

Світлана ГУЦУ,

кандидат юридичних наук, доцент, професор ХАІ,
професор кафедри права гуманітарно-правового факультету
Національного аерокосмічного університету
«Харківський авіаційний інститут», м. Харків, Україна
ORCID: <https://orcid.org/0000-0003-1373-6079>
e-mail: s.gutsu@khai.edu

Світлана ШИРОКА,

кандидат філософських наук, доцент кафедри філософії
та соціальних наук Національного аерокосмічного університету
«Харківський авіаційний інститут», м. Харків, Україна
ORCID: <https://orcid.org/0000-0327-2790-5902>
e-mail: s.shyroka@khai.edu

DOI: <https://doi.org/10.32620/pls.2025.8.49>

ЦИФРОВИЙ КОНТРОЛЬ І ТРУДОВІ ПРАВА: ЕТИЧНО-ПРАВОВІ РИЗИКИ ТА ВІДПОВІДАЛЬНІСТЬ РОБОТОДАВЦІВ У СЕКТОРАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Анотація. У статті досліджується феномен цифрового контролю у трудових відносинах у контексті цифрової трансформації та зростаючого використання штучного інтелекту в управлінні персоналом, особливо у секторах критичної інфраструктури. Розкрито вплив алгоритмічних HR-систем на безпеку, стійкість і безперервність функціонування критично важливих об'єктів, а також проаналізовано основні ризики цифрової експлуатації: втручання в приватність, порушення автономії працівника, обмеження свободи слова, дискримінація та алгоритмічна упередженість. Висвітлено етичні засади регулювання цифрового нагляду, включно з принципами прозорості, відповідальності та дотримання цифрових прав людини. Проаналізовано недоліки українського законодавства у сфері захисту працівників від надмірного цифрового моніторингу та запропоновано комплексний підхід до правового регулювання застосування ШІ в управлінні персоналом критичної інфраструктури. Сформульовано рекомендації щодо удосконалення законодавства, зокрема впровадження вимог до прозорості, аудиту алгоритмів, недискримінаційності та визначення відповідальності роботодавців. Обґрунтовується, що збалансоване правове регулювання та етичні стандарти є ключем до запобігання цифровій експлуатації та забезпечення гідних умов праці в цифровому середовищі.

Ключові слова: трудові правовідносини, етичні засади дотримання прав працівників, цифрова експлуатація працівників, цифровий моніторинг (контроль) в трудових відносинах, філософія технологій, цифрове суспільство, етика відповідальності, етика комунікації, свобода, цінності.

У сучасних умовах цифрової трансформації питання забезпечення ефективного функціонування, безпеки та стійкості критичної інфраструктури набуває особливої ваги. Одним із ключових факторів її стабільності є належне управління персоналом, яке дедалі частіше здійснюється за допомогою інструментів штучного інтелекту. На глобальному ринку вже налічується понад 250 спеціалізованих AI-рішень, орієнтованих на сферу HR, що застосовуються для оптимізації підбору, оцінювання, розподілу та професійного розвитку працівників, в тому числі і тих, які забезпечують роботу критично важливих систем.

Ці процеси цифровізації кадрового менеджменту мають прямий вплив на рівень захищеності та безперервності функціонування об'єктів критичної інфраструктури, адже алгоритмічні HR-системи стають невід'ємним елементом інфраструктурної стійкості.

Форми цифрового контролю у сфері трудових відносин охоплюють широкий спектр сучасних практик, спрямованих на спостереження за поведінкою, діяльністю та комунікаціями працівників. До найбільш поширених належать: моніторинг комп'ютерної активності (фіксація натискань клавіш, створення скріншотів робочого

столу, аналіз використання програмного забезпечення), контроль електронної пошти та цифрових комунікацій (перевірка вмісту повідомлень та мережевої активності), GPS-відстеження переміщень працівників як під час виконання службових обов'язків, так і поза їх межами, застосування біометричних технологій (сканування обличчя, відбитків пальців, голосова ідентифікація), а також системи відеоспостереження, що дедалі частіше доповнюються алгоритмами штучного інтелекту для аналізу поведінкових моделей.

За результатами дослідження Александра Ертель-Фернандеса (2020), частка великих компаній, які використовують цифрові інструменти для моніторингу працівників, після початку пандемії COVID-19 зросла вдвічі й досягла близько 60 % [1]. Отже, нагляд у робочому середовищі перестав бути поодиноким явищем і поступово перетворюється на системну практику, що суттєво актуалізує питання потенційних порушень прав людини та ризиків цифрової експлуатації у трудових відносинах.

Першою цінністю, яка опиняється під загрозою внаслідок цифрового спостереження, є право на приватність. У традиційному розумінні приватність передбачає існування сфери особистого життя, вільної від втручання третіх осіб. Натомість широке застосування моніторингових технологій дає роботодавцю можливість отримувати доступ до значних обсягів персональних даних – від деталей робочої активності до конфіденційної інформації, що зберігається на службових пристроях. Як справедливо зазначає Хелен Ніссенбаум, проблема полягає не лише у факті розкриття відомостей, а й у порушенні контекстуальних норм, які визначають допустимі умови їх використання [2, с. 231]. Вихід цифрового нагляду за межі виконання трудових функцій створює також підґрунтя для дискримінаційних практик, адже інформація, не пов'язана з якістю виконання роботи, може впливати на оцінювання працівника.

Під загрозою опиняється й автономія працівника – можливість самостійно організовувати власний робочий процес і підтримувати баланс між професійною та приватною сферами. Цифрові механізми контролю провокують ефект постійної доступності, породжують очікування миттєвої реакції на будь-яке службове повідомлення, що фактично формує феномен «цифрового рабства». Саме внаслідок таких ризиків у праві ЄС сформувалася концепція «права на відключення», яке сьогодні законодавчо закріплене у Франції, Іспанії, Словенії та інших державах. Як зазначалося у наших попередніх дослідженнях, воно забезпечує працівникові можливість протистояти розмиванню меж між роботою та особистим життям і захищає автономію людини в умовах цифрової комунікації [3, р. 87].

Вагомими є й наслідки цифрового контролю

для реалізації свободи слова. Розуміння того, що електронна пошта, корпоративні чати або інші види кореспонденції можуть підлягати моніторингу, спричиняє самоцензуру й стримування висловлювань. У робочому середовищі це призводить до появи штучної межі між «формальною» та «неформальною» комунікацією, що суперечить природі людської взаємодії. Подібна ситуація породжує «паноптичний ефект», описаний Мішелем Фуко: влада починає діяти не лише через контроль, а й через внутрішнє самостримування суб'єкта. У практичній площині це означає уникнення критики роботодавця, згорання відкритого обговорення проблем і деформацію корпоративної комунікації. Як підкреслює Юрген Габермас, публічна сфера може існувати лише за умов свободи від зовнішнього й внутрішнього примусу [4, с. 82], а цифровий нагляд ці умови порушує.

Таким чином, цифрове стеження – це багатовимірне явище, яке виходить далеко за рамки управління персоналом і загрожує трьом фундаментальним цінностям: приватності, автономії та свободі слова. Втрата приватності руйнує право на особистий простір; обмеження автономії перетворює працівника на постійно контрольований ресурс; пригнічення свободи слова послаблює комунікаційні основи професійного середовища. Життя під постійним наглядом формує атмосферу недовіри й нав'язує моделі самоконтролю, що зумовлює поступове звуження людської свободи.

Усе це вимагає комплексного філософсько-правового переосмислення цифрового контролю. Правове регулювання має доповнюватися етичними стандартами, щоб цифрові технології не перетворилися на інструмент прихованої влади. У правовій площині ключове значення мають міжнародні стандарти, серед яких — Загальний регламент ЄС про захист даних (GDPR) та національне трудове законодавство, орієнтоване на захист прав працівників у цифровому середовищі. Право встановлює зовнішні межі допустимого, а етика — внутрішні вимоги відповідальної поведінки суб'єктів, що впроваджують системи моніторингу.

Серед етичних засад особливе місце займає принцип прозорості, який забезпечує розуміння працівником того, які саме дані про нього збираються, з якою метою вони використовуються і як обробляються. У свою чергу, принцип відповідальності покладає на роботодавців і розробників технологій обов'язок враховувати можливі наслідки використання алгоритмічних інструментів і запобігати дискримінаційним чи маніпулятивним практикам. Важливим є також концепт цифрових прав людини, який, за Лучано Флоріді, ґрунтується на визнанні людини як «інформаційної істоти», чия гідність нерозривно пов'язана з умовами існування в цифровому середовищі [5, с. 4].

Отже, етичний вимір протидії надмірному цифровому контролю полягає не лише у мінімізації ризиків, а й у формуванні нової культури взаємодії, у межах якої технології сприяють розширенню людської свободи, а не обмежують її. Поєднання правових інструментів із філософсько-етичними підходами створює підґрунтя для ефективного захисту від цифрової експлуатації та утвердження гуманістичних принципів у цифровому трудовому середовищі.

Поширення платформеної зайнятості, алгоритмічного управління та дистанційних технологій контролю формує нові моделі організації праці, що можуть як підвищувати ефективність кадрових процесів, так і породжувати ризики цифрової експлуатації. Особливо небезпечними такі ризики є у сферах, пов'язаних із критичною інфраструктурою, оскільки некоректні алгоритмічні рішення, упередженість даних, непрозорі системи контролю або помилковий добір персоналу здатні прямо впливати на безпеку і стійкість об'єктів. У цьому контексті значущими стають концепції Smart Human Resources 4.0 та Algorithmic Human Resource Management, які базуються на використанні штучного інтелекту та аналітики великих даних для управління персоналом. Вони передбачають прогнозування кадрових потреб, моделювання ризиків людського фактору, персоналізацію навчальних програм і формування більш передбачуваних механізмів ухвалення управлінських рішень. Проте впровадження таких систем у секторах критичної інфраструктури потребує адекватних правових обмежень, адже алгоритми можуть як підвищувати ефективність, так і посилювати вразливості.

Однією з ключових проблем є ризики алгоритмічної упередженості, непрозорості автоматизованих рішень, надмірного цифрового контролю та втручання в приватність працівників. У сфері критичної інфраструктури такі ризики набувають якісно іншого виміру, адже здатні впливати не лише на трудові права, а й на функціональну безпеку об'єктів та їхню операційну стійкість. В цьому контексті треба зазначити, що європейська судова практика вже має певний досвід вирішення трудових конфліктів по справах надмірного використання ІКТ роботодавцями та порушення прав працівників. Так, у 2020 році Верховний суд Іспанії визнав, що кур'єри платформи Glovo не є самозайнятими особами, а фактично перебувають у трудових відносинах із компанією. Суд дійшов висновку, що: діяльність кур'єрів повністю контролювалася алгоритмом платформи (розподіл замовлень, рейтинг, санкції); працівники не могли самостійно визначати умови праці; Glovo фактично здійснювала управління процесом доставки. Тобто відносини мали ознаки трудових, а не цивільно-правовідносин. Ця справа стала судовим підтвердженням того, що алгоритмічне управління може створювати де-факто трудові відносини, навіть за формальної самозайнятості. Після справи Glovo Іспанія

ухвалила Закон № 12/2021 («Ley Riders»), який: зобов'язав цифрові платформи укладати трудові договори з кур'єрами; встановив обов'язок розкривати принципи роботи алгоритмів, що впливають на умови праці; передбачив відповідальність роботодавця за непрозорі алгоритмічні рішення. Це перший у ЄС приклад, коли держава на законодавчому рівні обмежила алгоритмічну експлуатацію праці, визнавши потребу у прозорості та захисті працівників цифрових платформ.[6].

Не менш істотно страждає автономія: людина, змушена бути онлайн навіть поза робочим часом, втрачає можливість відокремлювати професійне від особистого, а її життєвий ритм підпорядковується очікуванням роботодавця, що є неприпустимим. Ця теза знайшла своє відображення в Рішенні Європейського Суду з прав людини (ЄСПЛ) по справі *Bărbulescu v. Romania* (ЄСПЛ, № 61496/08, 2017). Працівник приватної компанії був звільнений після того, як роботодавець прочитав його особисті повідомлення в робочому чаті. Працівник звернувся до ЄСПЛ, стверджуючи, що це порушує статтю 8 Європейської конвенції (право на повагу до приватного життя). Суд визнав, що моніторинг електронних комунікацій без попереднього інформування працівника порушує його право на приватність. Ця справа встановила європейський стандарт пропорційності цифрового контролю на роботі та стала ключовою у формуванні концепції «цифрової автономії працівника».[7]

У національному контексті Україна поки що не має достатньо розвиненого правового регулювання алгоритмізованих кадрових практик, зокрема в секторах критичної інфраструктури. Закон України «Про критичну інфраструктуру»[8] визначає загальні вимоги до її захисту, але не охоплює питання цифрового управління персоналом. Трудове законодавство не враховує специфіку цифрового моніторингу, а законодавство про захист персональних даних потребує модернізації відповідно до європейських підходів, включаючи GDPR [9] та новий AI Act ЄС [10], який прямо регулює використання високоризикових AI-систем, у тому числі HR-рішень.

У світлі цих викликів важливим є формування комплексного правового підходу до регулювання використання ШІ у сфері управління персоналом критичної інфраструктури. До таких заходів можна віднести запровадження вимог до прозорості алгоритмів, створення механізмів незалежного аудиту автоматизованих рішень, забезпечення права працівників на оскарження рішень, ухвалених алгоритмами, встановлення стандартів недискримінаційності та заборони надмірного цифрового контролю. Не менш важливим є визначення юридичної відповідальності роботодавців за порушення трудових прав, що виникають унаслідок застосування алгоритмічних систем.

Упровадження таких правових гарантій дозволить зменшити ризики цифрової експлуатації, підвищити рівень довіри до алгоритмічних рішень та забезпечити баланс між інноваціями й безпекою. Гарантований правовий контроль над використанням ШІ у кадрових процесах сприятиме не лише захисту працівників, а й зміцненню стійкості та безперервності роботи критичної інфраструктури, що має принципове значення для національної безпеки, економічної стабільності та захисту суспільних інтересів.

Бібліографічні посилання

1. Hertel-Fernandez, Estimating the prevalence of automated management and surveillance technologies at work and their impact on workers' well-being (2023). <https://equitablegrowth.org/research-paper/estimating-the-prevalence-of-automated-management-and-surveillance-technologies-at-work-and-their-impact-on-workers-well-being/>
2. Н. Nissenbaum, Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford University Press (2010).
3. S. Gutsu, S. Shyroka, "The Right to Disconnect as an Implementation of the Employee's Constitutional Right to Rest: A Philosophical and Legal Approach." In Integrated Computer Technologies in Mechanical Engineering (2024), pp. 87–99. URL: https://doi.org/10.1007/978-3-031-94852-7_8
4. J. Habermas, The Structural Transformation of the Public Sphere. Polity Press (1989).
5. L. Floridi, The Ethics of Information. Oxford University Press (2013). URL: <https://doi.org/10.1093/acprof:oso/9780199641321.001.0001>
6. Manuel V. Gómez. Spanish Supreme Court rules food-delivery riders are employees, not self-employed. SEP 24, 2020. URL: https://english.elpais.com/economy_and_business/2020-09-24/spanish-supreme-court-rules-food-delivery-riders-are-employees.html?ref=hvper.com
7. The European Court of Human Rights ,CASE OF BĂRBULESCU v. ROMANIA № 61496/08, 2017. URL: <https://hudoc.echr.coe.int/fre#%7B%22itemid%22:%5B%22001-177082%22%5D%7D>
8. Про критичну інфраструктуру: Закон України. Відомості Верховної Ради (ВВР), 2023, № 5, ст.13. URL: <https://zakon.rada.gov.ua/laws/show/1882-20#Text>
9. Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних,

та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних). URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text.

10. Artificial Intelligence Act, Official Journal version of 13 June 2024. URL: <https://artificialintelligenceact.eu/ai-act-explorer/>

S. Gutsu, S. Shyroka

Digital surveillance and labour rights: ethical-legal risks and employer responsibility in critical infrastructure sectors.

Abstract. The article examines the phenomenon of digital control in labor relations in the context of digital transformation and the growing use of artificial intelligence in personnel management, particularly in critical infrastructure sectors. It reveals the impact of algorithmic HR systems on the security, resilience, and continuity of critically important infrastructure, and analyzes the key risks of digital exploitation, including privacy intrusions, violations of employee autonomy, restrictions on freedom of expression, discrimination, and algorithmic bias. The study highlights the ethical foundations of regulating digital surveillance, including the principles of transparency, accountability, and the protection of digital human rights. It also analyzes the shortcomings of Ukrainian legislation in protecting employees from excessive digital monitoring and proposes a comprehensive approach to regulating the use of AI in personnel management within critical infrastructure. The article formulates recommendations for improving legislation, such as implementing transparency requirements, algorithmic audits, non-discrimination standards, and clear employer liability. It argues that balanced legal regulation combined with ethical standards is essential for preventing digital exploitation and ensuring decent working conditions in the digital environment.

Keywords: labour relations, ethical principles of workers' rights protection, digital exploitation of employees, digital monitoring (control) in labour relations, philosophy of technology, digital society, ethics of responsibility, communication ethics, freedom, values.

Зразок для цитування:

Гуцу С., Широка С. Цифровий контроль і трудові права: етично-правові ризики та відповідальність роботодавців у секторах критичної інфраструктури. Пропілеї права та безпеки, 2025. №8. С. 199-202. DOI: <https://doi.org/10.32620/pls.2025.8.49>.