

*Чванкін С. А.,
доктор юридичних наук, доцент,
голова
Київського районного суду м. Одеси*

ЕКСТРАТЕРИТОРІАЛЬНИЙ ВПЛИВ ЗАГАЛЬНОГО РЕГЛАМЕНТУ ПРО ЗАХИСТ ДАНИХ (GDPR)

Анотація. У статті досліджується вплив Загального регламенту про захист даних не тільки на законодавство країн-членів ЄС, а й на законодавство третіх країн.

Відзначається, що всі країни-члени зв'язані законодавством ЄС, однак можуть існувати відмінності в тому, як кожна національна правова система забезпечує ефективний захист, що можна пояснити відмінною правовою традицією та специфікою правової системи та органів управління в кожній країні. В силу національної автономії національне регулювання має забезпечити, з одного боку, процедуру, адаптовану до конкретних потреб держав-членів, а з іншого – ефективний інструмент для досягнення гармонізованого застосування закону в усьому ЄС. Автономія держав-членів не є абсолютною і повинна реалізовуватися в загальному руслі Регламенту та підпорядковуватися принципам еквівалентності, ефективності, щирої співпраці.

Відзначено суттєвий вплив Регламенту на Україну як країну-кандидатку на вступ до ЄС, адже це є прямою вимогою Угоди про асоціацію між Україною та ЄС, за якою сторони домовились співпрацювати з метою забезпечення належного рівня захисту персональних даних відповідно до найвищих європейських та міжнародних стандартів.

Вплив ЄС та його правових положень у формуванні національних правових рамок можна віднайти не тільки у країнах географічної Європи, як тих, що мають статус кандидата на членство у ЄС, так і тих, що дотримуються позаблокового статусу, а й на інші правопорядки, зокрема, Аргентину, Бахрейн, Бразилію, Катар, Мексику, ОАЕ, Оман, Саудівську Аравію, США, Чилі тощо.

Зроблено висновок, що законодавство ЄС щодо захисту персональних даних має значний вплив на законодавство третіх країн. Оскільки ЄС є одним з найбільших економічних блоків у світі, вимоги GDPR стали стандартом в галузі захисту персональних даних і вимагають від третіх країн адаптації свого законодавства для відповідності цим стандартам при обробці даних європейських громадян. Це приводить до того, що значна кількість країн переглядають своє законодавство про захист персональних даних, щоб відповідати вимогам GDPR, навіть у тому випадку, коли не встановлено нормативного обов'язку гармонізації законодавства. Вказане обумовлюється так званим «брюссельським ефектом» – прагненням третіх країн та їх компаній-резидентів отримати доступ до економічних інструментів та ринків Європи.

Ключові слова: Загальний регламент про захист даних, GDPR, захист персональних даних, екстраєриторіальна юрисдикція, брюссельський ефект, гармонізація, Європейський Союз.

Постановка проблеми. Захист персональних даних розвивається в ЄС як автономне основне право з його норма-

тивним визнанням, закріпленим Загальним регламентом про захист даних (General Data Protection Regulation, Regulation (EU) 2016/679, далі – GDPR, Регламент), ухваленого 14 квітня 2016 року, та який почав застосовуватися з 25 травня 2018 року [1]. Важливість закріплення права на захист персональних даних на рівні законодавства ЄС полягає в тому, щоб захист персональних даних не займав ієрархічно нижчу позицію в конфлікті з іншими захищеними правами та інтересами, які можуть гарантуватися як на рівні ЄС, так і на національному рівні.

Існує широкий консенсус щодо того, що ЄС має великі джерела влади – великий внутрішній ринок, складні регуляторні можливості та суворі ринкові правила, що обумовлює різні способи взаємодії ЄС із зовнішнім регуляторним середовищем. Однак розуміння того, як і коли ЄС використовує свої внутрішні джерела влади для активного впливу на режими третіх країн, залишається неповним [2, с. 531; 3]. Регуляторна спроможність ЄС проявляється в тому, що таке наднаціональне об'єднання отримує можливість запроваджувати нові регуляторні акти та здійснювати контроль над їх виконанням не тільки на внутрішньому правовому просторі ЄС, а й впливати на інші правові системи: «проекція зовнішньої регулятивної влади є актуальною та ефективною лише за умови, що ЄС також має суворі правила внутрішнього ринку» [2, с. 533]. Для третіх країн і контролерів персональних даних основним стимулом прийняти стандарти захисту даних, еквівалентні стандартам ЄС, є побоювання втратити доступ до ринку ЄС.

Стан дослідження. Питання впливу Загального регламенту про захист даних на законодавство та комерційну практику є предметом більш широкої дискусії щодо нормотворчої експансії ЄС, відомої як «брюссельський ефект». Дослідженню вказаного явища присвячено низку праць Ану Бредфорда (Anu Bradford), який запровадив даний термін у 2012 році на позначення явища, що звільняє ЄС від прямої ролі в нав'язуванні стандартів, оскільки одних тільки ринкових сил часто достатньо для гармонізації іноземних правопорядків. Вказана концепція розвивається у роботах Шарлотти Зігман та Маркуса Андерлунга (Charlotte Siegmann, Markus Anderljug), Аннегрет Бендік та Ізабелли Штурцер (Annegret Bendiek, Isabella Stuerzer) та інших дослідників, які зосереджували увагу на секторальному впливі ефекту (у сфері трудових прав, застосування штучного інтелекту тощо). Однак захист даних характеризується певною дистанційністю: щоб підпадати під європейське регулювання, не обов'язково здійснювати реальні експортно-імпорتنі операції: весь обмін даними проходить на великій відстані у цифровому середовищі. Вплив GDPR на іноземні правопорядки досліджувався у працях Грегі Рудольфа та

Полонки Ковач (Grega Rudolf, Polonca Kovač), Біляни Петкової (Bilyana Petkova) та іншими дослідниками.

Метою дослідження є визначення основних напрямків впливу Загального регламенту про захист даних на національне законодавство не тільки країн, які є країнами-учасницями ЄС, а і країн, які не мають формальних зобов'язань щодо приведення власних законодавчих норм до стандартів ЄС.

Виклад основного матеріалу. Екстериторіальність ЄС формує глобальні стандарти захисту даних. Залишається нормативним питанням щодо того, наскільки наполегливо ЄС повинен нав'язувати свій закон про захист персональних даних іноземним постачальникам послуг або третім державам [4, с. 9]. Вказане явище отримало назву «брюссельський ефект» – «безпрецедентна та глибоко недооцінена глобальна влада, яку Європейський Союз здійснює через свої правові інституції та стандарти, а також те, як він успішно експортує цей вплив до решти світу. Без необхідності використовувати міжнародні інституції чи шукати співпраці з іншими націями, ЄС має потужну та зростаючу здатність оприлюднювати нормативні акти, які закріплюються в правових рамках як розвинутих ринків, так і ринків, що розвиваються, що призводить до помітної «європеїзації» багатьох важливих аспектів глобальної торгівлі» [5, с. 1].

Принципи захисту даних ЄС поширилися за кордоном і змусили змінити не тільки законодавство третіх країн, а й практику захисту даних міжнародних корпорацій або компаній, які не зареєстровані у ЄС, наприклад, Alphabet (основним продуктом якої є Google), Meta (Facebook, Instagram, WhatsApp та ін.) тощо, які зацікавлені у присутності на європейському цифровому ринку надання інформаційних послуг.

Можна стверджувати, що ЄС бере на себе екстериторіальні зобов'язання, коли здійснюється контроль над даними резидента ЄС. Це означає, що оскільки ЄС має можливість впливати на те, як дані обробляються за кордоном, він повинен використовувати цей вплив для захисту даних суб'єкта даних ЄС; Європейський Союз повинен тлумачити законодавство ЄС про захист даних таким чином, щоб воно захищало фундаментальне право суб'єктів ЄС на захист даних від посягань з боку третіх держав і операторів, розташованих у третіх державах [4, с. 6–7].

Незважаючи на те, що всі країни-члени зв'язані законодавством ЄС, можуть існувати відмінності в тому, як кожна національна правова система забезпечує ефективний захист, що можна пояснити відмінною правовою традицією та специфікою правової системи та органів управління в кожній країні [6, с. 153]. Національна автономія не заперечує необхідності узгодження внутрішнього законодавства із законодавством ЄС, адже законодавство ЄС закріплює ефективний спосіб або інструмент для застосування прав GDPR у відповідній державі-члені. Тоді як національне регулювання має забезпечити, з одного боку, процедуру, адаптовану до конкретних потреб держав-членів, а з іншого – ефективний інструмент для досягнення гармонізованого застосування закону.

Можливість національної автономії у регулюванні визнав і Суд ЄС у справі “Meta Platforms Ireland” C-319/20, в якій було розглянуто запит федерального суду Німеччини щодо можливості асоціації захисту прав споживачів після набрання чинності Загальним регламентом про захист даних подавати позови в цивільних судах щодо порушень цього регламенту, незалежно

від конкретного порушення прав окремих суб'єктів даних і без доручення цих суб'єктів даних, оскільки на думку національного суду з GDPR можна зробити висновок, що перевірка застосування положень цього Регламенту належить головним чином органам нагляду. Суд ЄС, розглянувши запит, додатково наголосив, що GDPR забезпечує гармонізацію національного законодавства щодо захисту персональних даних. Проте певні положення GDPR дозволяють державам-членам встановлювати додаткові правила, які залишають їм свободу розсуду щодо способу реалізації цих положень, за умови, що прийняті національні правила не підривають зміст і цілі цього положення. На думку Суду, GDPR не перешкоджає національним положенням, які передбачають подання позовів проти порушень прав щодо захисту персональних даних з підстав захисту споживачів або боротьби з недобросовісною комерційною практикою [7]. Однак автономія держав-членів не є абсолютною і повинна реалізовуватися в загальному руслі Регламенту.

У нещодавній справі “Nemzeti Adatvédelmi és Információszabadság Hatóság” № 132/21 Суд ЄС розглянув питання балансу між дотриманням національної процесуальної автономії, з одного боку, та забезпеченням того, щоб національні процедури не підривали гармонізуючу мету законодавства ЄС – з іншого. За відсутності правил ЄС, які врегульовують певні питання, кожна держава-член, відповідно до принципу процесуальної автономії, повинна встановити детальні правила адміністративних і судових процедур, призначених для забезпечення високого рівня захисту прав, які випливають із законодавства ЄС. У цій справі Суд ЄС роз'яснив межі процесуальної автономії, які завжди мають визначатися наступними принципами:

а) еквівалентності (правила, що деталізують європейське законодавство, не повинні бути менш сприятливими, ніж ті, що регулюють аналогічні внутрішньодержавні правовідносини);

б) ефективності (національне регулювання не повинно робити практично неможливим або надмірно ускладнювати здійснення прав, наданих законодавством ЄС);

в) щирої співпраці (суди держав-членів мають забезпечити судовий захист прав особи відповідно до права ЄС, держави повинні надавати засоби правового захисту, достатні для забезпечення ефективного судового захисту у сферах, які охоплюються правом ЄС) [8].

Таким чином, користуючись своєю процедурною автономією, країни-члени завжди повинні гарантувати, що їхні порядки не перешкоджають і не ставлять під загрозу здійснення прав, передбачених GDPR.

У правовій системі ЄС принцип субсидіарності виглядає як життєво важливий принцип, який сприяє децентралізації прийняття рішень і обмежує компетенцію Союзу сферами, які країни-члени не можуть ефективно реалізувати.

Вплив GDPR на Україну як країну-кандидатку на вступ до ЄС є суттєвим, адже це є прямою вимогою Угоди про асоціацію між Україною та Європейським Союзом, за якою сторони домовились співробітничати з метою забезпечення належного рівня захисту персональних даних відповідно до найвищих європейських та міжнародних стандартів. Також у Верховній Раді України зареєстровано проект Закону України про Національну комісію з питань захисту персональних даних та доступу до публічної інформації (реєстр. № 6177 від 18.10.2021 р.), який передбачає створення нового органу контролю у сфері захисту

персональних даних, а також визначає статус, повноваження, організаційну основу та порядок діяльності цього органу, та проект Закону України про захист персональних даних (реєстр. № 8153 від 25.10.2022 р.) [9; 10].

У висновку щодо законопроекту № 8153, підготовленому експертами Ради Європи, зазначається, що «законопроект містить розширену редакцію положень, які встановлюють комплексну правову базу захисту даних. <...> Загальний підхід Законопроекту досить близький до підходу, який випливає з європейських стандартів» [11]. Водночас, експертами рекомендовано переглянути, уточнити або змінити деякі положення законопроекту з огляду на приведення у відповідність із європейськими стандартами, зокрема GDPR.

Унікальна ситуація склалася щодо захисту персональних даних у Великобританії, яка 23 червня 2016 року на референдумі проголосувала за вихід з Європейського Союзу, а остаточний вихід (так званий “Brexit”) було реалізовано 31 січня 2020 року. Таким чином, Сполучене Королівство за короткий період пройшло трансформацію: від національного Закону про захист даних (Data Protection Act, DPA) 1998 року, який впроваджував Європейську директиву із захисту даних (Директива 95/46 ЄС), до заміни Директиви 95/46 ЄС Регламентом з 25 травня 2018 року, а потім – повернення до повної національної автономії у сфері захисту даних після виходу з ЄС. Велика Британія, по суті, могла реалізувати одразу декілька перехідних сценаріїв: а) вимагати, щоб GDPR ніколи не набув чинності у Великобританії, залишаючи в силі DPA 1998 року доки не буде прийнято нове національне законодавство про захист даних; б) зупинити впровадження GDPR на деякий час, очікуючи результатів переговорів між ЄС і Великою Британією; в) визнати GDPR і впровадити супутні законодавчі заходи, щоб повністю відповідати законодавству ЄС про захист даних [12, с. 167].

Очевидно, що вихід Великобританії з ЄС не означав повного розриву зв'язків, з цих причин модель виключно національного регулювання була б неефективною, тому було запроваджено новий Закон про захист даних 2018 року, який набув чинності 25 травня 2018 року одночасно з GDPR. Незважаючи на вихід з Європейського Союзу 31 січня 2020 року, Великобританія залишалася підпорядкована законодавству ЄС, включаючи GDPR, до кінця перехідного періоду по 31 грудня 2020 року, а відповідно до розділу 3 Закону про вихід з Європейського Союзу 2018 року GDPR включається безпосередньо у внутрішнє законодавство одразу після виходу Великобританії з Європейського Союзу. Така модель регулювання позначається як “UK GDPR”: з одного боку – це правонаступний правопорядок, що ввібрав основні елементи загальноєвропейського GDPR, а з іншого – відправна точка для подальших національних змін. Оскільки на даний час Великобританія більше не зв'язана напряму положеннями Регламенту, в його розумінні є «третьою країною», що унеможливило б передачу персональних даних доки не будуть застосовані відповідні гарантії або Європейська комісія не встановить відповідність британського законодавства про захист даних Регламенту. 28 червня 2021 року Комісія ЄС прийняла рішення щодо відповідності Великобританії Загальному регламенту захисту даних, що дозволило передавати дані без необхідності вживати додаткових заходів безпеки.

Вплив ЄС та його правових положень у формуванні національних правових рамок можна віднайти не тільки у країнах

географічної Європи (як тих, що мають статус кандидата на членство у ЄС, так і тих, що дотримуються позаблокового статусу), а й на інші правопорядки, зокрема, Аргентину, Бразилію, Мексику, Чилі тощо. Як зазначають А. Веронезе, А. Сільвейра та інші, «латиноамериканський рух щодо надання статусу захисту персональних даних як конституційного чи основного права у внутрішніх правових системах є результатом впливу моделі ЄС» [13, с. 59].

В даних країнах запозичення європейської регуляції пов'язане не тільки з вищевказаною регуляторною спроможністю ЄС, а й з історичними факторами – іспанським колоніалізмом, соціально-економічними та культурними особливостями регіону, внаслідок чого зберігаються тісні зв'язки з іспаномовними регіонами Центральної та Південної Америки, чим пояснюються спроби латиноамериканських країн узгодити законодавство зі стандартами ЄС. Як зазначається, саме Королівський указ Іспанії про захист персональних даних (Ley Orgánica 15/1999) у багатьох випадках слугував для багатьох країн Латинської Америки передумовою узгодження своїх національних правових норм із моделлю ЄС. Зокрема, аргентинське законодавство про захист персональних даних практично відтворює іспанське законодавство, через що в національне законодавство опосередковано було імplementовано європейські критерії [13, с. 66, 78].

Крім того, очевидний серед латиноамериканських країн прямий вплив законодавчої бази ЄС, заохочує сусідні країни приєднуватися до процесів гармонізації. Навпаки, вплив США на захист персональних даних у Латинській Америці загалом мінімальний, за винятком кількох країн, таких як Колумбія та Чилі. Ця відмінність виникає через те, що латиноамериканська модель розглядає захист персональних даних як незалежне, часто фундаментальне право, яке не походить від захисту прав споживачів. Важливо визнати, що, незважаючи на сильний вплив ЄС, Латинська Америка поступово формує свою законодавчу базу [14, с. 138].

Аналогічним чином вплив ЄС спостерігається і на законодавство країн-учасниць БРІКС (Бразилія, Росія, Індія, Китай і Південна Африка), «під час розробки своїх рамок країни БРІКС скористалися перевагою наявності найсучасніших стандартів захисту даних — головним чином, Європейського загального регламенту захисту даних (GDPR) — як джерела натхнення, одночасно адаптуючи норми до своїх внутрішніх правових традицій і політичної системи». Незважаючи на відсутність будь-якої офіційної угоди, яка б вимагала узгодження їхніх національних рамок, деякі з національних положень щодо захисту персональних даних встановлені подібним чином [15, с. 6, 9]. При цьому індійська та китайська моделі захисту персональних даних зазнали найменшого впливу європейських правових інструментів та тяжіють до розробки власних моделей регулювання.

Так само й Австралія, не маючи достатньо стійких зв'язків із ЄС, обирає шлях мінімального узгодження законодавства, оскільки дотримання всіх вимог щодо конфіденційності даних може бути обтяжливо (наприклад, стаття 37 GDPR вимагає від бізнесу призначення уповноваженого із захисту даних). Тому австралійський бізнес, враховуючи його значну присутність на австралійському ринку, повинен буде дотримуватися австралійського закону про конфіденційність даних, однак через дуже обмежену взаємодію з ринками ЄС, ймовірно, потрібно буде

враховувати лише ті положення про конфіденційність даних ЄС, які підпадають під «рівень запобігання зловживанням» [16, с. 135]. І враховуючи, що ці положення, загалом однакові для більшості законів про конфіденційність даних у світі, їхнє дотримання не буде обтяжливим для контролерів.

Щодо впливу законодавства ЄС на правопорядок США, відзначаються суперечливі тенденції. Так, на думку Б. Петкової, всупереч загальноприйнятому погляду на ЄС як на глобального нормотворця щодо конфіденційності даних, у багатьох випадках ЄС насправді приймав норми щодо стандартів і практик, що походять із Сполучених Штатів [17, с. 1156]. Хоча авторкою і відзначається вплив законів Каліфорнії на Загальний регламент про захист даних ЄС, вказується і на їх суттєві відмінності. Законодавство ЄС про конфіденційність даних продовжує наголошувати на фундаментальних правах, тоді як американський досвід, зазвичай обмежується трактуванням конфіденційності даних не як конституційного права, а як питання захисту споживачів. Крім того, законодавство США у даній сфері є фрагментованим, адже належить до сфери регулювання різних галузей права, а кожен штат, за відсутності єдиного федерального закону, може встановлювати власні правила захисту даних: каліфорнійський закон про конфіденційність споживачів (California Consumer Privacy Act) є прикладом закону штату галузевої спрямованості. Як зазначають О. Амоо та ін., «вплив GDPR викликав розмови про необхідність всеосяжного федерального закону про конфіденційність, однак взаємодія між державними та федеральними правилами продовжує створювати проблеми для бізнесу. Подолання цих складнощів вимагає стратегічного та гнучкого підходу до кібербезпеки, оскільки організації прагнуть відповідати зростаючим очікуванням щодо захисту даних у глобально взаємопов'язаному цифровому ландшафті» [18, с. 1340]. Сполучені Штати та ЄС пристосовуються до нормативних ідей один одного та роблять свій внесок у розвиток двох поки що різних підходів до конфіденційності комерційних даних в Інтернеті [17, с. 1156].

Багато третіх країн, включно з багатьма країнами, що розвиваються, ймовірно, мають намір впровадити положення GDPR у власне законодавство, щоб Європейська комісія потенційно визнала його «адекватним». Крім того, ухвалення законодавства про захист даних, яке по суті еквівалентне GDPR або перегляд існуючого законодавства відповідно до цього стандарту вимагатиме від третіх країн інвестувати в масштабний законодавчий процес, який може тривати багато років [19, с. 232]. Враховуючи міцні економічні зв'язки з Європейським Союзом, багато компаній Ради співробітництва арабських держав Перської затоки (Бахрейн, Катар, Кувейт, ОАЕ, Оман, Саудівська Аравія) підпадають під дію GDPR. І хоча на закони про захист персональних даних у країнах Перської затоки різною мірою вплинув GDPR, існує є значні розбіжності, особливо щодо підходів до захисту даних. Це свідчить про те, що рівень захисту даних у країнах Перської затоки не еквівалентний тому, який пропонує GDPR [20]. В останні роки країни Південно-Східної Азії прийняли або оновили закони про конфіденційність даних положеннями, які відповідають GDPR [21], оновлене законодавство В'єтнаму (Декрет № 13/2023/ND-CP від 1 липня 2023 р.) хоча і не відтворює повністю стандарти GDPR, все ж створює передумови для подальшої інтеграції відповідних положень [22].

Висновки. Законодавство Європейського Союзу щодо захисту персональних даних має значний вплив на законодав-

ство третіх країн. Оскільки ЄС є одним з найбільших економічних блоків у світі, вимоги GDPR стали стандартом в галузі захисту персональних даних і вимагають від третіх країн адаптації свого законодавства для відповідності цим стандартам при обробці даних європейських громадян.

Це приводить до того, що значна кількість країн переглядають своє законодавство про захист персональних даних, щоб відповідати вимогам GDPR, навіть у тому випадку, коли не встановлено нормативного обов'язку гармонізації законодавства. Деякі країни приймають нові закони або вносять зміни до існуючих, щоб забезпечити відповідність.

Література:

1. 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). *OJ L*. 119 4.5.2016. P. 1. ELI: <http://data.europa.eu/eli/reg/2016/679/2016-05-04>.
2. Jarlebring J. 'Regime vetting': a technique to exercise EU market power. *Journal of European Public Policy*. 2022. 29(4). P. 530–549. DOI: 10.1080/13501763.2021.1874042.
3. Cervi G. V. Why and How Does the EU Rule Global Digital Policy: an Empirical Analysis of EU Regulatory Influence in Data Protection Laws. *Digital Society*. 2022. 1(2). DOI: 10.1007/s44206-022-00005-3.
4. Ryngaert C., Taylor M. The GDPR as Global Data Protection Regulation? *AJIL Unbound*. 2020. № 114. P. 5–9. DOI: 10.1017/aju.2019.80.
5. Bradford A. The Brussels Effect. *Northwestern University Law Review*. 2012. Vol. 107. № 1, Columbia Law and Economics Working Paper No. 533. URL: <https://ssrn.com/abstract=2770634>.
6. Rudolf G., Kovač P. Procedural Challenges of Cross-border Cooperation and Consistency in Personal Data Protection in the EU. *NISPAcee Journal of Public Administration and Policy*. 2023. 16(2). P. 143–170. DOI: 10.2478/nispa-2023-0017.
7. Judgment in Case C-319/20 Meta Platforms Ireland : Judgment of the Court (Third Chamber) of 28 April 2022. URL: <https://curia.europa.eu/juris/liste.jsf?num=C-319/20>.
8. Judgment of the Court (First Chamber) of 12 January 2023. BE v Nemzeti Adatvédelmi és Információszabadság Hatóság : ECLI:EU:C:2023:2. URL: <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62021CJ0132>.
9. Проект Закону України про Національну комісію з питань захисту персональних даних та доступу до публічної інформації (№ 6177 від 18.10.2021 р. URL: <https://itd.rada.gov.ua/billInfo/Bills/Card/43424>).
10. Проект Закону про захист персональних даних № 8153 від 25.10.2022 р. URL: <https://itd.rada.gov.ua/billInfo/Bills/Card/40707>.
11. Opinion On The Draft Law Of Ukraine “On Personal Data Protection” (No. 8153 as of 25 october 2022) by 24 April 2023: Council of Europe Project “Supporting Implementation of the European Human Rights Standards in Ukraine” URL: <https://rm.coe.int/opinion-on-the-draft-law-on-personal-data-protection-in-ukraine-final-/1680ab9e06>.
12. Kuner Ch., Jerker D., Svantesson B., Fred H. Cate, Lynskey O., Millard Ch. The global data protection implications of ‘Brexit’. *International Data Privacy Law*. 2016. Vol. 6, Issue 3. P. 167–169. <https://doi.org/10.1093/idpl/ipw018>.
13. Veronese A., Silveira A., Lemos Igreja R., Lopes Espiñeira Lemos A. N., & Guimarães Moraes T. The concept of personal data protection culture from European Union documents: a “Brussels effect” in Latin America?. *UNIO – EU Law Journal*. 2023. Vol. 9, No. 1. P. 58–79. DOI: 10.21814/unio.9.1.5299.
14. Veronese A., Silveira A., Lemos Igreja R., Lopes Espiñeira Lemos A. N., & Guimarães Moraes T. The influence of European Union per-

- sonal data protection standards in Latin America from the perspective of social actors and Latin American authorities. *UNIO – EU Law Journal*. 2023. Vol. 9, No. 2. P. 118–138. DOI: 10.21814/unio.9.2.5531.
15. Belli L., Doneda D. Data protection in the BRICS countries: legal interoperability through innovative practices and convergence. *International Data Privacy Law*. 2023. Volume 13. Issue 1. P. 1–24. DOI: 10.1093/idpl/ipac019.
 16. Czerniawski M., Svantesson D. J. B. Dataskyddet 50 år – Historia, aktuella problem och framtid. In M. Brinnen, C. M. Sjöberg, D. Törngren, D. Westman, & S. Öman (Eds.). *Dataskyddet 50 år – historia, aktuella problem och framtid*. 2023. P. 127–153. URL: <https://research.bond.edu.au/en/publications/dataskyddet-50-%C3%A5r-historia-aktuella-problem-och-framtid>.
 17. Petkova B. Domesticating the “foreign” in making transatlantic data privacy law. *International Journal of Constitutional Law*. 2017. Volume 15, Issue 4. P. 1135–1156. DOI: 10.1093/icon/mox079.
 18. Olukunle Oladipupo Amoo, Akoh Atadoga, Femi Osasona, Temitayo Oluwaseun Abrahams, Benjamin Samson Ayinla, Oluwatoyin Ajoke Farayola. GDPR's impact on cybersecurity: A review focusing on USA and European practices. *International Journal of Science and Research Archive*. 2024. № 11(01). P. 1338–1347. DOI: 10.30574/ijrsra.2024.11.1.0220.
 19. Kuner Ch., Jerker D., Svantesson B., Cate Fred H, Lynskey O., Millard Ch., Loideain N. The GDPR as a chance to break down borders. *International Data Privacy Law*. 2017. Vol. 7. Issue 4. P. 231–232. DOI: 10.1093/idpl/ix023.
 20. Alshaleel Mohammed Khair. The Extraterritoriality of the GDPR and Its Effect on GCC Businesses. *Global Journal of Comparative Law*. 2024. https://www.researchgate.net/publication/376199051_The_Extraterritoriality_of_the_GDPR_and_Its_Effect_on_GCC_Businesses.
 21. Corning G. P. The diffusion of data privacy laws in Southeast Asia: learning and the extraterritorial reach of the EU's GDPR. *Contemporary Politics*, 2024. P. 1–22. DOI: 10.1080/13569775.2024.2310220.
 22. Anh D. Enhancing the Responsibilities of Data Controllers in Vietnam: Insights from the European General Data Protection Regulation. *VNU Journal Of Science: Legal Studies*. 2024. 40(1). DOI: 10.25073/2588-1167/vnuls.4610.

Chvankin S. Extraterritorial impact of the General Data Protection Regulation (GDPR)

Summary. The article examines the impact of the General Data Protection Regulation not only on the legislation

of EU member states, but also on the legislation of third countries.

It is noted that all member states are bound by EU law, but there may be differences in how each national legal system provides effective protection, which can be explained by the distinct legal tradition and specificity of the legal system and governing bodies in each country. By virtue of national autonomy, national regulation should ensure, on the one hand, a procedure adapted to the specific needs of member states, and on the other hand, an effective tool for achieving harmonized application of the law throughout the EU. The autonomy of the member states is not absolute and must be implemented in the general direction of the Regulation and subject to the principles of equivalence, efficiency, and sincere cooperation.

The significant impact of the Regulation on Ukraine as a candidate country for joining the EU was noted, because it is a direct requirement of the Association Agreement between Ukraine and the EU, under which the parties agreed to cooperate in order to ensure an adequate level of personal data protection in accordance with the highest European and international standards.

The influence of the EU and its legal provisions in the formation of national legal frameworks can be found not only in the countries of geographical Europe, both those that have the status of a candidate for EU membership and those that adhere to the non-aligned status, but also on law and order in other countries, in particular, Argentina, Bahrain, Brazil, Qatar, Mexico, UAE, Oman, Saudi Arabia, USA, Chile, etc.

It was concluded that the EU legislation on the protection of personal data has a significant impact on the legislation of third countries. Since the EU is one of the largest economic blocs in the world, GDPR requirements have become a standard in the field of personal data protection and require third countries to adapt their legislation to comply with these standards when processing data of European citizens. This has resulted in a significant number of countries revising their data protection legislation to comply with GDPR requirements, even where there is no regulatory obligation to harmonize legislation. This is due to the so-called “Brussels effect” – the desire of third countries and their resident companies to gain access to the economic instruments and markets of Europe.

Key words: General Data Protection Regulation, GDPR, personal data protection, extraterritorial jurisdiction, Brussels effect, harmonization, European Union.