

УДК 342:349.2(477)

**КРОНІВЕЦЬ Т.М.**, кандидат юридичних наук, доцент, завідувач кафедри фундаментальних і приватно-правових дисциплін факультету права, публічного управління та адміністрування Вінницького державного педагогічного університету імені Михайла Коцюбинського.  
ORCID: <https://orcid.org/0000-0002-5506-3418>.

**ДОРОШ В.С.**, здобувачка першого (бакалаврського) рівня освіти спеціальності 081 “Право” Вінницького державного педагогічного університету імені Михайла Коцюбинського.  
ORCID: <https://orcid.org/0000-0002-2319-9732>.

## ЗАБЕЗПЕЧЕННЯ КОНФІДЕНЦІЙНОСТІ ПЕРСОНАЛЬНИХ ДАНИХ У ТРУДОВИХ ВІДНОСИНАХ У ЗВ’ЯЗКУ З ПОШИРЕННЯМ ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ

**Анотація.** У статті висвітлено проблемні питання забезпечення конфіденційності персональних даних у трудових відносинах, особливо в контексті поширення технологій штучного інтелекту. Наголошено на важливості врахування етичних аспектів та встановлення чітких правил використання персональних даних співробітників. Авторами проведено ґрунтовне дослідження нормативно-правової бази, яка регулює запровадження штучного інтелекту в різні сфери життєдіяльності суспільства, зокрема, і в трудові відносини. На основі зазначеного аналізу також наведено конкретні пропозиції щодо вдосконалення національного законодавства шляхом прийняття Закону України “Про штучний інтелект”. Крім того, особливу увагу автори звернули на розробку практичних рекомендацій щодо впровадження ефективних стратегій і заходів, які здатні забезпечити високий рівень безпеки персональних даних співробітників.

**Ключові слова:** конфіденційність, персональні дані, трудові відносини, інноваційні технології, штучний інтелект.

**Summary.** The scientific article highlights the problematic issues of ensuring the confidentiality of personal data in labor relations, especially in the context of the spread of artificial intelligence technologies. The importance of taking into account ethical aspects and establishing clear rules for the use of employees' personal information was emphasized. The authors conducted a thorough study of the regulatory and legal framework that regulates the introduction of artificial intelligence in various spheres of society's life, in particular, in labor relations. On the basis of the above analysis, specific proposals regarding the improvement of national legislation through the adoption of the Law of Ukraine “On Artificial Intelligence” are also given. In addition, the authors paid special attention to the development of practical recommendations for the implementation of effective strategies and measures that can ensure a high level of security of personal data of employees.

**Keywords:** privacy, personal data, labor relations, innovative technologies, artificial intelligence.

**Постановка проблеми.** За останні десятиліття сучасний світ пережив значний стрибок у сфері інформаційного розвитку. Використання штучного інтелекту (далі – ШІ) стало невід’ємною частиною багатьох сфер життя, зокрема і трудових відносин. Так, у динамічному трудовому середовищі новітні методи обробки інформації використовуються для прийняття рішень щодо найму, аналізу робочої продуктивності та автоматизації багатьох аспектів бізнесу. Проте водночас з великими можливостями, які надають відповідні технології, виникають і проблеми, наприклад, щодо забезпечення конфіденційності персональних даних. У цьому контексті важливими є не лише технічні

аспекти забезпечення захисту персональних даних, але і правові, етичні та соціальні питання, що пов'язані з використанням ШІ. Таким чином, наукове дослідження цієї проблеми має безпосередній зв'язок з практикою, адже воно відкриває можливість розробки ефективних стратегій, які сприятимуть безпеці та довірі в трудових відносинах, забезпечуючи одночасно розвиток інновацій та підвищення робочої продуктивності.

**Результати аналізу наукових публікацій.** У статті проаналізовано наукові праці різних вітчизняних та зарубіжних вчених щодо питань забезпечення конфіденційності персональних даних працівників. Зокрема, ґрунтовною є, наприклад, робота Г. Спіциної та С. Гуцу щодо визначення правового регулювання захисту персональних даних співробітників. Не менш актуальним є також і дослідження І. Теличко, О. Теличко та Ю. Чабаненко, присвячене перспективним напрямом використання технологій ШІ у правовому середовищі. Варто зауважити, що вивченням теоретичних та практичних аспектів застосування ШІ у трудових відносинах займалися й інші науковці, а саме: А. Герbland, Т. Глушко, І. Зозуля, О. Зозуля, В. Камінський, К. Кармазіна, Б. Кастерс, Т. Кронівець, Дж. Мальгері, С. Мельничук, О. Охотнікова, Н. Федосенко, Р. Чанишев.

Проте, попри наявність чималої кількості досліджень відповідна проблема вважається актуальною і потребує подальшого вивчення та вдосконалення, адже стрімкий розвиток технологій ШІ створює достатню кількість невизначених аспектів, зокрема щодо наявності в законодавстві України правових норм, які б здійснювали регулювання використання ШІ в процесі обробки персональних даних працівників.

**Метою статті** є визначення проблем, пов'язаних із забезпеченням конфіденційності персональних даних у трудових відносинах в умовах поширення технологій ШІ.

Досягнення поставленої мети передбачає вирішення таких завдань:

- дослідити нормативно-правове регулювання забезпечення конфіденційності персональних даних в Україні та у світі;
- охарактеризувати правовий захист персональних даних у випадку їх обробки ШІ;
- визначити стадії трудових відносин, на яких можуть застосовуватися ШІ;
- сформулювати конкретні практичні рекомендації та пропозиції щодо вдосконалення механізму забезпечення конфіденційності персональних даних у трудових відносинах у зв'язку з поширенням використання технологій ШІ.

**Виклад основного матеріалу.** В епоху розвитку ШІ дані стають фундаментальним стратегічним ресурсом усіх держав світу. Але водночас із цим, користувачі Інтернету опиняються у "прозорій в'язниці", де вся їхня поведінка та персональні дані знаходяться під суворим наглядом інших осіб [1]. Багато зарубіжних вчених, зокрема і Дж. Мальгері та Б. Кастерс, говорять про так звану монетизацію персональних даних, яка вже стала реальністю майже в усіх сферах цифрового ринку. Європейська Комісія підкреслює, що ринок даних споживачів швидко зростає, а бізнес-моделі, засновані на монетизації даних, стають домінуючими [2].

У цьому контексті забезпечення конфіденційності персональних даних у трудових відносинах у зв'язку з поширенням використання технологій ШІ є значущим питанням, яке вимагає підвищеної уваги як з боку роботодавців, працівників, так і законодавців. ШІ завдяки своїм аналітичним та прогностичним можливостям надає змогу здійснювати ефективне управління персоналом, аналізувати та передбачати тенденції на ринку праці, а також автоматизувувати багато інших важливих процесів. Але, на думку О. Спіциної та С. Гуцу, технологічний прогрес не лише сприяє створенню нових можливостей для збору та обробки персональних даних, що знаходять широке застосування в різних галузях, але одночасно з цим може стати і засобом порушення прав та свобод людини [3, с. 256].

Відтак з метою недопущення можливостей витоку чи зловживання даними, порушення приватності працівників надзвичайно важливо здійснювати розробку та прийняття відповідного законодавства, що регулюватиме обробку ШІ персональних даних співробітників у трудових відносинах.

Наразі національне законодавство України містить низку нормативно-правових актів, які здійснюють регулювання цієї сфери. Насамперед варто згадати Конституцію України, яка статтею 32 забороняє “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” [4].

Також вагоме значення відіграє і Закон України “Про захист персональних даних”, що встановлює права та обов’язки суб’єктів персональних даних, а також вимоги до організацій, які обробляють такі дані. Він спрямований на забезпечення конфіденційності і захисту персональних даних громадян України та інших осіб, що перебувають на території України [5].

Крім цього, Кодекс законів про працю України у ст. 25 також прямо передбачає заборону при укладенні трудового договору вимагати від осіб, які приймаються на роботу, відомості про їх партійну і національну приналежність, походження, реєстрацію місця проживання чи перебування та документи, подання яких не передбачено законодавством [6]. Ця норма підкреслює важливість захисту приватності та недопущення дискримінації на робочому місці на підставі особистих характеристик.

Не менш важливо наголосити і на тому, що право на захист персональних даних, зокрема і на забезпечення конфіденційності інформації про стан здоров’я, як і будь-яке суб’єктивне право, має реальну цінність лише тоді, коли його можна захистити в разі порушення [7, с. 803].

Відтак ст. 188-39 КУпАП передбачає відповідальність за порушення законодавства у сфері захисту персональних даних [9].

Проте слід звернути увагу на те, що цивільним законодавством України право на захист не обмежується діяльністю держави чи інших уповноважених органів, які здатні застосовувати примусові заходи до правопорушника. Як справедливо зауважують І. Зозуля, О. Зозуля, С. Мельничук, Л. Луць, Т. Кронівець та К. Кармазіна, ст. 19 Цивільного кодексу України досить широко регулює відносини самозахисту прав потерпілих [7, с. 803; 8]. Таким чином, вчені приходять до логічного висновку, що людина самостійно має право обирати ті чи інші засоби захисту залежно від змісту порушеного права, характеру правопорушення та його наслідків, а також може взагалі відмовитися від використання будь-яких засобів [7, с. 804].

Що стосується міжнародних норм, то в цьому аспекті вважаємо за необхідне згадати ст. 8 Європейської Конвенції з прав людини (Конвенції про захист прав людини і основоположних свобод) [10], ст. 12 Загальної декларації прав людини [11] та Загальний регламент про захист даних (GDPR) [12]. Так, наприклад, ст. 8 Конвенції має на меті перш за все захистити особу від свавільного втручання у її приватне та сімейне життя, житло та кореспонденцію. В контексті цієї статті Європейський суд з прав людини сформулював процедурні зобов’язання держави, які мають особливе значення при визначенні меж розсуду, наданих державі-члену. Відтак, згідно з встановленою прецедентною практикою, хоча ст. 8 не містить жодних явних процедурних вимог, процес прийняття рішень, що веде до втручання, повинен бути справедливим та таким, що забезпечує належну повагу інтересів, гарантованих особі згідно зі статтею 8 (справа “Buckley проти Сполученого Королівства”, § 76) [13, с. 9, 11-12].

Що стосується Загального регламенту про захист даних, то варто відзначити і те, що він, зі свого боку, надає особам більший контроль над їхніми персональними даними, вимагає від організацій забезпечувати належний захист цих даних та повідомляти про порушення безпеки персональних даних.

Отже, загальна мета цих національних та міжнародних норм – забезпечення прав особистої конфіденційності та захисту персональних даних громадян, що є фундаментальними правами в сучасному світі. Вони створюють рамки для заборони незаконного збирання та використання персональних даних, а також регулюють питання, пов'язані з приватністю та конфіденційністю осіб на робочому місці та в інших сферах життя. Однак, усі згадані акти мають спільний недолік – відсутність дієвих норм, які б забезпечили правовий захист персональних даних у випадку їх обробки ШІ. Зокрема, Р. Чанишев відзначає, що розробка методів правового регулювання розвитку та використання цієї технології насправді все ще перебуває на початкових етапах і значно відстає від надзвичайно швидкого розвитку відповідних систем [14, с. 604].

Так, варто наголосити, що дослідники визначають технології ШІ як “комп'ютерні або кіберфізичні системи з антропоморфним (людиноподібним) “інтелектом”, а також як науково-технічний напрям, в рамках якого ставляться і вирішуються завдання по апаратному та програмному моделюванню видів людської діяльності, які відносяться до інтелектуальних” [15, с. 85].

Перелік видів ШІ, що допомагають оптимізувати трудові відносини, зокрема через застосування цієї технології роботодавцями, не є вичерпним [16, с. 82], як і процеси, що потребують їх використання.

Таким чином, вчені виокремлюються наступні стадії трудових відносин, які тісно пов'язані з програмами обробки даних, електронними базами даних, CRM-системами, що також збирають персональні дані:

1. Проведення співбесіди з потенційним кандидатом у працівники, адже на етапі отримання резюме роботодавець вже отримує його персональні дані.
2. Укладання трудового договору, заповнення особової картки та інших документів необхідних при прийнятті на роботу.
3. Процес звільнення, після якого персональні дані працівника повинні бути знищені одразу чи через певний строк, який обумовлений згодою, політикою обробки персональних даних роботодавцем [17, с. 206-207].

Переважає більшість цих процесів здійснюється HR-спеціалістами, які й використовують технології ШІ задля автоматизації відповідної діяльності. Доречно зауважити, що Всесвітній економічний форум, з огляду на аналітичні дані та різноманітні дослідження, прогнозує, що з 2025 року буде зростати галузь шифрування та розвиватиметься сфера роботизації, що також неодмінно відобразиться і на трудових відносинах [18, с. 206].

Зважаючи на це, роботодавці мають бути особливо обережними у зборі і використанні даних своїх працівників. Важливо законодавчо визначити чіткі межі та обсяги даних, які можуть бути оброблені за допомогою ШІ. Наприклад, якщо розглядати можливість прийняття Закону України “Про штучний інтелект” [16, с. 86], то відповідні норми було б доцільно закріпити саме в цьому акті.

Окрім цього, різні зарубіжні вчені також звертають увагу на те, що наразі людство демонструє загальну занепокоєність щодо конфіденційності своєї інформації, однак робить мало дій для захисту персональних даних [19]. Такі суперечливі результати досліджень доводять, що варто підвищувати рівень правової обізнаності громадян, адже доволі часто саме відсутність знань може призвести до неправильних рішень у вагомих

питаннях стосовно збереження конфіденційності персональних даних. Задля вирішення цієї проблеми можна впровадити обов'язкове ознайомлення працівників зі своїми правами при проведенні співбесіди, наприклад, шляхом видання відповідної пам'ятки.

Збереження конфіденційності можна досягти і за допомогою використання технік анонімізації чи псевдонімізації. Це може охоплювати видалення індивідуально ідентифікованої інформації або заміну її на анонімні або псевдонімізовані дані.

На нашу думку, при запровадженні ШІ в трудові відносини варто залучити у цей процес і фахівців у IT-сфері. Саме фахові професіонали здатні забезпечити обмежений доступ до персональних даних шляхом встановлення паролів, шифрування та інших технічних засобів для збереження безпеки даних. Вони також можуть проводити регулярний моніторинг та аудит систем і процедур обробки даних для виявлення потенційних загроз конфіденційності.

І насамкінець важливо також, щоб кожне підприємство, установа чи організація розробили плани реагування на порушення безпеки даних задля швидкого усунення проблем та сповіщення відповідних органів і осіб.

Отже, впровадження всіх запропонованих пропозицій має зменшити ризик порушень безпеки даних і таким чином забезпечити конфіденційність персональної інформації у трудових відносинах.

### **Висновки.**

Конфіденційність персональних даних є критично важливою у трудових відносинах, особливо з урахуванням використання технологій ШІ. Організації повинні приділяти цьому аспекту особливу увагу і розвивати механізми та стратегії, які здатні забезпечити належний захист даних працівників. Відтак використання ШІ в трудових відносинах, зокрема і для обробки персональних даних, має ретельно контролюватися роботодавцями задля запобігання можливим порушенням прав співробітників. Водночас ми визначили, що ця сфера потребує і належного правового регулювання, наприклад, прийняття Закону України "Про штучний інтелект", у якому можливо було б закріпити норми щодо меж та обсягу даних, які можуть бути оброблені за допомогою цієї інформаційної технології.

Крім цього, не менш важливо здійснювати і розробку та впровадження ефективних систем шифрування та автентифікації для забезпечення безпеки даних, а також вдосконалення процедур моніторингу та аудиту для виявлення загроз конфіденційності.

Таким чином, тільки такий комплексний підхід забезпечить збереження конфіденційності персональних даних у трудових відносинах та зменшить ризик можливих проблем у майбутньому.

### **Використана література**

1. Yu X., Zhao Y. Dualism in data protection: Balancing the right to personal data and the data property right. *Computer Law & Security Review*. 2019. Vol. 35(5): 105318. URL: <http://surl.li/mjull> (дата звернення: 19.10.2023).
2. Malgieri, G., Custers, B. Pricing privacy – the right to know the value of your personal data. *Computer Law & Security Review*. 2018. Vol. 34 (2). С. 289-303.
3. Спіцина Г.О., Гуцу С.Ф. Щодо питання правового захисту персональних даних працівників. *Науковий вісник Ужгородського Національного Університету. Серія Право*. Вип. 76 (1). 2023. С. 255-260.
4. Конституція України: Закон України від 28.06.96 р. № 254к/96-ВР, станом на 01.01.20 р. URL: <https://zakon.rada.gov.ua/laws/show/254k/96-вр#Text> (дата звернення: 11.09.2023).
5. Про захист персональних даних: Закон України від 01.06.10 р. № 2297-VI, станом на 27.10.22 р. URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text> (дата звернення: 11.09.2023).

6. Кодекс законів про працю України: Закон України від 10.12.71 р. № 322-VIII, станом на 30.07.23 р. URL: <https://zakon.rada.gov.ua/laws/show/322-08#Text> (дата звернення: 11.09.2023).
7. Zozulia I., Zozulia O., Melnychuk S., Luts L., Kronivets T., Karmazina S. Protection of the Right to Information on One's Health by Authorized State Bodies. *Systematic Reviews in Pharmacy*. 2020. Vol. 11, Issue 10. С. 803-806.
8. Цивільний кодекс України: Закон України від 16.01.03 р. № 435-IV, станом на 05.10.23 р. URL: <https://zakon.rada.gov.ua/laws/show/435-15#Text> (дата звернення: 11.10.2023).
9. Кодекс України про адміністративні правопорушення (статті 1 – 212-24): Закон України від 07.12.84 р. № 8073-X, станом на 20.08.23 р. URL: <https://zakon.rada.gov.ua/laws/show/80731-10#Text> (дата звернення: 11.09.2023).
10. Конвенція про захист прав людини і основоположних свобод: Конвенція Ради Європи від 4 листопада 1950 р., станом на 01.08.21 р. URL: [https://zakon.rada.gov.ua/laws/show/995\\_004#Text](https://zakon.rada.gov.ua/laws/show/995_004#Text) (дата звернення: 12.09.2023).
11. Загальна декларація прав людини: Декларація ООН від 10 грудня 1948 р. URL: [https://zakon.rada.gov.ua/laws/show/995\\_015#Text](https://zakon.rada.gov.ua/laws/show/995_015#Text) (дата звернення: 12.09.2023).
12. Загальний регламент про захист даних (GDPR). URL: <https://gdpr-text.com/uk> (дата звернення: 12.09.2023).
13. Право на повагу до приватного і сімейного життя: посібник за статтею 8 Конвенції про захист прав людини та основоположних свобод / пер. з доп. О. Дроздов, О. Дроздова. 2018. 83 с. URL: [https://unba.org.ua/assets/uploads/1259d4263dac852ef056\\_file.pdf](https://unba.org.ua/assets/uploads/1259d4263dac852ef056_file.pdf) (дата звернення: 21.10.2023).
14. Чанишев Р.І. Проблеми розвитку та правового регулювання штучного інтелекту: матеріали Міжнар. наук.-практ. конф. *Європейські орієнтири розвитку України в умовах війни та глобальних викликів XXI століття: синергія наукових, освітніх та технологічних рішень*. У 2 т., м. Одеса, 19 трав, 2023 р. / за заг. ред. С.В. Ківалова. Одеса: Видавництво "Юридика", 2023. Т. 1. С. 603-606.
15. Теличко І.О., Теличко О.А., Чабаненко Ю.С. Перспективи використання технологій штучного інтелекту у правовому середовищі: collection of scientific papers "SCIENTIA" with Proceedings of the I International Scientific and Theoretical Conference *The process and dynamics of the scientific path*. Vol 1., м. Афіни, 26 лют. 2021 р. Афіни, 2021. С. 85-87.
16. Охотнікова О.М., Дорош В.С. Штучний інтелект в процесі прийняття та реалізації управлінських рішень в сфері юридичного менеджменту. *Krakowskie Studia Malopolskie*. 2022. Nr. 4 (36). С. 78-93.
17. Спіцина Г.О., Федосенко Н.А. Актуальні питання міжнародно-правового регулювання захисту персональних даних працівників. *Аналітично-порівняльне правознавство*. 2023. № 2. С. 204-208.
18. Глушко Т.В., Камінський В.В. Інноваційний HR-інжиніринг на засадах компетентісного підходу. *Вісник ХНТУ*. 2022. № 2(81). С. 202-208.
19. Chua H.N., Ooi J.S., Herbland A. The effects of different personal data categories on information privacy concern and disclosure. *Computers & Security*. 2021. Vol. 110: 102453. URL: <http://surl.li/mjtyd> (дата звернення: 21.10.2023).