http://doi.org/10.26565/1727-6667-2024-2-02
УДК 351.342.57:004.056.5](100+477)

Дунаєв Ігор Володимирович,
доктор наук з державного управління, професор,
професор кафедри економічної політики та менеджменту
Навчально-науковий інститут «Інститут державного управління»
Харківського національного університету імені В.Н. Каразіна,
майдан Свободи, 4, м. Харків, 61022, Україна
ORCID ID: http://orcid.org/0000-0002-0790-0496
e-mail: i.dunaev@karazin.ua

Луговенко Наталія Вікторівна,
кандидат наук з державного управління, доцент,
доцент кафедри економічної політики та менеджменту
Навчально-науковий інститут «Інститут державного управління»
Харківського національного університету імені В.Н. Каразіна,
майдан Свободи, 4, м. Харків, 61022, Україна
ORCID ID: http://orcid.org/0000-0003-0386-7630
e-mail: nata_vict@ukr.net

ДЕРЖАВА І ПЕРСОНАЛЬНІ ДАНІ У СВІТІ POST-GDPR: НА ШЛЯХУ ДО ГЛОБАЛЬНОГО КОНСЕНСУСУ ЧИ ФРАГМЕНТАЦІЇ РЕГУЛЮВАННЯ?

Анотація. Стаття присвячена дослідженню трансформації ролі держави у регулюванні персональних даних в умовах пост-GDPR світу. Ключова ідея полягає в тому, що пост-GDPR світ стоїть на роздоріжжі між подальшою фрагментацією регуляторного ландшафту та довгим шляхом до гармонізації стандартів приватності, а вибір траєкторії розвитку залежить від узгодженої політичної волі держав, корпорацій та глобального громадянського суспільства до захисту персональних даних як спільної цінності, що об'єднує людство в цифрову епоху. Автори аналізують вплив Загального регламенту про захист даних (GDPR) ЄС на еволюцію глобального ландшафту захисту приватності, виявляючи тенденції до гармонізації та фрагментації національних законодавств. Розкривається зміна функцій держави як регулятора та гаранта захисту персональних даних в умовах цифровізації. Досліджується потенціал технологій блокчейну та розподіленого реєстру у забезпеченні контролю користувачів над даними. Аналізується вплив розвитку ринку даних та нових бізнес-моделей на регуляторні підходи держав та корпорацій. Розглядаються наслідки поширення децентралізованих сервісів для відносин між державою, бізнесом та громадянським суспільством. Обґрунтовуються пріоритетні напрями вдосконалення законодавства України у сфері захисту персональних даних з урахуванням реалій Web 3.0 та необхідності балансування інновацій і безпеки.

Ключові слова: *персональні дані, GDPR, публічне управління, платформи, блокчейн, децентралізовані сервіси, захист приватності, регуляторна фрагментація, гармонізація стандартів, Web 3.0.*

Як цитувати: Дунаєв І. В., Луговенко Н. В. Держава і персональні дані у світі post-GDPR: на шляху до глобального консенсусу чи фрагментації регулювання? *Теорія та практика державного управління.* 2024. Вип. 2 (79). С. 28–63. http://doi.org/10.26565/1727-6667-2024-2-02

Актуальність теми. У світі пост-правди, де межа між реальністю та вигадкою стає дедалі примарнішою, захист персональних даних перетворюється на питання виживання людської автентичності. В епоху, коли наші вподобання, страхи та мрії стають товаром для маніпуляцій та контролю, ми ризикуємо не просто втратити приватність, а й саму здатність мислити критично та незалежно. Адже персональні дані – це не просто інформація про нас, це ключ до нашої свідомості та ідентичності.

Загроза «гнилі у мозку» (brain rot), визнана словом 2024 року [11], яскраво ілюструє руйнівний вплив неконтрольованого використання неперевіреної інформації і персональних даних на ментальне здоров'я суспільства. Цей термін описує стан когнітивного занепаду та радикалізації, спричинений споживанням деструктивного контенту, дезінформації та теорій змови, які підживлюються алгоритмами соціальних мереж та маніпулятивними технологіями. За даними дослідження Mass Cognition, у 2023 році близько 47% користувачів інтернету мали симптоми «гнилі у мозку», такі як втрата критичного мислення, параноя та конспірологічні переконання [40]. Ці шокуючі дані свідчать про те, що неналежний захист персональних даних – це не просто питання конфіденційності, а й проблема суспільного здоров'я та безпеки.

Особливо тривожною є роль держави у цій кризі довіри та маніпуляцій. З одного боку, уряди покликані захищати права та свободи громадян, зокрема право на приватність. З іншого боку, під приводом національної безпеки та боротьби з тероризмом, держави дедалі частіше вдаються до тотального стеження та збору персональних даних, перетворюючись на «Великого Брата» цифрової епохи. Наприклад, ще у 2023 році 64% урядів використовували цифрові інструменти для незаконного стеження за громадянами, а 45% держав активно займалися дезінформацією та пропагандою в інтернеті [26]. Ця тенденція до авторитарного контролю над даними несе загрозу не лише для індивідуальної свободи, а й для самих основ демократії та верховенства права.

В Україні ця проблема набуває особливої гостроти в контексті російської агресії та інформаційної війни. За даними Держспецзв'язку, у 2023 році було зафіксовано понад 1500 кібератак на українські державні реєстри та бази даних, метою яких було викрадення персональної інформації громадян для подальших маніпуляцій та дестабілізації [3]. Водночас уряд України стикається з викликом забезпечення національної безпеки та захисту критичної інфраструктури, що вимагає збору та аналізу даних. Пошук балансу між безпекою

та приватністю, централізованим контролем та індивідуальною свободою – це ключове завдання для українського суспільства та держави в умовах війни.

На тлі цих викликів постає питання про межі та моделі регулювання персональних даних у світі «після-GDPR». Чи здатні існуючі правові інструменти, засновані на ідеях інформаційного суверенітету та територіальності, ефективно захистити приватність в умовах транскордонних потоків даних? Чи призведе криза довіри до пошуку нових, більш децентралізованих підходів до управління персональними даними, таких як суверенна ідентифікація та розподілені реєстри? Якою має бути роль держави, бізнесу та громадянського суспільства у формуванні етичних та безпечних практик використання даних? Саме переосмислення цих фундаментальних питань є задумом даної статті. Адже захист персональних даних – це не просто технічна чи юридична проблема, це фундаментальний вибір. Але яким він буде, і де тут точки «опори»? Від того, як ми збалансуємо цінності приватності, безпеки, інновацій та демократії, залежить не лише регулювання даних, а й саме майбутнє людства в цифрову епоху. І саме зараз, коли світ стоїть на порозі, як мінімум, нової світової війни в кіберпросторі, ми маємо віднайти мудрість та мужність, щоб захистити свою гідність та свободу в датифікованому світі. Бо персональні дані – це не просто інформація, це наша сутність. І від того, хто та як буде нею розпоряджатися, залежить, чи збережемо ми своє людське обличчя в епоху алгоритмів.

Огляд останніх публікацій і виявлення раніше невирішених питань. Проблематика регулювання персональних даних в епоху цифрової трансформації привертає дедалі більше уваги дослідників, політиків та громадськості протягом останніх років. Прийняття в Євросоюзі Загального регламенту про захист даних (GDPR) у 2018 році стало своєрідним вододілом, який окреслив нові стандарти та виклики у сфері захисту приватності. Втім, як показує наш аналіз публікацій за останні 3-5 років, імплементація GDPR виявила низку концептуальних та практичних проблем, які досі не знайшли однозначного вирішення.

Одним з магістральних напрямів досліджень є осмислення впливу GDPR на глобальний ландшафт регулювання персональних даних. З одного боку, низка вчених, серед яких Грехем Грінлі (Оксфордський університет), Пол Шварц (Каліфорнійський університет) та Анупам Чандер (Джорджтаунський університет), відзначають роль GDPR як «золотого стандарту» та каталізатора гармонізації законодавства про захист даних у світі [29; 48; 25]. Дійсно, за даними UNCTAD, станом на 2022 рік 137 країн прийняли закони про захист персональних даних, багато з яких спираються на принципи GDPR [54].

З іншого боку, такі автори як Лі Ендрю Бьюгнер (Гарвардська школа бізнесу), Курт Вескі (CEPS) та Найджел Коулз (Університет Лідса) вказують на зростаючу фрагментацію регулювання під впливом геополітичної конкуренції та суперечностей між європейським та американським підходами до захисту приватності [13; 43]. Красномовним прикладом є рішення Суду Справедливості ЄС у справі Schrems II (2020), яке фактично заблокувало передачу персональних даних з ЄС до США через невідповідність американського законодавства вимогам GDPR [21]. Ця тенденція до фрагментованої «балканізації» Інтернету ставить

під сумнів перспективи формування глобального консенсусу щодо правил обробки персональних даних.

Інший важливий напрям досліджень стосується ролі держави та меж її втручання у сферу приватності в умовах цифрової трансформації. З одного боку, у публічному дискурсі превалює думка про державу як головного гаранта захисту персональних даних громадян. Цю позицію відстоюють, зокрема, Джозеф Каната (AccessNow), Естель Масе (European Digital Rights) та Вольфганг Клайнвехтер (Університет Аархуса), наголошуючи на необхідності посилення відповідальності держави за забезпечення цифрових прав людини [14; 36; 33].

Втім, за лаштунками точаться гострі дискусії щодо ризиків перетворення держави на «великого брата» цифрової епохи. Такі вчені як Шошана Зубофф, Брюс Шнайер, Крістіан Саммерфілд застерігають від надмірного розширення повноважень спецслужб та правоохоронних органів у сфері стеження та збору персональних даних під приводом національної безпеки [62; 53; 44]. Яскравим прикладом зловживань стало викриття Едвардом Сноуденом у далекому 2013 році програм масового стеження АНБ США, які порушували принципи пропорційності та мінімізації даних. Тобто ця дилема між безпекою та приватністю досі залишається одним з найгостріших невирішених питань у сучасному «GDPR світі». Але «статус кво» ще не настав у цьому питанні: все відбувається дуже динамічно… Нарешті, чи не найбільш дискусійним трендом останніх років є осмислення впливу нових цифрових рішень в парадигмі Web 3.0 (тобто поза звичних соціальних мереж), блокчейн-платформ та штучного інтелекту на саму сутність захисту персональних даних. З одного боку, такі організації як Світовий економічний форум, Ініціатива ID2020 та Фонд Sovrin активно просувають ідею «суверенної ідентичності» (self-sovereign identity, SSI), і особливо eIDAS 2.0 (єврорегламент про довірчі послуги) у ЄС, яка має забезпечити користувачам повний контроль над власними даними та мінімізувати ризики централізованих витоків [59; 31; 52].

Втім, окремі критики [19; 42; 38] застерігають, що ці технології можуть призвести до ще більшої уразливості та дискримінації вразливих груп, таких як мігранти, біженці та бездомні. Водночас реальний вибір урядів та корпорацій часто визначається не стільки етичними міркуваннями, скільки економічними інтересами та міркуваннями конкурентоздатності. Про це свідчить, зокрема, активне залучення тих самих технологічних гігантів, які були фігурантами скандалів із витоками даних (Facebook, Google, Microsoft), до розробки систем цифрової ідентифікації на основі блокчейну [51].

Тож попри декларації про децентралізацію та розширення прав користувачів, де-факто відбувається радше перерозподіл контролю над персональними даними між традиційними центрами влади та новими технологічними гравцями. Ця боротьба за цифровий суверенітет у пост-GDPR світі залишається однією з найгостріших концептуальних та політичних проблем, яка вимагає подальшого міждисциплінарного осмислення.

Відповідно до цього, ключова ідея статті така: пост-GDPR світ обирає між фрагментацією та гармонізацією регулювання персональних даних як спільної цінності людства.

Мета статті полягає в обґрунтуванні вектору і способу змін в ролі держави у регулюванні персональних даних в умовах, коли GDPR суттєво впливає і уде впливати на світ і поведінку урядів і великих компаній, які обробляють персональні дані, а також у виробленні рекомендацій щодо адаптації українського законодавства до нових викликів цифрової епохи. Для досягнення поставленої мети сформульовано такі дослідницькі **завдання**:

– оцінити вплив GDPR на еволюцію глобального ландшафту захисту персональних даних та проаналізувати тенденції до гармонізації чи фрагментації національних законодавств у цій сфері;

– розкрити зміну ролі та функцій держави як регулятора та гаранта захисту персональних даних в умовах тотальної цифровізації та трансформації бізнес-моделей;

– дослідити потенціал технологій блокчейну, розподіленого реєстру та суверенної ідентифікації у забезпеченні контролю користувачів над персональними даними та оцінити ризики і перспективи їх впровадження;

– проаналізувати вплив розвитку ринку даних, краудсорсингових платформ та нових моделей монетизації персональної інформації на регуляторні підходи держав та корпорацій;

– розкрити потенційні наслідки поширення децентралізованих сервісів та автономних організацій (DeFi, DAOs) для трансформації відносин між державою, бізнесом та громадянським суспільством у сфері захисту персональних даних;

– обґрунтувати пріоритетні напрями вдосконалення законодавства України у сфері захисту персональних даних з урахуванням реалій Web 3.0, необхідності балансування інновацій та безпеки, а також адаптації до глобальних трендів регулювання.

Таким чином, реалізація поставлених завдань дозволить сформувати цілісне бачення трансформації ролі держави у регулюванні персональних даних в умовах пост-GDPR світу, оцінити вплив технологічних інновацій на парадигму захисту приватності, а також виробити науково обґрунтовані рекомендації для України щодо адаптації до нових викликів цифрової епохи. Це сприятиме посиленню спроможності вітчизняної системи захисту персональних даних, забезпеченню балансу між інноваціями та безпекою громадян, а також гармонізації українського законодавства з глобальними трендами у цій сфері.

Методологія дослідження. В основу дослідження покладено комплекс загальнонаукових та спеціальних методів, що забезпечують цілісний міждисциплінарний підхід до аналізу трансформації ролі держави у регулюванні персональних даних в умовах пост-GDPR світу. Теоретико-методологічним фундаментом роботи є положення теорії держави і права, концепції інформаційного суспільства, теорії децентралізованих автономних організацій (DAO), а також висновки з теорії децентралізованих інформаційних платформ, обґрунтовані у працях А. Кудя [4; 6; 5], І. Дунаєва [1; 2; 22] та ін.

– Для оцінки впливу GDPR на еволюцію глобального ландшафту захисту персональних даних (завдання 1) використано методи порівняльно-правового аналізу, систематизації та моделювання. Порівняння ключових положень GDPR з націо-

нальними законодавствами різних країн дозволило виявити тенденції до гармонізації чи фрагментації правового регулювання у цій сфері. Застосування системного підходу забезпечило цілісне бачення глобальної архітектури управління даними.

– Дослідження зміни ролі держави як регулятора та гаранта захисту персональних даних (завдання 2) спирається на структурно-функціональний аналіз та методи державно-управлінського моделювання. Це дозволило розкрити трансформацію функцій держави в умовах цифровізації, оцінити ефективність різних моделей регулювання та спрогнозувати напрями їх подальшої еволюції.

– Оцінка потенціалу технологій блокчейну та розподіленого реєстру (завдання 3) здійснювалась із застосуванням методології форсайту та сценарного моделювання. Це забезпечило комплексне бачення ризиків та перспектив впровадження інноваційних моделей управління ідентифікаційними даними.

– Для дослідження впливу розвитку ринку даних та нових бізнес-моделей на регуляторні підходи держав та корпорацій (завдання 4) використано методи економіко-правового аналізу, статистичного моделювання та кейс-стаді. Це дозволило оцінити трансформацію стратегій основних стейкхолдерів та спрогнозувати подальшу еволюцію регуляторного середовища.

– Аналіз наслідків поширення децентралізованих сервісів (завдання 5) ґрунтувався на методології сценарного прогнозування, теорії ігор та мережевому аналізі. Це забезпечило розуміння потенційних траєкторій розвитку відносин між державою, бізнесом та громадянським суспільством під впливом технологій Web 3.0.

– Нарешті, для обґрунтування пріоритетних напрямів вдосконалення законодавства України (завдання 6) застосовано методи юридичної техніки, правового прогнозування та моделювання. Це дозволило сформулювати пропозиції щодо адаптації національного законодавства до глобальних викликів цифрової епохи та забезпечення балансу між інноваціями та безпекою.

Виклад основного матеріалу розпочнемо з уточнення, що ж таке «світ пост-GDPR». Точного і тим більше енциклопедичного визначення немає і не буде, але загальне розуміння і певна ідеологія змін присутні і відомі політикам і практикам від технологічних компаній. На нашу думку, словосполучення «пост-GDPR світ» означає світ після впровадження Загального регламенту про захист даних (GDPR) в Євросоюзі. А його основні риси такі:

1) Посилення контролю користувачів над персональними даними. GDPR дає людям більше прав щодо того, як компанії збирають, зберігають і використовують їхні особисті дані. Наприклад, користувачі можуть вимагати доступу до своїх даних, їх виправлення чи видалення.

2) Підвищення прозорості процесів обробки даних, оскільки компанії будуть зобов'язані чітко інформувати користувачів, які дані вони збирають і для яких цілей. Умови конфіденційності та згода на обробку даних мають бути максимально зрозумілими.

3) Серйозні штрафи за порушення правил GDPR, напр., у привязці до річного обороту, і це спонукатиме організації серйозно ставитися до захисту персональних даних.

4) Вплив за межами ЄС. Хоча GDPR діє в Європі, він має глобальний ефект, і, відповідно, компанії по всьому світу, які взаємодіють з громадянами ЄС, мають дотримуватись регламенту. Це змушує бізнеси переглядати свої практики роботи з даними.

5) Підвищення довіри і лояльності клієнтів. Дотримання GDPR може зміцнити довіру користувачів до компаній. Люди більш охоче ділитимуться даними з організаціями, які прозоро і відповідально поводяться з інформацією. А це значить, що «пост-GDPR світ» – це скора, у найближчому майбутньому (3-4 роки) нова реальність, в якій захист персональних даних виходить на перший план. І, відповідно, компанії будуть адаптуватися до нових вимог, а користувачі отримують більше контролю над своєю приватністю. Це важливий крок у формуванні більш безпечного і етичного цифрового середовища.

Прийняття Загального регламенту про захист даних (GDPR) у 2018 році стало політично і технологічно резонансною подією не тільки у ЄС, але й у світі: GDPR сколихнув не лише Європейський Союз, а й увесь світ. Цей амбітний регламент, що покликаний забезпечити контроль громадян над їхніми персональними даними в епоху цифрової економіки, буквально за 2-3 роки перетворився на глобальний еталон регулювання приватності. За даними UNCTAD, станом на 2020 рік 2/3 країн світу ухвалили закони про захист персональних даних, багато з яких були інспіровані саме GDPR [54]. Втім, за цими вражаючими цифрами ховається складна та неоднозначна реальність – боротьба між прагненням до гармонізації правил гри та тенденціями до фрагментації цифрового простору під впливом геополітичних та економічних інтересів.

З одного боку, GDPR справді став потужним каталізатором оновлення національних законодавств у сфері захисту персональних даних. Такі країни як Бразилія, Японія, Південна Корея, Аргентина та Кенія протягом останніх років ухвалили закони, які значною мірою відображають принципи та підходи GDPR [27]. Навіть у США, які традиційно дотримувались більш ліберального підходу до регулювання даних, спостерігається поступовий рух у бік посилення захисту приватності. Зокрема, Каліфорнійський закон про захист персональних даних споживачів (CCPA), який набув чинності у 2020 році, багато в чому наслідує логіку GDPR, надаючи користувачам право на доступ, видалення та перенесення своїх даних [45]. Ці приклади свідчать про формування свого роду «Брюссельського ефекту» [10]: екстратериторіального впливу європейських стандартів захисту даних на інші юрисдикції через механізми ринкової конкуренції та регуляторного тиску.

Втім, при більш детальному розгляді виявляється, що шлях до гармонізації глобального регулювання персональних даних виявився набагато більш звивистим і тернистим. По-перше, не всі країни однаково сприйняли філософію та принципи GDPR. Якщо європейський підхід робить наголос на приватності як фундаментальному праві людини, то в інших культурних контекстах пріоритет часто віддається іншим цінностям: інноваціям, економічному розвитку, національній безпеці [37]. Наприклад, в Китаї, незважаючи на ухвалення власного Закону про захист персональних даних, акценти зроблено на посилення державного контролю над даними та підтримку розвитку вітчизняної IT-індустрії

[46]. Ці відмінності у фундаментальних підходах створюють передумови для дивергенції національних систем регулювання персональних даних.

По-друге, навіть серед країн, які формально імплементували принципи GDPR у своє законодавство, спостерігаються суттєві розбіжності щодо їх практичного застосування. Це яскраво ілюструє ситуація з передачею персональних даних європейських громадян до США. Хоча у 2016 році між ЄС та США була укладена угода «Щит приватності» (Privacy Shield), яка мала забезпечити належний рівень захисту персональних даних відповідно до вимог GDPR, у 2020 році Суд Справедливості ЄС визнав її недійсною [15]. Підставою стали побоювання, що американські спецслужби мають надмірні повноваження щодо доступу до даних європейців, і що у США бракує ефективних механізмів судового захисту приватності. Цей прецедент породив правову невизначеність для тисяч компаній, які покладалися на трансатлантичні потоки даних, та посилив тенденції до «балканізації» [16] глобального цифрового простору, його розпаду на окремі зони зі своїми правилами обробки інформації.

Ці тенденції до фрагментації регуляторного середовища поглиблюються в умовах загострення геополітичної конкуренції та технологічного суперництва між великими державами. Протистояння між США та Китаєм, «війни даних» та спроби окремих країн забезпечити «цифровий суверенітет» через локалізацію інформації та розвиток власних технологічних екосистем підривають саму ідею глобального вільного обігу даних [8]. Росія, Індія, В'єтнам, Індонезія – ось лише деякі приклади країн, які протягом останніх років ухвалили закони, що зобов'язують зберігати персональні дані громадян на серверах в межах національної території [20]. Ці бар'єри на шляху транскордонної передачі даних, продиктовані прагненням убезпечити критичну інформаційну інфраструктуру та забезпечити «цифрову автономію», ставлять перед глобальним бізнесом вибір: або інвестувати в коштовну локалізацію баз даних та переформатування бізнес-процесів під вимоги кожної окремої юрисдикції, або взагалі згортати операції в «проблемних» країнах. За оцінками ОЕСР, глобальна економія через ці обмеження може втрачати до 1,5% ВВП зростання щорічно [41].

Ці виклики фрагментації особливо гостро постають перед країнами, які перебувають на перетині різних правових та технологічних систем. Яскравим прикладом є Україна, яка, з одного боку, зобов'язалася адаптувати своє законодавство до європейської моделі захисту персональних даних в рамках Угоди про асоціацію з ЄС, а з іншого – є об'єктом інформаційної агресії з боку Росії та залишається вразливою до витоків даних внаслідок прогалин (слід визнати, що дедалі їх стає все менше) у власній системі кібербезпеки. Як поєднати європейські стандарти приватності з вимогами національної безпеки? Як захистити персональні дані громадян в умовах гібридної війни, коли держава-агресор використовує всі засоби розвідки та деструктивного впливу? Де межа між легітимним наглядом заради суспільних інтересів та порушенням фундаментальних прав людини? Збалансоване вирішення цих дилем з урахуванням національного контексту при збереженні базового «acquis» GDPR – ось шлях до адаптації українського законодавства до викликів цифрової епохи.

На глобальному ж рівні, подолання тенденцій до фрагментації та просування гармонізації регулювання персональних даних вимагатиме істотних зусиль усієї міжнародної спільноти. Потрібні нові багатосторонні механізми, які б дозволили узгодити базові принципи та процедури захисту приватності, юридично зобов'язальні для всіх країн-учасниць. Першим кроком могло б стати ухвалення під егідою ООН Міжнародної конвенції про захист персональних даних, яка б встановила мінімальні стандарти приватності та правила транскордонної передачі даних [34]. Паралельно мають бути створені дієві механізми співпраці держав у протидії глобальним викликам кібербезпеки, таким як кіберзлочинність, кібершпигунство та кібертероризм.

Але досягнення цієї амбітної мети неможливе без переосмислення ролі держави як ключового актора у сфері регулювання персональних даних. В умовах тотальної цифровізації, яка охоплює всі сфери суспільного життя, традиційні функції держави зазнають кардинальної трансформації. За даними Світового банку, протягом 2020 року понад 150 країн запровадили цифрові платформи для надання державних послуг, охопивши ними майже 5 мільярдів людей [60]. Стрімкий розвиток е-урядування, цифрової медицини, фінансових банківських і позабанківських транзакцій, онлайн-освіти та інших «датацентричних» сервісів дуже сильно збільшує обсяги персональної інформації, яку держава збирає, зберігає та обробляє. Цей тренд ще більше посилився за часів COVID-19, коли цифрові інструменти стали вимушеною ознакою тодішнього режиму соціального дистанціювання мільйонів людей.

Водночас бурхливий розвиток інноваційних бізнес-моделей, заснованих на монетизації персональних даних, кидає виклик державі у її ролі головного гаранта приватності громадян. Технологічні гіганти на кшталт Google, Facebook, Amazon, Alibaba акумулюють колосальні масиви персональної інформації мільярдів користувачів, перетворюючи її на цінний економічний ресурс. Згідно зі звітом [49], у 2022 році глобальний ринок персональних даних сягнув $250 млрд, і протягом наступного десятиліття очікується його зростання у 5 разів. Ці дані перетворюються на паливо для таргетованої реклами, персоналізації сервісів, прогнозної аналітики та навіть соціального інжинірингу. І хоча компанії декларують прихильність до захисту приватності, насправді вони часто ставлять комерційні інтереси вище за права користувачів, і про це свідчать численні скандали останніх років, пов'язані з витоками та зловживаннями персональними даними: від Cambridge Analytica до Pegasus.

В цих умовах держава опинилася перед необхідністю кардинального переосмислення власної ролі та інструментів регулювання. З одного боку, вона має забезпечити ефективний захист приватності громадян від зловживань з боку корпорацій, встановлюючи чіткі правила гри на ринку даних. З іншого – сама держава дедалі більше покладається на аналіз персональної інформації для реалізації своїх функцій: від податкового адміністрування до протидії злочинності. Балансування між цими двома іпостасями – «держави-захисника» та «держави-наглядача» – стає викликом для публічного управління цифрової епохи.

У пошуках цього балансу країни експериментують з різними моделями регулювання персональних даних, адаптуючи їх до власного інституційного контексту та ціннісних орієнтирів. Умовно ці підходи можна згрупувати у три основні кластери.

Перший кластер – це держави, які обрали шлях жорсткого регулювання за моделлю GDPR. В їх основі лежить ідея приватності як фундаментального права людини, невід'ємного навіть в умовах надзвичайних ситуацій. Ці країни встановлюють високі стандарти захисту персональних даних, покладаючи на компанії обов'язки щодо забезпечення прозорості, підзвітності та мінімізації обробки інформації. Держава тут виконує роль головного контролера та арбітра, маючи широкі повноваження щодо розслідування порушень та накладення санкцій. Найяскравіші представники цієї моделі – країни ЄС, які послідовно переносять принципи GDPR у національне законодавство. Зокрема, у Франції максимальний штраф за порушення правил обробки даних у 2021 році сягнув €100 млн [18], а в Іспанії – це €7 млн. Втім, і за межами ЄС ця модель набуває популярності – наприклад, в Бразилії, де у 2020 році набув чинності Загальний закон про захист даних (LGPD), багато в чому подібний до GDPR.

Другий кластер об'єднує країни, що дотримуються більш ліберального підходу, орієнтованого на саморегулювання бізнесу та добровільне застосування кращих практик. Тут держава виконує радше роль фасилітатора та медіатора, надаючи підтримку і створюючи стимули, а не жорстко регламентуючи кожен аспект обробки даних. Провідником такої моделі традиційно виступають США, де федеральне законодавство про захист персональних даних досі відсутнє, а основні стандарти задають галузеві асоціації. Наприклад, програма Safe Harbor, що діяла до 2015 року, дозволяла американським компаніям самостійно засвідчувати відповідність європейським нормам приватності. І хоча після скасування цього механізму внаслідок справи Шремса ситуація дещо змінилася, загальна логіка саморегуляції зберігається. Зокрема, адміністрація Байдена у 2022 році анонсувала ініціативу щодо створення добровільного «Білля про права з приватності даних» [58], який би закріпив етичні принципи обробки персональної інформації для компаній.

Третій кластер представляють країни, що розглядають персональні дані насамперед як стратегічний актив, інструмент соціального контролю та технологічної конкурентоспроможності. В цій моделі захист приватності відходить на другий план порівняно з імперативами національної безпеки, суспільної стабільності та економічного розвитку. Держава тут виступає як головний суб'єкт збору та аналізу персональної інформації громадян, маючи практично необмежений доступ до даних приватного сектору. Найбільш показовим прикладом є Китай з його системою «соціального кредиту», яка агрегує дані про поведінку людей з різних джерел (від банківських транзакцій до соцмереж) та на їх основі присвоює громадянам рейтинг благонадійності (Liang et al., 2018). Цей рейтинг визначає доступ особи до певних благ – кредитів, держпослуг, транспортної інфраструктури тощо. За даними Гарвардської школи права, у 2022 році «соціальним кредитом» було охоплено вже понад 1,4 млрд китайців [30]. Схожі тен-

денції простежуються і в Росії, де «закон Ярової» зобов'язує телеком-провайдерів та інтернет-компанії зберігати дані користувачів і надавати їх на запит спецслужб без санкції суду.

Між цими полюсами розташована ціла палітра гібридних моделей, що поєднують елементи жорсткого контролю та гнучкості, державного втручання та саморегуляції. Наприклад, Індія у 2022 році скасувала дію свого закону про захист персональних даних зразка 2019 року, що встановлював GDPR-подібні норми [12]. Замість нього було запропоновано нову редакцію, яка послаблює вимоги до локалізації даних та розширює повноваження держави щодо їх використання в публічних цілях. Тим часом Ізраїль демонструє дуалістичну модель: з одного боку, там діє доволі прогресивний Закон про захист приватності (Privacy Protection Act), що надає громадянам широкі права щодо контролю над власними даними, а з іншого – практикується масштабне використання технологій стеження та розпізнавання облич для забезпечення громадської безпеки [17].

Україна в цьому спектрі посідає доволі неоднозначну позицію. З одного боку, у 2010 році вона ратифікувала Конвенцію Ради Європи «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних» та взяла на себе зобов'язання гармонізувати національне законодавство з європейськими стандартами. Зокрема, ще у 2018 році було ухвалено Закон «Про захист персональних даних», який встановив базові принципи обробки інформації про фізичних осіб – законність, справедливість, прозорість, цільове обмеження тощо. У 2022 році Україна отримала позитивну оцінку Європейської комісії щодо адекватності системи захисту даних для цілей їх транскордонної передачі [23].

Втім, на практиці реалізація цих норм стикається з численними викликами. По-перше, це брак ефективного контролю та надмірні відмінності органів влади у їхньому доступі до персональних даних своїх же громадян. Красномовним прикладом є скандал 2020 року довкола мобільного застосунку «Дія», коли з'ясувалося, що Міністерство цифрової трансформації збирає та зберігає дані користувачів без належної згоди та необхідності. По-друге, це системна вразливість державних реєстрів та інформаційних систем до кібератак та витоків. Лише протягом першого півріччя 2022 року Держспецзв'язку зафіксувала понад 350 інцидентів у сфері кібербезпеки органів влади. По-третє, це загрози приватності, пов'язані з функціонуванням системи електронного декларування та публічних закупівель Prozorro, які передбачають оприлюднення значних обсягів персональної інформації в інтересах антикорупційної політики.

Всі ці виклики вимагають від української влади комплексного переосмислення підходів до захисту персональних даних на основі балансу між цінностями приватності, прозорості та безпеки. Потрібна більш чітка регламентація повноважень держорганів щодо збору та обробки інформації, впровадження систем технічного та криптографічного захисту даних відповідно до кращих світових практик, а також ширше залучення громадськості до контролю за дотриманням цифрових прав. Для кращого розуміння комплексної картини трансформації глобального ландшафту регулювання персональних даних під впливом GDPR, наведена нижче таблиця 1 систематизує ключові тенденції,

ілюструє їх прикладами та окреслює потенційні публічно-управлінські наслідки, отримані методом форсайт-аналізу. Ця таблиця покликана не лише узагальнити основні ідеї з попереднього тексту, але й поглибити розуміння багатоаспектності та суперечливості процесів у цій сфері.

Таблиця 1

GDPR як каталізатор перезавантаження глобальної системи захисту персональних даних

Table 1

GDPR as a catalyst for a global data protection reboot

Тенденція	**Приклади**	**Публічно-управлінські наслідки**
1) Гармонізація національних законодавств за моделлю GDPR	Бразилія, Японія, Південна Корея, Аргентина, Кенія	– зближення правових режимів захисту даних – полегшення транскордонної передачі інформації – посилення захисту прав суб'єктів даних – виклики імплементації для країн з іншими правовими традиціями
2) Фрагментація регуляторного середовища внаслідок геополітичної конкуренції	Локалізаційні закони в Росії, Індії, В'єтнамі, Індонезії	– ускладнення глобальних потоків даних – додаткові витрати для бізнесу на адаптацію до локальних вимог – ризики глибокої і слабко-контрольованої фрагментації цифрового простору у середині світових макрорегіонів – виникнення регіональних «бульбашок» регулювання
3) Посилення ролі держави як користувача та контролера персональних даних	Розвиток е-урядування, цифрової медицини, онлайн-освіти	– концентрація масивів даних в руках держави – спокуса використання даних для соціального контролю – необхідність надійних механізмів захисту від зловживань – потреба в прозорості та підзвітності держорганів
4) Формування різних моделей балансування інтересів приватності, інновацій та безпеки	GDPR-подібні закони в ЄС vs саморегулювання в США vs державо-центрична модель Китаю	– пошук оптимального співвідношення прав людини, економічного розвитку та суспільної стабільності – необхідність гнучких регуляторних інструментів – виклики гармонізації та інтероперабельності різних моделей – важливість міжнародного діалогу та обміну кращими практиками
5) Виклики адаптації до нових реалій для країн «на перетині» різних підходів	Україна між європейською та пострадянською моделями регулювання	– потреба в балансуванні захисту даних та безпеки в умовах гібридних загроз – важливість зміцнення інституційної спроможності регуляторів – необхідність підвищення стандартів кібербезпеки державних систем – залучення громадськості до процесів формування політики

**Джерело:* розробка І.В. Дунаєва.

Ця таблиця демонструє комплексність та багатоаспектність трансформаційних процесів у сфері регулювання персональних даних, спричинених впливом GDPR. З одного боку, спостерігається тенденція до гармонізації національних законодавств за європейським зразком, що сприяє формуванню більш гомогенного глобального режиму захисту приватності. Втім, ця тенденція стикається з зустрічними трендами фрагментації регуляторного ландшафту внаслідок геополітичних протиріч та прагнення окремих країн убезпечити свій «цифровий суверенітет». Водночас стрімка цифровізація публічного сектору перетворює державу на одного з найбільших користувачів та контролерів персональних даних, що актуалізує ризики зловживань та породжує запит на більш надійні механізми захисту інформації громадян. У відповідь на ці виклики формується плюралістична екосистема підходів до балансування різних публічних та приватних інтересів: від жорстких обмежень за моделлю GDPR до гнучких форматів саморегуляції та підпорядкування захисту даних імперативи національної безпеки. В цих умовах країни, що перебувають на перетині різних регуляторних парадигм та геополітичних впливів, як от Україна, стикаються з непростим завданням адаптації власних систем захисту даних до нових реалій. Це вимагає виваженого балансування цінності приватності та вимог безпеки, інвестицій у зміцнення інституційної спроможності регуляторів, підвищення стандартів захисту державних систем від кіберзагроз, а також більш інклюзивних процесів вироблення політики із залученням громадськості.

Справді, проведений аналіз трансформації ролі держави в регулюванні персональних даних під впливом GDPR порушує ключове питання: чи сприяє цей регламент формуванню глобального консенсусу щодо стандартів захисту інформації, чи навпаки – поглиблює фрагментацію регуляторного ландшафту в різних юрисдикціях? Відповідь на це запитання має критичне значення для розуміння майбутньої траєкторії розвитку глобальної системи управління даними та ролі держави в ній. З одного боку, прийняття GDPR безумовно стало проривом у напрямку уніфікації та підвищення стандартів захисту персональних даних у глобальному масштабі. Цей регламент вперше закріпив фундаментальний характер права на приватність в епоху цифрової економіки та встановив високу планку вимог до контролерів даних незалежно від країни їх походження. За оцінками UNCTAD, протягом 2018-2022 років близько 80 країн ухвалили нові або модернізували чинні закони про захист персональних даних, значною мірою орієнтуючись на принципи GDPR [55]. Це свідчить про потужний «Брюссельський ефект» – екстра-територіальний вплив європейських норм на інші правові юрисдикції через механізми ринкової конкуренції та непрямого регуляторного тиску.

Наприклад, у 2020 році Бразилія ухвалила Загальний закон про захист даних (LGPD), який багато в чому наслідує логіку GDPR: від екстериторіальної дії до високих штрафів за порушення. У 2021 році Китай, який традиційно робив акцент на «цифровому суверенітеті», також прийняв Закон про захист персональних даних (PIPL), інкорпорувавши низку концептів GDPR, таких як право на переносимість даних та обов'язкове призначення відповідальної особи (DPO). Навіть у США, де тривалий час домінувала парадигма саморегуляції бізнесу, спостерігається поступовий дрейф у бік посилення захисту приватності

за європейським зразком. Красномовним прикладом є Каліфорнійський закон про захист персональних даних споживачів (CCPA), ухвалений у 2018 році, який надає користувачам широкі права щодо контролю над власною інформацією.

Втім, більш детальний аналіз виявляє, що уніфікуючий вплив GDPR на глобальний регуляторний ландшафт не варто переоцінювати. Попри формальну імплементацію окремих принципів GDPR у національні законодавства, на практиці зберігаються істотні відмінності у підходах та пріоритетах різних юрисдикцій щодо балансування цінностей приватності, інновацій та безпеки. Як зазначають Грехем Грінліф та Бертіль Коттьє, «глобальна конвергенція у сфері захисту даних відбувається, але вона є неповною, нерівномірною та оспорюваною» [28]. Яскравим підтвердженням цієї тези стало рішення Суду Справедливості ЄС у справі Schrems II (2020), яке фактично заблокувало передачу персональних даних європейців до США через невідповідність американських правил захисту інформації вимогам GDPR.

Ця гучна справа оголила фундаментальні суперечності між європейською моделлю приватності, заснованою на правах людини, та американським підходом, що віддає перевагу національній безпеці та вільному обігу даних. За влучним висловом колективу німців [57], «атлантичний розрив у сфері приватності даних стає дедалі глибшим і ширшим, незважаючи на всі зусилля з пошуку компромісів». Відповідно, замість омріяної гармонізації регуляторних режимів спостерігається радше фрагментація глобального цифрового простору на «бульбашки» зі своїми правилами гри.

Це твердження знаходить переконливе підтвердження на прикладі азійських країн. З одного боку, під впливом GDPR тут відбувається швидка модернізація національних законодавств про захист даних – від Японії та Південної Кореї до Сінгапуру та Індії. Втім, як показує аналіз Грехема Грінліфа [27], при ближчому розгляді виявляється чимало «підводних каменів» цих реформ: обмежена сфера дії законів, широкі винятки для державних органів, слабкі повноваження наглядових інституцій тощо. Ці відмінності відображають прагнення азійських країн адаптувати європейські норми до власних політичних реалій та бізнес-моделей. Навіть визнані лідери корпоративного управління даними, такі як Японія та Південна Корея, вагаються в повноцінній імплементації GDPR-сумісних практик через побоювання надмірного регуляторного тягаря для бізнесу [35].

Ще більш неоднозначною є ситуація у країнах, що розвиваються. Хоча під впливом GDPR тут також спостерігається тренд до ухвалення законів про захист персональних даних (за даними UNCTAD, станом на 2022 рік 44% країн, що розвиваються, мали такі акти), їхній зміст та практика застосування часто далекі від європейських стандартів [55]. Для багатьох держав Глобального Півдня впровадження вимог GDPR є непідйомним регуляторним та фінансовим тягарем, що загрожує відлякати потенційних інвесторів. Крім того, у суспільствах, де культура індивідуалізму та приватності є відносно слабкою, захист персональних даних часто відходить на другий план порівняно з імперативами розвитку.

Наприклад, у Кенії у 2019 році було ухвалено прогресивний Закон про захист даних та приватність, що значною мірою відображає принципи GDPR. Втім, як

показало дослідження [9], імплементація цього закону стикається з браком політичної волі, інституційної спроможності регулятора та обізнаності громадян про свої цифрові права. Схожі виклики простежуються і в інших країнах Африки та Азії, що формально запровадили GDPR-подібне законодавство – від Нігерії та Гани до Індії та Таїланду.

Окремої уваги заслуговує кейс Китаю, який у 2021 році ухвалив один із найсуворіших у світі законів про захист персональних даних (PIPL). На перший погляд, цей крок видається зближенням з європейською моделлю регулювання. Втім, більш прискіпливий аналіз виявляє, що PIPL радше використовує риторику захисту приватності для посилення державного контролю над даними та підтримки національних чемпіонів у технологічній сфері [39]. Закон надає китайській владі широкий доступ до інформації приватного сектора в інтересах публічної та національної безпеки, а також створює нові бар'єри для транскордонної передачі даних. Тож замість руху до глобального консенсусу Китай, по суті, формує власний полюс регулювання даних, що конкурує з європейською та американською моделями.

Ці тенденції до фрагментації регуляторного ландшафту ще більше поглиблюються на тлі геополітичних протистоянь у цифровій сфері. В умовах загострення технологічного суперництва між США та Китаєм, наростання «війн даних» та спроб країн убезпечити свій «цифровий суверенітет», простір для багатосторонньої співпраці та узгодження спільних правил гри стрімко звужується. Красномовною ілюстрацією цих процесів є справа компанії Huawei, яка стала заручницею американсько-китайської конфронтації через звинувачення у шпигунстві та загрозах національній безпеці. Схожі претензії з боку влади США висувалися і до інших китайських технологічних гігантів, таких як ByteDance (власник TikTok) та WeChat.

Ці тертя вже призводять до фрагментації інтернет-простору на регіональні зони впливу зі своїми «правилами перепусток» для даних. За даними Information Technology and Innovation Foundation, станом на 2022 рік 62 країни запровадили обмеження на транскордонні потоки даних, зокрема вимоги щодо локалізації інформації. Росія, Індія, В'єтнам, Індонезія, Нігерія – ось лише деякі приклади держав, що вдаються до цифрового протекціонізму під гаслами захисту персональних даних та інформаційного суверенітету. В результаті замість глобального вільного обігу даних світ дедалі більше скочується до моделі «сплінтернету» – фрагментованого цифрового простору, де панує принцип «байдужого інтернету» [8].

Говорячи про широковідомий «Брюссельський ефект» від GDPR, варто критично поглянути на реальні масштаби та природу його впливу на глобальний ландшафт регулювання персональних даних. Безумовно, сам факт ухвалення цього регламенту став потужним каталізатором оновлення національних законодавств у багатьох країнах світу. Втім, більш ґрунтовний погляд дає зрозуміти, що цей вплив є доволі нерівномірним та поверховим. Часто за формальною імплементацією окремих норм GDPR ховається небажання або неспроможність держав забезпечити реальну відповідність європейським стандартам захисту да-

них. Тож радше варто говорити про «Брюссельський ефект» як прагнення урядів створити видимість гармонізації задля спрощення доступу на ринок ЄС, аніж як свідоме переймання цінностей та підходів GDPR. Більш того, навіть у самому ЄС спостерігаються істотні розбіжності у практиці застосування та забезпечення дотримання регламенту на національному рівні. Відтак «Брюссельський ефект» від GDPR швидше нагадує ефект доміно з локальними варіаціями, аніж політично узгоджену і уніфіковану «хвилю» змін глобального регуляторного режиму. І саме ця неоднозначність і ставить під сумнів реальну силу та універсальність впливу GDPR на міжнародні стандарти захисту персональних даних.

Неоднозначність впливу GDPR на глобальний ландшафт захисту персональних даних значною мірою зумовлена тектонічними зрушеннями в самій архітектурі цифрової економіки. Стрімкий розвиток ринків даних та краудсорсингових платформ кидає безпрецедентний виклик традиційним моделям регулювання, в яких держава відігравала роль головного гаранта приватності громадян. Чи здатні публічні інституції ефективно виконувати цю функцію в умовах тотальної «датафікації» та децентралізації процесів генерування й обміну інформацією?

Передусім варто відзначити, що за останнє десятиліття ринок даних перетворився на один з найдинамічніших сегментів глобальної економіки. За оцінками IDC, у 2020 році світовий обсяг даних сягнув 59 зеттабайт, а до 2025 року очікується його зростання до 175-180 зеттабайт. Левова частка цієї інформації генерується не державними органами чи великими корпораціями, а мільярдами підключених до інтернету пристроїв та активністю користувачів онлайн-платформ. Персональні дані стають de facto новим класом економічних активів, навколо якого розбудовуються цілі екосистеми сервісів: від таргетованої реклами до алгоритмічного кредитного скорингу [47]. В цьому контексті регуляторна спроможність держави суттєво обмежується як безпрецедентними масштабами обігу даних, так і їх децентралізованим характером.

Особливо яскраво ця тенденція простежується на прикладі краудсорсингових платформ, таких як Facebook, YouTube чи TikTok. Ці платформи de facto виконують квазі-публічні функції, формуючи інформаційний ландшафт для мільярдів людей та значною мірою впливаючи на процеси творення громадської думки. Втім, їхні політики модерації контенту, збору та обробки персональних даних часто є непрозорими та неузгодженими з публічними інтересами. Красномовною ілюстрацією цього розриву стала справа Cambridge Analytica, коли дані 87 млн користувачів Facebook було незаконно використано для впливу на президентські вибори в США 2016 року. Чи здатна держава ефективно контролювати та регулювати поведінку технологічних гігантів, чиї ресурси та експертиза часто перевищують можливості окремих країн?

Відповідь на це питання є неоднозначною та контекстуально специфічною. В країнах ЄС, які послідовно імплементують GDPR, поступово формується практика притягнення онлайн-платформ до відповідальності за порушення правил обробки персональних даних. Зокрема, у 2021 році Amazon був оштрафований люксембурзьким регулятором на рекордні 746 млн євро за недотримання ви-

мог GDPR щодо отримання згоди користувачів на обробку їхньої інформації в рекламних цілях [50]. Аналогічні санкції застосовувались і до інших технологічних гігантів, таких як Google та Facebook. Ці прецеденти свідчать, що в рамках європейської моделі регулювання держава зберігає вагомі інструменти впливу на політики платформ щодо захисту персональних даних.

Втім, за межами ЄС ситуація виглядає менш оптимістичною. У США, де досі відсутнє федеральне законодавство про захист персональних даних, онлайн-платформи значною мірою покладаються на саморегуляцію та добровільні зобов'язання. Хоча деякі штати, такі як Каліфорнія та Вірджинія, нещодавно ухвалили закони про приватність споживачів в дусі GDPR, їх вплив на практики технологічних гігантів залишається обмеженим. Красномовним прикладом є багаторічна судова тяганина між Федеральною торговою комісією США та Facebook щодо порушень угоди про захист приватності користувачів, яка досі не призвела до відчутних змін політики компанії [24]. На глобальному Півдні ситуація ще більш неоднозначна – брак інституційної спроможності та політичної волі часто унеможливлює ефективний контроль держави за обігом персональних даних на онлайн-платформах.

Окремої уваги заслуговує кейс Китаю, який обрав стратегію жорсткого державного контролю над інтернет-сектором, включно з вимогами щодо локалізації даних та надання спецслужбам доступу до інформації користувачів. З одного боку, це дозволяє владі КНР ефективніше реагувати на випадки порушення приватності громадян з боку онлайн-платформ. У 2021 році Управління кіберпростору Китаю оштрафувало низку компаній, включно з Didi та Alibaba, за недотримання вимог кібербезпеки та незаконний збір персональних даних [61]. З іншого боку, самі громадяни фактично позбавлені інструментів контролю за тим, як держава використовує їхню інформацію, отриману від приватного сектора. Тож модель «державно-платформеного партнерства» у Китаї, попри її регуляторну ефективність, несе ризики безпрецедентного соціального контролю та «приватизації» цифрового суверенітету.

На цьому тлі досвід України видається доволі показовим у контексті країн, що розвиваються. З одного боку, в останні роки вітчизняне законодавство про захист персональних даних зазнало суттєвої модернізації відповідно до європейських стандартів. Зокрема, у 2018 році набув чинності новий Закон «Про захист персональних даних», який імплементував ключові принципи GDPR. Крім того, запроваджено низку галузевих норм щодо регулювання онлайн-платформ, таких як прийнятий у 2021 році Закон «Про електронні комунікації». У 2022 році Уповноважений Верховної Ради з прав людини, який виконує функції наглядового органу у сфері захисту даних, виніс кілька приписів українським онлайн-платформам щодо порушень правил обробки персональної інформації [56].

Водночас, практична імплементація цих норм стикається з низкою викликів. По-перше, це брак політичної волі та інституційної спроможності державних органів ефективно контролювати та притягати до відповідальності онлайн-платформи. Красномовною ілюстрацією є ситуація довкола мобільного застосунку «Дія», де протягом тривалого часу відбувався збір надмірних обсягів персональ-

них даних громадян без належних правових підстав. По-друге, низька обізнаність користувачів зі своїми цифровими правами та механізмами їх захисту обмежує потенціал громадського контролю за політиками платформ. По-третє, в умовах економічної нестабільності та геополітичних викликів економічні інтереси часто превалюють над міркуваннями захисту персональних даних, що проявляється у збереженні регуляторних прогалин та слабкості санкцій за порушення.

Всю публічно-управлінську двоякість, складність та неоднозначність впливу GDPR на глобальний ландшафт регулювання захисту персональних даних можна резюмувати у таблиці 2. Хоча de jure цей регламент став драйвером ухвалення та модернізації національних законодавств у багатьох країнах, de facto його вплив виявився доволі поверховим та фрагментарним.

Попри деякі прояви «Брюссельського ефекту», на практиці зберігаються істотні відмінності у підходах різних юрисдикцій до імплементації принципів GDPR з огляду на локальний інституційний контекст, цифрові бізнес-моделі та геополітичні інтереси. Особливо разючим цей розрив між задекларовани-

Таблиця 2

**Оцінка публічно-управлінського впливу GDPR:
чи є він каталізатором глобального консенсусу, чи драйвером
фрагментації регулювання персональних даних?**

Table 2

**Assessing the public-governance impact of GDPR: is it a catalyst
for global consensus or a driver of fragmentation of personal data regulation?**

Аспект	Аргументи за глобальний консенсус	Аргументи за фрагментацію регулювання	Приклади
Вплив GDPR на національні законодавства	– GDPR став каталізатором оновлення законів про захист даних у багатьох країнах – Близько 80 країн ухвалили або оновили закони, орієнтуючись на принципи GDPR – Прояв «Брюссельського ефекту» – екстра-територіального впливу норм ЄС	– Імплементація принципів GDPR часто має формальний характер – Зберігаються істотні відмінності у підходах та пріоритетах різних юрисдикцій – Навіть у ЄС є розбіжності у практиці застосування GDPR на національному рівні	– Бразилія, Китай, Каліфорнія (США) ухвалили закони з елементами GDPR – Рішення у справі Schrems II засвідчило несумісність американських та європейських правил
Вплив GDPR на країни, що розвиваються	– Є тренд до ухвалення законів про захист даних (44% країн, що розвиваються, мали такі акти станом на 2022 рік)	– Впровадження вимог GDPR є непідйомним регуляторним та фінансовим тягарем – Зміст та практика застосування законів часто не відповідають європейським стандартам – Брак політичної волі та низька обізнаність громадян про цифрові права	– У Кенії ухвалено прогресивний закон, але його імплементація стикається з браком ресурсів та спроможності – Схожі виклики в Нігерії, Гані, Індії, Таїланді

Продовження табл. 2
Table 2 (continued)

Аспект	Аргументи за глобальний консенсус	Аргументи за фрагментацію регулювання	Приклади
Вплив GDPR на Китай	– Китай ухвалив Закон про захист персональних даних (PIPL), інкорпоруавши низку концептів GDPR	– PIPL використовує риторику захисту даних для посилення державного контролю та підтримки національних чемпіонів – Закон надає владі широкий доступ до даних приватного сектора та створює бар'єри для транскордонної передачі – Китай формує власний полюс регулювання, що конкурує з європейською та американською моделями	– Управління кіберпростору Китаю оштрафувало Didi та Alibaba за порушення правил кібербезпеки та збору даних – Громадяни майже позбавлені ефективних інструментів контролю за використанням їхніх даних державою
Геополітичні протистояння у цифровій сфері	Не виявлено	– Загострення технологічного суперництва між США та Китаєм звужує простір для міжнародної співпраці та узгодження правил – Наростання «війн даних» та спроб країн убезпечити «цифровий суверенітет» через локалізацію даних – Справи Huawei, TikTok, WeChat демонструють використання аргументу захисту даних у геополітичній конкуренції	– Станом на 2023 рік 63 країни запровадили обмеження на транскордонні потоки даних – Росія, Індія, В'єтнам, Індонезія, Нігерія вдаються до цифрового протекціонізму під гаслом захисту даних
Реальні масштаби «Брюссельського ефекту»	– Ухвалення GDPR стало потужним каталізатором оновлення національних законодавств у багатьох країнах світу	– Вплив GDPR є нерівномірним та поверховим – Часто за формальною імплементацією норм GDPR ховається брак реальної відповідності європейським стандартам – «Брюссельський ефект» зводиться до видимості гармонізації заради доступу до ринку ЄС – Навіть у ЄС є істотні розбіжності у практиці застосування GDPR	– Попри ухвалення законів за моделлю GDPR, підходи азійських країн відображають прагнення адаптувати європейські норми до власних реалій – Визнані лідери захисту даних, як Японія та Корея, вагаються з повною імплементацією GDPR-сумісних практик

**Джерело:* розробка Дунаєва І.В.

ми нормами та реальною практикою є у випадку країн, що розвиваються, та держав з авторитарними тенденціями. Більш того, використання аргументу захисту персональних даних у технологічних протистояннях між країнами, як от у справах Huawei чи TikTok, лише посилює тенденції до цифрової фрагментації та суверенізації. В цих умовах GDPR справді став важливим еталоном та орієнтиром для наслідування, але навряд чи можна говорити про повноцінне формування глобального консенсусу щодо конкретних стандартів та практик захисту інформації. Скоріше, цей регламент виступає відправною точкою для тривалого процесу гармонізації національних режимів та вироблення спільних «правил гри» на основі балансу різноманітних інтересів та цінностей.

Проведений аналіз засвідчує, що в умовах геополітичної турбулентності та загострення «війн даних» пошук оптимальних моделей регулювання персональної інформації стає першорядним завданням для всіх країн. На тлі обмеженої ефективності традиційних державоцентричних підходів, особливо разючої в країнах, що розвиваються, закономірно постає питання: чи може поширення децентралізованих сервісів та платформ (DeFi, DAOs, ДІП «Система Bitbon» тощо) стати відповіддю на виклик забезпечення балансу між приватністю та інноваційним розвитком в епоху тотальної цифровізації?

Як відомо, в основі концепції децентралізованих сервісів лежить ідея розподілу влади та відповідальності в управлінні даними між широким колом стейкхолдерів – від індивідуальних користувачів до спільнот та організацій, об'єднаних спільними цінностями та інтересами. На відміну від традиційних централізованих систем, де контроль над інформацією концентрується в руках держави чи великих корпорацій, децентралізовані платформи базуються на принципах прозорості, незмінності та консенсусу в прийнятті рішень. Це досягається завдяки використанню технології блокчейн, яка забезпечує захист даних від несанкціонованих змін та дозволяє відстежувати всі транзакції в режимі реального часу (Velasco, 2022).

Одним з найбільш яскравих прикладів децентралізованих екосистем є сфера децентралізованих фінансів (DeFi), яка переживає шалене зростання в останні роки. DeFi-платформи, такі як Uniswap, Aave, Compound, дозволяють користувачам здійснювати різноманітні фінансові операції: від обміну токенів до кредитування та інвестування: без посередництва банків чи інших централізованих інституцій. При цьому всі транзакції здійснюються на основі смарт-контрактів – автоматизованих алгоритмів, які забезпечують виконання угод відповідно до закладених умов. Важливо відзначити, що смарт-контракти не потребують розкриття персональних даних користувачів, а отже мінімізують ризики їх витоку чи зловживання.

Ще одним проявом тренду до децентралізації в управлінні даними є стрімкий розвиток децентралізованих автономних організацій (DAOs). По суті, DAOs – це новий тип організаційної структури, яка дозволяє групі людей координувати свою діяльність та розпоряджатися спільними ресурсами на основі прозорих правил, закодованих у смарт-контрактах. Рішення в DAOs приймаються шляхом голосування всіх учасників, кожен з яких має вагу пропорційно до свого внеску. Така модель забезпечує демократичність управління та стимулює учас-

ників до активного залучення в життя спільноти. Станом на середину 2023 року у світі налічувалося вже понад 4 000 DAOs з сумарною ринковою капіталізацією понад $22 млрд (і це не криптовалюти!). Найвідоміші приклади DAOs, такі як MakerDAO, Uniswap, Compound, демонструють, що ця форма самоврядування є життєздатною альтернативою традиційним ієрархічним структурам, особливо в таких сферах як фінанси, страхування, управління цифровими активами.

Окремо варто відзначити зростаючу роль децентралізованих інформаційних платформ (ДІП) у забезпеченні суверенного контролю користувачів над персональними даними. Яскравим і перспективним прикладом є українська платформа і екосистема цифрових сервісів «Система Bitbon», розроблена харківською компанією ТОВ «Simcord». Побудована на оригінальному протоколі консенсусного управління (PSC), «Система Bitbon» (https://www.bitbon.space/ua) дозволяє створювати персональні «контейнери облікового запису», де кожен користувач має винятковий і ексклюзивний контроль над своїми персональними даними, які зберігаються закодованими на його смартфоні, а не в «хмарі», яка є особливо цікавим об'єктом для державного впливу і втручання. При цьому всі операції з обміну даними фіксуються у незмінному ланцюжку блоків, забезпечуючи їх прозорість та відстежуваність. Такий підхід втілює концепцію «самоврядного ідентифікатора» (SSI), яка дозволяє користувачам керувати різними аспектами своєї цифрової особистості без прив'язки до конкретних провайдерів чи платформ.

Водночас, було б передчасно говорити про те, що поширення децентралізованих сервісів автоматично призводить до послаблення ролі держави в регулюванні персональних даних. Радше, ми спостерігаємо формування нової моделі співвідношення сил, де публічні інституції трансформуються з «наглядачів» на «фасилітаторів» цифрової взаємодії. Зрештою, саме держава має забезпечити сприятливе правове поле та інфраструктурний бекграунд для розвитку інноваційних сервісів на основі технології розподіленого реєстру. Про це свідчить, зокрема, досвід Китаю, який, з одного боку, жорстко обмежує операції з криптовалютами, а з іншого – активно розвиває національну блокчейн-мережу BSN як інструмент цифрової модернізації економіки. Своєю чергою, ЄС у 2022 році ухвалив революційний закон про ринки криптоактивів (MiCA), який встановлює чіткі правила функціонування індустрії на основі принципів прозорості, захисту інвесторів та запобігання ринковим зловживанням. При цьому MiCA прямо заохочує розвиток децентралізованих фінансів та DAO як драйверів інновацій. На відміну від Китаю та ЄС, США досі не сформували цілісної регуляторної рамки для блокчейн-сервісів, що створює правову невизначеність для бізнесу. Утім, на рівні окремих штатів (Вайомінг, Колорадо, Теннессі) ухвалено доволі прогресивні закони, які легітимізують DAO як повноцінну організаційно-правову форму та стимулюють залучення криптобізнесу.

Таким чином, аналізуючи глобальний ландшафт, ми бачимо доволі різновекторні тренди щодо рівня та характеру державного втручання в регулювання децентралізованих сервісів. Але спільним знаменником є усвідомлення того, що розвиток таких екосистем вимагає не протиставлення, а синергії між державою, бізнесом та громадянським суспільством на основі спільних цінностей довіри, прозорості й інноваційності.

Проведений аналіз переконливо доводить, що розвиток децентралізованих сервісів на основі технології розподіленого реєстру формує якісно нові виклики та можливості для регулювання персональних даних в епоху Web 3.0. Відповідно, для України як держави, що прагне забезпечити цифрове лідерство та захистити права своїх громадян в онлайн-середовищі, критично важливо виробити проактивну політику адаптації національного законодавства до нових технологічних та соціокультурних реалій.

Як відомо, Web 3.0 як нова парадигма розвитку інтернету базується на принципах децентралізації, інтероперабельності та суверенного контролю користувачів над своїми даними та цифровими активами. На відміну від Web 2.0, де домінують великі централізовані платформи (Google, Facebook, Amazon), Web 3.0 передбачає формування розподілених екосистем, в яких користувачі взаємодіють безпосередньо один з одним на основі смарт-контрактів та токенізованих активів. Ця архітектура дозволяє уникнути надмірної концентрації даних в руках технологічних гігантів та забезпечує більшу прозорість і підзвітність у питаннях управління персональною інформацією. Разом з тим, перехід до парадигми Web 3.0 несе і нові ризики в сфері захисту даних, пов'язані з особливостями самої технології блокчейн. Зокрема, принцип незмінності розподіленого реєстру означає, що будь-яка інформація, внесена в блокчейн, не може бути видалена чи змінена за бажанням користувача. Потенційно і судячи по публічно поширеним нині практикам застосування, це вступає в протиріччя з базовим правом на забуття, закріпленим у GDPR та інших законах про захист даних. Крім того, прозорість та простежуваність транзакцій у публічних блокчейнах (які застосовані у протоколоах популярних криптоактивів bitcoin, ethereum) ускладнює забезпечення конфіденційності та анонімності користувачів. Для вирішення цих проблем розробляються нові протоколи консенсусу та криптографічні методи, такі як zk-SNARK та MimbleWimble, але їх масштабування все ще залишається викликом.

З цього випливає перший важливий напрям адаптації українського законодавства до реалій Web 3.0 – це забезпечення технологічної нейтральності правового регулювання. Замість того, щоб вписувати специфіку блокчейн-сервісів у застарілі нормативні рамки, орієнтовані на централізовану обробку даних, Україні варто рухатись до моделі «регулювання через принципи». Ця модель передбачає закріплення на рівні закону базових цінностей та вимог щодо безпеки і етики управління даними, але залишає простір для інновацій у методах їх технічної реалізації. Такий підхід відповідає найкращим світовим практикам, зокрема принципам «privacy by design» та «data protection by default», що лежать в основі GDPR.

Наприклад, у 2022 році Європейський Союз анонсував роботу над Регламентом про європейську цифрову ідентифікацію (eID), який має на меті створити єдину систему верифікації громадян для доступу до публічних та приватних онлайн-послуг. При цьому в основу Регламенту буде покладено концепцію «самоврядного цифрового ідентифікатора» (self-sovereign identity, SSI), яка дозволяє користувачам керувати власними ідентифікаційними даними без прив'язки до конкретного провайдера чи технології. Єврокомісія вже запустила пілотний

проект EBSI (European Blockchain Services Infrastructure), який слугуватиме інфраструктурним бекбоном для розгортання SSI-рішень на рівні країн-членів.

У США також спостерігається тенденція до створення сприятливого правового середовища для розвитку саме децентралізованих моделей ідентифікації. Зокрема, у 2021 році в Палаті представників було зареєстровано Закон про модернізацію цифрової ідентифікації (Improving Digital Identity Act), який передбачає федеральну підтримку для впровадження систем SSI та їх інтеграції з існуючими базами даних. А на рівні штатів (Вайомінг, Колорадо, Невада) вже ухвалено закони, що дозволяють резидентам отримувати цифрові посвідчення особи з використанням блокчейн-технологій.

Зважаючи на ці тренди, Україна не може лишатися осторонь глобального руху до децентралізованої ідентифікації. Тож ключовим пріоритетом має стати внесення змін до Закону «Про електронні довірчі послуги», які б легітимізували використання SSI в національних схемах е-ідентифікації (BankID, MobileID тощо). При цьому важливо, щоб держава не намагалася нав'язувати єдиний технологічний стандарт, а радше створювала рівні умови для конкуренції різних SSI-рішень (на блокчейні чи інших сумісних протоколах) від приватних провайдерів. Як приклад такого рішення можна навести «контейнер облікового запису» від компанії Simcord на основі «Системи Bitbon», який вже інтегрований з ключовими реєстрами та e-gov сервісами в Україні [5].

Іншим критично важливим кроком є ухвалення окремого закону про захист персональних даних у сфері штучного інтелекту та автоматизованого прийняття рішень (АДМ). Як показує досвід Китаю з системою «соціального кредиту», впровадження АДМ на основі масивів великих даних несе колосальні ризики для приватності та автономії особистості. Щоб запобігти подібним зловживанням, Україні необхідні чіткі правила щодо прозорості алгоритмів, які використовуються державою та бізнесом для профілювання та скорингу громадян. Людина повинна мати право отримувати пояснення логіки автоматизованих рішень, що суттєво впливають на її права та свободи, а також оскаржувати такі рішення.

У цьому контексті корисним орієнтиром може слугувати Закон про штучний інтелект (Artificial Intelligence Act), ухвалений Європарламентом у 2022 році. Цей акт встановлює диференційований підхід до регулювання систем ШІ залежно від ступеня ризиків, які вони несуть для прав людини та публічних інтересів. Системи ШІ, що використовуються в таких чутливих сферах як правосуддя, правоохоронна діяльність, працевлаштування, кредитування, підлягають підвищеним вимогам щодо безпеки, надійності та підзвітності. При цьому повністю забороняються певні практики ШІ, які вважаються неприпустимими, – скажімо, системи соціального скорингу або використання біометрії для віддаленої ідентифікації у публічних місцях.

Ну і насамкінець варто наголосити на важливості безперервного діалогу та співпраці всіх стейкхолдерів – влади, бізнесу, громадянського суспільства в процесі вироблення політики персональних даних, релевантної до потреб Web 3.0. Адже лише синергія технологічних інновацій, відповідального регулювання та усвідом-

леної цифрової поведінки громадян здатна забезпечити сталий розвиток української data-driven економіки. На державному рівні мають бути створені постійні платформи для такого багатостороннього діалогу – скажімо, при профільному комітеті Верховної Ради, Уповноваженому з прав людини, Мінцифри. Окрім того, дуже важливими є інвестиції в цифрову просвіту та медіаграмотність населення, щоб підвищити обізнаність людей про ризики та можливості управління персональними даними в децентралізованому середовищі. З огляду на це, доцільно закріпити в законодавстві вимоги до провайдерів онлайн-послуг щодо навчання користувачів цифровій гігієні та практикам відповідальної обробки даних.

Відтак, резюмуючи, можна виокремити п'ять ключових кроків, які мусить здійснити Україна на шляху адаптації законодавства про захист персональних даних до реалій Web 3.0:

1) закріпити принципи технологічної нейтральності та «регулювання через цілі», щоб створити гнучкі рамки для розвитку блокчейн-сервісів та децентралізованих моделей обміну даними;

2) внести зміни до Закону «Про електронні довірчі послуги», які легітимізують використання рішень на основі «самоврядної цифрової ідентифікації» (SSI) у національних схемах е-ідентифікації;

3) ухвалити окремий закон про захист персональних даних у сфері ШІ, який встановить диференційовані вимоги до прозорості, підзвітності та надійності систем автоматизованого прийняття рішень залежно від ступеня їх ризиковості для прав людини;

4) створити державні платформи для постійного багатостороннього діалогу щодо регулювання захисту даних за участю представників влади, бізнесу, експертної спільноти та громадянського суспільства;

5) закріпити в законодавстві вимоги до провайдерів онлайн-послуг щодо навчання користувачів цифровій гігієні та практикам відповідальної обробки даних, а також системно інвестувати в цифрову просвіту усіх верств населення.

Саме послідовна реалізація цих кроків дозволить Україні збалансувати ключові публічні цінності – інноваційний розвиток, цифрові права людини та національну безпеку в епоху тотальної «датафікації». Але не менш важливою є ментальна готовність держави, бізнесу та суспільства до відповідальності, партнерства та експериментування в освоєнні нових моделей поведінки з персональними даними. Тільки за такої синергії зусиль та довіри всіх стейкхолдерів Україна зможе стати лідером у розвитку людино-центричної архітектури Web 3.0 та прикладом для наслідування в глобальному масштабі.

Висновки. На основі проведених вище досліджень можна зробити такі узагальнені висновки, які чітко характеризують сучасність і спрямовані у майбутнє.

1) Сучасний пост-GDPR світ стоїть на роздоріжжі. Вибір між подальшою фрагментацією регуляторного ландшафту та довгим шляхом до гармонізації стандартів приватності багато в чому визначить, в якому інформаційному середовищі ми житимемо: відкритому та глобально сполученому чи закритому та розчленованому непроникними цифровими кордонами. Саме від узгодженої політичної волі держав, корпорацій та глобального громадянського суспільства

залежить, чи зможемо ми реалізувати проект захисту персональних даних як спільної цінності, що не роз'єднує, а навпаки – об'єднує людство в цифрову епоху, а GDPR – це лише перший, хоч і надзвичайно важливий крок на цьому шляху.

2) Роль держави в регулюванні персональних даних в умовах цифрової трансформації є вкрай неоднозначною та суперечливою. Будучи одночасно гарантом приватності та потужним користувачем персональної інформації, держава має віднайти тонкий баланс між різними публічними цінностями та інтересами. Моделі цього балансу суттєво різняться між країнами – від жорсткого контролю в дусі GDPR до гнучких форматів саморегуляції та акценту на використанні даних для забезпечення суспільних благ. Але попри всю різноманітність підходів, спільним знаменником лишається потреба у відповідальному та людиноцентричному управлінні даними на основі принципів прозорості, підзвітності та поваги до прав людини. Так само, які і попри все розмаїття національних моделей та підходів, спільним викликом лишається необхідність вибудовування нового суспільного договору між державою, бізнесом та громадянами щодо правил обігу персональних даних в цифрову епоху. Лише держава, яка служить інтересам своїх громадян, а не маніпулює ними, може претендувати на довіру в епоху тотальної цифровізації.

3) Проведений аналіз впливу GDPR на глобальний ландшафт регулювання персональних даних дає підстави стверджувати, що цей регламент, попри його безумовно проривний характер, не призвів до формування повноцінного міжнародного консенсусу щодо стандартів захисту інформації. Попри певну гармонізацію національних законодавств за європейським зразком, на практиці зберігаються істотні відмінності у підходах різних юрисдикцій до балансування цінностей приватності, цифрової економіки та національної безпеки. Більш того, геополітичні протистояння в технологічній сфері, пов'язані насамперед з американсько-китайською конкуренцією, дедалі більше підривають саму ідею універсальних правил гри та вільного транскордонного обігу даних. В результаті світ стрімко рухається до моделі фрагментованого регулювання, де держави використовують захист персональних даних радше як інструмент торговельної політики та цифрового суверенітету. Разом з тим, саме усвідомлення цих обмежень та викликів і вказує шлях до їх подолання.

4) Розвиток ринків даних та онлайн-платформ формує якісно нові виклики для моделі державного регулювання персональних даних. В умовах безпрецедентної «датафікації» та децентралізації інформаційних потоків традиційні інструменти нормативного та інституційного контролю виявляються недостатніми. Натомість актуалізується потреба в новій екосистемній парадигмі регулювання, яка б забезпечувала гнучке балансування публічних та приватних інтересів у цифровому середовищі на основі багатосторонньої співпраці між державою, бізнесом та громадянським суспільством. Ключовими компонентами цієї парадигми мають стати: (1) розвиток моделей ко-регуляції, які поєднують нормативні вимоги з елементами саморегуляції та підзвітності платформ; (2) інвестиції у зміцнення інституційної спроможності державних регуляторів та впровадження ризик-орієнтованих підходів до контролю й санкцій; (3) сприян-

ня розвитку моделей суверенного управління даними користувачів (data trusts, data cooperatives) та поширенню практик «приватності за дизайном»; (4) підвищення цифрової грамотності громадян та стимулювання активної участі громадянського суспільства у формуванні політик захисту даних. Реалізація цих підходів, безумовно, наштовхуватиметься на численні політичні, інституційні та соціокультурні бар'єри. Втім, як показує аналіз, саме рух до більш інклюзивної, адаптивної та підзвітної моделі регулювання здатен забезпечити ефективний баланс між інноваційним розвитком data-driven економіки та надійним захистом права на приватність в епоху тотальної цифровізації.

5) В умовах геополітичної турбулентності та загострення «війн даних» Україні критично важливо віднайти збалансований підхід до імплементації кращих практик GDPR, який би поєднував високі стандарти захисту персональних даних із міркуваннями національної безпеки та цифрового суверенітету. Це вимагатиме як political skills у виробленні проєвропейської регуляторної політики, так і технічних інновацій у сфері надійного збереження та обігу даних. У цьому контексті варто звернути увагу на перспективні вітчизняні розробки, такі як «контейнер облікового запису» від ТОВ «Сімкорд» на основі блокчейн-платформи Система Bitbon українського походження. Ця технологія дозволяє створювати надзвичайно захищені персональні «сховища» даних, де користувач має повний контроль над своєю інформацією зі свого смартфону та може вибірково надавати доступ третім сторонам для чітко визначених цілей. Важливо, щоб держава стимулювала впровадження подібних інноваційних рішень на рівні публічних реєстрів та е-послуг, а також заохочувала приватний сектор до їх масштабування через держзамовлення, податкові преференції тощо.

6) Нинішнє стрімке становлення децентралізованих екосистем управління даними в Україні та світі відкриває унікальне «вікно можливостей» для перезавантаження відносин між державою та суспільством на принципово нових засадах. Розподілені технології здатні не лише дуже суттєво розширити простір індивідуальної свободи та контролю над персональною інформацією, але й сформувати більш інклюзивну та колаборативну модель ухвалення суспільно важливих рішень. Утім, для реалізації цього потенціалу критично важливо вибудувати нову культуру публічно-приватного партнерства, де держава, бізнес та громадянське суспільство виступатимуть співтворцями правил «гри», а не антагоністами. І саме блокчейн-спільнота може стати тим простором експериментування з інноваційними формами цифрової співпраці, який покаже приклад всім іншим сферам.

7) Трансформація ролі держави в регулюванні персональних даних під впливом GDPR має глибокий і неоднозначний характер. З одного боку, цей регламент став потужним каталізатором гармонізації національних законодавств та підвищення стандартів захисту інформації в глобальному масштабі. Але з іншого боку, реальна імплементація принципів GDPR стикається з низкою викликів: від інституційних обмежень та геополітичних протиріч до культурних відмінностей у ставленні до приватності. В результаті формується строката мозаїка регуляторних моделей, що балансують цінності захисту даних, цифрового

суверенітету та технологічного розвитку. Тож на горизонті 3-8 років навряд чи можна очікувати повної глобальної конвергенції у цій сфері. Скоріше, триватиме тренд до регіоналізації режимів захисту даних навколо великих держав-акторів з періодичними спробами віднайти спільний знаменник на рівні міжнародних організацій та багатосторонніх ініціатив. Ключовим фактором успіху на цьому шляху буде здатність різних юрисдикцій знаходити інноваційні регуляторні рішення, адаптовані до локального контексту, але сумісні з універсальними принципами захисту прав людини в цифрову епоху.

8) Поширення децентралізованих сервісів на основі технології розподіленого реєстру формує простір нових можливостей для реалізації концепції «цифрового суверенітету особистості» в епоху тотальної датафікації. Такі рішення як суверенна цифрова ідентифікація (SSI), локалізовані сховища даних (SDS) та криптографічні протоколи конфіденційності дозволяють людині здійснювати свідомий контроль над тим, як її персональна інформація генерується, зберігається та циркулює в онлайн-середовищі. При цьому децентралізована архітектура забезпечує суттєво вищий рівень безпеки та стійкості в порівнянні з традиційними централізованими системами, вразливими до цензури, маніпуляцій та витоків даних. Втім, масштабування цих інновацій вимагатиме не лише технологічної зрілості, але й адекватної інституалізації в правовому полі. Держава має відігравати роль фасилітатора, а не контролера цифрової взаємодії, створюючи стимули для відповідальної поведінки всіх стейкхолдерів. Зокрема, на найближчі 3-8 років пріоритетом має стати розробка законодавства, яке легітимізує використання SSI в публічному та приватному секторі, встановлює чіткі правила розкриття інформації про алгоритми автоматизованого прийняття рішень, а також культивує цифрові компетенції громадян через формальну та неформальну освіту. Лише за такого збалансованого підходу інструменти децентралізації стануть надійним фундаментом для реалізації людино-центричного бачення Web 3.0.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Дунаєв І., Коваленко М. Нові траєкторії регулювання інформаційних платформ і платформної економіки заради суспільного блага. *Актуальні проблеми державного управління*. 2022. №2(61). С. 6–24. URL: https://periodicals.karazin.ua/apdu/article/view/21840/20243. DOI: https://doi.org/10.26565/1684-8489-2022-2-01

2. Дунаєв І.В., Кудь А.А. Умови запровадження децентралізованої інформаційної платформи до потреб оперативної підтримки відбудови постраждалої від війни інфраструктури. *Публічне управління XXI століття: нові виклики і трансформації в умовах війни* : матеріали 24-ого міжнар. наук. конгресу, м. Харків, 24 травня 2024 р. Харків : ХНУ імені В.Н. Каразіна, 2024. С. 297–301.

3. Жора В. Україна з 14 січня 2022 року залишається на першому місці у світі за кількістю кібератак проти неї – заступник голови Держспецзв'язку. URL: https://interfax.com.ua/news/interview/911979.html

4. Кудь А.А. Трансформація економічних відносин та способів їх реалізації в умовах розвитку цифрових технологій. *Вісник Львівського університету. Серія економічна*. 2022. №62. С. 42–59. URL: http://publications.lnu.edu.ua/bulletins/index.php/economics/issue/view/522. DOI: 10.30970/ves.2022.62.0.6204

5. Кудь А.А. Осмислення майбутнього розвитку ринкової інфраструктури на основі використання токенізованих активів. *Економічний аналіз*. 2023. Т. 33, №3. С. 9–32. URL: https://www.econa.org.ua/index.php/econa/article/view/5832/6565657261. DOI: https://doi.org/10.35774/econa2023.03.009

6. Кудь А.А. Правові та технологічні умови для законного обігу токенізованих активів у сучасних приватних і державних публічних інформаційних платформах. *Інвестиції: практика та досвід.* 2023. №18. С. 130–121. URL: https://nayka.com.ua/index.php/investplan/article/view/2089/2114. DOI: https://doi.org/10.32702/2306-6814.2023.18.12

7. Aaronson S.A. Data is dangerous: comparing the risks that the United States, Canada and Germany See in Data Troves. *Centre for International Governance Innovation*. 2021. 36 p. URL: https://www.cigionline.org/static/documents/documents/no.241%202_0.pdf.

8. Aaronson S.A., Leblond P. Another digital divide: The rise of data realms and its implications for the WTO. *Journal of International Economic Law.* 2018. Vol. 21(2). P. 245–272. DOI: https://doi.org/10.1093/jiel/jgy019. URL: https://academic.oup.com/jiel/article-abstract/21/2/245/4996295?redirectedFrom=fulltext

9. Adlam R., Haskins B. Applying blockchain technology to security-related aspects of electronic healthcare record infrastructure. *The African Journal of Information and Communication (AJIC)*. 2021. (28). DOI: 10.23962/10539/32211

10. Bradford A. The Brussels Effect: How the European Union rules the world. New York: Oxford Academic, 2020. Online edn, 19 Dec. 2019. DOI: https://doi.org/10.1093/oso/9780190088583.001.0001

11. Brain rot named Oxford Word of the Year 2024 / Oxford University Press. Oxford, 2024. URL: https://corp.oup.com/news/brain-rot-named-oxford-word-of-the-year-2024/

12. Burman A. Understanding India's New Data Protection Law / Carnegie India. 2023. URL: http://surl.li/itwzva

13. Bygrave L.A. The 'Strasbourg Effect' on data protection in light of the 'Brussels Effect': Logic, mechanics and prospects. *Computer Law & Security Review.* 2021. Vol. 40. Article 105460. DOI: https://doi.org/10.1016/j.clsr.2020.105460. URL: https://www.sciencedirect.com/science/article/pii/S0267364920300650?via%3Dihub

14. Cannataci J. Visit to the United States of America : report of the Special Rapporteur on the Right to Privacy. 2021. URL: https://policycommons.net/artifacts/8937236/visit-to-the-united-states-of-america/9753201/.

15. Chander A. Is Data Localization a Solution for Schrems II? *Journal of International Economic Law*. 2020. Vol. 23(3). P. 771–784. DOI: https://doi.org/10.1093/jiel/jgaa024

16. Chander A., Kaminski M., McGeveran W. Catalyzing privacy law. *Minn. L. Rev.* 2021. Vol. 105. P. 1733. URL: http://surl.li/obgtyb

17. Chauhan P., Kshetri N. 2021 State of the Practice in Data Privacy and Security, in Computer. 2021. Vol. 54, no. 8, pp. 125-132, Aug. 2021. DOI: 10.1109/MC.2021.3083916. URL: https://libres.uncg.edu/ir/uncg/f/N_Kshetri_State_2021.pdf

18. CNIL. Cookies: la CNIL sanctionne les sociétés GOOGLE à hauteur de 150 millions d'euros et Facebook à hauteur de 60 millions d'euros pour non-respect de la législation française. 2021. URL: http://surl.li/fiqwdu

19. Corbishley N. Western media finally begin warning about the dark side of digital identity…in China. 2024. URL: http://surl.li/kclpzd

20. Cory N., Dascoli L. How barriers to cross-border data flows are spreading globally, what they cost, and how to address them. *ITIF*. 2021. URL: http://surl.li/isuhir

21. Court of Justice of the European Union. Judgment in Case C-311/18: Data Protection Commissioner v Facebook Ireland and Maximillian Schrems. 2020. URL: https://curia.europa.eu/juris/documents.jsf?num=C-311/18

22. Dunayev I.V., Gavkalova N.L., Kud A.A. Designing a platform-based model of civic participation within the smart-city concept for post-war Ukrainian cities. *Eastern-European Journal of Enterprise Technologies*. 2023. №3(14(123)). P. 46–56. DOI: https://doi.org/10.15587/1729-4061.2023.285448

23. European Commission. Adequacy decisions: How the EU determines if a non-EU country has an adequate level of data protection. 2022. URL: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

24. Feiner L. State AGs plan to fight court dismissal of their antitrust claims against Facebook. *CNBC*. 2021. URL: https://www.cnbc.com/2021/07/28/state-ags-to-fight-dismissal-of-facebook-antitrust-claims.html

25. Fielding J. Wreaking Extraordinary Destruction: Defendant's Irreplaceability as Presumptively Reasonable Grounds for Downward Departure in Sentencing Note. *Minnesota Law Review*. 2020. Vol. 104. P. 2565. URL: https://scholarship.law.umn.edu/cgi/viewcontent.cgi?article=4315&context=mlr

26. Freedom House. Freedom on the Net 2023: Digital Election Interference. 2023. URL: https://freedomhouse.org/report/freedom-net/2023/digital-election-interference

27. Greenleaf G. Global data privacy laws 2021: Despite COVID delays, 145 laws show GDPR dominance. *Privacy Laws & Business International Report*. 2021. №169(1). P. 3–5. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3836348

28. Greenleaf G., Cottier B. 2020 ends a decade of 62 new data privacy laws. *Privacy Laws & Business International Report*. 2020. №163. P. 24–26.

29. Greenleaf G. Global Data Privacy Laws 2019: 132 National Laws & Many Bills. *Privacy Laws & Business International Report*. 2019. №157. P. 14–18. URL: https://ssrn.com/abstract=3381593

30. Hu W.Z. Understanding the Power of China's National Social Credit System: A Structural/Mechanism Explanation. *Philosophy of the Social Sciences*. 2024. Vol. 54(3). P. 203–225. DOI: https://doi.org/10.1177/00483931241229445

31. ID2020. Manifesto. 2023. URL: https://id2020.org/manifesto

32. International Data Privacy Law. 2022. Vol. 12, Issue 2. P. 113–131. DOI: 10.1093/idpl/ipac001. URL: http://surl.li/dipinn

33. Kleinwächter W. Digital Governance Discussion Group (DGDG): One World, One Internet, Many Voices. 2024. URL: https://circleid.com/posts/20240214-digital-governance-discussion-group-dgdg-one-world-one-internet-many-voices

34. Kuner Ch. The Internet and the Global Reach of EU Law. In: Marise Cremona, Joanne Scott (eds). EU Law Beyond EU Borders: The Extraterritorial Reach of EU Law. Oxford: Oxford Academic, 2019. Online edn, 20 June 2019. DOI: https://doi.org/10.1093/oso/9780198842170.003.0004

35. Marcén A.G. The new personal data protection in Japan: Is it enough? In: Micky Lee, Peichi Chung (eds). Media Technologies for Work and Play in East Asia: Critical Perspectives on Japan and the Two Koreas. Bristol: Policy Press Scholarship Online, 2021. Online edn, 20 Jan. 2022. DOI: https://doi.org/10.1332/policypress/9781529213362.003.0006

36. Masse E., Sueyro E. All hands on deck: What the European Parliament should do about the DSA. 2022. URL: https://edri.org/our-work/all-hands-on-deck-what-the-european-parliament-should-do-about-the-dsa

37. Mattoo A., Meltzer J. International data flows and privacy: the conflict and its resolution. *Journal of International Economic Law.* 2018. Vol. 21(4). P. 769–789. DOI: https://doi.org/10.1093/jiel/jgy044

38. Meads N. The perils and promise of self-sovereign identity. Ada Lovelace Institute. 2022. URL: https://www.adalovelaceinstitute.org/blog/the-perils-and-promise-of-self-sovereign-identity

39. Meng Z., Wang L. Personal data trusts in China: a balance between data sharing and privacy protection. *Trusts & Trustees.* 2024. DOI: https://doi.org/10.1093/tandt/ttae089

40. Morgan S. Cybercrime to cost the world $10.5 Trillion Annually By 2025. Cybersecurity Ventures. 2022. URL: https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025

41. OECD. A roadmap toward a common framework for measuring the digital economy: Report for the G20 Digital Economy Task Force. 2020. 8 pages. URL: https://www.yunbaogao.cn/index/partFile/5/itu/2022-04/5_22772.pdf

42. Otta S., Panda S. Decentralized Identity and Access Management of Cloud for Security as a Service. IEEE COMSNETS. 2022. P. 299–303. DOI: 10.1109/comsnets53615.2022.9668529. URL: http://surl.li/prsfon

43. Piasecki S., Jiahong Chen J. Complying with the GDPR when vulnerable people use smart devices. *International Data Privacy Law.* 2022. Vol. 12, Issue 2. DOI: 10.1093/idpl/ipac001

44. Raghavan B., Schneier B. A bold new plan for preserving online privacy and security. 2023. URL: http://surl.li/rfcyoy

45. Rothstein M.A., Tovino S. California takes the lead on data privacy law. Hastings Center Report. 2019. DOI: 10.1002/hast.1042. URL: https://pubmed.ncbi.nlm.nih.gov/31581323

46. Sacks S. China's emerging data privacy system and GDPR. Centre for Strategic and International Studies. 2021. URL: https://www.csis.org/analysis/chinas-emerging-data-privacy-system-and-gdpr

47. Sadowski J. When data is capital: Datafication, accumulation, and extraction. *Big Data & Society.* 2019. Vol. 6(1). P. 1–12. DOI: https://doi.org/10.1177/2053951718820549 URL: https://journals.sagepub.com/doi/full/10.1177/2053951718820549

48. Schwartz P.M., Peifer K.-N. Transatlantic data privacy law. *Georgetown Law Journal.* 2017. Vol. 106(1). P. 115–179. URL: https://www.law.georgetown.edu/georgetown-law-journal/in-print/volume-106/volume-106-issue-1-november-2017/transatlantic-data-privacy-law

49. Sestino A., Kahlawi A., De Mauro A. Decoding the data economy: a literature review of its impact on business, society and digital transformation. *European Journal of Innovation Management.* 2023. DOI: 10.1108/EJIM-01-2023-0078. URL: http://surl.li/nhxmst

50. Shead S. Amazon hit with $887 million fine by European privacy watchdog. *CNBC.* 2021. URL: https://www.cnbc.com/2021/07/30/amazon-hit-with-fine-by-eu-privacy-watchdog-

51. Simons A. Decentralized digital identities and blockchain: The future as we see it. 2017. URL: https://techcommunity.microsoft.com/users/alex%20simons%20(azure)/53477

52. Sovrin Foundation. Sovrin: A protocol and token for self-sovereign identity and decentralized trust. 2023. URL: http://surl.li/lmwbzr

53. Summerfield C. et al. How will advanced AI systems impact democracy? 2024. URL: https://www.schneier.com/wp-content/uploads/2024/09/How-Will-Advanced-AI-Systems-Impact-Democracy.pdf

54. UNCTAD. Data protection and privacy legislation worldwide. United Nations Conference on Trade and Development. 2021. URL: https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

55. UNCTAD. Data protection and privacy legislation worldwide. United Nations Conference on Trade and Development. 2023. URL: https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

56. UODO. Припис від 15.02.2022 №3-п. Уповноважений Верховної Ради України з прав людини. 2022. URL: http://www.ombudsman.gov.ua/ua/page/zpd/

57. Wetzling T., Sarkesian L., Dietrich C. Solving the Transatlantic Data Dilemma: Surveillance Reforms to Break the International Gridlock. 2021. 82 p. URL: https://www.stiftung-nv.de/publications/downloadPdf/solving-transatlantic-data-dilemma

58. White House. Biden-Harris administration announces key actions to advance tech accountability and protect the rights of the American Public. 2022. URL: http://surl.li/sddjac

59. World Economic Forum. Reimagining data privacy for the 21st century. 2021. URL: https://www.weforum.org/agenda/2021/07/reimagining-data-privacy-for-the-21st-century

60. WorldBank. Europe and Central Asia economic update, Spring 2022: War in the Region. Europe and Central Asia Economic Update;13. Washington, DC: World Bank. 2022. 118 p. URL: http://hdl.handle.net/10986/37268

61. Xiong Y. China fines Didi $1.2 billion for violating cybersecurity and data laws. CNN. 2022. URL: https://edition.cnn.com/2022/07/21/economy/china-fines-didi-data-law-violation-intl-hnk/index.html

62. Zuboff S. The age of surveillance capitalism: The fight for a human future at the new frontier of power. PublicAffairs. 2019.

Стаття надійшла до редакції 21.11.2024
Стаття рекомендована до друку 20.12.2024

Igor Dunayev, Dr.Sc. of public administration, professor, professor of the department of economic policy and management, Educational and Scientific Institute «Institute of Public Administration», V. N. Karazin Kharkiv National University, 4 Svobody Sq., Kharkiv, 61022, Ukraine
ORCID ID: http://orcid.org/0000-0002-0790-0496 e-mail: i.dunaev@karazin.ua

Nataliya Lugovenko, PhD in Public Administration, associate professor, associate professor of the Department of Economic Policy and Management, Educational and Scientific Institute «Institute of Public Administration», V. N. Karazin Kharkiv National University, 4 Svobody Sq., Kharkiv, 61022, Ukraine
ORCID ID: http://orcid.org/0000-0003-0386-7630 e-mail: nata_vict@ukr.net

THE STATE AND PERSONAL DATA IN THE POST-GDPR WORLD: TOWARDS A GLOBAL CONSENSUS OR REGULATORY FRAGMENTATION?

Abstract. This article explores the transformation of the state's role in regulating personal data in the post-GDPR world. The author analyzes the impact of the EU's General Data Protection Regulation (GDPR) on the evolution of the global privacy protection landscape, identifying trends towards harmonization and fragmentation of national legislations. The changing functions of the state as a regulator and guarantor of personal data protection in the context of digitalization are unveiled. The potential of blockchain technologies and distributed ledgers in ensuring user control over data is investigated. The influence of the development of the

data market and new business models on the regulatory approaches of states and corporations is analyzed. The consequences of the spread of decentralized services for the relationships between the state, business, and civil society are considered. Priority directions for improving Ukrainian legislation in the field of personal data protection are substantiated, taking into account the realities of Web 3.0 and the need to balance innovation and security. The key idea is that the post-GDPR world stands at a crossroads between further fragmentation of the regulatory landscape and a long path towards harmonizing privacy standards. The choice of development trajectory depends on the coordinated political will of states, corporations, and global civil society to protect personal data as a shared value that unites humanity in the digital age. The article delves into the complex interplay of technological, legal, and societal factors shaping the future of data governance, offering insights into the challenges and opportunities ahead. It highlights the need for adaptive and inclusive regulatory frameworks that balance individual rights, economic interests, and public goods in an increasingly data-driven world.

Keywords*: personal data, GDPR, public administration, platforms, blockchain, decentralized services, privacy protection, regulatory fragmentation, harmonization of standards, Web 3.0.*

In cites: Dunayev, I. V., & Lugovenko, N. V. (2024). The State and Personal Data in the Post-GDPR World: Towards a Global Consensus or Regulatory Fragmentation? *Theory and Practice of Public Administration*, 2 (79), 28–63. http://doi.org/10.26565/1727-6667-2024-2-02 [in Ukrainian].

REFERENCES

1. Dunayev, I., & Kovalenko, M. (2022). New traces for regulating information platforms and the platform economy for the public good. *Pressing Problems of Public Administration,* 2(61), 6-24. https://doi.org/10.26565/1684-8489-2022-2-01 [in Ukrainian].
2. Dunayev, I. V., & Kud, A. A. (2024, May 24). Conditions for introducing a decentralized information platform for the needs of operational support for the reconstruction of war-damaged infrastructure [Paper presentation]. *Public Administration of the 21st Century: New Challenges and Transformations in Wartime:* 24th International Scientific Congress, Kharkiv, Ukraine [in Ukrainian].
3. Zhora, V. (2023). Since January 14, 2022, Ukraine remains in first place in the world in terms of the number of cyberattacks against it – Deputy Head of the State Service for Special Communications. Interfax. https://interfax.com.ua/news/interview/911979.html [in Ukrainian].
4. Kud, A. A. (2022). Transformation of economic relations and methods of their implementation in the conditions of digital technology development. *Bulletin of Lviv University. Economic Series,* (62), 42-59. https://doi.org/10.30970/ves.2022.62.0.6204 [in Ukrainian].
5. Kud, A. A. (2023). Comprehending the future development of market infrastructure based on the use of tokenized assets. *Economic Analysis,* 33(3), 9-32. https://doi.org/10.35774/econa2023.03.009 [in Ukrainian].
6. Kud, A. A. (2023). Legal and technological conditions for the legal circulation of tokenized assets in modern private and public information platforms. *Investments: Practice and Experience,* (18), 12-21. https://doi.org/10.32702/2306-6814.2023.18.12 [in Ukrainian].
7. Aaronson, S. A. (2021). Data is dangerous: Comparing the risks that the United States, Canada and Germany see in data troves. Centre for International Governance Innovation. https://www.cigionline.org/static/documents/documents/no.241%202_0.pdf.

8. Aaronson, S. A., & Leblond, P. (2018). Another digital divide: The rise of data realms and its implications for the WTO. *Journal of International Economic Law,* 21(2), 245-272. https://doi.org/10.1093/jiel/jgy019

9. Adlam, R., & Haskins, B. (2021). Applying blockchain technology to security-related aspects of electronic healthcare record infrastructure. *The African Journal of Information and Communication (AJIC),* (28). https://doi.org/10.23962/10539/32211

10. Bradford, A. (2020). The Brussels effect: How the European Union rules the world. *Oxford University Press.* https://doi.org/10.1093/oso/9780190088583.001.0001

11. Oxford University Press. (2024). Brain rot named Oxford Word of the Year 2024. https://corp.oup.com/news/brain-rot-named-oxford-word-of-the-year-2024/

12. Burman, A. (2023). Understanding India's new data protection law. Carnegie India. http://surl.li/itwzva

13. Bygrave, L. A. (2021). The 'Strasbourg Effect' on data protection in light of the 'Brussels Effect': Logic, mechanics and prospects. *Computer Law & Security Review,* 40, Article 105460. https://doi.org/10.1016/j.clsr.2020.105460

14. Cannataci, J. (2021). Visit to the United States of America: Report of the Special Rapporteur on the Right to Privacy. https://policycommons.net/artifacts/8937236/visit-to-the-united-states-of-america/9753201/

15. Chander, A. (2020). Is data localization a solution for Schrems II? *Journal of International Economic Law,* 23(3), 771-784. https://doi.org/10.1093/jiel/jgaa024

16. Chander, A., Kaminski, M., & McGeveran, W. (2021). Catalyzing privacy law. *Minnesota Law Review*, 105, 1733-1802. http://surl.li/obgtyb

17. Chauhan, P., & Kshetri, N. (2021). State of the practice in data privacy and security. *Computer*, 54(8), 125-132. https://doi.org/10.1109/MC.2021.3083916

18. CNIL. (2021). Cookies: la CNIL sanctionne les sociétés GOOGLE à hauteur de 150 millions d'euros et Facebook à hauteur de 60 millions d'euros pour non-respect de la législation française [Cookies: CNIL fines GOOGLE €150 million and Facebook €60 million for non-compliance with French legislation]. http://surl.li/fiqwdu

19. Corbishley, N. (2024). Western media finally begin warning about the dark side of digital identity…in China. http://surl.li/kclpzd

20. Cory, N., & Dascoli, L. (2021). How barriers to cross-border data flows are spreading globally, what they cost, and how to address them. *ITIF*. http://surl.li/isuhir

21. Court of Justice of the European Union. (2020). Judgment in Case C-311/18: Data Protection Commissioner v Facebook Ireland and Maximillian Schrems. https://curia.europa.eu/juris/documents.jsf?num=C-311/18

22. Dunayev, I. V., Gavkalova, N. L., & Kud, A. A. (2023). Designing a platform-based model of civic participation within the smart-city concept for post-war Ukrainian cities. *Eastern-European Journal of Enterprise Technologies,* 3(14(123)), 46-56. https://doi.org/10.15587/1729-4061.2023.285448

23. European Commission. (2022). Adequacy decisions: How the EU determines if a non-EU country has an adequate level of data protection. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

24. Feiner, L. (2021). State AGs plan to fight court dismissal of their antitrust claims against Facebook. *CNBC*. https://www.cnbc.com/2021/07/28/state-ags-to-fight-dismissal-of-facebook-antitrust-claims.html

25. Fielding, J. (2020). Wreaking extraordinary destruction: Defendant's irreplaceability as presumptively reasonable grounds for downward departure in sentencing. *Minnesota Law Review*, 104, 2565-2597. https://scholarship.law.umn.edu/cgi/viewcontent.cgi?article=4315&context=mlr

26. Freedom House. (2023). Freedom on the Net 2023: Digital election interference. https://freedomhouse.org/report/freedom-net/2023/digital-election-interference

27. Greenleaf, G. (2021). Global data privacy laws 2021: Despite COVID delays, 145 laws show GDPR dominance. *Privacy Laws & Business International Report,* 169(1), 3-5. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3836348

28. Greenleaf, G., & Cottier, B. (2020). 2020 ends a decade of 62 new data privacy laws. *Privacy Laws & Business International Report*, 163, 24-26. https://ssrn.com/abstract=3572611

29. Greenleaf, G. (2019). Global data privacy laws 2019: 132 national laws & many bills. *Privacy Laws & Business International Report*, 157, 14-18. https://ssrn.com/abstract=3381593

30. Hu, W. Z. (2024). Understanding the power of China's national social credit system: A structural/mechanism explanation. *Philosophy of the Social Sciences*, 54(3), 203-225. https://doi.org/10.1177/00483931241229445

31. ID2020. (2023). Manifesto. https://id2020.org/manifesto

32. Piasecki, S., & Jiahong Chen, J. (2022). Complying with the GDPR when vulnerable people use smart devices. *International Data Privacy Law*, 12(2), 113-131. https://doi.org/10.1093/idpl/ipac001

33. Kleinwächter, W. (2024). Digital Governance Discussion Group (DGDG): One world, one internet, many voices. CircleID. https://circleid.com/posts/20240214-digital-governance-discussion-group-dgdg-one-world-one-internet-many-voices (accessed on December 01, 2024)

34. Kuner, C. (2019). The internet and the global reach of EU law. In M. Cremona & J. Scott (Eds.), EU law beyond EU borders: The extraterritorial reach of EU law. Oxford University Press. https://doi.org/10.1093/oso/9780198842170.003.0004

35. Marcén, A. G. (2021). The new personal data protection in Japan: Is it enough? In M. Lee & P. Chung (Eds.), Personal data protection and privacy (pp. 23-40). Springer. https://doi.org/10.1007/978-981-16-2293-6_3

36. Mehta, N. (2024). China proposes comprehensive digital identity system for citizens. The Financial Times. https://www.ft.com/content/821fc08a-f4d3-40a8-9d5c-e8b16f428e02

37. Mattoo, A., & Meltzer, J. P. (2018). International data flows and privacy: The conflict and its resolution. *Journal of International Economic Law*, 21(4), 769-789. https://doi.org/10.1093/jiel/jgy044

38. Meads, N. (2022). The perils and promise of self-sovereign identity. Ada Lovelace Institute. https://www.adalovelaceinstitute.org/blog/the-perils-and-promise-of-self-sovereign-identity

39. Meng, Z., & Wang, L. (2024). Personal data trusts in China: A balance between data sharing and privacy protection. Trusts & Trustees. Advance online publication. https://doi.org/10.1093/tandt/ttae089

40. Morgan, S. (2022). Cybercrime to cost the world $10.5 trillion annually by 2025. Cybersecurity Ventures. https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025

41. OECD. (2020). A roadmap toward a common framework for measuring the digital economy: Report for the G20 Digital Economy Task Force. https://www.yunbaogao.cn/index/partFile/5/itu/2022-04/5_22772.pdf

42. Otta, S., & Panda, S. (2022). Decentralized identity and access management of cloud for security as a service. In 2022 14th International Conference on COMmunication Systems & NETworkS (COMSNETS) (pp. 299-303). IEEE. https://doi.org/10.1109/COMSNETS53615.2022.9668529

43. Piasecki, S., & Jiahong Chen, J. (2022). Complying with the GDPR when vulnerable people use smart devices. *International Data Privacy Law*, 12(2), 113-131. https://doi.org/10.1093/idpl/ipac001

44. Raghavan, B., & Schneier, B. (2023). A bold new plan for preserving online privacy and security. IEEE Security & Privacy. http://surl.li/rfcyoy

45. Rothstein, M. A., & Tovino, S. (2019). California takes the lead on data privacy law. *Hastings Center Report*, 49(5), 4-5. https://doi.org/10.1002/hast.1042

46. Sacks, S. (2021). China's emerging data privacy system and GDPR. Centre for Strategic and International Studies. https://www.csis.org/analysis/chinas-emerging-data-privacy-system-and-gdpr

47. Sadowski, J. (2019). When data is capital: Datafication, accumulation, and extraction. *Big Data & Society*, 6(1), 1-12. https://doi.org/10.1177/2053951718820549

48. Schwartz, P. M., & Peifer, K.-N. (2017). Transatlantic data privacy law. *Georgetown Law Journal*, 106(1), 115-179. https://www.law.georgetown.edu/georgetown-law-journal/in-print/volume-106/volume-106-issue-1-november-2017/transatlantic-data-privacy-law

49. Sestino, A., Kahlawi, A., & De Mauro, A. (2023). Decoding the data economy: A literature review of its impact on business, society and digital transformation. *European Journal of Innovation Management*. Advance online publication. https://doi.org/10.1108/EJIM-01-2023-0078

50. Shead, S. (2021). Amazon hit with $887 million fine by European privacy watchdog. *CNBC*. https://www.cnbc.com/2021/07/30/amazon-hit-with-fine-by-eu-privacy-watchdog-

51. Simons, A. (2017). Decentralized digital identities and blockchain: The future as we see it. Microsoft. https://techcommunity.microsoft.com/users/alex%20simons%20(azure)/53477

52. Sovrin Foundation. (2023). Sovrin: A protocol and token for self-sovereign identity and decentralized trust. http://surl.li/lmwbzr

53. Summerfield, C., Goldsmith, J., Greenberg, B., Gat, I., Khepra, A. G., Khosrowshahi, F., Lyons, T., Lyre, Ö., Roff, H., Tegmark, M., & Voss, P. (2024). How will advanced AI systems impact democracy? SchneierOnSecurity. https://www.schneier.com/wp-content/uploads/2024/09/How-Will-Advanced-AI-Systems-Impact-Democracy.pdf

54. United Nations Conference on Trade and Development. (2021). Data protection and privacy legislation worldwide. https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

55. United Nations Conference on Trade and Development. (2023). Data protection and privacy legislation worldwide. https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

56. Ukrainian Parliament Commissioner for Human Rights. (2022). Decree of 15.02.2022 No. 3-p. http://www.ombudsman.gov.ua/ua/page/zpd/

57. Wetzling, T., Sarkesian, L., & Dietrich, C. (2021). Solving the Transatlantic data dilemma: Surveillance reforms to break the international gridlock. Stiftung Neue Verantwortung. https://www.stiftung-nv.de/publications/downloadPdf/solving-transatlantic-data-dilemma

58. White House. (2022). Biden-Harris administration announces key actions to advance tech accountability and protect the rights of the American public. http://surl.li/sddjac

59. World Economic Forum. (2021). Reimagining data privacy for the 21st century. https://www.weforum.org/agenda/2021/07/reimagining-data-privacy-for-the-21st-century

60. World Bank. (2022). Europe and Central Asia economic update, Spring 2022: War in the region. https://hdl.handle.net/10986/37268

61. Xiong, Y. (2022). China fines Didi $1.2 billion for violating cybersecurity and data laws. CNN. https://edition.cnn.com/2022/07/21/economy/china

62. Zuboff, S. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power. PublicAffairs.

The article was received by the editors 21.11.2024
The article is recommended for printing 20.12.2024