ФП 2025-4
ISSN 1995-6134

УДК *347.51:004.8(4-6)*
DOI: http://doi.org/10.5281/zenodo.18338303

О.Р. ШИШКА,
професор кафедри цивільного, трудового та господарського права ННІ № 1 Харківського національного університету внутрішніх справ, кандидат юридичних наук, професор, м. Харків, Україна; e-mail: shyshkaor@gmail.com;
ORCID: https://orcid.org/0000-0002-1396-0508

Н.В. ШИШКА,
доцент кафедри цивільного, трудового та господарського права ННІ № 1 Харківського національного університету внутрішніх справ, кандидат юридичних наук, доцент, м. Харків, Україна; e-mail: natali.wiwa@gmail.com;
ORCID: https://orcid.org/0000-0002-3396-4530

ВІДПОВІДАЛЬНІСТЬ ЗА ШКОДУ, ЗАПОДІЯНУ ВИКОРИСТАННЯМ СИСТЕМ ТА ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ: СУДОВА ПРАКТИКА В ЄС

O.R. SHYSHKA,
Professor, Department of Civil, Labor and Commercial Law, Kharkiv National University of Internal Affairs, Ph.D. (Law), Professor, Kharkiv, Ukraine; e-mail: shyshkaor@gmail.com;
ORCID: https://orcid.org/0000-0002-1396-0508

N.V. SHYSHKA,
Associate Professor, Department of Civil, Labor and Commercial Law, Kharkiv National University of Internal Affairs, Ph.D. (Law), Ass. Professor, Kharkiv, Ukraine; e-mail: natali.wiwa@gmail.com;
ORCID: https://orcid.org/0000-0002-3396-4530

LIABILITY FOR DAMAGE CAUSED BY THE USE OF AI SYSTEMS AND TECHNOLOGIES: CASE LAW IN THE EU

АНОТАЦІЇ (ABSTRACTS), КЛЮЧОВІ СЛОВА (KEYWORDS)

Постановка проблеми. Стрімкий розвиток систем та технологій штучного інтелекту (ШІ) та їх широке застосування в різних сферах суспільного життя супроводжується зростанням випадків заподіяння шкоди суб'єктам цивільних прав (аварії, дискримінація, порушення приватності, поширення фейкового контенту тощо). Це актуалізує проблему визначення суб'єкта цивільно-правової відповідальності за шкоду, спричинену ШІ. Попри обговорення в науковій доктрині ідеї надання ШІ статусу "електронної особи", сучасна судова практика ЄС послідовно її відкидає. Водночас традиційні деліктні механізми виявляються недостатньо пристосованими до автономності та непрозорості ШІ, що призводить до "прогалини у відповідальності". У контексті європейської інтеграції України та необхідності адаптації національного законодавства до ризиків ШІ набуває актуальності аналіз судової практики ЄС як основи для формування спеціального правового регулювання. **Метою** роботи є комплексний аналіз прецедентів судової практики ЄС щодо відповідальності за шкоду, спричинену використанням систем та технологій ШІ. **Методи.** У дослідженні застосовано формально-юридичний метод для характеристики норм та підходів судів ЄС; порівняльно-правовий – для зіставлення прецедентів у різних сферах (транспорт, державне управління, гіг-економіка, фінанси, медіа); системний – для виявлення спільних тенденцій та прогалини у відповідальності; догматичний – для оцінки застосування традиційних норм (деліктне право, GDPR, ЄКПЛ) до ШІ-казусів. **Результати.** Аналіз ключових прецедентів (справи Tesla, SyRI, Deliveroo, Uber/Ola, SCHUFA, фейкове інтерв'ю Міхаеля Шумахера) показав, що суди ЄС не визнають ШІ суб'єктом права. Відповідальність завжди покладається на осіб, які створюють, експлуатують чи використовують ШІ. При цьому, виявлено, що концепція "електронної особи" не застосовується. З'ясовано, що через складність доведення вини, причинно-наслідкового зв'язку та передбачуваності шкоди в традиційному деліктному праві позивачі частіше використовують механізми захисту персональних даних та антидискримінаційне законодавство, які виявляються ефективнішими в умовах непрозорості та автономності ШІ. **Висновки.** Судова практика ЄС підтверджує, що ШІ залишається інструментом у руках людини, а відповідальність завжди людська (фізичних чи юридичних осіб), виключаючи самостійну правосуб'єктність технологій. Прогалина у відповідальності має системний характер і не усувається розширеним тлумаченням традиційних норм. Альтернативні механізми забезпечують переважно превентив-

Published on 15.12.2025
DOI: http://doi.org/10.5281/zenodo.18338303
© Шишка О.Р., Шишка Н.В., 2025
Open access, licensed under CC BY 4.0

ISSN 1995-6134

ний захист, але недостатньо відновлюють права потерпілих. Для ефективного та дієвого регулювання необхідний спеціальний правовий режим, який враховує автономність, непрозорість і багатосуб'єктний характер правовідносин щодо сучасних алгоритмічних систем. Для України це сигнал про потребу адаптації цивільного законодавства та впровадження сучасних стандартів цивільно-правової відповідальності в ЄС.

Ключові слова: *цивільне право; цивільні правовідносини; майно; штучний інтелект; судова практика; GDPR; AI Act; автономний транспорт; генеративний ШІ; безпілотні транспортні засоби; відповідальність; цивільно-правова відповідальність; цивільні спори; правове регулювання; правовий режим; електронна особа; захист персональних даних; міжнародний досвід; ЄС*

***

Problem statement. The rapid development of artificial intelligence (AI) systems and technologies and their widespread use across various spheres of social life are accompanied by a growing number of cases in which AI causes harm to subjects of civil rights (accidents, discrimination, violations of privacy, dissemination of fake content, etc.). This actualizes the problem of determining the subject of civil liability for damage caused by AI. Despite discussions in academic doctrine regarding the idea of granting AI the status of an "electronic person," contemporary EU case law consistently rejects this concept. At the same time, traditional tort law mechanisms prove insufficiently adapted to the autonomy and opacity of AI, resulting in a persistent "liability gap." In the context of Ukraine's European integration and the need to adapt national legislation to AI-related risks, the analysis of EU judicial practice becomes particularly relevant as a basis for shaping special legal regulation. The **purpose** of this study is to provide a comprehensive analysis of EU judicial precedents concerning liability for damage caused by the use of AI systems and technologies. **Methods.** The research employs the formal legal method to characterize EU legal norms and judicial approaches; the comparative legal method to compare precedents across different fields (transport, public administration, gig economy, finance, media); the systemic method to identify common trends and the existence of a liability gap; and the doctrinal method to assess the application of traditional legal norms (tort law, GDPR, ECHR) to AI-related cases. **Results.** An analysis of key precedents (the Tesla, SyRI, Deliveroo, Uber/Ola, SCHUFA cases, and the fake interview of Michael Schumacher) demonstrates that EU courts do not recognize AI as a subject of law. Liability is always imposed on the persons who develop, operate, or use AI systems. The study confirms that the concept of an "electronic person" is not applied in judicial practice. It is established that due to the difficulty of proving fault, causation, and foreseeability of harm within traditional tort law, claimants more frequently rely on personal data protection mechanisms and anti-discrimination legislation, which prove more effective under conditions of AI opacity and autonomy. **Conclusions.** EU judicial practice confirms that AI remains a tool in human hands, and liability is always human (borne by natural or legal persons), excluding the independent legal personality of technologies. The liability gap is systemic in nature and cannot be eliminated through an extensive interpretation of traditional legal norms. Alternative mechanisms primarily provide preventive protection but do not sufficiently restore the rights of injured parties. Effective regulation therefore requires a special legal regime that takes into account the autonomy, opacity, and multi-actor nature of legal relations involving modern algorithmic systems. For Ukraine, this serves as a signal of the need to adapt civil legislation and implement modern EU standards of civil liability.

Keywords: *civil law; civil legal relations; property; artificial intelligence; judicial practice; GDPR; AI Act; autonomous transport; generative AI; unmanned vehicles; liability; civil liability; civil disputes; legal regulation; legal regime; electronic person; personal data protection; international experience; EU*

Постановка проблеми

Стрімкий розвиток систем та технологій штучного інтелекту (ШІ) охоплює практично всі сфери життя – від автономного транспорту до прийняття рішень у соціальній чи судовій сфері, працевлаштуванні, фінансах тощо. Цей технологічний прогрес не лише відкриває нові можливості, але й призводить до зростання кількості інцидентів, коли використання систем та технологій ШІ спричиняє шкоду. Прикладами таких інцидентів є дорожні аварії за участі автономного транспорту, дискримінаційні рішення алгоритмів, порушення права на приватність чи розповсюдження хибної інформації генеративними моделями.

Ця ситуація ставить перед правовою наукою та практиками нагальну проблему юридичної відповідальності за наявну шкоду. Ключове питання, яке стоїть перед законотворцями та судами, полягає у визначенні суб'єкта, який має відповідати: розробник алгоритму, користувач, особа, якій належить системи та/або технологія ШІ, інший учасник, а можливо, й сама система ШІ? Це питання постає особливо нагально перед законотворцями, науковцями та практиками (судами, адвокатами й страховими компаніями).

З наукового погляду проблема пов'язана з дискусією про правосуб'єктність ШІ набуває окремого обговорення. Так, у науковій літературі [1–4] та окремих політичних ініціативах (зокрема в резолюції Європейського Парламенту [5]) ви-

ISSN 1995-6134

словлювалася пропозиція щодо надання автономним системам спеціального правового статусу – так званої "електронної особи", що дозволило б у правовому полі покладати на них самостійну відповідальність. Проте у сучасній юридичній практиці ЄС ШІ не визнаний суб'єктом права – відповідальність покладається на фізичних і юридичних осіб, що створюють та використовують такі системи.

Традиційні національні режими деліктного права, що засновуються на необхідності доведення вини (у цивільному, кримінальному чи адміністративному праві), виявилися недостатньо адаптованими до нових реалій, спричинених автономними, непрозорими та самонавчальними системами та технологіями ШІ. Це створює так звану "правову прогалину у відповідальності" (liability gap) – ситуацію, коли потерпіла сторона фактично не має ефективних правових механізмів для захисту своїх прав та інтересів через неможливість чітко визначити, хто несе відповідальність за наявну шкоду, спричинену ШІ. Наприклад, якщо автономний автомобіль на базі ШІ спричиняє аварію, неясно, кого притягати до відповідальності: розробника алгоритму, виробника системи, власника чи, можливо, саму систему ШІ, яка діяла самостійно. Ця прогалина виникає через унікальні характеристики ШІ: автономність (здатність приймати рішення без прямого та постійного контролю людини), непрозорість (складність пояснення логіки рішень, подібно до "чорної скриньки") та самонавчання (еволюція системи, коли її поведінка може відхилятися від початкового задуму розробників). Додатково прогалину посилює проблема багатьох рук – ланцюгова участь численних суб'єктів (розробники, постачальники даних, інтегратори, оператори тощо), через що відповідальність розмивається і кожен учасник може перекладати вину на іншого. У результаті потерпілий часто не може ефективно довести ні вину конкретного суб'єкта, ні причинно-наслідковий зв'язок між функціонуванням системи ШІ та шкодою, ні передбачуваність такої шкоди в традиційному розумінні деліктного права.

Практичний аспект проблеми полягає в тому, що суди змушені застосовувати традиційні норми деліктного, трудового чи іншого законодавства до принципово нових ситуацій, які не передбачалися під час їх створення. Наприклад, у справах, де ШІ є безпосереднім джерелом виникнення шкоди, суди намагаються адаптувати правила про відповідальність за дефектні продукти чи норми трудового права, якщо ШІ використовується в робочому процесі. Однак такі адаптації часто є вимушеними і не завжди ефективними, оскільки традиційні норми не враховують специфіки систем та технологій ШІ. Це призводить до правової невизначеності, коли потерпілі можуть залишатися без належного захисту чи справедливої компенсації.

Тому, актуальність проблеми полягає в необхідності комплексного аналізу наявних кейсів судових справ у ЄС, аби зрозуміти, які підходи формуються, які правові інструменти (GDPR, ЄКПЛ, національне законодавство про дефекти) виявляються найбільш ефективними для захисту прав потерпілих, та які тенденції судової адаптації можуть стати основою для подальшого регулювання.

Таким чином, *об'єктом дослідження* є прецеденти, в яких суди ЄС вирішували питання відповідальності за шкоду або порушення прав, пов'язані з використанням систем та технологій ШІ, тоді як *предметом дослідження* є підходи судів та правовий контекст застосування традиційних норм права до нових технологічних казусів. *Метою* роботи є комплексний аналіз прецедентів судової практики ЄС щодо відповідальності за шкоду, спричинену використанням систем та технологій ШІ. Її *новизна* полягає в систематизації судової практики ЄС щодо цивільно-правової відповідальності за шкоду, спричинену використанням систем штучного інтелекту, та доведенні послідовної відмови судів від визнання ШІ суб'єктом права; виявленні сьогоднішньої неефективності традиційних деліктних механізмів у ШІ-казусах і обґрунтованості потреби спеціального правового режиму відповідальності, що враховує автономність, непрозорість і багатосуб'єктний характер алгоритмічних систем. *Завданнями* статті є аналіз підходів судів ЄС до покладення цивільно-правової відповідальності за шкоду, спричинену використанням систем штучного інтелекту, а також оцінка адекватності традиційних і альтернативних механізмів правового захисту та визначення напрямів адаптації цивільного законодавства України до стандартів ЄС.

Судова практика ЄС

На сьогодні в країнах Європейського Союзу накопичено вже певний масив судових справ, де предметом спору є шкода або порушення прав, пов'язані з використанням систем та технологій ШІ. Розглянемо ключові прецеденти в різних сферах, аби проаналізувати підходи судів, позиції сторін та правовий контекст.

ISSN 1995-6134

Відповідальність у сфері автономного транспорту: між захистом прав споживачів і відповідальністю за дефектний товар

Автономний транспорт *(справа Tesla в Німеччині).* Одним із перших резонансних прикладів правового реагування на використання технологій автономного керування транспортними засобами стала судова справа, розглянута в Німеччині у 2020 році за позовом Центрального управління боротьби з недобросовісною конкуренцією (Wettbewerbszentrale) проти компанії Tesla. Мюнхенський регіональний суд дійшов висновку про оманливий характер маркетингових тверджень компанії, визнавши, що використання термінів "Autopilot" та "Full Self-Driving" формує у споживачів хибне уявлення про здатність автомобіля здійснювати повністю автономне керування. Такі твердження не відповідали ані чинному німецькому законодавству, яке на той момент не допускало повністю автономного руху транспортних засобів, ані фактичному рівню розвитку відповідних технологій. Фактично, за своїми функціональними характеристиками зазначені системи відповідали лише другому рівню автоматизації відповідно до міжнародної класифікації**,** що передбачає часткову автоматизацію та покладає на водія обов'язок постійного контролю за процесом керування і готовність негайно втрутитися. У подальшому Tesla оскаржила первинне судове рішення, і суд вищої інстанції скасував заборону на використання зазначених термінів. Водночас компанію було зобов'язано забезпечити належне інформування споживачів щодо реальних можливостей і обмежень систем Autopilot і Full Self-Driving на офіційному вебсайті [6; 7]. Таким чином, справа була вирішена в межах механізмів захисту прав споживачів, поєднавши збереження права на використання торговельних найменувань із вимогою підвищеної прозорості щодо ролі алгоритмів штучного інтелекту та незамінності участі людини в процесі керування транспортним засобом [8].

Ця справа Tesla в Німеччині є важливим прикладом того, як суди ЄС адаптують традиційні правові норми до нових викликів, пов'язаних із використанням ШІ у сфері автономного транспорту. Правова логіка рішень Мюнхенського регіонального суду та Вищого регіонального суду ґрунтувалася насамперед на захисті прав споживачів через забезпечення належного рівня інформаційної прозорості. Замість встановлення відповідальності у класичному деліктному розумінні суди зосередили увагу на оцінці маркетингових тверджень компанії Tesla щодо реальних можливостей систем Autopilot і Full Self-Driving та їх відповідності технічному рівню розвитку технологій і чинному правовому регулюванню. Зазначений підхід відображає характерну для ЄС тенденцію до превентивного регулювання відносин у сфері застосування ШІ, за якої акцент робиться не лише на реагуванні на вже заподіяну шкоду, а передусім на вимогах прозорості, правдивості та недопущення введення споживачів в оману на етапі комунікації про функціональні можливості технологій. Таким чином, справа щодо маркетингу Tesla в Німеччині може розглядатися як один із ранніх прикладів формування судової практики, у межах якої суди ЄС використовують наявні інструменти захисту прав споживачів для встановлення ex ante (превентивних) обов'язків виробників автономного транспорту щодо належного інформування про роль штучного інтелекту та незамінність участі людини в процесі керування.

Інший аспект відповідальності проявився у *справі про технічну несправність автопілоту Tesla Model X.* У липні 2022 року Мюнхенський регіональний суд постановив, що автопілот Tesla Model X неналежно функціонує в певних умовах і становить значну небезпеку, зобов'язавши виробника відшкодувати власниці 99 416 євро, що становить більшу частину вартості автомобіля (112 640 євро). Згідно з технічним звітом, автомобіль не завжди розпізнавав перешкоди, наприклад, звуження на ділянках ремонту дороги, і мав проблему "фантомного гальмування", що створювало ризик аварій у міських умовах. Суд підкреслив, що таке непередбачуване гальмування становить "масову небезпеку" для безпеки дорожнього руху. Адвокати Tesla заперечували, заявляючи, що автопілот не призначений для міського руху, але суд відхилив цей аргумент, зазначивши, що вимагати від водія постійно вмикати та вимикати автопілот залежно від умов дороги непрактично, оскільки це відволікає увагу і може спричинити аварію. У результаті суд визнав програмне забезпечення дефектним за нормами німецького законодавства про відповідальність продавця за товари неналежної якості, змусивши Tesla повернути кошти покупцю [9; 10].

Цей прецедент важливий тим, що суд фактично розцінив алгоритм автопілоту як складову частину товару (автомобіля), яка повинна відповідати стандартам безпеки. Недосконалість ШІ-системи була поставлена в один ряд із механічним дефектом товару. Тут відповідальність

ISSN 1995-6134

поніс виробник автомобіля (Tesla), навіть попри те, що сам алгоритм міг бути розроблений окремо – кінцевий товар продається виробником, і саме він відповідає за безпечність комплексу "залізо + програма". Це узгоджується з логікою про відповідальність виробника за дефектний товар. Автомобіль з автономними функціями є товаром, і виробник несе обов'язок перед споживачем щодо відсутності небезпечних дефектів.

Алгоритмічні системи держави та межі допустимого втручання: справа SyRI

Державні алгоритмічні системи (справа SyRI у Нідерландах). Прецедентом загальноєвропейського значення стала справа щодо системи SyRI (System Risk Indication) в Нідерландах. SyRI – це державна алгоритмічна система, розроблена для виявлення шахрайства у сфері соцзабезпечення та податків, яка шляхом обробки великих масивів даних повинна була виявляти громадян з високим ризиком порушень. Уряд впроваджував її для боротьби з зловживаннями соціальними виплатами, зокрема в бідних районах. Однак коаліція правозахисних організацій та профспілок оскаржила законність SyRI, стверджуючи, що вона порушує право на приватність і принцип недискримінації. Позивачі вказували, що система збирає і аналізує персональні дані надмірно та непрозоро, ставлячи під підозру цілий прошарок населення (мешканців бідних районів) без достатніх на то підстав [11].

У лютому 2020 року Окружний суд Гааги виніс історичне рішення, визнавши, що використання системи SyRI (System Risk Indication) порушує статтю 8 Європейської конвенції з прав людини (право на приватне життя) через недостатні гарантії проти свавільного втручання в приватність. Суд встановив, що законодавча база SyRI, зокрема стаття 65 Закону про структуру даних і глава 5a Указу SUWI, є недостатньо ясною і перевірюваною, а алгоритм працює непрозоро, створюючи ризик непрямої дискримінації за соціально-економічною та етнічною ознаками [12]. Особливо критично відзначено "серйозну відсутність прозорості": уряд не розкрив ризик-модель і критерії, за якими алгоритм визначав громадян як ризикових, що унеможливило перевірку його об'єктивності. Це створювало ризик непрямої дискримінації за соціально-економічною чи етнічною ознаками, оскільки мешканці бідних районів могли бути стигматизовані алгоритмом без достатніх підстав. Суд також врахував принципи захисту даних GDPR і Хартії ЄС, зазначивши, що SyRI не відповідає вимозі "справедливого балансу" між суспільною метою боротьби з шахрайством і правами людини, оскільки збирала значні обсяги даних без належного інформування громадян. Судді підкреслили, що відсутність прозорості може мати "охолоджувальний ефект" (chilling effect) для суспільства, змушуючи людей боятися цифрової обробки їхніх даних. Відповідно, положення, які регулювали функціонування SyRI, було визнано несумісними зі статтею 8 ЄКПЛ, а використання системи припинено [11; 12].

Ця справа стала одним із перших випадків у світі, коли суд зупинив використання державної ШІ-технології на підставі прав людини. Рішення підтвердило, що навіть легітимна мета боротьби з шахрайством не виправдовує використання "непрозорих скриньок" (black box systems), які загрожують приватності. Справа SyRI стала потужним сигналом для інших країн, зокрема Великобританії та Австралії, про необхідність суворого нагляду за впровадженням автоматизованих систем у соціальній сфері.

Алгоритмічне управління працею та захист прав працівників у гіг-економіці

ШІ у трудових відносинах *(справи Deliveroo, Uber, Ola).* Сфера гіг-економіки та платформ праці стала полігоном для конфліктів, пов'язаних з алгоритмічним управлінням працівниками. В ЄС сформувалася низка прецедентів, де кур'єри та водії оскаржували рішення, які прийняті за допомогою ШІ-систем через їхню непрозорість та дискримінаційний характер.

Однією з перших перемог працівників над алгоритмом стало рішення Суду Болоньї (Італія) у справі Deliveroo (грудень 2020 року). Deliveroo застосовувала алгоритмічну систему "Frank" для управління роботою кур'єрів, зокрема для розрахунку рейтингу та пріоритетного надання слотів (робочих змін/інтервалів) залежно від індексу надійності та участі у пікові години. Італійська загальна конфедерація праці (CGIL) разом з іншими профспілками (зокрема FILCAMS, NIDIL та FILT CGIL) оскаржила використання алгоритмічної системи оцінювання праці кур'єрів, стверджуючи, що вона є "сліпою" до законних причин відсутності на роботі (зокрема хвороби чи участі у страйку, які охороняються трудовим законодавством), через що несправедливо знижувала рейтинг працівників. Суд визнав це непрямою дискримінацією, зобов'язав компанію виплатити €50 000 компенсації та оприлюднити рішення на своєму сайті, а також модифікувати алгоритм, щоб виключити подібну дискримінa-

ISSN 1995-6134

цію [13–15].

Це рішення було названо "епохальним поворотним моментом" [16] для захисту прав працівників у сфері гіг-економіки та платформ праці. Воно вплинуло на низку подальших позовів проти інших платформ (наприклад, Glovo, Uber Eats) та посилило регуляторні дискусії в ЄС, підкресливши необхідність забезпечення прозорості, підзвітності та людського нагляду за алгоритмічним управлінням. Хоча на 2026 рік система "Frank" уже не застосовується в Італії (тобто замінена на інші моделі управління), прецедент залишається ключовим для розуміння ризиків непрозорих алгоритмів, які можуть призводити до непрямої дискримінації та прогалин щодо відповідальності відповідних суб'єктів у контексті автономних систем.

Інший напрямок боротьби – позови водіїв таксі та кур'єрів проти автоматизованих рішень платформ на кшталт Uber та Ola (індійська платформа, що мала присутність у Європі). Ключові справи розглянув Окружний суд Амстердама (Нідерланди) у березні 2021 року. Група водіїв Uber та Ola, за підтримки профспілки App Drivers & Couriers Union (ADCU) і Worker Info Exchange, подала позови, звинувачуючи компанії в "робо-звільненнях" (автоматизованій деактивації акаунтів через підозру в "фродовій активності" в Uber) та непрозорих штрафах (на основі "fraud probability score" в Ola) без належного людського контролю. Це, на думку позивачів, порушувало національні трудові норми, а також статтю 22 GDPR, яка забороняє рішення, засновані виключно на автоматизованій обробці (включаючи профілювання), якщо вони мають юридичні або аналогічно значущі наслідки для особи, та пов'язане з цим право на пояснення логіки таких рішень відповідно до статей 13–15 GDPR [17].

Рішення суду вийшло неоднозначним. Щодо Uber, суд не знайшов достатніх доказів, що звільнення водіїв або розподіл замовлень здійснювалися цілком автоматично без "значимого людського втручання". Суд визнав, що деактивація акаунтів передбачала людське втручання (EMEA Operational Risk team), а диспетчерська система не створює значущого юридичного ефекту для водіїв за статтею 22 GDPR. Вимоги водіїв про незаконність автоматизованих звільнень відхилили, але суд зобов'язав Uber надати водіям більше персональних даних про них, яких компанія раніше не розкривала. Зокрема, Uber повинна була поділитися з позивачами їхніми індивідуальними рейтингами, виставленими пасажирами, і деякими логами, визнавши, що запит цих даних є обґрунтованим [17]. Це частково посилило прозорість відносин. Водії отримали можливість дізнатися, як їх оцінює алгоритм (через оцінки клієнтів), хоча повного доступу до всіх алгоритмічних даних суд не надав, посилаючись на комерційну таємницю й захист персональних даних пасажирів.

Однак у подальшому ситуація суттєво змінилася після апеляційного розгляду. 4 квітня 2023 року Апеляційний суд Амстердама виніс рішення, яке значною мірою задовольнило вимоги водіїв, визнавши порушення положень GDPR з боку Uber та Ola Cabs. Зокрема, суд переглянув поняття "людського втручання" і відхилив аргумент Uber про те, що участь двох співробітників (зокрема команди з операційних ризиків EMEA) була достатньо значущою. Навпаки, суд визнав, що дії персоналу мали характер чисто символічного акту, а водіям не надавали реальної можливості висловити свою позицію перед деактивацією акаунтів. Крім того, компанія не довела, що відповідні працівники мали належну кваліфікацію та рівень знань для критичної, незалежної та контекстуальної оцінки алгоритмічно згенерованих сигналів можливого шахрайства, з урахуванням усіх релевантних даних та пояснень водіїв, як того вимагають керівні принципи EDPB [18].

Крім того, апеляційний суд дійшов висновку, що рішення про деактивацію акаунтів водіїв Uber мали для них істотні правові та економічні наслідки, оскільки призводили до припинення договірних відносин та втрати основного джерела доходу. За відсутності доведеного змістовного людського втручання такі рішення були кваліфіковані судом як виключно автоматизовані у розумінні статті 22 GDPR, що, своєю чергою, надає водіям право на отримання інформації відповідно до статті 15(1)(h) GDPR. У зв'язку з цим суд зобов'язав Uber надати водіям корисну та достатню інформацію про наявність автоматизованого прийняття рішень, зокрема щодо факторів, які враховувалися при деактивації акаунтів, та їх відносної ваги на агрегованому рівні, незважаючи на посилання компанії на комерційну таємницю. Така інформація, навіть якщо вона міститься у внутрішніх системах компанії, судом була визнана персональними даними, якщо вона стосується ідентифікованого водія та використовується для прийняття рішень, що істотно впливають на його правове або економічне становище [18].

Особливо важливим у цьому рішенні є підхід

ISSN 1995-6134

суду до співвідношення прозорості та захисту комерційної таємниці. Апеляційний суд дійшов висновку, що Uber не вправі повністю відмовляти водіям у наданні інформації про автоматизоване прийняття рішень, посилаючись на секретність алгоритмів або необхідність захисту своїх внутрішніх процесів, якщо така відмова позбавляє їх можливості зрозуміти причини рішень, які істотно впливають на їхнє правове та економічне становище, зокрема призводять до деактивації акаунтів і втрати доходу. Суд підкреслив, що інтереси компанії у збереженні комерційної таємниці не можуть виправдовувати повну відмову у запитах водіїв на на отримання корисної та зрозумілої інформації, необхідної для реалізації прав, гарантованих статтями 15 і 22 GDPR, з урахуванням принципів необхідності та пропорційності.

Таким чином, апеляційне рішення встановило важливий прецедент: платформи повинні забезпечувати реальну прозорість своїх алгоритмів, а формальна наявність людини в процесі ухвалення рішення (human-in-the-loop) не звільняє від відповідальності за автоматизовані рішення, якщо такий контроль є лише символічним і не дає можливості ефективного оскарження. Також, зазначений підхід узгоджується з подальшою практикою у сфері захисту персональних даних, зокрема з рішеннями національних органів нагляду ЄС, які наголошують на обов'язку платформ забезпечувати реальну, а не формальну прозорість алгоритмічного управління [19].

Судова практика ЄС у справах Deliveroo та Uber/Ola демонструє, що позивачі та їх представники (профспілки, водії тощо) свідомо не використовують традиційні режими цивільно-правової відповідальності, бо розуміють їхню низьку ефективність у контексті автономних і непрозорих алгоритмічних систем. Замість вимог про компенсацію шкоди в класичному розумінні (відшкодування втраченого доходу, моральної шкоди тощо) вони обирають інші правові механізми притягнення до відповідальності – насамперед норми про непряму дискримінацію та захист персональних даних. Саме ці інструменти дозволяють змусити платформи усунути порушення, забезпечити прозорість і накласти санкції, навіть якщо повне відновлення шкоди не відбувається. При цьому, такий вибір позивачів чітко показує, що в правовій системі ЄС існує так звана прогалина у відповідальності (англ. liability gap) – ситуація, коли потерпілий фактично не має ефективного механізму отримати відшкодування шкоди через неможливість застосувати традиційні механізми деліктного права. Прогалина виникає через ключові властивості ШІ-систем: автономність, непрозорість та самонавчання. У результаті неможливо довести: вину конкретного суб'єкта (розробник, платформа чи оператор?); прямий причинно-наслідковий зв'язок; передбачуваність шкоди для потенційно відповідальної особи. Класичне деліктне право вимагає саме цих елементів, тому позови про компенсацію шкоди майже не подаються. Натомість обрані механізми (антидискримінація + захист персональних даних) дозволяють досягти системних змін і санкцій, але не забезпечують повного відшкодування заподіяної шкоди потерпілому. Це робить прогалину у відповідальності стійкою проблемою, яка потребує спеціального регулювання не лише на рівні ЄС, але і в Україні.

Фінансовий скоринг і автоматизовані рішення: прецедент SCHUFA

Фінансові рішення та скоринг *(справа SCHUFA (Німеччина))*. Фінансовий сектор також зіткнувся з проблемою відповідальності за рішення, прийняті за допомогою ШІ, зокрема кредитними скоринговими системами. Яскравим прикладом є справа щодо німецького бюро кредитних історій SCHUFA. SCHUFA використовувала автоматизовані алгоритми для визначення кредитного рейтингу громадян, і цей показник впливав на рішення банків про видачу кредиту.

Так, у 2023 році Суд Європейського Союзу виніс ключове рішення (7 грудня 2023 р., справа C-634/21 SCHUFA Holding (Scoring)), об'єднане з іншими справами щодо зберігання даних. Ключовим тут було питання: чи підпадає кредитний скоринг під заборону суто автоматизованих рішень за статтею 22 GDPR? Зокрема, SCHUFA стверджувала, що вона лише надає інформацію своїм партнерам, які й приймають остаточні контрактні рішення (видавати кредит чи ні), тому стаття 22 GDPR не повинна застосовуватися до її діяльності. Однак Суд ЄС постановив, що в ситуаціях, коли банк сильно покладається на отриманий бал, а низький показник ймовірності майже у всіх випадках призводить до відмови у кредиті, встановлення такого значення саме по собі має кваліфікуватися як рішення, що створює юридичні наслідки або істотно впливає на особу. Суд також підкреслив, що обмежувальне тлумачення цієї норми створило б ризик обходу ст.22 GDPR та призвело б до прогалини у механізмі правового захисту,

ISSN 1995-6134

оскільки банк спирався б на висновки алгоритму без доступу до пояснення його логіки, а бюро кредитної інформації заперечувало б свою відповідальність. Таким чином, суд прийшов до висновку, що автоматизований скоринг за таких обставин підпадає під дію ст.22 GDPR, яка встановлює заборону на такі рішення. Це також накладає на розробника алгоритму (SCHUFA) обов'язок надавати громадянам змістовну інформацію про логіку роботи системи [20].

Окрім того, у паралельних справах (C-26/22 та C-64/22) суд розглянув питання правомірності тривалого зберігання приватними агентствами кредитної інформації, зокрема даних про звільнення осіб від залишкових боргів, отриманих із державних реєстрів. Згідно з німецьким законодавством, офіційна публікація таких рішень у публічному електронному реєстрі неплатоспроможності припинялася через 6 місяців, щоб надати боржнику другий шанс. Проте SCHUFA зберігала цю інформацію у власних базах протягом 3 років, посилаючись на затверджений ними кодекс поведінки. Суд ЄС постановив, що стаття 5(1)(a) та стаття 6(1)(f) GDPR забороняють приватним кредитним агентствам зберігати інформацію про платоспроможність довше, ніж вона може зберігатися у відкритому державному реєстрі. Головним аргументом суду стало те, що звільнення від боргу має на меті дозволити особі знову брати участь в економічному житті, а подальше використання цих даних як негативного фактора скорингу нівелює цю можливість. Таким чином, інтереси кредитного сектору не можуть виправдати обробку даних поза межами встановленого законом шестимісячного строку [21].

Важливим висновком суду стало також те, що кодекси поведінки, розроблені відповідно до ст.40 GDPR, не можуть встановлювати умови правомірності обробки даних, які відрізняються від передбачених у самому Регламенті. Навіть якщо такий кодекс був схвалений наглядовим органом і передбачав тирічний термін зберігання. Він не може бути підставою для балансування інтересів на користь контролера, якщо це суперечить захисту прав суб'єкта даних [21].

Щодо механізмів захисту, суд підкреслив, що згідно зі статтею 17(1)(d) GDPR, контролер зобов'язаний видалити незаконно оброблені дані якнайшвидше. Якщо обробка відбувалася протягом дозволених шести місяців, суб'єкт даних все одно має право заперечити проти неї (згідно зі ст.21(1) GDPR), і агентство повинно видалити інформацію, якщо не доведе наявність переважаючих законних підстав для її збереження.

Крім того, суд роз'яснив роль наглядових органів та судового контролю, зазначивши, що рішення наглядового органу за скаргою суб'єкта даних підлягає повному судовому перегляду. Це означає, що суд не може обмежуватися лише перевіркою процедурних моментів, а має право оцінювати суть рішення та, за необхідності, зобов'язати регулятора вжити конкретних заходів для виправлення порушень [21]. Такий підхід, на нашу думку, забезпечує ефективну охорону прав громадян на захист персональних даних, приватність, право на забуття та другий шанс після фінансової неспроможності у цифрову епоху, де автоматизовані висновки можуть суттєво обмежити права гарантовані законом.

Генеративний ШІ та відповідальність за фейковий контент у медіа

Генеративний ШІ *(справа про інтерв'ю Міхаеля Шумахера).* Окремо слід навести прецедент у медійній сфері, пов'язаний із відповідальністю за створення та поширення фальшивого контенту за допомогою генеративного ШІ. У справі про фейкове AI-"інтерв'ю" Міхаеля Шумахера порушувалися саме права на ім'я, репутацію, образ (імідж), автентичність висловлювань та право на приватне життя (особливо з огляду на стан здоров'я М. Шумахера). Так, у квітні 2023 року німецький журнал Die Aktuelle (видавництво Funke Mediengruppe) опублікував матеріал, який на обкладинці позиціонувався як: "Міхаель Шумахер – Перше інтерв'ю". Усі наведені в публікації цитати були повністю згенеровані із застосуванням штучного інтелекту, тоді як видання обмежилося лише побіжною вказівкою на те, що ці висловлювання "звучать оманливо правдоподібно", не забезпечивши належного та однозначного інформування читачів про їхній штучний характер. Родина Шумахера, яка з 2014 року захищає його приватність через серйозний стан здоров'я, подала позов проти видавця. У травні 2024 року сім'я виграла справу. Funke Mediengruppe виплатила компенсацію в розмірі €200 000 [22; 23], офіційно вибачилася перед сім'єю та визнала матеріал таким, що вводить в оману [24]. Головну редакторку Анне Гоффманн звільнили ще в 2023 році після скандалу. Суд визнав відповідальність видавця, а не розробника ШІ, за порушення права на ім'я та приватність, застосувавши норми про дифамацію і захист особистих прав [22; 23].

Ця справа стала показовою для європейської правозастосовної практики, оскільки чітко закріпила відповідальність саме видавця медіа-

ISSN 1995-6134

контенту, а не розробника ШІ-технології, за поширення недостовірної інформації, створеної із застосуванням генеративного ШІ. Суд підкреслив пріоритет захисту права на приватність, гідність та загального права особистості у випадках, коли ШІ використовується для створення оманливих медійних матеріалів.

Водночас справа актуалізувала проблему необхідності спеціального правового регулювання використання ШІ у медіасфері, продемонструвавши ризики зловживань генеративними технологіями та їхній потенційний вплив на фундаментальні права людини. У цьому контексті вона кореспондує із загальноєвропейською тенденцією до посилення вимог до прозорості й відповідальності при використанні ШІ, зокрема в межах підходів, закладених у AI Act (2024), а також слугує практичним застереженням для таблоїдних медіа щодо неприпустимості створення фальшивих інтерв'ю навіть за умови формального використання ШІ-інструментів.

Висновки

1. Судова практика Європейського Союзу щодо відповідальності за шкоду, заподіяну використанням систем і технологій штучного інтелекту, демонструє низку сталих тенденцій та водночас підтверджує наявність системної проблеми – так званої *"прогалини у відповідальності"* (*liability gap*).

2. У жодному з проаналізованих прецедентів суди не визнали штучний інтелект самостійним носієм прав та обов'язків. У справах, пов'язаних з автономним транспортом (Tesla, Німеччина), державними алгоритмічними системами (SyRI, Нідерланди), гіг-економікою (Deliveroo, Uber, Ola), кредитним скорингом (SCHUFA) та генеративним контентом (фейкове інтерв'ю М. Шумахера), відповідальність послідовно покладається на фізичних або юридичних осіб. ШІ розглядається виключно як інструмент, продукт або технологія, створена та введена в обіг людиною, тоді як концепція «електронної особи» залишається суто теоретичною і не знаходить відображення у правозастосовній практиці.

3. Автономність, непрозорість і здатність систем ШІ до самонавчання істотно знижують ефективність традиційних режимів деліктного права. Потерпілі часто не можуть довести вину конкретного суб'єкта, причинно-наслідковий зв'язок або передбачуваність шкоди, що зумовлює стійку *liability gap*. У відповідь на це позивачі дедалі частіше використовують альтернативні механізми правового захисту – норми антидискримінаційного законодавства, захисту персональних даних, прав споживачів і особистих немайнових прав. Саме ці інструменти дозволяють судам реагувати на порушення *ex ante*, зобов'язуючи змінювати алгоритми, надати інформацію, забезпечувати прозорість або припиняти використання проблемних систем.

4. Водночас зазначені механізми мають переважно превентивний характер і лише обмежено спрямовані на відновлення правового становища особи, якій завдано шкоди. Навіть у разі встановлення порушення прав судові рішення здебільшого зводяться до усунення порушень, накладення штрафів або виплати компенсацій, які не завжди відповідають реальному обсягу наявної шкоди. Це свідчить про те, що прогалина у відповідальності за шкоду, заподіяну ШІ, має системний характер і не може бути подолана виключно шляхом розширеного тлумачення чинних норм права.

5. Таким чином, судова практика ЄС фактично визнає обмеженість класичного деліктного права у сфері використання ШІ та формує підґрунтя для запровадження спеціального правового режиму відповідальності, який має враховувати автономність, складність і багатосуб'єктний характер сучасних алгоритмічних систем.

6. Для України ці висновки є особливо значущими, оскільки національна модель цивільно-правової відповідальності також базується на класичних категоріях вини та причинного зв'язку. Європейський досвід вказує на необхідність завчасного перегляду цих підходів у контексті використання ШІ з метою запобігання ситуаціям, коли технологічний розвиток випереджає можливості ефективного правового захисту та залишає потерпілих без належних механізмів відновлення порушених прав і законних інтересів.

Конфлікт інтересів

Під час дослідження не зафіксовано обставин потенційного конфлікту інтересів.

Вираз вдячності

Дослідження виконано відповідно до планів науково-дослідних робіт Харківського національного університету внутрішніх справ.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Стефанчук М. О. Теоретичні засади цивільної правосуб'єктності фізичних осіб та особливості її здійснення: автореф. дис. … докт. юрид. наук: 12.00.03. Київ, 2020. С. 6.

ISSN 1995-6134

2. Кармаза О., Грабовська О. Електронна особа (особистість) як суб'єкт правовідносин у цивілістичному процесі. *Підприємництво, господарство і право*. № 2. 2021. С. 5–10.
3. Шишка О. Р. Людиноподібний робот Софія як суб'єкт цивільних прав : деякі проблеми правової визначеності законодавства України. Учасники цивільних відносин: новації рекодифікації цивільного (приватного) права України: матеріали XIX наук.-практ. конф., присвяч. 99-й річниці з дня народж. д-ра юрид. наук, проф., чл.-кор. АН УРСР В. П. Маслова (м. Харків, 12 берез. 2021 р.). Харків: Право, 2021. С. 250–256.
4. Turner J. Robot Rules: Regulating Artificial Intelligence. Palgrave Macmillan, 2018. 377 p. https://doi.org/10.1007/978-3-319-96235-1
5. European Parliament Resolution of 16 February 2017 with Recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL). https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_EN.html
6. Christensen D. Tesla Autopilot Accidents: Legal Rights & Liability Explained. Team Justice. https://teamjustice.com/tesla-autopilot-accidents-legal-rights-liability
7. BBC News. Tesla's 'Autopilot' misleading, Germany rules. BBC Home - Breaking News, World News, US News, Sports, Business, Innovation, Climate, Culture, Travel, Video & Audio. https://www.bbc.com/news/technology-53418069
8. Шишка О., Шишка Н. Відповідальність за шкоду, заподіяну використанням систем та технологій ШІ: судова практика в ЄС. *Цифрова трансформація прав: ЄС та Україна:* матеріали II-ї міжнар. наук.-практ. конф. (м. Харків, 25 квітня 2025 р.). Харків: ХНУВС, 2025. С. 151–162.
9. Isobel Asher Hamilton. Tesla ordered by German court to reimburse a woman $101,000 because her Autopilot was unreliable and kept making the car brake, report says. Business Insider Nederland. https://www.businessinsider.com/tesla-ordered-to-refund-101000-over-unreliable-autopilot-german-court-2022-7
10. Waldersee V., Murray M., Oatis J. Munich court orders Tesla to reimburse customer for Autopilot problems. Reuters. https://www.reuters.com/legal/transactional/munich-court-orders-tesla-reimburse-customer-autopilot-problems-2022-07-15
11. Henley J., Booth R. Welfare surveillance system violates human rights, Dutch court rules. the Guardian. https://www.theguardian.com/technology/2020/feb/05/welfare-surveillance-system-violates-human-rights-dutch-court-rules
12. Netherlands: Court Prohibits Government's Use of AI Software to Detect Welfare Fraud. The Library of Congress. https://www.loc.gov/item/global-legal-monitor/2020-03-13/netherlands-court-prohibits-governments-use-of-ai-software-to-detect-welfare-fraud
13. Lomas N. Italian court rules against 'discriminatory' Deliveroo rider-ranking algorithm | TechCrunch. TechCrunch. https://techcrunch.com/2021/01/04/italian-court-rules-against-discriminatory-deliveroo-rider-ranking-algorithm/
14. Eurofound (2022), Italian Court rules that the Deliveroo Algorithm Discriminates Workers (Court ruling), Record number 2271, Platform Economy Database, Dublin, https://apps.eurofound.europa.eu/platformeconomydb/italian-court-rules-that-the-deliveroo-algorithm-discriminates-workers-106121
15. Sentenza del Tribunale Ordinario di Bologna (Sezione Lavoro) del 27 novembre 2020 nel procedimento n. R.G. 2949/2019 (FILCAMS CGIL Bologna, NIDIL CGIL Bologna, FILT CGIL Bologna v. Deliveroo Italia S.r.l.). https://www.algoritmolegal.com/wp-content/uploads/2021/01/Sentencia-Bologna-Italia-Deliveroo-dic-2020-Original-italiano.pdf
16. Geiger G. Court Rules Deliveroo Used 'Discriminatory' Algorithm. Business and Human Rights Centre. 5 January 2021. https://www.business-humanrights.org/en/latest-news/court-rules-deliveroo-used-discriminatory-algorithm/
17. Lomas N. Dutch court rejects Uber drivers' 'robo-firing' charge but tells Ola to explain algo-deductions | TechCrunch. TechCrunch. https://techcrunch.com/2021/03/12/dutch-court-rejects-uber-drivers-robo-firing-charge-but-tells-ola-to-explain-algo-deductions/
18. Uitspraak van het Gerechtshof Amsterdam van 4 april 2023, zaak nr. 200.295.742/01 (ECLI:NL:GHAMS:2023:793). Amsterdam, 2023. https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:GHAMS:2023:793
19. Burton C., Theodorakis N., Evans T., Kern M. EDPB issues first guidelines on the interplay between the Digital Services Act and the GDPR. Wilson Sonsini Goodrich & Rosati. 22 September 2025. https://www.wsgr.com/en/insights/edpb-issues-first-guidelines-on-the-interplay-between-the-digital-services-act-and-the-gdpr.html

20. Judgment of the Court (First Chamber), 7 December 2023, Case C-634/21, OQ v Land Hessen, intervener: SCHUFA Holding AG. https://curia.europa.eu/juris/document/document.jsf?docid=280426&doclang=EN
21. Judgment of the Court (First Chamber), 7 December 2023, Joined Cases C-26/22 and C-64/22, UF and AB v Land Hessen, intervener: SCHUFA Holding AG. https://curia.europa.eu/juris/document/document.jsf?docid=280428&doclang=EN
22. Mayalo M. Michael Schumacher's family win legal action over fake AI interview. IOL Sport. 2024. 23 May. https://iol.co.za/sport/2024-05-23-michael-schumachers-family-win-legal-action-over-fake-ai-interview
23. Guardian staff reporter. Michael Schumacher's family win case against publisher over fake AI interview. The Guardian. https://www.theguardian.com/sport/article/2024/may/23/michael-schumacher-family-win-legal-case-against-publisher-over-fake-ai-interview
24. FUNKE trennt sich mit sofortiger Wirkung von „die aktuelle"-Chefredakteurin Anne Hoffmann. *FUNKE Mediengruppe - FUNKE Mediengruppe*. https://www.funkemedien.de/de/presse/funke-trennt-sich-mit-sofortiger-wirkung-von-die-aktuelle-chefredakteurin-anne-hoffmann

REFERENCES

1. Stefanchuk, M. O. (2020). *Teoretychni zasady tsyvilnoi pravosubiektnosti fizychnykh osib ta osoblyvosti yii zdiisnennia* [Theoretical foundations of civil legal personality of individuals and peculiarities of its exercise]. Avtoref. dys. … d-ra yuryd. nauk: 12.00.03. Kyiv (in Ukr.).
2. Karmaza, O., & Hrabovska, O. (2021). Elektronna osoba (osobystist) yak subiekt pravovidnosyn u tsyvilistychnomu protsesi [Electronic person (personality) as a subject of legal relations in the civil process]. *Pidpryiemnytstvo, hospodarstvo i pravo,* (2), 5–10 (in Ukr.).
3. Shyshka, O. R. (2021). Liudynopodibnyi robot Sofiia yak subiekt tsyvilnykh prav: deiaki problemy pravovoi vyznachenosti zakonodavstva Ukrainy [Humanoid robot Sophia as a subject of civil rights: Some problems of legal certainty of Ukrainian legislation]. In: *Uchasnyky tsyvilnykh vidnosyn: novatsii rekodyfikatsii tsyvilnoho (pryvatnoho) prava Ukrainy* Proceedings of the XIX Scientific and Practical Conference (Kharkiv, March 12, 2021) (pp. 250–256). Kharkiv: Pravo (in Ukr.).
4. Turner, J. (2018). *Robot Rules: Regulating Artificial Intelligence. Palgrave Macmillan.* https://doi.org/10.1007/978-3-319-96235-1
5. European Parliament. (2017, February 16). European Parliament Resolution with Recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)). https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_EN.html
6. Christensen, D. Tesla Autopilot Accidents: Legal Rights & Liability Explained. Team Justice. https://teamjustice.com/tesla-autopilot-accidents-legal-rights-liability
7. BBC News. (2020, July 15). Tesla's "Autopilot" misleading, Germany rules. https://www.bbc.com/news/technology-53418069
8. Shyshka, O., & Shyshka, N. (2025). Vidpovidalnist za shkodu, zapodiianu vykorystanniam system ta tekhnolohii ShI: sudova praktyka v YeS [Liability for damage caused by the use of AI systems and technologies: EU case law]. In: *Tsyfrova transformatsiia prav: YeS ta Ukraina.* Proceedings of the II International Scientific and Practical Conference (Kharkiv, April 25, 2025) (pp. 151–162). Kharkiv: KhNUVS (in Ukr.).
9. Hamilton, I. A. (2022, July 18). Tesla ordered by German court to reimburse a woman $101,000 because her Autopilot was unreliable. Business Insider Nederland. https://www.businessinsider.com/tesla-ordered-to-refund-101000-over-unreliable-autopilot-german-court-2022-7
10. Waldersee, V., Murray, M., & Oatis, J. (2022, July 15). Munich court orders Tesla to reimburse customer for Autopilot problems. Reuters. https://www.reuters.com/legal/transactional/munich-court-orders-tesla-reimburse-customer-autopilot-problems-2022-07-15/
11. Henley, J., & Booth, R. (2020, February 5). Welfare surveillance system violates human rights, Dutch court rules. The Guardian. https://www.theguardian.com/technology/2020/feb/05/welfare-surveillance-system-violates-human-rights-dutch-court-rules
12. The Library of Congress. (2020, March 13). Netherlands: Court Prohibits Government's Use of AI Software to Detect Welfare Fraud. https://www.loc.gov/item/global-legal-monitor/2020-03-13/netherlands-court-prohibits-governments-use-of-ai-software-to-detect-welfare-fraud
13. Lomas, N. (2021, January 4). Italian court rules against "discriminatory" Deliveroo rider-ranking algorithm. TechCrunch. https://techcrunch.com/2021/01/04/italian-court-rules-against-discriminatory-deliveroo-rider-ranking-algorithm/
14. Eurofound. (2022). Italian Court rules that the Deliveroo algorithm discriminates workers. Platform Econ-

omy Database, Record No. 2271. https://apps.eurofound.europa.eu/platformeconomydb/italian-court-rules-that-the-deliveroo-algorithm-discriminates-workers-106121
15. Tribunale Ordinario di Bologna (Sezione Lavoro). (2020, November 27). Sentenza nel procedimento n. R.G. 2949/2019 (FILCAMS CGIL Bologna et al. v. Deliveroo Italia S.r.l.). https://www.algoritmolegal.com/wp-content/uploads/2021/01/Sentencia-Bologna-Italia-Deliveroo-dic-2020-Original-italiano.pdf
16. Geiger, G. (2021, January 5). Court Rules Deliveroo Used "Discriminatory" Algorithm. Business & Human Rights Resource Centre. https://www.business-humanrights.org/en/latest-news/court-rules-deliveroo-used-discriminatory-algorithm/
17. Lomas, N. (2021, March 12). Dutch court rejects Uber drivers' "robo-firing" charge but tells Ola to explain algo-deductions. TechCrunch. https://techcrunch.com/2021/03/12/dutch-court-rejects-uber-drivers-robo-firing-charge-but-tells-ola-to-explain-algo-deductions/
18. Gerechtshof Amsterdam. (2023, April 4). Uitspraak in zaak nr. 200.295.742/01 (ECLI:NL:GHAMS:2023:793). https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:GHAMS:2023:793
19. Burton, C., Theodorakis, N., Evans, T., & Kern, M. (2025, September 22). EDPB issues first guidelines on the interplay between the Digital Services Act and the GDPR. Wilson Sonsini Goodrich & Rosati. https://www.wsgr.com/en/insights/edpb-issues-first-guidelines-on-the-interplay-between-the-digital-services-act-and-the-gdpr.html
20. Court of Justice of the European Union. (2023, December 7). Judgment in Case C-634/21, OQ v Land Hessen (SCHUFA Holding AG). https://curia.europa.eu/juris/document/document.jsf?docid=280426&doclang=EN
21. Court of Justice of the European Union. (2023, December 7). Judgment in Joined Cases C-26/22 and C-64/22, UF and AB v Land Hessen (SCHUFA Holding AG). https://curia.europa.eu/juris/document/document.jsf?docid=280428&doclang=EN.
22. Mayalo, M. (2024, May 23). Michael Schumacher's family win legal action over fake AI interview. IOL Sport. https://iol.co.za/sport/2024-05-23-michael-schumachers-family-win-legal-action-over-fake-ai-interview
23. Guardian Staff Reporter. (2024, May 23). Michael Schumacher's family win case against publisher over fake AI interview. The Guardian. https://www.theguardian.com/sport/article/2024/may/23/michael-schumacher-family-win-legal-case-against-publisher-over-fake-ai-interview
24. FUNKE Mediengruppe. (2023, April 21). FUNKE trennt sich mit sofortiger Wirkung von „die aktuelle"-Chefredakteurin Anne Hoffmann. https://www.funkemedien.de/de/presse/funke-trennt-sich-mit-sofortiger-wirkung-von-die-aktuelle-chefredakteurin-anne-hoffmann

ІНФОРМАЦІЯ ПРО СТАТТЮ (ARTICLE INFO)

Published in:
Форум права, № 84 (4), 2025, pp. 205–216
ISSN: 1995-6134

Related identifiers:
Is published in:
http://forumprava.pp.ua/files/205-216-2025-4-FP-Shyshka,Shyshka_25.pdf
Is identical to:
http://nbuv.gov.ua/UJRN/FP_index.htm_2025_4_25.pdf

License (for files):
Creative Commons Attribution 4.0 International (CC BY 4.0)

Надійшла до редакції (Received): 17.11.2025
Прийнята до друку (Accepted): 12.12.2025
Опублікована (Published): 15.12.2025

Cite as:

Шишка, О. Р., Шишка, Н. В. (2025). Відповідальність за шкоду, заподіяну використанням систем та технологій штучного інтелекту: судова практика в ЄС. *Форум Права, 84*(4), 205-216. http://doi.org/10.5281/zenodo.18338303

Shyshka, O. R., & Shyshka, N. V. (2025). Vidpovidalnist za shkodu, zapodiyanu vykorystannyam system ta tekhnolohiy shtuchnoho intelektu: sudova praktyka v YES [Liability for Damage Caused By the Use of AI Systems and Technologies: Case Law in the EU]. *Forum Prava, 84*(4), 205–216. http://doi.org/10.5281/zenodo.18338303