

УДК 347.121.1:004

М.В. Гура,
кандидат юридичних наук,
старший викладач кафедри цивільно-правових дисциплін
Харківського національного університету імені В.Н. Каразіна
<https://orcid.org/0000-0002-7695-7672>

НОВЕЛИ ЗАКОНОПРОЄКТУ № 8153 ТА ЇХ ВПЛИВ НА ІТ-ІНДУСТРІЮ

Анотація: метою статті є проведення системно-правового аналізу проєкту Закону України № 8153 «Про захист персональних даних», прийнятого за основу Верховною Радою України та який готується до другого читання на його відповідність європейським стандартам (GDPR).

Дослідження фокусується на імплементації європейських стандартів (GDPR) у національне правове поле та виникаючих при цьому колізіях. У статті критично розглянуто проблему невідповідності застарілої парадигми чинного Закону 2010 року викликам цифрової економіки. Автор детально проаналізував трансформацію понятійного апарату (введення термінів «спільний контролер», «контролер» та «оператор»), нові інститути (DPO, Privacy by Design та інші), а також механізми транскордонної передачі даних, зокрема з неєвропейськими юрисдикціями, які не мають відповідного рівня захисту прав. Особливу увагу приділено правовій кваліфікації ролей в ІТ-аутсорсингу та ризикам солідарної відповідальності через призму актуальної судової практики CJEU. В статті досліджено досвід впровадження GDPR в Європейському Союзі та негативні наслідки для малого та середнього бізнесу. Окремо проаналізовано вплив створення нового наглядового органу, передбаченого проєктом Закону України № 6177 «Про Національну комісію з питань захисту персональних даних та доступу до публічної інформації» та трансфер повноважень від Омбудсмена до нього. Проаналізовано бізнес-ризики, які може викликати впровадження Закону України № 8153 «Про захист персональних даних» для суб'єктів господарювання в Україні, зокрема в частині закладання технічної можливості реалізації збереження персональних даних, зокрема проєктованої приватності та приватності за замовчуванням.

Науковець робить висновок, що механічна рецепція норм без урахування технологічних процесів (CI/CD, архівація даних) може призвести до правової невизначеності та пропонує конкретні зміни до законопроєкту.

Ключові слова: захист персональних даних, GDPR, законопроєкт № 8153, контролер, оператор, ІТ-комплаєнс, транскордонна передача даних, спільні контролери, Data Protection Officer.



Постановка проблеми та її зв'язок із важливими науковими та практичними завданнями. Невідповідність парадигми Закону України № 2297-VI сучасним технологічним реаліям створює правовий вакуум, у якому розвиток цифрової екосистеми відбувається поза межами ефективного державного регулювання. Чинне законодавство України у сфері захисту персональних даних було прийнято ще до прийняття державного курсу на цифровізацію, успадкувавши попередні нормативні правила часів паперової бюрократії. На сьогодні чинне законодавство вже не може якісно регулювати нові ринкові відносини, які розвиваються під впливом штучного інтелекту та Big Data. Україна, перебуваючи на шляху євроінтеграції, зіткнулася з критичним викликом: ЗУ «Про захист персональних даних» 2010 р. [1], який колись був кроком уперед, сьогодні потребує оновлення, адже виконувати його норми складно, а реального захисту приватності вони часто не гарантують. Отримання статусу кандидата в члени ЄС та зобов'язання за Угодою про асоціацію вимагають цілісної архітектурної перебудови нормативної системи захисту даних відповідно до стандартів Загального регламенту захисту даних (GDPR).

Сьогодні дана тема набуває нової актуальності, коли в умовах війни персональні дані громадян стали ціллю для кібератак, а питання інформаційної безпеки трансформувалися з суто технічних у питання національної безпеки. Але українська ІТ-індустрія, що залишається одним із стовпів економічної стійкості, потребує чітких правил гри для збереження та підвищення конкурентоспроможності на глобальному ринку. Європейські замовники вимагають від українських контрагентів не просто декларацій, а реального комплаєнсу.

Ключове наукове завдання даного дослідження полягає у пошуку балансу між забезпеченням фундаментального права на приватність та уникненням надмірного регуляторного тиску, що здатен загальмувати розвиток інноваційного сектору. З одного боку, необхідно забезпечити фундаментальне право людини на приватність на європейському рівні. З іншого боку, не завдати шкоди вітчизняному ІТ-бізнесу надмірною бюрократією та штрафами, які пропонує законопроект № 8153 (включений до порядку денного за номером 4775-IX від 10.02.2026, далі за текстом - законопроект № 8153). Це набуває особливої актуальності в контексті масової релокації українських ІТ-компаній в іноземні юрисдикції.

Аналіз останніх досліджень і публікацій, в яких розглядаються різні аспекти даної проблеми і на які спирається автор. Проблематика захисту персональних даних в Україні активно досліджується, хоча динаміка законодавчих змін часто випереджає доктринальне осмислення. Так, В. М. Брижко висловлює сумніви у наявності ефективної державної системи нагляду та контролю у сфері захисту персональних даних [2, с. 75]. О. А. Баранов досліджує права людини в умовах цифрової трансформації та правовий режим

інформаційних ресурсів, розуміння якого використано нами для теоретичного аналізу законопроекту № 8153. Особливу увагу привертають дослідження захисту даних в контексті розвитку штучного інтелекту та робототехніки, що додають необхідне розуміння доктринальних понять для аналізу пропонованих новел [3, с. 40–54].

Ю. Я. Самагальська, аналізує захист персональних даних в мережі Інтернет та наголошує, що окрім формального приведення національного законодавства до європейських стандартів, українській державі в особі її контролюючих органів варто приділити більше уваги правореалізації, оскільки більшість володільців та розпорядників персональних даних не усвідомлюють тих ризиків, які можуть бути пов'язаними з їх розголошенням [4, с. 263].

В. А. Світличний пропонує міждисциплінарний, технічно-правовий аналіз приділяючи увагу актуальним питанням, зокрема, проблематиці захисту персональних даних в умовах воєнного стану в Україні [5, с. 226–236]

Проте попри наявність ґрунтовних праць, комплексний аналіз тексту законопроекту № 8153 досі залишається не повним. Більшість публікацій носять загальнотеоретичний характер або є короткими оглядами юридичних фірм (зокрема, роботи експертів Sayenko Kharenko, аналітика Європейської Бізнес Асоціації [6; 7]), а не науковими дослідженнями. Простежується брак наукових публікацій, які б поєднували юридичний догматизм з розумінням технологічних процесів у сфері DevOps, Data Science та Cloud Computing.

На прикладі країн, що розвиваються (зокрема Киргизької Республіки), дослідники Е. Хіксо та Н. Пазілов вказують на універсальну проблему: «існуюча законодавча база потребує значної адаптації для забезпечення захисту даних та кібербезпеки в цифровому середовищі, що швидко розвивається» [8, с. 251]. Їхні висновки щодо необхідності модернізації правових рамок для підвищення довіри до цифрових сервісів та захисту критичної інфраструктури прямо корелюють із завданнями, які стоять перед українським законопроектом № 8153 [8, с. 266].

Формулювання мети статті (постановка завдання). Метою даної роботи є оцінка потенційного регуляторного впливу окремих пропонованих новел законопроекту № 8153 «Про захист персональних даних» на операційну діяльність, структуру витрат та комплаєнс-стратегії ІТ-компаній в Україні.

У законопроекті № 8153 запропоновано доктринальне переосмислення термінології, змінюючи застарілу радянську конструкцію «володілець бази даних», на європейську дихотомію «контролер» та «оператор», що призводить до зміни нормативного підходу до юридичної відповідальності: від формального володіння активом до відповідальності за прийняття рішень.

У 2024 р. законопроект № 8153 було прийнято за основу із доопрацюванням положень, 19 грудня 2025 р. було одержано повторну резолюцію та

направлено його на розгляд Комітету. Станом на січень 2026 р. законопроект готується до другого читання.

Аналіз проекту Закону України «Про захист персональних даних» (реєстр. № 8153) виявляє спробу запозичити структурну логіку GDPR, що є необхідною для вступу України до ЄС. В проекті закону пропонуються визначення та механізми, які концептуально ідентичні регламенту ЄС, проте їх практичне застосування в межах української правової системи потребує ретельного аналізу.

Згідно зі ст. 2 законопроекту, контролер персональних даних (контролер) визначається як будь-яка фізична або юридична особа, суб'єкт владних повноважень чи будь-який інший орган, який самостійно чи спільно з іншими визначає цілі та засоби обробки персональних даних, а також інші фізичні або юридичні особи, для яких цілі та засоби обробки визначені законом [9, ст. 2]. Це визначення майже дослівно імплементує статтю 4(7) GDPR [10, ст. 4]. Концепція контролера зміщує фокус на процес прийняття рішень замість майнового права на дані. Особа, визнана контролером, несе основний тягар відповідальності, якщо вирішує «навіщо» (мета) і «як» (інструментарій) обробляти дані [9, ст. 28].

Як демонструє аналіз (табл. 1), для IT-сектору критично важливою є правильна кваліфікація відносин на етапі архітектурного планування проекту. Помилкова ідентифікація оператора (процесора) як спільного контролера може призвести до неочікуваного зростання юридичних ризиків.

Рішення CJEU відображають розширення кола осіб, які визнаються «контролерами», що ускладнює дотримання вимог для бізнесу в країнах-кандидатах до ЄС. Так, у рішенні від 2 грудня 2025 р. у справі C-492/23 (*X v. Russmedia Digital SRL*) CJEU переглянув відповідальність онлайн-маркетплейсів. Суд постановив, що оператор онлайн-платформи може кваліфікуватися як контролер або спільний контролер, персональних даних у згенерованих користувачами оголошеннях, якщо він здійснює визначальний вплив на обробку для власних цілей шляхом категоризації, структурування, просування контенту тощо [11]. Інша критична справа прояснила відносини відповідальності між контролерами та операторами. Раніше у справі *Deutsche Umwelthilfe e. V. v. Bundesrepublik Deutschland* CJEU зазначив, що контролер може нести відповідальність за незаконну обробку, здійснену його оператором або процесором, якщо тільки оператор не діяв повністю за межами обсягу своїх інструкцій [12]. Наведені приклади підтверджують потребу в суворому договірному нагляді та *due diligence*, який лише формується в правовому полі України.

Таблиця 1 – Порівняльна характеристика ролей суб'єктів обробки даних в ІТ-проектах (за законопроектом № 8153 та GDPR)

Критерій порівняння	Контролер	Оператор	Спільні контролери
Ключова роль	Визначає мету («навіщо?») та засоби («як?») обробки.	Здійснює обробку від імені та за дорученням контролера.	Два або більше суб'єктів спільно визначають мету та засоби.
Прийняття рішень	Приймає стратегічні рішення щодо складу даних та строків зберігання.	Приймає лише технічні та організаційні рішення в межах інструкцій.	Розподіляють функції. Один може визначати мету, а інший технічну платформу.
Приклад в ІТ	Продуктова компанія, стартап-власник мобільного додатка, замовник програмного забезпечення.	Хмарний провайдер (IaaS, PaaS), аутсорсингова компанія (якщо пише програмний код за технічне завдання).	Рекламна мережа + власник сайту; мобільний додаток + інтегрований SDK аналітики.
Відповідальність	Повна відповідальність перед суб'єктом даних та регулятором.	Відповідальність за порушення інструкцій контролера або вимог безпеки.	Солідарна відповідальність. Суб'єкт може звернутися з позовом до будь-кого з них.
Договірне підґрунтя	Політика приватності для користувачів.	Договір про обробку даних (DPA, Data Processing Agreement).	Угода про спільний контроль (JCA, Joint Controller Arrangement).
Ризик для ІТ-бізнесу	Високі штрафи за нецільове використання даних.	Ризик автоматичної перекваліфікації в контролера при виході за межі інструкцій.	Складність розмежування зон відповідальності, «сірі зони» в API-інтеграціях.

Поняття оператор (яке відповідає європейському processor) визначено як будь-яка фізична або юридична особа, суб'єкт владних повноважень чи будь-який інший орган, який здійснює обробку персональних даних від імені контролера та уповноважена на це ним або законодавством [9, ст. 2]. Для ІТ-індустрії така розбіжність може носити критичний характер, адже раніше аутсорсери намагалися прикритися не чітко визначеною відповідальністю через статус «третьої особи» або «розпорядника». Для вирішення цієї проблеми, у ст. 31 законопроекту запропоновано закріпити, що оператор діє виключно в межах письмових інструкцій контролера, а вихід за ці межі

автоматично перекваліфіковує оператора в контролера з усіма наслідками, включаючи штрафи [9, ст. 31].

На наш погляд, найбільш дискусійною новелою для ІТ-бізнесу є пропонована ст. 30, у якій вводиться поняття спільних контролерів [9, ст. 30]. В іноземній правовій доктрині та керівних принципах Європейської ради із захисту даних (EDPB) наголошено, що спільний контроль не є питанням формального призначення, а функціональною реальністю, що впливає з фактичного впливу [13].

Прийняття запропонованої норми може призвести до випадків, коли дві або більше сторін спільно визначають цілі та засоби обробки. Потенційну проблему цього для практики можна розглянути на наступному прикладі. Уявімо українську ІТ-компанію, що розробляє мобільний додаток для замовника з ЄС. Якщо українські розробники не просто пишуть код, а пропонують аналітичні метрики, обирають хмарну інфраструктуру (AWS чи Azure) або визначають терміни зберігання логів користувачів, виконавці ризикують бути визнаними спільними контролерами. Результатом буде солідарна відповідальність перед суб'єктом даних [9, ст. 26].

Виходячи з зазначеного, користувач може позиватися до українського розробника за порушення, вчинене європейським замовником, і навпаки. Це вимагатиме від ІТ-компаній укладання детальних угод про розподіл відповідальності (Joint Controller Arrangement), що потенційно може суттєво ускладнити договірну роботу. К. Фішер зазначає, що спільні контролери несуть солідарну відповідальність за шкоду, що означає, що суб'єкт даних може вимагати повної компенсації від будь-якого з контролерів, який потім повинен шукати відшкодування від інших [14].

Також у законопроекті пропонується імплементація права «нового покоління», яке раніше було відсутнє в українському законодавстві.

У ст. 21 законопроекту пропонується надати суб'єкту право вимагати знищення своїх даних без невинуваченої затримки [9, ст. 21]. Нормативне введення права на забуття (Right to be forgotten) може створити проблему для українських реалій, адже більшість вітчизняних CRM-систем та державних реєстрів архітектурно не розраховані на повне фізичне видалення записів (hard delete), віддаючи перевагу маркуванню даних як видалених (soft delete). Вимога ст. 21 змусить бізнес переписувати архітектуру баз даних, щоб забезпечити реальне, а не фіктивне видалення. Однак слід уточнити, що європейська доктрина не трактує «видалення» виключно як миттєве фізичне знищення бітів інформації на всіх носіях одночасно. Згідно з роз'ясненнями EDPB та практикою європейських регуляторів (наприклад, CNIL), у випадках з резервними копіями (backups) допускається архівація даних, якщо контролер

чітко позначає їх як такі, що підлягають видаленню, та забезпечує їхнє вилучення з активного обігу («put beyond use»). Ключовою вимогою є те, щоб у разі відновлення системи з бекапу дані суб'єкта не були «реанімовані», а процедура видалення була застосована до них повторно в автоматичному режимі.

У ст. 23 передбачено закріплення права на отримання своїх даних у структурованому, машинозчитуваному форматі (JSON, XML, CSV) для передачі іншому контролеру [9, ст. 23]. Легітимізація права на мобільність даних (Data portability) може завдати шкоди монополіям екосистем, які утримують користувачів складністю переходу (vendor lock-in). Хоча для IT-стартапів це відкриття можливість переманити користувачів великих корпорацій, для великих компаній виникне необхідність розробки нових, дороговартісних API для експорту даних.

Також ст. 41 передбачено введення інституту відповідальної особи з питань захисту персональних даних (Data Protection Officer, DPO) [9, ст. 41]. Призначення DPO стане обов'язковим для наступних суб'єктів: 1) органи державної влади, окрім судів; 2) контролери, чия основна діяльність передбачає регулярний та систематичний моніторинг фізичних осіб у великих масштабах (трекінг, поведінкова реклама); 3) ті, хто обробляє чутливі дані (здоров'я, біометрія) у великих обсягах [9, ст. 41].

Законопроект дозволяє призначати одного DPO для групи підприємств, що є поступкою для бізнесу [9, ст. 41, ч. 2], проте вимоги до його незалежності та експертизи провокують кадрову кризу. Зокрема, DPO не може бути «звільнений за виконання своїх обов'язків», що надає йому імунітет, подібний до комплаєнс-офіцера в банку [9, ст. 41, ч. 9].

Окрім цього, у запропонованій редакції ст. 37 закріплено, що контролер зобов'язаний повідомити наглядовий орган про витік даних протягом 72 годин після того, як йому стало про це відомо [9, ст. 37]. Якщо витік становить високий ризик для людей, потрібно повідомити і їх самих [9, ст. 38]. Введення жорсткого дедлайну вимагає від бізнесу впровадження систем цілодобового моніторингу (SOC) та розробки планів реагування на інциденти (Incident Response Plans). Старі бюрократичні процедури більше не зможуть забезпечити потреби бізнесу, адже 72 години недостатньо для виконання зазначеної вимоги шляхом старих «паперових» процедур.

Законопроектом пропонується закріпити у ст. 29 принцип проектованої приватності та приватності за замовчуванням [9, ст. 29]. Це означає, що IT-компанії мають закласти механізми захисту (шифрування, псевдонімізацію) на етапі написання технічного завдання, а не перед завершенням продукту. Налаштування конфіденційності повинні бути максимально автоматизовані, але заздалегідь поставити всюди «+» на згоду не можна. Проблематика

імплементції ст. 29 у вітчизняних реаліях полягає у конфлікті між юридичними вимогами та методологією CI/CD (Continuous Integration/ Continuous Delivery). В умовах, коли реліз коду відбувається автоматично кілька разів на день, класична процедура оцінки впливу на захист даних (DPIA) може стати «вузьким місцем». Виникає необхідність впровадження «Automated Compliance Checks», автоматизованих перевірок коду на наявність вразливостей або несанкціонованого збору даних ще до етапу компіляції.

Найбільше занепокоєння викликає ст. 59 [9, ст. 59]. Законопроект передбачає заміну попередньої системи штрафів (зараз максимальний розмір штрафу – 34 тис. грн) на користь відсоткових. Хоча конкретна шкала штрафів законопроектом не передбачена, пропонується визначення «Загальний річний оборот» як бази для розрахунку фінансових санкцій, що узгоджується зі ст. 83 GDPR.

Для великих компаній штраф може сягати 5% від загального річного обороту або 150 мільйонів гривень, залежно від того, що більше [9, ст. 59, ч. 7]. Прихильники цієї позиції (правозахисники, експерти Ради Європи) стверджують, що тільки такі штрафи змусять олігархічні структури та Big Tech дотримуватися закону [15]. Натомість Європейська Бізнес Асоціація (ЄБА) попереджає про ризик банкрутства МСБ та можливість використання штрафів як інструменту тиску на бізнес в умовах корупційних ризиків [7]. Для тих, хто ігнорує закон, ці штрафи стануть суттєвим стимулом для зміни своєї бізнес моделі, але для законослухняного бізнесу це може стати стимулом інвестувати в кібербезпеку.

Хоча у законопроекті № 8153 передбачено підстави для відповідальності та граничні розміри фінансових стягнень, їхня реалізація потребує узгодження з нормами процесуального права. Реформа передбачає пакетний підхід, коли одночасно із законопроектом № 8153 розглядається проект № 6177, який має ввести зміни до Кодексу України про адміністративні правопорушення. Це дозволить розмежувати адміністративну відповідальність посадових осіб та адміністративно-господарські штрафи для юридичних осіб, за аналогією до механізмів, що вже успішно застосовуються Антимонопольним комітетом України.

При цьому слід зазначити, що інші положення законопроекту є принципово необхідними для українського ІТ-аутсорсингу, який працює на глобальному ринку. Так, передача даних дозволена до країн з «належним рівнем захисту» (white list). Для інших країн (наприклад, США, де ситуація з Privacy Shield є нестабільною) необхідно використовувати Стандартні договірні положення (SCCs) або Обов'язкові корпоративні правила (BCR) [9, ст. 46-47]. Якщо Україна не отримає статус «адекватної юрисдикції» від ЄС, то українські ІТ-компанії будуть змушені підписувати SCCs з кожним оєвропейським

клієнтом, що збільшує транзакційні витрати. Проте прийняття законопроекту № 8153 може стати підставою до внесення України до «білого списку» ЄС.

Серед іншого, у законопроекті передбачено трансфер функцій контролю від Омбудсмана до нового незалежного наглядового органу, створення якого визначено суміжним законопроектом № 6177. На сьогодні Омбудсман не має достатніх ресурсів та технічної експертизи для перевірки складних алгоритмів або хмарних сховищ, а тому створення нового державного органу з широкими повноваженнями (доступ до приміщень, вилучення обладнання) викликає у нас побоювання щодо можливих зловживань.

Без реальної незалежності та належного фінансування для залучення кваліфікованих ІТ-аудиторів, новий орган може перетворитися на черговий інструмент тиску або залишитися неефективним. Як зазначають у своєму дослідженні Е. Хіксо та співавтори, створення національних центрів кібербезпеки та впровадження міжнародних стандартів є критичними для стійкості цифрової інфраструктури [8, с. 251].

Щоб оцінити наслідки запропонованих законодавчих змін, доцільно звернутися до емпіричних доказів та інтерпретацій судової практики, що надходять з ЄС. Дослідження 2020–2025 років надають нюансовану картину економічного сліду GDPR, пропонуючи застереження для України, Молдови та Грузії. Хоча регламент посилив приватність і довіру споживачів, він наклав значні витрати на сторону пропозиції цифрової економіки.

Дослідження показують, що вартість дотримання GDPR є регресивною, тобто непропорційно впливає на малі та середні підприємства. Аналіз, на який посилається Федеральна торгова комісія США, зазначає, що в той час як великі підприємства можуть витрачати до 70 мільйонів доларів США на комплаєнс, відносний тягар для малих фірм діє як бар'єр для входу на ринок [16]. При цьому, як зазначається у звіті Cisco 2025 Data Privacy Benchmark Study, малі підприємства до 250 співробітників змушені зменшувати інвестиції у приватність через обмеженість ресурсів, тоді як великий бізнес продовжує нарощувати бюджети [17].

При цьому GDPR може опосередковано сприяти монополізації великих технологічних інкумбенів, коли великі корпорації мають достатні ресурси для покриття витрат на дотримання нормативних вимог, а конкуренти борються за виживання. Це явище, яке називають «GDPR Myopia», підкреслює ситуацію, коли у спробі захистити суб'єктів даних нормативне регулювання може зменшити конкурентоздатність на цифрових ринках [18].

К. Блайнд, К. Нібель та К. Рамер довели, що GDPR змінив характер інновацій у фірмах, стимулював «інкрементальні інновації» (покращення існуючих продуктів через краще управління даними), але водночас пригнічуючи «радикальні інновації» (розробка цілком нових продуктів на основі даних) [19].

Фактично, регламент змушує фірми більш якісно організовувати управління даними, виявляти неефективність та можливості для оптимізації. Але це вимагає ресурсів, які натомість могли бути використані на високоризикові та високоприбуткові R&D. Для перехідних економік, таких як Україна, де радикальні інновації є необхідною умовою для розвитку, імплементація правил GDPR у національне законодавство потребує розробку додаткових механізмів підтримки.

Також доведено, що дотримання норм GDPR призводить до негативного впливу на торговельні потоки ЄС у сфері послуг, які потребують значного використання даних. О. Сісто та Е. Марел підтверджують, що імпорту таких послуг до ЄС скоротився більш ніж на 8% після впровадження GDPR, але найбільше падіння відбулося у секторах з високою залежністю від даних [20].

Висновки. Законопроект № 8153 є революційним, актуальним документом, який виводить Україну з «сірої зони» захисту персональних даних. Його прийняття гармонізує національне право з GDPR, відкриваючи двері до Єдиного цифрового ринку ЄС. Однак, ціна цієї інтеграції може бути високою, викликати надмірне регуляторне навантаження на бізнес, вимагаючи повної перебудови процесів, від розробки ПЗ до маркетингу.

З метою мінімізації негативного впливу на ІТ-галузь та усунення виявлених правових колізій, пропонуємо внести наступні зміни до тексту законопроекту (табл. 2).

Таблиця 2 – Пропозиції щодо вдосконалення проекту Закону № 8153

Стаття проекту	Виявлений недолік / Ризик	Пропонована редакція / Зміна
Ст. 21 Право на забуття	Технічна неможливість миттєвого видалення даних з резервних копій (бекапів) без порушення цілісності системи.	Доповнити частиною: «Вимога щодо знищення не поширюється на резервні копії за умови їх технічної ізоляції та видалення у разі відновлення системи».
Ст. 30 Спільні контролери	Відсутність критеріїв розмежування відповідальності створює ризик подвійного стягнення штрафів.	Закріпити норму: «Відповідальність кожного спільного контролера обмежується межами його фактичного впливу на етапи обробки даних, визначеними в угоді».
Перехідні положення	Відсутність часу на технічну перебудову архітектури баз даних та CI/CD процесів.	Встановити <i>vacatio legis</i> : «Статті, що стосуються технічних стандартів захисту, набирають чинності через 24 місяці після опублікування закону».

Враховуючи викладене, майбутньому регулятору слід зосередитися на розробці галузевих настанов для ІТ, щоб бізнес не витрачав ресурси на створення однотипної документації. Також держава має сприяти створенню програм сертифікації ДРО, адже дефіцит фахівців може створити перепони для дотримання норм закону.

Конфлікт інтересів. Автор декларує, що немає конфлікту інтересів стосовно даного дослідження – фінансового, особистого, авторського чи іншого, який міг би вплинути на дослідження та його результати, представлені в цій статті.

Політика використання штучного інтелекту. Автор декларує, що під час створення даної роботи не використовував методи штучного інтелекту.

Література

1. Про захист персональних даних : Закон України від 01 черв. 2010 р. № 2297-VI. *Відомості Верховної Ради України*. 2010. № 34. Ст. 481. URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text> (дата звернення: 20.02.2026).
2. Брижко В. М. Безпека інформаційної приватності: види та схеми шахрайства у сфері електронно-інформаційної взаємодії. *Інформація і право*. 2022. № 3 (42). С. 65–79. DOI: [https://doi.org/10.37750/2616-6798.2022.3\(42\).270237](https://doi.org/10.37750/2616-6798.2022.3(42).270237) (дата звернення: 26.02.2026).
3. Баранов О. А. Особливості визначення правового статусу робота із штучним інтелектом. *Інформація і право*. 2023. № 4 (47). С. 40–54. DOI: [https://doi.org/10.37750/2616-6798.2023.4\(47\).291581](https://doi.org/10.37750/2616-6798.2023.4(47).291581) (дата звернення: 26.02.2026).
4. Самагальська Ю.Я. Захист персональних даних в мережі Інтернет. *Науковий вісник Ужгородського національного університету. Серія Право*. 2024. № 82 (2). С. 259–263. DOI: <https://doi.org/10.24144/2307-3322.2024.82.2.41> (дата звернення: 26.02.2026).
5. Світличний В.А. Захист персональних даних в умовах воєнного стану в Україні. *Право і безпека*. 2023. № 3 (90). С. 226–236. DOI: <https://doi.org/10.32631/pb.2023.3.19> (дата звернення: 22.02.2026).
6. Климчук О., Гаврилюк А. Штрафи за порушення законодавства про захист персональних даних у розмірах, наближених до GDPR? Що очікувати фізичним та юридичним особам в Україні від Законопроекту про захист персональних даних? / О. Климчук, А. Гаврилюк. *Sayenko Kharenko*. 2024. URL: <https://sk.ua/uk/shtrafi-za-porushennja-zakonodavstva-pro-zahist-personalnih-danih-u-rozmirah-nablizhenih-do-gddr-shho-ochikuvati-fizichnim-ta-juridichnim-osobam-v-ukraini-vid-novogo-zakonoproiektu-pro-zahist-personal/> (дата звернення: 20.02.2026).
7. Chernyavsky N., Khomenko I. Ukraine: Data Protection Laws and Regulations 2025-2026. *International Comparative Legal Guides (ICLG)*. 2026. URL: <https://iclg.com/practice-areas/data-protection-laws-and-regulations/Ukraine> (дата звернення: 22.02.2026).
8. Xhixho E., Pazylov N. Digital Transformation in the Legal Sector: Challenges and Opportunities for Cybersecurity and Data Protection / E. Xhixho, N. Pazylov, V. Savchenko, N. Patiev, M. Pazylova. *Law, State and Telecommunications Review*. 2025. Vol. 17, no. 1. P. 250–271. DOI: doi.org/10.26512/lstr.v17i1.56176 (дата звернення: 18.02.2026).
9. Про захист персональних даних : проєкт Закону України від 25 жовт. 2022 р. № 8153. URL: <https://itd.rada.gov.ua/billinfo/Bills/Card/40707> (дата звернення: 26.02.2026).

10. 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.
11. Case C-492/23. X v. Russmedia Digital SRL : CJEU, 2 December 2025. *InfoCuria : Case-law*. URL: <https://curia.europa.eu/juris/liste.jsf?num=C-492/23> (дата звернення: 21.02.2026).
12. Case C-683/21. Deutsche Umwelthilfe eV v. Bundesrepublik Deutschland : Judgment of the Court (Thirteenth Chamber) of 7 December 2023. *InfoCuria : Case-law*. URL: <https://infocuria.curia.europa.eu/tabs/document?docid=280324&doclang=EN> (дата звернення: 22.02.2026).
13. Guidelines 07/2020 on the concepts of controller and processor in the GDPR : Version 2.1 : Adopted on 07 July 2021. *European Data Protection Board*. 2021. 51 p. URL: https://www.edpb.europa.eu/system/files_en?file=2023-10/EDPB_guidelines_202007_controllerprocessor_final_en.pdf (дата звернення: 23.02.2026).
14. Fischer C. Re-thinking the allocation of roles under the GDPR in the context of cloud computing. *International Data Privacy Law*. 2024. Vol. 14, Iss. 1. P. 53–65. DOI: <https://doi.org/10.1093/idpl/ipad023> (дата звернення: 22.02.2026).
15. Discussion of the Draft Law 8153 "On Personal Data Protection". *European Business Association*. 2025. URL: <https://eba.com.ua/en/obgovorennya-zakonoprojektu-8153-pro-zahyst-personalnyh-danyh/> (дата звернення: 24.02.2026).
16. Harmeling T. How much does GDPR compliance really cost? Guide for 2025. *Consent Management Platform (CMP) Usercentrics*. URL: <https://usercentrics.com/knowledge-hub/cost-of-gdpr-compliance/> (дата звернення: 20.02.2026).
17. Cisco 2025 Data Privacy Benchmark Study. Cisco Systems. 2025. URL: https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-privacy-benchmark-study-2025.pdf (дата звернення: 22.02.2026).
18. Yun J. A Report Card on the Impact of Europe's Privacy Regulation (GDPR) on Digital Markets. *GEO. MASON L. REV. F.* 2024. Vol. 31, Iss. 104. URL: <https://lawreview.gmu.edu/forum/a-report-card-on-the-impact-of-europes-privacy-regulation-gdpr-on-digital-markets/> (дата звернення: 20.02.2026).
19. Blind K., Niebel C. M., Rammer C. The impact of the EU General Data Protection Regulation on innovation in firms. *ZEW Discussion Papers*. 2022. No. 22-047. 48 p. URL: <https://www.econstor.eu/handle/10419/265420> (дата звернення: 22.02.2026).
20. Sisto E., Marel E. Privacy at a Price? An Empirical Analysis of GDPR's Impact on EU Trade Flows. *European Centre for International Political Economy (ECIPE)*. 2025. URL: <https://ecipe.org/publications/gdpr-impact-on-eu-trade-flows/> (дата звернення: 22.02.2026).

THE INNOVATIONS OF BILL NO. 8153 AND THEIR IMPACT ON THE IT INDUSTRY

M. Hura

Abstract: to conduct a legal analysis of Draft Law of Ukraine No. 8153 “On the Protection of Personal Data” which has been adopted as a basis by the Verkhovna Rada of Ukraine and is currently being prepared for its second reading, to assess its compliance with European standards (GDPR).

Content: This study focuses on the implementation of European standards (GDPR) into national law and the resulting conflicts. The article critically examines the problem of the outdated paradigm of the current 2010 Law and its failure to meet the challenges of the digital economy. The author provides a detailed analysis of the transformation of the conceptual framework (the introduction of the terms “joint controller,” “controller,” and “processor”), new institutions (DPO, Privacy by Design, and others), as well as mechanisms for cross-border data transfers, particularly to non-European jurisdictions that lack an adequate level of data protection. Particular attention is paid to the legal characterization of roles in IT outsourcing and the risks of joint and several liability through the lens of current CJEU case law. The article examines the experience of GDPR implementation in the European Union and the negative consequences for small and medium-sized businesses. Separately, the article analyzes the impact of establishing a new supervisory authority, as provided for in Draft Law of Ukraine No. 6177 “On the National Commission for the Protection of Personal Data and Access to Public Information,” and the transfer of powers from the Ombudsman to this body. The article analyzes the business risks that the implementation of Law of Ukraine No. 8153 “On the Protection of Personal Data” may pose for business entities in Ukraine, particularly regarding the establishment of technical capabilities for the protection of personal data, including designed privacy and privacy by default.

Results and Conclusions: The researcher concludes that a mechanical application of regulations without considering technological processes (CI/CD, data archiving) could lead to legal uncertainty and proposes specific amendments to the draft law.

Keywords: personal data protection, GDPR, Bill No. 8153, controller, operator, IT compliance, cross-border data transfer, joint controllers, Data Protection Officer.

Стаття надійшла до редакції / Received: 27.02.2026

Прийнята до друку після рецензування / Revised and Accepted: 18.03.2026

Дата публікації статті / Published: 21.04.2026.