УДК 346.58
DOI: 10.31359/1993-0909-2023-30-4-304

Владислав Ігорович Камишанський

Відділ проблем модернізації господарського права та законодавства
Державна установа «Інститут економіко-правових досліджень
імені В. К. Мамутова Національної академії наук України»
Київ, Україна

ТРАНСКОРДОННА ПЕРЕДАЧА ДАНИХ У КОНТЕКСТІ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ ЗОВНІШНЬОЕКОНОМІЧНОЇ ПОЛІТИКИ

Анотація. *Взаємозалежність розвитку інновацій та транскордонної передачі даних стала новим викликом для зовнішньоекономічної політики країн світу та поставила на порядок денний багато регуляторних питань щодо їх суверенітету, захисту конфіденційності, національної безпеки та інших внутрішніх цінностей та інтересів. Як наслідок країни вдалися до розробки відповідного законодавства. Втім не завжди їх підходи узгоджуються між собою та підходами міжнародних інституцій, міжнародних торговельних угод тощо. За відсутності спільних зусиль усіх зацікавлених сторін (країн, міжнародних організацій, компаній та ін.) у напрямі правового регулювання транскордонної передачі даних така неузгодженість лише зростатиме. Метою статті є аналіз різноманітних підходів (зокрема, країн Європейського Союзу, Сполучених Штатів Америки, міжнародних інституцій) щодо правого регулювання транскордонної передачі даних (у тому числі захисту персональних даних при такій передачі) у рамках реалізації зовнішньоекономічної політики, положень міжнародних угод тощо, виявлення недоліків та розробки пропозицій для їх усунення. Аналіз доводить, що Україна та інші країни, які розглядають питання захисту персональних даних, стоять перед важливим вибором між регуляторними підходами Європейського Союзу та Сполучених Штатів Америки. Цей вибір впливає на можливості транскордонної передачі даних, торгівлю та розвиток інновацій, особливо для глобальних компаній, що працюють у зазначених вище регіонах. Країни, які імплементують Загальні правила захисту даних (General Data Protection Regulation) Європейського Союзу або аналогічні регуляторні підходи, зобов'язані дотримуватися цього законодавства для захисту прав громадян та уникнення санкцій з боку даного Союзу та інших регуляторів. Однак ця імплементація може бути дорогою та тривалою для компаній та країн, і має потенціал впливати негативно на зовнішньоекономічні відносини та інноваційний розвиток. Для уникнення конфліктів між різними регуляторними підходами, врахування правил міжнародних організацій, таких як Світова організація торгівлі, Організація економічного співробітництва та розвитку, і розробки єдиної стратегії в області обміну даними важливою є спільна співпраця різних стейкхолдерів. Обґрунтовано доцільність удосконалення General Data Protection*

Regulation з метою віднайдення балансу між захистом даних та підтримкою інновацій, включаючи розробку класифікації даних за чутливістю, використання технічних засобів анонімізації даних тощо. При цьому особливого значення набуває постійний моніторинг та оновлення таких правил з метою адаптації до нових технологічних реалій і викликів.

Ключові слова: *транскордонна передача даних, інновації, зовнішньоекономічна політика, персональні дані, штучний інтелект, цифрова трансформація.*

Vladyslav I. Kamyshanskyi

Department of Modernisation of Economic Law and Legislation
State Organization «V. Mamutov Institute of Economic and Legal Research of National Academy of Sciences of Ukraine»
Kyiv, Ukraine

CROSS-BORDER DATA TRANSFER IN THE CONTEXT OF DIGITAL TRANSFORMATION OF FOREIGN ECONOMIC POLICY

Abstract. *The interdependence between the development of innovations and cross-border data transmission has become a new challenge for the foreign economic policies of countries worldwide. This interdependence has brought regulatory issues to the forefront, pertaining to national sovereignty, data confidentiality, national security, and other internal values and interests. As a result, countries are faced with the development of relevant legislation. However, the approaches taken by different countries do not always align with each other or with the approaches of international institutions, international trade agreements, and more. In the absence of concerted efforts by all stakeholders, including countries, international organizations, companies, and others, to regulate cross-border data transmission, this lack of alignment will continue to grow. This article aims to analyze various approaches, including those of the European Union, the United States, international institutions, concerning the legal regulation of cross-border data transmission (including the protection of personal data during such transmission) within the framework of implementing foreign economic policies, international agreements, and more. The analysis seeks to identify shortcomings and develop proposals for their mitigation. The analysis reveals that Ukraine and other countries considering data protection issues face a crucial choice between regulatory approaches, such as those of the European Union and the United States. This choice significantly affects the potential for cross-border data transmission, international trade, and innovative development, particularly for global companies operating in these regions. Countries that implement the General Data Protection Regulation of the European Union or similar regulatory approaches are obliged to adhere to this legislation to protect the rights of citizens and avoid sanctions from the European Union and other regulators. However, this implementation can be costly and time-consuming for both companies and countries, potentially negatively impacting international trade relations and innovative development. To avoid conflicts between different regulatory approaches, it is essential to consider the rules of international organizations, such as the World Trade Organization and the Organization for Economic Co-operation and Development, and develop a unified strategy for data exchange. The article underscores the need to improve the General Data Protection Regulation continuously to strike a balance between data protection and innovation support. This includes devel-*

oping data classification based on sensitivity, using technical data anonymization measures, among other considerations. Additionally, constant monitoring and updates of these regulations are critical for adapting to new technological realities and challenges.

Keywords: *cross-border data transfer, innovation, foreign economic policy, personal data, artificial intelligence, digital transformation*.

ВСТУП

У контексті цифрової трансформації зовнішньоекономічної політики дані набувають особливого значення. Збільшення їх ролі у відносинах, на регулювання яких спрямована така політика, призводить до їх обміну між країнами (транскордонного обміну). У протилежному випадку інновації сучасної економіки, до яких звикло суспільство в повсякденному житті, наприклад, надання цифрових продуктів і послуг, аутсорсинг послуг, програми хмарних обчислень або Інтернет речей тощо не функціонуватимуть. Важливо також розуміти, що існує сильна взаємозалежність між транскордонними потоками даних та цифровими інноваціями. Наприклад, доступність даних та їх вільний потік через кордони часто розглядаються як важливі передумови розвитку технологій штучного інтелекту (ШІ) [1; 2].

Ця взаємозалежність стала новим викликом для зовнішньоекономічної політики країн світу, адже використання даних актуалізує багато регуляторних питань щодо їх суверенітету, захисту конфіденційності, національної безпеки й інших внутрішніх цінностей та інтересів. На цій підставі країни вдалися до розробки відповідного законодавства. Підходи деяких з них, зокрема країн Європейського Союзу (ЄС) [3], спрямовані на обмеження потоків даних і, відповідно міжнародної торгівлі, та в окремих випадках протирічать правилам Світової організації торгівлі, Угоди про преференційну торгівлю тощо [4]. І ця напруга між внутрішніми та міжнародними правилами загалом, а також між конфіденційністю та вільними потоками даних зокрема, неминуче зростатиме. В таких умовах політикам потрібно буде знайти певні рішення для віднайдення компромісу між ними [5]. Це може бути особливо складним завданням, оскільки підходи ЄС (зокрема, які Україна має імплементувати в умовах євроінтеграції), до захисту персональних даних є в дечому відмінними, наприклад від підходів Сполучених Штатів Америки (США), Сполученого королівства Великої Британії та Північної Ірландії). Відсутність єдності підходів до регулювання зазначених вище питань може призвести до конфліктів та непорозумінь, ускладнити транскордонний обмін даними, і, як наслідок, розвиток технологій в окремих країнах. Зазначене актуалізує проведення досліджень у відповідному напрямі.

1. ОГЛЯД ЛІТЕРАТУРИ

Науковий інтерес до вивчення особливостей транскордонної передачі даних у рамках реалізації зовнішньоекономічної політики (зокрема, зовнішньоторго-

вельної політики та політики іноземного інвестування), стрімко зростає. Відсутність єдності підходів країн та міжнародних організацій щодо правового регулювання цих процесів негативно вливає на зовнішньоекономічні відносини, розвиток інновацій, та підштовхує вчених до спроб віднайдення компромісних рішень у відповідному напрямі.

Загалом їх роботи присвячуються аналізу транскордонної передачі персональних даних за законодавством ЄС, зокрема Загальними правилами захисту даних (General Data Protection Regulation (GDPR)), міжнародними торговельними угодами (зокрема, угодами про цифрову торгівлю, цифрову економіку) тощо. Вчені зупиняються на дослідженні питань щодо «суперницьких стандартів» [6] або, як висловився один науковець, «транснаціонального нормативного конфлікту та взаємозалежності» [7, с. 1; 8], а також «перехрещенню норм» екстериторіальних законів [9], зокрема між США та ЄС.

Досить цікавою у відповідному напрямі є книга Naef Tobias «Data Protection without Data Protectionism», в якій автор вдається до аналізу особливостей юридичного конфлікту між конфіденційністю та торгівлею в цифровій сфері. Їх взаємопов'язаність стала темою світової уваги після викриття Едварда Сноудена щодо масового стеження в США. Ґрунтуючись на претензіях, висунутих активістом Максиміліаном Шремсом, Європейський суд ухвалив два резонансних рішення, які обмежують потоки даних між ЄС та США. Однак після цих рішень залишилося нез'ясованим, яким чином можна поєднати захист конфіденційності й торгівлю на міжнародному рівні. Автор наголошує, що основні права ЄС мають пріоритет перед міжнародним правом та, на цій підставі, пропонує рекомендації щодо регулювання потоків даних [10].

Подібний вектор досліджень простежується у роботі Julien Chaisse «The Black Pit: Power and Pitfalls of Digita lFDI and Cross-Border Data Flows», але у взаємозв'язку із політикою іноземного інвестування. В статті обговорюється взаємодія між національними та міжнародними правовими системами, а також те, як мінливий характер ліберального міжнародного порядку впливає на транскордонний потік даних. Автор підкреслює необхідність оновлення існуючих міжнародних угод і законів з метою врахування фактору цифрових інвестицій [11].

Leila Brännström розглядає підхід ЄС до управління даними, як такий, що сповнений протиріч [12]. Зокрема, відповідно до Європейської стратегії щодо даних, Союз прагне посилити вільний потік даних і підвищити довіру до механізмів обміну даними на внутрішньому ринку. Однак ця амбіція контрастує з більш «захисним» підходом ЄС до управління транскордонними потоками даних. Високі стандарти захисту даних у ЄС призвели до ряду обмежень на передачу персональних даних за межі Європейської економічної зони [13].

Як слушно зазначає Miadzvetskaya Yu. та інші автори, основний принцип полягає в тому, що європейський високий рівень захисту повинен поширюватися на дані за межі кордонів ЄС [13; 14]. У науковій літературі такі підходи називають

по різному: «протекціонізм даних» [15], «м'які» [16] або «фактичні « [17] заходи локалізації даних [18].

Саме тому систему захисту даних ЄС переважно вважають, як непродуктивну. Ця непродуктивність разом із прагненням піднятися вгору по сходах глобальних цифрових ланцюжків доданої вартості робить позицію ЄС щодо транскордонних потоків даних неоднозначною і послаблює його позиції на міжнародній арені [12].

Qing Chang та інші приділяють увагу дослідженню впливу транскордонних потоків даних та існуючих розривів у розвитку економіки даних на виробництво та міжнародну торгівлю [19]. Схожої думки додержується й Kulhari S. У своїй роботі «Bryan Mercurio and Ronald Yu: Regulating Cross-Border Data Flows» учений використовує територіальний підхід до проблем, викликів і впливу регулювання транскордонних потоків даних [20].

Деякі автори наголошують, що цифровий розрив, питання конфіденційності даних і проблеми безпеки, перешкоджають G20 реалізувати потенціал транскордонного потоку даних, а також відкритих інтерфейсів прикладного програмування та цифрової публічної інфраструктури. Для вирішення проблем, що виникають у зв'язку з цими питаннями, необхідна колективна відповідь від G20. Спираючись на досвід Індії у сфері цифрових платежів, автори намагаються розширити глобальний діалог і пропонують рамки, навколо яких може бути побудована цифрова державна інфраструктура для ефективної транскордонної передачі даних [21].

Слід відмітити і низку робіт з питань безпеки та відкритості моделі транскордонного потоку даних Китайської народної республіки [22; 23; 24].

На національному рівні вчені вдаються переважно до аналізу загальних питань правового забезпечення захисту персональних даних у країнах ЄС [25; 26] і окреслюють причини невідповідності інформаційного законодавства України вимогам сучасності [27].

В цілому літературний огляд указує на актуальність і складність проблеми транскордонної передачі даних та підкреслює необхідність подальших досліджень і розробки політичних рішень для регулювання цього процесу в рамках реалізації зовнішньоекономічної політики України.

2. МАТЕРІАЛИ ТА МЕТОДИ

Для досягнення поставленої мети дослідження щодо особливостей транскордонної передачі даних використані спеціальні методи наукового пізнання, які дозволили аналізувати дану тему з різних точок зору та розкрити її ключові аспекти. Серед них важливими є: діалектичний, герменевтичний, аналітико-синтетичний, формально-логічний методи, а також метод системно-структурного аналізу та узагальнення.

Діалектичний метод був використаний для аналізу суперечливості та взаємозв'язку між різними законодавчими підходами до транскордонної передачі даних (зокрема, персональних) в ЄС, США, Україні та інших країнах, а також для виявлення основних тенденцій у розвитку цієї сфери.

Аналітико-синтетичний метод був використаний для узагальнення та систематизації інформації про різні підходи до регулювання транскордонної передачі даних, а також для формулювання висновків і рекомендацій щодо оптимальних стратегій у цій сфері.

Формально-логічний метод застосовувався для аналізу логічних зв'язків та консистентності аргументації, що використовується в регулюванні транскордонної передачі даних. Цей метод допоміг виявити можливі суперечності та недоліки в існуючих підходах.

Аналіз показав, що зв'язок між регуляторними підходами ЄС і США до обробки персональних даних та їх впливом на міжнародну торгівлю, інновації та транскордонну передачу даних викликає значний інтерес у сучасному світі. Ця тема особливо актуальна для глобальних компаній, які здійснюють операції та мають клієнтів в обох регіонах, а також для країн, зокрема України, які прагнуть забезпечити відповідність свого законодавства регуляторним вимогам ЄС (GDPR) для уникнення санкцій з боку ЄС або інших регуляторів. Зазначені вище методи дозволили дійти висновку, що з одного боку, це сприяє підвищенню захисту прав індивідуальних осіб і виконанню міжнародних стандартів. З іншого боку, процес імплементації GDPR може вимагати значних фінансових та трудових ресурсів, а також завдати негативного впливу на зовнішньоекономічні відносини та інноваційний розвиток (зокрема, розвиток технологій ШІ). Це особливо важливо для країн-партнерів ЄС, які прагнуть дотримуватися стандартів GDPR для забезпечення безпеки даних та співпраці з європейськими компаніями.

Тлумачення та розуміння нормативних актів, міжнародних угод, підходів міжнародних організацій, зокрема СОТ, ОЕСР, АТЕС, що стосуються досліджуваного питання здійснено з використанням методу правової герменевтики. Це дозволило докладно проаналізувати зміст, обсяг прав і обов'язків сторін у відповідній сфері та обґрунтувати доцільність вироблення єдиної методології або підходу до обробки та передачі даних як з боку ЄС, так і міжнародних організацій. Взаємодія між ЄС та іншими країнами з цими організаціями в створенні спільних підходів може допомогти уникнути протиріч та торговельних суперечок, а також забезпечити захист прав та інтересів усіх зацікавлених сторін. Подібна співпраця також може сприяти розвитку загальних стандартів і принципів для захисту даних, розробці кращих практик і технологій, а також підвищенню рівня свідомості та підготовки країн для протидії кіберзагрозам.

За допомогою системно-структурного аналізу були досліджені взаємозв'язки та взаємодія різних елементів системи регулювання транскордонної передачі даних. Такий метод дозволив розглянути цю проблему як складну систему, що включає в себе багато взаємозалежних факторів.

Загалом завдяки використанню зазначених вище методів дослідження вдалося ретельно проаналізувати та систематизувати інформацію щодо транскордонної передачі даних, визначити основні тенденції й проблеми у цій сфері, а також

сформулювати рекомендації щодо подальшого розвитку правового регулювання. За допомогою методу узагальнення сформульовано висновок про те, що баланс між захистом даних і підтримкою інновацій може бути досягнутий за допомогою розробки класифікації даних, використання технічних засобів захисту та шифрування, а також спільної роботи між країнами й міжнародними організаціями.

3. РЕЗУЛЬТАТИ ТА ОБГОВОРЕННЯ

Повсюдне використання даних (яке стрімко зростає у міру цифрової трансформації економік світу) викликало занепокоєння з боку урядів країн щодо конфіденційності та безпеки їх передачі, а також актуалізувало розробку й прийняття відповідного законодавства. Втім одночасне досягнення потрійних політичних цілей, як-то забезпечення транскордонного потоку даних з метою розвитку цифрової економіки, збереження конфіденційності й надання урядам контролю над ними (даними) виявилося складним завданням. Це сприяло появі різноманітних підходів, як з боку міжнародних інституцій, так і окремих країн, у відповідному напрямі.

Організація економічного співробітництва та розвитку (ОЕСР) була першою організацією, яка «зіткнувшись із двома занепокоєннями щодо загроз конфіденційності через інтенсивніше використання персональних даних і ризики для глобальної економіки через обмеження потоку інформації», підготувала міжнародно узгоджені керівні принципи захисту конфіденційності. Метою документу стало досягнення глобального консенсусу щодо захисту персональних даних у державному та приватному секторах [28]. Він містить 8 принципів національного застосування, серед яких принципи: обмеження збору; якості даних; визначенні мети; обмеження використання; гарантії безпеки; відкритості; індивідуальної участі особи; підзвітності. Крім цього частиною третьою документу визначено 4 принципи міжнародного застосування, зокрема держави-члени повинні: враховувати наслідки внутрішньої обробки та реекспорту персональних даних для інших держав-членів; вживати всіх розумних і належних заходів для забезпечення безперебійності та безпеки транскордонних потоків персональних даних, у тому числі транзиту через країну-члена; утримуватися від обмеження транскордонних потоків персональних даних між нею та іншою країною-членом, за винятком окремих випадків; уникати розробки законів, політики та практики в ім'я захисту приватного життя та індивідуальних свобод, які б створювали перешкоди для транскордонних потоків персональних даних, які б перевищували вимоги до такого захисту [29].

Прийняття Керівних принципів вплинуло на розвиток національного законодавства та типових кодексів у країнах-членах ОЕСР та за їх межами. Востаннє оновлені в 2013 році, протягом тривалого часу, вони слугували основним орієнтиром для підтримки довіри до потоків даних, у тому числі й для розробки Загальних правил захисту даних (General Data Protection Regulations – GDPR) Єв-

ропейського Союзу 2016 року. Втім у 2020 році уряди країн-членів ОЕСР були звільнені від дотримання вказівок організації з міркувань «національної безпеки та державної політики». Після цього на прохання Групи 20 (G-20) ОЕСР було створено неофіційну експертну групу, яка розпочала працювати над темою «вільного потоку даних із довірою». Метою таких заходів було «підвищення довіри між демократичними системами, заснованими на верховенстві права, які, хоч і не є ідентичними, мають значні спільні риси…», та «забезпечення стандарту того, як демократичні, засновані на верховенстві права системи обмежують владу уряду на відміну від підходів, які є необмеженими, необґрунтованими, свавільними або непропорційними, що порушують права людини та міжнародні зобов'язання» [30].

Як наслідок роботи експертної групи, було прийнято Декларацію про державний доступ до персональних даних, що знаходяться в приватному секторі (Declaration on Government Access to Personal Data Held by Private Sector Entities). Документом визначено принципи державного доступу до персональних даних, що зберігаються суб'єктами приватного сектору [31]. Крім цього на базі бізнес-консультацій було підготовлено та опубліковано серію звітів. Серед іншого, як у звітах, так і в декларації підкреслюється необхідність посилення міжнародної нормативно-правової співпраці та використання повного спектру можливостей для підтримки довіри щодо конфіденційності та захисту даних у всьому світі [32; 33]. А отже видання Принципів ОЕСР не вичерпує можливості багатосторонньої роботи щодо доступу урядів до персональних даних. На цьому зауважує й сама організація. Зокрема, у Декларації наголошується на доцільності зацікавлених сторін у проведенні додаткової роботи зі сприяння довіри в контексті придбання комерційно доступних персональних даних, доступу до загальнодоступних персональних даних та отримання добровільного розкриття персональних даних правоохоронними органами та органами національної безпеки. ОЕСР утрималася від будь-яких зобов'язань щодо роботи над відповідними питаннями. Хоча вони мали б бути її (організації) логічними наступними кроками [30].

Серед іншого вдається доцільним розглянути можливість всебічного оприлюднення на спеціальній платформі відповідного національного законодавства із наданням країнам-членам доступу до цієї інформації. Такого компендіуму наразі не існує [30]. Втім він може бути важливим джерелом інформації для порівняльного аналізу та оцінки стандартів і практик у різних країнах з метою підвищення прозорості й відкритості в урядовій діяльності. Крім того наявність компендіуму сприятиме (1) стимулюванню країн-членів до вдосконалення своїх законів і практик доступу до інформації, оскільки це може позначитися на їх міжнародному рейтингу та репутації; (2) полегшенню проведення досліджень і аналізу в галузі доступу до інформації та прав людини (зокрема, вчені, ЗМІ та організації громадянського суспільства можуть використовувати цю інформацію для проведення різноманітних досліджень та аналізу); (3) забезпеченню до-

триманню зобов'язань (зокрема, шляхом використання інформації розміщеної на ньому для моніторингу й оцінки дотримання членами своїх зобов'язань у галузі прозорості та доступу до даних).

Наразі Агентство з основних прав ЄС опублікувало два звіти про відповідну практику держав-членів ЄС, але інформація, яка міститься в них є неповною й застарілою. Оприлюднення такого роду інформації серед членів ОЕСР продемонструвало б, що зобов'язання відносно прозорості в зазначеній вище Декларації сприймаються серйозно [30].

Окрім Керівних принципів ОЕСР слід відзначити Концепцію конфіденційності (Privacy Framework) Азійсько-Тихоокеанського економічного співробітництва (АТЕС) 2005 року [34]. За змістом вона схожа на Директиви ОЕСР щодо конфіденційності, але застосовуються виключно до обробки персональних даних у приватному секторі. Концепція конфіденційності АТЕС є набором принципів та рекомендацій, розроблених для забезпечення ефективного захисту конфіденційності, який би не створював перешкоди для потоків інформації в регіоні АТЕС, що включає 21 країну. На основі цього документу АТЕС розробила систему Правил конфіденційності через кордони (APEC Cross Border Privacy Rules), до якої формально приєдналися Австралія, Китайська Тайпеї, Канада, Японія, Південна Корея, Мексика, Сінгапур та Сполучені Штати.

Взаємодія між ОЕСР і АТЕС в напрямі забезпечення конфіденційності інформації, яка передається через кордони, є актуальною, зважаючи на зростаюче значення цифрової економіки й обміну даними між країнами. Зокрема, ОЕСР має багатий досвід та експертність у розробці стандартів і рекомендацій щодо захисту даних та приватності, які можуть бути корисними для країн азійсько-тихоокеанського форуму. Оскільки АТЕС включає в себе різноманітні економіки з різним рівнем розвитку, його спільна робота з ОЕСР сприятиме (1) створенню загальних стандартів та принципів, які враховують інтереси різних країн та забезпечують високий рівень конфіденційності даних, (2) спільному розвитку кращих практик і технологій для захисту даних, а також (3) підвищенню рівня свідомості та підготовки країн у напрямі протидії кіберзагрозам, безпеки передачі даних тощо.

Як уже було зазначено вище, декларації ОЕСР стали базовими для розробки національних законодавств з питань захисту персональних даних, зокрема при реалізації зовнішньоекономічної політики. Водночас спостерігається різне їх сприйняття країнами-членами організації на практиці.

В якості одного з прикладів, слід відмітити досвід Європейського Союзу, де у 2016 році було прийнято Загальний регламент про захист даних (GDPR). GDPR привернув увагу як один із найсуворіших і найнадійніших законодавчих підходів до захисту даних, що ґрунтується на визнанні права на конфіденційність як ключової концепції в законодавстві ЄС. Його вимоги розповсюджуються не лише на суб'єктів господарювання – резидентів, а й також на суб'єктів господарювання – нерезидентів, які обробляють дані громадян ЄС. Ця ініціатива

є важливою, оскільки Союз установлює власні стандарти щодо захисту даних і допускає передачу персональних даних лише до тих юрисдикцій, які вважаються належно захищеними від порушень конфіденційності. Наразі Андорра, Аргентина, Канада (комерційні організації), Фарерські острови, Гернсі, Ізраїль, острів Мен, Японія, Джерсі, Нова Зеландія, Республіка Корея, Швейцарія, Сполучене Королівство відповідно до GDPR та Директиви про правоохоронну діяльність (Law Enforcement Directive), Сполучені Штати (комерційні організації, які беруть участь у Рамковій угоді про захист даних між ЄС та США) та Уругвай визнані такими країнами [35]. Принагідно зазначимо, що оцінка адекватності рівня захисту доволі вибагливий процес. Зокрема, відповідно до ч. 2 ст. 45 GDPR Комісія бере до уваги такі елементи, як (1) верховенство права, повага до прав людини та основних свобод, відповідне законодавство, як загальне, так і галузеве, в тому числі щодо громадської безпеки, оборони, національної безпеки та кримінального права та доступу державних органів до персональних даних, а також виконання такого законодавства, правила захисту даних, професійні правила та заходи безпеки, включаючи правила подальшої передачі персональних даних до іншої третьої країни або міжнародної організації, які діють у цій країні або міжнародній організації, прецедентне право, а також дані, які є ефективними та мають юридичну силу права суб'єктів та ефективний адміністративний і судовий захист для суб'єктів даних, чиї персональні дані передаються; (2) існування та ефективне функціонування одного чи кількох незалежних наглядових органів у третій країні або підпорядкованих міжнародній організації, відповідальних за забезпечення та дотримання правил захисту даних, включаючи адекватні правозастосовні повноваження, для надання допомоги та консультування суб'єктів даних у здійсненні своїх прав і співпраці з наглядовими органами держав-членів; (3) міжнародні зобов'язання, які взяла на себе відповідна третя країна чи міжнародна організація, або інші зобов'язання, що випливають із юридично обов'язкових конвенцій чи інструментів, а також із її участі в багатосторонніх або регіональних системах, зокрема, щодо захисту персональних даних [36]. Наприклад, у відносинах ЄС із Японією в рамках Угоди про економічне партнерство (Economic Partnership Agreement), адекватність рівня захисту останньої були визнані союзом лише через три роки після її підписання [37; 38]. Таким чином, країнам, які не мають аналогічного рівня захисту даних, доведеться робити певні зміни в своєму законодавстві та практиках, щоб отримати статус «адекватності». Водночас сам процес імплементації GDPR є тривалим і складним завданням. Він включає в себе вдосконалення законодавства, створення органів регулювання та зміну практик обробки даних. За таких обставин виникають ризики затримки можливості обміну даними з ЄС на досить тривалий час.

Описана вище позиція ЄС кардинально відрізняється від підходу Сполучених Штатів Америки, де існує більш ліберальний підхід до управління даними. Це ви-

кликає напругу між країнами (ЄС і США). Хоча обмін інформацією все ж таки відбувається.

Крім цього, ЄС розглядає GDPR як інструмент зовнішньої політики для поширення власних стандартів захисту даних за межі своїх кордонів. Натомість США спираються на торговельні угоди (двосторонні чи регіональні) для регулювання транскордонної передачі даних. Такі угоди надають пріоритет вільному потоку даних і чітко забороняють обмеження їх локалізацією. А отже, «основою підходу США, як видається, є надання пріоритету торгівлі над правами на приватність. У той час як ЄС використовує торговельні угоди для забезпечення захисту даних як фундаментального права людини й наголошує на необхідності збереження свого регуляторного простору для заходів захисту даних» [39].

Включення статей, які забороняють використання вимог щодо локалізації даних, знову ж таки з урахуванням певних обґрунтованих стороною винятків, до угод про цифрову торгівлю є стандартною практикою (в тому числі серед країн, які пройшли тест ЄС на «адекватність»)[1]. Крім цього, досить розповсюдженими для них (угод) є положення, які зобов'язують сторони всіляко сприяти транскордонній передачі даних із можливістю застосування певних обмежень, за умови, якщо вони необхідні для досягнення мети державної політики та не є свавільними, невиправдано дискримінаційними, штучно не обмежують торгівлю та не накладають більших обмежень на передачу інформації, ніж ті, що необхідні для досягнення цієї мети [41; 42]. Щодо позиції ЄС, то він не проти вимог щодо локалізації даних, втім дуже обережно підходить до положень щодо вільного їх потоку. Винятки із правил «досягнення мети державної політики» вдаються недостатніми, на думку Союзу, для забезпечення фундаментального права своїх громадян на приватність [43].

Слід звернути увагу й на недоліки GDPR, які ускладнюють можливість упровадження інновацій. Найбільш значущими з них є наступні.

По-перше, відповідно до ст. 5 GDPR організації можуть збирати дані для чітко визначених цілей. Іншими словами вони не можуть збиратися безцільно та використовуватися в подальшому повторно (для інших цілей). Втім досить часто дані створюють цінність, коли їх об'єднують. Зокрема, точність та ефективність систем ШІ залежить від доступу до великих наборів об'єднаних даних. Наприклад, якщо компанія, яка знаходиться в ЄС і розробляє системи ШІ, має намір використовувати персональні дані користувачів для покращення своїх алгоритмів, вона повинна отримати таку згоду від користувача, і не може використовувати дані для інших цілей без додаткової згоди. Таке обмеження впливає на розвиток ШІ, оскільки воно ускладнює збір та використання даних для на-

[1] Угодою про цифрову торгівлю між Сполученим Королівством Великої Британії та Північної Ірландії та Україною, зокрема пунктами 1, 2 ст. 132-L передбачена заборона встановлення власних нормативних вимог щодо використання обчислювальних засобів на території однієї сторони як умови для ведення бізнесу на цій території [40].

вчання алгоритмів. Розробники такої технології можуть відчувати необхідність в обробці великих обсягів даних для створення більш точних і корисних систем ШІ, й обмеження мети може ускладнити цей процес.

Насправді, напруженість навколо GDPR викликана двома основними принципами обробки даних, які кодифіковані в цьому документі, але походять від «принципів справедливої інформаційної практики» початку 1970-х років [44]. Це принцип «обмеження мети», який передбачає, що обробка персональних даних має відбуватися для певних законних цілей, а не для подальших несумісних цілей (п. b ч. 1 ст. 5 GDPR), і принцип «мінімізації даних», який зазначає, що ці дані повинні бути достатніми, відповідними та обмеженими тим, що необхідно для досягнення мети, з якою вони обробляються (п. c ч. 1 ст. 5 GDPR). Аналізуючи їх у своїй роботі, Leila Brännström доходить висновку, що «європейське законодавство про захист даних надто сильно розходиться з цифровими економічними практиками XXI століття, а це є твердженням того, наскільки вищезазначені принципи не відповідають вимогам часу» [12].

У цьому контексті важливо збалансувати захист приватності й інтереси розробників ШІ, шукаючи способи забезпечити дотримання принципу обмеження мети, але при цьому не обмежувати можливості розвитку та використання ШІ.

Отже, організації, які підпадають під дію GDPR, можуть мати обмежений (первісними цілями) доступ до даних. Це ставить їх у менш вигідне становище в порівнянні, наприклад з конкурентами з США та Китаю, і не тільки в рамках розвитку інновацій, а й при здійсненні міжнародної торгівлі. Коли, наприклад, європейська компанія зберігає персональні дані своїх клієнтів та споживачів відповідно до стандартів GDPR і планує поділитися цими даними з американською компанією, вона повинна знайти обґрунтований механізм для передачі цих даних поза межі Європейського Союзу. Це стає необхідністю через те, що захист даних у США може не відповідати стандартам GDPR, що діють в ЄС.

По-друге, GDPR сприяє обмеженню використання даних ШІ для прийняття автоматизованих рішень щодо окремих осіб і, як наслідок, робить цей процес більш повільним та витратним. Зокрема, ст. 22 GDPR закріплює право таких осіб вимагати перевірки та пояснення, згенерованої технологією, інформації людиною (посадовою особою). Водночас залучення посадових осіб до «ручної» перевірки такої інформації є додатковою витратною статтею для компанії та негативно впливатиме на швидкість прийняття відповідних рішень. Таким чином, GDPR сприяє використанню людських ресурсів на користь точності та захисту клієнтів, і водночас обмежує використання ШІ для автоматизації багатьох процесів. Утім основною метою використання такої технології є оптимізація часу та ресурсів, які люди витрачають на обробку даних.

Крім цього, GDPR передбачає прямі витрати, такі як отримання згоди від фізичних осіб на обробку їхніх даних і працевлаштування спеціалістів із захисту даних. Компанії також стикаються зі значними комплаєнс-ризиками з огляду

на неоднозначні положення закону через: (1) невизначеність щодо того, як ці положення будуть інтерпретуватися органами захисту даних, а також (2) високі штрафи від регуляторів за порушення – як навмисні, так і ненавмисні. Компанії, швидше за все, будуть діяти обережно й обмежуватимуть використання даних, щоб уникнути конфліктів з регулюючими органами. Натомість у країнах, де GDPR не застосовується, таких як США і Китай, компанії будуть розвивати технології без таких обмежень, зокрема не чекаючи виходу з цієї регуляторної невизначеності.

Якщо не будуть вирішені ці проблеми GDPR може гальмувати торгівлю, а також розвиток та використання ШІ в Європі та інших країнах, які взяли на себе обов'язок імплементації європейського законодавства (зокрема, Україні[1]) і водночас пов'язані зобов'язаннями за торгівельними угодами із США тощо. Це ставитиме компанії відповідних країн у невигідне конкурентне положення в глобальній алгоритмічній економіці [45].

Різні підходи до конфіденційності та захисту даних також можуть кваліфікуватися як торговий бар'єр. Зокрема, у контексті передачі даних між США та ЄС часто повідомлялося, що розбіжності призводять до значних витрат і невизначеності для компаній, особливо для малих та середніх підприємств [5]. Тим більше, що чинним законодавством СОТ не передбачено конкретних положень відносно транскордонної передачі даних.

Підхід ЄС, що підсилює «Брюссельський ефект» (коли фірми мають відповідати внутрішнім стандартам ЄС, щоб мати доступ до ринку), є витратним для іноземних та місцевих компаній і країн. Ця стратегія також негативно впливає на економіку ЄС та її інноваційну складову в епоху Великих даних і ШІ. Сам ЄС ризикує опинитися в складному положенні, оскільки GDPR порушує правила СОТ, і рішення про адекватність не завжди відповідають вимогам Європейської хартії прав людини [39]. Водночас визнання країнами СОТ GDPR або подібних нормативно правових актів такими, що обмежують торговельні можливості та несумісні з правилами організації (СОТ), може призвести до торговельних суперечок і судових процесів. Задля уникнення можливих протиріч та віднайдення спільного розуміння щодо правил обробки даних та їх впливу на міжнародну торгівлю, доцільною є взаємодія між ЄС і СОТ (правила GDPR та СОТ мають співіснувати та враховувати права та інтереси всіх сторін).

Між тим низькі стандарти захисту даних можуть також розглядатися як торговельна перешкода, оскільки вони посилюють недовіру споживачів. А це є важливою умовою для розвитку цифрової торгівлі [5].

Деякі аналітики пропонують оновити GDPR. Йдеться про внесення в нього положень, які сприятимуть інноваціям і використанню нових технологій, таких як ШІ, що залежать від великих масивів даних. Створення регуляторних «пісоч-

[1] В Україні наразі триває робота над імплементацією GDPR ЄС у рамках проєкту Закону «Про захист персональних даних» (реєстр. номер 8153 від 25.10.2022).

ниць», які дозволять проводити подібні експерименти, сприятиме розробці більш ефективного й такого, що відповідає вимогам часу, законодавства [46].

Удосконалення GDPR – це завдання, яке потребує зусиль і співпраці різних стейкхолдерів, включаючи урядовців, експертів, компанії та громадські організації. Головною метою повинно бути збалансування захисту даних і сприяння інноваціям для користі суспільства. Серед можливих заходів у напрямі досягнення такої мети можуть бути: (1) розробка та запровадження класифікації даних, яка б ураховувала різні рівні їх чутливості (зокрема визначення, які дані потребують особливого захисту, а які можуть бути оброблені з меншими обмеженнями); (2) розгляд можливості використання технічних засобів анонімізації даних, які дозволяють використовувати дані для цілей досліджень і розвитку продуктів, не розкриваючи особисту ідентифікацію; (3) забезпечення постійного моніторингу й оновлення GDPR з метою адаптації до нових технологічних реалій і викликів; (4) розробка механізмів для постійного моніторингу й оновлення правил та стандартів тощо.

ВИСНОВКИ

Україна, як і інші країни, які розглядають питання захисту персональних даних, стикаються з вибором між регуляторними моделями ЄС та США. GDPR ЄС установлює жорсткі вимоги до обробки й передачі персональних даних, включаючи механізми для транскордонної передачі даних, які базуються на засадах адекватності, де деякі країни можуть визнаватися адекватними для передачі даних, а інші – ні. У той час як США мають інший підхід, оснований на різних механізмах передачі, таких як Privacy Shield (до його скасування), стандартні договори про обробку даних та ін.

Для країн, які ведуть бізнес як з ЄС, так і США, вибір регуляторного підходу може мати важливий вплив на можливості транскордонної передачі персональних даних, торгівлю, розвиток інновацій тощо. Це є особливо актуальним для глобальних компаній, які мають клієнтів та операції в обох регіонах. Україна, як і будь-яка інша країна, яка імплементує GDPR ЄС або інший регуляторний підхід, повинна сприяти відповідності цьому законодавству, щоб забезпечити захист прав індивідуальних осіб та не допустити санкцій з боку ЄС або інших регуляторів.

Водночас, аргументовано, що імплементація GDPR та забезпечення відповідності його вимогам (зокрема, отримання статусу «адекватності»), можуть бути витратними та тривалими як для компаній, так і для країн, в тому числі України, і завдавати негативного впливу на зовнішньоекономічні відносини, а також інноваційний розвиток не тільки країн партнерів, а й самого Союзу. В свою чергу, задля уникнення протиріч між підходами ЄС до транскордонного обміну даними із відповідними правилами міжнародних інституцій, зокрема СОТ, ОЕСР (членами яких є ЄС), та уникнення торговельних суперечок, доцільною є взаємодія між

ЄС та міжнародними інституціями в напрямі вироблення єдиних підходів з цих питань. Правила GDPR та СОТ, а також рекомендації ОЕСР мають співіснувати та враховувати права й інтереси всіх сторін.

Обґрунтовано створення компендіуму кращих практик упровадження директив ОЕСР на рівні національного законодавства країнами-членами та доступом кожної з них до спільних даних. Це може бути корисним інструментом для підвищення прозорості в урядовій діяльності та порівняльного аналізу стандартів і практик. Введення такого компендіуму сприятиме не тільки вдосконаленню законів у цій сфері, а й також допомагатиме країнам у дотриманні їх зобов'язань у галузі прозорості та доступу до інформації.

Взаємодія між ОЕСР і АТЕС у справах захисту конфіденційності даних, передаваних через кордони, також є корисною, враховуючи зростаюче значення цифрової економіки й обміну даними між країнами. Така співпраця сприятиме не тільки створенню загальних стандартів і принципів для захисту даних, розробці кращих практик і технологій, а й підвищенню рівня свідомості та підготовки країн для протидії кіберзагрозам.

Аргументовано, що вдосконалення GDPR потребує співпраці різних стейкхолдерів і ставить перед собою завдання збалансування захисту даних та підтримки інновацій. Серед можливих заходів у напрямі досягнення такої мети можуть бути: (1) розробка та запровадження класифікації даних, яка б ураховувала різні рівні їх чутливості (зокрема визначення, які дані потребують особливого захисту, а які можуть бути оброблені з меншими обмеженнями); (2) розгляд можливості використання технічних засобів анонімізації даних, які дозволяють використовувати дані для цілей досліджень і розвитку продуктів, не розкриваючи особисту ідентифікацію; (3) забезпечення постійного моніторингу й оновлення (зокрема, розробки механізму моніторингу й оновлення) GDPR, з метою адаптації до нових технологічних реалій і викликів.

РЕКОМЕНДАЦІЇ

Стаття рекомендована для фахівців-юристів у галузі економіки та права, включаючи науковців, викладачів і студентів, практичних працівників та всіх інших, хто цікавиться пошуком і застосуванням нових підходів у дослідженнях проблематики транскордонної передачі даних.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] Aaronsin S. A. Data Minefield? How AI Is Prodding Governments to Rethink Trade in Data. Working paper. 2018. 10 p.

[2] UNCTAD. Digital Economy Report 2019. Value Creation and Capture: Implications for Developing Countries. 17 p. URL: https://unctad.org/en/PublicationsLibrary/der2019_en.pdf (дата звернення 06.10.2023).

[3] Regulation (EU) 2016/679 General Data Protection Regulation in the current version of the OJ L 119, 04.05.2016. URL: https://gdpr-info.eu/

[4] Mitchell A. D., Mishra N. WTO Law and Cross-Border Data Flows An Unfinished Agenda. Big Data and Global Trade Law. Cambridge University Press. 2021. P. 83–112.
[5] Burri M. The Impact of Digitalization on Global Trade Law. German Law Journal. 24(3). P. 551–573.
[6] Drezner D. W. All politics is global: Explaining international regulatory regimes. Princeton University Press, 2009. 259 p.
[7] Shaffer G. Globalization and social protection: the impact of EU and international rules in the ratcheting up of US privacy standards. Yale J. Int'l L. 2000. 25. P. 1–88.
[8] Mercurio B., Yu R. Regulating Cross-Border Data Flows: Issues, Challenges and Impact. Anthem Press, 2023. URL: https://doi.org/10.1007/s40319-023-01298-8
[9] Farrell H., Newman A. L. Of privacy and power: The transatlantic struggle over freedom and security. Princeton University Press, 2019. P. 27–28.
[10] Naef T. Data Protection Without Data Protectionism: The Right to Protection of Personal Data and Data Transfers in EU Law and International Trade Law. Springer Nature, 2023. 431 p.
[11] Chaisse J. The Black Pit: Power and Pitfalls of Digital FDI and Cross-Border Data Flows. *World Trade Review*. 2023. 22(1). P. 73–89.
[12] Brännström L. Global Inequality and the EU International Law Position on Cross-Border Data Flows. *Nordic Journal of International Law*. 2023. 92(1). P. 119–137.
[13] Miadzvetskaya Yu. Data Governance Act: On International Transfers of Non-Personal Data and GDPR Mimesis. *European Data Protection Law Review*. 2023. 9(1). P. 13–26.
[14] Kuner C. Protecting EU Data Outside EU Borders under the GDPR. *Common Market Law Review*. 2023. 60 (1). P. 77–106.
[15] Yakovleva S. Privacy Protection(ism): The Latest Wave of Trade Constraints on Regulatory Autonomy. *University of Miami Law Review*. 2020. 74 (2). P. 473–481.
[16] Chander A. Is Data Localization a Solution for Schrems II? *Journal of International Economic Law*. 2020. 23(3). P. 771–784.
[17] Cory N. How 'Schrems II' Has Accelerated Europe's Slide Toward a De Facto Data Localization Regime. ITIF, 2021. URL: https://itif.org/publications/2021/07/08/how-schrems-ii-has-accelerated-europesslide-toward-de-facto-data
[18] Yakovleva S. Three Data Realms: Convergence or Competition (February 7, 2022). Amsterdam Law School Research Paper № 2022–58. URL: http://dx.doi.org/10.2139/ssrn.4028668
[19] Chang Q., Cong L. W., Wang L., Zhang L. Production, Trade, and Cross-Border Data Flow. Working paper. National Bureau of Economic Research. 2023. 48 p.
[20] Kulhari S. Bryan Mercurio and Ronald Yu. Regulating Cross-Border Data Flows – Issues, Challenges and Impact. IIC. 2023. 54. P. 487–490.
[21] Pandey S., Chaudhary G. Kaushal Mahan, V. P. Digital Public Infrastructure for Efficient Cross-Border Data Flow. 2023. 20 p.
[22] Du X., Liu A. Security and Openness China's Cross-Border Data Flow Scheme. *Pacific International Journal*. 2023. 6(1). P. 138–141. URL: https://doi.org/10.55014/pij.v6i1.326.
[23] Zhang C. RCEP Basic Security Exceptions for Cross-Border Data Flows and China's Response. *Journal of Education, Humanities and Social Sciences*. 2023. 14. P. 36–45. URL: https://doi.org/10.54097/ehss.v14i.8793.
[24] Hu T. Research on Legal Issues of Cross Border Flow of Financial Data from the Perspective of Economic Globalization. In 2023 9th International Conference on Humanities and Social

Science Research (ICHSSR). *Atlantis Press*. 2023. P. 1840–1844. URL: https://doi.org/10.2991/978-2-38476-092-3_236

[25] Врублевська-Місюна К., Тичина В. Міжнародно-правові стандарти захисту інформації про особу. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2022. 2(74). С. 149–154. URL: https://doi.org/10.24144/2307–3322.2022.74.58

[26] Федосенко Н. А., Спіцина Г. О. Актуальні питання міжнародно-правового регулювання захисту персональних даних працівників. *Аналітично-порівняльне правознавство*. 2023. №2. С. 204–208. URL: https://doi.org/10.24144/2788–6018.2023.02.34

[27] Легка О. В. Актуальні питання захисту персональних даних: вітчизняний та міжнародний досвід. *Правова позиція*. 2021. №2(31). С. 74–79. URL: https://doi.org/10.32836/2521–6473.2021–2.15

[28] The Evolving Privacy Landscape: 30 Years After OECD Privacy Guidelines». *OECD Digital Economy Papers*. OECD Publishing, Paris. 2011. №176. URL: https://doi.org/10.1787/5kgf09z90c31-en

[29] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. OECD Publishing, Paris. 2002. URL: https://doi.org/10.1787/9789264196391-en.

[30] Propp K. Gentlemen's Rules for Reading Each Other's Mail: The New OECD Principles on Government Access to Personal Data Held by Private Sector Entities. Lawfare. 2023. URL: https://www.lawfaremedia.org/article/gentlemens-rules-reading-each-others-mail-new-oecd-principles-government-access-personal-data-held

[31] Declaration on Government Access to Personal Data Held by Private Sector Entities. URL: https://legalinstruments.oecd.org/en/instruments/OECD–L

[32] Fostering cross-border data flows with trust. OECD Digital Economy Papers. OECD Publishing, Paris. 2002. №343. 37 p.

[33] Moving forward on data free flow with trust: New evidence and analysis of business experiences. *OECD Digital Economy Papers*. OECD Publishing, Paris. 2023. №353. 38 p. https://doi.org/10.1787/1afab147-en.

[34] APEC Privacy Framework.Reports. CTI Sub-Fora & Industry Dialogues Groups, Digital Economy Steering Group. 2005. 36 p. URL: https://www.apec.org/publications/2005/12/apec-privacy-framework

[35] Adequacy decisions. How the EU determines if a non-EU country has an adequate level of data protection. URL: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en#:~:text=The%20European%20Commission%20has%20so,commercial%20organisations%20participating%20in%20the

[36] Art. 45 GDPRTransfers on the basis of an adequacy decision. URL: https://gdpr-info.eu/art-45-gdpr/

[37] Article 8.81 of EU-Japan Economic Partnership Agreement (JEFTA). URL: https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/japan/eu-japan-agreement_en

[38] European Commission adopts adequacy decision on Japan, creating the world's largest area of safe data flows. URL:https://ec.europa.eu/commission/presscorner/detail/en/IP_19_421

[39] Burri M. Cross-border data flows and privacy in global trade law: has trade trumped data protection? *Oxford Review of Economic Policy*. 2023. 39(1). P. 85–97.

[40] UK/Ukraine: Digital Trade Agreement [CS Ukraine №2/2023] (Article 132-L). URL: https://www.gov.uk/government/publications/ukukraine-digital-trade-agreement-cs-ukraine-no22023
[41] Digital Economy Partnership Agreement (Article 4.3). URL: https://www.mti.gov.sg/Trade/Digital-Economy-Agreements/The-Digital-Economy-Partnership-Agreement
[42] Digital trade agreements between the United Kingdom of Great Britain and Northern Ireland and Ukraine (Article 132-K). URL: https://www.gov.uk/government/publications/ukukraine-digital-trade-agreement-cs-ukraine-no22023
[43] Yakovleva S., Hoboken Joris V. J. The Algorithmic Learning Deficit: Artificial Intelligence, Data Protection, and Trade. Big Data and Global Trade Law, ed. by Mira Burri, Cambridge University Press, Forthcoming, Amsterdam Law School. Research Paper. 2020. №2022–55. 19 p.
[44] Palka P. Data Management Law for the 2020s: The Lost Origins and the New Needs. *Buffalo Law Review*. 2020. P. 559–640.
[45] Castro D., Chivot E. Europe to have the best AI? Reform the GDPR. IAPP. URL: https://iapp.org/news/a/want-europe-to-have-the-best-ai-reform-the-gdpr/
[46] Eline Chivot. Is the EU's AI Policy Headed in the Right Direction? Evaluating EU AI White paper. Data Innovation webinar. 2020. URL: https://datainnovation.org/2020/07/is-the-eus-ai-policy-headed-in-the-right-direction/

REFERENCES

[1] Aaronson, S. A. (2018). Data Minefield: How AI is Prodding Governments to Rethink Trade in Data. *Working paper*, 10.
[2] UNCTAD. (2019). Value Creation and Capture: Implications for Developing Countries. *Digital Economy Report*. Retrieved from https://unctad.org/en/PublicationsLibrary/der2019_en.pdf
[3] Regulation (EU) 2016/679 General Data Protection Regulation in the current version of the OJ L 119, (2016, May). Retrieved from https://gdpr-info.eu/
[4] Mitchell, A. D, & Mishra, N. (2021). WTO Law and Cross-Border Data Flows An Unfinished Agenda. *Big Data and Global Trade Law. Cambridge University Press*, 83–112.
[5] Burri, M. (2023). The Impact of Digitalization on Global Trade Law. *German Law Journal*, 24(3), 551–573.
[6] Drezner, D. W. (2009). *All politics is global: Explaining international regulatory regimes*. Princeton University Press.
[7] Shaffer, G. (2000). Globalization and social protection: the impact of EU and international rules in the ratcheting up of US privacy standards. *Yale J. Int'l L.*, 25, 1.
[8] Farrell, H., & Newman, A. L. (2019). Of privacy and power: The transatlantic struggle over freedom and security. *Princeton University Press*, 27–28.
[9] Mercurio, B., & Yu, R. (2023). *Regulating Cross-Border Data Flows: Issues, Challenges and Impact*. Anthem Press. Retrieved from https://doi.org/10.1007/s40319-023-01298-8
[10] Naef, T. (2023). *Data Protection Without Data Protectionism: The Right to Protection of Personal Data and Data Transfers in EU Law and International Trade Law*. Springer Nature.
[11] Chaisse, J. (2023). 'The Black Pit:' Power and Pitfalls of Digital FDI and Cross-Border Data Flows. *World Trade Review*, 22(1), 73–89.

[12] Brännström, L. (2023). Global Inequality and the EU International Law Position on Cross-Border Data Flows. *Nordic Journal of International Law*, 92(1), 119–137.
[13] Miadzvetskaya, Yu. (2023). Data Governance Act: On International Transfers of Non-Personal Data and GDPR Mimesis. *European Data Protection Law Review,* 9(1), 13–26.
[14] Kuner, C. (2023). Protecting EU Data Outside EU Borders under the GDPR. *Common Market Law Review*, 60 (1), 77–106.
[15] Yakovleva, S. (2020). Privacy Protection(ism): The Latest Wave of Trade Constraints on Regulatory Autonomy. *University of Miami Law Review*, 74 (2), 473–481.
[16] Chander, A. (2020). Is Data Localization a Solution for Schrems II? *Journal of International Economic Law*, 23(3), 771–784.
[17] Cory, N. (2021). How 'Schrems II' Has Accelerated Europe's Slide Toward a De Facto Data Localization Regime. *ITIF*. Retrieved from https://itif.org/publications/2021/07/08/how-schrems-ii-has-accelerated-europesslide-toward-de-facto-data
[18] Yakovleva, S. (2022). Three Data Realms: Convergence or Competition. Amsterdam Law School Research Paper № 2022–58. Retrieved from http://dx.doi.org/10.2139/ssrn.4028668
[19] Chang, Q., Cong, L. W., Wang, L., & Zhang, L. (2023). *Production, Trade, and Cross-Border Data Flows* (No. w31416). National Bureau of Economic Research. Retrieved from https://doi.org/10.3386/w31416
[20] Kulhari, S. (2023). Bryan Mercurio and Ronald Yu: Regulating Cross-Border Data Flows – Issues, Challenges and Impact. *IIC*, 54, 487–490.
[21] Pandey, S., Chaudhary, G., & Kaushal Mahan, V. P. (2023). Digital Public Infrastructure for Efficient Cross-Border Data Flow, 20.
[22] Du, X., & Liu, A. (2023). Security and Openness China's Cross-Border Data Flow Scheme. *Pacific International Journal*, 6(1), 138–141. Retrieved from https://doi.org/10.55014/pij.v6i1.326
[23] Zhang, C. (2023). RCEP Basic Security Exceptions for Cross-Border Data Flows and China's Response. *Journal of Education, Humanities and Social Sciences*, 14, 36–45. Retrieved from https://doi.org/10.54097/ehss.v14i.8793
[24] Hu, T. (2023, September). Research on Legal Issues of Cross Border Flow of Financial Data from the Perspective of Economic Globalization. In 2023 9th International Conference on Humanities and Social Science Research (ICHSSR 2023) (pp. 1840–1844). Atlantis Press. Retrieved from https://doi.org/10.2991/978-2-38476-092-3_236
[25] Vrublevska-Misyuna, K., & Tychyna, V. (2022). International legal standards of personal information protection. *Scientific Bulletin of the Uzhhorod National University. Series: Law*, 2(74), 149–154. https://doi.org/10.24144/2307–3322.2022.74.58
[26] Fedosenko, N. A., & Spitsyna, G. O. (2023). Actual issues of international legal regulation of protection of personal data of employees. *Analytical and comparative jurisprudence*, (2), 204–208. https://doi.org/10.24144/2788–6018.2023.02.34
[27] Legka, O. V. (2021). Actual issues of personal data protection: domestic and international experience. *Legal position*, 2 (31), 74–79. https://doi.org/10.32836/2521–6473.2021–2.15
[28] OECD (2011). The Evolving Privacy Landscape: 30 Years After OECD Privacy Guidelines», *OECD Digital Economy Papers*, Publishing, Paris. Retrieved from https://doi.org/10.1787/5kgf09z90c31-en
[29] OECD (2002). OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, OECD Publishing, Paris. Retrieved from https://doi.org/10.1787/9789264196391-en.
[30] Propp, K. (2023). Gentlemen's Rules for Reading Each Other's Mail: The New OECD Principles on Government Access to Personal Data Held by Private Sector Entities.

Lawfare. Retrieved from https://www.lawfaremedia.org/article/gentlemens-rules-reading-each-others-mail-new-oecd-principles-government-access-personal-data-held
[31] Declaration on Government Access to Personal Data Held by Private Sector Entities. Retrieved from https://legalinstruments.oecd.org/en/instruments/OECD–L
[32] OECD. (2022). *Fostering cross-border data flows with trust. OECD Digital Economy Papers,* 343. Paris: OECD Publishing. Retrieved from https://doi.org/10.1787/139b32ad-en
[33] OECD. (2023). *Moving forward on data free flow with trust: New evidence and analysis of business experiences. OECD Digital Economy Papers*, 353. Paris: OECD Publishing. Retrieved from https://doi.org/10.1787/1afab147-en
[34] APEC. (2005). CTI Sub-Fora & Industry Dialogues Groups, Digital Economy Steering Group. *APEC Privacy Framework*, 36. Retrieved from https://www.apec.org/publications/2005/12/apec-privacy-framework
[35] Adequacy decisions. How the EU determines if a non-EU country has an adequate level of data protection. Retrieved from https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en#:~:text=The%20European%20Commission%20has%20so,commercial%20organisations%20participating%20in%20the
[36] Art. 45 GDPR. Transfers on the basis of an adequacy decision: Regulation (EU) 2016/679 General Data Protection Regulation in the current version of the OJ L 119. (2016, May). Retrieved from https://gdpr-info.eu/art-45-gdpr/
[37] Article 8.81 of EU-Japan Economic Partnership Agreement (JEFTA). (2020, February). Retrieved from https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/japan/eu-japan-agreement_en
[38] European Commission adopts adequacy decision on Japan, creating the world's largest area of safe data flows. (2019, January). Retrieved from https://ec.europa.eu/commission/presscorner/detail/en/IP_19_421
[39] Burri, M. (2023). Cross-border data flows and privacy in global trade law: has trade trumped data protection? *Oxford Review of Economic Policy*, 39(1), 85–97.
[40] UK/Ukraine: Digital Trade Agreement [CS Ukraine №2/2023] (Article 132-L). (May 2023). Retrieved from https://www.gov.uk/government/publications/ukukraine-digital-trade-agreement-cs-ukraine-no22023
[41] Digital Economy Partnership Agreement (Article 4.3). (2020, June). Retrieved from https://www.mti.gov.sg/Trade/Digital-Economy-Agreements/The-Digital-Economy-Partnership-Agreement
[42] Digital trade agreement between the United Kingdom of Great Britain and Northern Ireland and Ukraine ARTICLE 132-K. (2023, May) Retrieved from https://www.gov.uk/government/publications/ukukraine-digital-trade-agreement-cs-ukraine-no22023
[43] Yakovleva, S., & Hoboken, J. (2020). The Algorithmic Learning Deficit: Artificial Intelligence, Data Protection, and Trade. *Big Data and Global Trade Law, ed. by Mira Burri, Cambridge University Press, Forthcoming*.
[44] Palka, P. (2020). Data management law for the 2020s: the lost origins and the new needs. *Buffalo Law Review*, 68, 559–640.
[45] Castro, D., & Chivot, E. (2019). Want Europe to have the best AI? Reform the GDPR. *IAPP*. Retrieved from https://iapp.org/news/a/want-europe-to-have-the-best-ai-reform-the-gdpr/
[46] Chivot, E. (2020). Is the EU's AI Policy Headed in the Right Direction? Evaluating EU AI White paper. *Data Innovation webinar*. Retrieved from https://datainnovation.org/2020/07/is-the-eus-ai-policy-headed-in-the-right-direction/

Владислав Ігорович Камишанський
Здобувач вищої освіти ступеня доктор філософії з права
Молодший науковий співробітник відділу проблем модернізації
господарського права та законодавства
Держана установа «Інститут економіко-правових досліджень
імені В. К. Мамутова Національної академії наук України»
01032, бульвар Тараса Шевченка, 60, м. Київ, Україна

Vladyslav I. Kamyshanskyi
Academic Degree, Title
PhD student,
Junior Research Fellow at the Department of Modernisation
of Economic Law and Legislation
State Organization «V. Mamutov Institute of Economic and Legal
Research of National Academy of Sciences of Ukraine»
01032, 60 Taras Shevchenko Blvd, Kyiv, Ukraine

Рекомендоване цитування: Камишанський В. І. Транскордонна передача даних у контексті цифрової трансформації зовнішньоекономічної політики. *Вісник Національної академії правових наук України*. 2023. Том. 30 № 4. С. 304–324.

Suggested Citation: Kamyshanskyi, V. I. (2023). Cross-Border Data Transfer in the Context of Digital Transformation of Foreign Economic Policy. *Journal of the National Academyof Legal Sciences of Ukraine,* 30(4), 304–324.

Стаття надійшла / Submitted: 19/10/2023
Доопрацьовано / Revised: 20/11/2023
Схвалено до друку / Accepted: 22/12/2023