РОЗДІЛ 11
МІЖНАРОДНЕ ПРАВО

УДК 340.13
DOI https://doi.org/10.32782/2524-0374/2024-2/121

ПРАВОВЕ РЕГУЛЮВАННЯ ТРАНСКОРДОННОЇ ПЕРЕДАЧІ ПЕРСОНАЛЬНИХ ДАНИХ У КИТАЙСЬКІЙ НАРОДНІЙ РЕСПУБЛІЦІ: СУЧАСНИЙ СТАН, ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ

LEGAL REGULATION OF CROSS-BORDER TRANSFER OF PERSONAL DATA IN THE PEOPLE'S REPUBLIC OF CHINA: CURRENT STATUS, PROBLEMS AND PERSPECTIVES

Дрогін Є.Р., студент магістратури
Навчально-науковий інститут права Київського національного університету імені Тараса Шевченка

Статтю присвячено комплексному аналізу правового регулювання транскордонної передачі персональних даних у Китайській Народній Республіці (далі – КНР), а саме аналізу ключових документів у даній сфері: Закон КНР "Про захист персональних даних" (PIPL), Заходи оцінки безпеки передачі даних за кордон, Стандартні договірні положення щодо передачі персональних даних за кордон та інші.

Актуальність дослідження обумовлена динамічними змінами у законодавстві КНР у сфері транскордонної передачі персональних даних. В останні роки КНР значно посилила контроль за циркуляцією персональних даних через кордони, вводячи нові правила та обмеження, що створює виклики для міжнародного бізнесу та міждержавної співпраці.

В статті ідентифіковано ключові виклики та проблеми, які виникають у процесі транскордонної передачі даних, а саме відсутність єдності у правовому регулюванні транскордонної передачі персональних даних, що ускладнює взаємодію КНР з іншими країнами, високі вимоги до безпеки та захисту даних, що можуть обмежувати інноваційний розвиток даної сфери та міжнародну співпрацю тощо.

Особливу увагу було приділено аналізу Проєкту положень про стандартизацію та сприяння транскордонним потоком даних, що потенційно має посприяти послабленню поточних механізмів регулювання транскордонної передачі персональних даних задля стимулювання інноваційного розвитку у даній сфері та налагодження міжнародних відносин.

Ключові слова: персональні дані, транскордонна передача персональних даних, оцінка безпеки, сертифікація захисту, стандартні договірні положення, PIPL.

The article is devoted to a comprehensive analysis of the legal regulation of cross-border transfer of personal data in the People's Republic of China (hereinafter – the PRC), namely, the analysis of key documents in this area: The Personal Data Protection Law of the People's Republic of China (PIPL), the Measures for Assessing the Security of Data Transfers Abroad, the Standard Contractual Clauses for Personal Data Transfers Abroad, and others.

The relevance of the study is due to the dynamic changes in the PRC's legislation in the field of cross-border transfer of personal data. In recent years, the PRC has significantly tightened control over the circulation of personal data across borders by introducing new rules and restrictions, which creates challenges for international business and interstate cooperation.

The article identifies the key challenges and problems arising in the process of cross-border data transfer, namely, the lack of uniformity in the legal regulation of cross-border transfer of personal data, which complicates China's interaction with other countries, high requirements for data security and protection, which may limit the innovative development of this area and international cooperation, etc.

Particular attention was paid to the analysis of the Draft Regulations on Standardization and Facilitation of Cross-border Data Flows, which could potentially contribute to the weakening of current mechanisms for regulating cross-border transfer of personal data in order to stimulate innovative development in this area and establish international relations.

Key words: personal data, cross-border transfer of personal data, security assessment, security certification, standard contractual clauses, PIPL.

В еру глобалізації та стрімкого розвитку цифрових технологій, проблематика транскордонної передачі персональних даних набуває особливої ваги. Передусім це пов'язано з необхідністю забезпечення високого рівня захисту прав і свобод індивідів у контексті обробки та передачі їхніх персональних даних, а також з потребою врахування інтересів держави у сфері національної безпеки та економічного розвитку. КНР, як одна з провідних світових економік з активно розвиваючимся цифровим сектором, стикається з особливими викликами у цій сфері.

Однією з ключових проблем є відсутність досконалої теоретичної бази, яка б деталізувала питання пов'язані з регулюванням передачі персональних даних через кордон, що призводить до відсутності інтегрованого регуляторного підходу. Ця ситуація ускладнює процес знаходження оптимального балансу між забезпеченням безпеки даних та розвитком даної сфери.

Проблеми координації та визначення чітких меж між безпекою та розвитком підкреслюють критичну потребу в застосуванні більш наукового та систематизованого підходу до формування регуляторної стратегії. Переважний акцент на аспекти безпеки, межі якої безперервно розширюються, створює перешкоди для гармонізації національного законодавства з міжнародними правовими нормами та стандартами. Також це спричиняє зростання вимог до дотримання внутрішніх правил, що, в свою чергу, призводить до стримування розвитку відповідного сектору [1].

Закон КНР «Про захист персональних даних» (далі – PIPL), Закон КНР «Про кібербезпеку» (далі – CSL) та Закон «Про безпеку даних» (далі – DSL) утворюють основу Законів КНР, які регулюють питання пов'язані з даними, в тому числі персональними даними [1]. Ці нормативно-правові акти встановлюють комплексний регуляторний фреймворк, спрямований на забезпечення захисту та безпеки персональних даних і інших важливих даних у цифровому просторі. Вони регламентують широкий спектр питань, починаючи від збору та обробки персональних даних до їх транскордонної передачі, вимагаючи від організацій проведення оцінок безпеки та впровадження відповідних заходів захисту.

Але важливо підкреслити, що у положеннях PIPL, CSL та DSL немає конкретного визначення поняття «транскордонна передача персональних даних». Однак відповідь на

це питання можна знайти в таких документах, як Заходи оцінки безпеки передачі даних за кордон, Стандартні договірні положення щодо передачі персональних даних за кордон, Інструкції з оцінки безпеки передачі даних та декларування (перше видання) [2].

Відповідно до Заходів оцінки безпеки передачі даних за кордон транскордонна передача даних визначається як передача персональних даних та інших важливих даних, зібраних і згенерованих у процесі діяльності (ході операцій) на території КНР, установам, організаціям і фізичним особам, які знаходяться за межами країни (поза межами національного суверенітету) [3].

У Інструкції з оцінки безпеки передачі даних та декларування (перше видання) перераховані деякі конкретні обставини, які вважаються транскордонною передачею даних, а саме:

– коли оператор даних передає або зберігає за кордоном дані, які зібрані або згенеровані під час його роботи на території КНР;

– коли дані, зібрані та згенеровані оператором даних, зберігаються на території КНР для запиту, пошуку, завантаження та передачі закордонними установами, організаціями або фізичними особами;

– будь-які інші дії, пов'язані з даними, що підлягають передачі за кордон, передбачені Адміністрацією кіберпростору Китаю (далі – АКК) [4].

У Стандартних договірних положеннях щодо передачі персональних даних за кордон також окреслені конкретні обставини, які вважаються транскордонною передачею персональних даних, а саме:

– коли оператори персональних даних передають і зберігають персональні дані, зібрані та згенеровані під час внутрішніх операцій за кордоном;

– коли персональні дані, зібрані та згенеровані операторами персональних даних, зберігаються в КНР, але установи, організації чи фізичні особи, які знаходяться за кордоном можуть запитувати, отримувати, завантажувати та передавати персональні дані;

– інші дії з передачі персональних даних за кордон, визначені АКК [5].

Отже, виходячи з наведених вище визначень, можна зазначити, що транскордонна передача даних охоплює як безпосереднє переміщення персональних та інших важливих даних за межі національного суверенітету, так і віддалений доступ до таких даних, що зберігаються на території КНР, фізичними особами, установми або організаціями, які фізично розташовані за кордоном, тобто, якщо сторона даних відносин, знаходиться за кордоном та отримує віддалений доступ до персональних даних або важливих даних фізичної особи, яка знаходиться в КНР – така діяльність також буде вважатися транскордонною передачею персональних даних, навіть якщо ці дані неактивно передаються до місця, яке знаходиться за межами КНР.

Окремо хотілося би відмінити наявність пункту «інші дії з передачі персональних даних за кордон, визначені АКК», що відображає певну гнучкість у трактуванні та можливість адаптуватися до швидко змінюваних технологічних та глобальних умов, однак це також створює певну невизначеність для суб'єктів, що здійснюють транскордонну передачу даних, оскільки «відкриті» визначення можуть призводити до різних інтерпретацій та потребувати постійного моніторингу та адаптації до нових регуляторних вимог.

Особливу увагу слід приділити аналізу положень PIPL, оскільки даний нормативний акт займає ключове місце в нормативно-правовій базі КНР, що регламентує обробку та транскордонну передачу персональних даних. Цей акт встановлює комплексні вимоги до збору, використання, зберігання та передачі персональних даних, надаючи особливу увагу механізмам забезпечення конфіденційності та захисту даних при їх транскордонній передачі.

Глава 3 PIPL детально визначає правила транскордонної передачі персональних даних та обов'язки операторів персональних даних при транскордонній передачі персональних даних. Вона класифікує цей процес на три основні типи сценаріїв: перший пов'язаний з бізнес-потребами операторів, другий випливає з вимог міжнародних договорів та угод, до яких приєдналася КНР, і третій включає запити від іноземних судових або правоохоронних органів. Кожен з цих сценаріїв підпорядковується відповідним регуляторним правилам, які закріплюють різні підходи транскордонної передачі персональних даних [6].

В рамках аналізу правового регулювання транскордонної передачі персональних даних в КНР, ключове місце займають механізми оцінки безпеки, укладення договорів з наявними стандратними договірними положеннями та сертифікація захисту даних, які розглядаються як взаємодоповнюючі елементи, що теоретично мають створювати цілісну систему для безпечної транскордонної передачі персональних даних. Вони призначені для забезпечення комплексного підходу до зменшення ризиків, пов'язаних з обробкою та передачею даних між різними юрисдикціями, посилення захисту даних та забезпечення відповідальності сторін, що беруть участь у цьому процесі [7].

Проте, аналіз практичної реалізації цих регуляторних інструментів в КНР виявляє істотну «фрагментованість» у їх застосуванні та взаємодії. Ця «фрагментованість» проявляється через відсутність науково обґрунтованої та логічно послідовної структури між ними, що свідчить про недостатню систематизацію системи регулювання передачі даних КНР для адекватного задоволення потреб громадськості та викликів глобалізованого цифрового світу [1].

Відповідно до ст. 38 PIPL операторам даних надається чотири можливих механізми транскордонної передачі персональних даних:

1. Проходження офіційної оцінки безпеки, що проводиться Адміністрацією кіберпростору Китаю (АКК – далі).
2. Сертифікація захисту персональних даних професійною організацією, затвердженої АКК.
3. Укладення договору з наявними стандратними договірними положеннями з іноземним одержувачем даних за формою, встановленою АКК, та подання договору разом із супровідною оцінкою впливу до провінційної АКК.
4. Інші умови, передбачені Законами чи підзаконними актами або АКК.

Якщо міжнародні договори та угоди, які КНР уклала або в яких вона бере участь, містять положення про умови передачі персональних даних за межами території КНР, такі положення можуть бути застосовані.

Оператори персональних даних зобов'язані застосовувати відповідні заходи безпеки для забезпечення відповідності обробки даних, що здійснюється іноземними одержувачами, установленим цим Законом критеріям захисту персональних даних [6].

Відповідно до ст. 39 PIPL якщо оператор персональних даних здійснює передачу персональних даних фізичної особи за межі території КНР, він повинен проінформувати дану фізичну особу про такі питання, як ім'я іноземного одержувача, контактну інформацію, мету та спосіб обробки, тип персональних даних. Крім того, оператор має інформувати фізичну особу про процедури та засоби реалізації її прав у відношенні до даних, що передаються, відповідно до цього Закону, та отримати від неї виражену згоду на таку передачу [6].

Це положення акцентує на необхідності забезпечення прозорості у процесі транскордонної передачі персональних даних та підкреслює важливість інформованої згоди суб'єктів даних. Таким чином, PIPL спрямований на захист права фізичних осіб на приватність, надаючи їм контроль

над власними персональними даними, особливо у контексті міжнародного обміну інформацією.

Відповідно до ст. 40 PIPL оператори критичної інформаційної інфраструктури та оператори персональних даних, чиї обсяги обробки персональних даних перевищують порогові значення, встановлені АКК, зобов'язані зберігати персональні дані, зібрані та згенеровані на території КНР, в межах Китаю. У разі необхідності передачі таких даних іноземним суб'єктам, потрібно пройти оцінку безпеки, організовану АКК. Якщо закони, адміністративні правила або положення АКК передбачають, що оцінка безпеки не є обов'язковою, то такі положення мають переважну силу [6].

Офіційна оцінка безпеки в АКК є найбільш обтяжливим з усіх чотирьох механізмів. Суб'єкт буде зобов'язаний пройти офіційну оцінку безпеки, якщо він:

1) визнаний «Оператором критичної інформаційної інфраструктури»;

2) має намір передавати «Важливі дані»;

3) обробляє персональні дані понад 1 мільйон фізичних осіб; або

4) сукупно передав персональні дані понад 100 000 фізичних осіб або «чутливі персональні дані» понад 10 000 фізичних осіб з 1 січня попереднього року.

Суб'єкти, які не підпадають під вищезазначені критерії, можуть вільно обирати один з представлених механізмів [3].

Важливо підкреслити, що суб'єкти, які мають намір здійснити транскордонну передачу персональних даних та подати заявку на оцінку безпеки, спочатку зобов'язані ініціювати процес самооцінки ризиків передачі за кордон відповідних даних. Дана самооцінка має на меті виявлення потенційних ризиків, які транскордонна передача персональних даних може представляти для національної безпеки КНР, а також для особистих прав фізичних осіб або організацій, від яких ці дані були зібрані. Процедура самооцінки повинна охоплювати такі аспекти як оцінка законності, легітимності та необхідності мети, обсягу та способу транскордонної передачі персональних даних, визначення обсягу та типу даних, що передаються, оцінка ризиків підроблення, знищення, витоку, втрати або незаконної передачі даних, які передаються, перевірка наявності укладених договорів або інших юридично обов'язкових документів, пов'язаних з передачею даних тощо [3].

Для глибшого розуміння вищезазначених критеріїв, необхідно чітко визначити ключові терміни, такі як «оператор критичної інформаційної інфраструктури», «важливі дані» та «чутливі персональні дані».

Відповідно до статті 2 Положення про захист критичної інформаційної інфраструктури до «критичної інформаційної інфраструктури» відносяться державні комунікаційні та інформаційні послуги, енергетика, транспорт, водопостачання, фінанси, державні послуги, електронне урядування, національна оборона, науково-технічна промисловість, інформаційні системи та інші важливі галузі, сфери та мережеві об'єкти, пошкодження, втрата функціональності або витік даних з яких може серйозно загрожувати національній безпеці, стану національної економіки та засобів до існування, а також суспільним інтересам [8].

Відповідно до статті 19 Заходів оцінки безпеки передачі даних за кордон поняття «важливі дані» було визначено в досить широкому розумінні і включає «дані, які у разі несанкціонованого доступу, знищення, витоку чи незаконного використання можуть поставити під загрозу національну безпеку, економічну та соціальну стабільність, громадське здоров'я тощо» [3].

Ми вважаємо, що широке тлумачення поняття «важливі дані» породило деяку невизначеність, що могло мати наслідки для практичного застосування цього поняття. Таке визначення, охоплене великим діапазоном інтерпретацій, потенційно ускладнює ідентифікацію даних, що належать до цього типу, та вимагає додаткового уточнення з боку регуляторних органів для забезпечення юридичної ясності та уникнення юридичної невизначеності у їх обробці та передачі.

Згідно із статтею 28 PIPL «чутливі персональні дані» – це персональні дані, витік або незаконне використання яких може легко призвести до порушення особистої гідності фізичних осіб або заподіяння шкоди особистій чи майновій безпеці, зокрема біометричні дані, релігійні переконання, конкретні дані про особу, стан здоров'я, фінансові рахунки та місцезнаходження, а також персональні дані про неповнолітніх віком до 14 років.

Оператори персональних даних можуть обробляти чутливі персональні дані лише тоді, коли вони мають конкретну мету та достатню необхідність, а також вживають суворих заходів захисту [6].

Аналіз механізму оцінки безпеки, який застосовуються в КНР, свідчить про комплексний підхід держави до регулювання ризиків, пов'язаних з транскордонною передачею даних. У контексті цього підходу особливу увагу привертає відсутність суворого розмежування між різними типами даних у процесі їхньої оцінки безпеки. Регуляторна практика КНР передбачає універсальну оцінку даних з позицій потенційних ризиків для безпеки, які вони можуть представляти при передачі за кордон. Така уніфікована система оцінки безпеки даних виходить з припущення, що будь-які дані, незалежно від їх типу, можуть нести в собі ризики, які необхідно ідентифікувати та мінімізувати до моменту їх передачі за межі країни [1].

Якщо говорити про сертифікацію захисту персональних даних – вона має на меті довести, що збір, зберігання, використання, обробка, передача, надання, розкриття, видалення, в тому числі транскордонна передача та обробка персональних даних операторами персональних даних в межах сфери сертифікації відповідають вимогам стандартів, що лежать в основі сертифікації [9].

Для транснаціональних компаній, які здійснюють транскордонну передачу персональних даних між власними дочірніми або афілійованими компаніями, розташованими в іншій країні, місцева сторона може подати заявку на сертифікацію та взяти на себе юридичну відповідальність від імені обох сторін [2]. Оператори персональних даних, які знаходяться за кордоном, як визначено в PIPL, також можуть подавати заявки на сертифікацію через свої спеціалізовані агентства або призначених представників, які перебувають в КНР, і вони також можуть брати на себе юридичну відповідальність від їх імені [6].

Але при цьому PIPL містить імперативну норму, яка закріплює, що оператори персональних даних, які здійснюють за межами території КНР діяльність, пов'язану з персональними даними фізичних осіб у КНР, зобов'язані сформувати спеціалізоване агенство або призначити представника на території КНР, відповідального за вирішення питань, пов'язаних із обробкою та захистом персональних даних, та повідомити назву відповідного органу або ім'я та контактні дані представника [6].

Найменш обтяжливий шлях до отримання дозволу на проведення транскордонної передачі персональних даних є укладення договору з наявними стандартними положеннями, оскільки він не вимагає проведення аудиту ані АКК, ані акредитованою третьою стороною. Однак компанії, які йдуть цим шляхом, повинні будуть провести оцінку впливу на захист персональних даних (далі – PIPIA) [5].

Через спрощену процедуру даний механізм застосовується лише до відносно невеликих операторів даних і компаній, які не обробляють та передають дані, що становлять загрозу національній безпеці.

Відповідно до Стандартних договірних положень щодо передачі персональних даних за кордон, PIPIA має оцінити наступні питання:

1. Законність, легітимність та необхідність мети, обсягу та методу обробки даних оператором даних [в КНР] та іноземнимиодержувачами.

2. Масштаб, обсяг, тип і рівень чутливості персональних даних, які передаються, а також потенційні ризики, які передача персональних даних може становити для прав та інтересів суб'єктів персональних даних.

3. Відповідальність та зобов'язання, які бере на себе іноземний одержувач, а також те, чи можуть управлінські та технічні заходи і можливості, які залучаються для виконання цих обов'язків та зобов'язань забезпечити безпеку персональних даних, які передаються.

4. Ризик підробки, знищення, витоку, втрати або незаконного використання персональних даних після їх передачі, а також безперешкодність каналів захисту прав та інтересів суб'єктів персональних даних.

5. Вплив, який можуть мати на виконання договору з наявними стандартними положенням політика та правила захисту персональних даних в країні або регіоні, де знаходиться іноземний одержувач [5].

Механізми дотримання вимог PIPL представляють обмежувальний підхід до управління даними і нагадують механізми Загального регламенту про захист даних (GDPR) ЄС. Останній передбачає подібні механізми оцінки ризиків та впливу і дозволяє передачу даних за межі Європейської економічної зони (ЄЕЗ) лише за умови, що ці місця забезпечують належний рівень захисту персональних даних на законодавчому рівні [10].

З метою забезпечення національної безпеки та подальшої стандартизації і сприяння впорядкованому та вільному потоку даних відповідно до закону АКК розробила Проєкт положень про стандартизацію та сприяння транскордонним потокам даних [11].

Згідно з даним Проєктом положень, оператор даних буде звільнений від застосування будь-якого з механізмів транскордонної передачі персональних даних за наступних обставин:

1. *Відсутність передачі персональних даних або важливих даних.* У Проєкті положень зазначено, що якщо під час міжнародної торгівлі, наукового співробітництва або маркетингової діяльності не відбувається передача персональних даних або важливих даних – жоден з механізмів транскордонної передачі персональних даних не буде задіяний. Зокрема, оператору даних потрібно буде подати заявку на оцінку безпеки АКК, якщо галузевий або місцевий регулятор поінформував даного оператора даних про те, що ці дані дійсно кваліфікуються як важливі дані, або якщо ці дані підпадають під будь-який з переліків важливих даних або персональних даних, опублікованих китайськими регуляторними органами [12].

Цей виняток вирішує ключову проблему для транснаціональних компаній. Згідно з чинним законодавством, оператор даних несе відповідальність за визначення того, чи належить його інформація до категорії важливих даних [6], проте існує дуже обмежена кількість інструкцій щодо того, як робити таку кваліфікацію. Відповідно до Проєкту положень оператори даних зможуть виходити з презумпції, що вони не передають важливі дані, тобто вони не повинні подавати заявку на оцінку безпеки для передачі цих даних за межі КНР, якщо вони не були поінформовані регуляторними органами або не була публічна оприлюднена інформація про те, що певні типи даних, які вони обробляють або передають, були класифіковані як важливі дані.

2. *Передача персональних даних, зібраних або згенерованих за межами КНР.* Якщо дані, що передаються за межі КНР, не були спочатку зібрані або згенеровані в КНР – така передача даних не підпадає під дію жодного з механізмів транскордонної передачі персональних даних [12].

3. *Дані необхідні для укладення або виконання договору.* Оператор даних звільняється від дії механізмів транскордонної передачі персональних даних, якщо запропонована передача персональних даних необхідна для укладення або виконання договору, стороною якого є відповідний оператор даних. Приклади, наведені в Проєкті положень, включають, без обмежень, транскордонну електронну комерцію, транскордонні платежі, бронювання авіаквитків та готелів, а також подання візових заявок [12].

Цей виняток буде позитивно сприйнятий такими компаніями, як інтернет-магазини, туристичні агенції, провайдери послуг бронювання та фінансові установи, яким регулярно доводиться переміщувати дані по всьому світу для виконання своїх договірних зобов'язань.

4. *Дані необхідні для управління людськими ресурсами.* Передача персональних даних працівників, необхідна для здійснення управління персоналом, якщо така передача здійснюється відповідно до трудової політики компанії або колективного трудового договору, не підпадає під дію механізмів транскордонної передачі персональних даних.

Однак обсяг цього винятку все ще залежить від того, наскільки широко АКК тлумачить, що саме є «необхідним». Згідно зі статтею 8 Проєкту положень, передача чутливих персональних даних все ще підпадає під вимоги відповідних нормативно-правових актів або відомчих правил, що, схоже, вказує на те, що передача чутливих персональних даних працівників (наприклад, банківських рахунків або інформації про стан здоров'я) може не підпадати під це виключення [12].

5. *Дані необхідні для захисту життєво важливих інтересів.* Передача персональних даних, необхідних для захисту здоров'я та «майнової безпеки» фізичної особи в надзвичайних ситуаціях, не підпадає під дію жодного з механізмів транскордонної передачі персональних даних.

Проєкт положень значно збільшує поріг для оцінки безпеки АКК – зі 100 000 до одного мільйона осіб. Проєкт також змінює попередній підхід, який передбачав зосередження уваги на «кумулятивному» обсязі персональних даних, які були передані з КНР з 1 січня попереднього року, на «очікуваний» обсяг персональних даних, які будуть передані з КНР протягом календарного року. Однак у Проєкті положень нічого не сказано про те, що станеться, якщо компанія перевищить очікуваний обсяг за певний рік, або як слід робити початкові розрахунки.

Згідно з цими новими розрахунками, якщо компанія передасть персональні дані понад одного мільйона осіб – буде ініційована оцінка безпеки АКК. Якщо обсяг даних, які компанія планує передати з КНР протягом року, становить від 10 000 до одного мільйона осіб, вона повинна укласти договір з наявними стандартними положеннями або пройти сертифікацію захисту, але не проходити оцінку безпеки АКК. З іншого боку, компанія не зобов'язана використовувати жоден з механізмів транскордонної передачі персональних даних, якщо вона планує передавати персональні дані менше ніж 10 000 осіб протягом року [12].

Отже, у сучасному світі, де глобалізація та цифрова економіка стають все більш домінуючими факторами розвитку, питання транскордонної передачі персональних даних набуває особливої актуальності. Це стосується не лише економічного аспекту, але й правового регулювання та захисту особистої інформації фізичних осіб. КНР стоїть перед викликом адаптації свого правового поля до швидкозмінних умов цифрового світу. Враховуючи значну кількість міжнародних компаній, що працюють у КНР, а також китайських компаній, які виходять на зовнішні ринки, правове регулювання транскордонної передачі персональних даних стає критично важливим елементом налагодження міжнародних відносин. Але водночас КНР належить до країн, які мають найбільш обмежувальні режими захисту персональних даних у світі, що у свою чергу може призводити до певного стримування інноваційного розвитку даної сфери та міжнародного співробітництва. Незважаючи на існуючі виклики поточна політика КНР у даній

сфері вказує на формування позитивної динаміки, орієнтованої на послаблення механізмів регулювання транскордонної передачі персональних даних. Ця тенденція спрямована на стимулювання інноваційного розвитку, що, у свою чергу, сприяє підвищенню ефективності та гнучкості відповідних процесів, але при цьому також важливо пам'ятати про необхідність дотримання відповідних стандартів захисту даних.

ЛІТЕРАТУРА

1. Chuanxing Y., Wenguang Y. Current Situation, Problems, and Relief Path of China's Cross-Border Data System[J]. *Journal of Beijing University of Aeronautics and Astronautics Social Sciences Edition*. 2024. Vol. 37(1). P. 57–71. DOI: 10.13766/j.bhsk.1008-2204.2023.2035

2. Zhou Q., Huld A. PIPL 2023/24: Cross-Border Data Transfer in China Handbook: handbook. China: *Dezan Shira & Associates*. 2024. 39 p. URL: https://www.asiabriefing.com/store/book/pipl-cross-border-data-transfer-china-handbook.html?autodownload (date of access: 01.02.2024).

3. 数据出境安全评估办法. 国家互联网信息办公室令. 第11号. 2022年7月7日. URL: https://www.gov.cn/zhengce/zhengceku/2022-07/08/content_5699851.htm (申请日期: 01.02.2024).

4. 数据出境安全评估申报指南. 第一版 国家互联网信息办公室发布. 08月31. URL: http://www.cac.gov.cn/2022-08/31/c_1663568169996202.htm (申请日期: 01.02.2024).

5. 个人信息出境标准合同办法. 国家互联网信息办公室令. 第13号. 2023年2月22. URL: http://www.cac.gov.cn/2023-02/24/c_1678884830036813.htm (申请日期: 01.02.2024).

6. 中华人民共和国个人信息保护法. 2021年8月20日第十三届全国人民代表大会常务委员会第三十次会议通过. URL: https://www.gov.cn/xinwen/2021-08/20/content_5632486.htm (申请日期: 01.02.2024).

7. Liu J., Villanueva J. Navigating Cross-Border Data Transfers: Impacts on Privacy, Big Tech, Rule of Law, and US-China Relations. *JURIST*: website. URL: https://www.jurist.org/commentary/2024/01/us-china-data-transfers/ (date of access: 01.02.2024).

8. 关键信息基础设施安全保护条例. 中华人民共和国国务院令. 第745号. 2021年7月30日. URL: https://www.gov.cn/zhengce/content/2021-08/17/content_5631671.htm (申请日期: 01.02.2024).

9. 个人信息保护认证实施规则. 2022年11月04日. URL: https://www.cac.gov.cn/2022-11/18/c_1670399936983876.htm (申请日期: 01.02.2024).

10. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj (date of access: 01.02.2024).

11. Kennedy G., T. K. Woo J. China proposes easing of cross-border data controls. *Mayer Brown*: website URL: https://www.mayerbrown.com/en/insights/publications/2023/10/china-proposes-easing-of-cross-border-data-controls (date of access: 01.02.2024).

12. 规范和促进数据跨境流动规定（征求意见稿）. 国家互联网信息办公室. 2023年9月28日. URL: http://www.cac.gov.cn/2023-09/28/c_1697558914242877.htm (申请日期: 01.02.2024).