовано у справі *Scarlet Extended*¹⁵²: фільтрування всіх комунікацій мережі порушує заборону загального моніторингу і не забезпечує справедливого балансу фундаментальних прав — свободи підприємництва провайдера, захисту персональних даних і свободи інформації користувачів. Натомість точково спрямовані заходи допустимі: у справі *L'Oréal v eBay*¹⁵³ визнано можливість зобов'язати оператора запобігати подальшим порушенням того самого продавця щодо тих самих товарних знаків, а в *UPC Telekabel*¹⁵⁴ підкреслено, що заходи мають бути суворо цільовими і не зачіпати правомірний доступ користувачів до інформації. У справі *Glawischnig-Piesczek*¹⁵⁵ Суд допустив обов'язок видаляти й еквівалентний контент, однак лише за умови, що відмінності у формулюваннях не вимагають від провайдера самостійної оцінки. Стандарт обґрунтованості повідомлення був визначений таким, що може породжувати фактичне знання або обізнаність лише тоді, коли повідомлення дає дбайливому економічному оператору підстави встановити незаконність; недостатньо точне чи необґрунтоване повідомлення автоматично не позбавляє імунітету, але залишається фактором, який національний суд має врахувати¹⁵⁶.

¹⁵² Case C-70/10 *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* EU:C:2011:771, paras 38–40, 44–53

¹⁵³ Case C-324/09 *L'Oréal SA and Others v eBay International AG and Others* EU:C:2011:474, para 141

¹⁵⁴ Case C-314/12 *UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH and Wega Filmproduktionsgesellschaft mbH* EU:C:2014:192, para 56.

¹⁵⁵ Case C-18/18 *Eva Glawischnig-Piesczek v Facebook Ireland Limited* EU:C:2019:821, paras 41, 45–46

¹⁵⁶ *L'Oréal (n X)* paras 120–124; *Joined Cases C-682/18 and C-683/18 Frank Peterson v Google LLC and Others and Elsevier Inc v Cyando AG* EU:C:2021:503, paras 115–116

Часовий вимір обов'язку діяти конкретизується у практиці ЄСПЛ щодо відповідальності за затягнуте видалення: у справі *Delfi AS v Estonia*¹⁵⁷ тривале залишення доступними явно незаконних коментарів визнано неприйнятним; у *Pihl v Sweden*¹⁵⁸ видалення наступного дня після скарги на невеликому блозі — достатнім; у *Høiness v Norway*¹⁵⁹ оперативне реагування модерації — належним; у *Sanchez v France*¹⁶⁰ шеститижнева доступність явно незаконних коментарів на публічній сторінці політика — надмірною. З цієї практики та преамбули DSA (п. 52) випливає пропорційний стандарт своєчасності: контент, що загрожує життю чи безпеці, вимагає невідкладної реакції, тоді як повідомлення, що потребують зважування інтересів, допускають розумну затримку — за умови, що пріоритезація одних категорій повідомлень не блокує своєчасний розгляд інших.

Академічна критика механізму, передбаченого ст. 16 DSA, зосереджується насамперед на двох проблемних аспектах. По-перше, ст. 16 має обмежену матеріальну сферу застосування: вона стосується лише повідомлень про незаконний контент і не зобов'язує провайдерів створювати окремий механізм повідомлень про контент, який порушує лише умови користування платформи. Реагування на порушення внутрішніх правил, отже, залишається у сфері підприємницької та договірної автономії платформи. Водночас, якщо платформа добровільно запроваджує такий механізм і на його підставі ухвалює рішення щодо контенту або акаунта, ці рішення підпадають під процедури перегляду, передбачені статтями 20–21 DSA, — включно з рішенням не вживати заходів¹⁶¹.

По-друге, дискусійним залишається обсяг інформації, яку провайдер має надати особі, що подала повідомлення. Стаття 17 DSA прямо гарантує детальне мотивування насамперед користувачу, чий контент було обмежено. Натомість із

¹⁵⁷ *Delfi AS v Estonia* App no 64569/09 (ECtHR [GC], 16 June 2015)

¹⁵⁸ *Pihl v Sweden* App no 74742/14 (ECtHR (dec), 7 February 2017)

¹⁵⁹ *Høiness v Norway* App no 43624/14 (ECtHR, 19 March 2019)

¹⁶⁰ *Sanchez v France* App no 45581/15 (ECtHR [GC], 15 May 2023)

¹⁶¹ Martin Husovec, *Principles of the Digital Services Act* (OUP 2024); Milos Novovic, *The EU Digital Services Act (DSA): A Commentary* (Kluwer Law International 2024), commentary to art 16; Aleksandra Kuczerawy, 'Remedying Overremoval' (Verfassungsblog, 3 November 2022) <https://verfassungsblog.de/remedying-overremoval/>

тексту ст. 16 прямо не впливає обов'язок провайдера детально пояснювати повідомнику причини рішення не вживати заходів. Ця асиметрія процедурних позицій повідомника та автора контенту означає, що питання про право повідомника на повноцінне мотивування відмови діяти залежатиме від майбутньої практики тлумачення поняття «рішення» у DSA¹⁶².

Місце в системі регульованого саморегулювання. Стаття 16 DSA виконує функцію процедурного впорядкування першої стадії платформного правозастосування — отримання зовнішнього сигналу про потенційно незаконний контент і його перетворення на модераційне рішення провайдера.

Її значення полягає в тому, що рішення щодо контенту й надалі ухвалює сам провайдер, тобто елемент приватного правозастосування зберігається. Водночас DSA більше не залишає цей процес повністю на розсуд платформи. Регламент встановлює мінімальні публічно-правові вимоги до способу ініціювання такого рішення: механізм повідомлення має бути доступним, зручним, електронним, а саме повідомлення — достатньо точним і обґрунтованим. Крім того, ст. 16 визначає стандарт реагування провайдера: він має діяти своєчасно, дбайливо, недовільно та об'єктивно. У цьому сенсі ст. 16 конкретизує загальний стандарт ст. 14(4) DSA на рівні окремої процедури.

Контрольний елемент цієї конструкції забезпечується кількома механізмами. По-перше, належне повідомлення може мати значення для виникнення фактичного знання або обізнаності провайдера за ст. 6 DSA і, відповідно, для питання збереження чи втрати імунітету від відповідальності. По-друге, рішення провайдера можуть бути переглянуті через внутрішню систему розгляду скарг та

¹⁶² Pietro Ortolani, Shiva Vahed, Catalina Goanta and Alan G Sanfey, 'The Digital Services Act and the Psychology of Social Media Content Reporting: Drawing Legal Inferences from a Behavioural Experiment on Notice-and-Action Mechanisms' (2025) 4 *European Law Open* 464; Rocco Bellanova and Ronan Ó Fathaigh, 'Platforms, Online Surveillance, and the European Union Digital Services Act' (2026) *European Papers*

позасудове вирішення спорів за статтями 20–21 DSA. По-третє, належне функціонування механізму повідомлення і дії підлягає нагляду з боку координаторів цифрових послуг.

3.1.3. Стаття 17 DSA: обов'язок мотивування як гарантія раціональності платформного правозастосування

Якщо ст. 16 DSA врегульовує початкову стадію реагування провайдера на повідомлення про потенційно незаконний контент, то ст. 17 встановлює процесуальні вимоги до результату такого реагування, зобов'язуючи провайдера надати належне мотивування ухваленого обмежувального рішення. До DSA рішення про видалення, зниження видимості чи блокування зазвичай ухвалювалися без пояснень або з формальним посиланням на "порушення правил спільноти", що позбавляло користувача можливості зрозуміти підставу обмеження і оскаржити його¹⁶³. Обов'язок мотивування виконує подвійну функцію: він є передумовою ефективного використання засобів захисту (без знання підстав рішення оскарження за ст. 20–21 позбавлене сенсу) і водночас накладає обов'язки на самого провайдера, змушуючи його раціоналізувати рішення. Саме тому ст. 17 можна розглядати як перенесення на приватне правозастосування ядра публічно-правової культури мотивування, відомої адміністративному праву¹⁶⁴.

Зміст і механізм дії. Сфера обов'язку окреслена широко. Виклад підстав надається при будь-якому з чотирьох типів обмежень: обмеження видимості інформації (включно з видаленням, унеможливленням доступу та пониженням у ранжуванні); призупинення, припинення або інше обмеження грошових виплат (демонетизація); призупинення чи припинення надання сервісу повністю або частково; призупинення або закриття акаунта. Поняття видимості частково можна розтлумачити через п. 55 Преамбули DSA - пониження у рекомендаційних системах і shadow banning (виключення користувача зі спільноти без його відома);

¹⁶³ UNHRC, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression' (6 April 2018) UN Doc A/HRC/38/35; Kate Klonick, 'The New Governors' (2018) 131 Harvard Law Review 1598.

¹⁶⁴ Martin Husovec, Principles of the Digital Services Act (OUP 2024).

з цього випливає засаднича позиція, що обмеження можливості поширювати новий контент також є обмеженням видимості¹⁶⁵.

Мінімальний зміст викладу підстав охоплює: опис ужитого заходу, його територіальну сферу і тривалість; факти й обставини, покладені в основу рішення, включно із зазначенням, чи ухвалене воно за повідомленням (ст. 16) чи за власною ініціативою (ст. 7), та — лише за суворої необхідності — ідентичність повідомника; інформацію про використання автоматизованих засобів як у виявленні контенту, так і в ухваленні рішення; правову або договірну підставу з поясненням, чому інформація вважається незаконною або несумісною з умовами користування; і чіткі відомості про доступні засоби захисту: внутрішню скаргу, позасудове вирішення спорів і судовий захист⁴. Інформація має бути чіткою і зрозумілою — вимога, що продовжує лінію ст. 14 і практики Суду ЄС щодо прозорості умов.

Обов'язок не застосовується у трьох випадках: коли провайдер не має контактних даних отримувача; щодо оманливого комерційного контенту великого обсягу (спам, боти, фейкові акаунти); і коли провайдер виконує наказ органу за ст. 9 — в останньому випадку достатньо передати виклад підстав, що міститься в самому наказі¹⁶⁶.

Доктрина та практика застосування. Три аспекти статті заслуговують на критичну увагу. Перший — розмежування правової і договірної підстави (ст. 17(3)(d)–(e)). Провайдер зобов'язаний точно вказати, чи ґрунтується обмеження на незаконності контенту, чи на невідповідності власним умовам, з посиланням на конкретне положення. Це розмежування має принципове значення для моделі регульованого саморегулювання: воно унеможливорює маскування приватного розсуду під виконання закону — платформа, чії внутрішні правила суворіші за законодавчі, не може представляти застосування власної політики як реалізацію

¹⁶⁵ Milos Novovic, *The EU Digital Services Act (DSA): A Commentary* (Kluwer Law International 2024), commentary to art 17.

¹⁶⁶ Milos Novovic, *The EU Digital Services Act (DSA): A Commentary* (Kluwer Law International 2024), commentary to art 17.

правової заборони¹⁶⁷. Другий — виняток для оманливого комерційного контенту. Критерій "комерційності" проблемний: масовий маніпулятивний контент (дезінформація, координовані кампанії) не завжди піддається комерційній кваліфікації, що створює невизначеність на перетині потреби оперативного реагування і свободи вираження поглядів; доктрина закликає до вузького тлумачення винятку, аби дрібні порушення не ставали приводом для немотивованих обмежень¹⁶⁸. Третій — розкриття автоматизації: зазначення ролі автоматизованих засобів у виявленні контенту та ухваленні рішення створює інформаційну основу для реалізації прав за GDPR, зокрема права не бути об'єктом виключно автоматизованого рішення зі значними наслідками¹⁶⁹.

Практичним інструментом верифікації виконання ст. 17 стала база даних прозорості за ст. 24(5) DSA, до якої платформи подають усі виклади підстав: вона перетворює індивідуальне мотивування на масив публічних даних, придатний для системного аналізу модераційних практик регуляторами і дослідниками.

Місце в системі регульованого саморегулювання. Стаття 17 DSA виконує функцію раціоналізації та забезпечення перевірюваності платформного правозастосування. Вона не позбавляє провайдера права самостійно ухвалювати рішення щодо обмеження контенту, акаунта, доступу до сервісу чи монетизації. Однак DSA вимагає, щоб таке рішення було не мовчазним або довільним актом приватного розсуду, а мотивованим рішенням із чітким зазначенням фактичних обставин, правової або договірної підстави, ролі автоматизованих засобів та доступних способів оскарження.

¹⁶⁷ Milos Novovic, *The EU Digital Services Act (DSA): A Commentary* (Kluwer Law International 2024), commentary to art 17.

¹⁶⁸ Milos Novovic, *The EU Digital Services Act (DSA): A Commentary* (Kluwer Law International 2024), commentary to art 17.

¹⁶⁹ Chiara P Drolsbach and Nicolas Pröllochs, 'Content Moderation on Social Media in the EU: Insights from the DSA Transparency Database' in *Companion Proceedings of the ACM Web Conference 2024* (ACM 2024) 939 <https://doi.org/10.1145/3589335.3651482>; Gautam Kishore Shahi, Benedetta Tessa, Amaury Trujillo and Stefano Cresci, 'A Year of the DSA Transparency Database: What it (Does Not) Reveal About Platform Moderation During the 2024 European Parliament Election' (arXiv, 9 April 2025)

У системі базового процедурного рівня ст. 17 є продовженням механізму, передбаченого ст. 16. Якщо ст. 16 регулює порядок отримання і розгляду повідомлення про потенційно незаконний контент, то ст. 17 визначає, як має бути оформлено результат такого розгляду. Саме виклад підстав перетворює модераційне рішення на об'єкт подальшої перевірки: користувач отримує можливість оскаржити не абстрактне «порушення правил», а конкретну підставу обмеження — незаконність контенту або його несумісність з умовами користування.

Отже, ст. 17 є з'єднувальною ланкою між первинним реагуванням провайдера та подальшими механізмами захисту. Для користувача виклад підстав створює інформаційну основу для внутрішньої скарги за ст. 20, позасудового вирішення спору за ст. 21 або судового захисту. Для регуляторів, дослідників і громадськості *statements of reasons*, подані до бази даних прозорості, формують інструмент системного контролю за практиками модерації. У цьому сенсі ст. 17 підпорядковує рішення провайдерів публічно-правовим стандартам мотивованості, прозорості та перевірюваності.

3.1.4. Стаття 21 DSA: позасудове вирішення спорів як зовнішній елемент процедурного контролю

Регуляторна функція та передумови. Внутрішня система розгляду скарг за ст. 20 DSA, попри встановлені процедурні гарантії, не усуває базового конфлікту інтересів: онлайн-платформа переглядає власне рішення. Стаття 21 DSA відповідає на цю проблему шляхом створення зовнішнього щодо платформи способу перегляду — системи сертифікованих органів позасудового вирішення спорів (*out-of-court dispute settlement, ODS*), які сертифікуються координаторами цифрових послуг держав-членів.

Потреба в такій проміжній ланці зумовлена структурною нерівністю сторін. Судове оскарження модераційних рішень часто є складним для користувача через інформаційну асиметрію, обмежений доступ до доказів, брак спеціальних знань щодо функціонування платформних процедур і високі трансакційні витрати

судового захисту¹⁷⁰. Функція ODS полягає в тому, щоб забезпечити незалежну від платформи оцінку спору, зменшити інформаційну асиметрію та зробити подальший судовий захист більш реалістичним.

Зміст і механізм дії. Право звернення до сертифікованого ODS-органу має отримувач послуги, включно з особою або організацією, яка подала повідомлення за ст. 16 DSA, якщо спір стосується рішень онлайн-платформи, передбачених ст. 20(1) DSA. Йдеться, зокрема, про рішення щодо видалення інформації або обмеження доступу до неї, обмеження видимості, призупинення чи припинення надання послуги, призупинення чи закриття акаунта, а також обмеження можливості монетизації, якщо такі рішення ухвалені у зв'язку з незаконністю контенту або його несумісністю з умовами користування.

Сертифікацію ODS-органів здійснює координатор цифрових послуг відповідної держави-члена. Для отримання сертифікації орган має відповідати критеріям незалежності, неупередженості, належної експертизи, доступності, а також мати чіткі, справедливі та публічно доступні правила процедури. Розгляд спору має здійснюватися у розумний строк: за загальним правилом рішення має бути доступне сторонам протягом 90 календарних днів, а у складних спорах цей строк може бути продовжений.

Конструкція ст. 21 DSA має дві визначальні характеристики. Перша — не обов'язковість рішення ODS для сторін. Звернення до такого органу не є передумовою судового захисту, а користувач зберігає право звернутися до суду на будь-якій стадії. Цим забезпечується відповідність механізму гарантіям ефективного судового захисту за ст. 47 Хартії основних прав ЄС. Друга — обов'язок платформи брати участь у процедурі має компенсувати не обов'язковість результату: хоча рішення ODS не замінює судового чи адміністративного припису, недобросовісна участь платформи в процедурі може розглядатися як порушення

¹⁷⁰ Nataliia A Mazaraki and Volodymyr D Prymak, 'Механізм вирішення спорів між користувачами та онлайн-платформами в акті ЄС про цифрові послуги' (2026) 19 *Український політико-правовий дискурс* <https://doi.org/10.5281/zenodo.18662891>

обов'язку, встановленого ст. 21(2) DSA, і відповідно бути предметом наглядової оцінки компетентних органів у межах загального механізму забезпечення виконання Регламенту¹⁷¹.

Доктрина та практика застосування. Механізм ст. 21 уже набув практичного виміру: ЄК оприлюднює та оновлює перелік сертифікованих ODS-органів із зазначенням їхньої компетенції, мов розгляду та процедурних особливостей. Це дозволяє оцінювати конструкцію ст. 21 не лише нормативно, а й емпірично — через аналіз правил процедури таких органів, доступності їхніх послуг і якості ухвалюваних рішень.

Основна доктринальна критика ст. 21 стосується необов'язковості рішень ODS. З цієї позиції механізм може видаватися недостатньо ефективним, оскільки платформа, навіть програвши спір, формально не зобов'язана виконати рішення. Однак така критика виходить із розуміння ODS як самодостатньої квазісудової інстанції. Продуктивнішим видається функціональний підхід: практична цінність ODS полягає не лише і не стільки у примусовому виконанні рішення, скільки у створенні незалежної оцінки спору, яка може бути використана користувачем у подальшому судовому або регуляторному процесі.

У цьому сенсі вирішальне значення має якість мотивування ODS-рішення¹⁷². Якщо платформа відмовляється виконати результат позасудового розгляду, належно мотивоване рішення ODS може слугувати процесуально релевантною основою подальшого судового захисту: воно фіксує фактичну канву спору, позиції сторін, застосовані правила платформи, оцінку їхньої відповідності DSA та логіку висновку. Саме тому ODS виконує не лише примирну чи альтернативну функцію, а й процесуально-підготовчу: він допомагає перевести спір із непрозорої площини платформного рішення у форму, придатну для подальшої юридичної перевірки.

¹⁷¹ Див. ст.ст. 21(2), 49(1), 51(1), 52 ДСА

¹⁷² Nataliia A Mazaraki and Volodymyr D Prymak, 'Механізм вирішення спорів між користувачами та онлайн-платформами в акті ЄС про цифрові послуги' (2026) 19 Український політико-правовий дискурс <https://doi.org/10.5281/zenodo.18662891>

Водночас саме тут виявляється нормативна лакуна ст. 21 DSA. Регламент вимагає, щоб ODS-органи мали чіткі та справедливі правила процедури, однак не деталізує структуру та мінімальний зміст мотивування їхніх рішень. Це залишає значний простір для саморегулювання самих ODS-органів.

Місце в системі регульованого саморегулювання. Стаття 21 завершує базовий процедурний рівень DSA, додаючи до внутрішнього самоконтролю онлайн-платформи зовнішню сертифіковану ланку перегляду. Вона не змінює приватного характеру первинного рішення: обмеження контенту, акаунта, доступу до сервісу чи монетизації ухвалює сама онлайн-платформа, а рішення ODS не має обов'язкової сили для сторін. Однак DSA більше не залишає перегляд такого рішення виключно у внутрішній системі платформи. Регламент встановлює публічно-правову рамку зовнішньої перевірки: сертифікацію ODS-органів координаторами цифрових послуг, вимоги щодо незалежності, неупередженості, експертизи, доступності, справедливих процедур, розумних строків і добросовісної участі платформи.

У цьому сенсі ст. 21 є проміжною формою між внутрішнім платформним самоконтролем і судовим захистом. Вона не створює повноцінного юрисдикційного механізму, але забезпечує інституційно відокремлений від платформи перегляд, здатний зменшити інформаційну асиметрію, конкретизувати фактичну й правову основу спору та підготувати користувача до подальшого судового захисту. Сам ODS-сегмент відтворює логіку регульованого саморегулювання у мініатюрі: публічна сертифікація задає інституційну рамку, а конкретна організація процедури та стандарти мотивування значною мірою формуються правилами самих ODS-органів. Саме тому ст. 21 демонструє як потенціал, так і ризики регульованого саморегулювання: зовнішній контроль створюється, але його якість залежить від того, наскільки сертифіковані органи здатні забезпечити не лише формальний розгляд, а й змістовно мотивовану, зрозумілу та практично корисну оцінку платформного рішення.

3.2. Посилений ризик-орієнтований рівень регульованого саморегулювання для VLOPs/VLOSEs

До посиленого ризик-орієнтованого рівня в цьому дослідженні віднесено статті 34, 35, 37, 40, 41 і 42 DSA за трьома спільними ознаками. По-перше, за колом адресатів: ці обов'язки застосовуються лише до дуже великих онлайн-платформ і дуже великих онлайн-пошукових систем — суб'єктів, масштаб діяльності яких, що визначається через поріг понад 45 млн активних отримувачів послуг у Союзі, перетворює приватні правила, технічні архітектури та модераційні практики на фактор системного суспільного впливу. Саме тут реалізується пропорційна та ризик-орієнтована логіка диференціації обов'язків, обґрунтована у підрозділі 1.2.

По-друге, за предметом регуляторного впливу: на відміну від базового процедурного рівня, який впорядковує окремі рішення платформи щодо контенту, акаунтів або скарг користувачів, цей рівень спрямований на внутрішні системи управління платформою як такі. Йдеться не лише про процедуру ухвалення конкретного рішення, а про виявлення, оцінювання та мінімізацію системних ризиків, організацію комплаєнс-функції, документування діяльності, звітність і створення умов для зовнішньої перевірки.

По-третє, за регуляторною технікою: цей рівень поєднує два взаємодоповнювані механізми. Перший — метарегулювання внутрішніх систем управління, передбачене статтями 34, 35 і 41 DSA, за якого право визначає підходи до виявлення ризиків, ухвалення рішень, внутрішнього контролю та відповідальності за комплаєнс. Другий — зовнішня верифікація, закріплена у статтях 37, 40 і 42 DSA, яка має подолати обмеженість суто внутрішнього самоопису і самоперевірки платформ через аудит, доступ до даних і посилену прозорість.

Виклад у межах цього підрозділу побудовано відповідно до цієї логіки. Спочатку аналізується режим системних ризиків і заходів їх мінімізації за статтями 34–35 DSA; далі — внутрішня комплаєнс-функція за ст. 41 DSA; після цього — незалежний аудит за ст. 37 DSA; доступ до даних і посилена звітність за статтями

40 і 42 DSA. Завершується підрозділ проміжною оцінкою посиленого ризик-орієнтованого рівня як форми метарегулювання та зовнішньої верифікації платформного саморегулювання.

3.2.1. Статті 34–35 DSA: оцінка та мінімізація системних ризиків як ядро метарегулювання

Регуляторна функція та передумови. Статті 34–35 DSA утворюють ядро посиленого ризик-орієнтованого рівня¹⁷³ та є найвиразнішим проявом метарегуляторної техніки¹⁷⁴ в Регламенті. Їх передумовою є визнання того, що VLOPs/VLOSEs через масштаб своєї діяльності здатні істотно впливати не лише на окремих користувачів, а й на онлайн-безпеку, публічний дискурс, інформаційне середовище, демократичні процеси та онлайн-торгівлю. Такі впливи зумовлені не лише окремими рішеннями щодо конкретного контенту, а й загальною побудовою послуг платформи: рекомендаційними системами, рекламними механізмами, алгоритмічним ранжуванням, дизайном інтерфейсу, практиками модерації та застосуванням власних правил платформи.

Регуляторна проблема, на яку відповідають ці статті, має структурний характер. Шкода або суспільно значущі ризики, пов'язані з найбільшими платформами, часто виникають не з одиничного незаконного контенту, а з того, як платформа організовує видимість, поширення, монетизацію, рекомендацію та модерацію інформації. Саме тому процедурне впорядкування окремих рішень,

¹⁷³ Marie-Therese Sekwenz, Rita Gsenger, Scott Dahlgren and Ben Wagner, 'Doing Audits Right? The Role of Sampling and Legal Content Analysis in Systemic Risk Assessments and Independent Audits in the Digital Services Act' (arXiv, 6 May 2025) <https://arxiv.org/abs/2505.03601>; Sally Broughton Micova, Daniel Schnurr, Andrea Calef and Bryn Enstone, *Cross-Cutting Issues for DSA Systemic Risk Management: An Agenda for Cooperation* (CERRE, 10 July 2024) <https://cerre.eu/publications/cross-cutting-issues-for-dsa-systemic-risk-management-an-agenda-for-cooperation/>

¹⁷⁴ Cary Coglianese and Evan Mendelson, 'Meta-Regulation and Self-Regulation' in Robert Baldwin, Martin Cave and Martin Lodge (eds), *The Oxford Handbook of Regulation* (Oxford University Press 2010).

передбачене базовим рівнем DSA у статтях 14–21, є необхідним, але недостатнім. Воно дозволяє перевірити конкретне рішення платформи, однак не охоплює повною мірою системні ефекти, що виникають на рівні дизайну сервісу та внутрішньої організації управління ризиками.

У цьому полягає значення статей 34–35 DSA. Вони не замінюють приватне управління платформи прямим державним адмініструванням і не встановлюють вичерпного переліку конкретних рішень, які платформа має ухвалювати в кожній ситуації. Натомість DSA зобов'язує VLOPs/VLOSEs створити, підтримувати й документувати внутрішній цикл самооцінювання та самокоригування: виявляти системні ризики, оцінювати їхній характер і масштаб, а потім впроваджувати розумні, пропорційні та ефективні заходи їхньої мінімізації. Саме ця конструкція відповідає логіці метарегулювання: право регулює не стільки окрему поведінку платформи, скільки її внутрішню систему виявлення, оцінювання та управління ризиками.

Зміст і механізм дії. Стаття 34 DSA зобов'язує VLOPs/VLOSEs щонайменше раз на рік, а також перед запровадженням функціональностей, які можуть мати критичний вплив на системні ризики, здійснювати оцінку ризиків, що випливають із дизайну, функціонування та використання їхніх сервісів. Така оцінка охоплює основні категорії ризиків, визначені Регламентом: поширення незаконного контенту; фактичні або передбачувані негативні наслідки для фундаментальних прав, зокрема людської гідності, свободи вираження поглядів та інформації, свободи і плюралізму медіа, права на приватне життя, захисту персональних даних, недискримінації, прав дитини та захисту споживачів; негативний вплив на громадянський дискурс, виборчі процеси, громадську безпеку; а також негативні наслідки для громадського здоров'я, неповнолітніх, фізичного і психічного благополуччя особи та у сфері гендерно зумовленого насильства.

Під час оцінювання ризиків VLOPs/VLOSEs мають враховувати системні характеристики сервісу: дизайн рекомендаційних та інших алгоритмічних систем, системи модерації контенту, умови користування і практику їх застосування, механізми відбору та показу реклами, практики роботи з даними, а також інші

елементи технічної й організаційної архітектури сервісу. Принципово, що така оцінка не обмежується незаконним контентом. Вона може охоплювати також законний, але потенційно шкідливий або маніпулятивний контент, якщо його поширення чи алгоритмічне підсилення здатне сприяти системним ризикам, зокрема для фундаментальних прав, громадянського дискурсу, виборчих процесів, громадської безпеки або захисту неповнолітніх.

Стаття 35 DSA зобов'язує VLOPs/VLOSEs впроваджувати розумні, пропорційні та ефективні заходи мінімізації виявлених системних ризиків. Регламент не встановлює закритого переліку таких заходів, а лише наводить можливі напрями реагування: адаптацію дизайну сервісу та інтерфейсу, коригування алгоритмічних і рекомендаційних систем, зміну умов користування та практики їх застосування, адаптацію рекламних систем, посилення внутрішніх процесів і ресурсів для модерації, співпрацю з trusted flaggers, участь у кодексах поведінки, цільові заходи захисту дітей, а також маркування або інші заходи щодо синтетичного чи маніпульованого контенту. Пропорційність таких заходів має оцінюватися з урахуванням тяжкості ризиків, економічної та технічної спроможності провайдера, а також можливого впливу самих заходів на фундаментальні права користувачів.

Метарегуляторний характер конструкції полягає в тому, що DSA не визначає ані вичерпної методології оцінювання, ані єдиного набору обов'язкових заходів мінімізації для всіх платформ. Натомість Регламент встановлює обов'язок мати внутрішню систему управління системними ризиками, визначає її періодичність, категоріальну рамку, мінімальні фактори оцінювання та стандарт якості заходів. Цей цикл не завершується самозвітом платформи: результати оцінювання і мінімізації ризиків надалі підлягають перевірці через незалежний аудит, звітність, доступ до даних і наглядові повноваження Комісії. Саме тому статті 34–35 слід розглядати як ядро метарегулювання в DSA: право встановлює вимоги до

внутрішньої системи, через яку платформа повинна виявляти, пояснювати та коригувати власні системні ризики¹⁷⁵.

Доктрина та практика застосування статей 34–35 DSA. Практика застосування статей 34–35 DSA підтверджує як потенціал, так і слабкі місця ризик-орієнтованої моделі. З одного боку, запровадження обов’язкових звітів про оцінку ризиків, звітів про заходи з мінімізації ризиків, аудиторських звітів та звітів про виконання аудиторських рекомендацій створило принципово новий рівень прозорості: VLOPs/VLOSEs уперше були зобов’язані публічно описати, які системні ризики вони вбачають у дизайні та функціонуванні своїх сервісів, які заходи мінімізації застосовують і як ці заходи перевіряються незалежними аудиторами. Звіти мають публікуватися щорічно; провайдери також повинні передавати звіти Комісії та координаторам цифрових послуг¹⁷⁶.

Водночас перші цикли звітності показали, що сама наявність процесу оцінки ризиків ще не гарантує ефективного управління системними ризиками. KPMG¹⁷⁷ у порівняльному аналізі звітів за DSA у 2024-2025 роках зазначає значну різноманітність у тлумаченні статей 34–35: звіти суттєво відрізняються за обсягом, деталізацією та способом подання, а окремі платформи не включали оцінку ймовірності та впливу ризиків. Це підтверджує головну проблему метарегулювання: коли право встановлює рамку оцінювання, але не уніфікує методологію, платформи можуть формально виконувати обов’язок, не забезпечуючи достатньої порівнюваності й перевірюваності результатів.

Схожий висновок випливає з аналізу DSA Observatory¹⁷⁸. У першому циклі публікації щодо звітів з оцінки ризиків уже виникли питання щодо строків

¹⁷⁵ Milos Novovic, *The EU Digital Services Act (DSA): A Commentary* (Kluwer Law International 2024), commentary to arts 34–35

¹⁷⁶ European Commission, ‘Q&A on Risk Assessment Reports, Audit Reports and Audit Implementation Reports under DSA’ (18 February 2026) <<https://digital-strategy.ec.europa.eu/en/faqs/qa-risk-assessment-reports-audit-reports-and-audit-implementation-reports-under-dsa>>

¹⁷⁷ KPMG, *Analysis of the 2024/2025 Digital Services Act Audit Reports* (KPMG Netherlands 2025) <<https://assets.kpmg.com/content/dam/kpmg/nl/pdf/2025/kpmg-2024-dsa-audit-reports-benchmark.pdf>>

¹⁷⁸ John Albert, ‘DSA Risk Assessment Reports: A Guide to the First Rollout and What’s Next’ (DSA Observatory, 9 December 2024) <<https://dsa-observatory.eu/2024/12/09/dsa-risk-assessment-reports-are-in-a-guide-to-the-first-rollout-and-whats-next/>>

публікації, редагування, форматів звітів і можливості їх практичного використання для зовнішнього контролю. Подальший аналіз аудитів також показав, що статті 34–35 залишаються одними з найбільш відкритих і складних для оцінювання положень DSA: аудитори здебільшого перевіряли процедурні аспекти – чи існує формальний процес оцінки ризиків, чи задокументовані ризики, чи пов’язані вони із заходами мінімізації, – але не завжди могли глибоко оцінити реальну ефективність таких заходів¹⁷⁹.

Це означає, що на практиці статті 34–35 поки що працюють переважно як механізм процесуальної підзвітності, а не як повністю сформований механізм доказової оцінки ефективності ризик-мінімізації. Іншими словами, DSA вже змусив VLOPs/VLOSEs описувати свої ризики й заходи реагування, але ще не забезпечив достатньо стабільних критеріїв для відповіді на складніше питання: чи ці заходи справді зменшують системні ризики. Knight-Georgetown Institute¹⁸⁰ так само оцінює перший цикл як важливий крок до прозорості, але вказує, що звіти часто недостатньо враховують роль дизайну платформи у виникненні ризиків і бракують конкретики щодо даних, метрик і методів, використаних для оцінки ризиків та ефективності заходів у відповідь на них.

Окремо слід враховувати роль Європейської ради з цифрових послуг і Комісії. 18 листопада 2025 р. Рада у співпраці з Комісією оприлюднила перший щорічний звіт за ст. 35(2) DSA про найпомітніші та повторювані системні ризики і заходи їх мінімізації, підготовлений на основі оцінок ризиків платформ, аудиторських звітів, звітів прозорості, незалежних досліджень та внеску громадянського суспільства¹⁸¹. Значення цього циклу полягає в тому, що він переносить оцінку виконання статей 34–35 із площини самозвітності окремих

¹⁷⁹ John Albert, ‘Shortcomings of the First DSA Audits – and How to Do Better’ (DSA Observatory, 11 June 2025) <<https://dsa-observatory.eu/2025/06/11/shortcomings-of-the-first-dsa-audits-and-how-to-do-better/>>

¹⁸⁰ Knight-Georgetown Institute, ‘Systemic Risk Assessment under the Digital Services Act’ (15 May 2025) <<https://kgi.georgetown.edu/research-and-commentary/systemic-risk-assessment-under-the-digital-services-act>>

¹⁸¹ European Board for Digital Services, ‘First Report of the European Board for Digital Services in Cooperation with the Commission pursuant to Article 35(2) DSA on the Most Prominent and Recurrent Systemic Risks as well as Mitigation Measures’ (18 November 2025).

платформ у площину порівняльного регуляторного знання: розрізнені самоописи вперше агрегуються незалежним публічним суб'єктом у спільну картину ризиків. Водночас сам звіт замислений як відправна точка, що розширюватиметься в міру накопичення даних про ефективність заходів мінімізації, — це показує, що на цьому етапі модель перебуває у фазі формування, а не завершеної верифікованої практики.

Отже, ефективність статей 34–35 DSA на сучасному етапі слід оцінювати диференційовано. Як інструмент видимості та формалізації внутрішнього ризик-менеджменту платформ вони вже є ефективними: платформи змушені ідентифікувати ризики, описувати заходи мінімізації, проходити аудит і публікувати звіти. Як інструмент доказового контролю реального зменшення системних ризиків їх ефективність поки що обмежена. Основними проблемами залишаються різноманітність методологій, слабка порівнюваність звітів, недостатня конкретика щодо метрик і даних, обмежене врахування ризиків, пов'язаних із дизайном сервісу, а також залежність первинної оцінки від самоопису платформ.

3.2.2. Стаття 37 DSA: незалежний аудит як інституціоналізована зовнішня верифікація

Регуляторна функція та передумови. Метарегуляторна конструкція статей 34–35 DSA є недосконалою з точки зору того, що і оцінку системних ризиків, і вибір заходів їх мінімізації первинно здійснює сама платформа. Без зовнішньої перевірки такий цикл самооцінювання може виявитися хибним. Стаття 37 DSA відповідає на цю проблему через інституціоналізацію незалежного аудиту: VLOPs/VLOSEs зобов'язані щонайменше раз на рік і за власний рахунок проходити незалежну перевірку виконання обов'язків, передбачених главою III DSA, а також зобов'язань, взятих відповідно до кодексів поведінки та кризових протоколів.

Аудит у цій конструкції виконує функцію зовнішньої верифікації ризик-орієнтованого саморегулювання. Він не замінює нагляд Комісії та не перетворює аудитора на регулятора, але має розірвати замкненість платформної самозвітності: твердження платформи про наявність оцінки ризиків, заходів мінімізації,

внутрішніх процедур і комплаєнс-контролів стають предметом незалежної професійної перевірки. Саме тому ст. 37 є перехідною ланкою від метарегулювання внутрішніх систем управління до зовнішньої підзвітності VLOPs/VLOSEs.

Зміст і механізм дії. Аудит здійснюють організації, незалежні від провайдера VLOP/VLOSE та від пов'язаних із ним юридичних осіб. Такі організації не повинні мати конфлікту інтересів, зокрема не мають надавати провайдеру послуги, пов'язані з питаннями, що підлягають аудиту; вони повинні мати підтверджену експертизу у сфері управління ризиками, технічну компетентність, а також дотримуватися професійної етики, об'єктивності й належної професійної обачності. Аудит не може необмежено здійснювати один і той самий аудитор: DSA встановлює обмеження щодо тривалості послідовного аудиту того самого провайдера.

За результатами аудиту складається аудиторський звіт із висновком про відповідність: позитивним, позитивним із зауваженнями або негативним. Якщо висновок не є позитивним, аудитор має надати операційні рекомендації щодо заходів, необхідних для досягнення відповідності. Провайдер, отримавши такий звіт, повинен протягом одного місяця ухвалити звіт про виконання аудиторських рекомендацій, у якому визначити заходи з імплементації рекомендацій або, якщо він не виконує рекомендації, обґрунтувати причини такого рішення та зазначити альтернативні заходи.

Процедура аудиту деталізована Делегованим регламентом Комісії (ЄС) 2024/436, який застосовується з 22 лютого 2024 р. Він встановлює правила проведення аудитів VLOPs/VLOSEs, методологічні вимоги, стандартизовані шаблони аудиторських звітів та звітів про виконання аудиторських рекомендацій, що має забезпечити більшу порівнюваність і контрольованість аудиторської практики. Аудиторські звіти, звіти про оцінку ризиків, відомості про заходи з мінімізації ризиків і звіти про виконання аудиторських рекомендацій підлягають публікації відповідно до ст. 42(4) DSA, з можливістю вилучення інформації, що охороняється як конфіденційна.

Доктринальна критика незалежного аудиту за ст. 37 DSA зосереджується на тому, що цей механізм ще не гарантує повноцінної доказової перевірки ефективності ризик-орієнтованого саморегулювання¹⁸². По-перше, перші аудити часто мають процедурний характер і перевіряють радше наявність внутрішніх процесів, ніж фактичне зменшення системних ризиків. По-друге, відсутність усталених методологій, порівнюваних метрик і спільних стандартів вибірки (sampling) ускладнює аудит таких різномірних ризиків, як вплив на фундаментальні права, виборчі процеси, громадський дискурс чи психічне благополуччя. По-третє, аудитори значною мірою залежать від даних, наданих самими платформами, що створює ризик перевірки «самоопису» платформи замість її реального функціонування. По-четверте, публічна цінність аудиторських звітів (audit reports) обмежується непорівнюваністю форматів, різним рівнем деталізації та вилученням конфіденційної інформації¹⁸³. Тому ст. 37 слід розглядати як необхідну, але недостатню ланку зовнішньої верифікації: вона інституціоналізує перевірку платформного саморегулювання, однак її ефективність залежить від розвитку методологій аудиту, доступу до даних за ст. 40, посиленої звітності за ст. 42 та активного нагляду Комісії.

¹⁸²Daniel Holznagel, 'Shortcomings of the First DSA Audits — and How to Do Better' (DSA Observatory, 11 June 2025) <https://dsa-observatory.eu/2025/06/11/shortcomings-of-the-first-dsa-audits-and-how-to-do-better/>; John Albert, 'What Are DSA Audits Doing for Systemic Risk Enforcement? The Case of X' (DSA Observatory, 19 December 2025)

¹⁸³ Marie-Therese Sekwenz, Rita Gsenger, Scott Dahlgren and Ben Wagner, 'Doing Audits Right? The Role of Sampling and Legal Content Analysis in Systemic Risk Assessments and Independent Audits in the Digital Services Act' (arXiv, 6 May 2025) <https://arxiv.org/abs/2505.03601>; KPMG Netherlands, *Analysis of the 2024 Digital Services Act Audit Reports: Exploring the Inaugural DSA Audit Reports of 19 Platforms: A Benchmark Study* (KPMG, 24 February 2025); Sara Solarova, Matúš Mesarčík, Branislav Pecher and Ivan Srba, 'Beyond the Checkbox: Strengthening DSA Compliance Through Social Media Algorithmic Auditing' (arXiv, 26 January 2026) <https://arxiv.org/abs/2601.18405>;

Місце в архітектурі регульованого саморегулювання. Стаття 37 DSA є першою з трьох ланок зовнішньої верифікації посиленого ризик-орієнтованого рівня, поряд із доступом до даних за ст. 40 та посиленою прозорістю за ст. 42. Її функція полягає у тому, щоб перевести внутрішні процеси VLOPs/VLOSEs — оцінку системних ризиків, заходи їх мінімізації, комплаєнс-процедури та виконання зобов'язань за кодексами поведінки чи кризовими протоколами — у площину незалежної професійної перевірки.

Тобто аудиту підлягає система, створена самою платформою, а виконання аудиторських рекомендацій також залишається відповідальністю провайдера, який може або прийняти такі рекомендації, або мотивовано відхилити їх і запропонувати альтернативні заходи. Водночас DSA встановлює публічно-правові вимоги до обов'язковості й періодичності аудиту, незалежності аудитора, відсутності конфлікту інтересів, ротації, методології перевірки, рівня впевненості та форми аудиторського висновку.

Особливість ст. 37 полягає в тому, що зовнішню перевірку здійснює не державний орган, а приватний, проте юридично незалежний аудитор. Його висновок, у свою чергу, стає елементом публічної підзвітності через обов'язок публікації аудиторських звітів, звітів про оцінку ризиків і звітів про виконання аудиторських рекомендацій, а також через можливість подальшого використання цих матеріалів Комісією в межах нагляду за VLOPs/VLOSEs.

Отже, ст. 37 демонструє складну конструкцію зовнішньої верифікації в DSA: приватна система управління ризиками перевіряється приватним, але незалежним аудитором у межах публічно встановлених стандартів і під потенційним контролем Комісії. Саме тому ця стаття є показовою для оцінки життєздатності моделі регульованого саморегулювання: якщо незалежний аудит залишається формальним або надмірно залежним від звіту самооцінювання платформи, основний тягар перевірки неминуче зміщується на доступ до даних за ст. 40 та прямий нагляд Комісії.

3.2.3. Стаття 40 DSA: доступ до даних як інфраструктура незалежного знання про платформи

Регуляторна функція та передумови. Якщо незалежний аудит за ст. 37 DSA забезпечує зовнішню професійну перевірку внутрішніх систем платформи, то ст. 40 спрямована на подолання глибшої проблеми — інформаційної асиметрії між VLOPs/VLOSEs, з одного боку, та регуляторами, дослідниками і суспільством — з іншого. Оцінити виконання DSA найбільшими платформами неможливо без доступу до даних, які перебувають під їхнім фактичним контролем. Без такого доступу ані компетентні органи, ані незалежні дослідники не здатні належним чином перевірити твердження платформ про характер системних ризиків, ефективність заходів їх мінімізації та реальний вплив архітектури сервісу на користувачів, публічний дискурс і фундаментальні права.

Стаття 40 DSA створює два основні шляхи подолання цієї асиметрії. Перший — доступ до даних для Комісії та координаторів цифрових послуг з метою моніторингу й оцінки дотримання Регламенту. Другий — доступ до даних для перевірених дослідників, який має забезпечити незалежне вивчення системних ризиків у Союзі та оцінку адекватності заходів їх мінімізації.

Для цього DSA встановлює критерії надання статусу перевіреного дослідника, покликані збалансувати дослідницький інтерес у доступі до платформних даних, суспільний інтерес у незалежному й об'єктивному розумінні внутрішніх механізмів функціонування онлайн-платформ, а також легітимні інтереси самих платформ, зокрема захист комерційної таємниці, безпеку сервісу та свободу підприємницької діяльності. Саме тому доступ дослідників до даних у DSA не є загальним або необмеженим: він надається для конкретного дослідницького проєкту, за умови незалежності дослідника, прозорості фінансування, наявності належних гарантій захисту даних і доведення необхідності та пропорційності запитуваного доступу.

На момент перших етапів застосування ст. 40 DSA відкриті джерела не свідчать про наявність усталеної практики необґрунтованого надання доступу до

платформних даних або зловживання статусом перевіреного дослідника. Такий висновок є логічним з огляду на відносну новизну механізму: повноцінна процедура подання заявок через DSA Data Access Portal почала діяти лише з 29 жовтня 2025 р. Натомість практична й доктринальна дискусія зосереджена переважно на протилежній проблемі — складності отримання доступу, високому рівні конкретизації запиту, залежності дослідника від інформації про структуру даних, яку контролює сама платформа, а також ризику звуження доступу через посилення на безпеку сервісу, конфіденційність або комерційну таємницю¹⁸⁴.

Отже, реальний вплив ст. 40 DSA на модель регульованого саморегулювання стане зрозумілим лише в майбутній практиці її застосування. Поки що зарано оцінювати, чи забезпечить механізм доступу перевірених дослідників стабільний і достатній доступ до платформних даних. Водночас саме його нормативне закріплення вже є важливим кроком: DSA визнає, що ефективний контроль за VLOPs/VLOSEs потребує не лише державного нагляду й аудиту, а й незалежного наукового знання про внутрішні механізми платформ. У цьому сенсі ст. 40 є одним із найбільш перспективних елементів співрегуляторної архітектури DSA, оскільки створює правові передумови для зовнішньої, емпірично обґрунтованої перевірки платформного саморегулювання.

3.2.4. Стаття 42 DSA: посилена звітність як публічний вимір верифікації

Регуляторна функція та передумови. Аудит за ст. 37 DSA і доступ до даних за ст. 40 DSA створюють механізми верифікації для кваліфікованих суб'єктів — аудиторів, регуляторів і перевірених дослідників. Стаття 42 DSA додає до цієї конструкції третій, найширший контур — публічну прозорість. Її логіка полягає в тому, що інституціоналізована підзвітність VLOPs/VLOSEs залишається

¹⁸⁴ Michael Veale and Rachel Griffin, 'Data Access under the Digital Services Act: A Data Standoff' (arXiv, 2 May 2025) <https://arxiv.org/abs/2505.01122>; DSA Observatory, 'If at First You Don't Succeed: Reflections on a Rejected Art 40 DSA Data Access Request' (DSA Observatory, 12 March 2026) <https://dsa-observatory.eu/2026/03/12/if-at-first-you-dont-succeed-reflections-on-a-rejected-art-40-dsa-data-access-request/>

неповною, якщо результати самооцінювання, зовнішньої перевірки та ризик-менеджменту не стають доступними ширшому колу адресатів: користувачам, медіа, громадянському суспільству, науковій спільноті та іншим зацікавленим суб'єктам.

Для VLOPs/VLOSEs загальні обов'язки звітності, передбачені ст. 15 DSA для провайдерів посередницьких послуг і ст. 24 DSA для онлайн-платформ, посилюються як за періодичністю, так і за змістом. Стаття 42 вимагає регулярного оприлюднення звітів про модерацію контенту, а також публікації ключових документів ризик-орієнтованого комплаєнсу: звітів про оцінку ризиків, інформації про заходи з мінімізації ризиків, аудиторських звітів і звітів про виконання аудиторських рекомендацій. Саме через це ст. 42 виконує функцію публічного виміру зовнішньої верифікації.

Зміст і механізм дії. Стаття 42 DSA встановлює додаткові обов'язки розкриття для VLOPs/VLOSEs, що діють поряд із загальними обов'язками прозорості за статтями 15 і 24. Звіти про модерацію контенту, передбачені ст. 15 DSA, для VLOPs/VLOSEs мають публікуватися щонайменше кожні шість місяців. Крім інформації, передбаченої загальним режимом звітності, такі звіти повинні додатково розкривати людські ресурси, виділені на модерацію контенту щодо сервісу в Союзі, у розбивці за офіційними мовами держав-членів; кваліфікацію, мовну експертизу, навчання і підтримку персоналу модерації; а також показники точності автоматизованих засобів модерації у розбивці за офіційними мовами держав-членів.

Вимога мовної деталізації має окреме значення: вона робить видимішою нерівномірність модераційної спроможності між великими і малими мовними ринками та дозволяє оцінити, чи здатна платформа забезпечувати належний рівень модерації не лише англійською або кількома домінантними мовами, а й іншими офіційними мовами Союзу. Водночас перші емпіричні дослідження DSA-звітності показують, що сама наявність обов'язку розкриття ще не гарантує повної

порівнюваності: звіти платформ і надалі мають проблеми з форматуванням, своєчасністю, узгодженістю та повнотою даних¹⁸⁵.

Другий блок звітності стосується публікації документів циклу ризик-орієнтованої верифікації. Відповідно до ст. 42(4) DSA VLOPs/VLOSEs повинні передавати координатору цифрових послуг за місцем заснування та Комісії, а також робити публічно доступними звіти про оцінку ризиків за ст. 34, інформацію про конкретні заходи з мінімізації ризиків за ст. 35(1), аудиторські звіти за ст. 37(4) і звіти про виконання аудиторських рекомендацій за ст. 37(6).

Противагою публічності є можливість вилучення окремих відомостей із публічної версії документів. Провайдер може не розкривати інформацію, якщо її публікація призвела б до розкриття конфіденційної інформації провайдера або отримувачів послуги, створила б значні вразливості для безпеки сервісу, підірвала б громадську безпеку або могла б завдати шкоди отримувачам послуги.

Доктрина та практика застосування. Практика першого циклу звітності виявила передбачуване напруження навколо співвідношення публічності та конфіденційності. Обсяг вилучень у публічних версіях звітів різнився між платформами, а питання строків публікації, редагування конфіденційної інформації та різноманітності форматів називалися серед чинників, що ускладнювали зіставлення звітів про ризики й аудитів зовнішніми аналітиками¹⁸⁶. Це підтверджує амбівалентність ст. 42 DSA: з одного боку, вона відкриває для суспільного контролю документи, які раніше залишалися внутрішніми матеріалами платформ;

¹⁸⁵ Amaury Trujillo, Benedetta Tessa and Stefano Cresci, 'Disarranged Harmonization of Transparency Reporting by Social Media Platforms Under the Digital Services Act' (arXiv, 17 May 2026) <https://arxiv.org/abs/2605.17655>

¹⁸⁶ John Albert, 'DSA Risk Assessment Reports: A Guide to the First Rollout and What's Next' (DSA Observatory, 9 December 2024) <https://dsa-observatory.eu/2024/12/09/dsa-risk-assessment-reports-are-in-a-guide-to-the-first-rollout-and-whats-next/>; KPMG Netherlands, Analysis of the 2024 Digital Services Act Audit Reports: Exploring the Inaugural DSA Audit Reports of 19 Platforms: A Benchmark Study (KPMG, 24 February 2025) <https://assets.kpmg.com/content/dam/kpmgsites/nl/pdf/2025/services/kpmg-2024-dsa-audit-reports-benchmark.pdf.coredownload.inline.pdf>

з іншого — ефективність такого контролю залежить від повноти, зрозумілості та порівнюваності публічних версій.

Показово, що ст. 42 DSA вже стала предметом правозастосування. У січні 2026 р. Комісія відкрила нове формальне розслідування щодо X у зв'язку з Grok та рекомендаційними системами платформи¹⁸⁷; серед можливих порушень названо статті 34, 35 і 42 DSA, тобто оцінку системних ризиків, заходи їх мінімізації та обов'язки щодо прозорості.

3.3. Співрегуляторний рівень колективних інструментів DSA

До третього рівня віднесено статті 45–48 DSA — кодекси поведінки, кодекси щодо онлайн-реклами, кодекси доступності та кризові протоколи. Від перших двох рівнів його відрізняють три ознаки. По-перше, за критерієм, сформульованим у підрозділі 1.2.1, це власне співрегулювання, а не лише регульоване саморегулювання: приватне нормотворення тут є інструментом реалізації публічно визначених цілей — за ініціативи, сприяння та участі Комісії і Європейської ради з цифрових послуг. По-друге, за характером інструментів: ідеться про колективні механізми, що об'єднують багатьох провайдерів, а в окремих випадках також інших зацікавлених суб'єктів, на відміну від індивідуальних обов'язків перших двох рівнів. По-третє, за юридичною силою: ці інструменти формально залишаються добровільними і належать до «м'якого права», однак у контексті DSA набувають регуляторної ваги — насамперед тому, що участь у релевантних кодексах може враховуватися як захід мінімізації системних ризиків за ст. 35(1)(h), а відмова від такої участі може потребувати пояснення в контексті оцінки адекватності заходів мінімізації ризиків.

¹⁸⁷European Commission, 'Commission Investigates Grok and X's Recommender Systems under the Digital Services Act' (Press Release IP/26/203, 25 January 2026) https://ec.europa.eu/commission/presscorner/detail/en/ip_26_203

З огляду на спільність механізму статей 45–48 та їхню порівняну лаконічність, цей підрозділ, на відміну від попередніх, не структуровано за окремими статтями. Аналіз побудовано за чотирма функціональними блоками. Спочатку розкривається спільний механізм колективних інструментів — роль Комісії та Європейської ради з цифрових послуг, ключові показники ефективності, звітування та специфікації для окремих сфер. Далі аналізується практика застосування, насамперед трансформація добровільних кодексів, що передували DSA, у кодекси поведінки в межах його нормативної рамки. Третій блок присвячено головному аналітичному питанню підрозділу — амбівалентності добровільності, тобто тому, чи не перетворюється співрегуляторний підхід DSA на приховане розширення обов'язкового регулювання поза межами законодавчої процедури. Завершується підрозділ оцінкою співрегуляторного рівня. Суміжний інструмент — добровільні стандарти за ст. 44 DSA — залишається поза межами цього підрозділу, оскільки розроблення технічних стандартів європейськими організаціями стандартизації на запит Комісії відтворює класичну модель гармонізованої стандартизації, а не співрегулювання у розумінні, прийнятому в цьому дослідженні.

Регуляторна функція та передумови. Статті 45–48 DSA формують третій рівень триступеневої моделі регульованого саморегулювання та співрегулювання — власне співрегуляторний рівень колективних інструментів. Логіку його включення до Регламенту найкраще розкриває сама пропозиція Комісії¹⁸⁸ — там кодекси поведінки обґрунтовано як юридичну інституціоналізацію вже накопиченого добровільного досвіду: пропозиція прямо "враховує досвід, здобутий у саморегуляторних зусиллях, підтримуваних Комісією", — Кодексу поведінки щодо протидії незаконним висловлюванням ненависті 2016 р., Меморандуму про взаєморозуміння щодо продажу контрафактних товарів, Зобов'язання щодо

¹⁸⁸ Commission, 'Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC' COM(2020) 825 final, Explanatory Memorandum; Commission Recommendation (EU) 2018/334 of 1 March 2018 on measures to effectively tackle illegal content online C(2018) 1177 final.

безпеки продукції (Product Safety Pledge) та Інтернет-форуму ЄС (EU Internet Forum) щодо терористичного контенту, — і будується на Рекомендації Комісії щодо ефективної протидії незаконному контенту онлайн 2018 р. Комісія, отже, переносила під дах Регламенту практику, яка вже існувала, але мала слабкості, встановлені у підрозділі 1.2.4: відсутність санкцій, вибірковість участі та неможливість незалежної перевірки результатів¹⁸⁹.

Показово, що вже у 2020 р. Комісія окреслила траєкторію цієї інституціоналізації: меморандум зазначає, що правила про кодекси поведінки "могли б слугувати основою і бути доповненими переглянутим і посиленням Кодексом практики щодо дезінформації"¹⁹⁰ — план, який послідовно реалізовувався у посиленому Кодексі 2022 р. та його подальшій інтеграції у рамку DSA. Структурно пропозиція розмістила ці механізми серед "трансверсальних положень" щодо обов'язків належної обачності: колективні інструменти замислені як наскрізні механізми, що обслуговують застосування всього Регламенту. Кризові протоколи отримали окреме обґрунтування — реагування на "надзвичайні обставини, що зачіпають громадську безпеку або громадське здоров'я", у чому легко впізнати пандемічний контекст розроблення пропозиції. Фінальний текст DSA цю конструкцію зберіг і розширив: додано кодекси доступності (ст. 47), посилено роль Європейської ради з цифрових послуг та деталізовано вимоги до цілей і звітування за кодексами.

Логіка Комісії, таким чином, двоскладова. З одного боку, індивідуальні обов'язки окремих платформ, навіть у поєднанні з аудитом, доступом до даних і публічною звітністю, залишаються обмеженими щодо проблем міжплатформного, технічно складного або кризового характеру: поширення дезінформації, прозорість

¹⁸⁹ Commission, 'Assessment of the Code of Practice on Disinformation' SWD(2020) 180 final (див. підрозділ 1.2.4)

¹⁹⁰ Commission, 'Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC' COM(2020) 825 final, Explanatory Memorandum; Commission Recommendation (EU) 2018/334 of 1 March 2018 on measures to effectively tackle illegal content online C(2018) 1177 final.

онлайн-реклами, захист неповнолітніх, доступність сервісів і кризове реагування потребують узгодження практик між платформами, регуляторами, громадянським суспільством та експертною спільнотою. З іншого боку, досвід добровільних кодексів до DSA довів, що без публічно-правових вимог — цілей, показників, моніторингу — такі інструменти забезпечують лише часткову участь і залишають результати неперевірюваними. Статті 45–48 відповідають на обидві проблеми одночасно.

Механізм колективних інструментів. Загальні засади встановлює ст. 45 DSA: Комісія та Європейська рада з цифрових послуг заохочують і сприяють розробленню кодексів поведінки на рівні Союзу, які мають робити внесок у належне застосування Регламенту — з урахуванням, зокрема, викликів протидії різним видам незаконного контенту і системним ризикам. Конструкція статті визначає розподіл ролей. Ініціативна функція належить публічним інституціям: якщо виникає значний системний ризик у розумінні ст. 34(1), що стосується кількох VLOPs/VLOSEs, Комісія може запросити відповідних провайдерів та інших суб'єктів до участі у розробленні кодексу, включно з формулюванням зобов'язань щодо заходів мінімізації ризиків. Нормотворча функція залишається за учасниками: зміст зобов'язань виробляють самі провайдери разом з іншими стейкхолдерами — організаціями громадянського суспільства, а за потреби й іншими зацікавленими сторонами. Контрольна функція знову публічна: кодекси мають чітко визначати цілі, містити ключові показники ефективності для вимірювання їх досягнення та передбачати регулярне звітування учасників перед Комісією і Радою; Комісія і Рада оцінюють, чи відповідають кодекси своїм цілям, здійснюють моніторинг їх виконання і можуть запропонувати перегляд кодексу, а в разі систематичного невиконання — вжити відповідних заходів. Ця тричленна структура — публічна ініціатива, приватне наповнення, публічна оцінка — точно відтворює формулу співрегулювання, виведену у підрозділі 1.2.1: публічні цілі, реалізовані приватними засобами.

Статті 46 і 47 конкретизують ці вимоги для двох сфер. Кодекси щодо онлайн-реклами (ст. 46) спрямовані на посилення прозорості рекламного ланцюга понад вимоги ст. 26 і 39 — з огляду на те, що між розміщенням реклами та її показом стоїть багатоланкова посередницька інфраструктура, непрозорість якої перешкоджає і виконанню індивідуальних обов'язків платформ. Кодекси доступності (ст. 47) мають забезпечити повну та ефективну рівноправну участь осіб з інвалідністю через доступність сервісів відповідно до вимог Директиви (ЄС) 2019/882. В обох випадках механізм ідентичний ст. 45; специфікація стосується предмета і кола залучених суб'єктів.

Кризові протоколи за ст. 48 стоять окремо за призначенням, але відтворюють ту саму логіку. Рада може рекомендувати Комісії ініціювати розроблення добровільних кризових протоколів для реагування на кризові ситуації — надзвичайні обставини, що зачіпають громадську безпеку або громадське здоров'я. Протоколи визначають координацію дій провайдерів у кризі: помітне інформування про кризову ситуацію, призначення відповідальних осіб, адаптацію ресурсів модерації. Регламент прямо застерігає, що заходи за протоколами не повинні розумітися як загальний обов'язок моніторингу і мають бути суворо обмежені в часі тривалістю кризи. Функціонально ст. 48 є колективним доповненням до індивідуального кризового механізму ст. 36, який дозволяє Комісії вимагати від окремих VLOPs/VLOSEs кризових заходів: ст. 36 — вертикальний примусовий інструмент, ст. 48 — горизонтальний добровільний.

Спільний знаменник чотирьох статей — юридична конструкція "структурованої добровільності". Жодна з них не зобов'язує жодного провайдера підписати жоден кодекс; водночас кожна вбудовує добровільний інструмент у публічний цикл: ініціювання, вимоги до змісту (цілі, KPI), моніторинг, оцінка, реагування на невиконання. Саме ця конструкція відрізняє кодекси за DSA від їхніх добровільних попередників — і саме вона породжує головне аналітичне питання підрозділу, до якого ми повернемося після огляду практики.

Траєкторія, окреслена Комісією ще у пропозиції 2020 р., реалізувалася у 2025 р. наступним чином: 20 січня 2025 р. Комісія і Європейська рада з цифрових послуг схвалили інтеграцію Кодексу поведінки щодо протидії незаконним висловлюванням ненависті онлайн¹⁹¹ (наступника Кодексу 2016 р.) у механізм DSA — це перший кодекс, визнаний за ст. 45¹⁹¹; 13 лютого 2025 р. аналогічну процедуру пройшов Кодекс практики щодо дезінформації: за поданням підписантів (зокрема Google, Meta, Microsoft і TikTok) Комісія і Рада ухвалили позитивні висновки про відповідність Кодексу критеріям ст. 45 і схвалили його перетворення на Кодекс поведінки в межах DSA з 1 липня 2025 р.¹⁹². Показово, що текст Кодексу при цьому залишився практично незмінним порівняно з версією 2022 р.¹⁹³. Таким чином, зобов'язання Кодексу стали предметом незалежного аудиту: з 1 липня 2025 р. виконання Кодексу підписантами-VLOPs/VLOSEs перевіряється у межах щорічного аудиту за ст. 37. По-друге, Кодекс став "релевантним орієнтиром" оцінки відповідності DSA: повне дотримання Кодексу може розглядатися як належний захід мінімізації ризиків за ст. 35(1)(h) для підписантів. По-третє, моніторинг і оцінку досягнення цілей Кодексу здійснюють Комісія і Рада за ст. 45(4), а звітування відбувається через публічний Transparency Centre — перший цикл звітів у новому режимі охопив період з 1 липня по 31 грудня 2025 р. Сам Кодекс у редакції 2022 р. уже містив елементи, яких вимагає ст. 45(3): 43 зобов'язання і 128 конкретних заходів у сферах демонетизації дезінформації, прозорості політичної реклами, цілісності сервісів, розширення можливостей

¹⁹¹ European Commission, 'Code of Conduct on Countering Illegal Hate Speech Online+' (20 January 2025) <https://digital-strategy.ec.europa.eu/en/library/code-conduct-countering-illegal-hate-speech-online>

¹⁹² European Commission, 'Commission Endorses the Integration of the Voluntary Code of Practice on Disinformation into the Digital Services Act' (13 February 2025) <https://digital-strategy.ec.europa.eu/en/news/commission-endorses-integration-voluntary-code-practice-disinformation-digital-services-act>

¹⁹³ Transparency Centre, 'Code of Practice on Disinformation' <https://disinfocode.eu/>; проблематику трансформації кодексів поведінки під публічно-правовим впливом мною було досліджено окремо, див. Геннадій Щербак 'Регулювання саморегулювання: кодекси поведінки у системі цифрового врядування ЄС' (2026) 3(57) *Наука і техніка сьогодні* 417 [https://doi.org/10.52058/2786-6025-2026-3\(57\)-417-437](https://doi.org/10.52058/2786-6025-2026-3(57)-417-437)

користувачів і дослідників, з ключовими показниками ефективності, постійною робочою групою і системою швидкого реагування для виборчих періодів¹⁹⁴. Порівняння з докодексовою практикою підтверджує еволюцію положень Кодексу. Кодекс практики 2018 р. — той самий інструмент, недоліки якого Комісія зафіксувала у SWD(2020) 180: самооцінювання без верифікації, відсутність показників, вибіркова участь (підрозділ 1.2.4). Посилена редакція 2022 р. додала КРІ і звітність; конверсія 2025 р. додала зовнішній аудит, публічний моніторинг і зв'язок із системою обов'язків DSA. Той самий предмет регулювання за сім років пройшов шлях від автономного саморегулювання через структуровану добровільність до інструмента, вбудованого у вимоги DSA¹⁹⁵. Водночас практика загострила і питання меж добровільності. Формально невиконання Кодексу саме по собі не є автоматичним порушенням DSA, а підписання Кодексу не є обов'язком. Однак сукупність правових зв'язків — врахування участі за ст. 35(1)(h), застереження в преамбулі DSA про те, що відмова від запрошення Комісії до участі в Кодексі "без належних пояснень" може братися до уваги при встановленні порушення Регламенту, аудитуваність зобов'язань і публічний моніторинг — робить вихід із Кодексу або відмову від участі регуляторно значущими та такими, що можуть потребувати пояснення в контексті оцінки адекватності заходів мінімізації ризиків. Так, у січні 2025 р. Meta оголосила про згортання програми фактчекінгу: коментатори одразу зазначили, що імплементація таких змін у ЄС вимагатиме ретельної зв'язки з обома кодексами, інакше підписант ризикує посиленою увагою за DSA¹⁹⁶.

¹⁹⁴ The 2022 Code of Practice on Disinformation <https://disinfocode.eu/the-code/>

¹⁹⁵ Геннадій Щербак 'Регулювання саморегулювання: кодекси поведінки у системі цифрового врядування ЄС' (2026) 3(57) Наука і техніка сьогодні 417 [https://doi.org/10.52058/2786-6025-2026-3\(57\)-417-437](https://doi.org/10.52058/2786-6025-2026-3(57)-417-437)

¹⁹⁶ Center for Countering Digital Hate, 'How Will Meta's Policy Changes Affect European Users?' (8 January 2025) <https://counterhate.com/blog/how-will-metas-policy-changes-affect-european-users/>

Конструкція статей 45–48 DSA породжує питання, центральне для оцінки всього співрегуляторного рівня: чи залишаються кодекси поведінки добровільними інструментами по суті, а не лише за формою. Юридично відповідь є відносно однозначною: жоден провайдер не зобов'язаний підписувати кодекс, а невиконання кодексу саме по собі не становить автоматичного порушення Регламенту. Функціонально ж картина складніша, оскільки добровільність кодексів обмежується чотирма аспектами.

За ст. 35(1)(h) DSA участь у релевантних кодексах названа серед можливих заходів мінімізації системних ризиків. Для VLOP/VLOSE, зобов'язаного за ст. 35 вживати розумних, пропорційних та ефективних заходів, кодекс стає одним із найбільш очевидних і регуляторно визнаних способів продемонструвати виконання цього обов'язку — готовим, публічно схваленим пакетом заходів. У свою чергу пункт 104 преамбули зазначає, що відмова від запрошення Комісії до участі в кодексі без належних пояснень може братися до уваги при встановленні порушення Регламенту. Крім цього, зобов'язання за кодексом входять до предмета щорічного незалежного аудиту за ст. 37(1)(b), а отже, формально добровільні зобов'язання перевіряються тим самим механізмом, що й імперативні обов'язки DSA. Нарешті – публічний моніторинг Комісії та Європейської ради з цифрових послуг за ст. 45(4), включно з можливістю запропонувати перегляд кодексу і реагувати на його систематичне невиконання. У сукупності ці аспекти означають, що для найбільших платформ вартість неучасті або виходу з кодексу вимірюється не лише репутаційними наслідками, як у класичному саморегулюванні, а й регуляторним ризиком: неучасть створює прогалину в доказуванні виконання ст. 35, яку платформа муситиме заповнити власними, ще не валідованими заходами та пояснити регулятору¹⁹⁷.

¹⁹⁷ Rachel Griffin and Carl Vander Maelen, 'Codes of Conduct in the Digital Services Act: Exploring the Opportunities and Challenges' (2024) *Technology and Regulation* 167 <https://doi.org/10.26116/techreg.2024.016>

У доктрині ця конструкція отримала полярні оцінки. Критичний погляд кваліфікує її як ризик обходу законодавчої процедури: зобов'язання, які не були безпосередньо ухвалені законодавцем як імперативні приписи, набувають квазізобов'язкової сили через адміністративний тиск Комісії — причому у сферах, що безпосередньо зачіпають свободу вираження поглядів¹⁹⁸. Це особливо чутливо щодо дезінформації, яка як така не обов'язково є незаконним контентом, однак через кодекси може ставати предметом системної модераційної політики. За цією логікою співрегуляторний контур створює ризик “тіньової нормотворчості”: м'яке право із твердими наслідками, вироблене у переговорах між Комісією, платформами та іншими стейкхолдерами без повного набору гарантій законодавчого процесу.

Прихильний погляд, навпаки, виходить із того, що саме ця конструкція і становить сутність співрегулювання¹⁹⁹. Цілі визначені законодавцем у самому DSA, насамперед у статтях 34–35; кодекси лише конкретизують шляхи їх досягнення у технічно складних і швидкозмінних сферах. Участь платформ у виробленні зобов'язань забезпечує технічну реалістичність, якої не могла б дати надмірно деталізована імперативна норма, а моніторинг, аудит і публічна звітність відрізняють цю модель від слабкої добровільності, характерної для докодексового етапу. У цьому сенсі кодекси можуть розглядатися як легітимний інструмент динамічної конкретизації рамкових обов'язків DSA.

Механізм статей 45–48 сам по собі відповідає критеріям правомірного співрегулювання: публічні цілі встановлені законодавчим актом; приватна участь у конкретизації залишається формально добровільною; результат підлягає публічній оцінці, моніторингу та, для VLOPs/VLOSEs, аудиту. Проблема виникає на рівні тиску — там, де запрошення Комісії до участі фактично перестає бути

¹⁹⁸ Carl Vander Maelen, ‘Soft Law, Hardcore? The DSA’s Co-Regulatory Mechanisms and the Legitimacy of Platform Regulation’ (Verfassungsblog, 3 June 2024) <https://verfassungsblog.de/soft-law-dsa-co-regulation/>

¹⁹⁹ Martin Husovec, ‘The DSA as a Co-regulatory System’ in Martin Husovec, *Principles of the Digital Services Act* (Oxford University Press 2024) ch 20.

запрошенням. Ступінь цього тиску залежатиме від правозастосовної практики. Якщо Комісія трактуватиме неучасть у кодексі як самостійну ознаку невиконання ст. 35, добровільність стане фікцією. Якщо ж неучасть, компенсована власними ефективними, пропорційними й належно обґрунтованими заходами платформи, визнаватиметься рівноцінною, конструкція збереже співрегуляторний характер.

Іншими словами, межа між співрегулюванням і прихованим обов’язковим регулюванням у DSA не повністю проведена текстом Регламенту; вона проводитиметься практикою Комісії, аудиторам, реакцією Європейської ради з цифрових послуг і поведінкою самих платформ. Перші інтеграції кодексів у 2025 р., а також реакція на кейси на кшталт зміни Meta підходу до фактчекінгу, стануть першими тестами цієї межі²⁰⁰. Для цієї дисертації звідси впливає важливий висновок: колективні інструменти DSA можуть залишатися формою співрегулювання, але за певної правозастосовної практики здатні наблизитися до де-факто обов’язкового регулювання без формальної зміни тексту Регламенту.

Висновки до розділу 3

Нормативний аналіз DSA підтвердив центральну тезу дисертації на рівні конкретних механізмів: Регламент зберігає приватну нормотворчість і приватне правозастосування онлайн-платформ, підпорядковуючи кожен елемент цього циклу публічно-правовим стандартам. Застосована до всіх досліджених статей методологія аналізу — який елемент приватної автономії зберігається, які публічно-правові вимоги запроваджені, який суб’єкт і в якій процедурі перевіряє дотримання — показала, що механізми DSA не заміщують платформну автономію прямим державним адмініструванням, але й не залишають її поза юридичним впорядкуванням.

²⁰⁰ Alvaro Oleart and Luis Bouza García, ‘From Self to Co-regulation in the EU’s Approach to Disinformation: The Framing Power of Big Tech Business Lobbies in the Lead to the Digital Services Act’ (2025) *International Review of Public Policy* 235 <https://doi.org/10.4000/14rse>

Обґрунтовано триступеневу модель регульованого саморегулювання та співрегулювання у DSA. Базовий процедурний рівень, закріплений у статтях 14, 16, 17, 20 і 21, юридично впорядковує повний цикл саморегулятивної діяльності платформи: форму приватної нормотворчості — прозорість умов користування і загальний стандарт їх застосування за ст. 14(4); процедуру первинного правозастосування — notice-and-action за ст. 16 і мотивування за ст. 17; контроль за таким правозастосуванням — внутрішній перегляд і позасудове оскарження за статтями 20–21. У сукупності ці статті формують функціональний аналог належної процедури у приватному платформному середовищі, у якому кожна наступна ланка компенсує структурну слабкість попередньої: мотивування робить можливим оскарження, внутрішній перегляд пом'якшує помилки первинного рішення, а позасудовий механізм відповідає на конфлікт інтересів самоперегляду.

Посилений ризик-орієнтований рівень для VLOPs/VLOSEs поєднує дві взаємодоповнювані регуляторні техніки. Статті 34–35 і 41 реалізують метарегулювання: право визначає не кожне конкретне рішення платформи, а архітектуру його підготовки, оцінювання та контролю — обов'язковість, періодичність і категоріальну рамку оцінки системних ризиків, стандарт якості заходів мінімізації, внутрішню комплаєнс-функцію. Статті 37, 40 і 42 утворюють тришаровий контур зовнішньої верифікації: професійну перевірку через незалежний аудит, кваліфікований доступ до даних для регуляторів і перевірених дослідників, а також публічний контроль через посилену звітність.

Співрегуляторний рівень, передбачений статтями 45–48 DSA, відрізняється від перших двох за критерієм, сформульованим у підрозділі 1.2.1: приватне нормотворення тут є інструментом реалізації публічно визначених цілей. Аналіз пропозиції Комісії та практики інтеграцій 2025 р. — Кодексу поведінки щодо протидії незаконним висловлюванням ненависті онлайн+ та Кодексу поведінки щодо дезінформації — показав, що DSA інституціоналізував добровільний досвід попереднього десятиліття, додавши до нього публічний цикл: ініціювання, вимоги до цілей і показників, моніторинг, аудитованість зобов'язань. Водночас сукупність

правових зв'язків — ст. 35(1)(h), пункт 104 преамбули, аудит за ст. 37 — робить добровільність цих інструментів амбівалентною: межа між співрегулюванням і де-факто обов'язковим регулюванням не проведена текстом Регламенту остаточно і проводитиметься правозастосовною практикою Комісії.

Оцінка ефективності механізмів на основі першого циклу правозастосування 2024–2026 рр. є диференційованою. Як інструмент видимості та формалізації DSA вже працює: платформи ідентифікують ризики, мотивують рішення, проходять аудит, публікують звіти, а виклади підстав і звітність утворили безпрецедентний масив публічних даних про приватне правозастосування. Як інструмент доказового контролю реального зменшення ризиків модель поки що обмежена: перші звіти про системні ризики продемонстрували різноманітність методологій і недооцінку дизайн-зумовлених ризиків; перші аудити — переважання процедурної перевірки над змістовною оцінкою ефективності заходів; механізм доступу дослідників лише формується. Спільний знаменник цих обмежень — залежність ланок верифікації від даних і пояснень, наданих самими платформами.

Водночас динаміка правозастосування свідчить, що конструкція DSA продовжує розвиватися. Передбачені ст. 35(2) узагальнювальні звіти Європейської ради з цифрових послуг у співпраці з Комісією мають значення не лише як інструмент опису ризиків, а як спосіб порівняння практик різних VLOPs/VLOSEs: вони дозволяють виявляти повторювані системні ризики, типові слабкі місця ризик-менеджменту та підходи, які можуть розглядатися як кращі практики мінімізації ризиків. Розслідування Комісії, включно з провадженням щодо інтеграції Grok у сервіс X за статтями 34, 35 і 42, показують, що оцінка ризиків має здійснюватися не лише періодично, а й до запровадження функціональностей, здатних істотно змінити ризиковий профіль сервісу, а звітність використовується як інструмент нагляду. Інтеграція кодексів поведінки у рамку DSA, своєю чергою, робить формально добровільні зобов'язання аудитованими та регуляторно значущими. Отже, модель регульованого саморегулювання у DSA вже сформована на нормативному та інституційному рівнях, але її практична ефективність ще

перевіряється: остаточна оцінка залежатиме від того, чи зможе публічний нагляд регулярно перевіряти не лише документи платформ, а й реальну дієвість їхніх процедур, оцінок ризиків і заходів мінімізації.

Для теоретичних висновків дисертації цей розділ пропонує два уточнення. По-перше, регульоване саморегулювання в DSA не є однорідною технікою: воно реалізується щонайменше у трьох модусах — процедуризації індивідуальних рішень, метарегулюванні систем і структуруванні колективної добровільності. Ці модуси розрізняються за предметом публічного впливу, але підпорядковані єдиній логіці інституціоналізованої підзвітності. По-друге, межі між рівнями моделі є динамічними: колективні інструменти можуть наближатися до де-факто обов'язкових стандартів без формальної зміни норм, а ефективність базового рівня для користувача залежить від механізмів посиленого рівня.

У DSA можна виокремити три рівні регульованого саморегулювання та співрегулювання: базовий процедурний рівень платформного саморегулювання, юридично впорядкований статтями 14, 16, 17, 20 і 21; посилений ризик-орієнтований рівень для VLOPs/VLOSEs, закріплений у статтях 34, 35 і 41, що відображають метарегулювання внутрішніх систем управління, а також у статтях 37, 40 і 42, які забезпечують зовнішню верифікацію та підзвітність; і власне співрегуляторний рівень колективних інструментів, передбачений статтями 45–48. Стаття 22 DSA щодо *trusted flaggers* має проміжний характер, оскільки поєднує платформний механізм *notice-and-action* із залученням до правозастосування зовнішніх суб'єктів, сертифікованих координатором цифрових послуг.

ВИСНОВКИ

У дисертації здійснено теоретичне узагальнення та запропоновано розв'язання наукової проблеми, що полягає в обґрунтуванні цілісної теоретико-правової концепції саморегулювання онлайн-платформ у праві Європейського Союзу. Проведене дослідження дало підстави сформулювати такі висновки.

1. Онлайн-платформи є особливим об'єктом правового регулювання, оскільки одночасно виконують функції технологічного посередника, організатора багатостороннього ринку, інфраструктури публічної комунікації та приватного регулятора. Їхня правова природа не може бути зведена до надання технічної послуги або договірних відносин із користувачами. Через умови користування, стандарти спільноти, політики модерації, рекомендаційні системи та технічну архітектуру платформи встановлюють правила поведінки, визначають умови доступу до аудиторії та інформації, застосовують санкції й організовують процедури перегляду власних рішень.

2. Економічна природа платформних ринків посилює регуляторну владу онлайн-платформ. Мережеві ефекти, економія на масштабі, накопичення даних, ефекти блокування користувачів, контроль над доступом до аудиторії та інформаційна асиметрія створюють структурну нерівність між платформою та користувачем. У межах економіки уваги комерційні стимули платформи можуть не збігатися з публічними інтересами щодо захисту основоположних прав, недопущення маніпулятивних практик, забезпечення якості публічної комунікації та захисту неповнолітніх. Це обмежує можливість покладатися на виключно добровільне саморегулювання.

3. Платформне саморегулювання має структурну специфіку порівняно з класичним галузевим або професійним саморегулюванням. У традиційній моделі члени певної професійної чи господарської спільноти встановлюють правила для власної діяльності. Онлайн-платформа, натомість, самостійно створює правила,

адресовані переважно третім особам — користувачам, бізнес-користувачам, продавцям, рекламодавцям і творцям контенту. Тому саморегулювання онлайн-платформ поєднує самоорганізацію цифрового сервісу з приватним управлінням поведінкою інших суб'єктів, що посилює проблему легітимності платформної нормотворчості.

4. Саморегулювання онлайн-платформ запропоновано розуміти як сукупність правил, процедур, організаційних рішень і механізмів контролю, які платформа самостійно створює та застосовує для впорядкування функціонування власного сервісу, поведінки користувачів, модерації контенту, видимості інформації та використання алгоритмічних систем. Регульоване саморегулювання онлайн-платформ становить модель, у якій така приватна нормотворчість і внутрішнє правозастосування зберігаються, але підпорядковуються обов'язковим вимогам щодо прозорості, добросовісності, пропорційності, процедурної справедливості, підзвітності та зовнішнього контролю.

5. Умови користування онлайн-платформ мають подвійну правову природу. За юридичною формою вони є умовами договору приєднання між платформою та користувачем. За своєю функцією вони виступають актами приватного регулювання, оскільки встановлюють загальні правила поведінки для невизначеного кола осіб, визначають межі допустимого контенту, підстави застосування обмежень і умови доступу до суспільно значущої цифрової інфраструктури. Саме функціональна регуляторна природа цих актів обґрунтовує поширення на них не лише механізмів договірного права, а й публічно-правових вимог щодо прозорості, пропорційності, недискримінаційності та врахування основоположних прав.

6. Теоретично точна характеристика DSA потребує розмежування кількох взаємопов'язаних регуляторних концепцій. Реагувальне регулювання пояснює стратегію зміни інтенсивності регуляторного втручання залежно від поведінки суб'єкта, масштабу його діяльності та рівня ризиків. Метарегулювання визначає предмет правового впливу — внутрішні системи управління, оцінювання ризиків, комплаєнсу, контролю та звітності. Децентроване регулювання пояснює

розподіл регуляторних функцій між державними органами, платформами, аудиторамі, дослідниками, органами позасудового вирішення спорів, громадянським суспільством і користувачами. Регульоване саморегулювання характеризує загальне співвідношення приватної нормотворчості платформ із публічно-правовими вимогами.

7. Сформульовано критерій розмежування регульованого саморегулювання та співрегулювання за походженням і функцією приватних правил. У співрегулюванні приватне нормотворення виникає як засіб реалізації публічно визначених цілей і здійснюється в межах публічного мандата. У регульованому саморегулюванні приватні правила формуються платформою самостійно з огляду на її організаційні, договірні та комерційні потреби, а право впорядковує, обмежує і контролює вже наявну приватну нормотворчість, не делегуючи повноважень на її створення.

8. Порівняльно-правовий аналіз американської, китайської та європейської моделей регулювання онлайн-платформ, здійснений за критеріями джерела нормотворчості, механізму підзвітності та захисту фундаментальних прав, засвідчив відмінність їхніх регуляторних і ціннісних засад. Американський підхід історично надає перевагу свободі вираження поглядів, інноваціям, обмеженій відповідальності посередників і широкій приватній автономії платформ. Китайська модель ґрунтується на централізованому державному контролі, пріоритеті державного суверенітету, інформаційної та національної безпеки. Європейська модель сформувалася як самостійна конструкція, орієнтована на баланс основоположних прав, свободи підприємництва, безпеки користувачів та публічного інтересу. DSA займає проміжне місце між автономним саморегулюванням і державно-центричним імперативним регулюванням, приділяючи значну увагу забезпеченню фундаментальних прав людини.

9. DSA не усуває приватну регуляторну владу онлайн-платформ і не замінює платформні правила вичерпними публічно-правовими вимогами щодо допустимого контенту. Його концептуальна новизна полягає у трансформації автономного платформного саморегулювання в юридично впорядковану систему.

Приватна нормотворчість, модерація контенту, внутрішні процедури та системи управління ризиками інтегруються у публічно-правову рамку через процедурні вимоги, обов'язки прозорості, зовнішню верифікацію, інституційний нагляд і механізми відповідальності.

10. У DSA виокремлено три рівні регульованого саморегулювання та співрегулювання. Перший становить базовий процедурний рівень, закріплений у статтях 14, 16, 17, 20 і 21 DSA. Другий охоплює посилений ризик-орієнтований режим для дуже великих онлайн-платформ і дуже великих онлайн-пошукових систем, у якому статті 34, 35 і 41 реалізують метарегуляторний вплив на внутрішні системи управління, а статті 37, 40 і 42 забезпечують зовнішню перевірку та підзвітність. Третій рівень утворюють колективні співрегуляторні інструменти, передбачені статтями 45–48 DSA.

11. Базовий процедурний рівень юридично впорядковує способи створення та застосування правил платформи. Стаття 14 DSA встановлює вимоги до прозорості умов користування та підпорядковує застосування приватних обмежень критеріям сумлінності, об'єктивності, пропорційності й належного врахування основоположних прав. Статті 16 і 17 регулюють процедуру отримання повідомлень та обґрунтування модераційних рішень. Статті 20 і 21 створюють внутрішній та зовнішній рівні перегляду рішень платформи. У сукупності ці положення трансформують модерацію контенту з внутрішньої корпоративної практики у приватне правозастосування, підпорядковане публічно-правовим стандартам.

12. Внутрішні системи розгляду скарг мають значення як первинний механізм самоконтролю платформи, проте їхня ефективність обмежена тим, що платформа одночасно встановлює правила, ухвалює первинне рішення та переглядає його. Позасудове вирішення спорів зменшує цей конфлікт інтересів завдяки залученню сертифікованого зовнішнього органу. Водночас необов'язковий характер його рішень і відсутність уніфікованих мінімальних стандартів мотивування не дозволяють розглядати цей механізм як повноцінну заміну судового захисту.

13. Ризик-орієнтований рівень є найбільш виразним проявом метарегулювання в DSA. Регламент покладає на VLOPs та VLOSEs обов'язок самостійно виявляти, оцінювати та мінімізувати системні ризики, пов'язані з незаконним контентом, основоположними правами, виборчими процесами, громадянським дискурсом, захистом неповнолітніх, громадською безпекою та добробутом користувачів. Право регулює не кожне окреме рішення платформи, а архітектуру її внутрішнього управління: методологію оцінювання, вибір заходів мінімізації, організацію комплаєнсу, документування та здатність обґрунтувати ефективність ужитих заходів.

14. Зовнішня верифікація є необхідною умовою перетворення платформного саморегулювання на підзвітну модель. Незалежний аудит, доступ дослідників до даних, звітність і наглядові повноваження Європейської Комісії та координаторів цифрових послуг мають компенсувати інформаційну асиметрію між платформами та зовнішніми суб'єктами. Водночас перша практика застосування DSA виявляє ризики формалізації аудиту, залежності аудиторів від інформації платформи, недостатньої порівнюваності звітів, надмірного вилучення інформації з публічних версій документів і складності незалежної перевірки заявленої ефективності заходів.

15. Кодекси поведінки, кодекси щодо онлайн-реклами, кодекси доступності та кризові протоколи становлять власне співрегуляторний рівень DSA. Вони забезпечують колективне вироблення стандартів за участю платформ, інституцій ЄС та інших зацікавлених сторін. Їхня добровільність має амбівалентний характер: формально приєднання до таких інструментів залишається добровільним, проте зв'язок кодексів із заходами мінімізації системних ризиків, очікуваннями Комісії, аудитом і оцінюванням належного виконання обов'язків може надавати відповідним зобов'язанням де-факто обов'язкової регуляторної ваги.

16. Регульоване саморегулювання, закріплене в DSA, не є цілком новою технікою права Європейського Союзу. Воно розвиває підходи, раніше використані у праві захисту прав споживачів, захисту персональних даних, регулюванні медіа

та сфери телекомунікацій. DSA систематизує і поширює на платформне середовище стандарти прозорості, добросовісності, пропорційності, процедурної справедливості, оцінювання ризиків і зовнішньої підзвітності, які раніше формувалися фрагментарно у законодавстві та національній судовій практиці.

17. Регульоване саморегулювання в DSA реалізується на трьох взаємопов'язаних рівнях: процедуризації індивідуальних платформних рішень, метарегулюванні внутрішніх систем управління та структуруванні колективної добровільності. Ці модули відрізняються предметом і способом публічного впливу, але підпорядковані спільній меті — інституціоналізації підзвітності приватної регуляторної влади платформ. Межі між ними є динамічними: співрегуляторні інструменти можуть набувати фактично обов'язкового значення, а ефективність індивідуальних процедур захисту користувачів залежить від належного функціонування системних механізмів аудиту, доступу до даних і публічного нагляду.

18. Ефективність моделі DSA залежить від її реалізації, а не лише від нормативної конструкції. Формальна наявність політики модерації, системи скарг, аудиту або оцінки ризиків не гарантує належної підзвітності. Визначальними є якість мотивування рішень, реальна незалежність зовнішніх органів, доступність даних, можливість перевірки результатів, належна участь громадянського суспільства та спроможність Комісії і національних координаторів застосовувати наглядові й примусові повноваження.

19. Запропонована концепція дозволяє визначити DSA як багаторівневу модель регульованого саморегулювання онлайн-платформ, доповнену співрегуляторними, метарегуляторними та реагувальними механізмами. Її зміст полягає у збереженні технологічної, організаційної та нормотворчої спроможності платформ за одночасного встановлення правових меж її здійснення. Держава та інституції ЄС не перебирають на себе повне управління цифровим середовищем, але визначають цілі, процедури, критерії належності, механізми контролю та наслідки неналежного здійснення приватної регуляторної влади.

20. Загальний результат дослідження полягає в обґрунтуванні того, що саморегулювання онлайн-платформ у праві Європейського Союзу більше не може розглядатися як сфера виключної договірної автономії або добровільної корпоративної політики. У системі DSA воно набуває юридично впорядкованого характеру і стає елементом публічного управління цифровим середовищем. Така модель спрямована на забезпечення балансу між свободою підприємницької діяльності платформ, технологічною гнучкістю, захистом основоположних прав користувачів, відкритістю інформаційного середовища та належним функціонуванням демократичних процесів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бабаджанян Г. Б. Правове забезпечення саморегулювання господарсько-торговельної діяльності : дис. ... д-ра філософії : 081 Право. Київ : Державний торговельно-економічний університет, 2024. 230 с.
2. Геннадій Щербак 'Регулювання саморегулювання: кодекси поведінки у системі цифрового врядування ЄС' (2026) 3(57) Наука і техніка сьогодні 417 [https://doi.org/10.52058/2786-6025-2026-3\(57\)-417-437](https://doi.org/10.52058/2786-6025-2026-3(57)-417-437)
3. Гончаренко О. Види саморегулювання господарської діяльності. Підприємництво, господарство і право. 2016. № 11. С. 68–72. URL: <http://pgp-journal.kiev.ua/archive/2016/11/15.pdf>
4. Гончаренко О. М. Теоретико-правові засади саморегулювання господарської діяльності : дис. ... д-ра юрид. наук : 12.00.04. Київ, 2020.
5. Закон України «Про ринки капіталу та організовані товарні ринки» від 23 лютого 2006 р. № 3480-IV, ст. 143–144 <<https://zakon.rada.gov.ua/go/3480-15>>
6. Мазаракі Н, Жибак А, 'Зобов'язання гейткіперів, закріплені в Акті про цифрові ринки' (2024) 137(6) Ius Modernum 4 [https://doi.org/10.31617/3.2024\(137\)01](https://doi.org/10.31617/3.2024(137)01)
7. Наталія Мазаракі, Володимир Примак 'Механізм вирішення спорів між користувачами та онлайн-платформами в Акті ЄС про цифрові послуги' (2026) 19 Український політико-правовий дискурс <https://doi.org/10.5281/zenodo.18662891>
8. Примак В Д, Нескороджена Л Л, 'Основоположні права у цифровому середовищі: практика Суду Європейського Союзу' (2025) 11 Юридичний науковий електронний журнал 97 <https://doi.org/10.32782/2524-0374/2025-11/19>.
9. Тезаурус EUROVOC, 'Саморегулювання' (Законодавство України, Верховна Рада України) <<https://zakon.rada.gov.ua/laws/euro/6367>>
10. Філатова Н Ю, Саморегулівні організації як суб'єкти цивільного права (дис канд юрид наук, Національний юридичний університет імені Ярослава Мудрого, 2014).
11. Філатова-Білоус Н. Саморегулівні організації: юридичні особи на межі приватного і публічного права. Цивілістична платформа. 2024. № 2. С. 58-82. <https://doi.org/10.69724/2786-8834-2024-2-2-58-82> С. 76
12. 47 U.S. Code § 230 – Protection for private blocking and screening of offensive material (1996). <https://www.law.cornell.edu/uscode/text/47/230>
13. Access Now, Protecting Free Expression in the Era of Online Content Moderation: Preliminary Recommendations on Content Moderation and Facebook's Planned Oversight Board (Access Now 2019). <https://www.accessnow.org/wp-content/uploads/2019/05/AccessNow-Preliminary-Recommendations-On-Content-Moderation-and-Facebooks-Planned-Oversight-Board.pdf> (дата звернення 20 травня 2026 року)

14. Al Jazeera. (2021). Which online platforms banned Trump over Capitol riot? <https://www.aljazeera.com/news/2021/1/14/which-online-platforms-banned-trump-over-capitol-riot> (дата звернення 20 травня 2026 року)
15. Aleksandra Kuczerawy, 'Remedying Overremoval' (Verfassungsblog, 3 November 2022) <https://verfassungsblog.de/remedying-overremoval/>
16. Aleksandra Kuczerawy, 'Intermediary Liability & Freedom of Expression: Recent Developments in the EU Notice & Action Initiative' (2015) 31 Computer Law & Security Review 46.
17. Alvaro Oleart and Luis Bouza García, 'From Self to Co-regulation in the EU's Approach to Disinformation: The Framing Power of Big Tech Business Lobbies in the Lead to the Digital Services Act' (2025) International Review of Public Policy 235 <https://doi.org/10.4000/14rse>
18. Amaury Trujillo, Benedetta Tessa and Stefano Cresci, 'Disarranged Harmonization of Transparency Reporting by Social Media Platforms Under the Digital Services Act' (arXiv, 17 May 2026) <https://arxiv.org/abs/2605.17655>
19. Anthony Ogus, Regulation: Legal Form and Economic Theory (Hart Publishing 2004).
20. Anu Bradford, 'The False Choice Between Digital Regulation and Innovation' (2024) 118 Northwestern University Law Review 377.
21. Anu Bradford, Digital Empires: The Global Battle to Regulate Technology (Oxford University Press 2023).
22. ARTICLE 19, 'The Santa Clara Principles and the Push for Transparency' (8 December 2021). <https://www.article19.org/resources/international-santa-clara-principles-and-the-push-for-transparency/> (дата звернення 20 травня 2026 року).
23. Article 29 Working Party, 'Guidelines on Transparency under Regulation 2016/679' WP260 rev.01 (11 April 2018).
24. Balendra, S. (2024). Free Speech in the Puzzle of Content Regulation: Insights from the West and the Global South. Springer Nature Switzerland. C. 109
25. BBC. (2019). Trump threatens tariffs against "foolish" Macron. <https://www.bbc.com/news/world-us-canada-49131301> (дата звернення 15 травня 2026 року).
26. BBC. (2020). Twitter tags Trump tweet with fact-checking warning. <https://www.bbc.com/news/technology-52815552> (дата звернення 15 травня 2026 року).
27. Bernard Caillaud and Bruno Jullien, 'Chicken & Egg: Competition among Intermediation Service Providers' (2003) 34 RAND Journal of Economics 309.
28. Bernhard Georg Kern, Das Internet zwischen Regulierung und Selbstregulierung (doctoral dissertation, Humboldt-Universität zu Berlin 2009).
29. BEUC, The Digital Services Act Proposal: BEUC Position Paper (BEUC-X-2021-032, 9 April 2021).
30. BGH, Urteile vom 29.7.2021 – III ZR 179/20 und III ZR 192/20.

31. Bloomberg Law. (2024). Which States Have Consumer Data Privacy Laws? <https://pro.bloomberglaw.com/insights/privacy/state-privacy-legislation-tracker/#map-of-state-privacy-laws>
32. Booth, R. (2025). Meta to get rid of factcheckers and recommend more political content. The Guardian. <https://www.theguardian.com/technology/2025/jan/07/meta-facebook-instagram-threads-mark-zuckerberg-remove-fact-checkers-recommend-political-content>
33. Boyne, S. M. (2018). Data Protection in the United States. *The American Journal of Comparative Law*, (66), Supplement 1, 299–343. <https://www.scilit.com/publications/9cc47792af226bef0c996c5c21aec052> c. 318–321
34. California Consumer Privacy Act of 2018. (2018). https://coppa.ca.gov/regulations/pdf/ccpa_statute.pdf
35. Carl Vander Maelen, ‘Soft Law, Hardcore? The DSA’s Co-Regulatory Mechanisms and the Legitimacy of Platform Regulation’ (Verfassungsblog, 3 June 2024) <https://verfassungsblog.de/soft-law-dsa-co-regulation/>
36. Cary Coglianese and Evan Mendelson, ‘Meta-Regulation and Self-Regulation’ in Robert Baldwin, Martin Cave and Martin Lodge (eds), *The Oxford Handbook of Regulation* (OUP 2010) 146, 151–53.
37. Case C-18/18 *Eva Glawischnig-Piesczek v Facebook Ireland Limited* EU:C:2019:821, paras 41, 45–46
38. Case C-26/13 *Kásler and Káslerné Rábai v OTP Jelzálogbank Zrt* EU:C:2014:282, para 75.
39. Case C-314/12 *UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH and Wega Filmproduktionsgesellschaft mbH* EU:C:2014:192, para 56.
40. Case C-324/09 *L’Oréal SA and Others v eBay International AG and Others* EU:C:2011:474, para 141
41. Case C-70/10 *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* EU:C:2011:771, paras 38–40, 44–53
42. Case C-92/11 *RWE Vertrieb AG v Verbraucherzentrale Nordrhein-Westfalen eV* EU:C:2013:180, paras 44, 53.
43. CAUFFMAN C, GOANTA C. A New Order: The Digital Services Act and Consumer Protection. *European Journal of Risk Regulation*. 2021;12(4):758-774. doi:10.1017/err.2021.8 C. 1
44. Center for Countering Digital Hate, ‘How Will Meta’s Policy Changes Affect European Users?’ (8 January 2025) <https://counterhate.com/blog/how-will-metas-policy-changes-affect-european-users/> (дата звернення 15 травня 2026 року).
45. Chiara P Drolsbach and Nicolas Pröllochs, ‘Content Moderation on Social Media in the EU: Insights from the DSA Transparency Database’ in *Companion Proceedings of the ACM Web Conference 2024* (ACM 2024) 939 <https://doi.org/10.1145/3589335.3651482>

- 46.Children's Online Privacy Protection Act of 1998 (COPPA) (1998).
<https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa>
- 47.China Law Translate. (2016). Provisions on Management of Internet News Services.<https://www.chinalawtranslate.com/en/provisions-on-internet-news-information-managemen>
- 48.China Briefing. (2021). The PRC Personal Information Protection Law (Final): A full translation.<https://www.china-briefing.com/news/the-prc-personal-information-protection-law-final-a-full-translation/>
- 49.China Briefing. (2021). The PRC Personal Information Protection Law (Final): A full translation.<https://www.china-briefing.com/news/the-prc-personal-information-protection-law-final-a-full-translation/>
- 50.China Law Translate. (2019). Provisions on the governance of the online information content ecosystem.
<https://www.chinalawtranslate.com/en/provisions-on-the-governance-of-the-online-information-content-ecosystem/>
- 51.Christian Ollig, Europäische Plattformverfassungen: Die Konstitutionalisierung digitaler Kommunikationsräume durch Art 14 Abs 4 Digital Services Act (Mohr Siebeck 2025) <https://doi.org/10.1628/978-3-16-164538-9>
- 52.Christian Ollig, *Hybrid Speech Governance: Plattformregulierung zwischen privater Autonomie und öffentlicher Verantwortung* (Mohr Siebeck 2025)
- 53.Christine Parker, *The Open Corporation: Effective Self-Regulation and Democracy* (CUP 2002)
- 54.Christoph Busch and Vanessa Mak, 'Putting the Digital Services Act in Context: Bridging the Gap between EU Consumer Law and Platform Regulation' (2021) 10 Journal of European Consumer and Market Law 109.
- 55.Christoph Busch, 'Regulating the Expanding Content Moderation Universe: A European Perspective on Infrastructure Moderation' (2022) 27 UCLA Journal of Law & Technology 32.
- 56.Christopher T Marsden, *Internet Co-Regulation: European Law, Regulatory Governance and Legitimacy in Cyberspace* (CUP 2011) 46–52
- 57.Commission Decisions of 25 April 2023 designating Facebook and Instagram as very large online platforms pursuant to Article 33(4) of Regulation (EU) 2022/2065.
- 58.Commission Recommendation (EU) 2018/334 of 1 March 2018 on measures to effectively tackle illegal content online C (2018) 1177 final.
- 59.Commission, 'Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC' COM (2020) 825 final.
- 60.Commission, 'Assessment of the Code of Practice on Disinformation – Achievements and Areas for Further Improvement' (Staff Working Document) SWD (2020) 180 final, 10 September 2020
- 61.Commission, 'Designation Decisions for the First Set of Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs)' (20

- December 2023) <https://digital-strategy.ec.europa.eu/en/library/designation-decisions-first-set-very-large-online-platforms-vlops-and-very-large-online-search>
62. Commission, 'Impact Assessment Report Accompanying the Proposal for a Regulation on a Single Market for Digital Services' SWD(2020) 348 final.
 63. Commission, 'Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC' COM(2020) 825 final, Explanatory Memorandum.
 64. Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts [1993] OJ L95/29, art 5.
 65. Creemers, R. (2017). Cyber China: Upgrading propaganda, public opinion work and social management for the twenty-first century. *Journal of Contemporary China*, 26(103), 85–100.
 66. Damian Tambini (ed), *Regulating Big Tech: Policy Responses to Digital Dominance* (Oxford University Press 2021)
 67. Daniel Holznagel, 'Shortcomings of the First DSA Audits — and How to Do Better' (DSA Observatory, 11 June 2025) <https://dsa-observatory.eu/2025/06/11/shortcomings-of-the-first-dsa-audits-and-how-to-do-better/>
 68. David S Evans and Richard Schmalensee, 'The Industrial Organization of Markets with Two-Sided Platforms' (2007) 3 *Competition Policy International* 151
 69. Decarolis, Francesco and Li, Muxin, *Regulating online search in the EU: From the android case to the digital markets act and digital services act* (July 6, 2023). Available at SSRN: <https://ssrn.com/abstract=4660372> or <http://dx.doi.org/10.2139/ssrn.4660372> C. 5
 70. *Delfi AS v Estonia* App no 64569/09 (ECtHR [GC], 16 June 2015)
 71. DigiChina. (2017). Translation: Cybersecurity law of the People's Republic of China. <https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/>
 72. Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA <https://eur-lex.europa.eu/eli/dir/2017/541/oj/eng>
 73. Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities. <https://eur-lex.europa.eu/eli/dir/2018/1808/oj/eng>

74. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market [2000] OJ L178/1.
75. Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on the assessment of the effects of certain public and private projects on the environment (codification). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32011L0092>
76. DSA Observatory, 'If at First You Don't Succeed: Reflections on a Rejected Art 40 DSA Data Access Request' (DSA Observatory, 12 March 2026) <https://dsa-observatory.eu/2026/03/12/if-at-first-you-dont-succeed-reflections-on-a-rejected-art-40-dsa-data-access-request/>
77. Edoardo Celeste, 'Digital Constitutionalism: A New Systematic Theorisation' (2019) 33(1) *International Review of Law, Computers & Technology* 76.
78. European Board for Digital Services, 'First Report of the European Board for Digital Services in Cooperation with the Commission pursuant to Article 35(2) DSA on the Most Prominent and Recurrent Systemic Risks as well as Mitigation Measures' (18 November 2025).
79. European Commission, 'Code of Conduct on Countering Illegal Hate Speech Online+' (20 January 2025) <https://digital-strategy.ec.europa.eu/en/library/code-conduct-countering-illegal-hate-speech-online>
80. European Commission, 'Commission Endorses the Integration of the Voluntary Code of Practice on Disinformation into the Digital Services Act' (13 February 2025) <https://digital-strategy.ec.europa.eu/en/news/commission-endorses-integration-voluntary-code-practice-disinformation-digital-services-act>
81. European Commission, 'Commission Investigates Grok and X's Recommender Systems under the Digital Services Act' (Press Release IP/26/203, 25 January 2026) https://ec.europa.eu/commission/presscorner/detail/en/ip_26_203
82. European Commission, 'Q&A on Risk Assessment Reports, Audit Reports and Audit Implementation Reports under DSA' (18 February 2026) <<https://digital-strategy.ec.europa.eu/en/faqs/qa-risk-assessment-reports-audit-reports-and-audit-implementation-reports-under-dsa>
83. European Commission, 'Supervision of the Designated Very Large Online Platforms and Search Engines under DSA'
84. Eva Thomann, 'The Notions of Regulation and Self-Regulation in Political Science' (2017) 3 *Journal of Self-Regulation and Regulation* 55.
85. Evelyn Douek, 'Governing Online Speech: From "Posts-As-Trumps" to Proportionality and Probability' (2021) 121 *Columbia Law Review* 759.
86. Fabiana Di Porto and Marialuisa Zuppetta, 'Co-regulating Algorithmic Disclosure for Digital Platforms' (2021) 40(2) *Policy and Society* 272
87. Fanta A., Rudl T. (2019). Leaked document: EU Commission mulls new law to regulate online platform. <https://netzpolitik.org/2019/leaked-document-eu-commission-mulls-new-law-to-regulate-online-platforms/>

88. Financial Services Modernization Act of 1999 (1999). <https://fraser.stlouisfed.org/title/financial-services-modernization-act-1999-gramm-leach-bliley-act-1050/fulltext>
89. Fontaine, R., & Rogers, W. (2011, October). China's Arab Spring cyber lessons. *The Diplomat*. <https://thediplomat.com/2011/10/chinas-arab-spring-cyber-lessons>
90. Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harvard University Press 2015).
91. Fratangelo, Pierpaolo, 2001. "The E-Commerce Directive: first evaluations," MPRA Paper 5543, University Library of Munich, Germany. C. 3
92. FTC. (2024a). Facebook, Inc., FTC v. <https://www.ftc.gov/legal-library/browse/cases-proceedings/191-0134-facebook-inc-ftc-v> (дата звернення 17 травня 2026 року).
93. FTC. (2023). FTC Sues Amazon for Illegally Maintaining Monopoly Power. <https://www.ftc.gov/news-events/news/press-releases/2023/09/ftc-sues-amazon-illegally-maintaining-monopoly-power> (дата звернення 17 травня 2026 року).
94. FTC. (2024b). Microsoft/Activision Blizzard, In the Matter of. <https://www.ftc.gov/legal-library/browse/cases-proceedings/2210077-microsoftactivision-blizzard-matter> (дата звернення 17 травня 2026 року).
95. Gao, C. (2017, September). China fines its top 3 internet giants for violating cybersecurity law. *The Diplomat*. <https://thediplomat.com/2017/09/china-fines-its-top-3-internet-giants-for-violating-cybersecurity-law/>
96. Gautam Kishore Shahi, Benedetta Tessa, Amaury Trujillo and Stefano Cresci, 'A Year of the DSA Transparency Database: What it (Does Not) Reveal About Platform Moderation During the 2024 European Parliament Election' (arXiv, 9 April 2025)
97. Gerasymenko, A., Mazaraki, N. (2023). The "New Normal" in Competition—Filling the Gaps of Ukrainian Competition Law in the Digital Economy Age. In: Richter, H. (eds) *Competition and Intellectual Property Law in Ukraine*. MPI Studies on Intellectual Property and Competition Law, vol 31. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-66101-7_7
98. Giovanni De Gregorio, 'The Rise of Digital Constitutionalism in the European Union' (2021) 19(1) *International Journal of Constitutional Law* 41.
99. Google, 'YouTube Terms of Service' <https://www.youtube.com/t/terms> (дата звернення 14 травня 2026 року).
100. Gorwa, R. (2024). *The Politics of Platform Regulation: How Governments Shape Online Content Moderation*. Oxford University Press.
101. Hannah Bloch-Wehba, 'Global Platform Governance: Private Power in the Shadow of the State' (2019) 72 *SMU Law Review* 27
102. Health Insurance Portability and Accountability Act of 1996 (1996). <https://aspe.hhs.gov/reports/health-insurance-portability-accountability-act-1996>
103. Heiko Richter, Marlene Straub and Erik Tuchtfield (eds), *To Break Up or Regulate Big Tech? Avenues to Constrain Private Power in the DSA/DMA*

- Package (Max Planck Institute for Innovation and Competition Research Paper No 21-25, 2021).
104. Heldt, Amélie P. (2020) "Merging the Social and the Public: How Social Media Platforms Could Be a New Public Forum," *Mitchell Hamline Law Review*: Vol. 46: Iss. 5, Article 1. C. 1026
 105. Høiness v Norway App no 43624/14 (ECtHR, 19 March 2019)
 106. Ian Ayres and John Braithwaite, *Responsive Regulation: Transcending the Deregulation Debate* (OUP 1992).
 107. Ian Bogost and Nick Montfort, 'Platform Studies: Frequently Questioned Answers' (Digital Arts and Culture 2009 Conference, 2009) 4, and Marc Andreessen, 'The Three Kinds of Platforms You Meet on the Internet' (16 September 2007) https://pmarchive.com/three_kinds_of_platforms_you_meet_on_the_internet.html
 108. Instagram, 'Community Guidelines' <https://help.instagram.com/477434105621119> (дата звернення 14 травня 2026 року).
 109. Instagram, 'Terms of Use' <https://help.instagram.com/termsfuse> (дата звернення 14 травня 2026 року).
 110. Interinstitutional Agreement on Better Law-Making [2003] OJ C321/1, paras 18–22.
 111. Jack M Balkin, 'Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation' (2018) 51 *UC Davis Law Review* 1149
 112. Jamison, S. G. (2019). Creating a National Data Privacy Law for the United States. *Intellectual Property Law Review*, 10(1). <https://open.mitchellhamline.edu/cgi/viewcontent.cgi?article=1089&context=cylaris> C. 3
 113. Jean-Charles Rochet and Jean Tirole, 'Platform Competition in Two-Sided Markets' (2003) 1 *Journal of the European Economic Association* 990.
 114. Jean-Christophe Plantin, Carl Lagoze, Paul N Edwards and Christian Sandvig, 'Infrastructure Studies Meet Platform Studies in the Age of Google and Facebook' (2018) 20(1) *New Media & Society* 293.
 115. Jennifer M Urban, Joe Karaganis and Brianna L Schofield, *Notice and Takedown in Everyday Practice* (UC Berkeley Public Law Research Paper No 2755628, 2017).
 116. Joel R Reidenberg, 'Lex Informatica: The Formulation of Information Policy Rules through Technology' (1998) 76 *Texas Law Review* 55.
 117. John Albert, 'DSA Risk Assessment Reports: A Guide to the First Rollout and What's Next' (DSA Observatory, 9 December 2024) <<https://dsa-observatory.eu/2024/12/09/dsa-risk-assessment-reports-are-in-a-guide-to-the-first-rollout-and-whats-next/>
 118. John Albert, 'Shortcomings of the First DSA Audits – and How to Do Better' (DSA Observatory, 11 June 2025) <<https://dsa-observatory.eu/2025/06/11/dsa-audits-shortcomings-and-how-to-do-better/>

- observatory.eu/2025/06/11/shortcomings-of-the-first-dsa-audits-and-how-to-do-better/>
119. John Albert, 'What Are DSA Audits Doing for Systemic Risk Enforcement? The Case of X' (DSA Observatory, 19 December 2025)
 120. John M Newman, 'Attention Capitalism: The Law and Political Economy of Attention Markets' (2026) 78 *Stanford Law Review* 415
 121. Joined Cases C-682/18 and C-683/18 Frank Peterson v Google LLC and Others and Elsevier Inc v Cyando AG EU:C:2021:503, paras 115–116
 122. Julia Black, 'Decentring Regulation: Understanding the Role of Regulation and Self-Regulation in a "Post-Regulatory" World' (2001) 54 *Current Legal Problems* 103.
 123. Julie E Cohen, 'Law for the Platform Economy' (2017) 51 *UC Davis Law Review* 133.
 124. Karen Yeung, 'Hypermudge: Big Data as a Mode of Regulation through the Design of Choice Architecture' (2017) 20(1) *Information, Communication & Society* 118.
 125. Kate Klonick, 'The New Governors: The People, Rules, and Processes Governing Online Speech' (2018) 131 *Harvard Law Review* 1598.
 126. Klonick, 'The New Governors', *Harvard Law Review* 2018
 127. Klosowski, T. (2021). The State of Consumer Data Privacy Laws in the US (And Why It Matters). *Wirecutter*.
<https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/>
 128. Knight-Georgetown Institute, 'Systemic Risk Assessment under the Digital Services Act' (15 May 2025) <<https://kgi.georgetown.edu/research-and-commentary/systemic-risk-assessment-under-the-digital-services-act>
 129. KPMG Netherlands, *Analysis of the 2024 Digital Services Act Audit Reports: Exploring the Inaugural DSA Audit Reports of 19 Platforms: A Benchmark Study* (KPMG, 24 February 2025)
<https://assets.kpmg.com/content/dam/kpmgsites/nl/pdf/2025/services/kpmg-2024-dsa-audit-reports-benchmark.pdf.coredownload.inline.pdf>
 130. KPMG Netherlands, *Analysis of the 2024 Digital Services Act Audit Reports: Exploring the Inaugural DSA Audit Reports of 19 Platforms: A Benchmark Study* (KPMG, 24 February 2025).
 131. KPMG, *Analysis of the 2024/2025 Digital Services Act Audit Reports* (KPMG Netherlands 2025)
<<https://assets.kpmg.com/content/dam/kpmg/nl/pdf/2025/kpmg-2024-dsa-audit-reports-benchmark.pdf>
 132. Lawrence Lessig, *Code: Version 2.0* (Basic Books 2006)
 133. Leerssen P (2023) An end to shadow banning? Transparency rights in the digital services act between content moderation and curation. *Computer Law & Security Review* 48: 105790.
<https://www.sciencedirect.com/science/article/pii/S0267364923000018#section-cited-by> C. 2

134. Library of Congress. (2018, November 21). China: E-commerce law passed. Global Legal Monitor. <https://www.loc.gov/item/global-legal-monitor/2018-11-21/china-e-commerce-law-passed>
135. L'Oréal (n X) paras 120–124 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62009CJ0324>
136. Marie-Therese Sekwenz, Rita Gsenger, Scott Dahlgren and Ben Wagner, 'Doing Audits Right? The Role of Sampling and Legal Content Analysis in Systemic Risk Assessments and Independent Audits in the Digital Services Act' (arXiv, 6 May 2025) <https://arxiv.org/abs/2505.03601>
137. Mark Armstrong, 'Competition in Two-Sided Markets' (2006) 37 RAND Journal of Economics 6684 David S Evans, 'The Antitrust Economics of Multi-Sided Platform Markets' (2003) 20 Yale Journal on Regulation 325.
138. Martin Husovec, 'The DSA as a Co-regulatory System' in Martin Husovec, Principles of the Digital Services Act (Oxford University Press 2024) ch 20.
139. Martin Husovec, Principles of the Digital Services Act (OUP 2024).
140. Martin Kretschmer, 'Platforms and Digital Regulation' (Weizenbaum Journal of the Digital Society, 2021).
141. Meta, 'Facebook Community Standards' <https://transparency.meta.com/policies/community-standards/> (дата звернення 14 травня 2026 року).
142. Meta, 'Terms of Service' <https://www.facebook.com/terms/> (дата звернення 14 травня 2026 року).
143. Michael L Katz and Carl Shapiro, 'Network Externalities, Competition, and Compatibility' (1985) 75 American Economic Review 424.
144. Michael Veale and Rachel Griffin, 'Data Access under the Digital Services Act: A Data Standoff' (arXiv, 2 May 2025) <https://arxiv.org/abs/2505.01122>
145. Milos Novovic, The EU Digital Services Act (DSA): A Commentary (Kluwer Law International 2024), commentary to art 16.
146. Milos Novovic, *The EU Digital Services Act (DSA): A Commentary* (Kluwer Law International 2024), commentary to art 14.
147. Milos Novovic, The EU Digital Services Act (DSA): A Commentary (Kluwer Law International 2024), commentary to art 17.
148. Milos Novovic, *The EU Digital Services Act (DSA): A Commentary* (Kluwer Law International 2024), commentary to arts 34–35
149. Ministry of Commerce of the People's Republic of China. (2019). E-commerce law of the People's Republic of China. <http://mg.mofcom.gov.cn/article/policy/201912/20191202923971.shtml>
150. Miriam C Buiten, 'The Digital Services Act: From Intermediary Liability to Platform Regulation' (2021) 12(3) JIPITEC 361.
151. Natali Helberger, Jo Pierson and Thomas Poell, 'Governing Online Platforms: From Contested to Cooperative Responsibility' (2018) 34(1) *The Information Society* 1.

152. Natali Helberger, 'The Political Power of Platforms: How Current Attempts to Regulate Misinformation Amplify Opinion Power' (2020) 8(6) *Digital Journalism* 84.
153. Nataliia A Mazaraki and Volodymyr D Prymak, 'Механізм вирішення спорів між користувачами та онлайн-платформами в акті ЄС про цифрові послуги' (2026) 19 *Український політико-правовий дискурс* <https://doi.org/10.5281/zenodo.18662891>
154. Neil Gunningham and Peter Grabosky, *Smart Regulation: Designing Environmental Policy* (OUP 1998)
155. Nicolas Suzor, *Lawless: The Secret Rules That Govern Our Digital Lives* (Cambridge University Press 2019).
156. Nikolaus von Bernuth, 'The Premise of Good Faith in Platform Regulation: On the Changing Conditions of the Digital Services Act's Regulatory Approach' (Verfassungsblog, 14 April 2025) <https://doi.org/10.59704/5494324c1cc2203d>.
157. Olena Honcharenko, Mariia Pozhydaieva, Larysa Neskoro dzhen a and Oleksandra Kolohoida, 'Self-Regulatory Practices of Electronic Trade and Transnational Public Order in the Context of Ensuring the Economic Security of the State' (2024) 36 *Revista Jurídica Portucalense* 106 [https://doi.org/10.34625/issn.2183-2705\(36\)2024.ic-5](https://doi.org/10.34625/issn.2183-2705(36)2024.ic-5).
158. Peter Collin, Gerd Bender, Stefan Ruppert, Margrit Seckelmann and Michael Stolleis (eds), *Selbstregulierung im 19. Jahrhundert: Zwischen Autonomie und staatlichen Steuerungsansprüchen* (Vittorio Klostermann 2011).
159. Pietro Ortolani, Shiva Vahed, Catalina Goanta and Alan G Sanfey, 'The Digital Services Act and the Psychology of Social Media Content Reporting: Drawing Legal Inferences from a Behavioural Experiment on Notice-and-Action Mechanisms' (2025) 4 *European Law Open* 464.
160. *Pihl v Sweden* App no 74742/14 (ECtHR (dec), 7 February 2017)
161. Privacy Act of 1974, 5 U.S.C. § 552a (1974). <https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1279>
162. Rachel Griffin and Carl Vander Maelen, 'Codes of Conduct in the Digital Services Act: Exploring the Opportunities and Challenges' (2024) *Technology and Regulation* 167 <https://doi.org/10.26116/techreg.2024.016>
163. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng>
164. Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services. <https://eur-lex.europa.eu/eli/reg/2019/1150/oj/eng>
165. Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) <https://eur-lex.europa.eu/eli/reg/2022/1925/oj/eng>

166. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) <https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng>
167. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng>
168. Reuters. (2017). China closes 60 celebrity gossip social media accounts. <https://www.reuters.com/article/us-china-internet-censorship-idUSKBN18Z0J3/>
169. Rita Gsenger and others, 'Platform Governance under the Digital Services Act' (2025) *Information, Communication & Society* <https://doi.org/10.1080/1369118X.2025.2590561>.
170. Robert Baldwin and Julia Black, 'Really Responsive Regulation' (2008) 71 *MLR* 59.
171. Robert Baldwin, Martin Cave and Martin Lodge, *Understanding Regulation: Theory, Strategy, and Practice* (2nd edn, OUP 2012) ch 8.
172. Robert Gorwa, *The Politics of Platform Regulation: How Governments Shape Online Content Moderation* (Oxford University Press 2024).
173. Robert Gorwa, 'What Is Platform Governance?' (2019) 22(6) *Information, Communication & Society* 854
174. Rocco Bellanova and Ronan Ó Fathaigh, 'Platforms, Online Surveillance, and the European Union Digital Services Act' (2026) *European Papers*
175. Sally Broughton Micova, Daniel Schnurr, Andrea Calef and Bryn Enstone, *Cross-Cutting Issues for DSA Systemic Risk Management: An Agenda for Cooperation* (CERRE, 10 July 2024) <https://cerre.eu/publications/cross-cutting-issues-for-dsa-systemic-risk-management-an-agenda-for-cooperation/>
176. *Sanchez v France* App no 45581/15 (ECtHR [GC], 15 May 2023)
177. Sanger, D. E. (2000, March 9). Clinton sends to a wary Congress a long-delayed China trade bill. *The New York Times*. <https://www.nytimes.com/2000/03/09/world/clinton-sends-to-a-wary-congress-a-long-delayed-china-trade-bill.html>
178. Sapir, A., & Mavroidis, P. C. (2021, April 29). China and the WTO: An uneasy relationship. <https://cepr.org/voxeu/columns/china-and-wto-uneasy-relationship>
179. Sara Solarova, Matúš Mesarčík, Branislav Pecher and Ivan Srba, 'Beyond the Checkbox: Strengthening DSA Compliance Through Social Media Algorithmic Auditing' (arXiv, 26 January 2026) <https://arxiv.org/abs/2601.18405>
180. Seamus Simpson, 'The Limits of Internet Self-Regulation: The EU's Policy for Digital Internet Intermediaries' (2024) 9 *Frontiers in Communication*

181. Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (PublicAffairs 2019).
182. Strittmatter, K. (2013, July 3). Why China's internet censors can't get enough of Edward Snowden. <https://worldcrunch.com/world-affairs/why-china039s-internet-censors-can039t-get-enough-of-edward-snowden>
183. Tarleton Gillespie, *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media* (Yale University Press 2018)
184. The White House Archives. (2020). Executive Order on Preventing Online Censorship. <https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-preventing-online-censorship/>
185. The 2022 Code of Practice on Disinformation <https://disinfocode.eu/the-code/>
186. The Santa Clara Principles on Transparency and Accountability in Content Moderation (2nd edn, 2021).
187. Thomas Poell, David Nieborg and José van Dijck, 'Platformisation' (2019) 8(4) *Internet Policy Review* DOI: 10.14763/2019.4.1425
188. Tim Sprenger, *Das Plattformverfahren: Ausbalancierte Rechtsdurchsetzung mittels Verfahrensgrundsätzen* (Weizenbaum Institute 2024)
189. Tim Wu, *The Attention Merchants: The Epic Scramble to Get Inside Our Heads* (Knopf 2016)
190. Transparency Centre, 'Code of Practice on Disinformation' <https://disinfocode.eu/>
191. UNHRC, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression' (6 April 2018) UN Doc A/HRC/38/35.
192. Wang, J. (2022). Platform responsibility with Chinese characteristics. Defeating Disinformation. https://digitalplanet.tufts.edu/wp-content/uploads/2023/02/DD-Report_1-Jufang-Wang-11.30.22.pdf
193. Wang, J. (2020). Regulation of digital media platforms: The case of China. Oxford: The Foundation for Law, Justice and Society
194. Weber Digital. (2023). What is an ICP license? Types & requirements. <https://service.weber.digital/index.php?/en/Knowledgebase/Article/View/what-is-an-icp-license-types--requirements>
195. Webster, G. (2019). A brief history of the Chinese Internet. <https://logicmag.io/china/a-brief-history-of-the-chinese-internet/>
196. What is the Artificial Intelligence Act of the European Union (EU AI Act)? <https://www.ibm.com/think/topics/eu-ai-act> (дата звернення 21 травня 2026 року).
197. Wolfgang Hoffmann-Riem, 'Medienregulierung als regulierte Selbstregulierung' in *Regulierte Selbstregulierung als Steuerungskonzept des Gewährleistungsstaates* (Duncker & Humblot 2001).

198. Wolfgang Schulz and Thorsten Held, *Regulierte Selbstregulierung als Form modernen Regierens* (Arbeitspapiere des Hans-Bredow-Instituts No 10, Verlag Hans-Bredow-Institut 2002).
199. Wolfgang Schulz and Thorsten Held, *Regulated Self-Regulation as a Form of Modern Government: An Analysis of Case Studies from Media and Telecommunications Law* (University of Luton Press 2004).
200. YouTube, 'Community Guidelines' <https://www.youtube.com/howyoutubeworks/policies/community-guidelines/> (дата звернення 15 травня 2026 року).
201. Zheng, H. (2013). *Regulating the Internet: China's Law and Practice*. Beijing Law review, 4(1), 37–41. <http://dx.doi.org/10.4236/blr.2013.41005> с. 38