THE PERSONAL DATA PROTECTION UNDER UKRAINIAN LEGISLATION AND GDPR

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ ЗА ЗАКОНОДАВСТВОМ УКРАЇНИ ТА GDPR

Yana Odovichena[1]

DOI: https://doi.org/10.30525/978-9934-26-602-7-32

Abstract. The focus of this study is a comparative legal analysis of the concept of "personal data" and the legal grounds for its processing under Ukrainian legislation and the General Data Protection Regulation (GDPR) of the European Union. Particular attention is given to the fact that the definitions of "personal data" under both national law and the GDPR are largely aligned, broadly referring to any information relating to an identified or identifiable natural person. The study thoroughly examines the legal grounds for processing personal data, which the author classifies into two principal categories: processing based on the data subject's consent and processing based on alternative legal grounds that do not require consent. These include, among others: processing authorized by law for the performance of official duties by the data controller; processing necessary for the conclusion or execution of a contract to which the data subject is a party or in their interest; processing to safeguard the vital interests of the data subject; processing required to fulfill a legal obligation imposed on the data controller; and processing necessary to protect the legitimate interests of the controller or a third party, provided these do not override the fundamental rights and freedoms of the data subject. The legal framework for personal data processing is grounded in a clear delineation of when and how each of these legal bases may be applied. This structure is intended to strike a balance between the operational needs of data controllers and individuals' rights to informational privacy. The research further explores judicial practice related to the application of these legal grounds, with

[1] Candidate of Sciences in Law,
Associate Professor of the Department of Private Law,
Yuriy Fedkovych Chernivtsi National University, Ukraine

emphasis on the requirement that consent must be voluntary and informed – specifying the purpose, duration, and scope of data use.

Recommendations are made for improving Ukraine's legal framework for personal data protection, especially in light of analyzed court decisions and ongoing European integration efforts.

The methodology employed combines general scientific methods such as analysis, synthesis, induction, deduction, and comparative legal and formal-legal approaches, with specialized techniques including interpretation and case study analysis.

The goal of the study is to identify key patterns in the legal regulation of personal data processing through a comparative analysis of Ukrainian legislation, the draft Law of Ukraine "On the Protection of Personal Data," the GDPR, and judicial practice. This analysis aims to support legislative reform and enhance the protection of the individual's right to privacy.

In conclusion, the current system for protecting personal data in Ukraine requires significant reform. This includes harmonization with European standards, increasing public legal awareness, and enhancing the accountability of data processors. Adhering strictly to the legal grounds for data processing fosters responsible data use and empowers individuals to maintain control over their personal information – thereby ensuring more effective realization of the right to privacy in the digital age.

1. Вступ

Приватність особи та захист особистого й сімейного життя – це ключові цінності, гарантовані особі міжнародними нормами та законодавством України. Цінність приватності, недоторканість сімейного життя, нерозголошення особистої інформації та персональних даних закріплена у Загальній декларації прав людини ООН, Міжнародному пакті про громадянські і політичні права, Конвенції ООН про права дитини та в інших міжнародних угодах. Законодавчі механізми забезпечують захист конфіденційної інформації, сприяючи реалізації кожною особою права на невтручання в особисте життя.

Захист персональних даних на сучасному етапі розвитку цифрової епохи набуває критичної важливості. Глобальна цифровізація охоплює всі сфери життя, що зумовлює підвищену необхідність гарантування права особи на приватність. Сучасні технології стали основним

інструментом взаємодії між людьми, бізнесом та державними установами, а ідентифікація особи через надання персональних даних стала звичною практикою.

Недостатній рівень захисту особистої інформації може призвести до низки серйозних проблем – від використання даних для персоналізованої реклами до фінансового шахрайства, розповсюдження конфіденційних відомостей та кіберзлочинності. Саме тому важливо впроваджувати ефективні заходи збереження конфіденційності приватного життя та дотримання норм захисту персональних даних особи.

Мета дослідження полягає в порівняльно-правовому аналізі норм національного законодавства, проєкту Закону України «Про захист персональних даних», GDPR та судової практики, для всебічного розуміння поняття «персональні дані» та законних способів їх обробки, з метою подальшого удосконалення законодавства для максимального захисту права особи на приватність.

У межах даної статті поставлено такі **основні науково-дослідницькі завдання:** проаналізувати правову природу поняття «персональні дані» та підстави їх обробки; дослідити норми національного законодавства та GDPR, які регулюють відносини в сфері обробки персональних даних; виявити основні прогалини законодавства щодо застосування норм в сфері персональних даних шляхом аналізу судової практики; запропонувати шляхи вдосконалення правового регулювання обробки персональних даних.

Методологія дослідження базується на загальних методах: аналізу, синтезу, індукції, дедукції, порівняльно-правовому та формально-юридичному методах, так і на спеціальних: інтерпретаційному, кейс-методі та ін.

2. Суть та правове розуміння поняття «персональні дані особи»

Серед одних із найважливіших завдань держави є розвиток та вдосконалення правового регулювання сфери захисту персональних даних особи, що гарантовано статтею 32 Конституції України. Держава бере на себе обов'язок забезпечувати невтручання в особисте та сімейне життя людини, крім випадків, передбачених Конституцією України. Не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків,

визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини [1].

Така норма узгоджується із статтею 8 Конвенції про захист прав людини і основоположних свобод, згідно з якою органи державної влади не можуть втручатись у здійснення права на повагу до приватного і сімейного життя, за винятком випадків, коли втручання здійснюється згідно із законом і є необхідним у демократичному суспільстві в інтересах національної та громадської безпеки чи економічного добробуту країни, для запобігання заворушенням чи злочинам, для захисту здоров'я чи моралі або для захисту прав і свобод інших осіб [2].

Найчастіше право на невтручання в особисте життя порушується саме шляхом незаконного збирання, зберігання, використання та розповсюдження персональних даних особи.

Тому, норми про заборону збирання, зберігання, використання та розповсюдження персональних даних особи без її згоди, містяться в ряді нормативно-правових актів, що ще раз доводить важливість забезпечення права на невтручання в особисте життя особи. Так, зокрема, збирання, зберігання, використання і поширення інформації про особисте життя фізичної особи без її згоди не допускаються, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини (ч. 1 ст. 302 Цивільного кодексу України); поширення персональних даних без згоди суб`єкта персональних даних або уповноваженої ним особи дозволяється у випадках, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини (ч. 2 ст. 14 Закону України «Про захист персональних даних»); конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, визначених законом (ч. 2 ст. 21 Закону України «Про інформацію»); розпорядники інформації, які володіють конфіденційною інформацією, можуть поширювати її лише за згодою осіб, які обмежили доступ до інформації, а за відсутності такої згоди - лише в інтересах національної безпеки, економічного добробуту та прав людини (ч. 2 ст. 7 Закону України «Про доступ до публічної інформації»).

Звичайно ж, дослідження поняття персональних даних було б неповним, без аналізу європейського стандарту у сфері обробки та

захисту персональних даних General Data Protection Regulation або GDPR (далі – Регламент), який було прийнято в Європейському Союзі (далі – ЄС) 25 травня 2018 року, та який вважається одним з найсуворіших законів про конфіденційність. GDPR застосовується до компаній та організацій, що, в процесі їх функціонування, здійснюють збір, обробку та зберігання персональних даних громадян ЄС, а також у випадках, коли така компанія чи організація знаходиться в межах ЄС, незалежно від того, чи опрацювання персональних даних здійснюється в межах ЄС чи поза межами ЄС, а також незалежно від суб'єктів, персональні дані яких обробляються. На даний час, GDPR не є обов'язковим на території України, крім випадків перелічених вище, проте він має «екстратериторіальний ефект» – поширюється на діяльність будь-яких компаній, які збирають або ж передають персональні дані користувачів в ЄС. Тому в рамках адаптації законодавства України та ЄС, принципи GDPR слід враховувати компаніям при розробці системи захисту персональних даних фізичних осіб.

Основним завданням Регламенту є обробку персональних даних прозорою та зрозумілою для користувачів та дати їм більше контролю над тим яким способом їхні особисті дані збираються, обробляються та захищаються. Як зазначено в положенні 2 Регламенту: фізичні особи мають право на дотримання їхніх фундаментальних прав і свобод, зокрема їхнього права на захист персональних даних, незалежно від їхнього громадянства або місця проживання [3].

Звичайно, контроль за дотриманням норм права щодо захисту персональних даних покладається на певну уповноважену на це особу. Згідно Регламенту, таким органом є наглядовий орган, що відповідає за перевірку порушень та забезпечення дотримання юридичних зобов'язань у відповідності з GDPR. Кожна держава-член Європейського союзу зобов'язана створити один або кілька наглядових органів для контролю та забезпечення дотримання GDPR в межах своєї юрисдикції.

Роль наглядового органу полягає у забезпеченні того, щоб організації, які обробляють персональні дані, дотримувалися правила GDPR. Це включає в себе розслідування скарг, проведення аудитів та накладення санкцій і штрафів за недотримання. Наглядовий орган має право наказати організації вжити коригуючі дії для усунення будь-яких пору-

шень GDPR і при необхідності припинити або заборонити діяльність по обробці даних.

Для прикладу, Іспанське управління із захисту даних (AEPD) наклало штраф у розмірі 2 520 000 євро на іспанську мережу супермаркетів Mercadona, S.A. за незаконне використання системи розпізнавання облич. Після свого розслідування AEPD виявила, що Mercadona використовувала систему розпізнавання облич у 48 своїх магазинах по всій Іспанії протягом кількох місяців для виявлення осіб із кримінальними засудженнями або обмежувальними приписами (зокрема, осіб, які отримали обмежувальний припис після нападу на співробітника магазину або були засуджені за інцидент у магазині). Система розпізнавання облич і пов'язана з нею обробка біометричних даних також фіксували зображення облич всіх клієнтів, які заходять в супермаркети Mercadona, включаючи дітей і співробітників Mercadona.

AEPD встановила, що жодна з правових підстав, наявних у статті 9 Загального регламенту ЄС про захист даних (який встановлює правові підстави для обробки конфіденційних даних, включаючи біометричні дані), не могла бути використана Mercadona для обробки біометричних даних через свою систему розпізнавання обличь – отже, AEPD визнала обробку незаконною [4].

Ще один приклад, Уповноважений із ЗПД Франції наклав штраф 125 000 євро на компанію, що надає в оренду скутери, але їхня діяльність «пов’язана з визначенням геолокації» (кожні 30 секунд збираються дані про геолокацію електросамокатів), що, зокрема, порушує зобов’язання щодо мінімізації даних згідно зі статтею 5 GDPR. Наглядовий орган наполягав на тому, що ця послуга може надаватися без збирання даних геолокації на постійній основі (permanent basis) [5].

В Україні, наразі немає спеціально створеного органу по контролю за дотриманням захисту персональних даних. Відповідно до закону, контроль за дотриманням законодавства про захист персональних даних здійснюється Уповноваженим Верховної Ради України з прав людини та судами. Уповноважений з прав людини за скаргами юридичних та фізичних осіб, а також за власною ініціативою проводить перевірки дотримання вимог відповідних законів та видає обов'язкові для виконання вимоги (приписи) про запобігання або усунення порушень законодавства про захист персональних даних. Такий спосіб

захисту порушеного права є досить швидким та дієвим. Наприклад, до Уповноваженого звернувся заявник Д. щодо неправомірних дій одного з працівників психоневрологічного інтернату, що призвело до порушення права на приватність інших осіб. Заявник повідомив, що всупереч вимогам законодавства про захист персональних даних було допущено розголошення персональних даних (конфіденційної інформації) підопічних інтернату шляхом поширення у мережі Інтернет відеозапису, на якому їх зображено. За даними фактами оприлюднення персональних даних, сектором дізнання управління поліції ГУНП в Черкаській області відкрито кримінальне провадження за частиною першою статті 182 Кримінального кодексу України «Порушення недоторканості приватного життя» для перевірки щодо законності зберігання, використання, поширення конфіденційної інформації про особу [6].

Можемо сказати, що на даний час в Україні формується судова практика притягнення винних осіб до відповідальності за порушення законодавства у сфері захисту персональних даних. Для прикладу, постановою Броварського міськрайонного суду Київської області від 09.04.2020 р. у справі № 361/1579/20, голову правління СТ «Заліське» визнано винною у вчиненні правопорушення, передбаченого ч. 4 ст. 188-39 КУпАП так як вона не забезпечила належний рівень захисту персональних даних особи й поширила персональні дані у чаті месенджера Viber, розмістивши копію звернення заявниці (особи) до юридичної особи, в якому, крім прізвища, імені та по батькові заявниці, оприлюднено адресу її місця реєстрації, номер мобільного телефону, адресу електронної пошти, внаслідок чого до персональних даних цієї особи відбувся доступ невизначеного кола осіб. В результаті таких дій, було порушено право заявниці на захист персональних даних від незаконної обробки. Суд наклав на винну особу адміністративне стягнення у вигляді штрафу в розмірі 5 100 грн [7].

Ще одна подібна справа № 761/23532/20 Шевченківського районного суду м. Києва, який визнав винним у вчиненні адміністративного правопорушення т.в.о. президента Національної академії державного управління при Президентові України. Суть правопорушення зводилася до того, що на вебсайті Академії був опублікований наказ, який містив імена, прізвища, місця роботи та фактичного проживання

студентів, які мають заборгованість з оплати проживання в академічному гуртожитку.

Під час апеляційного оскарження сторона захисту наполягала на тому, що Академія є бюджетною установою, а отже, інформація щодо розрахунків, витрачання і надходження бюджетних коштів є публічною та становить суспільний інтерес. Суд апеляційної інстанції з такими доводами не погодився та наголосив на низці норм, що зобов'язують володільця персональних даних забезпечувати їх належний захист [8].

Як бачимо, право на невтручання в особисте життя через неправомірне використання персональних даних є актуальним питанням, яке підлягає контролю та захисту судом або спеціально уповноваженими органами.

Для повного розуміння відносин в сфері захисту персональних даних необхідним є дослідження самого поняття «персональні дані» в контексті національного законодавства та GDPR.

Як вже зазначалося, основними нормативно-правовими актами, які регулюють відносини в сфері захисту персональних даних, є закони України «Про інформацію» та «Про захист персональних даних».

Одразу відмітимо, що обидва закони дають однакові визначення поняттю «персональні дані», розуміючи їх як «відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована». Проєкт нового Закону України «Про захист персональних даних» дає аналогічне визначення даного поняття [9]. Наведені визначення є досить загальними та не місять переліку, які саме відомості є персональними даними.

Якщо звернутися до наукових визначень поняття «персональні дані», то відмітимо, що зазвичай вони також мають узагальнений характер. Наприклад, на думку О. Дяковського персональні дані - це відомості чи сукупність відомостей про живу фізичну особу, яка ідентифікована або може бути конкретно ідентифікована з урахуванням встановленого законом поділу персональних даних [10, с. 57].

О. Брижко зазначає, що поняття «персональні дані» охоплює об'єктивні та суб'єктивні відомості про особисте, сімейне чи публічне життя фізичної особи, що виражені у формі літер, чисел, графіки, фото, звуку чи відео, символів, якщо вони дозволяють ідентифікувати таку особу. Для визнання відомостей персональними даними

обов'язковою є наявність зв'язку між такими відомостями та конкретною особою [11, с. 59].

Як вважає О.Середа, в існуючих визначеннях поняття «персональні дані» в основу покладений термін «ідентифікація». У загальному значенні ідентифікація (від лат. Identifico – "ототожнюю") означає визначення відповідності предмета, біологічного організму, особи (юридичної, фізичної), певним, конкретним, лише їм властивим ознакам. Ідентифікація особи – визначення за допомогою спеціальних методів тотожності суб'єкта, конкретній особі [12, с. 191]. Зазначене ототожнення здійснюється за багатьма критеріями котрі чітко не розмежовані в чинному законодавстві України, що підтверджує думку вченого О. Брель про те, що немає вичерпного переліку, закріпленого в чинному законодавстві, котрий би вказував, які саме дані про фізичну особу можна вважати персональними, а які до них не відносяться.

Яке ж визначення поняття «персональні дані» дає GDPR? Стаття 4 Регламенту називає персональні дані як будь-яку інформацію, що стосується фізичної особи, яку ідентифіковано чи можна ідентифікувати («суб'єкт даних»). Аналогічне визначення міститься і в Конвенції Ради Європи № 108 про захист осіб у зв'язку з автоматизованою обробкою персональних даних, ратифікованою Україною в 2010 році [13].

Як бачимо, визначення, що містяться в національному законодавстві та в Регламенті й Конвенції досить подібні. При тому, законодавство України визначає персональні дані як відомості (сукупність відомостей), а GDPR та Конвенція – як інформацію. Поняття «відомості» та «інформація» вживаються як тотожні, але «інформація» є ширшою категорією, яка охоплює всі дані та факти про особу, за допомогою яких можна її ідентифікувати (звички, інтереси та ін.). Відомості – це дані про особу, які мають значення саме в певному контексті (дані паспорта, ідентифікаційний номер та ін.) [14].

Окрім поняття, важливим є визначити, яка саме інформація відноситься до персональних даних особи. Як зазначалося вище, національне законодавство України не містить переліку даних, які відносяться до персональних. Проте Конституційний Суд України у своєму рішенні від 20.01.2012 р. № 2-рп/2012 надав офіційне тлумачення ч. 1 та 2 ст. 32 Конституції України, в якому відніс до персональних даних

особи національність, освіту, сімейний стан, релігійні переконання, стан здоров'я, матеріальний стан, адресу, дату і місце народження, місце проживання та перебування тощо, дані про особисті майнові та немайнові відносини цієї особи з іншими особами, зокрема членами сім'ї, а також відомості про події та явища, що відбувалися або відбуваються у побутовому, інтимному, товариському, професійному, діловому та інших сферах життя особи, за винятком даних стосовно виконання повноважень особою, яка займає посаду, пов'язану зі здійсненням функцій держави або органів місцевого самоврядування [15].

GDPR визначає персональними даними такі, як ім'я фізичної особи, ідентифікаційний номер, дані про місцеперебування, онлайн-ідентифікатор або один чи декілька факторів, що є визначальними для фізичної, фізіологічної, генетичної, розумової, економічної, культурної чи соціальної сутності такої фізичної особи [3].

Персональні дані можна поділити на такі категорії:

– звичайні персональні дані (Article 4(1) GDPR) – будь-яка інформація, що стосується ідентифікованої або такої, що може бути ідентифікована, фізичної особи. Наприклад, ім’я та прізвище; дата народження; адреса електронної пошти; номер телефону; IP-адреса; ідентифікаційний номер платника податків (ІПН) та ін.

– спеціальні категорії персональних даних (Article 9 GDPR) – чутливі дані, що потребують підвищеного захисту, обробка яких заборонена, за винятком окремих випадків, передбачених законодавством. До них відносяться: расове або етнічне походження; політичні погляди: релігійні або філософські переконання; членство в профспілках; генетичні дані; біометричні дані (для ідентифікації особи); дані про здоров’я; про статеве життя або сексуальну орієнтацію.

– дані про кримінальні правопорушення (Article 10 GDPR) – інформація про кримінальні вироки та правопорушення, яка також потребує особливого захисту (про судимість, кримінальні провадження, адміністративні правопорушення вчинені особою).

Обробка останніх категорій наведених персональних даних повинна відбуватися лише у виняткових випадках із забезпеченням вищих стандартів як захисту, так і дотримання прав суб’єктів персональних даних. В основі такого поділу лежить те, що вказані категорії персональних даних мають у собі інформацію щодо ознак, які часто

можуть стати підставою для дискримінаційного ставлення до відповідного суб'єкта персональних даних.

Відмітимо, що проєкт Закону України «Про захист персональних даних» вже розмежовує та використовує такі категорії персональних даних як «біометричні дані», «генетичні дані», «дані про стан здоров'я» [9].

Крім того, рішення Європейського суду з прав людини (далі – ЄСПЛ) виражають сталу судову практику щодо важливості захисту приватного життя особи, гарантованого статтею 8 Європейської конвенції з прав людини, шляхом нерозголошення саме чутливих персональних даних особи. Так, наприклад справа S and Marper проти Сполученого Королівства є важливим прецедентом, який стосується захисту приватного життя та обробки біометричних даних.

Згідно обставин справи, у 2001 році двоє осіб із Шеффілда, Англія, були затримані: один – 11-річний підліток (позначений як S), звинувачений у спробі пограбування, та дорослий чоловік (Марпер), звинувачений у домаганнях до партнера. У обох випадках були взяті відбитки пальців та зразки ДНК. Після того, як обвинувачення були зняті або особи були виправдані, вони звернулися з проханням знищити їхні біометричні дані, але поліція відмовила. Згідно з політикою, дані зберігалися в Національній базі даних ДНК незалежно від результатів судового процесу.

4 грудня 2008 року Велика палата ЄСПЛ одноголосно постановила, що зберігання біометричних даних осіб, які не були засуджені, порушує їхнє право на повагу до приватного життя, гарантоване статтею 8 Європейської конвенції з прав людини. Суд зазначив, що вбачає порушення статті 8, а саме: зберігання біометричних даних осіб, які не були засуджені, є втручанням у їхнє право на приватне життя; необґрунтованість втручання: загальна та безумовна політика зберігання таких даних не є необхідною в демократичному суспільстві та не відповідає принципу пропорційності; спеціальний захист для неповнолітніх: Особливу увагу слід приділяти захисту приватного життя неповнолітніх осіб, оскільки збереження їхніх біометричних даних може мати негативні наслідки для їхнього розвитку та інтеграції в суспільство [16].

Проте є судові прецеденти, в яких розголошення вразливих персональних даних не вважається порушенням. Наприклад, справа Green

проти Сполучене Королівство, яка стосується балансу між правом на приватне життя та принципом парламентської автономії, зокрема використання парламентського привілею для розкриття конфіденційної інформації.

У 2018 році британський бізнесмен сер Філіп Грін отримав судову заборону, яка забороняла газеті The Telegraph публікувати його ім'я у зв'язку з обвинуваченнями у сексуальних домаганнях, расистських висловлюваннях та булінгу, висунутими колишніми працівниками. Однак член Палати лордів Пітер Гейн, посилаючись на парламентський привілей, публічно назвав Гріна під час виступу в парламенті, що призвело до широкого розголосу в ЗМІ та фактичного знецінення судової заборони.

Грін подав скаргу до Європейського суду з прав людини (ЄСПЛ), стверджуючи, що використання парламентського привілею для розкриття його особистості порушило його право на приватне життя.

В свою чергу, ЄСПЛ одноголосно постановив, що не було порушення статті 8 Конвенції. Суд визнав, що хоча розкриття особистості Гріна вплинуло на його приватне життя, питання контролю за парламентським привілеєм належить до компетенції національних парламентів, і втручання в цю сферу суперечило б принципу парламентської автономії [17].

Ще одна справа Gillberg проти Швеції, яка стосується балансу між захистом чутливих персональних даних, правом на приватне життя та доступом до публічної інформації.

Професор психіатрії Крістофер Гіллберг очолював дослідницький проєкт у Гетеборзькому університеті, присвячений гіперактивності та порушенням уваги у дітей. У період з 1977 по 1992 рік було зібрано велику кількість чутливих даних про учасників дослідження, зокрема медичні записи, відео та аудіозаписи. Учасникам та їхнім батькам були надані гарантії конфіденційності.

У 2002 році інші дослідники звернулися до університету з проханням надати доступ до цих даних. Після відмови університету, адміністративний суд ухвалив рішення про надання доступу, але з обмеженнями. Гіллберг відмовився передати матеріали, посилаючись на обіцянку конфіденційності, і в результаті дані були знищені його

колегами. У 2005 році проти Гіллберга було порушено кримінальну справу за зловживання службовим становищем.

ЄСПЛ не визнав, що кримінальне переслідування Гіллберга порушує його право на приватне життя, оскільки це було пов'язано з його службовими обов'язками як публічного службовця.

Суд наголошує на необхідності знаходження балансу між захистом особистої інформації та правом на доступ до публічної інформації.

Також, Суд не вбачав порушення статті 10 Конвенції та не визнав, що відмова Гіллберга передати дослідницькі матеріали є захищеним «негативним правом» на свободу вираження, оскільки матеріали належали університету і були публічними документами [18].

Отже, як висновок, можемо сказати, що право на приватність, захист особистого і сімейного життя, а також персональних даних особи, є визначальною складовою прав людини, як на міжнародному, так і на національному рівні. У сучасну цифрову епоху, коли персональні дані обробляються майже у всіх сферах суспільного життя, захист цієї інформації набуває особливої актуальності. Порушення права на недоторканність приватного життя часто проявляється у формі незаконного збирання, зберігання, використання чи поширення персональних даних.

Часто можна спостерігати як персональні дані використовуються третіми особами в різних видах фінансового шахрайства. Саме тому, одним із пріоритетних напрямків діяльності держави є захист таких даних та забезпечення прозорості при їх збиранні, використанні та обробці.

Крім того, створення ефективної системи захисту персональних даних є одним із міжнародних зобов'язань України, в тому числі в контексті європейської інтеграції. Зокрема, від виконання цього зобов'язання значною мірою залежать реалізація євроінтеграційних прагнень української держави.

Здійснений аналіз національного законодавства України та практики його застосування, а також положень Загального регламенту про захист даних ЄС (GDPR), показує потребу у необхідності вдосконалення правового регулювання у сфері захисту персональних даних, включаючи чітке визначення понять, пов’язаних з персональними даними, запровадження ефективного контролю та відповідальності за порушення цього права.

На сучасному етапі розвитку відносин із захисту персональних даних, можемо спостерігати формування судової практики, що підтверджує посилення уваги до дотримання права на захист персональних даних. Водночас відсутність спеціалізованого незалежного наглядового органу, подібного до європейських аналогів, є істотною прогалиною, що ускладнює забезпечення ефективного захисту цього права.

Отже, захист персональних даних в Україні потребує комплексного удосконалення, що передбачає узгодженість національного законодавства з європейськими стандартами, розвиток правової свідомості громадян та відповідальності суб'єктів обробки даних. Це дозволить ефективно забезпечити реалізацію права особи на приватність у цифровому суспільстві.

3. Підстави для обробки персональних даних

3.1. Згода суб'єкта як підстава для обробки персональних даних

Будь-які дії з персональними даними можуть здійснюватися виключно за наявності підстав, передбачених законодавством України. Одразу відмітимо, що Закон України «Про захист персональних даних» та Регламент містять 6 підстав для законності обробки даних.

Підстави для обробки персональних даних – це конкретні положення законодавчих актів або юридичні факти (дії чи події) щодо персональних даних, за наявності яких стосовно такої інформації уповноважені органи, посадові особи, або самі суб'єкти персональних даних можуть здійснювати конкретні дії з персональними даними.

Стаття 11 закону України «Про захист персональних даних» визначає підстави для обробки персональних даних. Як закон, так і GDPR, першою з підстав називає «згоду суб'єкта персональних даних на обробку його персональних даних».

Відповідно до ст. 2 Закону, згода суб'єкта персональних даних – це добровільне волевиявлення фізичної особи (за умови її поінформованості) щодо надання дозволу на обробку її персональних даних відповідно до сформульованої мети їх обробки, висловлене у письмовій формі або у формі, що дає змогу зробити висновок про надання згоди [19].

Згідно роз'яснення до Типового порядку обробки персональних даних, під інформованою згодою на обробку персональних даних

варто розуміти добровільне, компетентне прийняття особою рішення про обробку її персональних даних, яке ґрунтується на одержанні нею повної, об'єктивної і всебічної інформації стосовно майбутньої обробки персональних даних [20].

Визначення поняття згоди (consent) міститься в Регламенті із захисту персональних даних в параграфі 11 статті 4. Так, згода – це будь-яким способом вільно надана, конкретна, поінформована та однозначна вказівка на бажання суб'єкта даних, за яким він або вона, за допомогою заяви або чіткої позитивної дії, виражають згоду на обробку персональних даних, пов'язаних з ним або з нею [3].

Подібне визначення наводиться в проєкті Закону України «Про захист персональних даних», згода на обробку персональних даних (згода) – будь-яке вільне, чітке, інформоване та однозначне волевиявлення суб'єкта персональних даних, виражене у формі заяви та/або чіткої стверджувальної дії, яким він дозволяє обробку своїх персональних даних [9].

Як бачимо, наведені вище визначення поняття «згоди» є подібними та мають однакові ключові ознаки. Проте, отримання згоди – це складний та неоднозначний процес, що включає в себе не лише порядок отримання згоди, як такої, але й управління даними, які будуть отримані внаслідок такої згоди, їх обробку, видалення, за потреби, чи надання даних контролюючим органам.

Згоду на обробку персональних даних можна розглядати як принцип, що у свою чергу, робить акцент на добровільний та інформований характер дозволу на обробку даних. Згода суб'єкта даних визначає підставу для легальної обробки персональних даних, забезпечуючи гармонію між правами громадян та інтересами організацій. Завдяки цьому принципу суб'єкти даних можуть визначати, які дані вони надають та як вони можуть бути використані, що важливо для збереження їхньої конфіденційності та контролю над власною інформацією [21, с. 180].

При наданні згоди на обробку персональних даних потрібно звертати уваги на її форму. Закон України «Про захист персональних даних» зазначає, що згода на обробку персональних даних може бути висловлена в письмовій формі або у формі, що дає змогу зробити висновок про її надання [19].

Тобто, згода може бути надана шляхом фактичного підписання звичайним чи електронним підписом документу «Згода на обробку персональних даних» або шляхом проставлення відмітки у відповідній клітинці на вебсайті отримувача даних чи відповіді на електронний запит (лист), яким особа підтверджує свою згоду через зазначення свого імені та проставлення "надаю згоду".

Дещо більший перелік форм вираження згоди наведений в проєкті Закону України «Про захист персональних даних», зокрема, може бути надана:

1) у письмовій формі (заяви, анкети, заповнення бланку тощо), в тому числі поданої електронними засобами;

2) в електронній формі під час відвідування вебсайту або користування електронною інформаційною системою, шляхом заповнення передбаченої інтерфейсом форми, проставлення у відповідному полі відмітки (позначки);

3) шляхом обрання відповідних технічних налаштувань в інтерфейсі вебсайта, операційній системі, програмному забезпеченні чи мобільному додатку, які передбачають обробку персональних даних, за умови, що суб'єкт персональних даних попередньо повідомлений, що такі дії призведуть до обробки його персональних даних;

4) через іншу ствердну дію чи поведінку, яка однозначно вказує на те, що суб'єкт персональних даних в конкретному випадку згоден на подальшу обробку його персональних даних [9].

Для прикладу, постанова Вінницького апеляційного суду за позовом 14 осіб до АТ «Укрпошта» проте, що при наданні послуг відповідач самовільно обробляє їх персональні дані, самовільно вносить у розрахункові квитанції повідомлення про надання ними згоди на обробку персональних даних, примушує називати номер мобільного телефону для здійснення відправлення листа, посилки чи бандеролі тощо, мотивуючи це вимогою автоматизованої комп`ютерної програми.

Суд вважає, що позивачами не доведено, що їх персональні дані при наданні послуг відповідачем були отримані самовільно і незаконно. Оскільки здійснюючи оплату наданих послуг поштового зв`язку, вказавши свої паспортні дані, адресу, надавши розрахункові книжки з плати комунальних послуг, у яких міститься конкретна інформація

про особу, тощо, позивачі надали згоду на обробку своїх персональних даних – у формі, що дає змогу зробити про це висновок [22].

В якій би формі не була надана згода суб'єктом персональних даних на їх обробку, вона повинна відповідати таким вимогам: бути добровільною (вільно наданою); конкретною; інформованою; однозначною.

Проаналізуємо детальніше кожну з вимог. Добровільність наданої згоди на обробку персональних даних означає, що суб'єкт персональних даних добровільно, без будь-якого примусу чи тиску, надає свою згоду на збір, обробку та зберігання своїх персональних даних. Важливо, щоб ця згода була усвідомленою, тобто особа повинна мати повну інформацію про те, які дані збираються, з якою метою, хто буде їх обробляти та як довго вони будуть зберігатися.

Роз'яснення до Типового порядку обробки персональних даних рекомендує, щоб зробити свідомий вибір – давати чи не давати згоду на обробку персональних даних – особа до надання згоди повинна мати відповіді на такі питання:

– хто оброблятиме її персональні дані? (назва володільця персональних даних, його адреса, контактні телефони тощо);

– з якою метою оброблятимуться персональні дані? (Мета має бути сформульована чітко та зрозуміло);

– які персональні дані будуть оброблятися? (Конкретний вичерпний перелік персональних даних особи, який планується обробляти);

– які дії з персональними даними передбачатиме їх обробка? (збір, зберігання, передача, оприлюднення, знеособлення тощо);

– хто є розпорядником персональних даних? Які права і повноваження розпорядника щодо обробки персональних даних?

– кому можуть бути передані персональні дані? З якою метою? На яких підставах?

– скільки часу персональні дані будуть зберігатися у володільця?

– на яких умовах особа може відкликати згоду на обробку персональних даних та які наслідки такої дії? [20].

Проте часто відбувається так, що ненадання згоди на обробку персональних даних має наслідком відмову в наданні послуги чи доступі до інформації. Як приклад, іноді суб'єкт даних змушений надати згоду для уникнення на веб-сайті блокуючих вікон, розблокування яких можливе тільки після надання згоди на обробку персональних даних.

Якщо особа не матиме реального вибору, згода не вважається такою, яка надана вільно і, відповідно, вона буде отримана незаконно.

В країнах Європейського Союзу вже усталена практика щодо накладення штрафів за порушення умови добровільності надання згоди. Наприклад, наглядовий орган Фінляндії наклав штраф у розмірі 8 500 євро на видавця спортивного журналу за порушення вимог щодо прямого маркетингу – здійснення автоматизованих дзвінків підписникам без їхньої згоди. В ході розслідування було виявлено, що умови передплати журналу включали вимогу погодитись на прямий маркетинг, і якщо підписник відмовлявся надати таку згоду, журнал не можна було передплатити. Наглядовий орган констатував порушення Загального регламенту про захист даних (GDPR), оскільки спосіб отримання згоди не відповідав вимогам останнього: згода, отримана разом із підпискою, і поставлена в залежність від прийняття умов договору, не відповідає критерію добровільності для цілей прямого маркетингу.

Наразі, в Україні ще не до кінця сформований механізм отримання добровільної згоди на обробку персональних даних. Проєкт Закону України «Про захист персональних даних» пропонує не вважати згоду вільною якщо: 1) суб'єкт персональних даних знаходиться у залежному чи підпорядкованому становищі відносно контролера, якому надається згода; 2) у суб'єкта персональних даних немає вільного вибору або немає можливості відмовити в наданні згоди або немає можливості відкликати раніше надану згоду, без настання негативних наслідків для себе; 3) у суб'єкта персональних даних відсутні альтернативні шляхи реалізації своїх прав та законних інтересів, доступу до певних товарів, послуг, соціальних благ тощо, без надання ним згоди на обробку своїх персональних даних; 4) вона не передбачає окремого дозволу суб'єкта персональних даних на окремі види обробки персональних даних, незважаючи на те, що такий дозвіл є необхідним за індивідуальних обставин [9].

Друга вимога щодо згоди – це її конкретність. Конкретність означає, що особа, яка дає згоду на обробку, повинна чітко розуміти, для яких саме цілей її дані будуть використовуватися. Згода повинна бути однозначно сформульована щоб уникнути непорозумінь чи двозначностей. Інформація про обробку даних має бути конкретною і деталізованою, щоб власник персональних даних міг свідомо прийняти рішення.

Згода має бути надана для конкретної мети чи для конкретної операції, а не для будь-якої іншої або взагалі невизначеної операції з обробки даних. Якщо обробка персональних даних має більш ніж одну мету, згода має бути надана для кожної з цих цілей. Обробка з декількома цілями може викликати додаткові труднощі, оскільки не завжди можна заздалегідь знати, які операції з обробки фактично відбудуться, і тому згода, надана в певний момент часу, буде обмежена конкретними параметрами, встановленими на момент надання згоди.

Для прикладу, при отриманні згоди суб'єкта даних на обробку імені, прізвища, номеру телефону та електронної адреси для цілей надання освітніх послуг, отримувач персональних даних не має права використовувати їх для надсилання реклами, оскільки суб'єкт даних свою згоду щодо цієї цілі не надавав. Нова ціль (мета) обробки – нова згода суб'єкта даних.

Ще однією вимогою щодо згоди є її інформованість. Під інформованою згодою на обробку персональних даних варто розуміти добровільне, компетентне прийняття особою рішення про обробку її персональних даних, яке ґрунтується на одержанні нею повної, об'єктивної і всебічної інформації стосовно майбутньої обробки персональних даних.

Отримувач даних повинен забезпечити суб'єкта даних всією необхідною інформацією про всі деталі обробки персональних даних суб'єкта даних. Разом з тим, таке інформування повинно здійснюватися мовою, зрозумілою суб'єкту даних, а також у формі, яка б надала можливість останньому зрозуміти як обробка персональних даних може вплинути на нього.

Законодавство безпосередньо не визначає вимоги до інформації, яка має бути надана суб'єкту персональних даних, можна вважати, що вона повинна бути необхідною, доступною, достовірною та своєчасною. Необхідною інформацію щодо обробки персональних даних слід вважати тоді, коли вона включає відомості про: 1) суб'єктів (володільця чи розпорядника персональних даних, їх місцезнаходження або місце проживання (перебування); третіх осіб, яким передаються його персональні дані); 2) об'єкт (склад та зміст зібраних персональних даних); 3) суб'єктивні умови (права, визначені законом, мету збору персональних даних); 4) об'єктивні умови (джерела збирання, місцезнаходження

своїх персональних даних; умови надання доступу до персональних даних; механізм автоматичної обробки персональних даних; які дії з персональними даними передбачатиме їх обробка; скільки часу персональні дані будуть зберігатися у володільця). Доступність інформації вказує на два елементи: 1) зміст її повинен бути доступним для розуміння особою, яка не є спеціалістом у сфері законодавства про захист персональних даних; 2) інформація повинна подаватись у наочній формі, доступній для сприйняття суб'єктом персональних даних. Достовірність інформації вказує на те, що вона повинна відповідати дійсності та не вводити суб'єкта персональних даних в оману. Своєчасність такої інформації означає, що вся необхідна інформація повинна бути надана суб'єкту персональних даних у момент запитування згоди на обробку його персональних даних [14, с. 60].

Проєкт Закону «Про захист персональних даних» визначає, що згода суб'єкта персональних даних на обробку його персональних даних вважається інформованою, якщо до її надання або на момент її надання суб'єкт персональних даних був проінформований про: 1) підставу, мету, вид обробки його персональних даних; 2) персональні дані, які підлягають обробці; 3) контактні дані контролера : постійне місце розташування та засоби зв'язку з ними у обсязі, який дозволяє суб'єкту персональних даних ідентифікувати такого контролера та оператора та безперешкодно зв'язатися з ними; 4) права, передбачені законодавством у сфері захисту персональних даних, та способи їх реалізації; 5) будь-яку іншу інформацію, необхідну для забезпечення чесної та прозорої обробки персональних даних [9].

Для того, щоб згода була визнана однозначною, заява або чітка ствердна (підтверджуюча) дія суб'єкта даних не повинні залишати жодних сумнівів щодо наміру суб'єкта даних надати згоду на обробку персональних даних. Це означає, що особа, яка дає згоду, повинна ясно та недвозначно висловити своє погодження на обробку своїх даних. Іншими словами, згода не повинна містити жодних невизначеностей. Очевидним є те, що згода походить від конкретного суб'єкта персональних даних. [23, с. 120–121; 24, с. 30].

Реалізація принципу «однозначності згоди» передбачає певні технічні вимоги, які повинні реалізовуватися отримувачем даних. Зокрема, мова йде про те, що згода повинна отримуватися тільки,

наприклад, шляхом проставлення певної відмітки у відповідному вікні в рамках веб-сайту, якою б підтверджувалася згода на обробку персональних даних, або ж надання будь-якої заяви чи підписання окремого документу. Разом з тим, мовчання суб'єкта даних, бездіяльність суб'єкта даних, автоматичне заповнення клітинок позначками або проставлення відміток (pre-ticket boxes), відповідно, не слід вважати діями, які констатують надання згоди суб'єктом даних на їх обробку.

Отож можемо сказати, що згода на обробку персональних даних, яка надана з урахуванням всіх основних вимог, таких як добровільність, конкретність, інформованість та однозначність її отримання забезпечує прозорість процесу обробки даних, який здійснюється з повагою до приватності власника даних.

Механізм згоди покликаний втілювати конституційне право на інформаційну приватність, так як відповідно до ст. 32 Конституції України будь-який збір, зберігання чи розповсюдження конфіденційної інформації можливий лише за згодою особи. Фактично, згода надає суб'єкту контроль над його персональними даними та слугує гарантією інформаційної самовизначеності особистості.

3.2. Альтернативні підстави для обробки персональних даних не пов'язані зі згодою суб'єкта на обробку персональних даних

П.2 ч.1 ст.11 закону України «Про захист персональних даних» визначає підставою для обробки персональних даних *дозвіл на обробку персональних даних, наданий володільцю персональних даних відповідно до закону виключно для здійснення його повноважень*. Проєкт закону України «Про захист персональних даних» зазначає дану підставу як «необхідності виконання завдань в суспільних інтересах або повноважень, покладених на контролера законом».

За GDPR подібна підстава міститься в статті 6(1)(e), згідно якої обробка персональних даних є законною, якщо вона необхідна для виконання завдання, здійснюваного в суспільних інтересах, або під час здійснення офіційних повноважень, покладених на контролера. Ця підстава є ключовою для організацій, які виконують завдання в суспільних інтересах або здійснюють офіційні повноваження. Вона забезпечує баланс між необхідністю обробки даних для виконання публічних функцій і захистом прав та свобод суб'єктів даних.

Так, дана підстава дозволяє обробку персональних даних без окремої згоди суб'єкта даних, якщо така обробка прямо передбачена законом і необхідна для реалізації повноважень володільця персональних даних.

В даному випадку, володільцем персональних даних є органи державної влади, органи місцевого самоврядування, професійні спілки, професійні асоціації, які мають законодавчо визначені функції та ін.

Дозвіл на обробку персональних даних, наданий володільцю персональних даних відповідно до закону реалізується в таких випадках, для прикладу, коли органи місцевого самоврядування обробляють персональні дані громадян при реєстрації їхнього місця проживання або, коли центри надання адміністративних послуг обробляють персональні дані заявників для надання послуг, передбачених законодавством, також у випадку обробки персональних даних учнів та студентів для ведення обліку, організації навчального процесу, видачі документів про освіту, яка здійснюється школою чи вищим навчальним закладом. Ще одним прикладом застосування такої підстави може бути обробка персональних даних пацієнтів для надання медичних послуг, ведення медичної документації, відповідно до законодавства у сфері охорони здоров'я, що здійснюється лікарнями та іншими медичними закладами, також військові адміністрації, інші органи військового керівництва здійснюють обробку персональних даних саме на цій правовій підставі.

Про можливість законної обробки персональних даних без згоди суб'єкта персональних даних свідчить також судова практика. Так, у постанові Касаційного адміністративного суду від 28.09.2023 у справі № 120/2431/23 позивач вказувала, що суддя Жмеринського міськрайонного суду, використовуючи службові повноваження, розпочав у спосіб, не передбачений нормами чинного законодавства та поза межами судової справи, отримувати опрацьовані персональні дані щодо позивача та членів її родини, та в спосіб, що не передбачений нормами Закону «Про захист персональних даних» поширювати їх як загальновідомі відомості в чисельних судових рішеннях.

У цій справі суд визнав протиправними дії Жмеринського міськрайонного суду, який без згоди особи обробив її персональні дані, опублікувавши її прізвище у переліку судових рішень. Суд зазначив,

що обробка персональних даних має здійснюватися або на підставі згоди суб'єкта, або відповідно до закону для реалізації повноважень володільця даних. У цьому випадку обробка не відповідала жодній з цих підстав, що порушує вимоги Закону України «Про захист персональних даних» [25].

Судова практика в Україні підтверджує, що обробка персональних даних без згоди особи можлива лише у випадках, коли це передбачено законом і є необхідним для реалізації повноважень володільця даних. Усі інші випадки обробки персональних даних без згоди суб'єкта можуть бути визнані протиправними.

Також важливим є відмітити, що згідно статті 21 GDPR, суб'єкт даних повинен мати право заперечувати проти опрацювання його персональних даних, що здійснюються на підставі статті 6(1)(e) Регламенту. Контролер не повинен більше обробляти персональні дані за винятком доведення ним наявності істотних законних підстав для обробки, що переважають над інтересами, правами та свободами суб'єкта даних або для формування, здійснення або захисту правових претензій [3].

Подібна норма міститься в законодавстві України, зокрема серед прав суб'єкта персональних даних визнається право пред'являти вмотивовану вимогу володільцю персональних даних із запереченням проти обробки своїх персональних даних.

Отже, обробка персональних даних особи на підставі п. 2 ст. 11 закону України «Про захист персональних даних» здійснюється виключно в межах повноважень, визначених законом, оскільки використання даних для інших цілей потребує окремої згоди суб'єкта персональних даних. Також обсяг оброблюваних даних повинен бути обмежений до мінімально необхідного для досягнення мети обробки. Володілець персональних даних зобов'язаний забезпечити належний рівень захисту персональних даних відповідно до вимог законодавства.

Ще однією законною підставою для обробки персональних даних без згоди суб'єкта є *укладення та виконання правочину, стороною якого є суб'єкт персональних даних або який укладено на користь суб'єкта персональних даних чи для здійснення заходів, що передують укладенню правочину на вимогу суб'єкта персональних даних*.

З даної підстави слід виділити такі моменти:

– здійснюється обробка даних суб'єкта з яким укладається правочин;

– обробка даних суб'єкта на користь якого укладається правочин;

– для здійснення заходів, що передують укладенню правочину.

Згідно зі статтею 6(1)(b) (GDPR), обробка персональних даних з даної підстави є законною, якщо вона має критерій «необхідності»:

– необхідна для виконання правочину, стороною якого є суб'єкт даних;

– необхідна для вжиття заходів на запит суб'єкта даних перед укладенням правочину.

Дана підстава застосовується, коли є потреба обробити персональні дані контрагента при проведенні переддоговірної роботи або при укладенні цивільно-правового, господарського договору або при укладенні трудового договору між працівником та роботодавцем. В наведених прикладах спостерігаємо, що обробка персональних даних є необхідною та неминучою для виникнення між суб'єктами відносин на основі договору.

На цьому наголошує також й судова практика, зокрема, в рішенні Макарівського районного суду Київської області від 07.06.2021 № 370/2799/2 зазначається, що відповідно до п. 3 ст. 11 Закону України «Про захист персональних даних» , підставою для обробки персональних даних, зокрема, є: "3) укладення та виконання правочину, стороною якого є суб'єкт об'єкта персональних даних або який укладено на використання суб'єкта персональних даних чи для здійснення заходів, що передають укладення правочину на вимогу суб'єкта персональних даних". Виходячи із прямої норми даної статті та вимог законодавства у сфері фінансових послуг, відповідач не тільки може, а і зобов'язаний обробляти персональні дані позивача до моменту припинення договірних відносин [26].

Також обробка персональних даних без згоди суб'єкта за п. 3 ст. 11 Закону України «Про захист персональних даних» дозволяється при укладенні трудового договору. Як відомо, статтею 43 Конституції України гарантовано, що кожен має право на працю і, відповідно, від надання особою згоди на обробку її персональних даних не повинна залежати реалізація його права на працю. При цьому необхідність

виконання обов'язку володільця персональних даних, має передбачатися законом.

Тобто персональні дані повинні використовуватися роботодавцем виключно з метою здійснення прав і виконання своїх обов'язків у сфері трудових правовідносин: вести первинний облік працівників, забезпечувати додатковими гарантіями, надавати щорічні основні та додаткові відпустки на підставі підтвердних документів, тощо. І, оскільки персональні дані отримані роботодавцем під час виконання своїх обов'язків на підставі закону, отримувати згоду на їх обробку у працівника не потрібно.

При використанні даної підстави обробки слід дотримуватися умов щодо обсягу даних, які обробляються: обмежити обробку лише тими даними, які є необхідними для виконання договору, та інформування суб'єкта даних: суб'єкт персональних даних має бути поінформований про обробку його даних, мету обробки та його основних прав.

Для прикладу, працівник оскаржив встановлення відеоспостереження на робочому місці, стверджуючи, що не був належним чином поінформований про це. Суд зазначив, що роботодавець повинен мати законну підставу та обґрунтовану мету для встановлення відеоспостереження, а також забезпечити прозорість та інформування працівників.

Суд дослідив, що в повідомленні про зміну істотних умов праці, які були направлені працівникам відповідача, в тому числі й позивачу, зазначені мета та завдання необхідності введення відеоспостереження на території Товариства: серед яких фіксація з метою об`єктивної оцінки при виникненні конфліктних ситуацій між працівниками та відвідувачами, клієнтами роботодавця, недопущення матеріальних збитків в умовах дії дестабілізуючих факторів; забезпечення контролю за дотриманням норм з охорони праці, дотримання трудової дисципліни, забезпечення режиму безпеки, тощо. Після чого суд встановив, що позивачем не надано належних та допустимих доказів втручання відповідача в особисте та сімейне життя позивача та будь-якого порушення його прав введенням в дію відеоспостереження на підприємстві. Указані зміни в роботі Товариства суд розцінює як зміна істотних умов праці [27].

Важливим є відмітити, що на противагу законодавству України, GDPR містить спеціальну норму (ст.88) «Обробка в контексті зайня-

тості» щодо особливостей використання персональних даних працівників. Так, згідно цієї статті, держави-члени можуть, за допомогою закону чи колективних угод, передбачати спеціальні норми для забезпечення захисту прав і свобод у зв'язку з обробкою персональних даних працівників у контексті зайнятості, зокрема для цілей працевлаштування, виконання трудового договору, в тому числі, виконання обов'язків, установлених законом або колективними угодами, управління, планування та організації праці, рівності та різноманітності на робочому місці, здоров'я та безпеки на робочому місці, захисту майна працедавців чи споживачів, та для цілей реалізації і користування, індивідуально чи колективно, правами та перевагами, пов'язаними із зайнятістю, а також для цілей припинення трудових відносин [3].

Наразі є тлумачення застосування даної норми статті 88 GDPR, яке відбулося по справі C-34/21 Hauptpersonalrat der Lehrerinnen und Lehrer beim Hessischen Kultusministerium vs Minister des Hessischen Kultusministeriums, вирішеній 30 березня 2023 року. Європейський суд справедливості («Суд справедливості») надав попереднє рішення за запитом Адміністративного суду міста Вісбаден, Німеччина, в якому він звернувся до Суду з проханням вирішити питання про законність системи прямої трансляції занять, прийнятої під час пандемії COVID-19, без попередньої згоди відповідних вчителів.

Передумовою було те, що Міністр освіти та культури землі Гессен («міністр освіти») під час пандемії COVID-19 встановив рамки, згідно з якими учні, які не могли бути присутніми в класі, могли відвідувати свої заняття онлайн. Для забезпечення прав учнів щодо захисту персональних даних було вирішено, що на таку послугу прямої трансляції мають дати згода самі учні, а для молодших школярів – їхні батьки. Однак згода вчителів, які проводять заняття, не була передбачена, оскільки застосовувалося правила обробки даних у трудових відносинах. У зв'язку з цим Комітет директорів з питань вчителів («Комітет директорів штабу») при Міністерстві освіти подав позов до суду, скаржачись на те, що пряма трансляція занять у режимі відеоконференції не була поставлена в залежність від згоди відповідних вчителів.

Міністр освіти посилався на «необхідність» як на правову основу для обробки таких даних, що відповідає статті 88GDPR. Стаття 88 GDPR стосується обробки даних у контексті трудових відносин,

при цьому державам-членам надається дискреція передбачати більш конкретні правила щодо обробки персональних даних працівників.

Суд відповів, що «статтю 88 GDPR слід тлумачити як таку, що означає, що національне законодавство не може становити «більш конкретне правило» [...] якщо воно не відповідає умовам, викладеним у пункті 2 ст. 88», що означає, що воно повинна включати відповідні та конкретні заходи для захисту законних інтересів та основних прав суб'єкта даних.

Для роботодавців це рішення по суті означає, що щодо звичних процесів обробки персональних даних у трудових відносинах – мають застосовуватися правила GDPR. Зокрема, роботодавцям потрібно буде враховувати статтю 6(1) GDPR під час обробки даних про працівників та визначати конкретні підстави обробки. [28] У цьому випадку, обробка персональних даних вчителів без їхньої згоди на підставі внутрішнього закону Гессен про захист даних є несумісною з GDPR.

Отож, як бачимо, основними вимогами законного використання для обробки персональних даних, такої підстави як укладення та виконання правочину потребує дотримання ряду умов: конкретна мета обробки; мінімізація даних – обробляються тільки ті, які необхідні для укладення та виконання правочину; суб'єкти даних поінформовані про таку обробку.

Ще однією підставою законної обробки персональних даних без згоди суб'єкта законодавство визначає *«захист життєво важливих інтересів суб'єкта персональних даних».*

В період дії правового режиму воєнного стану в Україні обробка персональних даних часто здійснюється на підставі п. 4 ч. 1 ст. 11 Закону України «Про захист персональних даних» з метою захисту життєво важливих інтересів суб'єкта персональних даних.

Ця підстава застосовується у випадку надання суб'єкту персональних даних медичної допомоги, захисту його життя, здоров'я від протиправних посягань, проведення аварійно-рятувальних операцій щодо громадян. Водночас, фізична особа, або установа, яка здійснила обробку персональних даних для захисту життєво важливих інтересів суб'єкта персональних даних повинна отримати від нього згоду на таку обробку, коли це стане можливим, або припинити дії з персональними даними у разі відмови від надання такої згоди.

Особливості прояву цієї підстави обробки персональних даних суб'єктами персональних даних у період дії режиму воєнного стану полягають у наступному:

– надається переважно суб'єктам владних повноважень, включно з військовими адміністраціями, що утворюються відповідно до Закону України «Про правовий режим воєнного стану»;

– діє не довше, ніж це необхідно суб'єкту владних повноважень для виконання покладених на нього обов'язків;

– стосується лише чітко визначених персональних даних;

– має строковий характер;

– надається лише в межах компетенції суб'єкта владних повноважень.

Відповідно, за наявності вказаної підстави суб'єкти владних повноважень не повинні відбирати у громадян згоду на обробку їхніх персональних даних незалежно від того, чи є вони військово зобов'язаними особами, чи виконують обов'язки у складі Збройних сил України, Національної гвардії України, сил територіальної оборони [29].

Слід звернути увагу, обробка персональних даних для захисту життєво важливих інтересів суб'єкта персональних даних може здійснюватися в тих випадках, коли суб'єкт, який здійснює таку обробку не має на це прямого дозволу згідно із законодавством України, або згоду на дії з персональними даними неможливо отримати через фізичний, психо-емоційний стан особи, дані якої обробляються. Проте, фізична особа, або установа, яка здійснила обробку персональних даних для захисту життєво важливих інтересів суб'єкта персональних даних повинна отримати від нього згоду на таку обробку, коли це стане можливим, або припинити дії з персональними даними у разі відмови від надання такої згоди

Згідно Закону України «Основи законодавства України про охорону здоров'я», у разі наявності ознак прямої загрози життю особи та необхідності надання невідкладної медичної допомоги за умови неможливості отримання з об'єктивних причин згоди (наприклад, через втрату свідомості) на медичне втручання від самої особи чи її законних представників, медичне втручання проводиться без такої згоди [30]. Тож і обробка необхідних для цього персональних даних ведеться без згоди особи, безпосередньо на підставі п. 4 ч. 1 ст. 11 Закону України «Про захист персональних даних».

За GDPR (ст. 6(1)(d)) обробка є законною, якщо вона необхідна для захисту життєво важливих інтересів суб'єкта даних або іншої фізичної особи. Як бачимо, дана підстава за національним законодавством України та GDPR є тотожними.

Проаналізуємо одну з ключових справ у Європейській практиці щодо права на життя, медичної етики та обробки персональних даних у контексті захисту життєво важливих інтересів – справу Lambert v. France 2015 року.

Вінсент Ламбер, медичний працівник, потрапив у ДТП у 2008 році та перебував у вегетативному стані. У нього не було письмової згоди на припинення лікування. Його дружина та частина родини підтримували рішення лікарів припинити штучне харчування, посилаючись на його усні висловлювання про небажання підтримувати життя в такому стані. Батьки Ламбера оскаржили це рішення в судах Франції, посилаючись на право на життя.

Conseil d'État (Державна рада Франції) підтвердила право лікарів припинити лікування згідно з Законом Леонетті (2005), що дозволяє припинення лікування у разі "невиправданої медичної наполегливості". У цій справі ЄСПЛ вперше прямо визнав допустимість пасивної евтоназії за умов правових гарантій. Суд не визнав обов'язку держави зберігати життя будь-якою ціною, якщо така медична допомога суперечить інтересам пацієнта. Рішення ґрунтувалось на усних висловлюваннях Вінсента Ламбера, які вважалися достатньо чіткими для виявлення його волі.

Яким же чином дана справа пов'язана із ст. 6(1)(d) GDPR? У ході розгляду справи відбувалася обробка медичних даних Ламбера, його думки про життя і смерть, усні висловлювання, дані родичів. Така обробка відбувалася без згоди суб'єкта, але в інтересах його здоров'я, у межах медичної та судової компетенції, відповідно до національного та європейського законодавства на основі ст. 6(1)(d) GDPR [31].

Ця справа є прецедентною для визначення допустимості припинення підтримки життя на основі припущеної волі пацієнта.

Необхідність виконання обов'язку володільця персональних даних, який передбачений законом, як підстава обробки персональних даних без згоди суб'єкта, надає можливість володільцю персональних даних у повному обсязі виконати свої обов'язки, передбачені законодавством.

Така обробка здійснюється володільцем за умови, коли закон прямо вимагає виконання певного обов'язку, для реалізації якого неможливо обійтись без обробки персональних даних. При цьому, за загальним правилом, володілець самостійно вирішує, виходячи з покладених на нього обов'язків, чи потребує він для їх здійснення обробки персональних даних суб'єктів.

Як зазначає Маркіян Бем, вказана підстава перетинається з підставою, передбаченою п. 2 ч. 1 ст. 11 Закону України «Про захист персональних даних», де мова йде про обробку у зв'язку з необхідністю виконання повноважень (тобто прав та обов'язків). Така плутанина спричинена невдалим копіюванням положень європейського законодавства в національне: слово «task», що означає «завдання», яке використовується в Регламенті, неправильно перекладено, як «повноваження». Тому проведення обробки у зв'язку з виконанням повноважень (прав та обов'язків) частково перетинається з такою підставою, як обробка з метою виконання обов'язку, а саме в частині, що стосується обробки персональних даних державним органом з метою виконання обов'язків. Однак, як уже зазначено вище, підстава, передбачена п. 2 ч. 1 ст. 11 Закону (щодо повноважень), стосується здебільшого діяльності державних органів, а підстава, передбачена п. 5 ч. 1 ст. 11 Закону (необхідність виконання обов'язку), стосується також інших володільців – суб'єктів приватноправових відносин [14].

Прикладами застосування даної підстави є нарахування податків, що здійснюється податковими органами; подання інформації до Державної служби фінансового моніторингу України суб'єктами фінансового моніторингу; виконання судових рішень згідно Закону України «Про виконавче провадження» та ін.

Так, адміністративна справа, яка була розглянута Касаційним адміністративним судом у складі Верховного Суду України та Постанова у ній була ухвалена 24 квітня 2019 року, хоч не стосувалися безпосереднього порушення порядку обробки персональних даних, але було встановлено, підставою обробки є норма закону та договірні відносини.

У справі позивач оскаржував дії Фонду гарантування вкладів фізичних осіб (ФГВФО) та банку, які впливали на реалізацію його прав вкладника, включаючи блокування рахунків. В цьому випадку, обробка персональних даних (ідентифікація особи вклад-

ника, зберігання банківської інформації) була необхідною для виконання законного обов'язку банку та ФГВФО [32].

Остання підстава для обробки персональних даних без згоди суб'єкта, яка визначена в п. 6 ч. 1 ст. 11 Закону України «Про захист персональних даних», є захист *законних інтересів володільця персональних даних або третьої особи, за умови що не порушуються права і свободи суб'єкта даних.*

В ст. 6(1)(f) GDPR дана підстава викладена як «обробка необхідна для цілей законних інтересів контролера або третьої сторони, крім випадків, коли ці інтереси переважаються інтересами чи основними правами та свободами суб'єкта даних».

Перш за все слід визначити, що таке «законний інтерес», який ще називають «легітимний», так як саме термін «legitimate interests» вживається в ст. 6(1)(f) GDPR.

Законний інтерес – це реальний, обґрунтований інтерес, який випливає з діяльності або юридичних обов'язків володільця, не суперечить закону, не є надмірним щодо обсягу оброблювальних даних, не порушує права і свободи суб'єкта персональних даних.

Законний інтерес не може бути підставою для обробки персональних даних без згоди, якщо: обробка є надмірною (наприклад, збираються «зайві» дані), обробка непрозора або прихована, суб'єкт не може реалізувати своє право на заперечення, обробка може завдати шкоди репутації, здоров'ю, приватному життю особи; стосуватися вразливих категорій суб'єктів.

Регламент конкретно згадує використання даних клієнтів або співробітників, маркетинг, запобігання шахрайству, внутрішньогрупові передачі даних або IT-безпека як потенційні законні інтереси, але це не вичерпний перелік. Також зазначено, що є законний інтерес у розкритті інформації про можливі злочинні дії або загрози безпеці.

То як оцінити законність інтересу? Оцінка законного (легітимного) інтересу – це процес, який визначає, чи має володілець персональних даних (контролер) право обробляти дані без згоди суб'єкта на підставі своїх законних інтересів, і чи не переважають при цьому права та свободи самої особи.

GDPR визначає таку оцінку як LIA – Legitimate Interest Assessment, і є ключовою умовою законності обробки за ст. 6(1)(f) GDPR, а також

аналогічно застосовується в Україні згідно зі ст. 11 Закону «Про захист персональних даних».

Оцінка відповідності вимогам (LIA) поділяється на три етапи:

1) оцінка наявності законного інтересу (Purpose test) – аналізується чи не є інтерес протизаконним, чи є він обґрунтованим;

2) встановлення необхідності обробки (Necessity test) – аналізується чи є обробка пропорційною (не надмірною), необхідною (не просто бажаною), чи можна досягти цілей менш навязливими методами;

3) проведення тесту на балансування (Balancing test) – аналізується чи очікує суб'єкт таку обробку (reasonable expectations), чи може це обмежити його права (приватність, свобода, безпека), чутливість даних (спеціальні категорії даних, дані дітей), можливість реалізації прав (заперечення, доступ, видалення), чи передбачена відповідна прозорість і контроль [33].

Наприклад, Бельгійський наглядовий орган у справі № 46/2024 (рішення від 15.03.2024) дійшов висновку, що створення банком моделі клієнтських профілів з метою подальшого надання персоналізованих знижок слід розглядати як окрему обробку персональних даних, що здійснюється з урахуванням легітимного інтересу, адже вона є частиною позиціонування банку на ринку. Банк повинен сформувати уявлення про своїх клієнтів, реагуючи на суспільні зміни та тенденції, такі як оцифрування та персоналізація послуг. Без аналізу даних про транзакції модель не може навчатися й знижки не можуть бути запропоновані в персоналізованому порядку через додаток, а тому, за висновком наглядового органу, така обробка є необхідною для досягнення легітимного інтересу [34].

Наглядовий орган Греції погодив розкриття даних про здоров'я лікарнею на прохання адвоката захисту для цілей судового розгляду.

Лікарня звернулася до грецького Управління з захисту даних (DPA), чи дозволено їй розкривати певну медичну інформацію про пацієнта юридичній фірмі, яка запитує доступ до неї. Юридична фірма запросила інформацію щодо перебування пацієнта в лікарні (дата та тривалість) та його стан здоров'я. Обґрунтуванням запиту було те, що ця інформація була необхідною у відкритому судовому процесі, ініційованому пацієнтом проти клієнта юридичної фірми. Пацієнт вимагав

відшкодування збитків у розмірі 14 500 євро, стверджуючи, що будівельна недбалість призвела до перелому його руки та стегна.

У цьому випадку DPA вирішило, що розкриття конфіденційних записів дозволено. Воно стверджувало, що згідно з національним законодавством про захист даних таке розкриття дозволено за виняткових обставин, зокрема для цілей судового розгляду. DPA підтримало підстави законних інтересів, оскільки розкриття даних було пропорційно необхідним для спростування звинувачень суб'єкта даних проти його орендодавця, висунутих у позові. DPA також зазначило, що розкриття буде законним лише за умови, що суб'єкт даних буде повідомлений про обмін даними. У цьому випадку лікарня вже повідомила суб'єкта даних про існування запиту юридичної фірми [35].

Інший приклад, який відображає незаконне зберігання банківських даних інтернет-магазином для полегшення подальших платежів та оптимізації бізнес-операцій.

Французьке Управління з захисту даних (DPA) розслідувало практику інтернет-магазину щодо зберігання банківських даних клієнтів довше, ніж необхідно для здійснення транзакції. Було виявлено, що компанія зберігала банківські дані за замовчуванням після кожної транзакції (включаючи ім'я власника картки, номер картки, термін дії та деякі коди CVV). Продавець стверджував, що зберігав дані на двох законних підставах: необхідність укладення або виконання договору та необхідність у своїх законних інтересах. Заявленими законними інтересами були сприяння платежам та оптимізація бізнес-операцій.

Управління з захисту даних встановило, що зберігання банківських реквізитів виходить за рамки виконання договору на надання послуг для онлайн-покупки, оскільки метою було б сприяння неконкретним, гіпотетичним майбутнім покупкам. Воно також виявило, що обробка даних не була заснована на законних інтересах. DPA визнало існування законного комерційного інтересу роздрібного продавця у сприянні платежам та оптимізації бізнес-операцій. Однак це має бути збалансовано з правами відповідних суб'єктів даних. Враховуючи чутливість банківських даних, право суб'єкта на видалення даних після їх зберігання протягом певного періоду часу має більшу вагу, ніж інтерес контролера. DPA також зазначило, що продавець не вжив заходів

для зменшення небезпеки для суб'єктів даних шляхом запровадження відповідних заходів безпеки, оскільки дані кредитних карток мільйонів клієнтів зберігалися у відкритому тексті в єдиній базі даних, що робило її вразливою для зловмисних співробітників або зовнішніх вторгнень [35].

Наведені приклади демонструють, що застосування підстави «законного інтересу» вимагає ретельної оцінки та балансування між інтересами контролера і правами суб'єктів даних.

Якщо порівнювати з іншими можливими підставами для обробки персональних даних (виконання договору, згода та ін.), законний (легітимний) інтерес є значно більш гнучкою підставою і може використовуватись для ширшого кола відносин щодо обробки даних, обумовлених законним інтересом суб'єкта господарювання [34].

Захист законного інтересу – це гнучка, але не абсолютна підстава обробки персональних даних. Вона дозволяє володільцям даних діяти без згоди, коли це виправдано, але зобов'язує обґрунтовувати законність інтересу і дотримуватись балансу з правами людини.

4. Висновки

Отож, узагальнюючи все вищевикладене, можемо відмітити, що правове регулювання обробки персональних даних ґрунтується на чіткому визначенні її законних підстав, які забезпечують баланс між потребами володільців персональних даних та правами фізичних осіб на інформаційну приватність.

Одним з основних завдань володільця персональних даних можна вважати правильний вибір підстав обробки, адже це зумовлює дотримання основних прав особи щодо прозорості використання та захисту її персональних даних, що в свою чергу, є гарантією невтручання в особисте життя. Зокрема, у разі обробки персональних даних на підставі згоди суб'єкта, необхідно дотримуватися чіткого документування процесу її отримання, в той час як обробка з альтернативних підстав, що не передбачають згоду, – здійснюється з дотриманням вимог законності, необхідності, пропорційності, прозорості, конкретності.

Вбачається необхідність створення незалежного контролюючого органу із законодавчим закріпленням статусу та процедур взаємодії з володільцями й суб'єктами персональних даних.

Слід відмітити, що останні зміни українського законодавства в сфері захисту персональних даних максимально спрямовані на гармонізацію з європейськими стандартами. Так, у проєкті нового Закону «Про захист персональних даних» уніфікується термінологія та категорії персональних даних, деталізується перелік правових підстав їх обробки за моделлю GDPR, а також посилюється механізм захисту даних та відповідальність суб'єктів обробки.

Це свідчить про розвиток національного законодавства від декларативного до функціонально-орієнтованого підходу, в якому кожна підстава обробки має чітке нормативне обґрунтування, межі та гарантії.

Список літератури:

1. Конституція України: Закон України від 28 червня 1996 р. № 254к/96-ВР. *Відомості Верховної Ради України*. 1996. № 30. Ст. 141.

2. Конвенція про захист прав людини і основоположних свобод: Рада Європи. URL: http://zakon2.rada.gov.ua/laws/show/995_004 (дата звернення: 08.06.2025)

3. Загальний регламент із захисту персональних даних Європейського Союзу (GDPR) № 2018/1725. URL: http://aphd.ua/gdpr-ofitsiinyi-ukranskyi-pereklad (дата звернення: 08.06.2025)

4. Spanish DPA Fines Supermarket Chain 2,520,000 EUR for Unlawful Use of Facial Recognition System. URL: https://natlawreview.com/article/spanish-dpa-fines-supermarket-chain-2520000-eur-unlawful-use-facial-recognition (дата звернення: 08.06.2025)

5. French SA fines Cityscoot 125 000€. URL: https://edpb.europa.eu/news/national-news/2023/french-sa-fines-cityscoot-125-000eu_en (дата звернення: 08.06.2025)

6. Постанова Київського апеляційного суду від 18 грудня 2020 року, апеляційне провадження № 33/824/4207/2020 за матеріалами справи №761/23532/20. URL: https://verdictum.ligazakon.net/document/94663887

7. Постанова Броварського міськрайонного суду від 09.04.2020 року № 361/1579/20. URL: https://verdictum.ligazakon.net/document/88698313

8. Постанова Київського апеляційного суду від 18 грудня 2020 року, апеляційне провадження № 33/824/4207/2020 за матеріалами справи №761/23532/20. URL: https://verdictum.ligazakon.net/document/94663887 (дата звернення: 01.07.2025)

9. Проєкт закону України «Про захист персональних даних» від 20 листопада 2024 року № 4065-IX / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/4065-20#Text (дата звернення: 28.06.2025)

10. Дяковський О.С. Визначення поняття персональних даних як правової категорії: сучасні проблеми та шляхи вирішення. *Інформація і право*. 2017. № 3 (22). С. 51-56.

11. Брижко В.М., Радянська А.І., Швець М.Я. Порівняльно-правове дослідження відповідності законодавства України законодавству ЄС у сфері персональних даних. Київ : Тріумф, 2006. С. 22.

12. Середа О.Г., Красюк Т.В. Персональні дані працівника та їх захист в умовах цифровізації. *Аналітично-порівняльне правознавство. Розділ v. Трудове право; право соціального забезпечення*. 2023. № 3. С. 188-193.

13. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних від 28.01.1981 № 108. URL: https://zakon.rada.gov.ua/laws/show/994_326#Text (дата звернення: 28.06.2025)

14. Бем М., Городиський І. Захист персональних даних: правове регулювання та практичні аспекти: науково-практичний посібник. Київ : «К.І.С.», 2021. 157 с.

15. Рішення Конституційного Суду України у справі за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України № 2-рп/2012 від 20.01.2012 року. URL: https://zakon.rada.gov.ua/laws/show/v002p710-12#Text

16. Справа S. and marper v. the United Kingdom. 4 грудня 2008 року. URL: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-117631%22]}

17. Справа Green v. United Kingdom. 8 квітня 2025 року. URL: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-242635%22]}

18. Справа Gillberg v. Sweden. 3 квітня 2012 року. URL: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-110144%22]}

19. Про захист персональних даних: Закон України від 1 червня 2010 р. № 2297-VI. / Верховна Рада України. *Відомості Верховної Ради України*. 2010. № 34. Ст. 481.

20. Роз'яснення до Типового порядку обробки персональних даних. URL: https://zakon.rada.gov.ua/laws/show/n0001715-14#Text (дата звернення: 01.07.2025)

21. Головацький Н.Т. Прозорість та згода як основні принципи захисту персональних даних в Україні. *Науковий вісник Ужгородського Національного Університету. Серія ПРАВО.* 2024. Випуск 83: частина 2. С. 178-184.

22. Постанова Вінницького апеляційного суду від 24.06.2024 року по справі № 127/13877/19. URL: https://zakononline.com.ua/court-decisions/show/90109587

23. Borghi M., Ferretti F., Karapapa S. Online data processing consent under EU law: a theoretical framework and empirical evidence from the UK. *International Journal of Law and Information Technology*. Vol. 21. № 2(2013). P. 109-153.

24. Явор О. А., Піддубна В. Ф., Рубан О. О. Правові проблеми захисту персональних даних неповнолітніх осіб відповідно до вимог вітчизняного законодавства та вимог GDPR. *Journal «ScienceRise: Juridical Science».* 2023. № 3(25). С. 23-34.

25. Постанова Касаційного адміністративного суду від 28.09.2023 у справі №120/2431/23. URL: https://protocol.ua/ru/postanova_kas_vp_vid_28_09_2023_roku_u_spravi_120_2431_23/?utm_source=chatgpt.com

26. Рішенні Макарівського районного суду Київської області від 07.06.2021, № 370/2799/2. URL: https://verdictum.ligazakon.net/document/98662944

27. Рішення Саксаганського районного суду м. Кривого Рогу від 30.10.2024, № 122792073. URL: https://youcontrol.com.ua/catalog/court-document/122792073/?utm_source=chatgpt.com

28. Справа C-34/21 Hauptpersonalrat der Lehrerinnen und Lehrer beim Hessischen Kultusministerium проти Minister des Hessischen Kultusministeriums від 30 березня 2023 року. URL: https://curia.europa.eu/juris/document/document.jsf?docid=272066&doclang=DE

29. На яких основних підставах здійснюється обробка персональних даних у період запровадження воєнного стану? Платформа прав людини. URL: https://www.ppl.org.ua/wp-content/uploads

30. Основи законодавства України про охорону здоров'я: Закон України від 19 листопада 1992 року № 2801-XII. URL: https://zakon.rada.gov.ua/laws/show/2801-12#Text (дата звернення: 08.06.2025)

31. Справа Lambert і Інші проти Франції. 05 червня 2015 року. URL: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-155352%22]}

32. Постанова Верховного Суду України від 24 квітня 2019 року, №826/22950/1. URL: https://protocol.ua/ua/postanova_kas_vp_vid_24_04_2019_roku_u_spravi_826_22950_15/

33. The Legitimate interest as a lawful basis for processing personal data under the General Data Protection Regulation. URL: https://www.bchlaw.eu/articles/the-legitimate-interest-as-a-lawful-basis-for-processing-personal-data-under-the-general-data-protection-regulation/?utm_source=chatgpt.com

34. Полтавцева А. Законний інтерес як можлива підстава для обробки персональних даних. URL: https://blog.liga.net/user/apoltavtseva/article/53526?utm_source=chatgpt.com

35. Processing Personal Data on the Basis of “Legitimate Interests” Under the GDPR. URL: https://www.cpomagazine.com/data-protection/processing-personal-data-on-the-basis-of-legitimate-interests-under-the-gdpr/?utm_source=chatgpt.com

References:

1. 1.Konstytutsiia Ukrainy: Zakon Ukrainy vid 28 chervnia 1996 r. № 254k/96-VR [Constitution of Ukraine: Law of Ukraine of June 28, 1996 No. 254k/96-VR]. *Vidomosti Verkhovnoi Rady Ukrainy*. 1996. № 30. St. 141.

2. 2.Konventsiia pro zakhyst prav liudyny i osnovopolozhnykh svobod: Rada Yevropy [Convention for the Protection of Human Rights and Fundamental Freedoms: Council of Europe]. Available at: http://zakon2.rada.gov.ua/laws/show/995_004 (accessed: 08.06.2025)

3. 3.Zahalnyi rehlament iz zakhystu personalnykh danykh Yevropeiskoho Soiuzu (GDPR) № 2018/1725 [General Data Protection Regulation of the European Union (GDPR) No. 2018/1725]. Available at: http://aphd.ua/gdpr-ofitsiinyi-ukranskyi-pereklad (accessed: 08.06.2025)

4. Spanish DPA Fines Supermarket Chain 2,520,000 EUR for Unlawful Use of Facial Recognition System. Available at: https://natlawreview.com/article/spanish-dpa-fines-supermarket-chain-2520000-eur-unlawful-use-facial-recognition (accessed: 08.06.2025)

5. French SA fines Cityscoot 125 000€. Available at: https://edpb.europa.eu/news/national-news/2023/french-sa-fines-cityscoot-125-000eu_en (accessed: 08.06.2025)

6. Postanova Kyivskoho apeliatsiinoho sudu vid 18 hrudnia 2020 roku, apeliatsiine provadzhennia № 33/824/4207/2020 za materialamy spravy № 761/23532/20 [Resolution of the Kyiv Court of Appeal dated December 18, 2020, appeal proceedings No. 33/824/4207/2020 on the materials of the case No. 761/23532/20]. Available at: https://verdictum.ligazakon.net/document/94663887

7. Postanova Brovarskoho miskraionnoho sudu vid 09.04.2020 roku № 361/1579/20 [Resolution of the Brovary City District Court dated April 9, 2020 No. 361/1579/20]. Available at: https://verdictum.ligazakon.net/document/88698313

8. 8.Postanova Kyivskoho apeliatsiinoho sudu vid 18 hrudnia 2020 roku, apeliatsiine provadzhennia № 33/824/4207/2020 za materialamy spravy № 761/23532/20 [Resolution of the Kyiv Court of Appeal dated December 18, 2020, appeal proceedings No. 33/824/4207/2020 on the materials of the case No. 761/23532/20]. Available at: https://verdictum.ligazakon.net/document/94663887 (accessed: 01.07.2025)

9. Proiekt zakonu Ukrainy «Pro zakhyst personalnykh danykh» vid 20 lystopada 2024 roku № 4065-IX [Draft Law of Ukraine "On Personal Data Protection" dated November 20, 2024 No. 4065-IX]. Verkhovna Rada Ukrainy. Available at: https://zakon.rada.gov.ua/laws/show/4065-20#Text (accessed: 28.06.2025)

10. Diakovskyi O.S. (2017). Vyznachennia poniattia personalnykh danykh yak pravovoi katehorii: suchasni problemy ta shliakhy vyrishennia [Definition of the concept of personal data as a legal category: current problems and solutions]. *Informatsiia i pravo.* № 3 (22). S. 51-56.

11. Bryzhko V.M., Radianska A.I., Shvets M.Ia. (2006). Porivnialno-pravove doslidzhennia vidpovidnosti zakonodavstva Ukrainy zakonodavstvu YeS u sferi personalnykh danykh [Comparative legal study of the compliance of Ukrainian legislation with EU legislation in the field of personal data]. Kyiv : Triumf, s. 22.

12. Sereda O.H., Krasiuk T.V. (2023). Personalni dani pratsivnyka ta yikh zakhyst v umovakh tsyfrovizatsii [Employee personal data and their protection in the context of digitalization]. *Analitychno-porivnialne pravoznavstvo. Rozdil v. Trudove pravo; pravo sotsialnoho zabezpechennia*. № 3. S. 188-193.

13. Konventsiia pro zakhyst osib u zviazku z avtomatyzovanoiu obrobkoiu personalnykh danykh vid 28.01.1981 № 108 [Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28.01.1981 No. 108]. Available at: https://zakon.rada.gov.ua/laws/show/994_326#Text (accessed: 28.06.2025)

14. Bem M., Horodyskyi I. (2021). Zakhyst personalnykh danykh: pravove rehuliuvannia ta praktychni aspekty: naukovo-praktychnyi posibnyk [Protection of Personal Data: Legal Regulation and Practical Aspects: Scientific and Practical Guide]. Kyiv : «K.I.S.», 157 s.

15. Rishennia Konstytutsiinoho Sudu Ukrainy u spravi za konstytutsiinym podanniam Zhashkivskoi raionnoi rady Cherkaskoi oblasti shchodo ofitsiinoho tlumachennia polozhen chastyn pershoi, druhoi statti 32, chastyn druhoi, tretoi statti 34 Konstytutsii Ukrainy № 2-rp/2012 vid 20.01.2012 roku [Decision of the Constitutional Court of Ukraine in the case on the constitutional submission of the Zhashkiv District Council of Cherkasy Region on the official interpretation of the provisions of parts one, two of Article 32, parts two, three of Article 34 of the Constitution of Ukraine No. 2-rp/2012 dated January 20, 2012]. Available at: https://zakon.rada.gov.ua/laws/show/v002p710-12#Text

16. Sprava S. and marper v. the United Kingdom. 4 hrudnia 2008 roku [Case S. and Marper v. the United Kingdom. 4 December 2008]. Available at: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-117631%22]}

17. Sprava Green v. United Kingdom. 8 kvitnia 2025 roku [Case Green v. United Kingdom. 8 April 2025]. Available at: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-242635%22]}

18. Sprava Gillberg v. Sweden. 3 kvitnia 2012 roku [Case Gillberg v. Sweden. 3 April 2012]. Available at: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-110144%22]}

19. Pro zakhyst personalnykh danykh: Zakon Ukrainy vid 1 chervnia 2010 r. № 2297-VI [On the Protection of Personal Data: Law of Ukraine dated June 1, 2010 No. 2297-VI]. Verkhovna Rada Ukrainy. *Vidomosti Verkhovnoi Rady Ukrainy*. 2010. № 34. St. 481.

20. Roziasnennia do Typovoho poriadku obrobky personalnykh danykh [Clarifications to the Standard Procedure for Processing Personal Data]. Available at: https://zakon.rada.gov.ua/laws/show/n0001715-14#Text (accessed: 01.07.2025)

21. Holovatskyi N.T. (2024). Prozorist ta zghoda yak osnovni pryntsypy zakhystu personalnykh danykh v Ukraini [Transparency and Consent as the Basic Principles of Personal Data Protection in Ukraine]. *Naukovyi visnyk Uzhhorodskoho Natsionalnoho Universytetu. Seriia PRAVO*. Vypusk 83: chastyna 2. S. 178-184.

22. Postanova Vinnytskoho apeliatsiinoho sudu vid 24.06.2024 roku po spravi № 127/13877/19 [Resolution of the Vinnytsia Court of Appeal dated June 24, 2024 in case No. 127/13877/19]. Available at: https://zakononline.com.ua/court-decisions/show/90109587

23. Borghi M., Ferretti F., Karapapa S. (2013). Online data processing consent under EU law: a theoretical framework and empirical evidence from the UK. *International Journal of Law and Information Technology*. Vol. 21. № 2. P. 109-153.

24. Iavor O. A., Piddubna V. F., Ruban O. O. (2023). Pravovi problemy zakhystu personalnykh danykh nepovnolitnikh osib vidpovidno do vymoh vitchyznianoho zakonodavstva ta vymoh GDPR [Legal issues of protecting personal data of minors in accordance with the requirements of domestic legislation and GDPR requirements]. *Journal «ScienceRise: Juridical Science».* № 3(25). S. 23-34.

25. Postanova Kasatsiinoho administratyvnoho sudu vid 28.09.2023 u spravi № 120/2431/23 [Resolution of the Cassation Administrative Court dated 09/28/2023 in case No. 120/2431/23]. Available at: https://protocol.ua/ru/postanova_kas_vp_vid_28_09_2023_roku_u_spravi_120_2431_23/?utm_source=chatgpt.com

26. Rishenni Makarivskoho raionnoho sudu Kyivskoi oblasti vid 07.06.2021, № 370/2799/2 [Decision of the Makariv District Court of Kyiv Region dated 06/07/2021, No. 370/2799/2]. Available at: https://verdictum.ligazakon.net/document/98662944

27. Rishennia Saksahanskoho raionnoho sudu m. Kryvoho Rohu vid 30.10.2024, № 122792073 [Decision of the Saksagansky District Court of Kryvyi Rih dated 10/30/2024, No. 122792073]. Available at: https://youcontrol.com.ua/catalog/court-document/122792073/?utm_source=chatgpt.com

28. Case C-34/21 Hauptpersonalrat der Lehrerinnen und Lehrer beim Hessischen Kultusministerium proty Minister des Hessischen Kultusministeriums. Available at: https://curia.europa.eu/juris/document/document.jsf?docid=272066&doclang=DE

29. Na yakykh osnovnykh pidstavakh zdiisniuietsia obrobka personalnykh danykh u period zaprovadzhennia voiennoho stanu? Platforma prav liudyny [On what main grounds is personal data processed during the period of martial law? Human Rights Platform]. Available at: https://www.ppl.org.ua/wp-content/uploads

30. Osnovy zakonodavstva Ukrainy pro okhoronu zdorovia: Zakon Ukrainy vid 19 lystopada 1992 roku № 2801-XII [Fundamentals of Ukrainian legislation on health care: Law of Ukraine of November 19, 1992 No. 2801-XII]. Available at: https://zakon.rada.gov.ua/laws/show/2801-12#Text (accessed: 08.06.2025)

31. Sprava Lambert i Inshi proty Frantsii. 05 chervnia 2015 roku [Case Lambert and Others v. France. June 5, 2015]. Available at: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-155352%22]}

32. Postanova Verkhovnoho Sudu Ukrainy vid 24 kvitnia 2019 roku, №826/22950/1 [Resolution of the Supreme Court of Ukraine dated April 24, 2019, No. 826/22950/1]. Available at: https://protocol.ua/ua/postanova_kas_vp_vid_24_04_2019_roku_u_spravi_826_22950_15/

33. The Legitimate interest as a lawful basis for processing personal data under the General Data Protection Regulation. Available at: https://www.bchlaw.eu/ articles/the-legitimate-interest-as-a-lawful-basis-for-processing-personal-data-under-the-general-data-protection-regulation/?utm_source=chatgpt.com

34. Poltavtseva A. Zakonnyi interes yak mozhlyva pidstava dlia obrobky personalnykh danykh [Legitimate interest as a possible basis for processing personal data]. Available at: https://blog.liga.net/user/apoltavtseva/article/53526?utm_source=chatgpt.com

35. Processing Personal Data on the Basis of “Legitimate Interests” Under the GDPR. Available at: https://www.cpomagazine.com/data-protection/processing-personal-data-on-the-basis-of-legitimate-interests-under-the-gdpr/?utm_source=chatgpt.com