АКТУАЛЬНІ ПИТАННЯ ЕКОНОМІЧНИХ НАУК

Маркетинг

УДК 346.26:004.738.5

DOI https://doi.org/10.5281/zenodo.20666967

DIGITAL-КОМПЛАЄНС І ЙОГО ВПЛИВ НА РОЗРОБКУ ТА ПРОСУВАННЯ ТОВАРІВ

Романюк Надія Василівна

кандидат економічних наук, доцент

Чернівецький національний університет імені Юрія Федьковича

ORCID: https://orcid.org/0000-0002-9852-3023

Прийнято: 15.04.2026 | Опубліковано: 30.04.2026

Анотація. *У статті досліджено феномен digital-комплаєнсу як самостійної технічно-правової дисципліни, що визначає умови розробки та просування товарів у цифровій економіці. Розмежовано класичний корпоративний комплаєнс і digital-комплаєнс, який охоплює дотримання вимог захисту персональних даних, кібербезпеки, алгоритмічної прозорості та регулювання цифрової реклами. Проаналізовано нормативну архітектуру Європейського Союзу, зокрема системну логіку взаємодії GDPR, Digital Services Act, Digital Markets Act, AI Act та Cyber Resilience Act як «регуляторної воронки», що кумулятивно перетворює комплаєнс на наскрізний дизайн-принцип товарного циклу. Досліджено вплив комплаєнсних вимог на стадії життєвого циклу продукту – від privacy by design і Data Protection Impact Assessment до обов'язкової сертифікації IoT-пристроїв. Розкрито трансформацію маркетингових стратегій під впливом обмежень таргетованої реклами, cookie-*

consent, заборони темних патернів і регулювання інфлюенсер-маркетингу. Оцінено бізнес-ефекти digital-комплаєнсу через призму штрафної практики та концепції «compliance as competitive advantage». Визначено стан імплементації GDPR-подібного законодавства в Україні, проаналізовано проєкт Закону № 8153 та обґрунтовано стратегічні кроки гармонізації українського регулювання з acquis ЄС.

Ключові слова: *digital-комплаєнс, захист персональних даних, GDPR, Digital Services Act, privacy by design, цифровий маркетинг, євроінтеграція, темні патерни.*

DIGITAL COMPLIANCE AND ITS IMPACT ON PRODUCT DEVELOPMENT AND PROMOTION

Romaniuk Nadiia Vasylivna
PhD in Economics, Associate Professor
Yuriy Fedkovych Chernivtsi National University
ORCID: https://orcid.org/0000-0002-9852-3023

Abstract. *The article examines the phenomenon of digital compliance as an independent technical and legal discipline that determines the conditions for product development and promotion in the digital economy. The study distinguishes between classical corporate compliance and digital compliance, which encompasses adherence to personal data protection requirements, cybersecurity standards, algorithmic transparency obligations, and digital advertising regulations. The normative architecture of the European Union is analysed, particularly the systemic logic of interaction between GDPR, the Digital Services Act, the Digital Markets Act, the AI Act, and the Cyber Resilience Act as a «regulatory funnel» that cumulatively*

transforms compliance into a cross-cutting design principle throughout the entire product lifecycle. The impact of compliance requirements on product lifecycle stages is examined in detail – from privacy by design and Data Protection Impact Assessment at the design stage to mandatory conformity assessment and CE marking of IoT devices at the release stage, as well as post-market monitoring and regulated data deletion upon withdrawal from the market. The transformation of marketing strategies under the influence of targeted advertising restrictions, cookie consent mechanisms, dark pattern prohibition, and influencer marketing regulation is explored, with particular attention to the empirical evidence of the shift from data-driven to contextual-driven advertising models. The business effects of digital compliance are assessed through the lens of enforcement practice, including cumulative GDPR fines exceeding seven billion euros, and the «compliance as competitive advantage» concept. The state of GDPR-like legislation implementation in Ukraine is determined, draft Law No. 8153 is analysed, and strategic steps for harmonising Ukrainian regulation with the EU acquis are substantiated.

Keywords: *digital compliance, personal data protection, GDPR, Digital Services Act, privacy by design, digital marketing, European integration, dark patterns.*

Постановка проблеми

Цифрова трансформація економіки поставила під сумнів саму природу того, що традиційно розумілося під комплаєнсом. Якщо впродовж десятиліть ця функція зосереджувалася на запобіганні корупційним і антимонопольним ризикам через організаційні процедури (кодекси, навчання, whistleblowing-механізми, внутрішні розслідування), то стрімкий розвиток цифрових ринків породив принципово інший пласт регуляторних вимог, які не можуть бути дотримані суто організаційними засобами. Захист персональних даних,

кібербезпека продуктів, алгоритмічна прозорість, модерація контенту, правила цифрової реклами – усе це вимагає інкорпорації правового припису безпосередньо в код, архітектуру даних і бізнес-логіку продукту [1; 2]. Видається обґрунтованим стверджувати, що digital-комплаєнс не є просто розділом загального комплаєнсу: він формує окрему методологію, в якій традиційні поняття «контролю» та «нагляду» доповнюються концептами «privacy by design», «compliance by design», «risk management system» і «conformity assessment» (поняттями, що мають водночас правову й інженерну природу) [10]. Саме ця подвійна природа перетворює compliance-функцію на трансдисциплінарну діяльність, де юрист, інженер і product-менеджер стають співавторами єдиного комплаєнсного рішення.

Актуальність дослідження визначається безпрецедентним розширенням нормативної архітектури Європейського Союзу, яка за період 2016–2024 рр. еволюціонувала від одного горизонтального акту (GDPR) до цілісної регуляторної екосистеми, що включає Digital Services Act, Digital Markets Act, AI Act, Cyber Resilience Act та ePrivacy Regulation. Ця «регуляторна воронка» безпосередньо впливає на кожну стадію розробки й просування товарів і створює системний тиск на бізнес-моделі компаній, орієнтованих на європейські ринки. Для України, яка перебуває у процесі євроінтеграції і має значний сектор IT-аутсорсингу та цифрового експорту, розуміння цієї архітектури є не лише теоретичною, а й операційною необхідністю, зумовленою зобов'язаннями за Угодою про асоціацію [36]. Водночас вітчизняне регулювання демонструє суттєвий розрив із acquis ЄС: чинний Закон «Про захист персональних даних» (2010 р.) концептуально передує GDPR і позбавлений ключових інструментів регламенту, а регулювання цифрового маркетингу розпорошено між кількома нормативними актами без єдиної системної логіки [31; 33; 34; 35]. Якщо припустити, що цей розрив не буде подолано у найближчі роки, українські

компанії ризикують опинитися у подвійній регуляторній пастці: де-факто підпорядкованість GDPR за екстериторіальним принципом за одночасної відсутності внутрішніх стимулів до комплаєнсних інвестицій.

Аналіз останніх досліджень і публікацій

Проблематика digital-комплаєнсу перебуває на перетині кількох дослідницьких традицій, що відображає її міждисциплінарний характер. Критичний аналіз принципу захисту даних за задумом (privacy by design), закріпленого у ст. 25 GDPR, здійснено А. Е. Вальдманом, який показав текстуальну невизначеність формулювань «reasonable measures» та «state of the art» і попередив про ризик «privacy theater» (формального дотримання без реального захисту) [1]. Вплив регулювання захисту даних на стартап-інновації досліджено у роботі Н. Мартін, К. Метта, К. Нібеля та К. Блінда, де встановлено, що молоді компанії несуть непропорційно вищі compliance-витрати порівняно з великими корпораціями [2]. Це спостереження набуває ширшого контексту у пізнішому дослідженні К. Блінда, К. Нібеля та К. Раммера, які на основі панельних даних підприємств ЄС оцінили вплив GDPR на інновації і виявили значну неоднорідність ефектів залежно від розміру та галузі фірми, причому для малих підприємств негативний вплив виявився найвідчутнішим [3].

Регуляторні аспекти штучного інтелекту активно розробляються в контексті AI Act: Й. Шютт проаналізував систему ризик-менеджменту цього акту (вимоги ст. 9 до безперервного управління ризиками, data governance за ст. 10 і технічної документації за ст. 11) і дійшов висновку, що поточна архітектура створює надмірне документаційне навантаження на розробників [4]. М. Альмада і Н. Петі критично переглянули ризик-орієнтований підхід AI Act, продемонструвавши, що категорії ризику побудовані на закритому переліку

Annex III, а не на емпіричних даних, що ставить під сумнів його «truly risk-based» характер [5]. Кібербезпековий вимір digital-комплаєнсу досліджено Т. Малером зі співавторами: їхня «дорожня карта відповідності» Cyber Resilience Act висвітлює нові обов'язки виробників щодо Software Bill of Materials, повідомлення про вразливості та CE-маркування продуктів із цифровими елементами [6]. Регулювання цифрових платформ розглянуто у працях К. Сантоса, Н. Бєлової та ін., які проаналізували поширеність темних патернів і запропонували критерії для визначення, які платформи підпадають під ст. 25 DSA [7], а також К. Каругаті, який розробив принципи комплаєнсу для DMA, зосередившись на зобов'язаннях «гейткіперів» і проблемі пропорційності ex ante регулювання [8]. Ф. Паскуале і Г. Сунь дослідили вплив DSA на онлайн-рекламу та ad-tech, показавши, як поєднання заборони профілювання неповнолітніх, вимог прозорості та модерації контенту трансформує рекламну екосистему [9], тоді як С. Веццозо проаналізував принцип «compliance by design» на прикладі обов'язку інтероперабельності месенджерів за DMA, засвідчивши, що технічні стандарти стають невід'ємним елементом правового комплаєнсу [10].

Емпіричний вплив GDPR на ринки даних і реклами зафіксовано у низці впливових робіт. К. Пойкерт, С. Бехтольд, М. Батікас і Т. Кречмер виявили, що GDPR спричинив концентрацію ad-tech ринку, посиливши домінування великих платформ [11]. Г. Арідор, Й.-К. Че і Т. Зальц оцінили вплив регулювання на індустрію даних, показавши, що opt-out зменшив обсяг доступних даних, але не знищив ринок повністю [12]. Наслідки Apple App Tracking Transparency досліджено Н. Вернерфельтом, А. Тачманом, Б. Шапіро і Р. Моаклером, які зафіксували падіння CTR у conversion-optimized кампаніях Meta на 37 % [13]. Комплексну економічну оцінку GDPR здійснено С. Голдбергом, Г. Джонсоном і С. Шрайвером, які виявили зменшення зафіксованого трафіку на 12 % та зниження виручки e-commerce на 13,3 % у короткостроковій перспективі [14].

Концепцію «GDPR Муорія» запропоновано Д. Жераденом, Т. Каранікіоті і Д. Кацифісом, які стверджують, що регулювання ненавмисно сприяло формуванню ad-tech дуополії Google і Meta [15]. Стратегічні аспекти комплаєнсу як конкурентної переваги розроблено В. Г. Воссом і К. А. Гаузер (фреймворк п'яти стадій правової стратегії) [16], а А. Бляєр, А. Голдфарб і К. Такер переконливо продемонстрували, що privacy concerns стимулюють не лише обмеження, а й нові форми інновацій [17]. Регулювання комерційних комунікацій інфлюенсерів проаналізовано Р. Гонсалес-Діазом зі співавторами, які виявили переважання саморегулювання і запропонували hard-law рамку [18], а Л. Крафт, Б. Скіра і Т. Кошелла оцінили економічний вплив opt-in vs opt-out моделей на прикладі Apple ATT [19].

В українській науковій літературі проблематика digital-комплаєнсу досліджується переважно в контексті євроінтеграції. Комплаєнс як елемент корпоративного управління в IT-секторі України розглянуто В. А. Рекуном, який обґрунтував необхідність системного підходу до регуляторної відповідності [20]. Захист персональних даних працівника в умовах цифровізації проаналізовано О. Г. Середою і Т. В. Красюк, які зафіксували лише часткове відтворення стандартів GDPR у чинному законодавстві [21]. Електронну комерцію в Україні та ЄС дослідили О. М. Тур, І. О. Пригара та І. В. Новикова, визначивши регуляторну неузгодженість як один із ключових бар'єрів розвитку цифрової торгівлі [22]. Проблеми адаптації національного законодавства до acquis ЄС, зокрема термінологічну плутанину понять «адаптація», «апроксимація» та «гармонізація», окреслили А. О. Гнітій, Д. І. Козаченко та Є. П. Лисенко [23]. Євроінтеграційні орієнтири цифрової трансформації в державному управлінні проаналізувала Н. Орлова, визначивши пріоритети імплементації цифрового acquis [24].

Формулювання цілей статті

Метою статті є комплексний аналіз digital-комплаєнсу як технічно-правової дисципліни та дослідження його впливу на розробку й просування товарів в умовах нормативної архітектури ЄС, а також оцінка стану та перспектив імплементації відповідних стандартів в Україні. Для досягнення цієї мети поставлено такі завдання: розмежувати digital-комплаєнс і класичний корпоративний комплаєнс на категоріальному рівні; проаналізувати системну логіку взаємодії ключових регуляторних актів ЄС; дослідити вплив комплаєнсних вимог на стадії життєвого циклу продукту та маркетингові стратегії; оцінити бізнес-ефекти digital-комплаєнсу крізь призму штрафної практики і концепції «compliance as competitive advantage»; визначити розрив між українським регулюванням і acquis ЄС та обґрунтувати стратегічні кроки гармонізації.

Виклад основного матеріалу

Осмислення digital-комплаєнсу як окремої категорії вимагає передусім з'ясування його онтологічного статусу: чи маємо справу з підвидом загального комплаєнсу, який відрізняється лише предметною сферою, чи з якісно іншим феноменом, що потребує власного категоріального апарату? Якщо припустити, що digital-комплаєнс є лише проєкцією класичної compliance-функції на цифрове середовище, то його реалізація зводилася б до створення додаткових організаційних процедур (privacy policy, cookie-банер, навчання працівників), подібних до антикорупційних кодексів чи санкційних скринінгів. Однак практика останнього десятиліття засвідчує протилежне: ст. 25 GDPR вимагає не просто документального підтвердження дотримання, а інкорпорації захисту

даних у саму архітектуру продукту через принцип privacy by design, що перетворює правовий обов'язок на інженерне завдання [1; 25]. Це дає підстави стверджувати, що digital-комплаєнс утворює якісно нову дисципліну, в якій правовий припис інтегрується безпосередньо в код, алгоритми обробки даних і дизайн інтерфейсу. Поняття «compliance by design», проаналізоване С. Веццозо на прикладі обов'язку інтероперабельності месенджерів за DMA, засвідчує, що технічний стандарт стає нерозривною частиною правового обов'язку, а compliance-функція виходить за межі юридичного департаменту і набуває трансдисциплінарного характеру [10]. Видається, що саме ця трансдисциплінарність (поєднання юридичної, інженерної та управлінської компетенцій в єдиному рішенні) становить сутнісну ознаку digital-комплаєнсу, яка відрізняє його від усіх попередніх форм регуляторної відповідності.

Визначивши категоріальний апарат, доцільно перейти до аналізу нормативної архітектури, що формує регуляторну рамку digital-комплаєнсу в Європейському Союзі. Її можна уявити як багатошарову конструкцію, де кожен наступний акт не просто додає нові заборони, а кумулятивно перетворює комплаєнс на наскрізний дизайн-принцип. Базовий шар утворює GDPR із загальними принципами правомірності, мінімізації даних і прав суб'єктів [25]. Над ним надбудовується спеціальний режим електронних комунікацій: ePrivacy Directive 2002/58/EC (доповнена Директивою 2009/136/EC) та проєкт ePrivacy Regulation, що з 2017 р. перебуває в стадії міжінституційних переговорів і покликаний гармонізувати правила cookie-consent та електронного direct marketing [30]. Горизонтальне регулювання посередницьких послуг забезпечує Digital Services Act, який впроваджує обов'язки прозорості реклами, заборону темних патернів і захист неповнолітніх [26]; ринковий вимір представлений Digital Markets Act із ex ante обов'язками для «гейткіперів» [27]; технологічний шар формує AI Act з ризик-орієнтованим режимом для високоризикових систем

штучного інтелекту [28]; кібербезпековий фундамент закладає Cyber Resilience Act, який поширює вимоги secure by design на всі продукти з цифровими елементами [29]. Якщо спробувати осмислити цю архітектуру телеологічно, то її внутрішня логіка полягає в тому, що одна й та сама бізнес-практика (скажімо, профілювання неповнолітніх) одночасно потрапляє під ст. 22 GDPR, ст. 28 DSA та класифікацію високого ризику за Annex III AI Act, тобто підлягає кумулятивному регуляторному тиску, що робить фрагментований підхід до комплаєнсу неефективним [8; 9].

Описану вище архітектуру доцільно візуалізувати у вигляді концептуальної схеми (рис. 1).

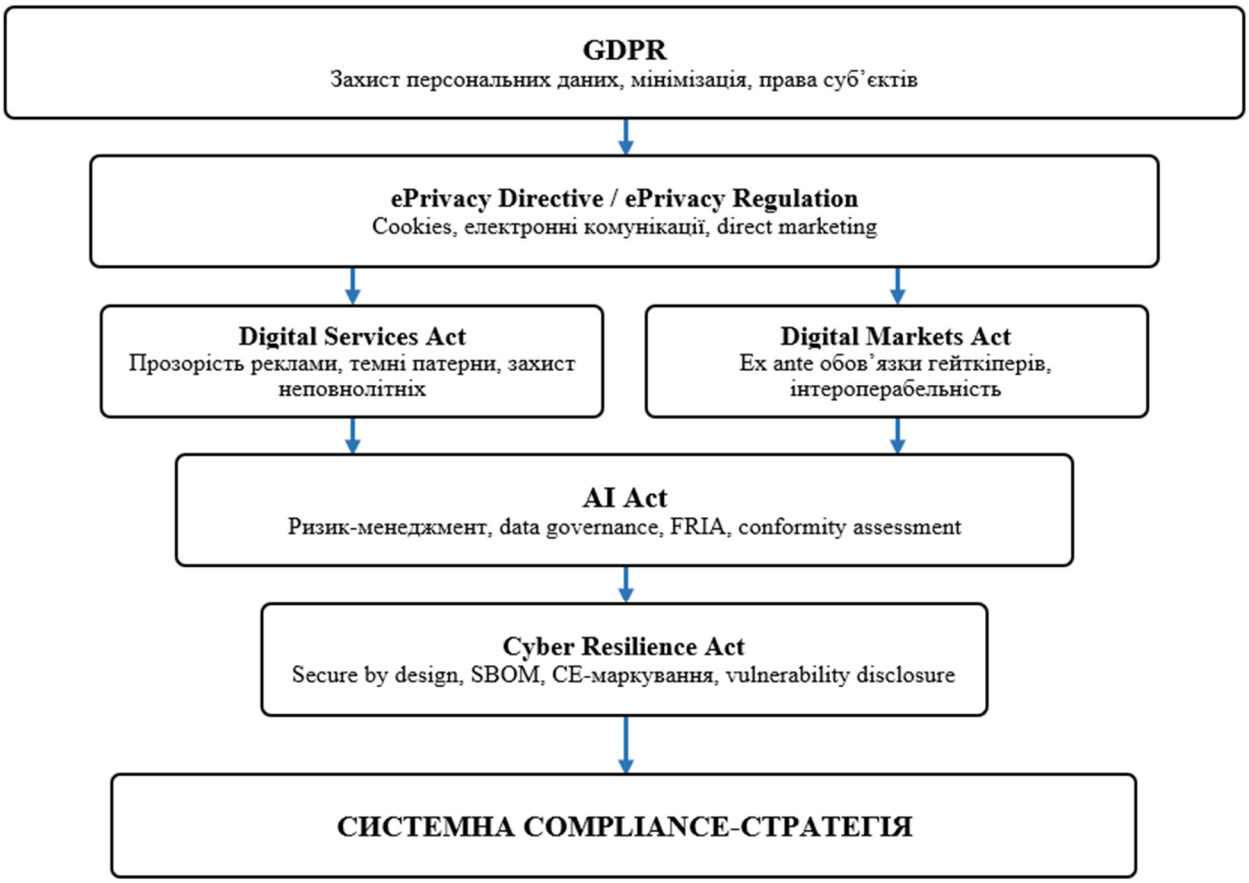

Рис. 1. Регуляторна воронка digital-комплаєнсу в ЄС

Джерело: розроблено автором

Описана інституційна архітектура становить організаційну рамку, проте її практичне значення розкривається лише через аналіз того, як саме вона трансформує конкретні стадії життєвого циклу продукту. Вихідним пунктом цієї трансформації є ст. 25 GDPR, яка зобов'язує контролера враховувати захист даних «у момент визначення засобів обробки», тобто на етапі архітектурного проєктування, а не запуску [25]. Слід вказати на текстуальну невизначеність цього припису, яка створює ризик «privacy theater» (формального документального дотримання без реального захисту), проте Guidelines 4/2019 EDPB і обов'язкова Data Protection Impact Assessment за ст. 35 GDPR частково компенсують цю невизначеність, перетворюючи DPIA на реальний gating-механізм, без проведення якого виведення high-risk продуктів на ринок ЄС стає юридично неможливим [1]. AI Act розширює цей підхід значно далі: постачальники високоризикових систем зобов'язані забезпечити безперервний risk management (ст. 9), належний data governance (ст. 10), технічну документацію за Annex IV (ст. 11), автоматичне логування (ст. 12), людський нагляд (ст. 14) та систему управління якістю (ст. 17), а користувачі таких систем мають проводити Fundamental Rights Impact Assessment (ст. 27) [4; 28]. Cyber Resilience Act додає кібербезпековий вимір: обов'язкову оцінку кіберризиків ще до випуску продукту, забезпечення прозорості ланцюга постачання через Software Bill of Materials, повідомлення про активно експлуатовані вразливості до ENISA протягом 24 годин і CE-маркування з конформіті-оцінкою (від внутрішньої для стандартних продуктів до обов'язкової сертифікації notified body для критичних класів I і II) [6; 29]. Це дає підстави стверджувати, що ми спостерігаємо фундаментальне переформатування product lifecycle: ідея проходить через privacy threshold analysis, дизайн – через DPIA та FRIA, розробка – через secure-by-default архітектуру, тестування – через verification наборів даних, реліз – через

conformity assessment і CE-маркування, експлуатація – через post-market monitoring, а виведення з ринку – через регламентоване видалення даних.

Послідовність впливу комплаєнсних вимог на стадії product lifecycle доцільно представити у вигляді схеми (рис. 2).

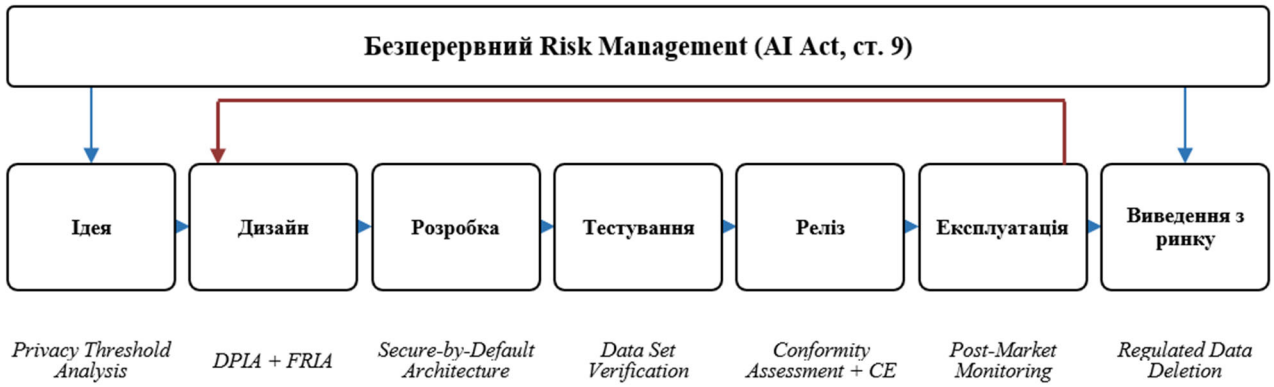

Рис. 2. Комплаєнсний фільтр життєвого циклу продукту

Джерело: розроблено автором

Водночас критичний погляд на цю архітектуру виявляє ризик over-regulation. Категорії ризику побудовані не на емпіричних даних, а на закритому переліку Annex III, тоді як надмірно широке визначення AI охоплює навіть прості предиктивні моделі без машинного навчання [5]. Якщо припустити, що ця критика справедлива (а емпіричних аргументів на її користь щораз більше), то виникає парадокс: регулювання, покликане захистити споживача від ризиків AI, саме стає джерелом ризику для інноваційних компаній, які не можуть дозволити собі compliance-інфраструктуру масштабу великих корпорацій. Ця критика, однак, не скасовує самого дизайн-орієнтованого підходу до комплаєнсу: вона радше вказує на необхідність подальшої калібровки, яка відповідала б природі цифрових продуктів як об'єктів, що безперервно еволюціонують і вимагають адаптивного, а не статичного регулювання.

Систематизація впливу ключових регуляторних актів ЄС на розробку та просування товарів наведена в таблиці 1.

Таблиця 1

Вплив регуляторних актів ЄС на розробку та просування товарів

Регуляторний акт	Вплив на розробку товарів	Вплив на просування товарів	Ключові механізми комплаєнсу
GDPR (2016/679)	Privacy by design / by default (ст. 25); DPIA для high-risk обробки (ст. 35); мінімізація даних у продуктовій архітектурі	Заборона таргетування на основі чутливих категорій даних (ст. 9); вимога законної підстави для обробки; право на заперечення проти direct marketing	DPO, Records of Processing, DPIA, Data Breach Notification (72 год.)
DSA (2022/2065)	Вимоги до модерації контенту на платформах, де продукт дистрибутується	Заборона профілювання неповнолітніх для реклами (ст. 28); прозорість рекламних систем (ст. 26); заборона dark patterns (ст. 25); реклама на основі чутливих даних заборонена	Ad Repository, алгоритмічний аудит для VLOP
DMA (2022/1925)	Обов'язок інтероперабельності (месенджери); заборона self-preferencing; доступ до даних для бізнес-користувачів	Заборона поєднання даних між сервісами гейткіпера без згоди; обмеження тайного використання даних бізнес-користувачів для конкуренції	Compliance report, регуляторний діалог з Комісією
AI Act (2024/1689)	Risk management system (ст. 9); data governance (ст. 10); технічна документація (Annex IV, ст. 11); автоматичне логування (ст. 12); людський нагляд (ст. 14); FRIA для deployers (ст. 27)	Прозорість AI-генерованого контенту; маркування deep fakes; обмеження маніпулятивних AI-технік у рекламі (ст. 5)	Conformity assessment, QMS, EU database, post-market monitoring
CRA (2024/2847)	Secure by design для всіх продуктів із цифровими елементами; SBOM; vulnerability disclosure; оцінка кіберризиків до випуску; CE-маркування	Непрямий вплив: продукт без CE-маркування не може бути виведений на ринок ЄС, що унеможливлює його просування	Internal control / EU-type examination / Full QA (залежно від класу)

Джерело: складено автором на основі [25; 26; 27; 28; 29]

Перехід від аналізу розробки до аналізу просування товарів є логічно обумовленим, адже маркетинг історично будувався на максимально щільному зборі поведінкових даних, і саме цю модель digital-комплаєнс ставить під найрадикальніший перегляд. GDPR обмежив її через вимогу законної підстави обробки, а ст. 9 заборонила таргетування на основі чутливих категорій даних (расового походження, релігії, стану здоров'я, сексуальної орієнтації) [25]. Digital Services Act посилив ці обмеження: ст. 26(3) прямо забороняє рекламу на основі профілювання спеціальних категорій даних, а ст. 28(2) забороняє рекламу на основі профілювання неповнолітніх, причому навіть батьківська згода не може легітимізувати таку практику, що є значно суворішим за загальний режим GDPR [9; 26]. Окрему проблему створює cookie-consent – з понад 254 тис. проаналізованих банерів лише близько 15 % є мінімально комплаєнтними, а понад половина сайтів встановлюють трекувальні cookies ще до того, як користувач зробив вибір [7]. Показово, що CNIL у 2021 р. наклав 150 млн євро штрафу на Google і 60 млн євро на Facebook саме за дизайн, у якому відмовитися від cookies було складніше, ніж погодитися, і цю практику DSA згодом інституціалізував як заборонений «темний патерн» за ст. 25 [26]. Видається обґрунтованим стверджувати, що ці регуляторні обмеження об'єктивно підштовхують маркетинг до парадигмального зсуву від data-driven до contextual-driven моделі.

Емпіричні дані підтверджують масштаб цієї трансформації, хоча й з важливими застереженнями. Класичне дослідження Голдфарба і Такер ще щодо ePrivacy Directive 2002 р. зафіксувало падіння ефективності display-реклами на близько 65 % для сайтів із загальним контентом, і цей ефект відтворюється на якісно новому рівні у пост-GDPR реальності [14]. Впровадження Apple App Tracking Transparency знизило частку трекованого трафіку в США з 73 % до 18 %, що Крафт, Скіра і Кошелла оцінюють у 21–23 % втраченого рекламного

доходу видавців [19], а Вернерфельт і колеги фіксують падіння CTR у conversion-optimized кампаніях Meta на 37 % [13]. Якщо припустити, що ці тенденції зберігатимуться, цифровий маркетинг у його нинішній data-intensive формі стане структурно невигідним. На сайтах із релевантним контентом негативний ефект мінімальний, а контекстна реклама за певних умов підвищує purchase intent [12]. Це дає підстави для обережного оптимізму: ринок не стільки стискається, скільки перебудовується через privacy-enhancing technologies (PETs), federated learning і first-party data стратегії, що поступово заміщують модель суцільного третьостороннього трекінгу [17].

До цього додається посилення регулювання інфлюенсер-маркетингу й остаточне оформлення заборони темних патернів як окремої правової категорії. Поточні режими розкриття спонсорства (ASA у Великій Британії, FTC у США, AGCM в Італії) переважно тримаються на саморегулюванні і виконуються вкрай незадовільно, що обґрунтовує необхідність жорсткої нормативної рамки [18]. Ст. 25 DSA вперше на рівні регламенту кваліфікує як протиправний дизайн інтерфейсу, що «обманює або маніпулює» користувачем, причому 97 % популярних сайтів і додатків ЄС використовують щонайменше один темний патерн [7]. Якщо осмислити цю тенденцію в ширшому філософському контексті, вона свідчить про поступове визнання того, що інтерфейс є не нейтральним посередником між користувачем і сервісом, а потужним інструментом формування поведінки, відповідальність за дизайн якого має бути не менш строгою, ніж відповідальність за фізичну безпеку продукту. Перший штраф за DSA (120 млн євро на X у грудні 2025 р. за оманливий дизайн «синього checkmark», непрозорість рекламного репозиторію і блокування доступу дослідників) підтверджує, що Комісія готова перетворити цю філософську позицію на правозастосовну реальність.

З погляду бізнес-ефектів digital-комплаєнс утворює те, що можна назвати «парадоксом регуляторного тиску»: одне й те саме регулювання одночасно генерує витрати і створює конкурентні переваги, причому розподіл цих ефектів між учасниками ринку є нерівномірним. Кумулятивна сума штрафів за GDPR станом на середину 2025 р. перевищила 7 млрд євро за понад 2800 рішеннями, з яких вісім найбільших видано ірландським DPC. Серед знакових санкцій: 1,2 млрд євро на Meta за нелегальне передавання даних до США (2023 р.), 746 млн євро на Amazon за рекламний таргетинг без згоди (2021 р.), 530 млн євро на TikTok за передачу даних користувачів ЄЕЗ до Китаю (2025 р.) [11; 14]. Ці суми перетворюють digital-комплаєнс із бухгалтерської статті витрат на стратегічну категорію ризик-менеджменту [11; 15].

Чинний Закон України «Про захист персональних даних» (2010 р., № 2297-VI) концептуально передує GDPR і позбавлений ключових інструментів регламенту: обов'язкової фігури DPO, процедури DPIA, принципів privacy by design і by default, режиму повідомлення про витоки протягом 72 годин, екстериторіальної юрисдикції та режиму adequacy [31]. Санкції за статтями 188-39 і 188-40 КУпАП (від 1 700 до 34 000 грн) є несумірними із ризик-стримувальною функцією: на тлі європейських штрафів у мільярди євро вони створюють спотворений сигнал ринку, за якого комплаєнсні інвестиції є економічно невигідними для компаній, що оперують виключно на внутрішньому ринку. Проєкт Закону «Про захист персональних даних» № 8153, прийнятий за основу 20.11.2024 (Постанова ВРУ № 4065-IX), частково усуває цей розрив: запроваджує DPO, DPIA, privacy by design, штрафи до 4 % обороту, а також передбачає створення незалежної Національної комісії захисту даних замість поточної моделі контролю Уповноваженим ВРУ з прав людини [20; 32]. Однак на час підготовки статті законопроєкт залишається в очікуванні другого читання,

а строки гармонізації, передбачені Угодою про асоціацію (ст. 15) та Планом заходів Кабміну від 25.10.2017, давно прострочено [36].

Регулювання digital-маркетингу в Україні демонструє не менш проблемну фрагментованість: норми про прямий маркетинг розпорошено між Законом «Про електронну комерцію» (№ 675-VIII), Законом «Про рекламу» (№ 270/96-ВР) і Законом «Про електронні комунікації» (№ 1089-IX), при цьому жоден із цих актів не містить ePrivacy-логіки, чітких вимог до cookie-consent або спеціального регулювання інфлюенсер-маркетингу [33; 34; 35]. Частка електронної комерції в Україні суттєво відстає від показника ЄС, і одним із базових бар'єрів є саме регуляторна неузгодженість, яка зменшує довіру споживачів і ускладнює транскордонні операції [22]. Навіть у такій класичній для трудового права сфері, як захист персональних даних працівника, стандарти GDPR відтворюються лише частково, а правозастосовна практика не виробила сталих орієнтирів [21]. Видається обґрунтованим стверджувати, що за такого стану справ українські компанії, орієнтовані на ринок ЄС, опиняються у стані подвійної регуляторної невизначеності: де-факто зобов'язані дотримуватися GDPR за екстериторіальним принципом, вони водночас позбавлені внутрішніх інституційних механізмів підтримки комплаєнсу.

Особливо чутливі ризики випливають із екстериторіальної дії GDPR (ст. 3): український IT-аутсорсинг, e-commerce, fintech і AdTech уже підпадають під європейський режим за фактом обслуговування клієнтів у ЄС, а відсутність adequacy decision означає, що передача даних із ЄС в Україну вимагає Standard Contractual Clauses або Binding Corporate Rules, що тягне за собою додаткові витрати і юридичні ризики. Якщо припустити, що Комісія прийматиме рішення про adequacy для окремих секторів (за моделлю ст. 45 GDPR «specified sector within third country»), лобіювання такого рішення для української IT-індустрії є раціональним кроком, проте без внутрішньої реформи, яка включала б

повноцінний незалежний DPA, чіткі процедури DPIA, режим повідомлення про витоки та пропорційні санкції, цей крок не матиме шансів на успіх. Подальша імплементація acquis у сфері електронних комунікацій, започаткована оновленнями Доповнення XVII-3 за рішеннями Комітету асоціації № 1/2021 і № 1/2023, є необхідним, але ще не достатнім кроком на шляху до повноцінного digital-комплаєнсу [36]. Цей шлях вимагатиме не лише законодавчих змін, а й формування комплаєнсної культури (тобто усвідомлення бізнесом, що дотримання цифрових регуляторних вимог є не тягарем, а стратегічною інвестицією у доступ до глобальних ринків).

Висновки

Проведене дослідження дає підстави стверджувати, що digital-комплаєнс є не просто підвидом загального комплаєнсу, а самостійною технічно-правовою дисципліною, сутнісною ознакою якої є трансдисциплінарність: правовий припис інкорпорується безпосередньо в архітектуру продукту, алгоритми обробки даних і дизайн інтерфейсу, що вимагає системної взаємодії юристів, інженерів і product-менеджерів. Нормативна архітектура ЄС утворює «регуляторну воронку», в якій GDPR, DSA, DMA, AI Act і Cyber Resilience Act кумулятивно перетворюють комплаєнс на наскрізний дизайн-принцип, і одна й та сама бізнес-практика може одночасно підпадати під кілька регуляторних режимів, що робить фрагментований підхід неефективним.

Вплив digital-комплаєнсу на розробку товарів виявляється у фундаментальному переформатуванні product lifecycle: від privacy threshold analysis на стадії ідеї до post-market monitoring при експлуатації та регламентованого видалення даних при виведенні з ринку. Privacy by design, DPIA, FRIA та CE-маркування перетворилися на обов'язкові gating-механізми, без яких виведення high-risk продуктів на ринок ЄС є юридично неможливим.

Водночас критичний аналіз AI Act виявляє ризик over-regulation, пов'язаний із закритим переліком високоризикових систем і надмірно широким визначенням AI, що вимагає подальшої калібровки ризик-орієнтованого підходу.

У сфері просування товарів digital-комплаєнс об'єктивно підштовхує маркетинг до парадигмального зсуву від data-driven до contextual-driven моделі. Хоча короткостроковий негативний ефект є значним (падіння виручки e-commerce на 12–13 %, зниження ефективності таргетованих кампаній на 21–37 %), емпіричні дані свідчать, що ринок не стільки стискається, скільки перебудовується через PETs, federated learning і first-party data стратегії, які поступово заміщують модель суцільного третьостороннього трекінгу.

Бізнес-ефекти digital-комплаєнсу утворюють «парадокс регуляторного тиску»: регулювання ненавмисно посилило ринкову концентрацію і непропорційно тисне на малий бізнес, проте компанії, які перейшли до проактивного позиціонування приватності як продуктового активу, отримують реальний trust premium. Концепція «compliance as competitive advantage» є емпірично підтвердженою стратегічною позицією, доступною, втім, переважно компаніям із достатнім compliance-бюджетом, що ставить питання про необхідність компенсаційних механізмів для малого та середнього бізнесу.

Українське регулювання демонструє суттєвий розрив із acquis ЄС: чинний Закон «Про захист персональних даних» позбавлений ключових інструментів GDPR, санкції є несумірними із ризик-стримувальною функцією, а регулювання digital-маркетингу фрагментоване між кількома законами без єдиної ePrivacy-логіки. Стратегічні кроки гармонізації мають включати ухвалення проєкту Закону № 8153 у максимально близькій до GDPR редакції, інституційне відокремлення наглядового органу з реальною фінансовою автономією, консолідацію регулювання digital-маркетингу в єдиному ePrivacy-сумісному акті та включення digital-комплаєнсу до програм підготовки юристів, інженерів і

маркетологів як трансдисциплінарної компетенції. Лише за такого комплексного підходу Україна зможе перетворити євроінтеграційні зобов'язання з тягаря на інструмент конкурентної переваги у цифровій економіці.

Список використаних джерел

1. Waldman A. E. Data Protection by Design? A Critique of Article 25 of the GDPR. *Cornell International Law Journal*. 2020. Vol. 53, № 1. P. 147–168. URL: https://community.lawschool.cornell.edu/wp-content/uploads/2021/03/Waldman-final.pdf

2. Martin N., Matt C., Niebel C., Blind K. How Data Protection Regulation Affects Startup Innovation. *Information Systems Frontiers*. 2020. Vol. 21, № 6. P. 1307–1324. DOI: 10.1007/s10796-019-09974-2. URL: https://link.springer.com/article/10.1007/s10796-019-09974-2

3. Blind K., Niebel C., Rammer C. The impact of the EU General Data Protection Regulation on innovation in firms. *Industry and Innovation*. 2024. Vol. 31, № 8. P. 1057–1083. DOI: 10.1080/13662716.2023.2271858. URL: https://www.tandfonline.com/doi/full/10.1080/13662716.2023.2271858

4. Schuett J. Risk Management in the Artificial Intelligence Act. *European Journal of Risk Regulation*. 2024. Vol. 15, № 2. P. 367–386. DOI: 10.1017/err.2023.1. URL: https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/risk-management-in-the-artificial-intelligence-act/2E4D5707E65EFB3251A76E288BA74068

5. Almada M., Petit N. Truly Risk-based Regulation of Artificial Intelligence: How to Implement the EU's AI Act. *European Journal of Risk Regulation*. 2025. DOI: 10.1017/err.2024.78. URL: https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/truly-riskbased-regulation-of-artificial-intelligence-how-to-implement-the-eus-ai-act/E526C1D0D7368F9691082220609D60F4

6. Mahler T. et al. The Cyber Resilience Act as a New Paradigm for Product Security: A Compliance Roadmap. *International Cybersecurity Law Review*. 2025. Vol. 6. DOI: 10.1365/s43439-025-00162-4. URL: https://link.springer.com/article/10.1365/s43439-025-00162-4

7. Santos C., Bielova N., Ahuja S., Utz C., Gray C., Mertens G. Which Online Platforms and Dark Patterns Should Be Regulated under Article 25 of the DSA? *SSRN Working Paper*. 2024. DOI: 10.2139/ssrn.4899559. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4899559

8. Carugati C. Compliance Principles for the Digital Markets Act. *Bruegel Policy Brief*. 2023. № 21. DOI: 10.2139/ssrn.4738733. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4738733

9. Pasquale F., Sun H. EU Digital Services Act: what does it mean for online advertising and adtech? *International Journal of Law and Information Technology*. 2024. DOI: 10.1093/ijlit/eaaf004. URL: https://academic.oup.com/ijlit/article/doi/10.1093/ijlit/eaaf004/8133991

10. Vezzoso S. 'Compliance by Design' With the Messenger Interoperability Obligation Under the Digital Markets Act. *SSRN Working Paper*. 2023. DOI: 10.2139/ssrn.4558135. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4558135

11. Peukert C., Bechtold S., Batikas M., Kretschmer T. Regulatory Spillovers and Data Governance: Evidence from the GDPR. *Marketing Science*. 2022. Vol. 41, № 4. P. 746–768. DOI: 10.1287/mksc.2021.1339. URL: https://pubsonline.informs.org/doi/10.1287/mksc.2021.1339

12. Aridor G., Che Y.-K., Salz T. The effect of privacy regulation on the data industry: Empirical evidence from GDPR. *RAND Journal of Economics*. 2023. Vol. 54, № 4. P. 695–730. URL: https://onlinelibrary.wiley.com/doi/10.1111/1756-2171.12455

13. Wernerfelt N., Tuchman A., Shapiro B., Moakler R. Evaluating the Impact of Privacy Regulation on E-Commerce Firms: Evidence from Apple's App Tracking Transparency. *Management Science*. 2025. DOI: 10.1287/mnsc.2024.06600. URL: https://pubsonline.informs.org/doi/abs/10.1287/mnsc.2024.06600

14. Goldberg S., Johnson G., Shriver S. Regulating Privacy Online: An Economic Evaluation of the GDPR. *American Economic Journal: Economic Policy*. 2024. Vol. 16, № 1. P. 325–358. DOI: 10.1257/pol.20210309. URL: https://www.aeaweb.org/articles?id=10.1257/pol.20210309

15. Geradin D., Karanikioti T., Katsifis D. GDPR Myopia: how a well-intended regulation ended up favouring large online platforms – the case of ad tech. *European Competition Journal*. 2021. Vol. 17, № 1. P. 47–92. DOI: 10.1080/17441056.2020.1848059. URL: https://www.tandfonline.com/doi/full/10.1080/17441056.2020.1848059

16. Voss W. G., Houser K. A. Personal Data and the GDPR: Providing a Competitive Advantage for U.S. Companies. *American Business Law Journal*. 2020. Vol. 56, № 2. P. 287–344. DOI: 10.1111/ablj.12139. URL: https://onlinelibrary.wiley.com/doi/10.1111/ablj.12139

17. Bleier A., Goldfarb A., Tucker C. Consumer Privacy and the Future of Data-Based Innovation and Marketing. *International Journal of Research in Marketing*. 2020. Vol. 37, № 3. P. 466–480. DOI: 10.1016/j.ijresmar.2020.03.006. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3570156

18. González-Díaz R. et al. Regulating influencers' commercial communication: No legislation, hardly any self-regulation and policy recommendations. *Policy & Internet*. 2024. Vol. 16, № 3. DOI: 10.1002/poi3.411. URL: https://onlinelibrary.wiley.com/doi/full/10.1002/poi3.411

19. Kraft L., Skiera B., Koschella T. Economic Impact of Opt-In Versus Opt-Out Requirements for Personal Data Usage: The Case of Apple's App Tracking

Transparency (ATT). *Marketing Science (working paper)*. 2024. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4598472

20. Рекун В. А. Комплаєнс як елемент корпоративного управління в IT-секторі України: євроінтеграційний курс. *Аналітично-порівняльне правознавство*. 2025. URL: https://journal-app.uzhnu.edu.ua/article/view/357644

21. Середа О. Г., Красюк Т. В. Персональні дані працівника та їх захист в умовах цифровізації. *Аналітично-порівняльне правознавство*. 2023. № 2. С. 188–193. URL: https://app-journal.in.ua/wp-content/uploads/2023/07/35.pdf

22. Тур О. М., Пригара І. О., Новикова І. В. Електронна комерція в Україні та ЄС: трансформація, виклики та перспективи. *Актуальні питання у сучасній науці. Серія «Економіка»*. 2025. № 5 (35). С. 186–198. DOI: 10.52058/2786-6300-2025-5(35)-186-198. URL: https://essuir.sumdu.edu.ua/items/21821b63-f08f-48ff-b336-188e42f06a15

23. Гнітій А. О., Козаченко Д. І., Лисенко Є. П. Адаптація національного законодавства України до acquis ЄС. *Юридичний науковий електронний журнал*. 2023. № 12. URL: http://lsej.org.ua/12_2023/119.pdf

24. Орлова Н. Євроінтеграційні орієнтири цифрової трансформації у державному управлінні України. *Публічне управління: концепції, парадигма, розвиток, удосконалення*. 2025. URL: https://pa.journal.in.ua/index.php/pa/article/view/205

25. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation). *Official Journal of the European Union*. 2016. L 119. P. 1–88. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj

26. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services (Digital Services Act). *Official Journal of the European Union*. 2022. L 277. P. 1–102. URL: https://eur-lex.europa.eu/eli/reg/2022/2065/oj

27. Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector (Digital Markets Act). *Official Journal of the European Union*. 2022. L 265. P. 1–66. URL: https://eur-lex.europa.eu/eli/reg/2022/1925/oj

28. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). *Official Journal of the European Union*. 2024. L, 2024/1689. URL: https://eur-lex.europa.eu/eli/reg/2024/1689/oj

29. Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 (Cyber Resilience Act). *Official Journal of the European Union*. 2024. L, 2024/2847. URL: https://eur-lex.europa.eu/eli/reg/2024/2847/oj

30. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 (ePrivacy Directive). *Official Journal of the European Communities*. 2002. L 201. P. 37. URL: https://eur-lex.europa.eu/eli/dir/2002/58/oj

31. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI. *Офіційний вісник України*. 2010. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text

32. Проєкт Закону про захист персональних даних № 8153 від 25.10.2022 : картка законопроєкту. *Верховна Рада України*. URL: https://itd.rada.gov.ua/billinfo/Bills/Card/40707

33. Про електронну комерцію : Закон України від 03.09.2015 № 675-VIII. *Відомості Верховної Ради України*. 2015. URL: https://zakon.rada.gov.ua/laws/show/675-19#Text

34. Про рекламу : Закон України від 03.07.1996 № 270/96-ВР. *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/270/96-вр#Text

35. Про електронні комунікації : Закон України від 16.12.2020 № 1089-IX. *Відомості Верховної Ради України*. 2021. URL: https://zakon.rada.gov.ua/laws/show/1089-20#Text

36. Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони (Додаток XVII-3). *Офіційний вісник України*. 2014. URL: https://zakon.rada.gov.ua/laws/show/984_011#Text