DOI: 10.35774/app2026.01.098
УДК 342.9:347.121.1:004.62(477)

Дмитро Костюк,
аспірант НДІ приватного права і підприємництва імені академіка Ф. Г. Бурчака НАПрН України.
ORCID: https://orcid.org/0009-0007-9507-1993

НОРМАТИВНО-ПРАВОВЕ РЕГУЛЮВАННЯ ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ У ПУБЛІЧНИХ ЕЛЕКТРОННИХ РЕЄСТРАХ УКРАЇНИ

У статті досліджено нормативно-правове регулювання обробки персональних даних у публічних електронних реєстрах України в умовах інтенсивної цифрової трансформації публічного управління та євроінтеграційного курсу держави. Встановлено, що публічні електронні реєстри є одними з найбільших операторів персональних даних у сучасній державі, а їхнє функціонування породжує правові колізії між принципами відкритості реєстрових даних та вимогами захисту права на приватність. Проаналізовано багаторівневу систему нормативно-правового регулювання у відповідній сфері, що охоплює конституційні гарантії, спеціальне законодавство, зокрема закони України «Про захист персональних даних» та «Про публічні електронні реєстри», галузеві нормативні акти й підзаконне регулювання.

Методологічну основу дослідження становлять загальнонаукові та спеціально-юридичні методи, зокрема діалектичний, формально-юридичний, системно-структурний і порівняльно-правовий, використані для аналізу нормативно-правового регулювання захисту персональних даних у публічних електронних реєстрах, виявлення прогалин законодавства та формулювання пропозицій щодо його вдосконалення.

Розглянуто такі ключові принципи обробки персональних даних у реєстрових системах, як: законність, функціональна достатність, цільова обмеженість, точність та безпека даних. Виявлено, що практика агрегування реєстрових даних через інтегровані портали електронних послуг суттєво ускладнює дотримання принципу мінімізації даних і створює додаткові ризики для конфіденційності персональної інформації громадян. Досліджено стандарти Загального регламенту про захист даних ЄС (GDPR) та практику Суду справедливості ЄС як ключові орієнтири для гармонізації національного законодавства.

Визначено основні прогалини чинного законодавства: надмірно широкий суб'єктний склад осіб, що мають право спеціального доступу до реєстрових даних; відсутність законодавчо закріпленого принципу «конфіденційність за замовчуванням»; фрагментарність регулювання транскордонного переміщення реєстрових даних. Сформульовано пропозиції щодо диференціації правових режимів доступу до реєстрових даних, кодифікації інформаційного законодавства та посилення заходів кібербезпеки на нормативному рівні.

Ключові слова: *персональні дані, публічні електронні реєстри, захист персональних даних, GDPR, цифрова трансформація, право на приватність, доступ до реєстрових даних, принципи обробки персональних даних*

Kostiuk D.

Regulatory and Legal Framework for Personal Data Processing in Ukraine's Public Electronic Registries

The article examines the legal regulation of personal data processing in public electronic registers of Ukraine in the context of intensive digital transformation of public administration and the country's European integration course. It is established that public electronic registers are among the largest personal data operators in the modern state, and their functioning gives rise to legal conflicts between the principles of openness of registry data and the requirements for the protection of the right to privacy. The article analyses the multi-level system of legal regulation in this sphere, encompassing constitutional guarantees, special legislation – in particular the Laws of Ukraine «On Personal Data Protection» and «On Public Electronic Registers» – sectoral normative acts and subordinate legislation.

The methodological framework of the study is based on general scientific and special legal methods, in particular the dialectical, formal-legal, systemic-structural, and comparative-legal methods, which were used to analyze the legal regulation of personal data protection in public electronic registers, identify legislative gaps, and formulate proposals for its improvement.

The key principles of personal data processing in registry systems are examined: lawfulness, functional sufficiency, purpose limitation, accuracy and data security. It is revealed that the practice of aggregating registry data through integrated electronic service portals significantly complicates compliance with the data minimisation principle

and creates additional risks to the confidentiality of citizens' personal information. The standards of the EU General Data Protection Regulation (GDPR) and the case law of the Court of Justice of the European Union are examined as key reference points for the harmonisation of national legislation.

The main gaps in the current legislation are identified: an excessively broad range of persons entitled to special access to registry data; the absence of a legislatively enshrined «privacy by default" principle; and the fragmented regulation of cross-border transfers of registry data. Proposals are formulated regarding the differentiation of legal access regimes for registry data, the codification of information legislation, and the strengthening of cybersecurity measures at the normative level.

Keywords: *personal data, public electronic registers, personal data protection, GDPR, digital transformation, right to privacy, access to registry data, personal data processing principles.*

Постановка проблеми. В умовах інтенсивної цифрової трансформації публічного управління персональні дані громадян набули значення одного з найбільш цінних інформаційних ресурсів держави. Публічні електронні реєстри акумулюють значні масиви відомостей про фізичних осіб – від даних про майновий і цивільний стан до відомостей про підприємницьку та освітню діяльність. Ці дані забезпечують функціонування механізмів державного управління, надання адміністративних послуг, здійснення судочинства та реалізацію права на захист прав та свобод громадян.

Водночас відкритість реєстрових систем і розширення доступу до них породжують правові проблеми, пов'язані із забезпеченням конфіденційності персональних даних, запобіганням їх несанкціонованому використанню та дотриманням міжнародних стандартів у цій сфері. Особливої гостроти ці питання набувають в умовах воєнного стану, коли ризики кіберагресії проти державних інформаційних систем суттєво зростають, а витік персональних даних може становити безпосередню загрозу як для окремих громадян, так і для цифрового суверенітету держави загалом [1].

Актуальність теми підсилюється і зовнішньополітичним контекстом: курс України на євроінтеграцію зумовлює необхідність гармонізації національного законодавства у сфері захисту персональних даних із правом Європейського Союзу (далі – ЄС), зокрема з Загальним регламентом про захист даних (GDPR) та Хартією основоположних прав ЄС. Ці завдання вимагають системного переосмислення чинної нормативно-правової бази регулювання обробки персональних даних у публічних електронних реєстрах.

Мета статті – проаналізувати систему нормативно-правового регулювання обробки персональних даних у публічних електронних реєстрах України, виявити наявні правові прогалини та суперечності, а також визначити напрями вдосконалення законодавства з урахуванням стандартів ЄС.

Аналіз останніх досліджень і публікацій. Проблематика правового регулювання персональних даних перебуває в полі зору значної кількості дослідників. Стан українських електронних реєстрів і персональних баз даних, що зберігають інформацію про населення країни, досліджено у колективній монографії Інституту демографії та соціальних досліджень НАН України [2]; зарубіжний досвід формування реєстрових систем у державах ЄС – у роботі О. М. Гладун та співавторів [3]. Теоретико-правові засади охорони баз персональних даних за законодавством України, а також особливості суб'єктного складу відносин, пов'язаних із персональними даними, досліджувалися у працях В. І. Теремецького [4; 5]. Питання імплементації зарубіжного досвіду правового захисту персональних даних в Україні висвітлено у праці В. І. Теремецького та Д. В. Цвірюка [6].

Юридичні виміри функціонування реєстрових систем в контексті цифрової трансформації розглядали І. П. Касперський [7], Ю. В. Осика [8], Н. В. Маслак [9]. Технічні аспекти захисту персональних баз даних державних реєстрів та розробки комплексних систем контролю доступу досліджували О. В. Задерейко, О. Г. Трофименко та ін. [1]. Водночас питання нормативно-правового регулювання обробки персональних даних безпосередньо у сфері публічних електронних реєстрів як комплексна проблема залишається недостатньо розробленою, що й визначає мету пропонованої статті.

Виклад основного матеріалу дослідження. Персональні дані в сучасному праві традиційно визначаються як будь-яка інформація, що стосується ідентифікації фізичної особи. Законодавство України сприйняло цей підхід: Закон України «Про захист персональних даних» від 01.07.2010 № 2297-VI закріплює поняття персональних даних як «відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована» [10]. Закон України «Про інформацію» від 02.10.1992 № 2657-XII об'єднує поняття «інформація про фізичну особу» та «персональні дані» спільним визначенням, що є тотожним визначенню попереднього закону [11].

Публічні електронні реєстри за своєю природою є автоматизованими інформаційними системами, що забезпечують збір, зберігання, обробку та надання реєстрових даних у процесі здійснення функцій публічного управління. Оскільки значна частина цих даних стосується конкретних фізичних осіб, реєстри є одними з найбільших за обсягом операторів персональних даних у сучасній державі. В Україні функціонує розгалужена система реєстрів, що охоплює Єдиний державний демографічний реєстр, Державний реєстр виборців, Єдиний державний реєстр юридичних осіб, фізичних осіб-підприємців та громадських формувань, Державний реєстр речових прав на нерухоме майно, Єдину державну електронну базу з питань освіти, Державний реєстр актів цивільного стану громадян та багато інших [1].

У правовій доктрині персональні дані, що містяться у реєстрах, набувають подвійного статусу: з одного боку, вони є об'єктом публічного інтересу, оскільки забезпечують функціонування механізмів державного управління; з іншого – є об'єктом конституційно захищеного права особи на приватність та інформаційне самовизначення. Саме ця подвійність є джерелом численних правових колізій, що виникають у сфері регулювання доступу до реєстрових даних [8].

Особливу категорію серед персональних даних, що зберігаються у реєстрах, становлять чутливі дані, а саме: відомості про стан здоров'я, расову та етнічну належність, політичні переконання, судимість тощо. Розголошення таких відомостей здатне завдати суттєвої шкоди правам і свободам осіб, стати підставою для дискримінації, шантажу або психологічного впливу.

Правове регулювання обробки персональних даних у публічних електронних реєстрах України здійснюється на основі розгалуженої системи нормативно-правових актів, яка охоплює кілька рівнів.

На конституційному рівні право на захист персональних даних ґрунтується на статтях 32 та 34 Конституції України, що гарантують недоторканність особистого і сімейного життя, свободу збирання, зберігання, використання та поширення інформації. Конституційний захист персональних даних органічно пов'язаний із загальним принципом поваги до людської гідності та забезпечення прав і свобод людини як найвищої соціальної цінності.

Центральне місце у системі спеціального законодавства посідає Закон України «Про захист персональних даних» [10]. Він закріплює такі основні принципи обробки персональних даних, як: законність, цільова обмеженість, пропорційність, точність, обмеженість зберігання, а також права суб'єктів персональних даних, зокрема право на доступ, видалення та заперечення проти обробки. Закон визначає підстави для обробки персональних даних, вимоги до забезпечення їх безпеки та встановлює відповідальність за порушення у цій сфері.

Принципово важливим у контексті реєстрових систем є Закон України «Про публічні електронні реєстри» від 18.11.2021 № 1907-IX [12]. Він встановлює правові, організаційні і фінансові засади створення та функціонування публічних електронних реєстрів із метою захисту прав та інтересів фізичних і юридичних осіб під час створення, зберігання, оброблення та використання реєстрової інформації. Серед задекларованих принципів закону – відкритість та доступність реєстрових даних, що покликане сприяти підвищенню прозорості державного управління. Водночас закон містить положення про захист персональних даних у реєстрах, хоча практика його застосування виявляє суттєві прогалини у механізмах забезпечення цього захисту [9].

Відповідно до ст. 34 зазначеного закону будь-якій фізичній чи юридичній особі надано право на отримання інформації з реєстрів у режимі спеціального доступу, в тому числі відомостей про власників нерухомості, обтяження речових прав тощо – за плату. Ця норма викликає обґрунтовані застереження з точки зору принципу пропорційності доступу до персональних даних: широке коло суб'єктів, яким надається такий доступ, істотно підвищує ризики зловживання реєстровою інформацією – від незаконного комерційного використання до несанкціонованого заволодіння правами на об'єкти реєстрації.

Окрему роль у системі нормативно-правового регулювання відіграють галузеві закони, що регламентують обробку персональних даних у конкретних реєстрових системах: Закон України «Про державну реєстрацію актів цивільного стану», Закон України «Про державну реєстрацію юридичних осіб та фізичних осіб-підприємців та громадських формувань», Закон України «Про державні фінансові гарантії медичного обслуговування населення» (щодо електронної системи охорони здоров'я eHealth) та інші. Кожен із цих актів містить спеціальні норми щодо захисту персональних даних в обсязі, зумовленому специфікою відповідної сфери [8].

Слід також згадати підзаконне регулювання, що доповнює законодавчу базу: Наказ Міністерства цифрової трансформації України від 20.05.2020 № 72 «Про затвердження Порядку обробки та захисту персональних даних, власником яких є Міністерство цифрової трансформації України», а також

Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджені постановою Кабінету Міністрів України від 29.03.2006 № 373. Ці акти конкретизують вимоги до технічного й організаційного захисту персональних даних у реєстрових системах.

Системний аналіз чинного законодавства дозволяє виокремити ключові принципи обробки персональних даних у публічних електронних реєстрах України, дотримання яких є обов'язковою умовою правомірності відповідної діяльності.

Принцип законності передбачає, що будь-яка обробка персональних даних у реєстрах повинна мати чітку правову підставу: або згоду суб'єкта даних, або пряму норму закону, що уповноважує відповідний орган здійснювати обробку. Він реалізується через систему спеціальних законів, що регламентують ведення окремих реєстрів.

Принцип функціональної достатності (мінімізації даних) вимагає, щоб обсяг зібраних персональних даних не перевищував необхідного для досягнення законної мети реєстру. Дієвість цього принципу може змінюватися під впливом тенденцій до агрегування даних із різних реєстрів та створення інтегрованих інформаційних систем. Зокрема, функціонування Єдиного державного вебпорталу електронних послуг «Дія» – системи, що через єдиний ідентифікатор надає доступ до даних з численних реєстрів одночасно, – викликає серйозні застереження з точки зору дотримання принципу мінімізації [7]. Правозахисна організація Privacy International вказувала, що агрегування даних різних реєстрів за одним незмінюваним ідентифікатором становить серйозну загрозу безпеці персональних даних.

Принцип цільової обмеженості означає, що персональні дані, зібрані для певної реєстрової мети, не можуть використовуватися для інших цілей, не сумісних з первісною. Однак практика формування інтегрованих реєстрових систем нерідко розмиває цю межу: дані, зібрані, наприклад, для реєстрації права власності, можуть бути доступні суб'єктам, яким вони не призначалися, через режим відкритого або спеціального доступу.

Принцип точності та актуальності передбачає підтримання реєстрових даних у стані, що відповідає дійсності, та їх своєчасне оновлення. На практиці забезпечення актуальності даних у взаємодіючих між собою реєстрових системах є складним організаційним завданням, некоректне вирішення якого може призводити до порушення прав суб'єктів даних.

Принцип безпеки даних вимагає вжиття відповідних технічних та організаційних заходів для захисту персональних даних від несанкціонованого доступу, знищення, зміни або розголошення. В умовах збройної агресії проти України та постійних кібератак на державну цифрову інфраструктуру цей принцип набуває особливої актуальності. Досвід воєнного стану показав уразливість реєстрових систем: у перші дні повномасштабного вторгнення було прийнято вимушене рішення про тимчасове припинення доступу до державних реєстрів, що, водночас, виявило значну залежність функціонування публічного управління від доступності цих систем.

Одним із найгостріших правових питань у сфері публічних реєстрів є питання про межі допустимої відкритості реєстрових даних. Відкритість реєстрів є безперечним позитивом з погляду прозорості державного управління, боротьби з корупцією та покращення інвестиційного клімату. Запровадження Державного реєстру речових прав на нерухоме майно, ЄДРПОУ, Державного реєстру знищеного та пошкодженого майна, системи єВідновлення – все це приклади корисного застосування відкритих реєстрових даних [9].

Зауважимо, що надмірна відкритість може перетворити реєстр на інструмент збору персональних даних із метою шантажу, переслідування або незаконного заволодіння майновими правами. Саме цю проблему виявив законопроєкт № 10242, що передбачав кримінальну відповідальність за несанкціонований доступ до публічних реєстрів: ініціатори законопроєкту прагнули встановити кримінально-правові заборони, водночас не обмеживши право широкого кола осіб на спеціальний доступ до тих самих даних [15]. Очевидна непослідовність такого підходу унеможливлює досягнення ефективного захисту персональних даних виключно засобами кримінально-правових заборон.

Реакцією на такі виклики повинна бути не лише у криміналізація зловживань, а насамперед у переосмислення самої архітектури доступу до реєстрових даних. Відповідно до стандарту, закладеного практикою Суду справедливості ЄС [13], доступ до чутливих персональних даних у реєстрах має бути диференційованим: відкритий доступ – до даних, що мають явну суспільну цінність і не містять суттєвих персональних ідентифікаторів; обмежений доступ – для органів влади, банків, нотаріусів та інших суб'єктів, що мають правомірний інтерес; закритий доступ – для персональних даних, відкриття яких не виправдовується жодною суспільною необхідністю.

Окремою проблемою є агрегування персональних даних через портали електронних послуг. Аналіз функціонування порталу «Дія» засвідчив, що він фактично виступає агрегатором значного обсягу персональних даних, отриманих із загальнодержавних реєстрів [7]. Повідомлення про спроби продажу персональних даних користувачів «Дії» з індивідуальними податковими номерами, номерами телефонів, паспортними даними та фотографіями документів виявили системну проблему: концентрація ідентифікаторів різних реєстрів в єдиному ресурсі різко збільшує цінність такого масиву для зловмисників і одночасно масштаб потенційного витоку.

Цифрова трансформація публічного управління відкриває нові можливості для ефективного надання адміністративних послуг та оптимізації функцій держави, однак одночасно збільшує ризики для персональних даних громадян. Інтеграція реєстрів через платформу «Трембіта», функціонування Єдиного державного вебпорталу відкритих даних та інших систем електронної взаємодії створюють умови, за яких порушення безпеки однієї ланки потенційно загрожує цілісності всього інформаційного простору держави [1].

У цьому контексті першочергового значення набуває запровадження комплексних систем захисту персональних баз даних реєстрів. Дослідження у сфері кібербезпеки реєстрових систем вказують на необхідність поєднання інструментів шифрування, криптографії, систем запобігання витоку даних (DLP), мережевого екранування та блокчейн-технологій для забезпечення цілісності та конфіденційності реєстрових даних. Поряд із технічними заходами принципово важливими є організаційні – чіткі процедури надання та розмежування доступу, впровадження багатофакторної автентифікації, регулярний аудит безпеки.

Воєнний стан актуалізував питання резервування та фізичної безпеки реєстрових систем. Зберігання персональних даних у хмарних сервісах на серверах країн ЄС стало одним із практичних рішень, що дозволило забезпечити безперервність функціонування реєстрів в умовах ракетних ударів по інфраструктурі [14]. Водночас таке рішення породжує нові правові питання: про застосовне право, підстави та межі обробки даних за кордоном, про відповідальність оператора у разі інцидентів. З огляду на вимоги GDPR розміщення персональних даних на серверах країн ЄС забезпечує високий рівень правової захищеності відповідно до суворих законодавчих вимог регламенту; водночас слід враховувати і ризики, пов'язані з можливими політичними змінами.

Прикладом нормативного відгуку на виклики воєнного часу може бути запровадження системи відновлення втраченого майна – Державного реєстру знищеного та пошкодженого майна та програми єВідновлення. Утім ці системи потребують обробки значного обсягу персональних даних постраждалих осіб, що ставить питання про відповідні гарантії їх захисту. Зокрема, необхідним є закріплення чітких правил щодо строків зберігання таких даних, кола суб'єктів доступу та заходів їх безпеки.

Висновки. Нормативно-правове регулювання обробки персональних даних у публічних електронних реєстрах України характеризується розгалуженою, проте недостатньо систематизованою нормативною базою, що поєднує конституційні гарантії, спеціальне законодавство, галузеві норми та підзаконне регулювання. Ключовою проблемою залишається забезпечення балансу між принципами відкритості та доступності реєстрових даних – як засобів підвищення прозорості публічного управління – та вимогами захисту права на приватність і персональних даних громадян.

Аналіз чинного законодавства виявляє такі основні прогалини: недостатня деталізація принципу функціональної достатності при агрегуванні даних різних реєстрів; надмірно широкий суб'єктний склад осіб, що мають право на спеціальний доступ до реєстрових даних без достатнього обґрунтування правомірного інтересу; відсутність законодавчо закріплених стандартів оцінки впливу на захист персональних даних при розробці нових реєстрових систем; фрагментарність регулювання питань транскордонного переміщення реєстрових даних.

Напрями вдосконалення законодавства повинні включати: приведення режиму доступу до реєстрових даних у відповідність до стандартів пропорційності, вироблених практикою Суду справедливості ЄС; законодавче закріплення принципу «конфіденційність за замовчуванням» як обов'язкової вимоги до архітектури реєстрових систем; диференціацію правових режимів доступу до різних категорій реєстрових даних залежно від їх чутливості; кодифікацію нормативного матеріалу у сфері персональних даних у форматі Інформаційного кодексу України з урахуванням вимог GDPR; посилення заходів кібербезпеки реєстрових систем на нормативному рівні.

Реалізація цих заходів не лише сприятиме наближенню законодавства України до стандартів ЄС, а й забезпечить ефективний захист фундаментальних прав і свобод громадян в умовах цифрової держави.

Перспективи подальших наукових досліджень убачаються у розробленні теоретико-прикладних засад удосконалення адміністративно-правового регулювання обробки та захисту персональних даних у

публічних електронних реєстрах з урахуванням європейських стандартів, розвитку цифрового публічного управління та практики застосування автоматизованих рішень.

Список використаних джерел

1. Задерейко О. В., Трофименко О. Г., Єленич С. І., Логінова Н. І., Гура В. І. Системний аналіз захищеності державних електронних реєстрів та баз персональних даних. *Кібербезпека: освіта, наука, техніка.* 2025. № 4 (28). С. 57–70. DOI: 10.28925/2663-4023.2025.28.735.
2. Електронні реєстри: стан в Україні: кол. монографія. Київ : НАН України, Інститут демографії та соціальних досліджень ім. М.В. Птухи, 2021. URL: https://www.idss.org.ua/arhiv/registers3.pdf (дата звернення: 12.02.2026).
3. Гладун О. М., Пугачова М. В., Виноградова М. В. Електронні реєстри: зарубіжний досвід формування та використання: колективна монографія. Київ : НАН України, Інститут демографії та соціальних досліджень ім. М.В. Птухи, 2021. 271 с. URL: https://idss.org.ua/arhiv/registers.pdf (дата звернення: 12.02.2026).
4. Теремецький В. І. Загальна характеристика охорони бази персональних даних за законодавством України. *Підприємництво, господарство і право.* 2015. № 11. С. 3–5.
5. Теремецький В. І. Суб'єкти відносин, пов'язаних з персональними даними. *Право і безпека.* 2015. № 2 (57). С. 171–176.
6. Теремецький В. І., Цвірюк Д. В. Застосування зарубіжного досвіду правового захисту персональних даних в Україні. *Часопис Академії адвокатури України.* 2014. Т. 7, № 2. С. 73–82. URL: http://nbuv.gov.ua/UJRN/Chaau_2014_7_2_11 (дата звернення: 14.02.2026).
7. Касперський І. П. Проблеми забезпечення принципів захисту персональних даних у процесах цифрової трансформації. *Соціальна і цифрова трансформація: теоретичні та практичні проблеми правового регулювання* : матеріали ІІ всеукр. наук.-практ. конф., Київ, 25 грудня 2022 р. С. 33–37.
8. Осика Ю. В. Правове регулювання використання персональних даних. *Ірпінський юридичний часопис.* 2023. Вип. 3 (12). С. 343–351. DOI: 10.33244/2617-4154.3(12).2023.343-351.
9. Маслак Н. В. Відкритість та доступність публічних електронних реєстрів України: переваги та виклики на шляху апроксимації *acquis communautaire* Європейського Союзу. *Європеїзація кримінального права України*: матеріали міжнар. наук. конф., 19 груд. 2024 р. С. 253–257.
10. 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: 11.02.2026).
11. Про інформацію: Закон України від 02.10.1992 № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 12.02.2026).
12. Про публічні електронні реєстри : Закон України від 18.11.2021 № 1907-IX. URL: https://zakon.rada.gov.ua/laws/show/1907-20#Text (дата звернення: 15.02.2026).
13. Luxembourg Business Registers, Case C-37/20. Court of Justice of the European Union, Judgment of 22 November 2022. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62020CJ0037 (дата звернення: 15.02.2026).
14. Пазюк А., Слабко Т. Використання комерційних хмарних технологій для обробки даних державних реєстрів України. 2024. URL: https://www.ifesukraine.org/wp-content/uploads/2024/01/ifes-ukraine-the-use-of-commercial-cloud-technologies-for-processing-data-from-state-registers-of-ukraine-1.pdf (дата звернення: 12.02.2026).
15. Проект Закону про внесення змін до Кримінального кодексу України щодо встановлення кримінальної відповідальності за несанкціоноване втручання, збут або розповсюдження інформації, що обробляється в публічних електронних реєстрах, та посилення кримінальної відповідальності під час дії воєнного стану за кримінальні правопорушення у сфері використання інформаційно-комунікаційних систем. URL: https://itd.rada.gov.ua/billinfo/Bills/Card/43139 (дата звернення: 12.02.2026).

References

1. Zadereiko, O. V., Trofymenko, O. H., Yelenych, S. I., Lohinova, N. I., & Hura, V. I. (2025). Systemnyi analiz zakhyshchenosti derzhavnykh elektronnykh reiestriv ta baz personalnykh danykh [System analysis of the security of state electronic registers and personal data databases]. *Kiberbezpeka: osvita, nauka, tekhnika* –

Cybersecurity: education, science, technology, 4(28), 57–70. Retrieved from https://doi.org/10.28925/2663-4023.2025.28.735 [in Ukrainian].
2. *Elektronni reiestry: stan v Ukraini [Electronic registers: the state in Ukraine]*. (2021). Kyiv: NAN Ukrainy, Instytut demohrafii ta sotsialnykh doslidzhen im. M. V. Ptukhy. Retrieved from https://www.idss.org.ua/arhiv/registers3.pdf [in Ukrainian].
3. Hladun, O. M., Puhachova, M. V., & Vynohradova, M. V. (2021). Elektronni reiestry: zarubizhnyi dosvid formuvannia ta vykorystannia [Electronic registers: foreign experience of formation and use]. Kyiv: NAN Ukrainy, Instytut demohrafii ta sotsialnykh doslidzhen im. M. V. Ptukhy. Retrieved from https://idss.org.ua/arhiv/registers.pdf [in Ukrainian].
4. Teremetskyi, V. I. (2015). Zahalna kharakterystyka okhorony bazy personalnykh danykh za zakonodavstvom Ukrainy [General characteristics of personal data database protection under the legislation of Ukraine]. *Pidpryiemnytstvo, hospodarstvo i pravo – Business, Economics and Law, 11,* 3–5 [in Ukrainian].
5. Teremetskyi, V. I. (2015). Subiekty vidnosyn, poviazanykh z personalnymy danymy [Subjects of relations related to personal data]. *Pravo i bezpeka – Law and Security, 2(57),* 171–176 [in Ukrainian].
6. Teremetskyi, V. I., & Tsviriuk, D. V. (2014). Zastosuvannia zarubizhnoho dosvidu pravovoho zakhystu personalnykh danykh v Ukraini [Application of foreign experience of legal protection of personal data in Ukraine]. *Chasopys Akademii advokatury Ukrainy – Journal of the Ukrainian Bar Association, 7(2),* 73–82. Retrieved from http://nbuv.gov.ua/UJRN/Chaau_2014_7_2_11 [in Ukrainian].
7. Kasperskyi, I. P. (2022). Problemy zabezpechennia pryntsypiv zakhystu personalnykh danykh u protsesakh tsyfrovoi transformatsii [Problems of ensuring the principles of personal data protection in the processes of digital transformation]. *Sotsialna i tsyfrova transformatsiia: teoretychni ta praktychni problemy pravovoho rehuliuvannia: materialy II vseukr. nauk.-prakt. konf. (Kyiv, 2022, Hruden 25) – Social and Digital Transformation: Theoretical and Practical Issues in Legal Regulation: Proceedings of the 2nd All-Ukrainian Scientific and Practical Conference (Kyiv, 2022, December 25),* 33–37 [in Ukrainian].
8. Osyka, Yu. V. (2023). Pravove rehuliuvannia vykorystannia personalnykh danykh [Legal regulation of the use of personal data]. *Irpinskyi yurydychnyi chasopys – Irpin Law Journal, 3(12),* 343–351. Retrieved from https://doi.org/10.33244/2617-4154.3(12).2023.343-351 [in Ukrainian].
9. Maslak, N. V. (2024, December 19). Vidkrytist ta dostupnist publichnykh elektronnykh reiestriv Ukrainy: perevahy ta vyklyky na shliakhu aproksymatsii acquis communautaire Yevropeiskoho Soiuzu [Openness and accessibility of public electronic registers of Ukraine: advantages and challenges on the way to approximation of the acquis communautaire of the European Union]. *Yevropeizatsiia kryminalnoho prava Ukrainy: materialy mizhnar. nauk. konf., 2024, 19 Hrubnia – The Europeanisation of Ukrainian Criminal Law: Proceedings of the International Scientific Conference, 19 December 2024,* 253–257 [in Ukrainian].
10. Verkhovna Rada Ukrainy (2010, June 1). *Pro zakhyst personalnykh danykh: Zakon Ukrainy № 2297-VI [On Personal Data Protection: Law of Ukraine No. 2297-VI]*. Retrieved from https://zakon.rada.gov.ua/laws/show/2297-17#Text [in Ukrainian].
11. Verkhovna Rada Ukrainy (1992, October 2). *Pro informatsiiu: Zakon Ukrainy №2657-XII [On Information: Law of Ukraine No. 2657-XII]*. Retrieved from https://zakon.rada.gov.ua/laws/show/2657-12#Text [in Ukrainian].
12. Verkhovna Rada Ukrainy. (2021, November 18). *Pro publichni elektronni reiestry: Zakon Ukrainy № 1907-IX [On Public Electronic Registers: Law of Ukraine No. 1907-IX]*. Retrieved from https://zakon.rada.gov.ua/laws/show/1907-20#Text [in Ukrainian].
13. *Court of Justice of the European Union. (2022, November 22). Luxembourg Business Registers, Case C-37/20 [Judgment in case C-37/20]*. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62020CJ0037 [in English].
14. Paziuk, A., & Slabko, T. (2024). *Vykorystannia komertsiinykh khmarnykh tekhnolohii dlia obrobky danykh derzhavnykh reiestriv Ukrainy [The use of commercial cloud technologies for processing data from state registers of Ukraine]*. Retrieved from https://www.ifesukraine.org/wp-content/uploads/2024/01/ifes-ukraine-the-use-of-commercial-cloud-technologies-for-processing-data-from-state-registers-of-ukraine-1.pdf [in Ukrainian].
15. Verkhovna Rada Ukrainy. (n.d.). *Proekt Zakonu pro vnesennia zmin do Kryminalnoho kodeksu Ukrainy shchodo vstanovlennia kryminalnoi vidpovidalnosti za nesanktsionovane vtruchannia, zbut abo rozpovsiudzhennia informatsii, shcho obrobliaietsia v publichnykh elektronnykh reiestrakh, ta posylennia*

kryminalnoi vidpovidalnosti pid chas dii voiennoho stanu za kryminalni pravoporushennia u sferi vykorystannia informatsiino-komunikatsiinykh system [Draft Law on Amendments to the Criminal Code of Ukraine regarding the establishment of criminal liability for unauthorized interference, sale or dissemination of information processed in public electronic registers, and strengthening criminal liability during martial law for criminal offenses in the field of use of information and communication systems]. Retrieved from https://itd.rada.gov.ua/billinfo/Bills/Card/43139 [in Ukrainian].

Стаття надійшла 20.02.2026
Стаття прийнята до друку 23.03.2026
Стаття опублікована 30.04.2026.

