УДК 341.9:341.17:342.738
DOI https://doi.org/10.32782/2307-1745.2026.83.31

Микитенко В. С.,
аспірант кафедри права Європейського Союзу
Національного юридичного університету імені Ярослава Мудрого
ORCID: https://orcid.org/0009-0005-2004-5024

ФРАГМЕНТАЦІЯ ПРАВОВОГО РЕЖИМУ ОСОБЛИВИХ (ЧУТЛИВИХ) КАТЕГОРІЙ ПЕРСОНАЛЬНИХ ДАНИХ У ЄС: КОЛІЗІЙНО-ПРАВОВИЙ ВИМІР

Анотація. Стаття присвячена дослідженню фрагментації правового режиму чутливих персональних даних у праві Європейського Союзу та її наслідків для внутрішнього ринку. Доведено, що мета GDPR щодо усунення розрізненості національних режимів часів Директиви 95/46/ЄС у сфері чутливих даних досягнута лише частково. Надання державам-членам права встановлювати власні обмеження на обробку генетичних, біометричних і медичних даних (ст. 9(4)), а також інформації про працівників і наукові дослідження, фактично призвело до повторної фрагментації законодавства. Водночас колізійну норму Директиви 95/46/ЄС не було перенесено до GDPR: його ст. 3 визначає лише територіальну сферу дії самого Регламенту, але не вказує, право якої саме країни застосовується там, де залишено простір для національної нормотворчості. На основі аналізу національного законодавства, ухваленого на підставі застережних положень GDPR у Німеччині, Франції, Польщі, Данії та Нідерландах, а також звітів інституцій ЄС показано, що ця фрагментація поглиблюється через розбіжну практику наглядових органів і невизначеність щодо застосовного права. Для внутрішнього ринку це означає нерівні умови конкуренції саме в тому сегменті, де до контролерів висуваються найсуворіші вимоги, а свобода вибору місця заснування створює для них стимул віддавати перевагу юрисдикціям із менш обтяжливим режимом. Сама по собі розбіжність національних матеріальних режимів відповідає принципу субсидіарності, однак вона не пояснює відсутності в праві ЄС колізійних норм, які розмежовували б сфери їхньої дії. У роботі критично проаналізовано три доктринальні підходи до вирішення колізійного питання (місце фактичної присутності контролера, lex loci laboris та звичайне місце проживання суб'єкта даних), оцінено значення рішення Суду ЄС у справі C-34/21, а також розглянуто деліктний вимір проблеми (зокрема, ризики forum shopping через розрив між юрисдикцією та застосовним правом). Доведено, що навіть пакет Digital Omnibus не усуває цю колізійну прогалину. Запропоновано відновити в GDPR колізійну норму як функціональний аналог ст. 4 Директиви, що поєднував би загальний критерій місця фактичної присутності контролера із захисними правилами для відносин зі слабшою стороною. Визначено значення результатів для України: показано, що гармонізація законодавства за моделлю GDPR імпортує і його структурні дефекти, проте пізніший старт реформи дає українському законодавцю змогу заздалегідь усунути цю правову невизначеність.

Ключові слова: чутливі персональні дані, особливі категорії персональних даних, GDPR, застережні положення, колізійна норма, застосовне право, внутрішній ринок ЄС, гармонізація законодавства України.

Постановка проблеми. Ухвалення Загального регламенту про захист даних (GDPR) [1] мало покласти край розрізненості національних режимів захисту персональних даних, що склалася за понад два десятиліття дії Директиви 95/46/ЄС [2]. Вибір правової форми був принциповим, адже регламент підлягає прямому застосуванню в усіх державах-членах і тому мав гарантувати тотожність правил у всіх державах-членах. Мета акта подвійна: захист фундаментальних прав фізичних осіб та вільний рух персональних даних, який у межах Союзу згідно зі ст. 1(3) не може бути обмежений з міркувань, пов'язаних із захистом фізичних осіб [1]. GDPR, отже, від початку замислювався як інструмент внутрішнього ринку, покликаний усунути регуляторні бар'єри та вирівняти умови конкуренції для контролерів і операторів персональних даних.

Щодо чутливих даних, або, в термінології GDPR, особливих категорій персональних даних, уніфікаційний задум реалізовано лише частково. Стаття 9(4) GDPR прямо уповноважує держави-члени зберігати або запроваджувати додаткові умови, у тому числі обмеження, щодо обробки генетичних, біометричних даних і даних стосовно здоров'я [1]. Подібні застереження містять ст. 88 (обробка даних працівників) та ст. 9(2)(j) у поєднанні зі ст. 89(1) (наукові дослідження).

Проблема, однак, не зводиться до неповноти гармонізації. Директива 95/46/ЄС містила у ст. 4 спеціальне правило визначення застосовного національного права у сфері захисту персональних даних [2]. Це не була класична двостороння колізійна норма: ст. 4 не обирала між правопорядками на основі нейтральної прив'язки, а визначала просторову сферу застосування національного законодавства, ухваленого на виконання Директиви. Функціонально вона все ж виконувала колізійно-алокативну роль, дозволяючи встановити, законодавство якої держави-члена регулює конкретну транскордонну обробку, тож надалі характеризуємо її як односторонню колізійну норму. GDPR аналогічної норми не має: його ст. 3 окреслює лише територіальну сферу застосування самого Регламенту, тобто визначає чи застосовується GDPR як такий. Наслідком стало парадоксальне становище, за якого інструмент, покликаний усунути фрагментацію, у сфері чутливих даних її відтворив і водночас ліквідував механізм, який цю фрагментацію принаймні впорядковував. Для роботодавців, страховиків, медичних і дослідницьких установ це означає правову невизначеність у цілком типових транскордонних ситуаціях. Актуальності темі додають визнання фрагментації у другому звіті Комісії про застосування GDPR [3; 4] та розпочатий наприкінці 2025 р. перегляд Регламенту в межах пакета

Digital Omnibus [5], який ані ст. 9(4), ані колізійної прогалини не торкається.

Стан дослідження. У зарубіжній доктрині вагоме значення для цієї статті мають праці К. Чакарової [7], К. Пормейстер [8], Г. Абрахи [17], М. Свєрчинського [18] та М. Бркан [20]. Порівняльний вимір представлений колективною монографією за редакцією К. Мак-Каллах, О. Тамбу та С. Буртона [10] і дослідженнями на замовлення інституцій ЄС [12]. У вітчизняній науці розглядаються переважно питання адаптації українського законодавства до acquis ЄС (К. Боднар [28], О. Яворська [29]), тоді як колізійний вимір обробки чутливих даних усередині Союзу залишається практично недослідженим.

Метою статті є розкриття нормативного механізму фрагментації правового режиму чутливих персональних даних у ЄС, оцінка її наслідків для внутрішнього ринку, визначення підходів до вирішення питання застосовного права при транскордонній обробці, а також з'ясування значення виявленої фрагментації для гармонізації українського законодавства із законодавством ЄС у сфері захисту персональних даних.

Виклад основного матеріалу. Відповідно до ст. 288 ДФЄС регламент є обов'язковим у повному обсязі та підлягає прямому застосуванню в усіх державах-членах [6], тож заміна директиви регламентом подавалася як спосіб остаточно усунути розбіжності, породжені неоднаковою транспозицією. Проте GDPR став продуктом компромісу з державами-членами, які прагнули зберегти регуляторну автономію у чутливих сферах: трудових відносинах і охороні здоров'я, а також у науці. Юридичною формою компромісу стали застережні положення (opening clauses)[1], що уповноважують або зобов'язують держави-члени ухвалювати власне регулювання. Їх кількість у GDPR є безпрецедентною для регламенту, адже мова про кілька десятків норм, що делегують нормотворчість на національний рівень. Як зазначає К. Чакарова, через це GDPR нерідко характеризують як гібрид між регламентом і директивою, а обсяг делегування загрожує повторною фрагментацією правової бази ЄС у сфері захисту даних [7, с. 6, 88].

Для особливих категорій персональних даних ця фрагментація закладена не лише у ст. 9(4), а в самій нормативній архітектурі ст. 9 GDPR. Поряд із загальною забороною обробки таких даних у ст. 9(1) та переліком винятків у ст. 9(2), низка останніх прямо пов'язує допустимість або умови обробки з правом Союзу чи держав-членів. Це стосується, зокрема, трудового права та соціального забезпечення (ст. 9(2)(b)), істотного суспільного інтересу (ст. 9(2)(g)), охорони здоров'я (ст. 9(2)(h)–(i)) та наукових досліджень (ст. 9(2)(j) у поєднанні зі ст. 89). Крім того, ст. 9(2)(a) допускає встановлення правом Союзу або держави-члена випадків, коли заборона обробки не може бути знята згодою суб'єкта даних. Найвиразнішою формою такого національного регуляторного розсуду є ст. 9(4), яка прямо дозволяє державам-членам зберігати або запроваджувати додаткові умови, включно з обмеженнями, щодо обробки генетичних, біометричних даних та даних про здоров'я. Тому йдеться не про «мінімальну гармонізацію» у класичному значенні цього поняття, а про контрольований національний нормотворчий розсуд усередині застосовного регламенту [7, с. 32].

Неповнота гармонізації не була б настільки серйозною проблемою, якби правова система ЄС зберегла механізм упорядкування національних розбіжностей. У Директиві 95/46/ЄС він був: ст. 4 визначала застосовне національне право за критерієм осідку (establishment)[2] контролера, у контексті діяльності якого здійснювалася обробка персональних даних [2]. GDPR цієї норми не успадкував. Окремі елементи колишнього режиму територіальної дії трансформувалися у ст. 3 GDPR, однак функція цієї статті принципово інша: вона визначає територіальну сферу застосування самого Регламенту як безпосередньо застосовного акта права ЄС, а не здійснює розмежування сфер дії національного законодавства держав-членів [8, с. 715–716]. Це розмежування набуває особливого значення саме там, де GDPR залишає державам-членам простір для власних матеріально-правових вимог, адже висновок про застосовність Регламенту за ст. 3 ще не дає відповіді, приписи якої держави-члена регулюють конкретну обробку.

Особливого значення для розмежування цих нормативних площин набуває рішення Суду ЄС у справі C-191/15 Verein für Konsumenteninformation v Amazon EU [9]. Суд виходив із того, що питання права, застосовного до обробки персональних даних, має визначатися відповідно до спеціального правила ст. 4 Директиви 95/46/ЄС, а не лише на підставі загальних колізійних механізмів. Тим самим практика Суду підтвердила самостійну алокативну функцію ст. 4 у системі європейського міжнародного приватного права. Після скасування Директиви ця нормативна основа зникла, тож проблема полягає не у відсутності в GDPR текстуальної копії ст. 4, а у втраті самого механізму визначення застосовного національного законодавства у транскордонних ситуаціях.

Точкові відсилання до застосовного права в тексті все ж трапляються, але вони розрізнені, додаткових умов за ст. 9(4), 88 і 89 не охоплюють і конфлікту односторонніх національних норм між собою не знімають. К. Чакарова схиляється до того, що загальну колізійну норму пропущено ненавмисно: колізійні правила прибрали, не запропонувавши ні заміни, ні бодай орієнтирів [7, с. 7]. Найімовірніше, розробники мислили категоріями повної уніфікації, за якої колізійна норма справді не потрібна, але кілька десятків застережних положень цю передумову знімають. Наслідком стає або паралельна застосовність кількох національних законів із неоднаковими вимогами, або, якщо жоден із них не визначає сфери власної дії, утворюється прогалина, адже односторонні норми про просторову дію національні акти містять далеко не завжди [7, с. 79, 82, 84].

У Німеччині федеральний закон про захист даних (BDSG) у § 22 визначає власний перелік підстав обробки особливих категорій даних, а § 26 встановлює спеціальний режим обробки даних працівників на підставі ст. 88 GDPR, що дослідники оцінюють як відхилення від положень Регламенту, несумісне з його гармонізаційною метою [10, с. 31; 11]. Схожі відхилення фіксують і в інших державах-членах. Колективна монографія за редакцією К. Мак-Каллах, О. Тамбу та С. Буртона констатує, що більшість національних транспозицій GDPR залишаються неповними та викликають сумніви щодо відповідності самому Регламенту. Там само наведено попередження Європейської

[1] У контексті GDPR opening clauses слід розуміти не просто як застереження, а як положення Регламенту, які прямо залишають державам-членам нормативний простір для встановлення, конкретизації або збереження національного правового регулювання у певних питаннях.

[2] Осідок (establishment) контролера – під ним розуміється автономне поняття права ЄС, яке відповідно до практики Суду ЄС передбачає реальне й ефективне здійснення діяльності через стабільну організаційну присутність та не зводиться до місця реєстрації чи інкорпорації контролера.

Комісії, що відтворення чи доповнення положень Регламенту національним законодавцем повертає бізнес до незнання застосовних правил [10, с. 26]. Системність картини підтверджує дослідження для Генерального директорату Комісії з питань здоров'я (DG SANTE), яке охопило всі держави-члени. Його автори констатують, що відмінності у тлумаченні Регламенту та в національному законодавстві призвели до фрагментованого підходу, який ускладнює транскордонну співпрацю в медичній допомозі та дослідженнях [12, с. 9, 80]. Через ст. 9(4), зазначають вони, GDPR у сфері охорони здоров'я не застосовуватиметься однаково в кожній державі-члені: у Франції автоматизована обробка генетичних даних потребує авторизації, у Нідерландах вона за загальним правилом заборонена щодо даних, які не стосуються суб'єкта, від якого їх отримано, а Данія обмежила використання генетичної інформації роботодавцями та страховиками [12, с. 26, 30].

Хоча GDPR ґрунтується вже на спеціальній компетенції ст. 16 ДФЄС [6], вільний рух даних прямо визначено предметом Регламенту (ст. 1(1)), і за однакових правил контролери отримують єдине правове середовище, а сам Регламент, як зазначає Європейська Комісія, створює рівні умови конкуренції для бізнесу [3]. У сегменті чутливих даних цієї передумови немає, адже заборона обмежувати вільний рух даних за ст. 1(3) формально нікуди не поділася, тоді як однаковість застосовних правил зруйнована застережними положеннями.

Розбіжність між задумом і реальністю зафіксовано вже і в офіційних документах: у огляді Європейського Парламенту констатовано, що застережні положення та інтерпретаційні неоднозначності призвели до фрагментації, зокрема щодо умов обробки генетичних, біометричних даних і даних про здоров'я [4], що узгоджується з труднощами, про які повідомляють стейкхолдери у другому звіті Комісії про застосування GDPR [3]. Держави-члени схильні вважати певний ступінь фрагментації корисним, тоді як компанії, що працюють у кількох державах, повідомляють про неоднакові рівні захисту [4]. Другий рівень проблеми утворює правозастосовна практика, оскільки наглядові органи неоднаково тлумачать ключові поняття Регламенту, а деякі публікують настанови, що суперечать позиціям Європейської ради із захисту даних [4]. Для внутрішнього ринку це означає, що контролери, які самостійно обирають місце заснування, отримують стимул віддавати перевагу юрисдикції з найменш обтяжливим режимом. Сама по собі така розбіжність відповідає принципу субсидіарності, проте складність виникає на наступному кроці, адже право ЄС не визначає, регулювання якої держави-члена підлягає застосуванню. Наприклад, роботодавець, заснований у Німеччині, обробляє дані про здоров'я працівника, який дистанційно виконує роботу в Польщі. Застосовність самого GDPR сумнівів не викликає (ст. 3(1)), проте обидві держави скористалися застережними положеннями Регламенту. Німеччина ухвалила спеціальні режими § 22 і § 26 BDSG [11], а польський законодавець конкретизував правила обробки особливих категорій даних працівників, зокрема даних про здоров'я, у ст. 22^{1b} Кодексу праці [13], допустивши їх обробку на підставі згоди лише тоді, коли дані передано з ініціативи самого працівника. Відповідно, у роботодавця виникає логічне питання: дотримуватися німецьких вимог, польських чи обох одночасно.

Доктрина запропонувала щонайменше три підходи до визначення застосовного права, і кожен із них має істотні вади. Перший, оснований на критерії осідку контролера, продовжує логіку скасованої ст. 4 Директиви. К. Пормейстер розглядає можливість перенесення на нові умови позиції Суду ЄС у справі C-230/14 *Weltimmo* [14], за якої застосовним є право держави-члена, в контексті діяльності осідку якої здійснюється обробка. Такий критерій дає контролерові єдиний режим і передбачуваність, однак контролер у державі А, який не має осідку у державі Б, не підпадатиме під законодавство держави Б, навіть обробляючи чутливі дані її резидентів [8, с. 714, 718, 721, 723]. Працівник, відповідно, втрачає спеціальні гарантії власного правопорядку саме тоді, коли той свідомо їх посилив. До того ж ця конструкція виведена доктриною з практики тлумачення норми, якої більше не існує, і суд держави-члена не зобов'язаний її дотримуватися. Другий підхід, lex loci laboris, спирається на аналогію зі ст. 8 Регламенту Рим I, яка для трудових договорів вказує на право держави звичайного виконання роботи і захищає слабшу сторону [15]. Він системно послідовний, але переносить договірну колізійну норму на режими переважно публічно-правової, наглядової природи, а для роботодавця з персоналом у кількох державах означає стільки ж паралельних режимів адміністрування. Третій підхід, орієнтований на звичайне місце проживання суб'єкта даних, найповніше відповідає правозахисній меті Регламенту, однак множить паралельні режими за кількістю держав проживання працівників чи клієнтів.

До проблематики застережних положень долучився і Суд ЄС. У рішенні у справі C-34/21 *Hauptpersonalrat der Lehrerinnen und Lehrer* він визначив, що більш конкретні норми у розумінні ст. 88(1) GDPR мусять мати нормативний зміст, відмінний від загальних правил Регламенту, а національне законодавство, яке лише відтворює його умови або не задовольняє вимог ст. 88(2), не підлягає застосуванню, якщо тільки воно не може становити правової основи обробки за ст. 6(3) GDPR [16, п. 61, 82–84]. Г. Абраха підкреслює, що наслідки рішення є далекосяжними, оскільки несумісним з Регламентом виявляється і структурно подібний § 26(1) BDSG, а більшість національних норм про обробку даних працівників, нотифікованих Комісії за ст. 88(3) GDPR, навряд чи відповідатиме вимогам ст. 88 [17, с. 493–495]. Попри позитивний ефект рішення у вигляді обмеження нових національних винятків, його дія вичерпується перевіркою валідності норми, залишаючи відкритим питання визначення застосовного законодавства у разі конфлікту декількох легітимних режимів. У короткостроковій перспективі невизначеність навіть зростає, адже роботодавець як контролер мусить спершу оцінити чинність потенційно застосовних норм за критеріями Суду. Деякі держави-члени почали заповнювати прогалину односторонньо. Наприклад, оновлений французький закон про захист даних містить власну колізійну норму за критерієм місця проживання суб'єкта даних, яка здатна суперечити підходам інших держав і сама фрагментує територіальну сферу дії правил захисту даних [10, с. 56]. Унаслідок цього розбіжності виникають одночасно на двох рівнях: у матеріальних режимах чутливих даних і в національних підходах до визначення застосовного права.

Виявлена проблема має два взаємопов'язані, але юридично різні виміри, які не слід ототожнювати. Перший є регуляторним і полягає у визначенні просторової сфери дії національних спеціальних приписів, ухвалених державами-членами на підставі opening clauses GDPR. Саме цю функцію за режиму Директиви виконувала ст. 4. Другий виникає вже у приватноправовій пло-

щині, коли порушення правил захисту даних породжує вимогу про відшкодування шкоди та необхідно визначити право, застосовне до відповідного недоговірного зобов'язання. У цій площині постає питання співвідношення GDPR із системою європейського міжнародного приватного права, передусім Регламентом Рим II та національними колізійними нормами.

Третю, окрему площину становить міжнародна юрисдикція. Стаття 79(2) GDPR надає суб'єкту даних альтернативні юрисдикційні можливості, але визначення компетентного суду не тотожне визначенню права, яке цей суд має застосовувати. Саме відсутність необхідного паралелізму між forum та ius робить проблему особливо складною.

У контексті деліктної площини порушення національних специфікацій породжує вимоги про відшкодування шкоди за ст. 82 GDPR, однак Регламент, як констатує М. Свєрчинський, містить лише норми міжнародного цивільного процесу, а не колізійне регулювання, тож суди змушені звертатися до національного міжнародного приватного права [18, с. 40, 43]. Регламент Рим II тут не допомагає, оскільки прямо виключає зі своєї сфери позадоговірні зобов'язання, що виникають із порушень приватності та прав особистості [19]. До них, зокрема, доктриною відноситься і захист персональних даних, хоча сам текст Регламенту про нього не згадує (і цю прогалину законодавець так і не заповнив) [20, с. 27–28]. При цьому доктриною пропонуються несумісні шляхи вирішення проблеми. М. Бркан, чий аналіз стосувався ще режиму Директиви 95/46/ЄС, розглядає два варіанти: або ст. 4 Директиви цілком лежить поза сферами дії Рим I і Рим II та застосовується самостійно, або співвідноситься з ними як lex specialis із lex generalis [20, с. 27–28], причому при скасуванні ст. 4 обидві конструкції втратили нормативну опору. У свою чергу М. Свєрчинський обґрунтовує пряму застосовність моделі Рим II, доводячи, що сформульоване задовго до GDPR виключення не охоплює порушень створеного ним режиму, хоч і визнає дискусійність такої позиції [18, с. 49, 52–55]. Додаткову невизначеність створює розрив між юрисдикцією та застосовним правом, на відсутність паралелізму між якими у сфері захисту даних, на відміну від споживчого права, звертає увагу М. Бркан [20, с. 15]. За ст. 79(2) GDPR суб'єкт даних може позиватися не лише в державі осідку контролера чи оператора, а й, альтернативно, у державі свого звичайного місця проживання, право якої, найімовірніше, не збігатиметься із застосовним, а сполучення сприятливих для позивача юрисдикційних правил із браком уніфікованих колізійних норм створює передумови для *forum shopping*, тобто обрання позивачем найзручнішого суду.

Шляхи розв'язання. Наявні пропозиції різняться глибиною втручання та адресованим рівнем проблеми. Тлумачний шлях представлений у роботі К. Чакарової застосовувати за аналогією правила визначення провідного наглядового органу за ст. 56 GDPR, вважаючи застосовним право держави цього органу [7, с. 87–88]. Вразливість підходу полягає в тому, що механізм провідного органу створений для розподілу наглядової компетенції, тож його перенесення в колізійну площину є доктринальною творчістю без опори в позитивному праві. Матеріально-правовий шлях, тобто точкову гармонізацію правил використання чутливих даних у дослідженнях на рівні ЄС, пропонує К. Пормейстер [8, с. 723]. Однак ухвалений у 2025 р. Регламент про Європейський простір даних про здоров'я (EHDS) показав межі цього напряму, адже його ст. 51(4) дозволяє державам-членам суворіші заходи щодо генетичних, епігеномних і геномних даних при вторинному використанні [21], відтворюючи логіку застережних положень на новому рівні. Міжнародно-приватноправовий шлях охоплює пропозицію М. Бркан доповнити Регламент Брюссель I bis спеціальною секцією про юрисдикцію у спорах щодо захисту даних [20, с. 24, 36–37] та вже згадане обґрунтування застосовності моделі Рим II, проте обидві пропозиції адресують юрисдикційний і деліктний шари, тоді як регуляторний потребує власного вирішення.

Запропоноване вирішення також потребує розмежування компетенційних підстав права ЄС. Якщо майбутня норма має визначати просторову сферу застосування національних спеціальних вимог, ухвалених на підставі GDPR, її функція залишається безпосередньо пов'язаною із системою захисту персональних даних, для якої спеціальну правову основу встановлює ст. 16 ДФЄС. Інша ситуація виникає щодо права, застосовного до цивільно-правових наслідків порушення таких вимог: у цій частині питання належить до сфери судового співробітництва у цивільних справах та колізійного регулювання, передбаченого ст. 81(2)(c) ДФЄС. Тому пропонований функціональний аналог ст. 4 Директиви доцільно розуміти насамперед як спеціальне правило просторового розмежування національних регуляторних режимів усередині GDPR, а не як універсальну колізійну норму для всіх приватноправових наслідків обробки персональних даних.

На нашу думку, доцільним було б відновлення в самому GDPR односторонньої колізійної норми як функціонального аналога ст. 4 Директиви, де загальний критерій осідку (establishment) контролера поєднувався б із захисними правилами для відносин зі слабшою стороною, насамперед трудових, за зразком ст. 8 Регламенту Рим I [15]. Від тлумачної аналогії, описаної в доктрині [7, с. 87–88], такий варіант відрізняється тим, що правило закріплюється в тексті самого Регламенту і діє як загальний критерій незалежно від наявності провідного органу, а захисний елемент стає складовою самої норми. Вирішальним при цьому є не вибір конкретного критерію з розглянутих вище, а сам факт його нормативного закріплення на рівні ЄС.

Нагода для такого вибору формально існує: пропозиція Комісії від 19 листопада 2025 р. передбачає звуження сфери посиленого захисту до даних, які безпосередньо розкривають чутливі характеристики особи [5], та нові винятки для чутливих даних, які без цілеспрямованого збирання залишково потрапляють до наборів даних систем штучного інтелекту, за умови суворих гарантій їх видалення чи невпливу на результати системи, і для біометричної верифікації під одноосібним контролем суб'єкта [22, с. 19]. У пропозиції Комісії стаття 9(4) при цьому залишається недоторканою, а колізійної норми для внутрішньосоюзних ситуацій пакет не запроваджує. Оцінки пакета полярні, проте в питанні узгодженості критики та прибічники сходяться. Організація noyb застерігає, що елементи запропонованого Комісією тексту, які залишають державам-членам простір для власного регулювання (national options), як-от передбачена запропонованою ст. 88c можливість запроваджувати вимогу згоди на обробку даних для цілей штучного інтелекту, самі здатні спричинити нову фрагментацію єдиного цифрового ринку [23, с. 79], а М. Барчентевич, підтримуючи новий виняток ст. 9(2)(k), констатує, що Комісія визнає потребу в послідовнішому та гармонізованішому правозастосуванні, не пропонуючи механізму, здатного це забезпечити [24, с. 2–3]. Отже, запропоновані зміни стосуються обсягу ст. 9, тоді як механізм ст. 9(4) і питання застосовного права залишаються поза межами перегляду.

Український вимір проблеми. Гармонізація законодавства про захист персональних даних з acquis ЄС є зобов'язанням України за Угодою про асоціацію [25] і набула додаткової ваги з отриманням статусу кандидата на членство. Чинний Закон України «Про захист персональних даних» 2010 р. [26] будувався ще на моделі Директиви 95/46/ЄС, а покликаний замінити його законопроєкт № 8153 [27] майже повністю відтворює архітектуру GDPR. На темп реформи впливає також внутрішній контекст. За спостереженням К. Боднар, євроінтеграційний регуляторний трек поступається пріоритетністю воєнному, і парламент ухвалив законопроєкт у першому читанні лише 20 листопада 2024 р., через два роки після подання [28, с. 425–426]. У світлі результатів цього дослідження українська перспектива потребує уточнення, оскільки, ухвалюючи закон за моделлю GDPR, Україна разом із гарантіями Регламенту переймає і його структурні дефекти. При цьому орієнтація на єдиний європейський стандарт обробки чутливих даних в значній мірі ілюзорна, адже він складається із загальної рамки GDPR і десятків національних спеціальних вимог, правила розмежування яких не визначені. Для українських контролерів, які оброблятимуть дані суб'єктів із держав-членів, відповідність майбутньому закону сама по собі не зніматиме питання про застосовність посилених вимог конкретних національних правопорядків, тож теза про усунення юридичних бар'єрів у співпраці з партнерами з ЄС [29, с. 119] справдиться лише з урахуванням фрагментованості самого європейського права. При цьому пізніший старт реформи дає українському законодавцеві певну перевагу – колізійну визначеність можна закласти заздалегідь, прямо окресливши в законі просторову сферу дії українських спеціальних вимог до обробки чутливих даних, чого свого часу не зробила більшість держав-членів.

Висновки. Фрагментація правового режиму чутливих персональних даних у ЄС має нормативно закладений характер. Внаслідок застережних положень статей 9(4), 88 та 9(2)(j) у поєднанні зі ст. 89(1) GDPR держави-члени отримали право посилювати вимоги Регламенту на національному рівні. Водночас, при скасуванні Директиви 95/46/ЄС, її колізійна норма (ст. 4) що визначала застосовне право конкретної країни не була відтворена в новому акті. Перехід від Директиви 95/46/ЄС до GDPR загалом істотно підвищив рівень уніфікації права захисту персональних даних у Союзі. Водночас у тих сферах, де GDPR свідомо зберіг простір для національного нормотворення, виникла специфічна асиметрія: матеріально-правова фрагментація була легітимована самим Регламентом, тоді як передбачений ст. 4 Директиви механізм визначення застосовного національного права не отримав функціонального аналога. Тому йдеться не про загальний регрес рівня гармонізації, а про регрес у механізмі координації залишкових національних режимів.

Розбіжності національних режимів зафіксовані доктриною та офіційними дослідженнями інституцій ЄС і стосуються ключових параметрів режиму, від підстав обробки до меж використання генетичної інформації і не обмежуються текстами національних законів, оскільки до них додаються розбіжна правозастосовна практика наглядових органів та неоднакові методи визначення застосовного права. Для внутрішнього ринку подібна конфігурація створює нерівні умови конкуренції саме на тому рівні, де до контролерів висуваються найсуворіші вимоги. І хоча принцип субсидіарності виправдовує розбіжності між матеріально-правовими режимами, він не пояснює, чому в праві ЄС відсутні колізійні норми для розмежування сфер їхньої дії.

Ядром виявленої проблеми є не відсутність у GDPR колізійного регулювання взагалі, а відсутність уніфікованого механізму розмежування просторової сфери дії національних спеціальних приписів, існування яких прямо допускається самим Регламентом. У цьому регуляторному вимірі доктрина пропонує декілька конкуруючих критеріїв – установу контролера, звичайне місце виконання роботи та звичайне місце проживання суб'єкта даних, – жоден з яких не отримав нормативного закріплення на рівні ЄС. Від цієї проблеми необхідно відмежовувати колізійне питання у власному міжнародно-приватноправовому значенні, яке виникає щодо цивільно-правових наслідків порушення правил захисту даних. Виключення окремих порушень приватності та прав особистості зі сфери Регламенту Рим II, альтернативні юрисдикційні підстави ст. 79(2) GDPR та відсутність необхідного паралелізму між forum і ius утворюють окремий, хоча й пов'язаний, рівень правової невизначеності. Саме розмежування цих двох площин дозволяє точніше визначити напрями реформування: регуляторна проблема потребує спеціального правила в GDPR щодо застосування національних специфікацій, тоді як приватноправовий деліктний вимір має вирішуватися засобами європейського міжнародного приватного права.

Реформа Digital Omnibus змінює обсяг матеріального захисту чутливих даних, залишаючи конструкцію ст. 9 (4) і колізійну прогалину поза межами перегляду, а елементи пакета, що допускають національні варіанти регулювання, здатні породити додаткову фрагментацію. Для України, що гармонізує законодавство за моделлю GDPR, це означає перенесення у національне право тих самих конструктивних вад. Водночас український законодавець може закласти колізійну визначеність заздалегідь, окресливши просторову сферу дії національних спеціальних вимог до обробки чутливих даних, й уникнути відтворення описаної правової невизначеності. Перспективи подальших досліджень пов'язані з опрацюванням конкретної моделі колізійного регулювання для GDPR, аналізом практики наглядових органів і судів держав-членів щодо визначення застосовного права та з'ясуванням форми, в якій відповідне правило доцільно закріпити в українському законодавстві.

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). *Official Journal of the European Union*. 2016. L 119. P. 1–88.
2. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. *Official Journal of the European Communities*. 1995. L 281. P. 31–50.
3. Second Report on the application of the General Data Protection Regulation : Report from the Commission to the European Parliament and the Council, COM(2024) 357 final of 25 July 2024 / European Commission. Brussels, 2024. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52024DC0357 (дата звернення: 29.07.2026).
4. Second report on the application of the GDPR : at a glance / European Parliamentary Research Service. Brussels, 2024. 2 p. URL: https://www.europarl.europa.eu/RegData/etudes/ATAG/2024/762475/EPRS_ATA(2024)762475_EN.pdf (дата звернення: 29.07.2026).
5. Proposal for a Regulation of the European Parliament and of the Council on the simplification of the digital legislative framework

(Digital Omnibus) : COM(2025) 837 final of 19 November 2025 / European Commission. Brussels, 2025. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52025PC0837 (дата звернення: 29.07.2026).
6. Consolidated version of the Treaty on the Functioning of the European Union. Official Journal of the European Union. 2016. C 202. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12016E/TXT (дата звернення: 29.07.2026).
7. Chakarova K. General Data Protection Regulation: Challenges Posed by the Opening Clauses and Conflict of Laws Issues. *Stanford-Vienna European Union Law Working Papers*. 2019. No. 41. URL: https://law.stanford.edu/wp-content/uploads/2019/11/chakarova_eulawwp41.pdf (дата звернення: 29.07.2026).
8. Pormeister K. Genetic research and applicable law: the intra-EU conflict of laws as a regulatory challenge to cross-border genetic research. *Journal of Law and the Biosciences*. 2018. Vol. 5. No. 3. P. 706–723. DOI: https://doi.org/10.1093/jlb/lsy023.
9. Judgment of the Court (Third Chamber) of 28 July 2016 in Case C-191/15 Verein für Konsumenteninformation v Amazon EU Sàrl, ECLI:EU:C:2016:612 / Court of Justice of the European Union.
10. National Adaptations of the GDPR / eds. K. Mc Cullagh, O. Tambou, S. Bourton. Luxembourg : Blogdroiteuropéen, 2019. 130 p. URL: https://hal.science/hal-03521416 (дата звернення: 29.07.2026).
11. Bundesdatenschutzgesetz vom 30. Juni 2017 / Bundesrepublik Deutschland. Bundesgesetzblatt. 2017. Teil I. S. 2097.
12. Assessment of the EU Member States' rules on health data in the context of the GDPR / European Commission. Luxembourg : Publications Office of the European Union, 2021. URL: https://health.ec.europa.eu/system/files/2021-02/ms_rules_health-data_en_0.pdf (дата звернення: 29.07.2026).
13. Ustawa z dnia 26 czerwca 1974 r. – Kodeks pracy. Dziennik Ustaw. 1974. Nr 24, poz. 141 (z późn. zm.).
14. Judgment of the Court (Third Chamber) of 1 October 2015 in Case C-230/14 Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság, ECLI:EU:C:2015:639 / Court of Justice of the European Union.
15. Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I). *Official Journal of the European Union*. 2008. L 177. P. 6–16.
16. Judgment of the Court (First Chamber) of 30 March 2023 in Case C-34/21 Hauptpersonalrat der Lehrerinnen und Lehrer beim Hessischen Kultusministerium v Minister des Hessischen Kultusministeriums, ECLI:EU:C:2023:270 / Court of Justice of the European Union.
17. Abraha H.H. Hauptpersonalrat der Lehrerinnen: Article 88 GDPR and the Interplay between EU and Member State Employee Data Protection Rules. *The Modern Law Review*. 2024. Vol. 87. No. 2. P. 484–496. DOI: https://doi.org/10.1111/1468-2230.12849.
18. Świerczyński M. Prawo właściwe dla zobowiązań deliktowych wynikających z naruszenia zasad ochrony danych osobowych przyjętych w RODO. *Problemy Prawa Prywatnego Międzynarodowego*. 2020. T. 27. S. 39–59. DOI: https://doi.org/10.31261/PPPM.2020.27.02.
19. Regulation (EC) No 864/2007 of the European Parliament and of the Council of 11 July 2007 on the law applicable to non-contractual obligations (Rome II). *Official Journal of the European Union*. 2007. L 199. P. 40–49.
20. Brkan M. Data Protection and European Private International Law. Florence : European University Institute, 2015. 37 p. (EUI Working Paper RSCAS ; 2015/40). URL: https://hdl.handle.net/1814/36335 (дата звернення: 29.07.2026).
21. Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847. *Official Journal of the European Union*. 2025. L, 2025/327.
22. Skiotytė G., Sadauskaitė A. A Digital Omnibus: Identifying Interlinks and Possible Overlaps Between Different Legal Acts in the Field of Digital Legislation to Streamline Tech Rules : study requested by the IMCO Committee / European Parliament, Policy Department for Economy and Growth. Brussels, 2026. URL: https://www.europarl.europa.eu/RegData/etudes/STUD/2026/772641/ECTI_STU(2026)772641_EN.pdf (дата звернення: 29.07.2026).
23. Digital Omnibus Report V3: Analysis of Select GDPR and ePrivacy Proposals by the Commission / noyb – European Center for Digital Rights. Vienna, 2026. URL: https://noyb.eu/en/digital-omnibus-report-v3-analysis-select-gdpr-and-eprivacy-proposals-commission (дата звернення: 29.07.2026).
24. Barczentewicz M. ICLE Comments to the European Commission on GDPR and ePrivacy in the Digital Omnibus. *International Center for Law & Economics* : веб-сайт. 2026. URL: https://laweconcenter.org/resources/icle-comments-to-the-european-commission-on-gdpr-and-eprivacy-in-the-digital-omnibus/ (дата звернення: 29.07.2026).
25. Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони : Міжнародний документ від 27.06.2014 р. URL: https://zakon.rada.gov.ua/laws/show/984_011 (дата звернення: 29.07.2026).
26. Про захист персональних даних : Закон України від 01.06.2010 р. № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17 (дата звернення: 29.07.2026).
27. Про захист персональних даних : проєкт Закону України від 25.10.2022 р. № 8153 (прийнятий за основу 20.11.2024 р.). URL: https://itd.rada.gov.ua/billInfo/Bills/Card/40707 (дата звернення: 29.07.2026).
28. Bodnar K. Regulatory Adaptation of Personal Data Protection Standards to Hybrid Threats in the EU and Ukraine. *Pressing Problems of Public Administration*. 2025. No. 2 (67). P. 419–436. DOI: https://doi.org/10.26565/1684-8489-2025-2-21.
29. Яворська О.С. Захист персональних даних у цифровому середовищі: досвід ЄС. *Юридичний науковий електронний журнал*. 2024. № 9. С. 117–119. https://doi.org/10.32782/2524-0374/2024-9/26.

Mykytenko V. Fragmentation of the legal regime for special (sensitive) categories of personal data in the EU: the conflict-of-laws dimension

Summary. This article investigates the fragmentation of the legal regime governing sensitive personal data in European Union law and its consequences for the internal market. It argues that the GDPR's goal to eliminate the divergence of national regimes originating from Directive 95/46/EC regarding sensitive data has been only partially achieved. Granting Member States the right to introduce their own restrictions on the processing of genetic, biometric, and health data (Art. 9(4)), as well as data concerning employment and scientific research, has effectively led to the re-fragmentation of the legislation. Concurrently, the conflict-of-laws rule from Directive 95/46/EC was not transposed into the GDPR: Article 3 only defines the territorial scope of the Regulation itself, without specifying which country's law applies in areas where room for national rulemaking is retained. Based on an analysis of national adaptations (in Germany, France, Poland, Denmark, and the Netherlands) and reports from EU institutions, the study demonstrates that this fragmentation is exacerbated by the divergent practices of supervisory authorities and uncertainty regarding the applicable law. For the internal market, this entails unequal conditions of competition precisely in the segment where the most stringent requirements are imposed on controllers, while the freedom to choose the place of establishment gives them an incentive to favour jurisdictions with a less burdensome regime. The divergence of national

substantive regimes is itself consistent with the principle of subsidiarity; it does not, however, explain the absence in EU law of conflict-of-laws rules delimiting their respective scopes. The paper critically analyzes three doctrinal approaches to resolving the conflict-of-laws issue (the place of the controller's actual establishment, lex loci laboris, and the habitual residence of the data subject), evaluates the significance of the CJEU ruling in Case C-34/21, and considers the tort dimension of the problem (particularly the risks of forum shopping due to the disconnect between jurisdiction and applicable law). It is demonstrated that even the Digital Omnibus package fails to eliminate this conflict-of-laws gap. The article proposes restoring a conflict-of-laws rule in the GDPR as a functional analogue to Article 4 of the Directive, which would combine the general criterion of the controller's place of establishment with protective rules for relations involving a weaker party. Finally, the implications of these findings for Ukraine are outlined: it is shown that harmonizing legislation following the GDPR model also imports its structural defects; however, the delayed start of the reform affords the Ukrainian legislator the opportunity to preemptively address this legal uncertainty.

Key words: sensitive personal data, special categories of personal data, GDPR, opening clauses, conflict-of-laws rule, applicable law, EU internal market, harmonisation of Ukrainian legislation.

Стаття поширюється на умовах ліцензії відкритого доступу (CC BY 4.0)

Використання штучного інтелекту. Під час підготовки статті інструменти штучного інтелекту використовувалися виключно для мовного редагування, перевірки граматики, перекладу або інших допоміжних завдань, без використання згенерованих ними об'єктів як результатів академічної діяльності.

Дата першого надходження статті до видання: 14.08.2026
Дата прийняття статті до друку після рецензування: 10.09.2026
Дата публікації (оприлюднення) статті: 09.11.2026