

ТРУДОВЕ ПРАВО

УДК 349.2:004.056.53 (477)

DOI <https://doi.org/10.32782/2408-9257-2024-6-9>

Колб С. О.,

*кандидат юридичних наук,
доцент кафедри права*

*Волинського інституту імені В'ячеслава Липинського
Міжрегіональної академії управління персоналом*

ПРАВОВЕ РЕГУЛЮВАННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ПРАЦІВНИКІВ: МІЖНАРОДНІ СТАНДАРТИ ТА ПЕРСПЕКТИВИ ВДОСКОНАЛЕННЯ В УКРАЇНІ

LEGAL REGULATION OF PERSONAL DATA PROTECTION OF EMPLOYEES: INTERNATIONAL STANDARDS AND PROSPECTS FOR IMPROVEMENT IN UKRAINE

У статті досліджено актуальні проблеми правового регулювання захисту персональних даних працівників в умовах цифровізації трудових процесів, розвитку автоматизованих систем управління персоналом (ATS) і впровадження новітніх технологій. Аналізується сучасний стан національного законодавства України щодо відповідності міжнародним і європейським стандартам, зокрема Загальному регламенту із захисту даних (GDPR) та Конвенції Ради Європи 108+. Виявлено ключові проблеми: відсутність спеціалізованих норм для регулювання обробки персональних даних у трудових відносинах, недосконалість механізмів контролю за дотриманням законодавства роботодавцями, недостатню деталізацію правового режиму чутливих і біометричних даних.

Особливу увагу приділено питанням правового регулювання використання цифрових засобів моніторингу працівників. Акцентовано на необхідності встановлення чітких меж і правил щодо моніторингу працівників на робочому місці з дотриманням принципів прозорості, мінімізації втручання у приватне життя і захисту конфіденційності. Обґрунтовано важливість посилення гарантій щодо обробки біометричних даних як чутливої категорії інформації, зокрема шляхом впровадження посилених стандартів захисту та отримання добровільної, інформованої згоди працівників.

У статті висвітлено необхідність удосконалення Кодексу законів про працю України шляхом закріплення обов'язків роботодавців щодо забезпечення конфіденційності персональних даних працівників. Зазначено необхідність упровадження принципів «захисту даних за призначенням» і «захисту даних за замовчуванням», закріплення права працівників на доступ, виправлення, видалення даних, зокрема реалізацію «права бути забутим». Підкреслено, що імплементація міжнародних стандартів, таких як GDPR, сприятиме гармонізації національного законодавства з європейськими підходами, підвищенню рівня правової обізнаності громадян, забезпеченню ефективного захисту права на приватність, інтеграції до Єдиного цифрового ринку ЄС. Наголошено, що формування прозорих і безпечних механізмів обробки персональних даних дозволить досягти балансу між правами працівників на приватність і законними інтересами роботодавців щодо організації трудового процесу в умовах глобальної цифрової трансформації.

Ключові слова: *трудове право, конфіденційність, цифрові технології, право на приватність, європейські стандарти, біометричні дані, роботодавець.*

The article explores pressing issues related to the legal regulation of personal data protection for employees in the context of labor process digitalization, the development of automated personnel management systems (ATS), and the implementation of new technologies. It analyzes the current state of Ukraine's national legislation regarding compliance with international and European standards, particularly the General Data Protection Regulation (GDPR) and the Council of Europe's Convention 108+. Key issues identified include the absence of specialized norms regulating the processing of personal data in labor relations, insufficient mechanisms for monitoring employers' compliance with legal requirements, and a lack of detailed provisions regarding the legal regime for sensitive and biometric data.

Particular attention is paid to the legal regulation of digital monitoring tools used for employee surveillance. The necessity of establishing clear boundaries and rules for monitoring employees in the workplace is emphasized, with

adherence to the principles of transparency, minimal interference with privacy, and confidentiality protection. The article underscores the importance of enhancing safeguards for processing biometric data as a sensitive category of information, specifically through the implementation of strengthened security standards and the requirement for obtaining voluntary and informed consent from employees.

The study highlights the need to improve Ukraine's Labor Code by enshrining employers' obligations to ensure the confidentiality of employees' personal data. It stresses the necessity of introducing principles such as «data protection by design» and «data protection by default,» as well as enshrining employees' rights to access, correct, and delete their data, including exercising the «right to be forgotten.» The article argues that the implementation of international standards, such as GDPR, will promote the harmonization of national legislation with European approaches, enhance citizens' legal awareness, ensure effective privacy protection, and facilitate Ukraine's integration into the EU's Digital Single Market. Furthermore, the formation of transparent and secure mechanisms for data processing is seen as a way to balance employees' privacy rights and employers' legitimate interests in organizing the labor process amidst global digital transformation.

Key words: labor law, confidentiality, digital technologies, privacy rights, European standards, biometric data, employer.

Постановка проблеми. Сучасний розвиток цифрових технологій та новітніх форм зайнятості створює нові виклики у сфері захисту персональних даних працівників. Інформація про працівників, яка збирається та обробляється роботодавцями, набуває стратегічного значення як для забезпечення прав працівників, так і для організації ефективного управління трудовими ресурсами. Проте, в умовах зростаючої залежності від автоматизованих систем та розширення інструментів моніторингу виникає небезпека порушення прав на приватність та конфіденційність. Особливо важливим є завдання створення правових механізмів, які б забезпечували справедливий баланс між правами працівників на захист їхньої приватності та інтересами роботодавців у здійсненні контролю за робочим процесом. Актуальність цієї проблеми визначається не лише науковим інтересом до захисту фундаментальних прав людини, але й необхідністю адаптації національного законодавства до міжнародних та європейських стандартів. Удосконалення нормативного регулювання обробки персональних даних є важливим завданням для України як країни, що інтегрується до європейського правового простору. Недоліки чинного законодавства, відсутність спеціалізованих норм у сфері трудових відносин та недостатній рівень правозастосування створюють значні ризики як для працівників, так і для роботодавців, ускладнюючи виконання міжнародних зобов'язань України та обмежуючи її конкурентоспроможність у глобальній економіці.

Вирішення зазначеної проблеми має ключове значення для створення ефективного

механізму захисту персональних даних, формування прозорого та безпечного цифрового середовища, а також для підвищення рівня правової обізнаності громадян. Науковий аналіз і розробка рекомендацій для вдосконалення національного законодавства в контексті міжнародного досвіду є важливими кроками для досягнення цих цілей.

Аналіз останніх досліджень і публікацій. У сфері захисту персональних даних працівників відзначається активний науковий інтерес до проблематики, пов'язаної із правовим регулюванням цього питання. Зокрема, Г. Спіцина та С. Гуцу у своїй роботі аналізують особливості колізії між правом працівника на приватність та правом роботодавця здійснювати контроль за трудовою діяльністю, наголошуючи на необхідності встановлення чітких меж між цими правами (2023). Ф. Хендрікс досліджує загальні принципи захисту персональних даних працівників у міжнародному контексті, приділяючи особливу увагу ролі міжнародних трудових стандартів у формуванні правового регулювання цієї сфери (2022). О. Середа акцентує на прогалинах у національному законодавстві України, особливо у контексті гармонізації з європейськими стандартами, та пропонує шляхи вдосконалення правового механізму захисту персональних даних працівників (2023).

Інший важливий аспект – нормативне регулювання в умовах цифрової трансформації – розкрито в дисертаційному дослідженні А. Михайлика, де автор аналізує виклики, пов'язані із впровадженням новітніх технологій у сферу трудових відносин (2023). Дослі-

дження Цвірюка Д. В. та Сопілка І. М. акцентують увагу на проблемах і недоліках у чинному законодавстві України, серед яких недосконалість понятійного апарату, недостатня деталізація правового режиму персональних даних та слабкий контроль за виконанням законодавчих норм (2013). Окремо слід відзначити роботи, які висвітлюють міжнародний досвід. Так, І. Яворська та М. Микієвич у своїх дослідженнях аналізують специфіку регулювання захисту персональних даних у праві Європейського Союзу, зокрема у контексті впровадження GDPR (2019).

Метою статті є аналіз сучасного стану правового регулювання захисту персональних даних працівників в Україні, вивчення міжнародних і європейських стандартів у цій сфері, визначення їхнього впливу на національне законодавство та обґрунтування шляхів його вдосконалення з метою забезпечення ефективного захисту прав працівників в умовах цифровізації та інтеграції до європейського правового простору.

Виклад основного матеріалу. Право на приватність, закріплене у міжнародних і європейських стандартах, визнано одним із фундаментальних прав людини, що регулюється такими документами, як Загальна декларація прав людини та Конвенція про захист прав людини і основоположних свобод. У сфері трудових відносин це право набуває специфічного змісту, зумовленого взаємодією працівника і роботодавця. Відносини підпорядкування, які лежать в основі трудових відносин, передбачають право роботодавця керувати робочим процесом, здійснювати моніторинг виконання обов'язків працівника, його поведінки та місцезнаходження, а також застосовувати дисциплінарні заходи за необхідності. Як зазначають Г. Спіцина та С. Гуцу, у таких умовах виникає колізія між правом працівника на приватність, що включає право «бути залишеним наодинці», та правом роботодавця здійснювати контроль за діяльністю працівника у робочий час [12, с. 257].

Питання конфіденційності стають особливо актуальними в умовах дистанційної та гнучкої зайнятості, де відсутність територіальної прив'язки зумовлює зростання контролю роботодавців за допомогою цифрових технологій.

У зв'язку з цим виникає необхідність встановлення чітких правових меж для обробки персональних даних працівників на основі принципів мінімізації, обмеження цілей використання та забезпечення прозорості процедур збору й обробки інформації. Право працівників на конфіденційність і захист даних повинно бути закріплене законодавчо шляхом створення універсальних стандартів, що гарантують однаковий рівень захисту для всіх працівників. Френк Хендрікс зазначає, що право на приватність і захист даних є фундаментальним правом людини, захищеним міжнародними інструментами та конституціями багатьох країн. Він підкреслює, що втручання в приватне життя повинно бути оцінене крізь призму правозахисних механізмів. У трудових відносинах права на конфіденційність і захист персональних даних є невід'ємно пов'язаними, що вимагає інтеграції принципів захисту прав людини у сферу праці [15].

У сучасних умовах, коли питання конфіденційності набувають все більшої ваги, особливо важливо звертати увагу на міжнародний досвід і стандарти у цій сфері. Глобалізація трудових відносин і активне впровадження цифрових технологій роблять міжнародні й європейські підходи до захисту персональних даних невід'ємною складовою формування правової бази. Україна, як частина світового співтовариства, інтегрує ці стандарти у національне законодавство, тим самим сприяючи зміцненню прав працівників на захист персональних даних. Серед основних міжнародних документів, що формують правові засади у сфері захисту персональних даних, варто виділити Рекомендації Генеральної Асамблеї ООН від 14 грудня 1990 р. щодо регулювання комп'ютеризованих файлів персональних даних. У цьому документі закріплено мінімальні гарантії захисту даних, які зберігаються в інформаційних системах урядових та міжнародних організацій. У подальшому, 18 грудня 2013 р., Генеральна Асамблея ООН прийняла Резолюцію № 68/167 про право на конфіденційність у цифрову епоху, в якій акцентується на тому, що розвиток технологій створює можливості для спостереження, перехоплення та збору даних, що потенційно можуть порушувати права людини, зокрема право на приватність

[8]. 18 грудня 2014 р. була ухвалена Резолюція № 69/166, присвячена праву на приватне життя в епоху цифрових технологій. На її основі Радою з прав людини була прийнята Резолюція 28/16, що деталізує захист права на приватність у цифрову епоху [9].

На європейському рівні правове регулювання захисту персональних даних здійснюється як у рамках Європейського Союзу, так і Ради Європи. Особливе значення має ст. 8 Європейської конвенції з прав людини, яка закріплює право кожного на повагу до приватного та сімейного життя. Визначальним документом Ради Європи у цій сфері стала Резолюція 1165 від 1998 р., яка розширила тлумачення права на приватність, включивши до нього «право жити своїм особистим життям з мінімальним втручанням» та право особи контролювати інформацію про себе.

З боку Європейського Союзу також було розроблено низку нормативних актів, спрямованих на захист персональних даних у сфері праці. Важливою є Європейська директива із захисту даних 1995 р., яка заклала основу для подальших законодавчих ініціатив. На її основі Європейська «Робоча група із захисту даних» ухвалила низку рекомендацій, що стосуються обробки персональних даних у контексті трудових відносин. Серед них Висновок 8/2001 від 13 вересня 2001 р., що став базовим документом для регулювання збору та обробки персональних даних працівників. Крім того, у 2002 р. було прийнято Робочий документ ЄС щодо комунікації на робочому місці, а в 2017 р. – Висновок 2/2017, який оновив підходи до обробки даних працівників з урахуванням сучасних технологічних викликів. Впровадження Загального регламенту захисту даних (GDPR) у 2018 р. суттєво трансформувало систему регулювання обробки персональних даних. Хоча «Робочу групу із захисту даних» замінила Європейська рада із захисту даних, її попередні рекомендації залишаються актуальними для правозастосування. 25 травня 2018 р. набув чинності Загальний регламент із захисту персональних даних (General Data Protection Regulation, GDPR), прийнятий Європейським Союзом 26 квітня 2016 р. [14]. Цей регламент встановив високі стандарти захисту персональних даних у державах-членах ЄС та

створив механізм для поширення його вимог на суб'єкти господарювання, які здійснюють діяльність поза межами ЄС, але обробляють дані громадян ЄС [12, с. 257–258].

Щодо України, то в нашій державі основним нормативно-правовим актом, що регулює захист персональних даних в Україні, є Закон України від 01.06.2010 р. № 2297-VI «Про захист персональних даних» у редакції від 18.01.2025 [1]. Його положення доповнено трьома підзаконними актами, затвердженими наказом Уповноваженого Верховної Ради України з прав людини від 8 січня 2014 р. № 1/02-14 [7]. До них належать: Типовий порядок обробки персональних даних; Порядок здійснення контролю Уповноваженим за додержанням законодавства у сфері захисту персональних даних; Порядок повідомлення Уповноваженого про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних.

Попри деталізацію у вказаних нормативно-правових актах, їхні положення залишаються загальними й не враховують специфіку регулювання трудових відносин [10, с. 209]. У трудовому законодавстві України на сьогодні відсутні спеціалізовані норми, які регулювали б права, обов'язки та відповідальність роботодавців у контексті захисту персональних даних працівників. Хоча роботодавці володіють правом збору, обробки та використання персональних даних працівників у межах трудових відносин, вони зобов'язані забезпечити конфіденційність таких даних і їхній належний захист. Відтак, гарантії захисту персональних даних набувають стратегічного характеру, формуючи основу для побудови ефективного механізму правового регулювання у цій сфері.

У сучасному законодавстві України виділено кілька основних аспектів гарантій захисту персональних даних. До них належать: заборона на обробку окремих категорій персональних даних або запровадження спеціальних умов для їх обробки; забезпечення права працівників на доступ до інформації про себе; функціонування спеціального органу, який здійснює контроль за дотриманням вимог законодавства у сфері захисту персональних даних; встановлення юридичної відповідальності за порушення відповідних норм [2].

Гарантії захисту персональних даних працівників – це нормативно визначена система заходів, спрямованих на забезпечення конфіденційності інформації про працівника на всіх етапах її обробки та запобігання несанкціонованому доступу третіх осіб. Вони поділяються на загальні, що поширюються на всіх фізичних осіб, і спеціальні, які враховують особливості правового статусу працівника [4]. До загальних гарантій належать законодавчо встановлені вимоги до обробки персональних даних, зокрема визначені у статтях 6, 7 та 11 ЗУ «Про захист персональних даних» [1]. Обробка персональних даних має відповідати чітко визначеній меті, наприклад, перевірці кваліфікації, нарахуванню заробітної плати чи сплаті податків, а також бути прозорою та законною. Працівники мають право на безперешкодний доступ до своїх персональних даних, а будь-які обмеження такого доступу визнаються незаконними. До спеціальних гарантій належать заборона обробки певних категорій інформації, таких як дані про расове походження, політичні чи релігійні переконання, стан здоров'я, біометричні та генетичні дані, крім випадків, передбачених законом. Під час збирання додаткової інформації роботодавець зобов'язаний отримати письмову згоду працівника. Крім того, роботодавець несе обов'язок забезпечити належний захист персональних даних та заборонити доступ сторонніх осіб до цієї інформації без законних підстав.

Сучасне законодавство України передбачає нові підходи до регулювання згоди працівників на обробку їхніх персональних даних. Як зазначає А. Михайлик, відповідно до ст. 11 Закону України «Про захист персональних даних», письмова згода працівника не потрібна у випадках, коли обробка персональних даних здійснюється з метою виконання роботодавцем своїх зобов'язань, передбачених законодавством (п. 5 ст. 11) [1]. Це дає можливість роботодавцям реалізовувати трудові відносини відповідно до Кодексу законів про працю України за умови дотримання вимог щодо захисту персональної інформації [3, с. 75].

Водночас необхідно розмежовувати поняття згоди працівника на обробку персональних даних та зобов'язання про нерозголошення конфіденційної інформації. Зобов'язання про

нерозголошення обов'язкове для підписання працівниками, які мають доступ до персональних даних інших осіб, і є ключовим аспектом дотримання законодавства, оскільки його виконання перевіряється компетентними органами.

Окремого регулювання потребує використання персональних даних працівників у публічних джерелах, таких як корпоративні вебсайти або соціальні мережі. Закон дозволяє таку обробку без письмової згоди лише за умови, що це пов'язано з реалізацією трудових відносин. Якщо персональні дані використовуються для інших цілей, наприклад, у маркетингових кампаніях, роботодавець зобов'язаний отримати письмову згоду працівника. Як приклад, використання фотографій, професійних профілів, інформації про освіту та досвід роботи у рекламній кампанії маркетингової компанії вимагає письмового дозволу кожного працівника, оскільки це виходить за межі трудових відносин [4, с. 135].

Згода суб'єкта персональних даних є добровільним волевиявленням фізичної особи щодо надання дозволу на обробку її персональних даних, висловленим у письмовій формі або в інший спосіб, що дозволяє зробити висновок про її надання. Заборонено обробляти конфіденційну інформацію без згоди особи, за винятком випадків, коли це визначено законом, і виключно в інтересах національної безпеки, економічного добробуту чи захисту прав людини. Роботодавець повинен надати працівнику можливість обмежити право на обробку персональних даних у межах наданої згоди. Працівник має право відкликати згоду у будь-який момент без пояснення причин, після чого роботодавець зобов'язаний припинити обробку даних. Ця вимога поширюється на випадки, коли згода є єдиною підставою для обробки.

Документи, які підтверджують надання згоди, мають зберігатися протягом усього періоду обробки персональних даних. Законодавство не визначає конкретного структурного підрозділу, де слід зберігати такі документи, залишаючи це питання на розсуд роботодавця. Згода на обробку персональних даних повинна зберігатися до моменту припинення обробки відповідних даних, наприклад, до видалення інформації про працівника з вебсайту або соціальних мереж. Якщо згода надана на визначений строк,

персональні дані можуть використовуватися лише в межах цього строку. У разі зміни мети обробки персональних даних, яка є несумісною з попередньою, роботодавець зобов'язаний отримати нову згоду працівника. Така згода повинна відповідати новій меті, якщо інше не передбачено законодавством. Сучасний розвиток цифрових та телекомунікаційних технологій породжує нові виклики у сфері захисту персональних даних, зокрема в контексті обробки біометричних даних. Одним із таких викликів є питання запровадження допуску працівників на територію підприємств, установ чи організацій через використання відбитків пальців.

Відповідно до чинного законодавства, обробка біометричних даних, зокрема відбитків пальців, не заборонена, однак потребує дотримання вимог щодо захисту персональних даних. Біометричні дані належать до особливо чутливих категорій персональних даних, обробка яких становить підвищений ризик для прав і свобод суб'єкта даних. ЗУ «Про захист персональних даних» дозволяє обробку таких даних лише за наявності однозначної згоди суб'єкта персональних даних (ч. 2 ст. 7) [1].

Роботодавець зобов'язаний отримати від кожного працівника свідому згоду на обробку біометричних даних. Ця згода має бути добровільною, а працівник повинен бути належним чином поінформований про мету обробки, відповідальну особу, заходи захисту, а також можливі ризики. Якщо хоча б один працівник відмовиться надати згоду, запровадження системи допуску через обробку відбитків пальців стає неможливим. Крім того, відмова працівника надати згоду не може бути підставою для його звільнення за ініціативою роботодавця.

У разі отримання згоди від усіх працівників роботодавець повинен виконати низку юридичних та організаційних вимог:

- призначити відповідального за організацію роботи із захисту персональних даних відповідно до наказу (ч. 2 ст. 24);
- внести зміни до локального Положення про обробку і захист персональних даних працівників;
- повідомити Секретаріат Уповноваженого Верховної Ради України з прав людини про обробку чутливих персональних даних, що становить особливий ризик для прав і свобод суб'єктів персональних даних.

Повідомлення до Секретаріату необхідно направити упродовж 30 робочих днів із дня початку обробки таких даних (ст. 9). У документі слід детально зазначити мету обробки біометричних даних, організаційні та технічні заходи для забезпечення їхнього захисту. Недотримання цих вимог може призвести до адміністративної відповідальності за ст. 188-39 та ст. 188-40 КУпАП.

Порушення вимог законодавства у сфері захисту персональних даних передбачає адміністративну та кримінальну відповідальність. Законодавство України регламентує порядок обробки, зберігання, використання та передачі персональних даних, встановлюючи санкції за його порушення.

Адміністративна відповідальність визначена статтею 188-39 Кодексу України про адміністративні правопорушення. За несвоєчасне повідомлення Уповноваженого Верховної Ради України з прав людини про обробку персональних даних, які становлять особливий ризик для прав і свобод осіб, передбачено штрафи: для громадян – від 100 до 200 неоподатковуваних мінімумів доходів громадян (далі – нмдг), для посадових осіб та суб'єктів підприємницької діяльності – від 200 до 400 нмдг [4]. Таке повідомлення має бути надіслане протягом 30 робочих днів з моменту початку обробки даних, відповідно до статті 9 Закону України «Про захист персональних даних» [1].

Невиконання законних вимог Уповноваженого щодо усунення порушень також тягне за собою штрафи: для громадян – від 200 до 300 нмдг, для посадових осіб та підприємців – від 300 до 1000 нмдг. Повторні порушення протягом р. передбачають підвищення штрафів: для громадян – до 500 нмдг, для посадових осіб і підприємців – до 2000 нмдг.

Незаконна обробка даних, що призвела до порушення прав суб'єктів або незаконного доступу, карається штрафом: для громадян – від 100 до 500 нмдг, для посадових осіб і підприємців – від 300 до 1000 нмдг. Повторні порушення передбачають санкції до 2000 нмдг.

Кримінальна відповідальність за незаконне збирання, використання, зберігання чи поширення конфіденційної інформації встановлена статтею 182 Кримінального кодексу України. Такі дії караються штрафом від 500 до

1000 нмдг, виправними роботами до 2 років, арештом до 6 місяців або обмеженням волі до 3 років. Якщо порушення вчинене повторно або завдало істотної шкоди, передбачено арешт від 3 до 6 місяців, обмеження волі до 5 років або позбавлення волі на той самий строк [4, с. 139–144].

На сучасному етапі розвитку інформаційних технологій постає нагальна потреба у вдосконаленні правового механізму захисту персональних даних працівників, зумовлена широким впровадженням цифрових технологій, автоматизованих систем управління персоналом та новітніх форм зайнятості. Науковці виділяють ключові прогалини у законодавстві, що регулює захист персональних даних працівників. Зокрема, І. М. Сопілко акцентує увагу на відсутності чіткого законодавчого визначення категорій персональних даних працівника, що спричиняє численні зловживання у цій сфері [11]. Д. В. Цвірюк додає, що недоліками є неврегульованість складу інформації, яка входить до поняття «персональні дані», відсутність єдиного нормативного визначення цього терміну та ігнорування сучасних економічних реалій, таких як облік фінансового стану працівників, їхніх банківських рахунків і прав власності [13].

Серед чинників, що сприяють порушенням у цій сфері, А. Михайлик виділяє надмірне навантаження на Уповноваженого Верховної Ради України з прав людини, що ускладнює охоплення перевітками всіх володільців персональних даних. У багатьох регіонах відсутні представники Уповноваженого, що перешкоджає оперативному реагуванню на звернення громадян. Низька правова обізнаність працівників також зумовлює їхню пасивність у захисті своїх прав. Додатковими проблемами є низька активність самого Уповноваженого у здійсненні перевірок, безвідповідальність роботодавців як володільців персональних даних та недостатня судова практика у цій сфері. Особливо гостро це проявляється у випадках, коли суб'єктами персональних даних є працівники приватного сектору [3; 4].

Для вдосконалення законодавства необхідно оновити понятійний апарат Закону України «Про захист персональних даних», чітко розмежувати процеси обігу та обробки даних, кла-

сифікувати персональні дані за категоріями та встановити для кожної з них окремий правовий режим. Необхідно прийняти закон, який врахуватиме специфіку автоматизованої обробки даних, цифрових технологій і професійного використання персональних даних.

Запровадження механізмів балансу між правом на свободу інформації та правом на захист персональних даних є важливим аспектом удосконалення. Доцільним є чітке закріплення прав суб'єктів персональних даних, таких як право на виправлення і видалення даних, зокрема «право бути забутим». У контексті локального регулювання рекомендується прийняття внутрішніх положень, що регламентують порядок обробки персональних даних на підприємствах з урахуванням специфіки їхньої діяльності. Ці положення мають відповідати законодавству та не погіршувати правове становище працівників.

Автоматизовані системи управління персоналом (ATS), які використовуються у кадрових процесах, значно оптимізують роботу, але створюють додаткові ризики для захисту даних. Їх впровадження вимагає забезпечення високих стандартів кібербезпеки, а роботодавці зобов'язані дотримуватись законодавчих вимог щодо збору, обробки і зберігання даних.

Також актуальним є регулювання використання засобів контролю за працівниками, таких як поліграфи чи системи спостереження. Їх застосування має бути чітко обмеженим, здійснюватися виключно за наявності правових підстав і попереднього повідомлення працівників.

Варто зазначити, що в цьому напрямі вже здійснюються практичні кроки. Україна, підписавши Угоду про асоціацію з Європейським Союзом, взяла на себе зобов'язання забезпечити належний рівень захисту персональних даних, що стало підґрунтям для розроблення та затвердження Плану заходів із вдосконалення національного законодавства у відповідності до стандартів GDPR [5]. У рамках цього процесу 25 жовтня 2022 р. було внесено законопроект № 8153 «Про захист персональних даних», а 20 листопада 2024 р. Верховна Рада України ухвалила постанову про прийняття законопроекту за основу для подальшого доопрацювання [6].

Законопроект має на меті адаптацію національного законодавства до сучасних міжнародних стандартів, зокрема GDPR і Конвенції Ради Європи 108+, що забезпечить гармонізацію нормативного регулювання, підвищення рівня захисту персональних даних, а також створення дієвих механізмів боротьби з кіберзлочинністю. Як зазначено у пояснювальній записці до законопроекту, чинний Закон України «Про захист персональних даних» 2011 р. не відповідає сучасним викликам цифрової економіки, зокрема через широке використання великих даних та автоматизованих технологій, що створює бар'єри для міжнародного співробітництва та негативно впливає на діяльність українських компаній, орієнтованих на європейський ринок.

Основними цілями законопроекту є приведення термінології та принципів обробки даних у відповідність до міжнародного права, регулювання нових аспектів обробки даних, включаючи відеоспостереження, використання біометричних даних і прямих маркетингових комунікацій, а також розширення прав суб'єктів персональних даних. Законопроект передбачає запровадження прав на забуття, портативність даних, обмеження обробки та захист від автоматизованого прийняття рішень, встановлення зобов'язань контролерів і операторів даних, а також введення інституту відповідальної особи із захисту персональних даних у державних органах.

Окрему увагу приділено обробці даних у трудових відносинах, правоохоронних цілях, електронних комунікаціях і під час передачі даних іноземним державам. Законопроект запроваджує принципи «захисту даних за призначенням» і «захисту даних за замовчуванням», що спрямовані на забезпечення конфіденційності на всіх етапах обробки інформації.

Очікується, що ухвалення цього законопроекту сприятиме виконанню міжнародних зобов'язань України, забезпечить інтеграцію до Єдиного цифрового ринку ЄС, полегшить обмін інформацією з європейськими партнерами, зміцнить правову базу для боротьби

з кіберзлочинністю та підвищить конкурентоспроможність українських підприємств на європейському ринку.

Висновки. Правове регулювання захисту персональних даних працівників є однією з ключових проблем сучасного трудового права, особливо в умовах цифровізації трудових процесів. Основними викликами залишаються недостатня адаптація національного законодавства до міжнародних стандартів, відсутність чіткого правового режиму обробки персональних даних у трудових відносинах та прогалини у регулюванні автоматизованої обробки даних. Запровадження правових норм, які враховують особливості обробки персональних даних працівників, зокрема біометричних і чутливих даних, а також вдосконалення механізмів контролю за дотриманням законодавства є необхідним для забезпечення ефективного захисту права на приватність. Імплементация міжнародних стандартів, таких як GDPR, та встановлення чітких зобов'язань для роботодавців, включаючи обов'язок інформувати працівників про використання їхніх даних, сприятимуть посиленню гарантій конфіденційності.

Окрему увагу слід приділити врегулюванню використання цифрових технологій у кадрових процесах, автоматизованих систем управління персоналом (ATS) і засобів моніторингу працівників. Необхідно встановити баланс між інтересами роботодавців щодо контролю за працівниками та правом останніх на захист персональної інформації, закріпивши норми щодо прозорості процедур спостереження. Впровадження спеціальних норм у Кодекс законів про працю України, створення механізмів відповідальності за порушення у сфері обробки даних та посилення міжнародного співробітництва у цьому питанні сприятимуть розвитку правового регулювання. Формування належної законодавчої бази забезпечить ефективний захист фундаментального права на приватність працівників, підвищить інвестиційну привабливість України та сприятиме інтеграції до європейського правового простору.

ЛІТЕРАТУРА:

1. Закон України «Про захист персональних даних». Відомості Верховної Ради України. 2010. № 34. Ст. 481. URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text>
2. Легка О. В. Актуальні питання захисту персональних даних: вітчизняний та міжнародний досвід. Правова позиція. 2021. № 2(31). С. 74–79.

3. Михайлик А. С. До питання нормативно-правового регулювання захисту персональних даних працівників в Україні. Науковий вісник Ужгородського національного університету. Серія: Право. 2022. Вип. 72 (2). С. 82–87.
4. Михайлик А. С. Захист персональних даних працівників в умовах цифрової трансформації: дис. ... докт. філософії в галузі знань 08 «Право» : спец.: 081 – Право / наук. керівник О. М. Ярошенко. Національний юридичний університет імені Ярослава Мудрого. Харків, 2023. 203 с.
5. План заходів з виконання Угоди про асоціацію між Україною та ЄС: затв. постановою Кабінету Міністрів України від 25.10.2017 р. № 1106. URL: <https://zakon.rada.gov.ua/laws/show/1106-2017-p#Text>
6. Постанова Верховної Ради України «Про прийняття за основу проекту Закону України про захист персональних даних». URL: <https://zakon.rada.gov.ua/laws/show/4065-20#Text>
7. Про затвердження документів у сфері захисту персональних даних: наказ Уповноваженого Верховної Ради України з прав людини від 08.01.2014 № 1/02-14. URL: https://zakon.rada.gov.ua/laws/show/v1_02715-14#Text
8. Резолюція Ради Європи 1165 Право на приватність. URL: <https://cedem.org.ua/library/rezolyutsiya-1165-1998-pravo-na-pryvatnist/>
9. Резолюція, ухвалена Радою з прав людини 28/16. Право на приватність в епоху цифрових технологій. URL: http://repository.un.org/bitstream/handle/11176/311688/A_HRC_RES_28_16-EN.pdf?sequence=3&isAllowed=y
10. Середа О. Г. Актуальні питання правового механізму захисту персональних даних працівника в умовах європейської інтеграції. Юридичний науковий електронний журнал. 2023. № 1. С. 207–211.
11. Сопілко І. М. Механізм захисту персональних даних: проблеми та перспективи. Юридичний вісник. 2013. № 2(27). С. 66–70.
12. Спіцина Г., Гуцу С. Ф. Щодо питання правового захисту персональних даних працівників. Науковий вісник Ужгородського національного університету. Серія: Право. 2023. Вип. 76, ч. 1. С. 255–260. DOI: <https://doi.org/10.24144/2307-3322.2022.76.1.40>
13. Цвірюк Д. В. Аналіз недоліків законодавства України у сфері захисту персональних даних. Право і безпека. 2013. № 4(51). С. 58–64.
14. Яворська І., Микієвич М. Захист персональних даних у праві Європейського Союзу. Вісник Львівського університету. Серія міжнародні відносини. 2019. Вип. 46. С. 234–240.
15. Hendrickx, F. Protection of workers' personal data: General principles, ILO Working Paper 62. Geneva: ILO, 2022. URL: <https://www.ilo.org/legacy/english/intserv/working-pape>