УДК 349.22+342.721
DOI https://doi.org/10.32782/1813-338X-2025.3.19

С. А. Чванкін
доктор юридичних наук, доцент,
голова Київського районного суду м. Одеси
ORCID ID: 0000-0002-9800-854X

ДО ПИТАННЯ СПІВВІДНОШЕННЯ ЗАГАЛЬНОГО РЕГЛАМЕНТУ ПРО ЗАХИСТ ДАНИХ (GDPR) ТА ЗАКОНУ ЄС ПРО ШТУЧНИЙ ІНТЕЛЕКТ

У статті досліджено взаємозв'язок між двома ключовими регуляторними актами Європейського Союзу – Загальним регламентом про захист даних (GDPR) та Законом ЄС про штучний інтелект (Artificial Intelligence Act, AIA), що разом формують правову основу цифрового простору ЄС.

Розглядається питання гармонізації їхніх положень, визначаються потенційні сфери конфлікту, дублювання чи взаємного доповнення норм. Зазначено, що попри спільну мету – забезпечення захисту прав людини в умовах цифровізації – ці документи спираються на різні підходи: GDPR зосереджується на захисті персональних даних і приватності, тоді як Закон ЄС про штучний інтелект – на контролі ризиків, безпеці та етичності систем ШІ.

У ході аналізу показано, що GDPR не регулює ШІ безпосередньо, оскільки був прийнятий до появи спеціального законодавства у цій сфері. Водночас його принципи – законність, обмеження мети, мінімізація даних та заборона автоматизованих рішень – впливають на розробку та застосування ШІ-технологій. Закон про ШІ запроваджує ризик-орієнтований підхід до використання алгоритмів та зміцнює відповідальність розробників, але не завжди узгоджується з положеннями GDPR щодо обробки персональних даних. У роботі виокремлено проблему фрагментації регулювання, яка виникає через паралельний розвиток правових режимів захисту даних та регулювання ШІ.

Підкреслюється, що GDPR може бути витлумаченим та застосованим у спосіб, який не перешкоджає використанню ШІ, а допомагає узгодити інновації з етичними та правовими принципами ЄС.

Зроблено висновок, що GDPR та Закон ЄС про штучний інтелект слід розглядати не як взаємовиключні, а як взаємодоповнюючі інструменти регулювання. Їх співіснування потребує подальшого уточнення через судову практику та практичне застосування у галузях з високими технологічними ризиками. Підкреслюється провідна роль Європейського Союзу у формуванні етико-правових стандартів цифрової економіки та необхідність створення синергії між захистом персональних даних і розвитком штучного інтелекту.

Ключові слова: *GDPR, Закон ЄС про штучний інтелект, штучний інтелект, персональні дані, право на приватність, Європейський Союз, цифрове право, захист даних.*

Постановка проблеми. Попри постійне оновлення як національного законодавства, так і законодавства ЄС щодо запровадження нових правил регулювання штучного інтелекту (далі – ШІ) модель взаємодії між різними регуляторними актами у європейському просторі традиційно залишається дискусійною. Проблема фрагментації права на національному, наднаціональному та міжнародному рівні, конкуренція законодавства різних рівнів спонукає законодавців до ухвалення універсальних актів, якими намагаються охопити якомога більшу сферу відносин на шкоду деталізації регулювання. Причинами цього явища є, головним чином, зростання технічної складності кожної галузі, динамічний технологічний прогрес та потреба у вузькій фаховій експертизі. Водночас постає необхідність подолання цієї фрагментації, особливо тоді, коли різні галузі права розвиваються паралельно, розглядаючи подібні проблеми, але з різних юридичних позицій.

Аналіз останніх досліджень і публікацій. Різним аспектам співвідношення Загального регламенту про захист даних (GDPR) та Закону ЄС про штучний інтелект приділялася увага у дослідженнях Р. Браун, Дж. Трубі, І.А. Ібрагім

(R. Brown, J. Truby, I.A. Ibrahim), які здійснили критичний аналіз прогалин між GDPR та пропозиціями Закону ЄС про штучний інтелект. Дж. Сартор (Giovanni Sartor) ще до прийняття спеціального законодавства ЄС про штучний інтелект досліджував вплив GDPR на застосування технологічних рішень у сфері ШІ. Однак практика співвідношення обох актів ще не напрацьована і залишає вільний простір для дискусій.

Метою статті є всебічний аналіз взаємозв'язку, узгодженості та потенційних точок конфлікту між Загальним регламентом про захист даних 2016 року (далі – GDPR) та Законом ЄС про штучний інтелект (Artificial Intelligence Act, AIA), із з'ясуванням того, яким чином ці два регуляторні акти впливають один на одного, чи створюють ризики фрагментації правового регулювання цифрового середовища Європейського Союзу та засади гармонізації їх застосування, що можуть забезпечити баланс між захистом прав людини та розвитком інновацій.

Завданням дослідження є: а) охарактеризувати нормативно-правову природу та предметне спрямування GDPR і Закону ЄС про штучний інтелект, визначивши їхню роль у формуванні цифрового правопорядку ЄС; б) проаналізувати підходи інституцій ЄС до регулювання ШІ, включаючи резолюції Європейського Парламенту та пропозиції Європейської Комісії, стосовно взаємодії з GDPR та розкрити проблему фрагментації правового регулювання, яка виникає через паралельний розвиток законодавства про захист даних і законодавства про ШІ; в) оцінити вплив базових принципів GDPR (законності, обмеження мети, мінімізації даних, пропорційності, заборони необґрунтованих автоматизованих рішень) на розробку, навчання та застосування систем ШІ; г)сформулювати висновки щодо оптимальної моделі співіснування двох регуляторних режимів та визначити, чи потребує будь-який із них змін для ефективного правового врегулювання ШІ в ЄС.

Виклад основного матеріалу. 14 квітня 2016 року Парламент Європейського Союзу та Рада Європейського Союзу ухвалили Загальний регламент про захист даних 2016 року, який набрав чинності 25 травня 2018 року як регламент ЄС (замість директиви) [1]. GDPR безпосередньо застосовується і має силу закону сам по собі без необхідності транспозиції та вважається одним із найсуворіших законів про конфіденційність та безпеку даних у світі. Як наголошувалося раніше, 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 [2, с. 158].

Співвідношення захисту персональних даних із технологіями штучного інтелекту опинилось у сфері уваги інституцій ЄС одразу після запровадження GDPR: Резолюцією Європейського Парламенту від 16 лютого 2017 року з рекомендаціями Комісії щодо норм цивільного права з робототехніки (2015/2103(INL)), серед іншого, було підкреслено, що все ще потребують подальшого вирішення аспекти доступу до даних та захисту персональних даних і конфіденційності, враховуючи, що проблеми конфіденційності можуть виникати через взаємодію програм і пристроїв один з одним та з базами даних без втручання людини [3]. Наскрізне для європейського правового простору право на повагу до приватного життя та захист персональних даних, закріплене у статтях 7 та 8 Хартії та у статті 16 Договору про функціонування Європейського Союзу, застосовується до всіх сфер робототехніки, а правові засади ЄС щодо захисту даних має бути повністю дотримані.

Наступною Резолюцією Європейського Парламенту з рекомендаціями Комісії щодо режиму цивільної відповідальності за штучний інтелект (2020/2014(INL)) від 20 жовтня 2020 року наголошено на важливості визначення чіткого та гармонізованого режиму цивільної відповідальності в Європі за розробку технологій штучного інтелекту, а також продуктів і послуг, які отримують від них користь, з метою забезпечення належної правової визначеності для виробників, операторів, постраждалих осіб та інших третіх сторін [4]. За аналогією з інспекторами із захисту даних за GDPR, розробники ШІ, зареєстровані як в межах Союзу, так і за його межами, будуть зобов'язані призначити представника з питань відповідальності за шкоду, завдану штучним інтелектом у Союзі.

У сфері штучного інтелекту інституції ЄС розробили низку документів, в яких окреслено основні пріоритети. Ці пріоритети включають стимулювання технологічного та промислового потенціалу ЄС, контрольоване поширення штучного інтелекту в різних секторах економіки, підготовку до очікуваних соціально-економічних змін, викликаних запровадженням ШІ, розробку відповідних етичних та правових стандартів, заснованих на цінностях ЄС. Шлях на

запровадженні гармонізованого регулювання можна відраховувати від розробленої Європейською Комісією Пропозиції щодо регламенту Європейського Парламенту та Ради, що встановлює гармонізовані правила щодо штучного інтелекту (Закон про штучний інтелект) та внесення змін до деяких законодавчих актів Союзу (COM(2021) 206 final, 2021/0106(COD)) [5].

Одразу ж постало питання забезпечення узгодженість з Хартією основних прав ЄС та чинним вторинним законодавством Союзу щодо захисту даних, захисту прав споживачів, недискримінації та гендерної рівності. Розробники зазначали, що пропозиція не обмежує, а навпаки, доповнює Загальний регламент про захист даних (Регламент (ЄС) 2016/679) та Директиву про правоохоронну діяльність (Директива (ЄС) 2016/680) набором гармонізованих правил, що застосовуються до проектування, розробки та використання певних систем ШІ з високим рівнем ризику, та обмежень на певні види використання систем дистанційної біометричної ідентифікації, а також не обмежує застосування законодавства Союзу про конкуренцію.

Резолюція Європейського Парламенту від 20 жовтня 2020 року з рекомендаціями Комісії щодо рамкових етичних аспектів штучного інтелекту, робототехніки та пов'язаних з ними технологій (2020/2012(INL)) вважає, що чинна правова база Союзу, зокрема щодо захисту, конфіденційності та персональних даних, повинна повністю застосовуватися до штучного інтелекту, робототехніки та пов'язаних з ними технологій, і її необхідно регулярно переглядати та ретельно перевіряти, а також оновлювати за необхідності, щоб ефективно боротися з ризиками, створюваними цими технологіями, і в цьому відношенні вона могла б отримати користь від доповнення надійними керівними етичними принципами; зазначає, що там, де прийняття правових актів було б передчасним, слід використовувати систему м'якого права; будь-які технології штучного інтелекту, робототехніки та пов'язані з ними технології, включаючи програмне забезпечення, алгоритми та дані, що використовуються або виробляються такими технологіями, розроблені, розгорнуті та використані в Союзі, повинні повністю поважати права громадян Союзу на конфіденційність та захист персональних даних здійснюється відповідно до Регламенту (ЄС) 2016/679 та Директиви 2002/58/ЄС.

Як вказується, використання ШІ не вимагає вносити зміни до GDPR, а будь-яке нове нормативне регулювання ще більше ускладнить його впровадження, і саме майбутня судова практика буде уточнювати особливості застосування GDPR до технологій штучного інтелекту [6, с. 53].

Згадана Резолюція 2020/2012(INL) зазначає, що з метою аналізу впливу штучного інтелекту, робототехніки та пов'язаних з ними технологій на споживачів, доступ до даних може бути, за умови повного дотримання законодавства Союзу, такого як законодавство щодо захисту даних, конфіденційності та комерційної таємниці, поширений на національні компетентні органи. Ефективну транскордонну співпрацю можна досягти лише за умови, що всі зацікавлені сторони, серед іншого, зобов'яжуться дотримуватися встановлених принципів конфіденційності, управління даними та захисту даних, зокрема тих, що закріплені в Регламенті (ЄС) 2016/679 [7].

13 березня 2024 року Парламент Європейського Союзу ухвалив перший у світі закон, що регулює штучний інтелект – Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (далі – Закон ЄС про штучний інтелект, AIA) [8]. Хоча обидва регламенти мають спільну мету захисту прав осіб, їхні конкретні сфери застосування та вимоги до дотримання приватності, актуалізують питання щодо їхньої потенційної взаємодії: від моделі посилення сукупного регуляторного впливу на учасників відносин (від споживачів до IT-гігантів) до моделі протидії та зіткнення сфер регулювання, що призведе до фрагментації захисту права на приватність, уповільненню прогресу цифрових технологій.

Однак деякі науковці все ж визначають потенційний недолік Закону ЄС про штучний інтелект щодо сумісності та узгодженості з існуючим регуляторним ландшафтом, адже нова регуляція не робить значного внеску у чинне законодавство, також може суперечити або бути несумісною з іншими нормативними актами, а потенційний вплив дублювання нормативних актів залишається невизначеним, і очікуються конфлікти між регуляторними стандартами ЄС [9, с. 7]. Як зазначають Рафаель Браун, Джон Трубі та Імад Антуан Ібрагім, «майбутні правила, які будуть

прийняті щодо захисту даних та штучного інтелекту на рівні ЄС, а також на міжнародному рівні, щоб врахувати необхідність створення синергії між цими двома правовими галузями, враховуючи їхню взаємозалежність» [10, с. 87]. Однак деякі вчені припускають, що найефективніші правила ЄС щодо застосування ШІ в цифровій економіці будуть міститися не у вказаному Законі про ШІ, а в Законі про цифрові ринки (DMA), вплив якого на моделі ШІ та бази даних відзначають у чотирьох ключових сферах: вимоги до розкриття інформації; регулювання даних для навчання ШІ; правила доступу; та режим справедливого ранжування [11].

Для полегшення переходу до нової регуляторної бази Європейська Комісія також розробила Пакт про штучний інтелект (AI Pact) – добровільну ініціативу, метою якої є підтримка майбутнього впровадження, взаємодії із зацікавленими сторонами та запрошення постачальників і розгортачів штучного інтелекту з Європи та інших країн достроково виконати ключові зобов'язання Закону про штучний інтелект. Однак деякі вимоги щодо систем штучного інтелекту з високим рівнем ризику та інші положення застосовуватимуться лише після закінчення перехідного періоду (тобто часу між набранням чинності та датою застосування).

Основна проблема співвідношення із GDPR полягає у тому, що він напряму не регулює використання ШІ (адже був ухвалений на п'ять років раніше спеціального закону), однак і з підготовчих матеріалів Закону ЄС про штучний інтелект, із вищезгаданих етичних аспектів застосування штучного інтелекту вбачається, що Європейська комісія прагнула поширити, на скільки це можливо, положення GDPR і на сферу застосування штучного інтелекту.

Дж. Сартор, досліджуючи вплив Загального регламенту про захист даних на штучний інтелект, зазначив, що ШІ прямо не згадується в GPDR, але багато положень GDPR стосуються ШІ, а деякі з них кидають виклик новими способами обробки персональних даних, які забезпечуються ШІ, оскільки існує суперечність між традиційними принципами захисту даних (обмеженням мети, мінімізацією даних, спеціальною обробкою «чутливих даних», обмеженням автоматизованих рішень) та можливостями ШІ (збір величезної кількості даних про осіб та їхні соціальні зв'язки та обробку таких даних для цілей, які не були повністю визначені на момент збору) [12, с. II]. На його думку, ймовірно, GDPR буде тлумачитися таким чином, щоб узгодити обидві цілі: захист суб'єктів даних та забезпечення корисного застосування штучного інтелекту, адже в іншому випадку ЄС постане перед дилемою – або відмовитися від застосування GDPR, або програти гонку проти тих інформаційно-орієнтованих економік, таких як США та Китай, які здатні повною мірою використовувати ШІ [12, с. 76].

Так само й група дослідників на чолі з М. Еберс відзначають, що Закон ЄС про штучний інтелект видається достатньо чітким, щоб створити правову основу для обробки спеціальних категорій даних, адже GDPR та Закон ЄС про штучний інтелект дотримуються різних підходів: якщо GDPR стосується переважно захисту прав особи, втілюючи цінності європейських фундаментальних прав, то Закон ЄС про штучний інтелект спрямований на контроль, не встановлюючи безпосередньо жодних прав особи. Однак автори, пропонуючи зміни до законодавства, дотримуються позиції, за якої Закон ЄС про штучний інтелект має чітко зазначати, що використання систем штучного інтелекту повинно відповідати законодавству про захист даних, а не просто декларативно про це заявляти [13, с. 600].

У регулювання ШІ існує значна суперечність між економічними та політичними інтересами в технологічних інноваціях з одного боку, та етичними цінностями та правами людини, з іншого [14, с. 78]. А. Рувруа також підкреслює наявність економічного змісту у захисті персональних даних, вказуючи, що склалися два протилежні підходи щодо інструментів захисту даних та «статусу» персональних даних: а) підхід «права та економіки», який виступає за «ринок» персональних даних у якому персональні дані є «товаром», що фактично продається (компаніями, брокерами даних тощо), і дозволяє особам домовлятися про передачу «своїх» даних за фінансову винагороду, б) підхід, що розглядає персональні дані з точки зору влади, яку вони надають їхнім контролерам, прагнучи запобігти надмірній нерівності між тими, хто обробляє дані, та самими особами. При цьому дослідниця відзначає переважаючим у сучасній Європі саме другу модель [15, с. 6]. ЄС також розуміє свою провідну роль у запровадженні етичних стандартів у запровадженні ШІ та економічним зиски від цього – у згаданій Резолюції 2020/2012(INL) наголошено, що правові зобов'язання Союзу та етичні принципи щодо розробки, розгортання та використання цих технологій можуть зробити Європу світо-

вим лідером у секторі штучного інтелекту, і тому їх слід просувати в усьому світі шляхом співпраці з міжнародними партнерами, продовжуючи критичний та етичний діалог з третіми країнами, які мають альтернативні моделі регулювання, розробки та розгортання штучного інтелекту. Європейську Комісію закликано взяти на себе ініціативу щодо оцінки того, які двосторонні та багатосторонні договори та угоди слід скоригувати, щоб забезпечити послідовний підхід та сприяти європейській моделі етичної відповідності в усьому світі.

Отже, GDPR можна тлумачити та застосовувати таким чином, щоб він не перешкоджав корисному застосуванню ШІ до персональних даних і не ставив компанії ЄС у невигідне становище порівняно з конкурентами з неєвропейських країн. Таким чином, GDPR, здається, не потребує жодних суттєвих змін для вирішення проблеми використання ШІ [12, с. 79-78].

Натомість, дослідники відзначають і наявність суттєвих прогалин у регулюванні обох з регламентів, це перш за все пояснюється тим, що на меті регламентів не було втручатися у сфери регулювання один одного. Так, у GDPR врегульовано використання персональних даних, однак відсутнє змістовне регулювання алгоритмів обробки конфіденційних даних, що є ядром використання ШІ (для обробки даних, навчанні на даних тощо), який, у свою чергу, регулює використання даних. Тому не дивно, що GDPR не згадує алгоритм. Згідно з GDPR залишається незрозумілим, чи всі дані, згенеровані ШІ, підпадають під дію GDPR [10, с. 82].

Досвід застосування GDPR показує, що надмірна залежність від правозастосування національними органами влади призводить до дуже різних рівнів захисту в ЄС через різні ресурси органів влади, а також через різні погляди на те, коли і як (часто) вживати заходів [16]. Закон про ШІ можна розглядати як крок у правильному напрямку, проте залишається ризик того, що законодавство залишається занадто невизначеним щодо цілей, яких воно намагається досягти, зокрема, просування етичного застосування ШІ [17, с. 52].

Висновки і пропозиції. Проведене дослідження дозволяє зробити низку узагальнень щодо співвідношення GDPR та Закону ЄС про штучний інтелект, які разом формують фундамент правового регулювання цифрового середовища Європейського Союзу. GDPR і Закон ЄС про штучний інтелект мають різну предметну спрямованість, однак спільну мету: перший зосереджується на забезпеченні права особи на приватність і захист персональних даних, другий – на мінімізації ризиків і встановленні вимог до безпечного, етичного та контрольованого використання систем штучного інтелекту. Обидва регламенти є складовими ширшої стратегії цифрової політики ЄС, спрямованої на формування довіри до технологій та забезпечення захисту фундаментальних прав людини.

GDPR має непрямий, але суттєвий вплив на розвиток та застосування технологій штучного інтелекту. Його базові принципи – законність, пропорційність, обмеження мети, мінімізація даних, прозорість та контроль суб'єкта даних – залишаються чинними орієнтирами для будь-якої обробки інформації, у тому числі у процесах навчання алгоритмів і прийняття автоматизованих рішень. Це дозволяє GDPR виконувати роль «етичного фільтра» для технологічних інновацій.

Водночас між двома регламентами існує потенційна суперечність, що потребує узгодження. Закон ЄС про штучний інтелект не завжди узгоджується з нормами GDPR у частині визначення правових підстав для обробки даних, меж автоматизованого профілювання та відповідальності за шкоду, заподіяну алгоритмами. Ця розбіжність може призвести до правової невизначеності як для розробників і користувачів систем ШІ, так і для органів нагляду.

Подальший розвиток правового регулювання ЄС повинен ґрунтуватися на принципі взаємодоповнюваності: GDPR і Закон ЄС про штучний інтелект мають діяти як взаємопов'язані інструменти, які спільно забезпечують баланс між інноваціями, безпекою та правами людини, що дозволить уникнути дублювання норм, знизити регуляторне навантаження на бізнес і водночас гарантувати високий рівень етичного контролю над технологіями штучного інтелекту.

Список використаної літератури:

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. Чванкін С.А. Екстратериторіальний вплив Загального регламенту про захист даних (GDPR). *Науковий вісник Міжнародного гуманітарного університету. Серія «Юри-*

спруденція». 2024. № 68. С.158-162. URL: https://www.vestnik-pravo.mgu.od.ua/archive/juspradenc68/33.pdf.
3. European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)). *OJ*. C 252, 18.7.2018, P. 239–257. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=oj:JOC_2018_252_R_0026.
4. European Parliament resolution of 20 October 2020 with recommendations to the Commission on a civil liability regime for artificial intelligence (2020/2014(INL)). *OJ* C 404. 6.10.2021. P. 107–128. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=oj:JOC_2021_404_R_0006.
5. Proposal for a Regulation of The European Parliament and of the Council Laying Down Harmonised Rules On Artificial Intelligence (Artificial Intelligence Act) And Amending Certain Union Legislative Acts (SEC(2021) 167 final) – (SWD(2021) 84 final) – (SWD(2021) 85 final). URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex:52021PC0206.
6. Gültekin Várkonyi, G. A Case Study on the Interaction Between the General Data Protection Regulation and Artificial Intelligence Technologies. *Pro Futuro.* 2021. 10(4). P. 45-57. https://doi.org/10.26521/profuturo/2020/4/9570.
7. European Parliament resolution of 20 October 2020 with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies (2020/2012(INL)). *OJ.* C 404, 6.10.2021, P. 63–106. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=oj:JOC_2021_404_R_0005.
8. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance) PE/24/2024/REV/1. *OJ L*. 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj.
9. Vainionpää Fanny, Väyrynen Karin, Lanamaki Arto, Bhandari, Aayush, A Review of Challenges and Critiques of the European Artificial Intelligence Act (AIA). *ICIS.* 2023. Proceedings. 14. URL: https://aisel.aisnet.org/icis2023/aiinbus/aiinbus/14.
10. Brown R., Truby J., Ibrahim I.A. Mending Lacunas in the EU's GDPR and Proposed Artificial Intelligence Regulation. *European Studies*. 2022. 9(1). 2022. P. 61-90. URL: https://doi.org/10.2478/eustu-2022-0003.
11. Hacker P., Cordes J., Rochon J. Regulating Gatekeeper Artificial Intelligence and Data: Transparency, Access and Fairness under the Digital Markets Act, the General Data Protection Regulation and Beyond. *European Journal of Risk Regulation*. 2024. 15(1). P. 49-86. https://doi.org/10.1017/err.2023.81.
12. Giovanni Sartor. The impact of the General Data Protection Regulation (GDPR) on artifcial intelligence : Study for the Panel for the Future of Science and Technology, European Parliament. 2020. URL: https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf.
13. Ebers M., Hoch V.R.S., Rosenkranz F.; Ruschemeier H.; Steinrötter, B. The European Commission's Proposal for an Artificial Intelligence Act—A Critical Assessment by Members of the Robotics and AI. *Law Society (RAILS). J.* 2021. 4. P. 589–603. URL: https://doi.org/10.3390/j4040043.
14. Hijmans H., Raab C. Ethical Dimensions of the GDPR, AI Regulation, and Beyond. *Direito Público*. 2022. 18(100). URL: https://doi.org/10.11117/rdp.v18i100.6197.
15. Rouvroy Antoinette. "Of Data and Men":Fundamental Rights And Freedoms In a World of Big Data. Bureau of the Consultative Committee of the Convention for the Protection Of Individuals With Regard to Automatic Processing of Personal Data [Ets 108] (T-Pd-Bur) T-Pd-Bur(2015)09rev. 2016. URL: https://www.academia.edu/16699608/_Of_Data_And_Men_Fundamental_Rights_And_Freedoms_In_A_World_Of_Big_Data.
16. Massé E. Two Years under the EU GDPR: An Implementation Progress Report. URL: https://www.accessnow.org/cms/assets/uploads/2020/05/Two-Years-Under-GDPR.pdf.
17. Bitar Ralph. Data protection in the world of AI. https://www.diva-portal.org/smash/get/diva2:1761981/FULLTEXT01.pdf.

Cvankin S. A. On the Relationship Between the General Data Protection Regulation (GDPR) and the EU Artificial Intelligence Act

The article explores the interrelation between two key regulatory instruments of the European Union –the General Data Protection Regulation (GDPR) and the Artificial Intelligence Act (AIA), which together shape the legal framework of the EU's digital space. The paper examines the harmonization of their provisions and identifies potential areas of conflict, overlap, or mutual complementarity. It is

noted that despite their shared objective –ensuring the protection of human rights in the context of digitalization –these instruments are based on different approaches: the GDPR focuses on personal data protection and privacy, whereas the AIA emphasizes risk control, safety, and the ethical use of AI systems.

The analysis demonstrates that the GDPR does not directly regulate artificial intelligence, as it was adopted prior to the emergence of specific AI legislation. Nevertheless, its core principles –lawfulness, purpose limitation, data minimization, and the restriction of automated decision-making –influence the development and deployment of AI technologies. The AI Act introduces a risk-based approach to algorithmic systems and strengthens the accountability of developers, yet it does not always align with GDPR provisions on personal data processing. The paper highlights the issue of regulatory fragmentation arising from the parallel evolution of data protection and AI governance frameworks.

It is emphasized that the GDPR can be interpreted and applied in a way that does not hinder the use of AI but rather facilitates the alignment of innovation with the ethical and legal principles of the European Union. The study concludes that the GDPR and the AI Act should be viewed not as mutually exclusive but as complementary regulatory instruments. Their coexistence requires further clarification through judicial practice and practical application in high-risk technological sectors. The article underlines the leading role of the European Union in establishing ethical and legal standards for the digital economy and the need to create synergy between data protection and AI development.

Key words: *GDPR, Artificial Intelligence Act, personal data, right to privacy, European Union, digital law, data protection.*

Дата першого надходження рукопису до видання: 23.07.2025
Дата прийнятого до друку рукопису після рецензування: 26.08.2025
Дата публікації: 30.09.2025