

УДК 343.61:342.9:004.6(477)

АДМІНІСТРАТИВНА ВІДПОВІДАЛЬНІСТЬ ЗА ПОРУШЕННЯ ЗАКОНОДАВСТВА У СФЕРІ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ: ТЕОРЕТИКО-ПРАВОВІ ТА ПРАКТИЧНІ АСПЕКТИ

Ковбас Ігор*, Колотило Марія**

**Чернівецький національний університет імені Юрія Федьковича,
вул. Коцюбинського, 2, Чернівці, Чернівецька область, Україна, 58012,
e-mail: kovbasigor@ukr.net*

ORCID ID: 0000-0001-7039-1586

***Публічне акціонерне товариство «Укрнафта»,
Несторівський пров., 3–5, Київ, Україна, 04053,
e-mail: mary.kolotylo@gmail.com*

ORCID ID: 0009-0003-6327-4439

Присвячено аналізу адміністративної відповідальності за порушення законодавства у сфері захисту персональних даних в Україні, з особливим акцентом на теоретичні, правові та практичні аспекти цього питання. Розглянуто актуальність та необхідність посилення захисту персональних даних в умовах стрімкого розвитку цифрових технологій та поширення інформаційних систем. Досліджено наявні механізми адміністративної відповідальності, їхні вади та потенціал для удосконалення, базуючись на аналізі чинного законодавства та судової практики. Особливу увагу приділено Конституційному праву громадян на конфіденційність персональних даних, порушення якого часто не супроводжуються адекватними адміністративними санкціями. Представлено конкретні рекомендації щодо реформування адміністративно-правових норм, зокрема ст. 188-39 Кодексу України про адміністративні правопорушення, аби зробити систему відповідальності ефективнішою та справедливішою. Висвітлено декілька судових рішень, що ілюструють практичне застосування цих норм та підкреслюють проблеми в їхньому втіленні. Запропоновано шляхи вдосконалення законодавства для підвищення захисту прав громадян і зміцнення правової охорони персональних даних.

Аналізуючи чинні нормативні акти, можна виявити значні прогалини у правовому регулюванні захисту персональних даних. Це, зокрема, стосується недостатньої чіткості визначення обов'язків та відповідальності суб'єктів, що здійснюють обробку даних. Слабке врегулювання цієї сфери призводить до того, що порушення можуть залишатися без належного реагування та покарання, а отже, знижується ефективність захисту персональних прав громадян.

У світлі цих викликів, наявність ефективної системи адміністративної відповідальності є важливою для забезпечення права кожної особи на конфіденційність своїх даних. Потрібно не тільки реформувати наявні норми, а й забезпечити їхнє дотримання через більш ефективні контрольні механізми та освітні програми для суб'єктів, які працюють із персональними даними. Розробка чітких, доступних та зрозумілих інструкцій для організацій, які обробляють персональні дані, може значно підвищити рівень їх захисту від зловживань і неправомірного використання.

Ключові слова: захист приватності, інформаційна відповідальність, повноваження контролюючих органів, європейські підходи, доступ до інформації.

DOI: <http://dx.doi.org/10.30970/vla.2025.80.220>

Вступ. В епоху діджиталізації питання захисту персональних даних є одним із ключових елементів правової безпеки особи. Адміністративна відповідальність є важливим інструментом реагування на порушення у цій сфері. Водночас Україна стикається з низкою викликів і нормативного, і практичного характеру. Актуальність теми зумовлена необхідністю увідповіднення національного законодавства до міжнародних, насамперед європейських, стандартів. Метою цієї статті є аналіз теоретико-правових засад та практики застосування адміністративної відповідальності у сфері персональних даних.

Постановка проблеми. Захист персональних даних у сучасному світі набуває дедалі більшої актуальності, враховуючи стрімкий розвиток цифрових технологій та поширення інформаційних систем. Це ставить під загрозу конфіденційність особистих даних та вимагає ефективних механізмів їх захисту. Проте наявні санкції за порушення законодавства про захист персональних даних часто виявляються невідповідними або неефективно застосованими, що знижує стримувальний ефект відповідальності. Тому виникає необхідність перегляду та удосконалення адміністративної відповідальності в цій сфері для забезпечення реального захисту прав громадян.

Стан опрацювання. Тема захисту персональних даних залишається високоактуальним у науковому дискурсі, що відображається у численних дослідженнях. Зокрема, праці таких учених, як М. В. Різак, А. В. Тунік та Ю. С. Самойленко, присвячені аналізу правових механізмів, наявних прогалин у регулюванні та потенційним шляхам модернізації українського законодавства в цій галузі. Крім того, значний внесок у розвиток теми зробили й інші дослідники, які продовжують формувати сучасне наукове підґрунтя для забезпечення ефективного захисту персональних даних.

Метою цього дослідження є аналіз чинного законодавства України та судової практики, щоб визначити ефективність норм, що регулюють захист персональних даних, та виявити прогалини, що потребують удосконалення, з метою підвищення захисту прав громадян у цій сфері.

Виклад основного матеріалу. Захист персональних даних у сучасному інформаційному суспільстві набуває особливого значення, оскільки дотримання конфіденційності особистих даних є фундаментальним правом кожної людини. Ст. 32 Конституції України гарантує кожному громадянину право на доступ до інформації про себе, яка не є державною таємницею [1]. Порушення у цій сфері несе суттєві ризики для особистої конфіденційності та може призвести до небажаних наслідків для приватного життя особи.

Теоретичні аспекти адміністративної відповідальності за порушення законодавства у сфері захисту персональних даних.

Адміністративна відповідальність у контексті захисту персональних даних охоплює дії, що порушують законодавчі вимоги щодо їх обробки та захисту. Часто порушення відбуваються без наявності реальної шкоди, проте потенційний ризик для інформаційної безпеки особи вимагає суворих заходів реагування. Ці порушення загрожують стабільності інформаційних відносин та збільшують вразливість систем до незаконних втручань.

У контексті адміністративних проступків ці порушення часто розглядаються як відхилення від адміністративно-регламентних норм із помірним ступенем суспільної небезпеки. Законодавець, однак, не завжди визначає такі дії, як суспільно небезпечні, що не дозволяє автоматично наступати відповідальності. Тому виникає необхідність деліктизації порушень прав суб'єктів персональних даних і встановлення юридичної відповідальності безпосередньо за факт вчинення протиправних дій.

Передусім, з'ясуємо, що таке персональні дані. Закон України «Про захист персональних даних» [2] разом із Законом «Про інформацію» [3] визначають ці дані як відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути ідентифікована. Це означає, що будь-яка інформація, яка дозволяє встановити особу, особистість людини, вважається персональними даними.

Адміністративна відповідальність за порушення законодавства у сфері захисту персональних даних в Україні передбачена ст. 188-39 Кодексу України про адміністративні правопорушення (далі – КУПАП). Ця стаття детально регулює відповідальність за різні види порушень, пов'язаних з персональними даними, і встановлює конкретні штрафи за такі дії.

Ст. 188-39 визначає кілька основних видів порушень:

- «неповідомлення або несвоєчасне повідомлення Уповноваженого Верховної Ради України з прав людини про обробку персональних даних або про зміну відомостей, які підлягають повідомленню згідно із законом, повідомлення неповних чи недостовірних відомостей;

- невиконання законних вимог (приписів) Уповноваженого Верховної Ради України з прав людини або визначених ним посадових осіб секретаріату Уповноваженого Верховної Ради України з прав людини щодо запобігання або усунення порушень законодавства про захист персональних даних;

- повторне протягом року вчинення порушення з числа передбачених частинами першою або другою цієї статті, за яке особу вже було піддано адміністративному стягненню;

- недодержання встановленого законодавством про захист персональних даних порядку захисту персональних даних, що призвело до незаконного доступу до них або порушення прав суб'єкта персональних даних;

- повторне протягом року вчинення порушення, передбаченого частиною четвертою цієї статті, за яке особу вже було піддано адміністративному стягненню» [4].

Практичні аспекти адміністративної відповідальності за порушення законодавства у сфері захисту персональних даних.

Однією з перешкод на шляху до ефективної реалізації цих механізмів є недосконалість формулювання відповідних юридичних норм. Наприклад, ст. 188-39 КУПАП регулює відповідальність за порушення порядку захисту персональних даних, що призвело до незаконного доступу, однак порядок захисту не має чіткого визначення в законодавстві, що ускладнює кваліфікацію таких дій та вибір належного покарання [4].

Відсутність єдиного тлумачення ключових понять («персональні дані», «згода суб'єкта даних», «обробка даних») у нормативних актах створює ґрунт для дисперсії у правозастосовній практиці. Це провокує розбіжності у кваліфікації правопорушень суб'єктами, які здійснюють оцінку відповідності (наприклад, судами або органами нагляду).

У практичній площині реалізація положень ст. 188-39 Кодексу України про адміністративні правопорушення виявляється не завжди результативною. Аналіз рішень, ухвалених Шевченківським районним судом м. Києва та Придніпровським районним судом м. Черкаси, демонструє обмежену ефективність цієї норми, що значною мірою зумовлено її недостатньо чітким законодавчим формулюванням. У низці справ відповідальність осіб встановлюється переважно за повторне порушення, що свідчить про наявність системних недоліків у механізмах контролю та загальну неефективність процедур правозастосування у сфері охорони персональних даних.

Однією з ключових проблем є відсутність Закону «Про захист персональних даних» у переліку нормативних актів, які регулюють обов'язок надання інформації. Така законодавча прогалина породжує правову невизначеність і ускладнює трактування меж відповідальності, зокрема в контексті застосування положень ст. 212-3 Кодексу України про адміністративні правопорушення. Відсутність чітких орієнтирів для суб'єктів правозастосування щодо кваліфікації дій, пов'язаних із ненаданням інформації про персональні дані, створює умови для неоднозначного правозастосування та, як наслідок, зниження рівня гарантій права на доступ до інформації.

Інший важливий аспект стосується нормотворчої техніки та потреби постійного оновлення КУпАП відповідно до змін у законодавстві. Така системна вимога є не тільки ресурсозатратною, а й сприяє затримкам у законодавчому реагуванні на нові виклики у сфері захисту даних. Це може призводити до правового вакууму, де нові законодавчі ініціативи не мають належного адміністративно-правового забезпечення, залишаючи певні суспільні відносини незахищеними на перехідний період.

Зміна редакції ст. 212-3 КУпАП у 2014 р., що розділила порушення, пов'язані з доступом до інформації, на кілька окремих частин, заслуговує на окрему увагу. Це рішення, що мало на меті уточнити відповідальність, насправді ускладнило процес юридичної кваліфікації порушень через різноманітність норм, кожна з яких вимагає окремого застосування. Це може сприяти неоднаковому застосуванню правосуддя та утрудненню правозастосування.

Важливим є відсутність у новій редакції ст. 212-3 КУпАП згадки про Закон «Про інформацію» [3]. В результаті цього, право людини на інформацію про себе залишається без необхідних правових гарантій, що є серйозним упущенням з погляду захисту особистих даних.

Як було зазначено, ст. 212-3 КУпАП, хоч і зазнала кількох редакційних змін з моменту свого існування, все ж таки залишає бажати кращого в контексті включення вичерпного переліку можливих порушень права на інформацію. Значне розширення вимог до охоплення всіх аспектів обробки персональних даних є вкрай необхідним для адекватного реагування на порушення.

Ст. 212-3 КУпАП, незважаючи на свої редакційні переробки, продовжує мати суттєві недоліки в частині належного конструювання санкцій. Розміри штрафів, передбачені за адміністративні порушення у цій сфері, залишаються недостатніми для реального відображення ступеня небезпеки цих діянь. Як наслідок, ефективність таких санкцій часто опиняється під сумнівом. Зазначені недоліки в конструкції санкцій ст. 212-3 КУпАП вказують на необхідність їх глибшого перегляду та зміни.

Оновлення ст. 212-3 КУпАП повинно включати повний перегляд санкцій з метою їх узгодження із реальними економічними та соціальними умовами та рівнем небезпеки порушень. Окрім того, важливим кроком стане деталізація ст. 182 КК України з урахуванням усіх видів обробки персональних даних, що мають бути визначені Законом «Про захист персональних даних». Такі зміни сприятимуть усуненню невизначеностей і непорозумінь під час кваліфікації злочинів, а також підвищенню рівня правової охорони приватності.

Серед інших проблем, які потребують уваги, варто вказати на неузгодженість у визначенні часових рамок для повторних порушень у чинному КУпАП. Відсутність чітких вказівок щодо моменту початку річного терміну для повторного порушення створює плутанину і несправедливість у притягненні до відповідальності.

Окрім того, законодавче конструювання уповноважених суб'єктів зі складанням адміністративних протоколів вимагає переосмислення. Наприклад, зараз відповідно до ст. 255 КУпАП право на складання протоколів мають лише посадові

особи секретаріату уповноваженого, що ставить під сумнів ефективність і повноту їхніх адміністративно-процесуальних функцій.

Важливою є також необхідність перегляду санкцій, аби зменшити розрив між нижніми та верхніми межами штрафів, який нині сягає від 100% до 500% залежно від статті. Таке широке коливання не сприяє створенню справедливої та ефективної системи покарань і надає простір для суб'єктивного трактування законодавства, що підриває довіру громадян до механізмів захисту їхніх прав.

Значні проблеми виникають з недостатньою визначеністю понять та процедур у Законі України «Про захист персональних даних», що ставить під сумнів можливість ефективного їх застосування [2]. Припущення про неіснування порушень відображає нестачу реальних механізмів контролю за дотриманням законодавства. Удосконалення цих аспектів, зокрема через введення чітких вимог до захисту персональних даних і обов'язку їх дотримання, може значно покращити ситуацію.

Відповідно до положень Закону України «Про захист персональних даних», на суб'єктів, які здійснюють обробку персональної інформації, покладаються чітко визначені обов'язки та відповідальність [2]. Порушенням законодавства, зокрема, визнаються такі дії, як відсутність повідомлення суб'єкта про факт збору його даних, незаконна їх обробка або ненадання доступу до відповідної інформації. Вказані порушення можуть слугувати підставою для притягнення до адміністративної відповідальності. Водночас результати аналізу правозастосовної практики та матеріали щорічних доповідей Уповноваженого Верховної Ради України з прав людини [13] засвідчують низький рівень фактичного застосування санкцій. Це, своєю чергою, свідчить про відсутність належного стимулюючого впливу на суб'єктів обробки персональних даних із метою дотримання законодавчих вимог.

Процес виявлення та реагування на порушення є багатоетапним: від перевірок Уповноваженим з прав людини до можливості винесення припису про усунення порушень. Винесення припису не завжди супроводжується реальними наслідками для порушника, а випадки невиконання приписів часто завершуються лише формальними протоколами без подальшого реального покарання. Це свідчить про неефективність наявної системи адміністративної відповідальності.

Аналіз національних судових рішень показує, що навіть коли особу визнають винною у порушенні, часто суди не накладають штрафи через затягування процесів або закінчення строків давності для накладення покарань. Велика кількість порушень, які вимагають тривалого часу для виявлення та документування, ускладнює швидке та ефективне вирішення проблем, пов'язаних із захистом персональних даних [5; 6].

Така ситуація вказує на необхідність реформ у системі адміністративної відповідальності за порушення законодавства про захист персональних даних. Зокрема, важливо переглянути наявні норми та положення, зробити їх чіткішими та передбачуваними, а також встановити реальні механізми відповідальності, які ефективно стимулюватимуть суб'єктів до дотримання закону. Водночас доцільно враховувати положення Загального регламенту ЄС про захист даних (General Data Protection Regulation, GDPR), який передбачає комплексний підхід до регулювання цієї сфери, включаючи прозорість обробки даних, права суб'єктів персональних даних та сувору систему санкцій. Урахування міжнародних стандартів сприятиме гармонізації національного законодавства та підвищенню рівня захисту інформації.

Одним із виразних прикладів є справа №361/1579/20, розглянута Броварським міськрайонним судом Київської області, де голова правління СТ «Заліське» була

визнана винною в незаконному розповсюдженні персональних даних через месенджер Viber. Не забезпечивши належний захист персональних даних, вона розмістила копію звернення особи з відкритим доступом до її персональної інформації, що призвело до незаконного доступу невизначеного кола осіб.

Суд, аналізуючи докази, встановив, що дії відповідачки спричинили порушення правил захисту персональних даних, зокрема, їх незаконне поширення та відкритий доступ до них, що суперечить положенням ст. 32 Конституції України та Закону України «Про захист персональних даних». Правопорушення мало місце з 27 грудня 2019 р. до 02 березня 2020 р. На підставі зібраних доказів та норм законодавства суддя визнала ОСОБУ_2 винною у вчиненні адміністративного правопорушення та наклала штраф у розмірі 5 100 грн [7].

Цей випадок підкреслює кілька важливих аспектів. По-перше, він вказує на необхідність чіткого розуміння суб'єктами, що обробляють персональні дані, їхніх обов'язків та вимог законодавства. По-друге, винесений штраф слугує попередженням для інших потенційних порушників про серйозність наслідків порушень законодавства про захист персональних даних.

Також слід розглянути справу №761/23532/20, де Шевченківський районний суд Києва також визнав особу винною за аналогічні порушення. У цій справі було виявлено, що тимчасово виконуючий обов'язки президента Національної академії державного управління допустив публікацію на офіційному вебсайті наказу, що містив персональні дані мешканців гуртожитку. Цей випадок порушення став предметом судового розгляду, внаслідок чого посадову особу притягнуто до відповідальності згідно з ч. 4 ст. 188-39 КУпАП.

Згідно зі Законом України «Про захист персональних даних», кожен громадянин має право на захист своїх персональних даних від неправомірного збору, зберігання та поширення. Порушення цих норм призводить до адміністративної відповідальності, що було демонстровано в цій справі. Розголошення даних без згоди осіб або за відсутності законних підстав є серйозним порушенням, яке тягне за собою не тільки моральні, а й юридичні наслідки.

У ході судового процесу було встановлено, що докази, надані обвинуваченням, достатньо підтверджують факт порушення. Проте через процедурні особливості, зокрема через вплив терміну давності на момент розгляду справи, провадження було закрито. Це підкреслює важливість не тільки законності дій посадових осіб, а й своєчасності реакції правоохоронних органів та судових інстанцій. Справа № 761/23532/20 є показовим прикладом адміністративної відповідальності за порушення законодавства у сфері захисту персональних даних [8].

Удосконалення адміністративної відповідальності за порушення законодавства у сфері захисту персональних даних.

Наукові дослідження та практичний досвід свідчать про потребу системного перегляду адміністративних санкцій і штрафів, які застосовуються за порушення в обробці персональних даних. Наприклад, зараз відповідальність за несвоєчасне повідомлення про зміни в обробці персональних даних, як передбачено ст. 188-39 Кодексу України про адміністративні правопорушення, вимагає ревізії з метою її узгодження з принципами справедливості та пропорційності [4].

Ключовим аспектом є впровадження більш гнучких підходів до визначення відповідальності, які б враховували характер порушення та його наслідки для прав суб'єктів даних. Це може включати запровадження різних рівнів штрафів залежно від тяжкості порушень і потенційного ризику для прав та свобод осіб. Також розглядається можливість введення попереджень за менш серйозні порушення, що

надасть суб'єктам можливість виправити недоліки без застосування фінансових санкцій, в такий спосіб підвищуючи ефективність регуляторних механізмів.

Заразом, із метою забезпечення адекватного рівня захисту персональних даних, слід розглянути можливість створення більш жорстких рамок відповідальності за систематичні порушення, які можуть завдавати значної шкоди особистісним правам. Вирішенням цього питання могла б стати взаємодія з міжнародними організаціями та впровадження кращих практик захисту даних, що використовуються у світі [9], [10].

Як слушно зауважує Ю. Самойленко «запровадження змін у законодавство, яке визначає адміністративну відповідальність за порушення правил обробки, використання та захисту персональних даних, вимагає коригування. Поточні норми часто встановлюють надто високі штрафи за порушення, що не завжди корелюють із ступенем ризику або наслідками. Наприклад, штрафи за порушення, описані в ч. 1 ст. 188–39 КУпАП [4], які стосуються затримки у повідомленні про обробку персональних даних або подання некоректних відомостей, досягають від 1 700 до 6 100 грн, що суттєво перевищує штрафи за порушення у багатьох інших сферах, наприклад, проїзд на заборонювальний сигнал світлофора, що незалежно від волі водія могло призвести до тяжких наслідків, встановлена відповідальність у вигляді штрафу на суму 425 грн (ч. 2 ст. 122 КУпАП), за порушення порядку благоустрою (створення несанкціонованих звалищ сміття), що може призвести до негативних екологічних наслідків, встановлена відповідальність у вигляді штрафу на суму від 340 до 1 360 грн (ст. 152 КУпАП)» [11].

Така невідповідність у розмірах штрафів може сприяти виникненню корупційних ризиків та відчуттю несправедливості у відповідальності, особливо у випадках несвідомих порушень або через нестачу кваліфікованих кадрів у малому та середньому бізнесі. У зв'язку з цим доцільним є внесення змін до ст. 188–39 КУпАП, зокрема шляхом передбачення можливості застосування попередження за малозначні порушення та зниження розміру штрафів — наприклад, встановлення фіксованої санкції в обсязі ста неоподатковуваних мінімумів доходів громадян. Це дозволить узгодити стримувальні заходи із принципами справедливого правосуддя.

У цьому контексті особливої уваги набуває процедура надання адміністративних послуг, під час якої часто здійснюється обробка персональних даних громадян. Важливо забезпечити, щоб така діяльність відповідала вимогам законодавства щодо захисту персональної інформації. Як зазначає І. В. Ковбас, «адміністративні послуги являють собою законодавчо-врегульовану діяльність органів публічної адміністрації, яка здійснюється ними на підставі звернення і в інтересах фізичної чи юридичної особи та кінцевим результатом якої є видання адміністративного акту, що створює умови для виникнення прав та обов'язків у його користувача» [12]. Це визначення підкреслює не лише функціональний, а й правовий аспект надання адміністративних послуг, що має важливе значення для дотримання стандартів конфіденційності.

Висновки. Адміністративна відповідальність за порушення законодавства у сфері захисту персональних даних має важливе значення для забезпечення права кожної особи на конфіденційність своїх персональних даних. Оскільки недотримання цих норм може призводити до значних порушень приватності, відповідальність повинна бути адекватною та стримувальною, щоб запобігти незаконному використанню чи витоку даних. Проте практична реалізація санкцій часто виявляється неефективною, оскільки штрафи та інші міри можуть не відповідати суспільній небезпеці діянь, що призводить до потреби в перегляді встановлених покарань та методів їх застосування. На практиці зміни в законодавство повинні

сприяти більшій прозорості та справедливості в процесі накладення штрафів. Потреба в точніших визначеннях порушень та більш ретельному розмежуванні ступеня їх впливу на права індивідів є критичною. Зміцнення правового поля для захисту персональних даних вимагає також освіти суб'єктів, які здійснюють обробку даних, щодо їх обов'язків і наслідків порушень, що сприятиме загальній правовій освіченості та зниженню кількості випадків недотримання норм.

Список використаних джерел

1. Конституція України від 28.06.1996. URL: <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80/conv#Text> (дата звернення: 05.03.2025).
2. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI. URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text> (дата звернення: 05.03.2025).
3. Про інформацію : Закон України від 02.10.1992 № 2657-XII. URL: <https://zakon.rada.gov.ua/laws/show/2657-12#Text> (дата звернення: 05.03.2025).
4. Кодекс України про адміністративні правопорушення (статті 1 - 212-24) : Кодекс України; Закон. Кодекс від 07.12.1984 № 8073-X. URL: <https://zakon.rada.gov.ua/laws/show/80731-10#Text> (дата звернення: 05.03.2025).
5. Постанова Московського районного суду міста Харкова від 04 травня 2017 р. по справі № 643/3384/17. URL: <http://reyestr.court.gov.ua/Review/66441353> (дата звернення: 05.03.2025).
6. Постанова Золочівського районного суду Львівської області від 20 грудня 2016 р. по справі 445/2022/16-п. URL: <http://reyestr.court.gov.ua/Review/63869054> (дата звернення: 05.03.2025).
7. Постанова Броварського міськрайонного суду Київської області від 09 квітня 2020 року у справі № 361/1579/20. URL: <https://reyestr.court.gov.ua/Review/88698313> (дата звернення: 05.03.2025).
8. Постанова Шевченківського районного суду міста Києва від 15 вересня 2020 року у справі № 761/23532/20. URL: <https://reyestr.court.gov.ua/Review/91799128> (дата звернення: 05.03.2025).
9. Різак М. В. Правове регулювання відносин обігу персональних даних : дис.... канд. юрид. наук : 12.00.07. *Держ. НДІ МВС України*. Київ, 2012. 214 с.
10. Тунік А. В. Правові основи захисту персональних даних: дис.... канд. юрид. наук : 12.00.07. *Нац. авіаційний університет*. Київ, 2012. 213 с.
11. Самойленко Ю. С. Особливості, вади та шляхи вдосконалення правового забезпечення захисту персональних даних в Україні. *Право і суспільство*. 2020. № 6–2. Ч. 2. URL: http://pravouspilstvo.org.ua/archive/2020/6-2_2020/part_2/7.pdf (дата звернення: 05.03.2025).
12. Ковбас І., Боднар С. Адміністративні послуги: поняття та порядок їх надання органами публічної адміністрації. *Visegrad Journal on Human Rights*. 2016. № 1. С. 96–102 (дата звернення: 05.03.2025).
13. Щорічна доповідь про стан додержання та захисту прав і свобод людини і громадянина в Україні за 2023 рік. URL: <https://ombudsman.gov.ua/report-2023> (дата звернення: 22.04.2025).

References

1. *Constitution of Ukraine of 28.06.1996*. Retrieved from <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80/conv#Text> (accessed: 05.03.2025).
2. *On the Protection of Personal Data Law of Ukraine of 01.06.2010. No. 2297-VI*. Retrieved from <https://zakon.rada.gov.ua/laws/show/2297-17#Text> (accessed: 05.03.2025).
3. *On Information Law of Ukraine of 02.10.1992. No. 2657-XII*. Retrieved from <https://zakon.rada.gov.ua/laws/show/2657-12#Text> (accessed: 05.03.2025).

4. *Code of Ukraine on Administrative Offences (Articles 1 - 212-24) : Code of Ukraine; Law. Code of 07.12.1984 No. 8073-X*. Retrieved from <https://zakon.rada.gov.ua/laws/show/80731-10#Text> (accessed: 05.03.2025).
5. *Resolution of the Moscow District Court of Kharkiv of 04 May 2017 in case No. 643/3384/17*. Retrieved from <http://reyestr.court.gov.ua/Review/66441353> (accessed: 05.03.2025).
6. *Resolution of the Zolochiv District Court of Lviv Region of 20 December 2016 in case 445/2022/16-p*. Retrieved from <http://reyestr.court.gov.ua/Review/63869054> (accessed: 05.03.2025).
7. *Ruling of the Brovary City District Court of Kyiv Region of 09 April 2020 in case No. 361/1579/20*. Retrieved from <https://reyestr.court.gov.ua/Review/88698313> (accessed: 05.03.2025).
8. *Resolution of the Shevchenkivskyi District Court of Kyiv of 15 September 2020 in case No. 761/23532/20*. Retrieved from <https://reyestr.court.gov.ua/Review/91799128> (accessed: 05.03.2025).
9. Rizak, M. V. (2012). Legal regulation of relations of personal data circulation: PhD in Law: 12.00.07. *State Research Institute of the Ministry of Internal Affairs of Ukraine*. Kyiv.
10. Tunik, A. V. (2012). Legal basis for the protection of personal data : Candidate of Laws: 12.00.07. *National Aviation University*. Kyiv.
11. Samoilenko, Y. S. (2020). Features, shortcomings and ways to improve the legal support for the protection of personal data in Ukraine. *Law and Society*, 6–2, 2. Retrieved from http://pravoisuspilstvo.org.ua/archive/2020/6-2_2020/part_2/7.pdf (accessed: 05.03.2025).
12. Kovbas, I., Bodnar, S. (2016). Administrative services: the concept and procedure for their provision by public administration bodies. *Visegrad Journal on Human Rights*, 1, 96–102 (accessed: 05.03.2025).
13. *Annual report on the state of observance and protection of human and civil rights and freedoms in Ukraine for 2023*. Retrieved from <https://ombudsman.gov.ua/report-2023> (accessed: 04.22.2025).

ADMINISTRATIVE LIABILITY FOR VIOLATIONS OF PERSONAL DATA PROTECTION LEGISLATION: THEORETICAL, LEGAL AND PRACTICAL ASPECTS

Ihor Kovbas*, Mariia Kolotylo**

**Yurii Fedkovych Chernivtsi National University,
2, Kotsiubynskoho Str., Chernivtsi, Chernivtsi region, Ukraine, 58012,
e-mail: kovbasigor@ukr.net*

ORCID ID: 0000-0001-7039-1586

***Zaporizhzhia National University, PJSC Ukrnafta,
3-5, Nestorivskiy lane, Kyiv, Ukraine, 04053,
e-mail: mary.kolotylo@gmail.com,
ORCID ID: 0009-0003-6327-4439*

The article examines administrative liability for violation of legislation in the field of personal data protection in Ukraine. The purpose is to identify the shortcomings of the current administrative and legal regulations, to analyze its effectiveness and to formulate practical recommendations for improvement. The object of the study is the mechanism of administrative liability for offences in the field of personal data processing. The authors use the methods of system analysis, comparative jurisprudence, formal legal and empirical methods to analyze legislation, court decisions and the practice of the Ukrainian Parliament Commissioner for Human Rights.

As a result, it is established that the current edition of Articles 188-39 of the Code of Administrative Offences is ineffective, contains evaluative wording, does not provide for adequate punishment for violations, and the court practice shows that it is difficult to prove the elements of the offence. A low level of law enforcement is identified due to the lack of clear procedural instructions and methodological recommendations for controlling authorities. The authors propose to amend the Code of Administrative Offences by specifying the *corpus delicti*, expanding the list of subjects of liability, and increasing the amount of penalties with due regard for the severity of the consequences.

The authors substantiate the need to combine legal regulation with preventive measures, including raising awareness of entities processing personal data. The article provides a comparative description of the Ukrainian approach and the provisions of the GDPR, which allowed the authors to identify key differences and potential benchmarks for improving national legislation. In particular, attention is drawn to the need to harmonize terminology, control mechanisms and sanctions in accordance with European standards.

The authors also analyse the concept of damage caused by the violation of privacy rights and emphasize the importance of defining clear criteria for its assessment. For the first time, the authors propose a specific algorithm for improving administrative and legal provisions in the field of personal data protection, including regulatory detailing of the offence, updating the competencies of regulatory authorities, digitalization of the process of recording violations and creation of an open register of violators.

The practical value of the paper lies in the possibility of using the results of the study in the development of legislative initiatives, in the work of the Commissioner, the National Police, judicial authorities, as well as business entities that process personal data. The proposed provisions are aimed at strengthening the legal protection of an individual, increasing legal certainty and the effectiveness of prosecution.

Keywords: privacy protection, information responsibility, powers of regulatory authorities, European approaches, access to information.

*Стаття: надійшла до редакції 14.03.2025
прийнята до друку 22.05.2025*