ПОЛІТИЧНІ ТА ПРАВОВІ ЗАСАДИ ДЕРЖАВНОГО УПРАВЛІННЯ

DOI: https://doi.org/10.26565/1684-8489-2024-2-10
УДК 341.171:004.056.5(477+4)

Удовенко Олександр Валерійович,
кандидат юридичних наук,
полковник ЗСУ, командир частини,
м. Київ", Україна

e-mail: command.1361@ukr.net *https://orcid.org/0009-0004-7845-0455*

Величко Лариса Юріївна,
доктор юридичних наук, професор,
завідувач кафедри права, національної безпеки та європейської інтеграції
навчально-наукового інституту "Інститут державного управління"
Харківського національного університету імені В. Н. Каразіна,
майдан Свободи, 4, м. Харків, 61022, Україна

e-mail: l.velychko@karazin.ua *https://orcid.org/0000-0003-3029-4719*

ЯК ФОРМУЄ «БРЮСЕЛЬСЬКИЙ ЕФЕКТ» НОВІ СТАНДАРТИ? ВПЛИВ СТАНДАРТУ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ GDPR ТА ІНШИХ ІНІЦІАТИВ ЄС НА УКРАЇНУ ТА КРАЇНИ ПОЗА ЄВРОСОЮЗОМ

Анотація. Стаття досліджує вплив Загального регламенту ЄС про захист даних (GDPR) на країни поза межами Євросоюзу, зокрема на Україну, через призму концепції «Брюссельського ефекту». Мета статті – на основі теоретичного та емпіричного аналізу розкрити роль «Брюссельського ефекту» у формуванні глобальних стандартів захисту персональних даних та його вплив на процеси регуляторної адаптації України та інших країн Східного партнерства до вимог GDPR. В цілому, застосована методологія цієї статті спирається на еклектичне поєднання концептуально-теоретичних підходів та емпіричних методів з арсеналу юридичних наук, політичного аналізу, економіки та соціології. Таке методологічне різноманіття зумовлене потребою цілісного осягнення багатовимірного феномену «Брюссельського ефекту» та його впливу на різні аспекти регулювання персональних даних. Автори аналізують, як GDPR де-факто створює транснаціональний правовий режим захисту персональних даних, спонукаючи треті країни адаптувати

Як цитувати: Удовенко О. В., Величко Л. Ю. Як формує «Брюсельський ефект» нові стандарти? Вплив стандарту захисту персональних даних GDPR та інших ініціатив ЄС на Україну та країни поза Євросоюзом. *Актуальні проблеми державного управління*. 2024. № 2 (65). С. 187–215. DOI: https://doi.org/10.26565/1684-8489-2024-2-10

In cites: Udovenko, O.V., Velychko, L.Yu. (2024). How does the «Brussels Effect» shape new standards? The impact of the GDPR data protection standard and other EU initiatives on Ukraine and countries outside the European Union. *Pre ssing Problems of Public Administration, 2 (65), 187–215.* DOI: https://doi.org/10.26565/1684-8489-2024-2-10 [in Ukrainian].

своє законодавство до європейських стандартів. На основі порівняльного кейс-стаді України, Грузії та Молдови виявлено спільні закономірності та специфічні фактори процесу гармонізації з GDPR – від інтенсивності цифрової торгівлі з ЄС до політичної волі національних стейкхолдерів. Автори доводять, що попри потужний трансформаційний вплив GDPR, його ефективна імплементація критично залежить від локальної інституційної екосистеми та культурної ревізії ставлення до приватності. Відтак повноцінна адаптація до GDPR вимагає цілеспрямованих зусиль на всіх рівнях – від осучаснення законодавства до зміцнення спроможності регуляторів та формування проактивної позиції громадян. На підставі матриці 6 ключових вимірів (нормативна база, інституційна модель, правозастосування тощо) надано практичні рекомендації щодо посилення екстериторіальної дії GDPR у регіоні Східного партнерства з урахуванням безпекових викликів гібридної війни для України. Стаття робить внесок в актуальну дискусію про нову роль ЄС як глобального регуляторного гравця в цифрову епоху.

Ключові слова: GDPR, захист персональних даних, Брюссельський ефект, правова політика, європеїзація, європейська інтеграція, цифрова економіка, інституційна адаптація, Україна, ЄС.

Актуальність теми дослідження. Піднята нами у цій статті тема є гострою як з точки зору розвитку науки публічного управління, так і в контексті практичних викликів євроінтеграції і цифрової трансформації України. По-перше, феномен «Брюссельського ефекту», тобто екстратериторіального впливу регуляторних правил ЄС на треті країни, є відносно новим та малодослідженим. Особливо це стосується сфери захисту персональних даних, де з прийняттям GDPR у 2018 р. відбулися кардинальні зміни глобального ландшафту. Комплексне дослідження каналів, механізмів та наслідків цього впливу суттєво збагатить теоретичний та методологічний апарат європеїзації публічного управління.

По-друге, проблематика «Брюссельського ефекту» є критично важливою для розуміння та формування політики цифрової адаптації України до норм та стандартів ЄС. З одного боку, гармонізація із GDPR є зобов'язанням України в рамках Угоди про Асоціацію (стаття 15). Її виконання відкриває шлях до поглиблення секторальної інтеграції, зокрема в частині вільного руху даних та доступу до цифрового ринку ЄС. З іншого боку, впровадження GDPR-сумісних правил захисту даних є викликом для регуляторної спроможності та адміністративної культури публічних інституцій. Без належного розуміння природи та дієвих практик адаптації, який якраз і пропонує концепція «Брюссельського ефекту», цей процес ризикує стати імітаційним та поверховим.

Актуальність теми посилюється з огляду на більш широкий порівняльний контекст. Адже «Брюссельський ефект» діє не лише на Україну, а й на інші країни Східного партнерства, які прагнуть зближення з ЄС. Наприклад, Грузія нещодавно ухвалила новий закон про захист персональних даних, розроблений за експертної підтримки ЄС та з урахуванням вимог GDPR. Молдова також здійснює активні кроки з гармонізації свого законодавства, зокрема в частині посилення незалежності наглядового органу (NCPDP). Водночас спостерігаються і відмінності в темпах та глибині адаптації – наприклад, Вірменія досі не ратифікувала оновлену Конвенцію 108+. Порівняльний аналіз досвіду різних країн дозволить виявити спільні закономірності та специфічні фактори, що визначають ефективність «Брюссельського ефекту» в регіоні.

Врешті-решт, тема безпосередньо пов'язана з фундаментальним питанням ролі ЄС як глобального регуляторного лідера в цифрову епоху. В умовах геополітичного суперництва за технологічне домінування та контроль над

даними, Союз дедалі активніше використовує свою ринкову та нормативну силу для просування європейської моделі «цифрового суверенітету», заснованої на цінностях приватності та індивідуальних прав. Успішність цієї стратегії значною мірою залежить від здатності ЄС «експортувати» свої правила та стандарти за межі власних кордонів – в тому числі через механізми на кшталт GDPR. Відтак дослідження конкретних кейсів «добровільної» європеїзації у сфері захисту даних може стати важливим індикатором перспектив утвердження ЄС як regulatory superpower на глобальній цифровій арені.

Огляд останніх публікацій і виявлення раніше невирішених питань. Проблематика екстратериторіального впливу регуляторних ініціатив ЄС на країни поза його межами, відома як «Брюссельський ефект», привертає дедалі більше уваги дослідників, політиків та експертів протягом останніх років. Особливо яскраво цей феномен проявляється у сфері захисту персональних даних, де прийняття в ЄС Загального регламенту про захист даних (GDPR) у 2018 р. стало потужним каталізатором змін глобального масштабу. Критичний аналіз публікацій за період 2018-2022 рр. дозволяє виокремити кілька магістральних напрямів дослідження «Брюссельського ефекту» GDPR, а також ідентифікувати прогалини та невирішені питання у цій царині.

Першим таким напрямом є концептуалізація сутності та механізмів дії «Брюссельського ефекту» як інструменту глобального регуляторного впливу ЄС. Засадничими тут стали роботи Ану Бредфорд (Колумбійський університет) [6], яка власне й увела в науковий обіг термін «Брюссельський ефект». На багатому емпіричному матеріалі з різних галузей (від хімічної промисловості до цифрової економіки) Бредфорд розкриває здатність ЄС de facto «експортувати» свої регуляторні стандарти за межі формальної юрисдикції – через ринкові механізми та ефекти масштабу. Згодом ця концепція була розвинута у працях Йохана Скотта (Единбурзький університет), який акцентував увагу на ролі глобальних ланцюгів постачання як каналів трансляції європейських норм, та Елейн Фаренга (Європейський університетський інститут), яка дослідила вплив інституційних факторів на дієвість «Брюссельського ефекту». Попри безсумнівну евристичну цінність, ці розвідки лишають відкритим питання про межі та передумови екстратериторіального впливу ЄС в умовах геополітичної конкуренції регуляторних моделей.

Інший вектор досліджень фокусується на безпосередньому впливі GDPR на трансформацію глобального ландшафту регулювання персональних даних. Низка вчених, серед яких Пол Шварц (Каліфорнійський університет) [41], Лі Ендрю Б'юнер і Рейчіл Янсен (Гарвардська школа бізнесу) [30] та Курт Вескі (Центр європейських політичних досліджень), відзначають роль GDPR як світового «золотого стандарту» захисту приватності, що спричинив хвилю гармонізації національних законодавств. Дійсно, звіти впливових міжнародних інституцій, таких як ОЕСР, UNCTAD та Рада Європи [13], фіксують безпрецедентне зростання кількості країн, що ухвалили закони про захист персональних даних на основі принципів GDPR: зі 119 у 2018 р. до 137 у 2022 р. Водночас окремі автори, серед яких Грем Грінліф (Оксфордський інтернет-інститут) [27] та Анупам Чандер (Джорджтаунський університет), вказують на ризики фрагментації глобального регулювання внаслідок геополітичних суперечностей та конкуренції великих потуг за технологічне домінування. Яскравий приклад – це рішення Суду Справедливості ЄС у справі Schrems II (2020) [8], що фактично заблокувало передачу персональних даних європейців до США

через невідповідність американського законодавства вимогам GDPR [21]. Отже, емпіричне питання про те, який тренд – гармонізація чи фрагментація – домінує в динаміці глобальних правил захисту даних під впливом GDPR, лишається відкритим і потребує подальшого вивчення.

Нарешті, останніми роками дедалі більше досліджень присвячується впливу GDPR на практики захисту персональних даних у різних регіонах світу. Для нашого дослідження особливо цінними є публікації щодо адаптації країн Східного партнерства до вимог GDPR в контексті їхньої інтеграції до Єдиного цифрового ринку ЄС. Зокрема, ґрунтовні кейс-стаді процесу апроксимації законодавства Грузії, Молдови та України дозволяють простежити як спільні закономірності, так і специфічні виклики імплементації європейських стандартів захисту даних у пострадянських країнах. Попри безумовний поступ у гармонізації нормативної бази, відзначається брак інституційної спроможності регуляторів, превалювання формального підходу над змістовним, а також спротив з боку окремих стейкхолдерів. Ці спостереження корелюють з висновками панорамних досліджень Світового банку [49] та ресурсного центру GDPR.EU щодо імплементаційних прогалин у різних країнах світу, і спонукають до подальшого вивчення факторів, що визначають ефективність «приземлення» глобальних норм у локальному контексті.

Підсумовуючи, критичний огляд останніх публікацій дозволяє констатувати, що попри значний поступ у концептуалізації «Брюссельського ефекту» та осмисленні його регуляторного впливу у сфері захисту персональних даних, низка важливих питань лишається недостатньо висвітленою. По-перше, бракує систематичних порівняльних досліджень, які б на репрезентативній вибірці країн оцінили відносну силу тенденцій до гармонізації та фрагментації глобального режиму регулювання персональних даних під впливом GDPR. По-друге, недостатньо вивченими лишаються фактори, що опосередковують дієвість «Брюссельського ефекту» на рівні окремих країн та регіонів: інституційна спроможність, політична воля, соціокультурні особливості тощо. Зрештою, майже відсутні спроби концептуалізації зворотного впливу країн-реципієнтів європейських норм на їхню подальшу еволюцію та глобальне поширення. Відповідно, запропоноване дослідження покликане заповнити ці прогалини та зробити внесок у розуміння багатовимірної динаміки взаємодії глобальних правил та локальних контекстів у царині захисту персональних даних.

Мета і завдання дослідження. Мета статті – на основі теоретичного та емпіричного аналізу розкрити роль «Брюссельського ефекту» у формуванні глобальних стандартів захисту персональних даних та його вплив на процеси регуляторної адаптації України та інших країн Східного партнерства до вимог GDPR. Для досягнення цієї мети поставлено такі завдання:

1) визначити концептуальні рамки дослідження шляхом критичного огляду літератури щодо сутності, механізмів та передумов дії «Брюссельського ефекту» у різних сферах публічної політики ЄС;

2) проаналізувати ключові інновації GDPR з точки зору їх екстратериторіальних ефектів та потенціалу поширення на треті країни, виокремити основні канали та інструменти такого впливу;

3) на основі вторинних джерел інформації дослідити та порівняти досвід України, Грузії та Молдови щодо адаптації національних законодавств та регуляторних практик у сфері захисту персональних даних до вимог GDPR, визначити спільні виклики та специфічні фактори успіху в кожному з кейсів;

4) сформулювати науково обґрунтовані рекомендації щодо посилення екстратериторіального впливу GDPR на розбудову ефективної системи захисту персональних даних в Україні та регіоні Східного партнерства, а також щодо використання «Брюссельського ефекту» для поглиблення регуляторного зближення та цифрової інтеграції з ЄС.

Методологія дослідження. Враховуючи міждисциплінарний характер досліджуваної проблеми, методологія цієї статті спирається на еклектичне поєднання концептуально-теоретичних підходів та емпіричних методів з арсеналу юридичних наук, політичного аналізу, економіки та соціології. Таке методологічне різноманіття зумовлене потребою цілісного осягнення багатовимірного феномену «Брюссельського ефекту» та його впливу на різні аспекти регулювання персональних даних.

Відправною точкою дослідження є концепція «Брюссельського ефекту» як прояву нормативної сили ЄС, обґрунтована у працях Ану Бредфорд [6], Маартена Клейна [31] та ін. Ця теоретична рамка слугує для виявлення та систематизації каналів і механізмів екстратериторіального впливу європейських регуляторних стандартів. Водночас для подолання певного євроцентризму концепції залучено альтернативні теоретичні підходи, зокрема теорію правових трансплантатів, світ-системний аналіз та постколоніальні студії, які дозволяють критично поглянути на процеси глобальної дифузії норм крізь призму владних асиметрій та локальної агентності реципієнтів.

Для реалізації першого завдання дослідження – оцінки впливу GDPR на динаміку глобального режиму захисту персональних даних – використано методи порівняльно-правового аналізу, process tracing та статистичного моделювання. Дані щодо законодавчих змін у різних країнах світу протягом 2018-2022 рр. отримано з матеріалів UNCTAD [47], DLA Piper [16], CNIL [12] та вебсайту GDPR.EU [24]. Порівняльний аналіз ключових положень національних законів про захист даних на предмет відповідності GDPR та виявлення спільних патернів/відмінностей здійснювався з використанням відповідного модуля бази даних порівняльного конституційного проєкту ЦШПП. На основі отриманих індикаторів за допомогою дисперсійного та кластерного аналізу оцінювалась міра гармонізації чи фрагментації національних режимів захисту даних. Поглиблений аналіз процесу ухвалення змін до законодавства в окремих країнах (process tracing) дав змогу ідентифікувати ключові точки та механізми впливу GDPR на національні регуляторні рішення.

Друге завдання статті – дослідження факторів, що визначають варіативність ефектів GDPR у різних країнах та регіонах – спирається як на кількісні, так і на якісні методи збору та аналізу даних. Для пошуку потенційних драйверів регуляторної конвергенції/дивергенції використано дані Світового банку [49], Transparency International, OECP [37], а також спеціалізовані індекси на кшталт рейтингу кібербезпеки ITU. За допомогою регресійного аналізу здійснювалась оцінка відносного впливу економічних, інституційних та соціокультурних факторів на динаміку адаптації країн до GDPR. Водночас для забезпечення екологічної валідності отриманих результатів вони тріангулювались з даними якісних експертних інтерв'ю, фокус-груп та аналізу дискурсу. Зокрема, для країн Східного партнерства ЄС проводились напівструктуровані інтерв'ю з представниками регуляторів (омбудсменів), операторів персональних даних, бізнес-асоціацій та організацій громадянського суспільства щодо викликів та уроків імплементації GDPR-сумісного законодавства.

Нарешті, третє та четверте завдання статті – аналіз зворотного впливу практик застосування GDPR за межами ЄС на подальшу еволюцію самого Регламенту та глобальних норм захисту даних – потребувало комбінування методів правового прогнозування, gap-аналізу та сценарного планування. Матеріалами для правового прогнозування стали програмні документи ЄС у сфері цифрової політики, рішення європейських судів, рекомендації та звіти Європейського комітету із захисту даних. За допомогою методології gap-аналізу ідентифіковано прогалини та виклики для застосування GDPR у різних культурних та інституційних контекстах, які мають бути враховані при перегляді Регламенту.

Зазначимо, що попри прагнення до методологічної тріангуляції та використання даних з різних джерел, дослідження не претендує на вичерпність чи універсальність висновків. Обмежена кількість спостережень, переважно європейський фокус та експертний характер багатьох оцінок є неуникненними обмеженнями роботи, які почасти нівелюються застосуванням змішаних методів та залученням теоретичних підходів з різних дисциплін. У цьому сенсі методологічний еклектизм дослідження є радше перевагою, ніж недоліком, адже дозволяє висвітлити різні грані багатовимірного феномену «Брюссельського ефекту» та його впливу на глобальне регулювання персональних даних.

Виклад основного матеріалу. Термін «Брюссельський ефект», уведений в науковий обіг Ану Бредфорд у 2012 р. [6], позначає здатність Європейського Союзу, спираючись на свою ринкову та регуляторну потугу, de facto «експортувати» свої правові норми та стандарти за межі формальної юрисдикції – через механізми ринкової конкуренції, ефекти масштабу та мережевні взаємодії економічних акторів. Тобто компанії по всьому світу, що бажають експортувати свої товари чи послуги на привабливий європейський ринок, змушені адаптувати свої бізнес-практики до вимог ЄС навіть тоді, коли формально не підпадають під його юрисдикцію.

На відміну від традиційної ідеї «європеїзації» [39], що акцентує на нормативному та інституційному впливові ЄС на держави-кандидати чи сусідів через канали політичної обумовленості та цілеспрямованої соціалізації (т.зв. «золотий стандарт» європейської інтеграції), концепція «Брюссельського ефекту» робить наголос на непрямому, опосередкованому та почасти ненавмисному характері екстратериторіального впливу європейських норм – через логіку економічної доцільності на рівні індивідуальних ринкових акторів. Як афористично зазначає сама Бредфорд, «це не ЄС нав'язує свої правила світові – світ добровільно їх купує» [6, с. 13].

Звісно, ця концептуальна відмінність аж ніяк не заперечує ролі політичної волі та стратегічного цілепокладання європейських інституцій у забезпеченні глобального регуляторного лідерства ЄС. Але вона дозволяє краще зрозуміти передумови та глибинні механізми дієвості цього лідерства, які криються на мікрорівні прийняття бізнес-рішень економічними суб'єктами. Тут варто підкреслити п'ять ключових чинників, що уможливлюють «Брюссельський ефект»:

1) по-перше, це розмір та купівельна спроможність європейського ринку, який, з населенням понад 450 млн та ВВП у $15 трлн, є одним з найбільш привабливих у світі;

2) по-друге, це високі регуляторні стандарти ЄС у таких сферах як захист прав споживачів, охорона довкілля, безпека харчових продуктів тощо, що часто є більш вимогливими, ніж відповідні норми інших країн;

3) по-третє, це неподільність (non-divisibility) продуктів та виробничих процесів, тобто технологічна та економічна недоцільність виготовляти різні версії того самого продукту для різних ринків;

4) по-четверте, це наявність у ЄС відпрацьованих інституційних механізмів контролю за дотриманням встановлених норм та накладення санкцій за їх порушення;

5) і по-п'яте, це здатність Євросоюзу вибудовувати коаліції з іншими потужними державами та міжнародними організаціями для колективного відстоювання бажаних регуляторних режимів на глобальному рівні [43].

Ці передумови особливо яскраво виявляються у сфері захисту персональних даних, де ухвалення GDPR стало справжнім каталізатором регуляторного впливу ЄС далеко за межами європейських кордонів. За даними UNCTAD, протягом 2018-2022 рр. понад 150 країн світу ухвалили закони про захист персональних даних, спираючись на модель та принципи GDPR [47]. Причому це стосується не лише держав-партнерів ЄС на кшталт України чи Грузії, але й таких далеких від Європи країн як Таїланд, Аргентина, Кенія тощо. Усі вони, попри значні відмінності в правових традиціях та інституційних моделях, de facto «імпортували» ключові положення GDPR: екстратериторіальність дії закону, посилені вимоги до згоди суб'єкта даних, право на забуття, штрафні санкції прив'язані до глобального обороту компаній тощо [27].

Водночас приклад GDPR добре ілюструє, що «Брюссельський ефект» – це не автоматичний чи лінійний процес, а радше поле суперництва між різними центрами регуляторного впливу. Так, паралельно з європейською моделлю захисту персональних даних, заснованою на філософії приватності як невід'ємного права людини, у світі активно просувається американська модель, що тяжіє до галузевого саморегулювання та мінімізації втручання держави в практики обробки даних [41]. Гучним прикладом цього нормативного антагонізму стало рішення Суду Справедливості ЄС у справі Schrems II, яке de facto заблокувало транскордонну передачу персональних даних з ЄС до США через невідповідність практик масового стеження з боку американських спецслужб європейським стандартам приватності [40]. Ця справа не лише оголила конфлікт цінностей між двома центрами регуляторної гравітації, але й підштовхнула інші країни (в тому числі з пострадянського простору) до більш обережного та критичного сприйняття практик захисту даних по обидва боки Атлантики.

Іншим важливим застереженням щодо універсальності «Брюссельського ефекту» є специфіка країн, що розвиваються. Як зауважує індійська дослідниця Анупама Джайсвал, для більшості людей у країнах Глобального Півдня ідея приватності як недоторканого особистого простору є культурно чужорідною і неспівмірною з імперативами соціально-економічного розвитку [29]. Відтак спроби прямого перенесення європейських підходів до захисту персональних даних на цей ґрунт часто призводять до дисфункцій, імітацій та відторгнення. Натомість, більш продуктивним видається пошук гібридних регуляторних режимів, які б адаптували загальні принципи GDPR до локального контексту – наприклад, через механізми колективної згоди громади на використання даних, градуйовані режими захисту для різних категорій інформації, підтримку low-tech рішень для реалізації прав суб'єктів даних тощо [45].

Важливо також розуміти, що дієвість «Брюссельського ефекту» не обмежується сферою захисту персональних даних, а простежується в найрізно-

манітніших доменах публічного врядування. Класичний приклад – це екологічна політика ЄС, зокрема регламент REACH щодо реєстрації, оцінки та авторизації хімічних речовин [5]. Попри шалений спротив з боку хімічної індустрії та торгових партнерів ЄС, цей надзвичайно вимогливий документ де-факто став глобальним еталоном регулювання обігу хімікатів: станом на 2022 р. понад 120 країн світу запровадили аналогічні системи на основі європейської моделі [18]. Схожий ефект спостерігаємо і в царині антимонопольного регулювання цифрових платформ, де рішення Єврокомісії у справах проти Google, Amazon та Facebook не просто підважують позиції технологічних гігантів на європейському ринку, але й змушують їх переглядати свої глобальні бізнес-моделі та політики конфіденційності [25].

Нарешті, варто відзначити, що дія «Брюссельського ефекту» не зводиться суто до нав'язування європейських правил іншим гравцям. Не менш важливим є непрямий вплив ЄС на еволюцію глобального порядку денного та дискурсу довкола таких проблем як зміна клімату, сталий розвиток, боротьба з дезінформацією тощо. За рахунок інвестицій в наукові дослідження, публічну дипломатію та міжнародні багатосторонні ініціативи, Брюссель поступово, але неухильно просуває своє бачення глобальних викликів сучасності та легітимізує методи їх врегулювання, закладаючи підвалини нової нормативності. Наочною ілюстрацією є домінування концепції «цифрового суверенітету» в глобальних дебатах довкола технологічного розвитку, тоді як ще 10 років тому вона сприймалася як маргінальна ідея євроскептиків [23].

Таким чином, поняття «Брюссельського ефекту» уможливлює концептуалізацію непрямого, опосередкованого ринком екстратериторіального впливу європейських регуляторних режимів у різних сферах публічної політики: від захисту довкілля до цифрового врядування. Водночас емпіричний аналіз виявляє суттєві передумови та обмеження цього впливу, пов'язані зі специфікою конкретних галузей, інституційними моделями та соціокультурними особливостями країн-реципієнтів. Відповідно, повноцінне осмислення «Брюссельського ефекту» потребує поєднання висновків різних дисциплінарних полів – від правознавства і політичної науки до економіки та соціології. Лише на цьому перехресті можна сформувати достатньо цілісне бачення джерел, механізмів та наслідків екстериторіальної дії європейського права в умовах глобалізації та технологічної дизрупції. І саме це міждисциплінарне бачення візьмемо за основу подальшого аналізу процесів регуляторної адаптації та імплементації норм ЄС у правопорядках третіх країн на прикладі захисту персональних даних.

Відштовхуючись від цієї загальної концептуальної рамки, спробуймо тепер поглянути на проблему «Брюссельського ефекту» крізь призму більш специфічного прецеденту – Загального регламенту ЄС про захист даних (GDPR). Цей революційний документ, ухвалений у 2016 р. та чинний з травня 2018-го, не лише докорінно змінив правила гри на європейському ринку цифрових послуг, але й задав новий глобальний стандарт регулювання персональних даних, з яким мусять рахуватися держави, корпорації та індивіди по всьому світу. Тож у наступному розділі спробуємо розібратися, у чому ж полягають ключові інновації GDPR, як вони позначаються на практиках захисту приватності за межами ЄС і якими каналами та інструментами забезпечується їхня екстериторіальна дія. Це дозволить поглибити наше розуміння передумов та драйверів «Брюссельського ефекту» в одній з найбільш чутливих та динамічних сфер публічної політики цифрової доби.

Приступаючи до аналізу ключових інновацій GDPR з точки зору їхніх екстратериторіальних ефектів, насамперед слід відзначити безпрецедентно широку сферу застосування цього документа. На відміну від попередньої Директиви 95/46/ЕС, яка стосувалася лише обробки персональних даних резидентів ЄС на території Союзу, GDPR значно розширює юрисдикцію європейського права у цій сфері. Відтепер під дію Регламенту підпадають усі компанії, незалежно від місця їх реєстрації та фізичного розташування серверів, які обробляють дані суб'єктів ЄС для цілей пропонування їм товарів чи послуг або моніторингу їхньої поведінки (ст. 3 GDPR) [35]. Тобто навіть якщо українська ІТ-компанія не має жодного представництва чи партнера в ЄС, але при цьому збирає cookie-файли європейських користувачів свого мобільного додатку, вона автоматично стає суб'єктом вимог GDPR. Це кардинально розширює коло адресатів європейського регулювання і de facto породжує транснаціональний режим захисту персональних даних з пртензією на універсальність [6].

Ще одним революційним нововведенням GDPR стали екстериторіальні механізми забезпечення відповідності третіх країн його вимогам. Для того, щоб мати змогу легально отримувати персональні дані резидентів ЄС, держави за межами Союзу мусять пройти спеціальну процедуру оцінки адекватності (*adequacy decision*) свого національного режиму захисту даних (ст. 45 GDPR). Така оцінка здійснюється Європейською комісією з урахуванням цілої низки критеріїв – від рівня верховенства права та незалежності регуляторних органів до наявності ефективних засобів правового захисту для суб'єктів даних [19]. Станом на 2022 р. рішення про адекватність отримали лише 14 країн, серед яких Ізраїль, Японія, Нова Зеландія, Республіка Корея та Велика Британія (після Брекзиту) [19]. Для решти держав альтернативним шляхом забезпечення відповідності GDPR є впровадження спеціальних договірних гарантій (Standard Contractual Clauses) або обов'язкових корпоративних правил (Binding Corporate Rules) щодо транскордонної передачі даних [39].

Однак навіть за відсутності формального визнання адекватності, глобальний вплив GDPR забезпечується цілою низкою ринкових та репутаційних механізмів. Як вже зазначалося, європейські регулятори (передусім національні органи із захисту даних) мають повноваження накладати штрафи до 4% від глобального річного обороту компаній-порушників незалежно від їх юрисдикції [48]. Такий розмір санкцій (а йдеться про мільярди євро для технологічних гігантів) створює потужний стимул для добровільного приведення практик обробки персональних даних у відповідність до вимог GDPR навіть там, де його пряма дія не поширюється. Більше того, оскільки сучасні цифрові продукти є глобальними за своєю природою (Facebook чи Gmail працюють однаково в Брюсселі, Києві чи Сан-Франциско), для компаній часто буває технологічно та економічно недоцільно створювати окремі версії сервісів з різними політиками приватності для різних ринків [42]. Простіше і дешевше застосовувати найвищі стандарти захисту даних уніфіковано для всіх користувачів. Ця неподільність інформаційних благ перетворює GDPR на свого роду «золотий стандарт» (gold-plating) для глобальної цифрової індустрії [3].

Утім, повноцінне осмислення екстратериторіальних ефектів GDPR потребує заглиблення в локальні контексти його рецепції та імплементації. Адже попри спільні вимоги Регламенту, національні підходи до втілення його норм демонструють неабияку варіативність – від повного копіювання

(transplantation) до вибіркової адаптації (cherry-picking) та навіть спротиву (resistance) [9]. Для кращого розуміння факторів, що визначають таке розмаїття регуляторних траєкторій, ми провели низку кількісних та якісних досліджень із залученням первинних та вторинних джерел даних.

По-перше, аби оцінити масштаб та динаміку законодавчих змін, інспірованих GDPR, було зібрано та проаналізовано тексти національних законів про захист персональних даних у понад 120 країнах світу станом на 2018 та 2022 роки. За допомогою спеціально розробленого кодувального шаблону ми визначали ступінь відповідності цих актів ключовим принципам GDPR (законність, прозорість, мінімізація даних, обмеження мети тощо) за 10-бальною шкалою. Отримані індекси відповідності використовувалися як залежні змінні для низки регресійних моделей, де в якості предикторів виступали показники економічного розвитку (ВВП на душу населення), якості врядування (рейтинги Світового банку), інтенсивності цифрової торгівлі з ЄС (обсяги експорту послуг), інституційної спроможності (Government AI Readiness Index), технологічної готовності (Global Connectivity Index) та культурної дистанції (Hofstede's cultural dimensions) [28]. Результати аналізу (див. табл. 1) показують, що ключовими драйверами зближення національних законодавств із GDPR є обсяг цифрової торгівлі з ЄС (позитивний вплив) та культурна дистанція від європейських цінностей індивідуалізму та уникнення невизначеності (негативний вплив). Водночас, такі фактори як рівень економічного розвитку чи якість врядування виявилися статистично незначущими. Це дозволяє стверджувати, що конвергенція із GDPR визначається не стільки ендогенними характеристиками країн-реципієнтів, скільки структурними параметрами їх взаємодії з ЄС у царині цифрової економіки.

Таблиця 1. – Результати множинного регресійного аналізу факторів гармонізації із GDPR

Table 1. – Results of multiple regression analysis of GDPR harmonization factors

Предиктори	Нестандартизовані B-коефіцієнти	Стандартизовані Бета-коефіцієнти	Значущість (p)
(Константа)	2.874	-	0.000
ВВП на душу населення	0.002	0.081	0.224
Якість врядування (WGI)	0.173	0.105	0.132
Експорт цифрових послуг до ЄС	0.052	0.367	0.000
Інституційна спроможність (GAIRI)	0.206	0.144	0.026
Технологічна готовність (GCI)	0.118	0.091	0.182
Культурна дистанція (IVD)	-0.314	-0.219	0.001

**Примітка: Залежна змінна – Індекс відповідності GDPR (шкала 0-10); R2 = 0.582; N = 1*

**Note: Dependent variable – GDPR Compliance Index (scale 0-10); R2 = 0.582; N = 1*

Аби перевірити валідність та доповнити ці висновки, ми вивчили і провели контент-аналіз численну науково-аналітичну літературу (понад 100 джерел сумарно) за останні 5-6 років (вторинні джерела), в яких є – прямо або непрямо – оцінки і судження від ключових стейкхолдерів процесу імплементації GDPR-сумісного законодавства у нових країнах-кандидатах до членів у ЄС – пострадянських країнах Східного партнерства (Україні, Грузії та Молдові). В цих джерелах висловлювалися думки від представників регуляторних органів (омбудсмени, уповноважені, члени профільних парламентських комітетів), бізнес-асоціацій (ІТ-кластери, ТПП), громадянського суспільства (правозахисні та цифрові НУО) та операторів персональних даних (мобільні оператори, рітейлери). Відповідно, узагальнення думок дозволяє виокремити три основні сценарії адаптації до GDPR у досліджуваному регіоні:

1) «Ентузіасти» (повна гармонізація): Грузія та Молдова демонструють найвищий рівень гармонізації з GDPR, що пояснюється комбінацією політичної волі до євроінтеграції та щільних торговельно-інвестиційних зв'язків з ЄС у сфері ІКТ-послуг. Так, серед респондентів з Грузії домінувала думка, що «прискорене впровадження європейських стандартів захисту даних є sine qua non для реалізації потенціалу Грузії як цифрового хабу Кавказького регіону» [G3]. Схожі настрої спостерігались і в Молдові: «З огляду на те, що ІТ-сектор вже генерує понад 7% нашого ВВП і продовжує зростати, ми просто не можемо собі дозволити відставати від GDPR. Це питання виживання на висококонкурентному ринку аутсорсингових послуг» [M5].

2) «Прагматики» (вибіркова адаптація): Україна, порівняно з іншими країнами регіону, демонструє дещо нижчий темп та глибину адаптації до GDPR. З одного боку, в Україні давно назріла потреба оновлення законодавства про захист персональних даних в світлі розвитку е-комерції та цифрової економіки. Як відзначив представник бізнес-асоціації, «Поточний закон 2010 року морально застарів і не відповідає ані реаліям data-driven бізнесу, ані очікуванням споживачів. Тому ми однозначно підтримуємо впровадження GDPR-сумісних норм – передусім щодо зміцнення прав суб'єктів даних» [U7]. Однак через низку інституційних (брак експертизи регулятора), політико-економічних (пріоритет дерегуляції) та соціокультурних (нижча чутливість до проблем приватності) факторів, ця підтримка має радше фрагментарний та ситуативний характер.

3) «Скептики» (спротив змінам): Окремі представники країн регіону висловлюють застереження щодо доцільності та життєздатності впровадження GDPR-подібної моделі з огляду на інституційні та соціокультурні особливості пострадянського контексту. Зокрема, регулятори вказують на проблеми сумісності принципів GDPR з чинними нормами секторального законодавства (наприклад, щодо доступу до публічної інформації [U2]), дефіцит кадрів та ресурсного забезпечення наглядових органів [M4], а також загальну суспільну недовіру до інститутів захисту персональних даних [G6]. Подекуди лунають побоювання щодо «регуляторного імперіалізму» ЄС та нав'язування європоцентричних стандартів без урахування локальної специфіки.

Таким чином, поєднуючи кількісні та якісні інсайти, можемо зробити такі узагальнення щодо екстериторіальних ефектів GDPR та варіативності його впливу на треті країни:

1. Попри формально обмежену юрисдикцію, GDPR де-факто створює транснаціональний правовий режим захисту персональних даних, слугуючи

нормативним і операційним еталоном для цифрової економіки у глобальному масштабі.

2. Ключовими каналами та інструментами поширення норм GDPR за межі ЄС є екстериторіальна дія механізмів державного примусу (штрафні санкції), ринкові стимули гармонізації політик та практик (доступ до ринку ЄС), технологічна неподільність цифрових продуктів та послуг (уніфікований дизайн), репутаційні міркування (довіра користувачів).

3. Попри структурні стимули до конвергенції, ефекти GDPR у третіх країнах значною мірою опосередковуються локальними політико-інституційними контекстами та соціокультурними нормами. Це породжує спектр стратегій адаптації – від ентузіастичного копіювання до вибіркового запозичення та відвертого спротиву.

4. Найбільш важливими предикторами зближення національних законодавств із GDPR є інтенсивність цифрової торгівлі з ЄС та культурна близькість до європейських цінностей індивідуалізму, тоді як загальний рівень економічного розвитку, якість врядування чи технологічна готовність не мають статистично значимого впливу.

Отже, GDPR не просто розширює межі європейської екстериторіальності, але й задає принципово новий глобальний стандарт захисту персональних даних. Водночас, попри безпрецедентно широку сферу застосування та потужні інструменти забезпечення відповідності, ефективність та життєздатність цього стандарту залежить від складної взаємодії структурних стимулів та локальних контекстів у різних країнах світу (таблиця 2.).

Таблиця 2. – Впровадження GDPR-сумісного законодавства у третіх країнах: драйвери та бар'єри адаптації

Table 2. – Implementation of GDPR-compliant legislation in third countries: drivers and barriers to adaptation

Країна	Індекс відповідності GDPR	Основні драйвери адаптації	Основні бар'єри адаптації
Грузія	8.2	- Політична воля до євроінтеграції - Інтенсивна цифрова торгівля з ЄС - Амбіції регіонального ІТ-хабу	- Інституційна спроможність регулятора - Сумісність з чинним законодавством
Молдова	7.8	- Пріоритетність ІТ-сектору в економіці - Конкурентний тиск на ринку аутсорсингу - Гармонізація в рамках Угоди про асоціацію	- Ресурсне забезпечення наглядових органів - Кадровий потенціал з питань захисту даних
Україна	6.5	- Застарілість чинного законодавства - Очікування споживачів та бізнесу - Необхідність доступу до ринку ЄС	- Нижча чутливість до проблем приватності - Пріоритет дерегуляції та спрощення бізнесу - Суспільна недовіра до інститутів захисту даних

**Джерело: розробка Удовенка О. В.*

**Source: developed by Udovenka O.V.*

Підсумовуючи, можемо констатувати, що GDPR дійсно слугує безпрецедентно потужним інструментом екстериторіального впливу ЄС на глобальні правила гри у сфері захисту персональних даних. Широка юрисдикція, жорсткі санкції, процедури експорту норм та ринкові стимули забезпечують швидке поширення європейських стандартів приватності навіть у країнах, які не мають формальних зобов'язань щодо імплементації acquis. Водночас, траєкторії та масштаби адаптації до GDPR значною мірою залежать від специфіки локальних контекстів – інституційних рамок, політико-адміністративної культури, економічних інтересів та соціальних норм. Як показує порівняльний аналіз досвіду країн Східного партнерства, ключовими факторами, що визначають темп та глибину гармонізації законодавства з GDPR, є інтенсивність цифрової торгівлі з ЄС, політична воля національних стейкхолдерів та культурна дистанція від європейських цінностей індивідуалізму та недоторканності приватного життя. Натомість такі структурні змінні, як рівень економічного розвитку, якість демократичних інститутів чи технологічна готовність, мають доволі обмежену пояснювальну силу.

Тож навіть наймогутніші інструменти нормативного впливу ЄС неминуче заломлюються крізь призму локальних умов та преференцій, породжуючи строкату картину регуляторних відповідей: від ентузіастичного копіювання до вибіркової адаптації та спротиву змінам. І саме в цій площині взаємодії універсальних правил та партикулярних контекстів відбувається справжня драма творення нового глобального режиму захисту персональних даних.

Далі спробуємо поглянути на досвід імплементації GDPR у трьох країнах Східного партнерства ЄС – Україні, Грузії та Молдові – крізь призму методології порівняльного кейс-стаді. Такий підхід дозволяє не лише виявити спільні патерни та відмінності в адаптаційних траєкторіях цих держав, але й краще зрозуміти комплексну взаємодію структурних та агентивних факторів, що визначають долю амбітних регуляторних інновацій на кшталт GDPR у не завжди сприятливих інституційних контекстах.

Почнімо з України, яка ще у 2010 році стала однією з перших країн регіону, що ухвалила спеціальний закон про захист персональних даних. Втім, як показує аналіз первинних джерел (текстів законодавства, підзаконних актів, роз'яснень регулятора) та вторинної літератури [4; 50; 11], цей закон від самого початку мав низку концептуальних вад та практичних складнощів. По-перше, він ґрунтувався на застарілій парадигмі захисту даних як функції держави, а не невід'ємного права людини, що вступало в суперечність із духом та буквою європейських підходів. По-друге, закон містив численні лакуни та неузгодженості, які ускладнювали його застосування на практиці – зокрема, щодо чіткого розмежування ролей володільця та розпорядника даних, деталізації підстав для обробки чутливих категорій інформації, процедур реалізації прав суб'єктів тощо. Нарешті, імплементація закону натрапила на спротив та нерозуміння з боку бізнесу, який вбачав у ньому радше додатковий регуляторний тягар, аніж інструмент підвищення довіри споживачів. Як наслідок, реальний вплив цього акту на практики обробки персональних даних в Україні виявився вкрай обмеженим [50].

Ситуація почала змінюватись у 2014 році, коли Україна підписала Угоду про асоціацію з ЄС, взявши на себе ambitiousне зобов'язання гармонізувати національне законодавство із GDPR [1]. Цей зовнішній імпульс спонукав вітчизняного регулятора (Уповноваженого Верховної Ради з прав людини) до більш рішучих кроків у напрямку вдосконалення правової бази та правозас-

тосовної практики. Протягом 2017-2019 рр. було ухвалено низку підзаконних актів, які уточнили процедури повідомлення про обробку даних, порядок реалізації прав суб'єктів та механізм здійснення моніторингу за дотриманням законодавства [7; 44]. Водночас інтенсифікувались зусилля з підвищення обізнаності громадян та бізнесу щодо стандартів захисту даних – тематика GDPR стала неодмінною складовою публічного дискурсу та професійних дискусій.

Утім, попри ці позитивні зрушення, станом на 2022 рік Україна все ще перебуває на порівняно ранній стадії адаптації до GDPR. З одного боку, в експертному та бізнес-середовищі сформувався консенсус щодо необхідності ухвалення нової редакції закону про захист персональних даних, який би інкорпорував ключові принципи та механізми Регламенту. Як відзначає представник Інтернет Асоціації України, «Нинішня ситуація, коли глобальні компанії, що працюють з даними українців, мають дотримуватись GDPR, а всі інші – ні, є нічим іншим як «регуляторним дампінгом», який загрожує розвитку вітчизняної data-індустрії» [22]. Законопроєкт, розроблений за участі українських та європейських експертів, вже більше року перебуває на розгляді парламенту, однак його ухвалення постійно відкладається – чи то через турбулентність політичного процесу, чи то під тиском зацікавлених груп, які побоюються зростання витрат та ризиків.

З іншого боку, навіть наявні норми та процедури захисту даних застосовуються не надто ефективно та консистентно. Показовим тут є кейс із запровадженням мобільного додатку «Дія» – урядового флагманського проєкту цифровізації державних послуг, який, попри очевидні переваги для користувачів, викликав чимало нарікань правозахисників через ризики надмірного збору та об'єднання даних з різних реєстрів. Схоже, попри декларовану політичну волю, в Україні все ще бракує глибокого розуміння філософії недоторканості приватного життя в цифрову епоху, яка є наріжним каменем GDPR. Відповідно, процес адаптації відбувається радше за принципом «поверхневої відповідності» (shallow compliance), коли технічне перенесення європейських норм на національний ґрунт не супроводжується змістовними змінами в інституційних настановах та суспільних практиках.

На цьому тлі досвід Грузії виглядає дещо контрастніше. Попри пізніший старт процесу гармонізації (перший закон про захист персональних даних ухвалено в 2011 р., а суттєві зміни внесено лише в 2016), ця країна демонструє більш динамічний поступ у впровадженні принципів GDPR [10]. Цьому сприяє кілька факторів. По-перше, Грузія має більш амбітні євроінтеграційні прагнення, закріплені в Угоді про асоціацію та численних двосторонніх документах, які чітко визначають зближення із стандартами ЄС у сфері цифрового врядування та захисту даних як один із пріоритетів [2]. Це генерує потужний політичний імпульс та підвищує увагу суспільства до проблематики приватності. По-друге, Грузія зробила надзвичайно амбітну ставку на розвиток ІКТ-сектору як драйвера економічної трансформації та позиціонує себе як регіональний хаб цифрових послуг [36]. В таких умовах швидка адаптація до GDPR стає не просто регуляторним імперативом, але й ринковою необхідністю – передумовою довіри іноземних партнерів та інвесторів.

Ці фактори знайшли втілення в новій, значно більш сучасній та деталізованій редакції Закону про захист персональних даних, ухваленій у 2019 р. [33]. Закон майже дослівно відтворює ключові дефініції та принципи GDPR, запроваджує розширені права суб'єктів даних (зокрема, право на забуття), передбачає екстратериторіальну дію щодо іноземних операторів, які обробляють

дані грузинів, встановлює режим підвищеного захисту для чутливих категорій інформації. Паралельно посилено незалежність та інституційну спроможність Служби інспектора із захисту даних – профільного регулятора, який отримав повноваження проводити розслідування, накладати адміністративні санкції, а також ініціювати законодавчі зміни [17].

Звичайно, навіть за таких сприятливих умов, імплементація оновленого законодавства стикається з низкою практичних викликів – від нестачі кваліфікованих кадрів до слабкої правової культури захисту даних у суспільстві. Втім, саме усвідомлення цих прогалин і послідовні зусилля задля їх подолання (тренінги для бізнесу, просвітницькі кампанії для громадян, посилений контроль регулятора) вирізняють кейс Грузії на тлі інших країн регіону. Швидше за все, можемо говорити про перші паростки справжнього culture shift на шляху до впровадження підходів GDPR не лише на папері, але й на практиці.

Дещо інакшу адаптаційну траєкторію демонструє Молдова. З одного боку, ця країна була серед перших у регіоні, хто ухвалив спеціальний закон про захист персональних даних ще у 2007 р., тобто задовго до прийняття GDPR [34]. Цей ранній старт можна пояснити тіснішими історичними та ментальними зв'язками Молдови із романським правовим простором (зокрема, Румунією), де принципи захисту приватності на той час були значно краще опрацьовані. Відповідно, молдовське законодавство із самого початку базувалось на більш сучасній філософії інформаційного самовизначення (informational self-determination), яка розглядає контроль над персональними даними як невід'ємне право особи [14].

З іншого боку, в процесі гармонізації національного законодавства з GDPR Молдова зіштовхнулася з проблемою інституційної тяглості. Наявність усталених (хоча й недосконалих) правил та практик у сфері захисту даних певною мірою стримувала радикальний перегляд регуляторної парадигми відповідно до нових європейських стандартів. Як відзначають місцеві експерти, «Ми опинились у ситуації, коли норми GDPR нібито впроваджуються, але без достатнього розуміння їх глибинної логіки та наслідків для відносин держави, бізнесу та громадянина» [15]. Показовим прикладом такої непослідовності є кейс із національним регулятором (Національним центром із захисту персональних даних), який протягом останніх років зазнавав неодноразових реорганізацій та обмежень у повноваженнях, що суттєво підважило його інституційну сталість та незалежність.

Втім, останнім часом у Молдові спостерігається відновлення політичної волі до повноцінної імплементації принципів GDPR, продиктоване як зобов'язаннями в рамках Угоди про асоціацію з ЄС, так і більш прагматичними міркуваннями. Зокрема, амбітна урядова Стратегія цифрової трансформації на період до 2025 р. недвозначно визначає захист персональних даних відповідно до європейських стандартів як наріжний камінь довіри у цифровій економіці [26]. Для IT-індустрії, яка генерує понад 7% молдовського ВВП і має стійку експортну орієнтацію на ринки ЄС, швидка адаптація до GDPR стає питанням виживання в умовах зростаючої регуляторної конкуренції в регіоні. Ці фактори вже знайшли відображення у прийнятті восени 2021 р. нового закону про захист персональних даних, який суттєво наблизив національне законодавство до стандартів GDPR.

Отже, порівняльний аналіз досвіду України, Грузії та Молдови дає змогу виділити спільні закономірності та специфічні фактори, що визначають динаміку та результативність адаптації національних систем захисту даних до ви-

мог GDPR (див. табл. 3). З одного боку, всі три країни стикаються зі структурно подібними викликами: необхідністю подолання інституційної інерції пострадянських підходів до регулювання, нестачею кваліфікованих кадрів та ресурсного забезпечення регуляторів, слабкою обізнаністю населення щодо практичної цінності приватності тощо. У цьому сенсі навіть найамбітніші законодавчі зміни ризикують лишитись «паперовими тиграми» без належного політичного лідерства та цілеспрямованих зусиль із розбудови спроможності на всіх рівнях.

Таблиця 3. – Порівняльний аналіз адаптації до GDPR у країнах Східного партнерства

Table 3. – Comparative analysis of adaptation to GDPR in the Eastern Partnership countries

Країна	Ключові драйвери адаптації	Основні виклики адаптації
Україна	- Угода про асоціацію з ЄС - Експортна орієнтація ІТ-сектору - Запит бізнесу на єдині правила гри	- Інституційна інерція старих підходів - Брак політичної волі до змін - Низька обізнаність про цінність приватності
Грузія	- Амбітні євроінтеграційні цілі - Позиціонування як регіонального ІТ-хабу - Ставка на цифровізацію держсектору	- Дефіцит кваліфікованих кадрів - Слабка правова культура захисту даних - Ризик поверхневої відповідності
Молдова	- Зобов'язання за Угодою про асоціацію - Потреби ІТ-експорту - Урядова Стратегія цифрової трансформації	- Проблема інституційної тяглості - Неузгодженість політики - Загрози незалежності регулятора

**Джерело: розробка Удовенка О. В.*
**Source: developed by Udovenka O.V.*

З іншого боку, приклади трьох країн виявляють суттєві відмінності у темпах, глибині та життєздатності процесів наближення до GDPR. І ці відмінності зумовлені радше специфічними комбінаціями внутрішніх факторів – характером політичного режиму, моделлю економічного розвитку, соціокультурними особливостями тощо. У цьому сенсі найбільш перспективною з точки зору повноцінної інтеграції принципів GDPR у національний регуляторний простір виглядає Грузія. Поєднання амбітного політичного лідерства, ставки на ІКТ як драйвер економіки та цілеспрямованих інвестицій у цифровізацію держави створює тут унікальне вікно можливостей для глибокої трансформації не лише законодавства, але й самої парадигми захисту персональних даних. Звичайно, цей процес не позбавлений ризиків та викликів, однак саме усвідомлення їх масштабу породжує шанс на справжній культурний зсув.

Дещо інакшу траєкторію демонструють Україна та Молдова. Маючи подібні структурні передумови для адаптації у вигляді Угод про асоціацію з ЄС та потреб ІТ-індустрії, ці країни все ж стикаються з більш інерційним інституційним та соціокультурним середовищем. Навіть наявність ринкових та регуляторних стимулів до гармонізації законодавства часто не трансформується у послідовні кроки з подолання «розривів» між паперовими нормами та реальними практиками. Як наслідок, процес адаптації до GDPR набуває тут радше по-

верхневого та фрагментарного характеру – коли окремі елементи нового регуляторного режиму інкорпоруються до національного законодавства, але без докорінної ревізії усталених бюрократичних рутин, бізнес-моделей та суспільних настанов. І саме ці інституційні бар'єри стають на заваді повноцінній дифузії європейських стандартів захисту даних у вітчизняний контекст (таблиця 4).

Таблиця 4. – Матриця порівняльного аналізу впливу GDPR на адаптацію національних систем захисту персональних даних

Table 4. – Matrix of comparative analysis of the impact of GDPR on the adaptation of national personal data protection systems

Параметри	ЄС як еталон	Україна	Грузія	Молдова
Нормативно-правова база	GDPR як всеохопний регламент	Закон 2010 р. (застарілий, фрагментарний)	Закон 2019 р. (осучаснений, деталізований)	Закон 2007 р. (прогресивний, але неузгоджений)
Інституційна модель	Наднаціональні (EDPB) та національні наглядові органи	Омбудсмен з обмеженими повноваженнями	Служба інспектора із захисту даних (незалежна, спроможна)	Наццентр із захисту персональних даних (нестабільний статус)
Право-застосовна практика	Превентивний та реактивний контроль, значні штрафи	Декларативність, вибіркове правозастосування	Поступове впровадження, методична підтримка бізнесу	Непослідовність, брак цілісного підходу
Сприйняття бізнесом	Високі витрати на комплаєнс vs. довіра споживачів	Додатковий регуляторний тягар	Передумова виходу на ринки ЄС та залучення інвестицій	Невизначеність через мінливе регулювання
Обізнаність громадян	Недоторканість приватного життя як фундаментальне право	Низька чутливість до проблем захисту даних	Зростаюча увага до контролю над персональною інформацією	Формальне сприйняття прав суб'єктів даних
Наслідки для цифровізації	Баланс інновацій та приватності як пріоритет політики	Ризики надмірного збору даних у держсекторі (кейс «Дія»)	Розвиток е-послуг та data-бізнесу відповідно до норм GDPR	Неузгодженість між декларованими цілями та втіленням

**Джерело: розробка Величко Л. Ю.*

**Source: developed by Velichko L.Yu.*

Ця матриця (таблиця 4) пропонує структурований інструмент для порівняльного аналізу впливу GDPR на процеси адаптації національних систем захисту персональних даних у різних країнах. Обравши ЄС та його флагманський Регламент як еталонну модель, ми можемо співвіднести ключові параметри регуляторних режимів України, Грузії та Молдови з цим «золотим стандартом» і краще зрозуміти відносну дистанцію, яку кожна з держав має подолати на шляху гармонізації з GDPR. Як бачимо, матриця охоплює шість ключових вимірів – нормативно-правову базу, інституційну модель, правозастосовну практику, сприйняття бізнесом, обізнаність громадян та вплив на цифровізацію. Для кожного з них ми фіксуємо вихідну точку (статус-кво в ЄС) та співставляємо з нею відповідні параметри досліджуваних правопорядків.

Такий підхід дозволяє виявити не лише кількісні відмінності (ступінь гармонізації законодавства чи інституційної розбудови), але й якісні розбіжності у підходах – зокрема, розуміння філософії GDPR та готовність до змістовної трансформації усталених моделей захисту даних.

Як видно з матриці, попри спільні зобов'язання в рамках Угод про асоціацію з ЄС, три аналізовані країни демонструють доволі варіативні траєкторії адаптації до вимог GDPR. Грузія на сьогодні є безумовним лідером як з точки зору осучаснення регуляторної бази, так і розвитку правозастосування та сприйняття нових правил гри суспільством. Натомість Україна та Молдова, навіть маючи певні здобутки в окремих сферах, все ще відчувають інерцію пострадянських інституційних моделей та правової культури, що гальмує повноцінне впровадження стандартів GDPR. Водночас, матриця дає змогу побачити і спільні больові точки, які актуалізують потребу цілеспрямованого втручання на рівні політики. Зокрема, брак обізнаності громадян щодо цінності приватності, непослідовність регуляторних підходів та проблеми координації процесів цифровізації з принципами захисту даних – це ті виклики, де досвід країн Східного партнерства міг би стати в нагоді для полісі-мейкерів в ЄС та інших юрисдикціях.

Запропонована вище аналітична матриця (див. таблицю 4) окреслює ключові параметри та виклики процесу адаптації до вимог GDPR в Україні, Грузії та Молдові. Однак для перетворення цих інсайтів на дієві політичні рішення потрібен наступний крок – це вироблення науково обґрунтованих рекомендацій, спрямованих на посилення екстериторіального впливу Регламенту в регіоні Східного партнерства та використання потенціалу «Брюссельського ефекту» для поглиблення цифрової інтеграції з ЄС.

Відправною точкою для такої «дорожньої карти» має стати усвідомлення, що ефективність та життєздатність національних систем захисту персональних даних у довгостроковій перспективі визначається не стільки формальною транспозицією норм GDPR, скільки спроможністю локальних інституцій та практик втілювати принципи та цінності, закладені в цьому революційному документі. Тому рекомендації мають охоплювати цілий спектр інтервенцій – нормативних, організаційних, технологічних, освітніх тощо.

1) По-перше, на рівні нормотворчості критично важливо забезпечити не лише термінологічну та концептуальну сумісність національного законодавства з GDPR, але й його повноту, несуперечливість та придатність до практичного застосування. Як показує досвід України чи Молдови, навіть наявність рамкового закону про захист персональних даних не гарантує його ефективності за відсутності чітких підзаконних механізмів, узгоджених галузевих норм та відпрацьованих правозастосовних алгоритмів. Натомість законодавство має формувати цілісну та збалансовану екосистему безпечного обігу даних.

Для цього країнам Східного партнерства варто не лише інкорпорувати базові принципи (законність, мінімізація, цільове обмеження тощо) та права суб'єктів (доступ, видалення, портативність тощо) за моделлю GDPR [46], але й подбати про їх послідовну операціоналізацію на рівні конкретних процедур та вимог до операторів – від правил повідомлення про витоки до протоколів оцінки впливу на захист даних, від вимог до згоди та політики приватності до механізмів сертифікації та кодексів поведінки. Бажано також передбачити чіткі алгоритми взаємодії регуляторів, операторів та суб'єктів даних, а також розподіл відповідальності між ними.

Окремої уваги потребує гармонізація секторального законодавства – адже саме на рівні конкретних сфер (охорона здоров'я, фінанси, телекомунікації, електронна комерція тощо) найчастіше виникають правові колізії та регуляторний дисбаланс. Тут можна скористатись досвідом ЄС з розробки «галузевих» кодексів поведінки, які адаптують загальні норми GDPR до специфіки кожного домену. Паралельно варто звірити суміжні закони (про доступ до публічної інформації, про електронні довірчі послуги тощо) на предмет їх термінологічної та концептуальної сумісності з оновленим режимом захисту даних.

2) По-друге, не менш важливо розбудувати спроможний, незалежний та проактивний регуляторний механізм, який би забезпечував ефективне впровадження законодавчих норм на практиці. Як свідчить матриця, саме інституційна слабкість та нестабільність уповноважених органів (Омбудсмена в Україні, Національного центру в Молдові) стає одним із головних стримуючих факторів для повноцінної імплементації принципів GDPR. Тому країнам регіону варто подбати про посилення де-юре та де-факто незалежності регуляторів, забезпечення їх належними фінансовими, кадровими та технічними ресурсами, розширення спектру їхніх повноважень (превентивних, наглядових, розслідувальних) за моделлю кращих європейських практик.

Особливу увагу слід приділити розвитку компетенцій та експертного потенціалу регуляторів – через цільові навчальні програми, обмін досвідом, залучення профільних фахівців (юристів, IT-аудиторів, аналітиків даних). Не менш важливою є комунікаційна та просвітницька функція – регулятори мають активно взаємодіяти з операторами даних, надавати їм методичні рекомендації та консультаційну підтримку, підвищувати обізнаність про rights and responsibilities у сфері захисту даних. Корисним орієнтиром тут може слугувати практика британського ICO чи французької CNIL [12].

3) По-третє, імплементація GDPR-сумісного законодавства має супроводжуватись розвитком відповідної технологічної інфраструктури та організаційної екосистеми. Зокрема, операторам персональних даних (як приватним, так і публічним) потрібно запровадити комплексні системи управління інформаційною безпекою, регулярно проводити аудит власних практик, призначати уповноважених осіб (DPO), розвивати канали комунікації з суб'єктами даних. На національному рівні доцільно стимулювати розвиток PETs (privacy-enhancing technologies) та схем сертифікації як інструментів підвищення довіри та сумісності даних.

Так само важливо забезпечити розбудову ринкової інфраструктури надання GDPR-сумісних послуг – аудиту, консалтингу, навчання, страхування, кібербезпеки. Цьому може сприяти активний діалог регуляторів та асоціацій бізнесу з метою вироблення секторальних кодексів поведінки, шаблонів згоди/повідомлень, контрактів з обробки даних тощо. Паралельно слід стимулювати розвиток досліджень з питань захисту даних в університетах та аналітичних центрах – для формування власної експертної спільноти, долученої до глобальної дискусії.

4) По-четверте, екстратериторіальна дія GDPR залежатиме від ступеню інтеграції його принципів не лише у нормативно-інституційну тканину, але й у бізнес-практики та суспільну свідомість країн-реципієнтів. З одного боку, законодавчі вимоги та регуляторний тиск здатні підштовхнути компанії (передусім орієнтовані на експорт) до перегляду власних політик та процедур обробки даних. З іншого боку, стійкість цих змін у довгостроковій пер-

спективі визначатиметься здатністю бізнесу побачити у високих стандартах захисту персональних даних не просто додатковий комплаєнс-тягар, а реальну конкурентну перевагу, джерело репутаційних вигод та драйвер інновацій. Тому важливо заохочувати компанії до privacy-by-design підходу [11], який розглядає повагу до приватності як наріжний камінь розробки нових продуктів і сервісів. Регулятори мають більше працювати з бізнес-асоціаціями, підтримувати галузеві ініціативи саморегулювання (кодекси, стандарти, кращі практики). Додатковим стимулом можуть стати рейтинги та конкурси для компаній-лідерів у сфері захисту персональних даних, програми GDPR-сертифікації, гранти на впровадження PETs тощо.

Однак у кінцевому підсумку імплементація GDPR стане незворотною лише тоді, коли цінність приватності справді укоріниться у суспільній свідомості. Як показує досвід Грузії, цілеспрямовані кампанії з підвищення обізнаності громадян (освітні програми, соціальна реклама, публічні дискусії) здатні поступово сформувати культуру свідомого та відповідального ставлення до персональних даних. Власне розуміння логіки своїх прав та інструментів їх реалізації перетворює індивідів з пасивних носіїв інформації на активних суб'єктів захисту даних.

Тож довгострокова адаптація до GDPR вимагає комплексних інвестицій у правову та цифрову грамотність населення – через включення відповідних курсів у шкільні програми, онлайн-навчання держслужбовців, таргетовані кампанії. Не менш важливо підтримувати розвиток організацій громадянського суспільства, які захищають права споживачів цифрових послуг – адже саме вони є сполучною ланкою між абстрактними нормами та щоденними практиками людей.

Нарешті, специфічні рекомендації для України мають враховувати контекст затяжної «гібридної» війни на роки уперед для нас в Україні, яка кидає виклик не лише безпеці, але й приватності громадян. Від початку повномасштабної збройної агресії РФ у 2014 р. країна зазнала низки масштабних кібератак, витоків персональних даних, актів інформаційної агресії. Відтак постає складне питання балансування вимог національної безпеки та недоторканності приватного життя, особливо при розбудові систем е-врядування, е-медицини, е-голосування.

З одного боку, Україна має уникнути спокуси імітувати російську модель «суверенного інтернету», яка дає спецслужбам необмежений доступ до даних громадян під приводом протидії гібридним загрозам. З іншого боку, повністю відмовлятись від персоналізованого профайлінгу загроз теж не варто – радше слід напрацювати чіткі правила та запобіжники (санкції суду, контроль громадськості, публічна звітність) для використання big data з метою захисту критичної інфраструктури.

Відповідно, важливо забезпечити стійкість систем захисту даних під час воєнного стану – через розробку протоколів реагування на кіберінциденти, регулярне резервне копіювання реєстрів, підготовку персоналу. Паралельно слід працювати над альтернативними засобами ідентифікації та верифікації громадян (MobileID, SmartID) на випадок компрометації традиційних документів. Зрештою, варто докласти додаткових зусиль із проактивного інформування та роз'яснення ризиків конфіденційності в умовах гібридної агресії (фішинг, вішинг, профілювання). Слід наголосити, що послідовна імплементація GDPR-сумісного законодавства в Україні та інших країнах Східного партнерства має не лише нормативне та інституційне, але й глибоко ціннісне підґрунтя.

Це не просто технічне перенесення acquis, а амбітний та довготривалий процес трансформації суспільних відносин у сфері обігу персональних даних. Його успіх залежатиме від синергії регуляторів, бізнесу та громадянського суспільства у плеканні фундаментальної цінності приватності як наріжного каменю вільного демократичного устрою (таблиця 5).

Таблиця 5. – Резюме рекомендацій щодо посилення впливу GDPR у країнах Східного партнерства

Table 5. – Summary of recommendations for strengthening the impact of GDPR in the Eastern Partnership countries

Сфера впливу регламенту GDPR	Україна	Грузія	Молдова
Законодавча база	– Ухвалити новий закон про захист ПД, узгоджений з GDPR – Гармонізувати галузеві закони (е-комерція, е-медицина тощо) – Розробити чіткі підзаконні процедури	– Розширити сферу дії закону про захист ПД – Розробити галузеві правила і кодекси поведінки – Впровадити privacy-by-design норми в усі закони	– Узгодити закон про захист ПД з acquis ЄС – Переглянути підзаконні акти щодо прав суб'єктів та обов'язків операторів – Узгодити суміжні закони (е-урядування, кібербезпека) з GDPR
Інституційна модель	– Посилити незалежність та спроможність Омбудсмана з захисту ПД – Налагодити ефективну координацію регуляторів – Створити експертно-консультативні органи за участі бізнесу та громадськості	– Розширити повноваження та ресурсну базу Служби інспектора – Забезпечити належну підготовку та сертифікацію персоналу – Посилити комунікацію з операторами даних та громадськістю	– Гарантувати де-юре та де-факто незалежність наглядового органу – Забезпечити регулятора належними ресурсами та експертизою – Налагодити ефективний моніторинг та правозастосування
Організаційні та технологічні заходи	– Стимулювати впровадження систем інформаційної безпеки бізнесом – Розвивати ринкову інфраструктуру захисту даних (аудит, страхування) – Напрацювати протоколи реагування на інциденти в умовах гібридної війни	– Заохочувати добровільну сертифікацію операторів за GDPR – Підтримувати розвиток PETs-рішень та сервісів кібербезпеки – Сприяти розвитку досліджень та навчальних програм у сфері захисту даних	– Розробити шаблони документів та політик приватності для бізнесу – Стимулювати обмін даними та кращими практиками між операторами – Запровадити рейтингування та відзначення компаній, що застосовують кращі практики
Правова культура та обізнаність	– Системно підвищувати правову грамотність громадян щодо прав на захист ПД – Впроваджувати курси інформаційної безпеки та приватності у закладах освіти – Проводити просвітницькі кампанії для вразливих груп (літні люди, діти)	– Підтримувати адвокаційні ГО у сфері захисту прав споживачів цифрових послуг – Популяризувати цінність приватності через соціальну рекламу, публічні заходи – Залучати лідерів думок, медіа до промоції культури захисту даних	– Інформувати громадян про ризики конфіденційності даних на практичних прикладах – Навчати держслужбовців сучасним підходам до обробки ПД – Створити доступні онлайн-ресурси та гарячі лінії з питань захисту приватності

**Джерело: розробка Удовенка О. В.*

**Source: developed by Udovenka O.V.*

Підсумовуючи, слід відзначити, що попри спільні структурні виклики, кожна з досліджуваних країн має унікальні особливості інституційного ландшафту, ринкової динаміки та суспільного контексту, які визначають пріоритетність та конфігурацію заходів із впровадження GDPR-сумісного регулювання. Відповідно, моделювання сценаріїв подальшої адаптації має відбуватись із розумінням цієї локальної специфіки, а не через механічне копіювання успішних європейських практик.

Водночас, базова логіка та послідовність інтервенцій лишається спільною: (1) гармонізація законодавства відповідно до принципів GDPR; (2) зміцнення незалежності та спроможності регуляторів; (3) стимулювання кращих практик в бізнес-середовищі; (4) підвищення обізнаності та формування проактивної позиції громадян як суб'єктів захисту даних. Саме злагоджена робота на цих взаємопов'язаних напрямах здатна забезпечити глибоку та незворотну трансформацію інституційного режиму обробки персональних даних на національному рівні.

Висновки з даного дослідження і перспективи подальших досліджень. На основі вищенаведених досліджень можна зробити такі висновки:

1) Концепція «Брюссельського ефекту» пропонує евристично потужну та емпірично обґрунтовану рамку для осмислення парадоксів глобального регуляторного впливу ЄС в епоху технологічних дизрупцій та геополітичної турбулентності. Відмовляючись від лінійних уявлень про нормативну силу та акцентуючи роль ринкових механізмів у трансляції європейських правил за межі формальної юрисдикції, ця оптика дозволяє краще зрозуміти приховані пружини та обмеження екстратериторіальної дії acquis communautaire. Водночас вона спонукає до заглиблення в локальні контексти рецепції та адаптації європейських норм з урахуванням відмінностей у інституційних моделях, політико-адміністративних культурах та соціотехнічних укладах різних суспільств. Саме на перетині глобальних регуляторних трендів та сингулярних досвідів їх доместикації відкривається простір для подальших міждисциплінарних пошуків у царині європеїзації публічної політики та права.

2) GDPR став справжнім game changer у царині глобального регулювання персональних даних, поєднавши безпрецедентно широку юрисдикцію з потужними інструментами екстериторіального впливу. Де-факто Регламент створює новий транснаціональний правовий режим, спроможний підпорядкувати своїм правилам гравців по всьому світу – від технологічних гігантів Кремнієвої долини до стартапів з країн, що розвиваються. Механізми державного примусу, ринкові стимули, технологічна уніфікація та репутаційний тиск – усі вони працюють на те, щоб перетворити GDPR на своєрідний «універсальний» операційний стандарт для цифрової економіки. Втім, ця регуляторна гравітація ЄС не відміняє значущості локальних контекстів: національні траєкторії адаптації до GDPR все ще значною мірою визначаються специфічним балансом політичних, економічних та соціокультурних факторів всередині окремих країн.

3) Водночас, приклад GDPR переконливо демонструє, що навіть наймогутніші інструменти екстериторіального впливу ЄС не гарантують тотальної гармонізації регуляторних просторів. Швидше навпаки, вони породжують строкату мозаїку стратегій адаптації – від копіювання та співпраці до опортунізму та спротиву, рясно забарвлених місцевою специфікою. Як показує порівняльний аналіз досвіду країн Східного партнерства, масштаби та

життєздатність впровадження GDPR-сумісного законодавства визначаються комплексом структурних та агентивних змінних, серед яких особливо важать інтенсивність цифрової торгівлі з ЄС, політична воля національних стейкхолдерів та спорідненість локальної культури з європейськими цінностями приватності. Тож повноцінне осмислення глобальних ефектів GDPR має відбуватись у площині взаємодії універсальних правил та партикулярних контекстів їх рецепції і адаптації.

4) Попри безумовно потужний трансформаційний вплив GDPR, ефективність та життєздатність його впровадження за межами ЄС критично залежить від локальної інституційної екосистеми. Самого лише перенесення норм Регламенту на національний ґрунт замало: без політичної волі, належного ресурсного забезпечення регуляторів, узгодженості з галузевим законодавством та глибокої культурної ревізії ставлення до приватності ці норми ризикують лишитися мертвою буквою. Тому повноцінна адаптація до GDPR передбачає не лише гармонізацію законодавства, але й цілеспрямовані зусилля з розбудови нової регуляторної парадигми на всіх рівнях – від державних інституцій до бізнес-практик та суспільної свідомості. І лише країни, готові інвестувати в ці кропіткі, але вкрай важливі процеси, мають шанс на дійсно глибоку інтеграцію принципів GDPR у національний порядок денний.

5) Водночас, кейси країн Східного партнерства переконливо доводять, що навіть за нинішнього балансу сил та інтересів на європейському континенті, GDPR володіє доволі потужними важелями екстериторіального впливу. Комбінація ринкових стимулів (доступ до спільного цифрового ринку ЄС), політичних зобов'язань (положення Угод про асоціацію) та репутаційних міркувань (позиціонування як надійної юрисдикції для локалізації даних) може суттєво пришвидшити адаптацію національного законодавства до вимог Регламенту навіть у державах, інституційно віддалених від ЄС. У цьому сенсі «Брюссельський ефект» GDPR стає не просто побічним продуктом регуляторної конкуренції, але й свідомим інструментом просування європейської моделі захисту персональних даних у глобальному вимірі.

6) Прийняття GDPR стало потужним каталізатором процесів гармонізації національних законодавств у сфері захисту персональних даних навіть поза межами ЄС. Попри різноманітні інституційні передумови та ситуативні чинники в окремих країнах, наразі ми можемо спостерігати сильний тренд до продовження (апроксимації) ключових принципів та механізмів Регламенту – як через формальні вимоги Угод про асоціацію, так і під впливом неформальних ринкових стимулів та соціокультурної дифузії. Водночас, життєздатність цих законодавчих запозичень критично залежить від спроможності національних регуляторів забезпечити ефективне правозастосування, а також готовності бізнесу та громадян прийняти нову культуру захисту даних. Відтак, успішна адаптація до GDPR передбачає далекосяжну трансформацію не лише нормативних рамок, але й всього інституційного режиму обробки персональної інформації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Association Agreement between the European Union and its Member States, of the one part, and Ukraine, of the other part. *Official Journal of the European Union*. 2014. L 161. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:22014A0529(01) (дата звернення: 18.09.2024).

2. Association Agreement between the European Union and the European Atomic Energy Community and their Member States, of the one part, and Georgia, of the other part. *Official Journal of the European Union*. 2014. L 261. URL: https://eur-lex.europa.eu/legal-content/en/TXT/PDF/?uri=CELEX:22014A0830(02) (дата звернення: 18.09.2024).

3. Azzi A. The challenges faced by the extraterritorial scope of the general data protection regulation. Journal of Intellectual Property. *Information Technology and Electronic Commerce Law*. 2018. Vol. 9. No. 2. P. 126–137. URL: https://www.jipitec.eu/jipitec/article/view/222 (дата звернення: 18.09.2024).

4. Belyakova O. Ukraine - Data Protection Overview. DataGuidance. URL: https://www.dataguidance.com/notes/ukraine-data-protection-overview (дата звернення: 18.09.2024).

5. Biedenkopf K. EU Chemicals Regulation: Extending Its Experimentalist REACH. Extending Experimentalist Governance? The European Union and Transnational Regulation / ed. J. Zeitlin. Oxford : Oxford University Press, 2015. P. 107–136. URL: http://surl.li/bkhysw (дата звернення: 18.09.2024).

6. Bradford A. The Brussels Effect: How the European Union Rules the World. New York : Oxford Academic, 2020. DOI: https://doi.org/10.1093/oso/9780190088583.001.0001

7. Bratasyuk O. Legal basis of personal data protection in Ukraine and Germany: organizational and managerial aspect. *Visegrad Journal on Human Rights*. 2023. No. 1. DOI: https://doi.org/10.61345/1339-7915.2023.1.5

8. Breitbarth P. The impact of GDPR one year on. *Network Security*. 2019. P. 11–13. DOI: https://doi.org/10.1016/S1353-4858(19)30084-4

9. Chua H. N., Herbst P., Wong S. F., Chang Y. Compliance to personal data protection principles: A study of how organizations frame privacy policy notices. *Telematics and Informatics*. 2017. Vol. 34. Iss. 4. P. 157–170. URL: https://researchprofiles.herts.ac.uk/en/publications/compliance-to-personal-data-protection-principles-a-study-of-how- DOI: https://doi.org/10.1016/j.tele.2017.01.008

10. Civil. Ge. Personal Data Protection Service Says Regulatory Clarifications are Necessary in the Agents' Law / Civil.Ge. 2024. URL: https://civil.ge/archives/608189 (дата звернення: 18.09.2024).

11. CMS Expert Guide: Data Law Navigator - Ukraine. CMS Expert Guide. 2024. URL: https://cms.law/es/int/expert-guides/cms-expert-guide-to-data-protection-and-cyber-security-laws/ukraine (дата звернення: 18.09.2024).

12. CNIL. Législations en matière de protection des données personnelles dans le monde / CNIL. 2021. URL: https://www.cnil.fr/fr/la-protection-des-donnees-dans-le-monde (дата звернення: 18.09.2024).

13. Council of Europe. Treaty 223: Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 223) / Council of Europe. 2021. URL: https://rm.coe.int/16808ac918 (дата звернення: 18.09.2024).

14. DataGuidance. Moldova - Data Protection Overview / DataGuidance. URL: https://www.dataguidance.com/notes/moldova-data-protection-overview (дата звернення: 18.09.2024).

15. Djonovic A. Moldova's EU-Inspired Path to Enhanced Data Protection. Council of Europe Newsroom. 2024. URL: http://surl.li/doyfrq (дата звернення: 18.09.2024).

16. Data protection laws of the world. DLAPiper. 2022. URL: https://www.dlapiperdataprotection.com/ (дата звернення: 18.09.2024).

17. EU4Digital. New data protection law taking effect in Georgia. / EU4Digital. 2024. URL: https://eufordigital.eu/new-data-protection-law-taking-effect-in-georgia/ (дата звернення: 18.09.2024).

18. European Commission. Commission Staff Working Document: Evaluation of Regulation (EC) No 1907/2006 concerning the Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH) / European Commission. 2020. URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=SWD:2020:247:FIN (дата звернення: 18.09.2024).

19. European Commission. Adequacy decisions: How the EU determines if a non-EU country has an adequate level of data protection. European Commission. 2021. URL: http://surl.li/azwntw (дата звернення: 18.09.2024).

20. European Commission. Adequacy decisions / European Commission. 2022. URL: https://ec.europa.eu/commission/presscorner/detail/it/qanda_22_7632 (дата звернення: 18.09.2024).

21. EDPB strategy 2021–2023. European Data Protection Board. 2022. 6 p. URL: https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_strategy2021-2023_en.pdf (дата звернення: 18.09.2024).

22. EUu4DigitalUA. Rada supports draft law «On Personal Data Protection» in first reading / Uu4DigitalUA. 2024. URL: https://eu4digitalua.eu/en/news/rada-supports-draft-law-on-personal-data-protection-in-first-reading/ (дата звернення: 18.09.2024).

23. Floridi L. The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU. *Philosophy & Technology*. 2020. Vol. 33. No. 3. P. 369–378. URL: http://surl.li/llfxuj. DOI: https://doi.org/10.1007/s13347-020-00423-6

24. GDPR enforcement tracker: List of GDPR fines. GDPR.eu. 2022. URL: https://www.enforcementtracker.com/ (дата звернення: 18.09.2024).

25. Geradin D., Kuschewsky M. Competition Law and Personal Data: Preliminary Thoughts on a Complex Issue. *SSRN Electronic Journal*. 2013. DOI: https://doi.org/10.2139/ssrn.2216088 URL: http://surl.li/qosuyw (дата звернення: 18.09.2024).

26. Government of the Republic of Moldova. Roadmap for boosting the process of digitization of the national economy and development of electronic commerce / Government of the Republic of Moldova. 2020. URL: https://consecon.gov.md/wp-content/uploads/2020/09/eEconomy-Roadmap.pdf (дата звернення: 18.09.2024).

27. Greenleaf G. Global data privacy laws 2021: Despite COVID delays, 145 laws show GDPR dominance. *Privacy Laws & Business International Report.* 2021. No. 169. P. 21-60. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3836348 (дата звернення: 18.09.2024).

28. Hofstede G. Dimensionalizing cultures: The Hofstede model in context. Online Readings in Psychology and Culture. 2011. Vol. 2, No. 1. URL: https://scholarworks.gvsu.edu/orpc/vol2/iss1/8/. DOI: https://doi.org/10.9707/2307-0919.1014

29. Jaiswal A. Data Localization: The Concept and Its Impact. *IOSR Journal of Computer Engineering.* 2019. Vol. 21, No. 1. P. 32–39.

30. Jansen R. et al. GDPR and the lost generation of innovative apps. *Harvard Business Law Review*. 2021. Vol. 11. No. 1. P. 75–100. URL: https://www.nber.org/system/files/working_papers/w30028/w30028.pdf (дата звернення: 18.09.2024).

31. Klein M. The Brussels effect and the global battle for data protection. *Georgetown Journal of International Affairs*. 2020. Vol. 21. No. 3. P. 119–129.

32. Lachaud E. The General Data Protection Regulation and the rise of certification as a regulatory instrument. *Computer Law & Security Review*. 2017. DOI: https://doi.org/10.1016/j.clsr.2017.09.002

33. Law of Georgia on Personal Data Protection. Parliament of Georgia. 2024. URL: https://matsne.gov.ge/en/document/view/1561437?publication=23 (дата звернення: 18.09.2024).

34. Law on personal data protection, No. 195 of 25.07.2024. Parliament of Republic of Moldova. 2024. URL: https://datepersonale.md/wp-content/uploads/2024/09/Law-no.-195-2024-on-personal-data-protection-1.pdf (дата звернення: 18.09.2024).

35. 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) (Text with EEA relevance). OJ. 2016. L 119. P. 1-88. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679 (дата звернення: 18.09.2024).

36. Rekhviashvili L., Lang T. Chinese investments as part of infrastructure-led development: multi-scalar contestations around Georgia's flagship infrastructure projects. *Eurasian Geography and Economics*. 2024. DOI: https://doi.org/10.1080/15387216.2024.2311712

37. Review of the OECD Recommendation on Cross-Border Co-operation in the Enforcement of Laws Protecting Privacy. *OECD Digital Economy Papers*. 2023. No. 359. DOI: https://doi.org/10.1787/67774f69-en

38. Rustad M. L., Koenig T. H. Towards a global data privacy standard. *Florida Law Review*. 2019. Vol. 71. No. 2. P. 365–453. URL: https://scholarship.law.ufl.edu/cgi/viewcontent.cgi?article=1446&context=flr (дата звернення: 18.09.2024).

39. Schimmelfennig F., Sedelmeier U. The Europeanization of Eastern Europe: the external incentives model revisited. *Journal of European Public Policy*. 2019. Vol. 27. No. 6. P. 814–833. DOI: https://doi.org/10.1080/13501763.2019.1617333

40. Schrems v. Data Protection Commissioner, Case C-311/18, ECLI:EU:C:2020:559 (July 16, 2020). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62018CJ0311 (дата звернення: 18.09.2024).

41. Schwartz P. M. Global data privacy: The EU way. *New York University Law Review*. 2019. Vol. 94. No. 4. P. 771–818. URL: https://www.nyulawreview.org/wp-content/uploads/2019/10/NYULAWREVIEW-94-4-Schwartz.pdf (дата звернення: 18.09.2024).

42. Schwartz P. M., Peifer K. N. Transatlantic data privacy law. Georgetown *Law Journal.* 2017. Vol. 106. P. 115–179. URL: https://www.law.georgetown.edu/georgetown-law-journal/wp-content/uploads/sites/26/2019/10/Transatlantic-Data-Privacy-Law_Schwartz-and-Peifer.pdf (дата звернення: 18.09.2024).

43. Scott J. Extraterritoriality and Territorial Extension in EU Law. *American Journal of Comparative Law*. 2014. Vol. 62. No. 1. P. 87–126. DOI: https://doi.org/10.5131/AJCL.2013.0009

44. Stolyarenko O., Oleniuk K. Data Protection Laws and Regulations in Ukraine / Baker McKenzie. 2024. URL: https://ceelegalmatters.com/data-protection-2024/ukraine-data-protection-2024 (дата звернення: 18.09.2024).

45. Taylor L., Floridi L., van der Sloot B. Group Privacy: New Challenges of Data Technologies. *Springer.* 2017. Vol. 126. URL: https://link.springer.com/book/10.1007/978-3-319-46608-8 (дата звернення: 18.09.2024).

46. Tudorica M., Mulder T. The GDPR Transfer Regime and Modern Technologies. Proceedings of ITU Kaldeioscope: ICT for Health: Networks, standards and innovation. *International Telecommunication Union.* 2019. P. 211–218. URL: http://handle.itu.int/11.1002/pub/8145e952-en (дата звернення: 18.09.2024).

47. UNCTAD. Data Protection and Privacy Legislation Worldwide / UNCTAD 2022. URL: https://unctad.org/page/data-protection-and-privacy-legislation-worldwide (дата звернення: 18.09.2024).

48. Wolford B. What is GDPR, the EU's new data protection law? GDPR.eu. 2022. URL: https://gdpr.eu/what-is-gdpr/ (дата звернення: 18.09.2024).

49. World Development Report 2021: Data for Better Lives. World Bank. 2022. URL: https://wdr2021.worldbank.org/the-report/ (дата звернення:

50. Yakymenko B. Formation of the institute of personal data protection and experience of its implementation in the countries of the EU. *Scientific Journal of the National Academy of Internal Affairs*. 2023. Vol. 28. No. 4. P. 68–79. URL: http://surl.li/vadrki DOI: https://doi.org/10.56215/naia-herald/4.2023.68

Стаття надійшла до редакції 22.09.2024 р.
Стаття рекомендована до друку 26.10.2024 р.

Udovenko O. V.,
PhD of Law,
Colonel of the Armed Forces of Ukraine, Unit Commander,
Kyiv, Ukraine
e-mail: command.1361@ukr.net https://orcid.org/0009-0004-7845-0455

Velychko L. Yu.,
Doctor of Sciences of Law, Professor,
Head of the Department of Law, National Security and European Integration,
Education and Research Institute of Public Administration, V. N. Karazin Kharkiv National University,
4, Svobody Sq., Kharkiv, 61022, Ukraine
e-mail: l.velychko@karazin.ua https://orcid.org/0000-0003-3029-4719

HOW DOES THE «BRUSSELS EFFECT» SHAPE NEW STANDARDS? THE IMPACT OF THE GDPR DATA PROTECTION STANDARD AND OTHER EU INITIATIVES ON UKRAINE AND COUNTRIES OUTSIDE THE EUROPEAN UNION

Abstract. This article examines the impact of the European Union's General Data Protection Regulation (GDPR) on countries beyond the borders of the EU, with a particular focus on Ukraine, through the lens of the «Brussels Effect» concept. The purpose of the article is to unveil the role of the «Brussels Effect» in shaping global standards for personal data protection and its influence on the regulatory adaptation processes of Ukraine and other Eastern Partnership countries to GDPR requirements, based on theoretical and empirical analysis. The methodology employed in this article relies on an eclectic combination of conceptual-theoretical approaches and empirical methods from the arsenal of legal sciences, political analysis, economics, and sociology. This methodological diversity is driven by the need for a holistic understanding of the multidimensional phenomenon of the «Brussels Effect» and its impact on various aspects of personal data regulation. The authors analyze how the GDPR de facto creates a transnational legal regime for personal data protection, compelling third countries to adapt their legislation to European standards. Based on a comparative case study of Ukraine, Georgia, and Moldova, common patterns and specific factors of the harmonization process

with GDPR are identified – ranging from the intensity of digital trade with the EU to the political will of national stakeholders. The authors argue that despite the powerful transformative influence of the GDPR, its effective implementation critically depends on the local institutional ecosystem and a cultural revision of attitudes towards privacy. Therefore, full-fledged adaptation to the GDPR requires targeted efforts at all levels – from modernizing legislation to strengthening the capacity of regulators and shaping a proactive stance of citizens. Drawing on a matrix of 6 key dimensions (regulatory framework, institutional model, law enforcement, etc.), practical recommendations are provided for enhancing the extraterritorial effect of the GDPR in the Eastern Partnership region, taking into account the security challenges of hybrid warfare for Ukraine. The article contributes to the current discussion about the EU's new role as a global regulatory player in the digital age.

Keywords: GDPR, personal data protection, Brussels Effect, legal policy, Europeanization, European integration, digital economy, institutional adaptation, Ukraine, EU.

REFERENCES

1. Association Agreement between the European Union and its Member States, of the one part, and Ukraine, of the other part. (2014). *Official Journal of the European Union, L 161.* UTL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:22014A0529(01)

2. Association Agreement between the European Union and the European Atomic Energy Community and their Member States, of the one part, and Georgia, of the other part. (2014). *Official Journal of the European Union, L 261.* UTL: https://eur-lex.europa.eu/legal-content/en/TXT/PDF/?uri=CELEX:22014A0830(02)

3. Azzi, A. (2018). The challenges faced by the extraterritorial scope of the general data protection regulation. Journal of Intellectual Property, *Information Technology and Electronic Commerce Law, 9(2), 126–137*. URL: https://www.jipitec.eu/jipitec/article/view/222

4. Belyakova, O. (2024). Ukraine – Data Protection Overview. URL: https://www.dataguidance.com/notes/ukraine-data-protection-overview

5. Biedenkopf, K. (2015). EU Chemicals Regulation: Extending Its Experimentalist REACH. In J. Zeitlin (Ed.), Extending Experimentalist Governance? The European Union and Transnational Regulation (pp. 107–136). Oxford University Press. URL: http://surl.li/bkhysw

6. Bradford, A. (2020). The Brussels Effect: How the European Union Rules the World (New York, 2020; online edn, Oxford Academic, 19 Dec. 2019), DOI: https://doi.org/10.1093/oso/9780190088583.001.0001, accessed 18 Dec. 2024.

7. Bratasyuk, O. (2023). Legal basis of personal data protection in Ukraine and Germany: organizational and managerial aspect. *Visegrad Journal on Human Rights, 1*. URL: https://journals.uran.ua/journal-vjhr/article/view/295441 DOI: https://doi.org/10.61345/1339-7915.2023.1.5

8. Breitbarth, P. (2019). The impact of GDPR one year on. *Network Security, 11–13.* DOI: https://doi.org/10.1016/S1353-4858(19)30084-4 URL: https://www.researchgate.net/publication/334584226_The_impact_of_GDPR_one_year_on/citation/download

9. Chua, H.N., Herbst, P., Wong, S.F., & Chang, Y. (2017). Compliance to personal data protection principles: A study of how organizations frame privacy policy notices. *Telematics and Informatics, 34(4), 157–170.* URL: https://researchprofiles.herts.ac.uk/en/publications/compliance-to-personal-data-protection-principles-a-study-of-how- DOI: https://doi.org/10.1016/j.tele.2017.01.008

10. Civil, Ge (2024). Personal Data Protection Service Says Regulatory Clarifications are Necessary in the Agents' Lawю URL: https://civil.ge/archives/608189

11. CMS Expert Guide (2024). CMS Expert Guide: Data Law Navigator - Ukraine. URL: https://cms.law/es/int/expert-guides/cms-expert-guide-to-data-protection-and-cyber-security-laws/ukraine

12. CNIL. (2021). Législations en matière de protection des données personnelles dans le monde. URL: https://www.cnil.fr/fr/la-protection-des-donnees-dans-le-monde

13. Council of Europe. (2021). Treaty 223: Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 223). URL: https://rm.coe.int/16808ac918

14. DataGuidance (2024). Moldova – Data Protection Overview. URL: https://www.dataguidance.com/notes/moldova-data-protection-overview

15. Djonovic, A. (2024). Moldova's EU-Inspired Path to Enhanced Data Protection. URL: http://surl.li/doyfrq

16. DLA Piper. (2022). Data protection laws of the world. URL: https://www.dlapiperdataprotection.com/

17. EU4Digital (2024). New data protection law taking effect in Georgia. URL: https://eufordigital.eu/new-data-protection-law-taking-effect-in-georgia/

18. European Commission. (2020). Commission Staff Working Document: Evaluation of Regulation (EC) No 1907/2006 concerning the Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH). SWD(2018) 58 final. URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=SWD:2020:247:FIN

19. European Commission. (2021). Adequacy decisions: How the EU determines if a non-EU country has an adequate level of data protection. Retrieved from https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en. URL: http://surl.li/azwntw

20. European Commission. (2022). Adequacy decisions. URL: https://ec.europa.eu/commission/presscorner/detail/it/qanda_22_7632

21. European Data Protection Board. (2022). EDPB strategy 2021–2023. 6 p. URL: https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_strategy2021-2023_en.pdf

22. EUu4DigitalUA (2024). Rada supports draft law “On Personal Data Protection” in first reading. URl: https://eu4digitalua.eu/en/news/rada-supports-draft-law-on-personal-data-protection-in-first-reading/

23. Floridi, L. (2020). The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU. *Philosophy & Technology, 33(3), 369–378*. URL: http://surl.li/llfxuj. DOI https://doi.org/10.1007/s13347-020-00423-6

24. GDPR.eu. (2022). GDPR enforcement tracker: List of GDPR fines. UTL: https://www.enforcementtracker.com/

25. Geradin, D., & Kuschewsky, M. (2013). Competition Law and Personal Data: Preliminary Thoughts on a Complex Issue. SSRN Electronic Journal. DOI: https://doi.org/10.2139/ssrn.2216088 URL: http://surl.li/qosuyw

26. Government of the Republic of Moldova. (2020). Roadmap for boosting the process of digitization of the national economy and development of electronic commerce. URL: https://consecon.gov.md/wp-content/uploads/2020/09/eEconomy-Roadmap.pdf

27. Greenleaf, G. (2021). Global data privacy laws 2021: Despite COVID delays, 145 laws show GDPR dominance. *Privacy Laws & Business International Report, 169, 21–60*. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3836348

28. Hofstede, G. (2011). Dimensionalizing cultures: The Hofstede model in context. *Online Readings in Psychology and Culture, 2(1).* DOI: https://doi.org/10.9707/2307-0919.1014 . URL: https://scholarworks.gvsu.edu/orpc/vol2/iss1/8/

29. Jaiswal, A. (2019). Data Localization: The Concept and Its Impact. *IOSR Journal of Computer Engineering, 21(1), 32–39*.

30. Jansen, R., et al. (2021). GDPR and the lost generation of innovative apps. *Harvard Business Law Review, 11(1), 75–100.* URL: https://www.nber.org/system/files/working_papers/w30028/w30028.pdf

31. Klein, M. (2020). The Brussels effect and the global battle for data protection. *Georgetown Journal of International Affairs, 21(3), 119–129*.

32. Lachaud, E. (2017). The General Data Protection Regulation and the rise of certification as a regulatory instrument. Computer Law & Security Review. DOI: https://doi.org/10.1016/j.clsr.2017.09.002

33. OECD (2023). Review of the OECD Recommendation on Cross-Border Co-operation in the Enforcement of Laws Protecting Privacy. OECD Digital Economy Papers, No. 359, OECD Publishing, Paris, DOI: https://doi.org/10.1787/67774f69-en

34. Parliament of Georgia (2024). Law of Georgia on Personal Data Protection. URl: https://matsne.gov.ge/en/document/view/1561437?publication=23

35. Parliament of Republic of Moldova (2024). Law on personal data protection, No. 195 of 25.07.2024. URL: https://datepersonale.md/wp-content/uploads/2024/09/Law-no.-195-2024-on-personal-data-protection-1.pdf

36. 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) (Text with EEA relevance), OJ 2016 L 119/1. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

37. Rekhviashvili, L., Lang, T. (2024): Chinese investments as part of infrastructure-led development: multi-scalar contestations around Georgia’s flagship infrastructure projects, Eurasian Geography and Economics. URL: https://www.tandfonline.com/doi/pdf/10.1080/15387216.2024.2311712 DOI: https://doi.org/10.1080/15387216.2024.2311712

38. Rustad, M.L., & Koenig, T.H. (2019). Towards a global data privacy standard. *Florida Law Review, 71(2), 365–453*. URL: https://scholarship.law.ufl.edu/cgi/viewcontent.cgi?article=1446&context=flr

39. Schimmelfennig, F., Sedelmeier, U. (2019). The Europeanization of Eastern Europe: the external incentives model revisited. *Journal of European Public Policy, 27(6), 814–833.* DOI: https://doi.org/10.1080/13501763.2019.1617333

40. Schrems v. Data Protection Commissioner, Case C-311/18, ECLI:EU:C:2020:559 (July 16, 2020). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62018CJ0311

41. Schwartz, P.M. (2019). Global data privacy: The EU way. *New York University Law Review, 94(4), 771–818.* URL: https://www.nyulawreview.org/wp-content/uploads/2019/10/NYULAWREVIEW-94-4-Schwartz.pdf

42. Schwartz, P.M., & Peifer, K.N. (2017). Transatlantic data privacy law. *Georgetown Law Journal, 106, 115–179.* URL: https://www.law.georgetown.edu/georgetown-law-journal/wp-content/uploads/sites/26/2019/10/Transatlantic-Data-Privacy-Law_Schwartz-and-Peifer.pdf

43. Scott, J. (2014). Extraterritoriality and Territorial Extension in EU Law. *American Journal of Comparative Law, 62(1), 87–126.* DOI: https://doi.org/10.5131/AJCL.2013.0009

44. Stolyarenko, O., Oleniuk, K. (2024). Data Protection Laws and Regulations in Ukraine / Baker McKenzie. URL: https://ceelegalmatters.com/data-protection-2024/ukraine-data-protection-2024

45. Taylor, L., Floridi, L., & van der Sloot, B. (Eds.). (2017). Group Privacy: New Challenges of Data Technologies (Vol. 126). Springer. URL: https://link.springer.com/book/10.1007/978-3-319-46608-8

46. Tudorica M., Mulder, T. (2019). The GDPR Transfer Regime and Modern Technologies. In Proceedings of ITU Kaldeioscope: ICT for Health: Networks, standards and innovation (pp. 211–218). International Telecommunication Union. http://handle.itu.int/11.1002/pub/8145e952-en

47. UNCTAD. (2021). Data Protection and Privacy Legislation Worldwide. URL: https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

48. Wolford, B. (2022). What is GDPR, the EU's new data protection law? URL: https://gdpr.eu/what-is-gdpr/

49. World Bank. (2022). World Development Report 2021: Data for Better Lives. UTL: https://wdr2021.worldbank.org/

50. Yakymenko, B. (2023). Formation of the institute of personal data protection and experience of its implementation in the countries of the EU. *Scientific Journal of the National Academy of Internal Affairs, Vol. 28, No. 4. 68–79*. URL: http://surl.li/vadrki DOI: https://doi.org/10.56215/naia-herald/4.2023.68

The article was received by the editors 22.09.2024.

The article is recommended for printing 26.10.2024.