DOI: 10.31617/3.2024(137)08
УДК 341.1(510):004.773.7

ЩЕРБАК Геннадій,
магістр, аспірант кафедри
міжнародного, цивільного та
комерційного права
Державного торговельно-економічного
університету
вул. Кіото, 19, м. Київ, 02156, Україна
H.Shcherbak@knute.edu.ua

SHCHERBAK Hennadii,
Master, Postgraduate Student
of the Department of International,
Civil and Commercial Law
State University of Trade and Economics

19, Kyoto St., Kyiv, 02156, Ukraine
ORCID: 0000-0002-8569-9812

РЕГУЛЮВАННЯ ОНЛАЙН-ПЛАТФОРМ У ПРАВІ КНР

Регулювання діяльності онлайн-платформ стало очевидною тенденцією останнього десятиліття, що пов'язано зі значним впливом їх функціонування на мільйони користувачів. Водночас підходи до такого регулювання є відмінними та виділяють три основні підходи – американський, європейський та китайський. Проаналізовано підхід до регулювання онлайн-платформ у Китайській Народній Республіці (КНР). Унікальність китайського підходу зумовлена: з одного боку, залученням авторитарних методів управління та регулювання для контролю за населенням, а з іншого – успішним сприянням розвитку інновацій та технологічного прогресу в цій сфері, що дозволило створити в КНР за майже 30 років один із найбільших цифрових ринків у світі, де онлайн-платформи відіграють ключову роль у соціальних, економічних і політичних процесах. Гіпотеза дослідження полягає в тому, що регулювання онлайн-платформ у КНР спирається на авторитарну модель управління, яка дає змогу оперативно реагувати на виклики та забезпечує підтримку внутрішньої політики, а також успішно підтримує розвиток інновацій у цифровій сфері. Аналіз наукових джерел забезпечив розуміння регулювання онлайн-платформ з точки зору балансу публічного і приватного інтересу, а також з'ясування особливостей державної політики Китаю. Своєю чергою, саме висвітлення особливостей китайського підходу досягнуто шляхом послідовного телеологічного тлумачення китайських нормативно-правових актів, предметом яких є регулювання доступу до інтернету та його використання і безпосередньо онлайн-платформ. У дослідженні виявлено ключові особливості китайського підходу до регулювання: впровадження політичної цензури, деанонімізації користувачів, створення інституційного контролю за платформами й обмеження впливу іноземних IT-компаній. Основними результатами є виявлення подвійного характеру регулювання: з одного боку, воно спрямоване на захист користувачів від зловживань платформ, а з іншого – забезпечує

REGULATION OF ONLINE PLATFORMS IN CHINESE LAW

Regulation of online platforms has become an obvious trend in the last decade, which is associated with the significant impact of their functioning on millions of users. At the same time, approaches to such regulation are different and distinguish three main approaches – American, European and Chinese. The approach to regulating online platforms in the People's Republic of China (PRC) is analysed. The uniqueness of the Chinese approach is due to: on the one hand, the involvement of authoritarian methods of management and regulation to control the population, and on the other hand, the successful promotion of innovation and technological progress development in this area, which allowed the creation in the PRC of one of the largest digital markets in the world in almost 30 years, where online platforms play a key role in social, economic and political processes. The hypothesis of the study posits that the regulation of online platforms in the PRC relies on an authoritarian management model, enabling swift response to challenges while providing support for domestic policy, as well as successfully supports the development of innovations in the digital sphere. The analysis of scientific sources provided an understanding of the regulation of online platforms from the point of view of public and private interest balance, as well as clarification of the peculiarities of Chinese state policy. In turn, the highlighting of the peculiarities of the Chinese approach was achieved through a consistent teleological interpretation of Chinese regulatory acts, the subject of which is the regulation of access to the Internet and its use, and directly online platforms. The study identifies key features of the China's approach to regulation: the implementation of political censorship, user de-anonymization, the creation of institutional platform oversight, and limiting the influence of foreign IT companies. The main results are the identification of the the dual nature of regulation: on the one hand, it is aimed at protecting users from platform abuses, and on the other hand, it ensures state control over information flows. Thus, the Chinese model of online

державний контроль над інформаційними потоками. Отже, китайська модель регулювання онлайн-платформ демонструє унікальний підхід, що поєднує технократичний контроль із політичними цілями.

Ключові слова: онлайн-платформи, саморегулювання господарської діяльності, конкурентне право, кібербезпека, Китай.

platform regulation demonstrates a unique approach combining technocratic control with political objectives.

Keywords: online platforms, self-regulation of economic activity, competition law, cybersecurity, China.

JEL Classification: K20, K24, L86.

Вступ

Протягом останніх років уряди різних держав впроваджують регуляторні інструменти щодо контенту, який розміщується на онлайн-платформах, переслідуючи мету захисту прав інтелектуальної власності, боротьби з дезінформацією, шкідливими та протиправними матеріалами. Великі онлайн-платформи зі стабільно зростаючою кількістю користувачів набувають значної ролі у формуванні суспільної думки, впливу на соціально-економічні процеси, культурне життя, що зумовлює державну інтервенцію у правила, політики й алгоритми, що застосовуються на таких платформах. Зокрема, це проявляється як у специфічному регулюванні в межах "традиційних" галузей права (конкурентного, інформаційного, права захисту споживачів та ін.), так і прийнятті спеціальних норм, безпосередньо спрямованих на онлайн-платформи.

Очевидні тенденції до все більш широкого втручання держави у функціонування цифрових ринків та цифрових платформ стали предметом дослідження багатьох вчених (*Bradford*, 2023, 2024; *Gorwa*, 2024; *Zhang*, 2024 та ін.), які приходять до погодженої позиції, що у світі формується три підходи до регулювання цифрових ринків та онлайн-платформ: ліберальний, орієнтований на розвиток технологій та інновацій за мінімального державного втручання (наприклад, США), орієнтований на захист фундаментальних прав в інтернет-просторі (ЄС) та орієнтований на підтримку внутрішньої політики держави (КНР). При цьому в останніх двох випадках регулювання платформ стає все більш деталізованим, комплексним і складним для впровадження цільовими компаніями.

Політика китайського уряду в цьому контексті є найбільш показовою, інтенсифікація регуляторного втручання у функціонування онлайн-платформ за останні 5 років набула характеру лісової пожежі, що стрімко розповсюджується (*Yang*, 2021) у сферах фінтеху, соціальних мереж, онлайн-платформ послуг доставки та таксі. Підходи Китаю є доволі унікальними з огляду на обґрунтування, цілі державної політики щодо інтернет-простору, а також підходи, що застосовуються (*Zhang*, 2022). Показовим є також і те, що регуляторна інтервенція китайського уряду в інтернет-просторі не спиняється, зокрема, у квітні 2024 р. прийнято Тимчасові заходи захисту від недобросовісної конкуренції в інтернеті (*China's State Administration for Market Regulation Releases Interim Provisions on Anti-Unfair Competition on the Internet*, 2024).

Дослідницький інтерес до регулювання онлайн-платформ, підкріплений доктринальним аналізом, привів до формулювання гіпотези цього дослідження, яка полягала в тому, що регулювання онлайн-платформ у Китаї базується на успішному досвіді регулювання інтернету, де авторитарний режим дозволив ефективно залучати різні державні органи та достатньо швидко приймати необхідні регуляторні заходи, спрямовані на захист державного устрою і державної політики в країні.

З огляду на сформульовану гіпотезу мета цього дослідження полягала в з'ясуванні особливостей авторитарного підходу регулювання онлайн-платформ у Китайській Народній Республіці. Під особливостями розуміються: характер зобов'язань, які покладаються на онлайн-платформи, та відповідальність за їх порушення, комплекс прав користувачів, які мають забезпечуватися онлайн-платформою, можливості держави щодо впливу і втручання в діяльність онлайн-платформ та їх характер, рівень і характер політичної цензури у сфері онлайн-платформ тощо.

Для цього проаналізовано нормативно-правові акти КНР, наукові та публіцистичні матеріали з тематики дослідження, а до текстів регуляторних актів застосовано телеологічний метод (у перекладі на англійську з онлайн-ресурсу www.chinalawtranslate.com/en/).

Структурно дослідження побудовано так: у першій частині розкрито сутність основних підходів до регулювання онлайн-платформ, у другій – особливості розвитку інтернету в КНР, у третій частині послідовно висвітлено ключові компоненти основних актів, що регулюють онлайн-платформи в інтернеті.

1. Основні підходи до регулювання онлайн-платформ

Онлайн-платформи відіграють ключову роль у сучасному суспільно-економічному житті, впливаючи на формування громадської думки, розвиток цифрової економіки та забезпечення доступу до інформації. Вони стали невіддільною частиною комунікації, торгівлі та розваг, залучаючи мільярди користувачів по всьому світу. Однак їхній вплив не обмежується лише позитивними аспектами – онлайн-платформи можуть сприяти поширенню дезінформації, порушенню приватності та зловживанню монопольним становищем. Це зумовлює необхідність ефективного регулювання, яке має знайти баланс між свободою слова, захистом користувачів і забезпеченням конкурентного середовища. Дослідження різних підходів до регулювання платформ, таких як американська, європейська та китайська модель, є важливим для розуміння можливостей і викликів у цій сфері. Воно дозволяє оцінити ефективність різних стратегій і адаптувати їх до потреб інших країн та регіонів.

В основі класифікації підходів до регулювання онлайн-платформ лежить балансування між приватним і державним інтересом. Державний інтерес може охоплювати категорії національної безпеки, громадського

порядку, захисту прав громадян, забезпечення існування наявного політико-правового режиму, економічну стабільність і конкуренцію, соціальну справедливість, тоді як приватний інтерес може включати категорії свободи слова, свободи підприємницької діяльності, саморегулювання, просування інновацій. Отже, виділяються три вищезгадані підходи: американський підхід, який ґрунтується на невтручанні держави в діяльність онлайн-платформ, щоб не заважати прискоренню інновацій у цифровій сфері, а тому його балансування зрушено в бік приватного інтересу; європейський підхід, який спрямований на захист фундаментальних прав користувачів онлайн-платформ, а тому він намагається балансувати між вимушеним державним контролем та регулюванням задля забезпечення фундаментальних прав і приватними інтересами онлайн-платформ; китайський підхід, який розглядає регулювання онлайн-платформ як ще один з інструментів контролю держави за суспільством та забезпечення подальшого існування політично-правового режиму, а тому в цьому випадку балансування сильно зрушено в напрямі державного інтересу (*Bradford*, 2023).

Історично найпершим з'явився саме американський підхід до регулювання онлайн-платформ. По-перше, хоча швейцарський *CERN* і є місцем виникнення сучасного глобального інтернету, Сполучені Штати Америки – місце створення його попередника, який виник з мережі, що об'єднувала комп'ютери низки наукових закладів та університетів, під назвою *ARPANET*. У США виникли одні з перших онлайн-платформ та інтернет-спільнот. По-друге, саме США стали батьківщиною найперших транснаціональних *IT*-гігантів, що були власниками онлайн-платформ. Американські інтернет-користувачі в 1980–1990 рр. (до яких належали і власники перших онлайн-платформ) просували ідеї вільного інтернет-простору, вільного насамперед від державного втручання та регулювання, бо вважалося, що інтернет-спільнота загалом і онлайн-платформи безпосередньо зможуть ефективно здійснювати саморегулювання. Оскільки формування онлайн-платформ у США супроводжувалося стрімким розвитком цифрових технологій та інновацій, це було достатнім для американської влади аргументом того, що мінімальна роль держави в регулюванні онлайн-платформ є вірним варіантом. Окрім того, з розповсюдженням доступу до інтернету по світу американські онлайн-платформи були ефективним способом поширення американських цінностей в інших країнах світу.

Водночас американський підхід до регулювання онлайн-платформ 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 зловживань (*Bradford*, 2024). Також американський підхід, окрім просування ідеї мінімального втручання держави в діяльність платформ,

підтримував ідею абсолютної свободи слова. Це спричинило інший негативний наслідок – абсолютна свобода слова призвела до поширення мови ненависті, дезінформації та маніпуляцій з інформацією, що, своєю чергою, порушувало інші фундаментальні права людини. Саме це стало причиною формування європейського підходу до регулювання онлайн-платформ, яке орієнтувалося на захист фундаментальних прав користувачів за допомогою комплексного врегулювання діяльності онлайн-платформ (Акт про цифрові послуги ЄС, Акт про цифрові ринки ЄС тощо). За цього підходу державне втручання сприймається як вимушений захід для забезпечення та захисту прав користувачів онлайн-платформ від зловживань з боку їх власників.

У КНР також виник скептицизм щодо американського підходу, але вочевидь не через порушення фундаментальних прав користувачів, а через те, що цей підхід ніс загрозу для існування політичного режиму в КНР, оскільки, як було сказано вище, американські платформи були інструментом поширення американських цінностей, які могли підірвати "соціальну стабільність" у КНР, що могло б поставити під загрозу існування політичного режиму. Тому китайський підхід регулювання онлайн-платформ міг ґрунтуватися тільки на всеохопному державному втручанні та контролі з метою розбудови власних онлайн-платформ, які будуть підконтрольні китайській владі (*Bradford*, 2023).

2. Особливості розвитку інтернету в Китаї

2.1. Поява інтернету на території Китаю

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 р., але його використання було обмежено державними органами та науково-дослідними установами. З 1995 р. інтернет стає доступним в Китаї вже для широкого загалу, а також з метою комерційного використання (*Mubarak*, 2020). Як наслідок, кількість користувачів почала стрімко зростати: протягом 1995 р. їхня кількість зросла від 3000 до 40 000 осіб. Також упродовж наступних років були засновані нинішні китайські *IT*-гіганти, такі як *NetEase* (1997 р.), *Tencent* (лютий 1999 р.), *Alibaba* (квітень 1999 року), *Baidu* (січень 2000 р.) (*Webster*, 2019) тощо.

Поява інтернету в Китаї відбулася в період економічної та часткової політичної лібералізації, який розпочався після смерті Мао Цзедуна у 1976 р. і закінчення руйнівної двадцятирічної культурної революції та часткової міжнародної ізоляції, що нанесла країні значні економічні збитки. З приходом до влади Дена Сяопіна КНР почала реалізовувати політику покращення зіпсованих дипломатичних відносин з країнами Заходу, у т. ч. зі Сполученими Штатами, та політику інтеграції КНР у міжнародну спільноту та систему міжнародної торгівлі. Так, зокрема, КНР розпочала процес вступу до Світової організації торгівлі та вступила до неї у 2001 р. (*Sapir& Mavroidis*, 2021).

Вочевидь причина початку цієї епохи лібералізації була досить прагматичною: культурна революція замість "великого стрибка" 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, що могли поставити під сумнів легітимність керівного авторитарного режиму КПК (*Webster*, 2019).

У той самий час країни Заходу позитивно зустріли початок епохи лібералізації та, зокрема, поширення на території Китаю доступу до інтернету, оскільки були переконані, що це приведе до ще більшої перебудови всередині КНР та перетворить її на демократичну країну. Так, наприклад, Білл Клінтон у своїй промові у 2000 р. зазначив: "Ми знаємо, наскільки інтернет змінив Америку, і ми вже є відкритим суспільством. …Уявіть, наскільки це може змінити Китай" (примітка – переклад автора) (*Sanger*, 2000).

2.2. Перші спроби влади КНР щодо врегулювання інтернет-простору та онлайн-платформ

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 й обмеження свободи висловлення. У країні вже існувала система політичної цензури й обмежень свободи 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 країні здійснювалося державою, інтернет-провайдери повинні були мати ліцензію для здійснення своєї діяльності та хоча б на 51% належати державним компаніям (*Weber Digital*, 2023). Отже, китайська влада могла досить легко реалізувати впровадження обмежень до свого інтернет-простору. З цього приводу Ану Бредфорд влучно зазначила, що "Китайський уряд перетворив інтернет із 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) (*Bradford*, 2023).

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, що відповідав за щоденне управління пропагандою, Інформаційного бюро Державної ради, яке стежило за новинами, та низки органів на рівні міністерства, які здійснювали нагляд за державними ЗМІ (*Creemers*, 2017).

Разом з тим у 1996 р. 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: інформація щодо національної безпеки, державної таємниці, інформація, яка порушує соціальну стабільність, та матеріали сексуального характеру. А у 2000 р. цей перелік був розширений у новому документі – Заходи 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 у 2003 р. для посилення політичної цензури в Китаї була впроваджена фільтраційна система "Золотий щит", яка обмежувала користувачам доступ до інформації, що містить заборонені слова (*Zheng*, 2013).

Отже, 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 зі сфери традиційних китайських ЗМІ. Діяльність китайської влади протягом цього періоду фокусувалася 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 *IT*-гігантів, які б, по-перше, могли стимулювати технологічний прогрес у сфері китайських цифрових технологій, а по-друге, конкурували з американськими *IT*-гігантами як на території Китаю, так і за його межами. А це дало б можливість убезпечити китайських користувачів від американського впливу, який розповсюджували американські корпорації, та мати можливість здійснювати свій вплив на треті країни. Саме тому китайська влада дуже активно інвестувала у формування та розширення власних онлайн-платформ, а також стимулювання розвитку інновацій. І це принесло свої результати: так, зокрема, станом на 2024 р. 8 з 20 найбільших інтернет-компаній за доходом є китайськими *IT*-гігантами (*Jingdong Mall, Alibaba, Tencent, Pinduoduo, Meituan, DiDi, Kuaishou Technology, Vipshop*) (*Companies Market Cap*, 2024). Окрім того, в Китаї було заблоковано з політичних причин (переважно через висвітлення протестів) низку популярних американських платформ (*Facebook*, *Twitter/X*, *Google*, *YouTube* тощо), що також убезпечувало китайські онлайн-платформи від конкуренції із західними платформами за багатомільйонний китайський ринок (*Hamza*, 2024).

2.3. Створення спеціальних законів для врегулювання інтернет-простору та онлайн-платформ

Зміни в напрямі регулювання онлайн-платформ розпочалися з обранням Сі Цзіньпіна головою КНР у 2013 р. 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" задля 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 і втрати контролю, зокрема в інтернеті (*Creemers*, 2017).

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

- занепокоєння китайської влади щодо використання соціальних мереж для координації протестів та інших соціальних заворушень на прикладі Арабської весни (*Fontaine* & *Rogers*, 2011);
- оприлюднення Едвардом Сноуденом секретних документів, які розкривають можливості американської розвідки зі спостереження за іноземними чиновниками (*Strittmatter*, 2013);
- китайські *IT*-гіганти майже повністю забезпечували китайських користувачів власними цифровими сервісами;
- необхідність приборкати *IT*-гігантів, які стали монополістами завдяки державній підтримці та блокуванню західних платформ.

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

Протягом наступних років в Китаї були прийняті чотири ключові закони, які стали основою державного регулювання інтернет-простору в країні (і зокрема онлайн-платформ), 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.

3.1 Ключові положення Закону про кібербезпеку КНР 2016 року

Закон про кібербезпеку КНР прийнятий у 2016 р. Як зазначається в самому законі, його ціллю є захист китайського кіберпростору, державних та приватних інтересів у 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 мережевих даних, а також поняття "оператора мережі", що охоплює власників мереж, адміністраторів та постачальників мережевих 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. Впровадження багаторівневої системи захисту кібербезпеки для запобігання несанкціонованим втручанням та захисту персональних даних користувачів (створення правил внутрішньої безпеки, технічних заходів із запобігання зараженню комп'ютерними вірусами, зі спостереження за статусом операцій в мережі та їх запису, боротьби з кібератаками, а також таких заходів, 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 користувачів чітко зазначати про це та здійснювати збір тільки у випадку їхньої згоди.

3. При реєстрації користувачів отримання від них відомостей, які підтверджують їхню особу. Без цього реєстрація не дозволяється; має надаватися технічна підтримка та допомога відповідним органам державної влади за їхнім запитом, зокрема у сфері сприяння розслідуванню кримінальних правопорушень.

4. Провайдери інтернет-послуг, які збирають персональні дані китайських користувачів, мають зберігати їх на серверах у межах материкового Китаю. Для отримання дозволу на передачу даних за межі Китаю має бути проведена 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 мають 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 участі в діяльності, яка загрожує

національній безпеці та інтересам, не закликати до повалення соціалістичного режиму, терористичних або екстремістських актів, не розпалювати сепаратистські настрої, не пропагувати дискримінацію чи етнічну ворожнечу, не поширювати неправдиву інформацію, жорстокий або порнографічний контент, не 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 вебсайти 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 й 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 повинні встановлювати зловмисне програмне забезпечення або містити інформацію, публікацію чи передачу якої заборонено законами й адміністративними правилами.

Закон наділяє державу повноваженнями, зокрема:

1. З формування стратегій, регламентів та вимог у сфері кібербезпеки, а також вживати заходів для попередження та боротьби з кібербезпековими ризиками, захищати критичну інформаційну структуру тощо. Безпосередньо відповідальним за реалізацію цих повноважень є Адміністрація з кіберпростору (далі – CAC), 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 її видалення.

3. Департаменти та їхній персонал, який відповідає за нагляд та адміністрування кібербезпеки, повинні зберігати особисту інформацію, приватну інформацію і 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 50 000 до 500 000 юанів

з конфіскацією незаконного прибутку й арештом до 5 діб, а в серйозних випадках штраф збільшується до 100 000 юанів та арешт – до 15 діб; по-друге, створення вебсайтів для здійснення незаконної або злочинної діяльності в серйозних випадках може каратися штрафом у 50 000–500 000 юанів та арештом від 5 до 15 діб; по-третє, оператор критичної інформаційної інфраструктури не справляється зі своїми основними зобов'язаннями у сфері кібербезпеки, за що йому може загрожувати штраф від 100 000 до 1 000 000 юанів (*DigiChina*, 2017).

Отже, Закон про кібербезпеку є основою нового режиму комплексного регулювання інтернет-простору в Китаї. З одного боку, він 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 він закріплює повноваження державних органів зі спостереження за діяльністю онлайн-платформ та зобов'язує платформи надавати технічну допомогу на вимогу державних органів, а також за діяльністю користувачів на платформах – і у разі виявлення незаконного контенту надсилати платформі вимогу про його видалення.

3.2. Ключові положення Закону про електронну комерцію КНР 2018 року

Закон про електронну комерцію КНР прийнято у 2018 р. Під "електронною комерцією" мається на увазі комерційна діяльність з продажу товарів або надання послуг через інтернет або будь-яку іншу інформаційну мережу. Однак існує низка винятків: фінансові продукти і послуги, інформація про новини, аудіо- та відеопрограми, публікації, культурні продукти та інші контент-послуги, що надаються через інформаційні мережі.

Виділяються такі категорії суб'єктів, як:

"бізнес електронної комерції", що означає фізичних або юридичних осіб, які займаються підприємницькою діяльністю з продажу товарів або надання послуг через інтернет чи будь-яку іншу інформаційну мережу, включаючи підприємства платформи електронної комерції, компанії, що працюють на платформі, та компанії електронної комерції, які продають товари або надають послуги за допомогою самостійно створеного вебсайту чи 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-майданчики для бізнесу, пошук партнерів і оприлюднення інформації, щоб вони могли самостійно вести торгову діяльність;

"бізнес на платформі" – бізнес електронної комерції, який продає товари або надає послуги через платформу.

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

1. На бізнеси електронної комерції покладаються певні зобов'язання: при продажі товарів або наданні послуг, дотримуючись вимог гарантії особистої та майнової безпеки тощо, гарантувати користувачам право вибору шляхом повного і точного розкриття інформації про товари та послуги, які надаються; гарантувати користувачам право на виправлення та видалення особистої інформації; гарантувати користувачам можливість відмовитися від таргетованої реклами; надавати на вимогу державних органів відповідні дані й інформацію, пов'язані з електронною комерцією.

2. Від бізнес-платформ електронної комерції вимагається: при реєстрації бізнесів на своїй платформі отримувати від них зазначення особистих даних, адреси тощо; у разі виявлення порушень, які здійснені бізнесами на платформі, повідомляти про це відповідні органи; вживати заходів із запобігання кіберзлочинам та іншій незаконній діяльності у себе на платформі; записувати та зберігати інформацію про товари і сервіси на платформі, а також про транзакції.

3. Відповідно до Закону про електронну комерцію, якщо власник прав інтелектуальної власності (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 вебсторінок 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 платформи (*Library of Congress*, 2018).

Загалом Закон про електронну комерцію встановлює різні зобов'язання для комерційних онлайн-платформ та права для користувачів для запобігання зловживанням з боку платформ. Законом встановлюється досить зручний та зрозумілий поділ на бізнеси електронної комерції, які надають свої послуги і товари за допомогою одного сайту, бізнес-платформи електронної комерції, які окрім вищезазначеної діяльності можуть надавати майданчик для суб'єктів підприємницької діяльності, бізнеси на платформі, які є фізичними або юридичними особами, які здійснюють свою діяльність на майданчику комерційної онлайн-платформи (*Ministry of Commerce of the People's Republic of China*, 2019).

3.3. Ключові положення Закону про захист персональних даних КНР 2021 року та Закону про охорону персональних даних КНР 2021 року

Закон про захист персональних даних та Закон про охорону даних прийняті у 2021 р. 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 належить інформація, яка пов'язана з особистою гідністю, майновою й 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 й оброблятися тільки за виправданої та визначеної мети цього процесу і за згоди особи. Однак встановлено низку винятків, коли згода особи не потрібна, а саме: у випадку загрози життю чи здоров'ю особи, коли дані використовуються в ЗМІ 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 згоди особи. Так само як в Законі про кібербезпеку, 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, передача персональних даних за кордон тощо). Оцінка впливу охоплює визначення того, чи має обробка виправдану та законну мету, вплив на права та інтереси осіб тощо.

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

1. Сформувати 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 й адміністративні правила щодо обробки особистої інформації.

3. Регулярний випуск звіту про соціальну відповідальність щодо захисту персональної інформації, що 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 ці суб'єкти вносяться до переліку організацій, яким забороняється здійснювати обробку персональних даних осіб.

Передбачено 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, видалити персональні дані, 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, передбачає повноваження CAC, а саме: створювати стандарти захисту персональних даних, наглядати за обробкою персональних даних державними органами, приймати скарги (зокрема й анонімні) щодо порушень у сфері обробки персональних даних тощо. Також передбачається відповідальність за порушення зобов'язань у сфері захисту персональних даних. У випадку відмови усунути порушення може бути накладено штраф розміром до 1 000 000 юанів, а у серйозних випадках – до 50 000 000 юанів або 5% від річного обороту. Проти іноземних провайдерів також може бути застосований такий захід, як заморожування їх фінансових активів на території Китаю, або накладені інші види санкцій (*China Briefing*, 2021).

Закон про охорону персональних даних прийнятий у 2021 р. Метою регулювання цього документа є стандартизація діяльності з обробки даних, забезпечення безпеки даних, сприяння розвитку та використанню даних. Значна частина положень стосується зобов'язань держави зі створення стандартів захисту даних, відповідної інфраструктури тощо. Також держава повинна встановити систему захисту даних за категоріями та ступенями, впроваджуючи захист даних відповідно до ступеня їх важливості для економічного та соціального розвитку, а також ступеня небезпеки для національної безпеки, суспільних інтересів або законних прав та інтересів окремих осіб або організацій, що 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:

1. Проведення діяльності з обробки даних повинно здійснюватися відповідно до положень законів та адміністративних правил, створення і завершення системи управління безпекою даних для всього робочого процесу, організації та проведення навчання з безпеки даних, а також прийняття відповідних технічних та інших необхідних заходів для забезпечення безпеки даних.

2. Проведення діяльності з обробки даних має посилити моніторинг ризиків, і, якщо 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 застосовувати методи їх усунення, одразу 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 мають включати тип і обсяг важливих даних, що обробляються, обставини діяльності з обробки даних, ризики безпеки даних, з якими зіткнулися, та заходи щодо їх уснення тощо.

За порушення цих положень провайдери отримують попередження та вимогу усунути порушення, а також можливе накладення штрафу від 50 000 до 500 000 юанів, а у випадку неусунення порушення може бути накладено штраф розміром у 500 000–2 000 000 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 юанів (*China Briefing*, 2021).

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 проводитися інтернет-провайдерами й онлайн-платформами, дещо повторюють положення із Закону про кібербезпеку. Втім, 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 даватиме змогу державі втручатися в особисте життя користувачів. Також цими законами значно ускладнюється діяльність іноземних суб'єктів у сфері оброки 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. Отже, ці два закони спрямовані й на обмеження впливу іноземних *IT*-гігантів (насамперед американських). Окрім того, Законами закріплюється можливість заборони діяльності іноземних суб'єктів як покарання за порушення положень цих Законів.

3.4. Приклади реалізації політичної цензури щодо онлайн-платформ

Особливо важливим елементом у китайській системі регулювання онлайн-платформ є політична цензура. Загалом поняття "незаконний контент" у КНР містить у собі три категорії: політично шкідливий або чутливий контент, вульгарний контент та контент, пов'язаний з

неполітичною дезінформацією і чутками (*Wang*, 2020). Питання забороненої інформації детально висвітлено в Положеннях про управління екосистемою інформаційного контенту онлайн, виданих CAC. 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, підривом державної влади; інформація, яка шкодить національній честі та національним інтересам Китаю; інформація, яка розпалює етнічну ворожнечу, расову дискримінацію або порушує етнічну єдність; інформація, яка заподіює шкоду національній релігійній політиці та поширює феодальні забобони; інформація, що поширює чутки, порушує суспільний порядок і стабільність; інформація, що підбурює до незаконних зборів, демонстрацій, протестів, порушення громадського порядку тощо (*China Law Translate*, 2019). Вочевидь цей перелік забороненої інформації написано максимально розпливчасто, що дозволяє відносити до неї будь-який контент, який не подобається китайській владі.

Також варто додати, що для виробництва новин в інтернет-просторі онлайн-платформам та новинним сайтам необхідно отримати ліцензію від CAC. Згідно з Положеннями про управління інформаційних служб новин в інтернеті до новин відносяться саме висвітлення або повідомлення про публічні події або разючі соціальні інциденти, тоді як, наприклад, новини про спортивні події або в розважальній сфері цим документом не регулюються (*China Law Translate*, 2016). Ці положення, зокрема, можуть стосуватися і користувачів онлайн-платформ, які у своїх дописах можуть повідомляти власну інформацію про певні публічні події, а не просто поширювати дані, взяті з офіційних джерел. Однак в адміністрацій китайських онлайн-платформ часто виникають труднощі з визначенням, що входить до поняття "новини" згідно з вищезгаданими положеннями, а тому вони 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 капіталом (*Wang*, 2022).

Прикладами реалізації політичної цензури можуть слугувати такі випадки, які сталися з китайськими *IT*-гігантами. Наприклад, Китайська CAC змусила низку популярних китайських онлайн-платформ (*WeChat*, *Weibo* та *Tieba*) видалити майже 60 популярних акаунтів, які розповсюджували контент, в якому китайська влада вбачала "вульгарне та сенсаційне висвітлення скандалів зі знаменитостями та показного способу життя" (*Reuters*, 2017). Далі CAC у серпні 2017 р. наклала штрафи (у 500 000 юанів) на трійку провідних китайських інтернет-гігантів (*Tencent*, *Baidu* та *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, незначну 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-платформою (*Gao*, 2017).

Висновки

Можна підсумувати, що за майже 25 років Китай зумів успішно побудувати власну систему регулювання онлайн-платформ та контролю за власним сегментом інтернет-простору, засновану на авторитарному підході, що підтверджує зазначену у вступі гіпотезу. З одного боку, КНР змогла створити комплексну правову систему захисту своїх інтернет-користувачів від свавілля та порушень онлайн-платформ, яка є схожою на європейську систему регулювання онлайн-платформ; за допомогою державної підтримки в КНР були сформовані власні *IT*-гіганти, які могли конкурувати з американськими щодо розвитку інновацій у цифровій сфері. З іншого ж боку, ця система забезпечує тотальний контроль держави над інформацією, яка рухається китайським інтернет-сегментом, тобто створюється система політичної цензури.

Отже, можна виділити такі ключові особливості китайського авторитарного 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);
- формування 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 і виявлення незаконного контенту;
- забезпечення деанонімізації 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 розпливчастим трактуванням, що дозволяє забороняти будь-який контент, який не подобається китайській владі;
- формування власних *IT*-гігантів, які займаються розвитком інновацій з метою забезпечення Китаю технологічною незалежністю та суверенітетом у сфері цифрових технологій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ / REFERENCE

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

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

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/

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

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/

China's State Administration for Market Regulation releases interim provisions on Anti-Unfair competition on the internet. (2024, May 13). https://www.chinaiplawupdate.com/2024/05/chinas-state-administration-for-market-regulation-releases-interim-provisions-on-anti-unfair-competition-on-the-internet/

Companies Market Cap. (2024). *Top publicly traded internet companies by revenue.* https://companiesmarketcap.com/internet/largest-internet-companies-by-revenue/

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.

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/

DigiChina. (2021). *Translation: Data security law of the People's Republic of China.* https://digichina.stanford.edu/work/translation-data-security-law-of-the-peoples-republic-of-china/

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

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/

Gorwa, R. (2024). *The politics of platform regulation: How governments shape online content moderation.* Oxford Studies in Digital Politics. Oxford Academic. https://doi.org/10.1093/oso/9780197692851.001.0001

Hamza, A. (2024). *10 U.S. Websites Banned in China and Other Countries.* Listverse. https://listverse.com/2024/11/26/10-u-s-websites-banned-in-china-and-other-countries/

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/

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

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

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

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

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

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

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

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

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

Yang, S. (2021, June 6). China's tech clampdown is spreading like wildfire. *The Wall Street Journal.* https://www.wsj.com/articles/chinas-tech-clampdown-is-spreading-like-wildfire-11622971802

Zhang, A. H. (2022). Agility over stability: China's great reversal in regulating the platform economy. In *Harvard International Law Journal*, *63*(2). https://journals.law.harvard.edu/ilj/wp-content/uploads/sites/84/HLI203_crop-3.pdf

Zhang, A. H. (2024). *High wire: How China Regulates Big Tech and Governs Its Economy.* Oxford University Press.

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

Конфлікт інтересів. Автор заявляє, що він не має фінансових чи нефінансових конфліктів інтересів щодо цієї публікації; не має відносин з державними органами, комерційними або некомерційними організаціями, які могли б бути зацікавлені у поданні цієї точки зору. З огляду на те, що автор працює в установі, яка є видавцем журналу, що може зумовити потенційний конфлікт або підозру в упередженості, остаточне рішення про публікацію цієї статті (включно з вибором рецензентів і редакторів) приймалося тими членами редколегії, які не пов'язані з цією установою.

Автор не отримував прямого фінансування для цього дослідження.

Щербак Г. Регулювання онлайн-платформ у праві КНР. *Зовнішня торгівля: економіка, фінанси, право*. 2024. № 1. С. 111–129. Серія. Юридичні науки. https://doi.org/10.31617/3.2024(137)08

Надійшла до редакції 22.11.2024.
Прийнято до друку 02.12.2024.
Публікація онлайн 16.12.2024.