УДК [004.62:004.855.5]+342.723

**ДУБНЯК М.В.,** *кандидат юридичних наук,* в.о. завідувача наукової лабораторії правового забезпечення цифрової трансформації Наукового центру цифрової трансформації і права ДНУ "ІІБП" НАПрН України. Старший викладач кафедри інформаційного, господарського та адміністративного права КПІ ім. Ігоря Сікорського.
ORCID: https://orcid.org/0000-0001-7281-6568.

# ПРАВО НА РЕЗУЛЬТАТИ ОБРОБКИ ДАНИХ У ФОРМІ ПРОГНОЗНИХ ВИСНОВКІВ ОТРИМАНИХ ШТУЧНИМ ІНТЕЛЕКТОМ

***Анотація.*** *У статті досліджується правовий режим "прогнозних висновків" сформульованих за результатом обробки комбінованих наборів Великих Даних. Аналізуються право доступу та право на виправлення, як потенційні правові механізми протидії ефектам впливу прогнозних висновків. Доводиться, що прогнозні висновки, які отримуються штучним інтелектом у результаті обробки Великих Даних, впливають на суб'єкта даних в умовах економіки даних. Разом з цим встановлюється, що ні право доступу, ні право на виправлення не захищають суб'єкта даних від результатів використання прогнозних висновків. Обґрунтовується необхідність запровадження нового права, яке має доповнити систему правових гарантій захисту персональних даних – "право на результати обробки даних".*

***Ключові слова:*** *персональні дані, штучний інтелект, прогнозні висновки, права суб'єкта даних, право на результат обробки даних, Великі Дані, набори не персональних даних.*

***Summary****. The article investigated the legal regime of "predictive conclusions" formulated as a result of processing Big Data combined sets. The right of access and the right to rectification are analyzed as potential legal mechanisms for counteracting the effects of predictive conclusions. It is proven that predictive conclusions obtained by artificial intelligence as a result of processing Big Data affect the data subject in the conditions of the data economy. At the same time, it is established that neither the right of access nor the right of rectification protect the data subject from the results of the use of predictive conclusions. The necessity of introducing a new right, which should supplement the system of legal guarantees of personal data protection – "the right to the results of data processing" is substantiated.*

***Keywords****: personal data, artificial intelligence, predictive conclusions, data subject rights, the right to the result of data processing. Big Data, sets of non-personal data.*

**Постановка проблеми.** В епоху збору та обробки Великих Даних, розвитку економіки даних, важливе місце займає захищеність приватного життя особи та існування реальних правових інструментів управління власними персональними даними (далі – ПД).

Поширення аналітики Великих Даних збільшило можливості збору та доповнення даних про особу. Великі Дані можуть включати в себе комбінований набір персональних і не персональних даних. Результат обробки такої категорії даних технологіями штучного інтелекту (далі – ШІ) дозволяє отримати прогнозні висновки. Такі висновки забезпечують конкурентні переваги для компанії, оскільки дозволяють змоделювати поведінку, а інколи, і безпосередньо вплинути на рішення особи. Суб'єкт ПД не може відстежити, що його ПД були включені до набору Великих Даних, особливо якщо їх було анонімізовано, отже важко навіть оцінити безпрецедентні масштаби втручання в право на приватність у процесі аналізу наборів Великих Даних.

З урахуванням особливостей розвитку технологій суб'єкти даних мають отримувати додаткові права для забезпечення приватності. Норми Регламенту (ЄС) 2016/679 Європейського Парламенту та Ради від 27 квітня 2016 р. (Загальний Регламент щодо захисту персональних даних, далі – GDPR) встановлюють ряд прав для суб'єкта даних, зокрема: право бути поінформованим про збирання даних (ст. 13-14), право доступу до даних (ст. 15), право на виправлення (ст. 16), право на стирання (право бути забутим) (ст. 17), обмеження опрацювання (ст. 18), право на мобільність (перенесення) даних (ст. 20), право на заперечення (ст. 21), захист від профайлінгу (ст. 22) [1].

Виникає сумнів, чи може суб'єкт ПД реалізувати право на доступ чи виправлення даних, та інші права передбачені GDPR, щодо даних, які були отримані у результаті обробки наборів даних технологіями ШІ. Попередньо назвемо таку категорію даних "прогнозними висновками". Особливістю такого виду даних є те, що ШІ обробляє дані з використанням різних алгоритмів, і інколи навіть розробники технологій не можуть пояснити, на підставі яких комбінацій, доступних наборів та методів обробки даних, ШІ сформував прогнозний висновок (ефект "чорної скриньки"). Ускладнює таку ситуацію динамічна властивість даних, оскільки одна і та сама інформація може одночасно перебувати у різних правових режимах захисту. Тому можуть виникати спори щодо правових підстав обробки даних, визначення власника отриманих результатів обробки [2, с. 72], а також те, що до набору даних могли не входити ПД, а тому суб'єкт даних не може вимагати доступу до них чи їх виправлення.

Практика тлумачення норм щодо захисту персональних даних в ЄС схиляється до розширеного тлумачення, коли до ПД можуть прирівняти інші дані, якщо вони "стосуються" фізичної особи чи здатні вплинути на неї [3]. Тобто норми GDPR надають суб'єктам даних права контролювати межі збору та обробки даних, але не надають механізмів для управління новими даними, які були отримані у результаті їх аналізу, та описують поведінку та можливі інтереси суб'єкта даних. Фактично це дані аналітичних прогнозів, на яких базуються комерційні інтереси суб'єктів економіки даних. Отже маємо проблему правової невизначеності даних, отриманих в результаті аналізу Великих Даних та отриманих прогнозних висновків. Крім того, у суб'єкта даних немає спеціальних прав (виправлення, стирання, мобільності, обмеження опрацювання), на результати обробки даних у формі прогнозних висновків, оскільки ці дані є згенерованими та не персональними і не охоплюються первісною згодою на обробку ПД. З іншого боку, при розробці законодавчого регулювання права на результати обробки даних це право має врівноважуватись із нормами про захист інтелектуальної власності, комерційної таємниці, свободи підприємництва [4].

Певні прогнозні висновки формуються у процесі надання адміністративних послуг на підготовчому етапі (до прийняття остаточного рішення). У такому випадку, у суб'єкта даних має бути чітко встановлено права на доступ до проміжних результатів обробки його даних (запиту), оскільки такі результати попередньої обробки можуть вплинути на остаточне рішення і остаточний результат надання адміністративної послуги.

Досліджуючи проблеми обробки ПД з урахуванням методів аналізу Великих Даних, машинного навчання, інших технологій ШІ необхідно відзначити, що не всі Великі Дані містять ПД. Але враховуючи прецедентну практику Суду ЄС, який використовує широкий підхід до тлумачення категорії "персональні дані", зокрема через критерій "стосується" фізичної особи, яку може бути ідентифіковано [3], виникає необхідність відмежування різних категорій даних, правових режимів їх захисту, та встановлення меж дії законодавства про захист персональних даних, у тому числі і GDPR.

**Метою статті є** обґрунтування права суб'єкта даних на результати обробки даних (прогнозних висновків), отриманих у зв'язку із використанням технологій штучного інтелекту і визначення місця такого права в системі інформаційного права.

**Результати аналізу наукових публікацій.** Особливості обігу даних в соціальних мережах, формування комбінованих наборів даних досліджували Graef I, Gellert R., Husovec, M. [3], Scism L. [4], Altenburger K., Ugander J. [7], особливості збирання даних в умовах розвитку Інтернету речей досліджували Cook J. [8], особливості застосування деяких прав згідно GDPR аналізуються в роботі Korff D. [9]. У роботі Wachter S., Mittelstadt B.D. [19] комплексно проаналізовано проблему, що фокус правового регулювання зміщено в бік процедур збору ПД, а не їх аналізу. Правовий режим ПД та окремі проблеми правового регулювання в умовах застосування технологій Інтернету речей досліджували Баранов О.А., Брижко В.М. [21], Пилипчук В.Г., Фурашев В.М. Деякий теоретичний аналіз необхідності впровадження "права на висновки" є в роботі Wachter S., Mittelstadt B.D. [19], однак, у цій праці аналізується як результати обробки даних формують враження третіх осіб про нас, як суб'єкта даних. З урахуванням деяких положень з роботи Wachter S., Mittelstadt B.D. [19] невирішеним залишилось питання місця права на результат обробки даних в системі інформаційного права, що є метою цього дослідження.

**Виклад основного матеріалу.** Методи аналізу Великих Даних можна розрізняти відповідно до ціннісного критерію. Існує дві сфери застосування Великих Даних для здійснення аналітики:

1) аналітика вихідних даних для прийняття рішень;

2) автоматизовані аналітичні процеси, які надають описову, діагностичну, прогнозну та практичну аналітику [5].

Описова аналітика надає відповіді на питання: "Що сталося?" і "Що відбувається зараз", описуючи світ таким, яким він є, і надаючи історію та сучасне уявлення про світ у минулому та теперішньому часі.

Діагностична аналітика руйнує закономірності та усталені тенденції, та відповідає на питання: "Чому це сталося?". При цьому аналізуються статистичні моделі з ключовими змінними параметрами та зв'язками між даними (наприклад, ринкова аналітика, цінова пластичність, моделі шахрайства, інтелектуальний аналіз і кореляція даних, виявлення взаємозв'язків у даних тощо). Діагностична модель необхідна для визначення дійсності даних, отриманих в Інтернеті речей.

Прогнозна аналітика зосереджена на отриманні даних, необхідних для розуміння майбутнього. Така аналітика представляє прогнози щодо невідомих майбутніх подій на основі діагностичної аналітики та генерує нові рішення на основі цих даних [6]. Тобто Великі Дані, які були оброблені методами прогнозної аналітики, необхідні для побудови нових соціальних моделей .

Використання даних для розвитку технологій машинного навчання створюють нові можливості для прийняття дискримінаційних та упереджених рішень, що порушують конфіденційність. Наприклад, через аналіз весільних фотографій, опублікованих у соціальній мережі, можна зробити висновок про релігійну приналежність особи, а з аналізу даних про "спільних друзів" та фотографій з місця відпочинку страхові компанії можуть використати для встановлення розміру страхових внесків [7]. Голосовий помічник Alexa від Amazon може оцінювати стан здоров'я з урахуванням особливостей мовлення [8]. Таким чином, більше занепокоєння викликають не стільки дані, які про себе поширюють користувачі соціальних мереж, а ті висновки, які впливають на конфіденційність особи після обробки та аналізу таких даних.

Процедури збору та аналізу Великих Даних для розробки технологій ШІ не регламентовані у правовому полі. Хоча у Кодексах етики розробки технологій ШІ містяться вимоги до прозорості і чесності обробки даних [9 – 13]. Звернемо увагу, що дотримання принципу прозорості компаніями-розробниками технологій ШІ, які його реалізують через опис процедур розробки ШІ, створення внутрішніх комітетів етики, для аналізу корпоративних правил компанії та "прозорість" у розумінні норм GDPR, це не одне і те саме. Наприклад, "прозорість", відповідно до ст. 12 GDPR встановлює, що *"контролер повинен вжити необхідних заходів для надання будь-якої інформації ...щодо опрацювання, суб'єкту даних у стислій, прозорій, доступній для розуміння формі";* п. 78 Преамбули GDPR *"прозорість щодо функцій та опрацювання персональних даних* (включає – *від Авт.*) *можливості суб'єкта даних відстежувати опрацювання даних*" [1].

Дотримання принципу прозорості часто виконується так, що компанія-розробник технологій ШІ, описує як працює алгоритм, але це не означає конкретного обґрунтування процесу отримання прогнозних висновків (результатів обробки даних). Адже повний і "прозорий" опис такого процесу позбавить компанію конкурентних переваг. Принцип прозорості для суб'єкта даних, означає можливість управляти тим, які дані збираються, з якою метою, і бути поінформованим про використання отриманих результатів обробки.

Отже, у суб'єкта даних має бути право управляти результатами обробки у формі прогнозних висновків, до того, як буде сформовано дані, які можуть порушити його конфіденційність.

У контексті дослідження проблем аналітики Великих Даних та впливу отриманих результатів на права суб'єкта даних поставимо питання – чи може суб'єкт даних отримати результати обробки даних, які його стосуються та чи має компанія право застосовувати отримані дані для формування прогнозних висновків щодо такого суб'єкта? Наприклад, прийняття рішення страховою компанією про розмір страхових внесків для конкретного клієнта, або рішення роботодавця щодо потенційного кандидата за результатом аналізу його профілю у соціальній мережі.

Для відповіді на ці питання звернемось до норм GDPR.

Положення статей 13, 14 GDPR, описують обов'язки контролера щодо змісту та порядку отримання згоди суб'єкта ПД, і окремі положення не застосовуються (до змісту згоди – *від Авт.*), якщо п. (b) ч.5 "надання такої інформації (строк опрацювання, цілі, категорії ПД, період зберігання, законні інтереси для опрацювання, джерело отримання даних та інші підстави визначенні вказаними статтями – прим. *Авт.*), стає неможливим, чи викликало б несумісні наслідки, зокрема, для опрацювання (даних) задля досягнення цілей суспільних інтересів, цілей наукового чи історичного дослідження або статистичних цілях" [1].

Таким чином, компанії, які обробляють ПД, у разі посилання на "суспільний інтерес обробки", або "статистичні цілі", формально отримують звільнення від обов'язку інформування суб'єкта даних про факт обробки його даних.

Згідно з ст. 15 GDPR право доступу означає, що:

*"1. Суб'єкт даних повинен мати право на отримання від контролера підтвердження факту опрацювання її або його персональних даних і, якщо це так – доступ до персональних даних та інформації.*

*3. Контролер повинен надати копію персональних даних, які знаходяться у процесі опрацювання...*

*4. ...отримання такої копії не повинно негативно впливати на права та свободи інших осіб"* [1].

Згідно ст. 16 GDPR право на виправлення надає *"суб'єкту даних ...право на виправлення його або її неточних персональних даних, яке повинен здійснити контролер без будь-якої необґрунтованої затримки"* [1].

Для розуміння особливостей реалізації цих норм звернемось до практики Суду ЄС. Досліджуючи особливості реалізації права доступу до даних у справах "YS, M і S" [15] Суд ЄС розглянув питання про те, чи можна вважати правовий аналіз, сформований спеціалістом під час надання адміністративної послуги, персональними даними. Ця справа є актуальною для дослідження правового статусу результатів обробки даних.

У процесі прийняття рішення щодо розгляду запиту громадян "YS, M і S", посадова особа, яка не має повноважень підписувати остаточне рішення по суті заяви, готує протокол щодо процесу прийняття остаточного рішення для внутрішнього обґрунтування дотримання усіх процедур. Протокол є частиною підготовчого процесу в цій службі, але не є частиною остаточного рішення, навіть незважаючи на те, що деякі пункти, згадані в ньому, можуть знову з'явитися в поясненні причин такого остаточного рішення.

У протоколі описуються як персональні дані заявника (ім'я, дата народження, національність) так і не персональні дані, які його стосуються: деталі процесуальної історії; відомості про заяви заявника та подані документи; правові положення, які застосовуються до ситуації заявника; оцінка вищевказаної інформації через призму застосовних правових положень. Ця оцінка називається "правовим аналізом".

Підкреслимо, що дані протоколу містять комбінований набір персональних і не персональних даних. Тому виникає питання: при реалізації прав суб'єкта даних, вони будуть стосуватись всього документу в цілому, чи тільки в частині, де є персональні дані, або і протоколу в цілому і отриманих оцінок (прогнозних висновків)?

Спірні питання, які розглядав Суд у цій справі, були такі:

- чи є правовий аналіз, включений до протоколу, персональними даними в розумінні Директиви 95/46/ЄС ?;
- чи має державний орган надати доступ до протоколу?;
- чи може державний орган відмовити в наданні доступу до протоколу на підставі "дотримання законних інтересів конфіденційності".

Якщо заявник просить доступ до протоколу, державний орган має надати копію цього документа чи достатньо надати опис (резюме, пояснення), які ПД заявника обробляються ? [15].

Це рішення є цікавими, ще і тому, що розгляд справи дозволяє встановити правовий статус даних, які можна перевірити (наприклад, фактів про особу), а не оцінок або даних, які не підлягають перевірці.

Розглядаючи викладені обставини справи Суд ЄС встановив, що дані внесені в протокол, є персональними даними. Правовий аналіз "стосується" конкретної фізичної особи, ґрунтується на ситуації індивідуальних характеристиках цієї особи, тому підпадає під дію поняття "персональні дані".

Але сама по собі сукупність правових норм юридичного аналізу не може тлумачитись як ПД, не може бути предметом судової перевірки і не є об'єктом реалізації права на виправлення (п. 39, 41, 42 рішення [15]).

У п. 40 рішення вказано, що *"правовий аналіз не є інформацією, що стосується заявника, оскільки він не обмежується суто абстрактним тлумаченням закону. Це інформація про оцінку та застосування компетентним органом цього закону до ситуації заявника, а сама ситуація встановлюється, серед іншого, за допомогою персональних даних, які доступні для державного органу"* [15].

Таким чином, похідні оцінки (прогнозні висновки), які зроблені з використанням ПД заявника, підпадають під норми законодавства про захист ПД, оскільки зроблені оцінки і висновки безпосередньо стосуються заявника і впливають на його життя.

Згідно п. 44 рішення принцип поваги до приватного життя, у контексті обробки ПД, означає, що: "*особа може бути впевнена, що персональні дані, які її стосуються, є правильними, і що вони обробляються в законний спосіб. Право доступу є необхідним для того, щоб дозволити суб'єкту даних отримати, залежно від обставин, виправлення, видалення або блокування своїх даних контролером"* і, у такий спосіб, реалізувати вказане право [15].

У п. 60 рішення суд вирішує питання меж реалізації права доступу та права отримувати копію документів. Зокрема, *"заявник має право доступу до всіх персональних даних, що стосуються його, які обробляються національними адміністративними органами. Для дотримання цього права достатньо, щоб заявнику було надано повне резюме цих даних у зрозумілій формі, тобто формі, яка дозволяє йому ознайомитися з цими даними та перевірити їх точність, і те, що вони оброблюється відповідно до цієї директиви, щоб заявник міг, у відповідних випадках, користуватися правами, наданими йому цією директивою"* [15].

У рішенні Суду ЄС чітко зазначено, що аналіз і складові висновки не вважаються персональними даними. Суд ЄС не розрізняє правовий аналіз і результати обробки даних у вигляді окремих коментарів чи висновків, створених у процесі обробки вихідного набору даних (п. 39 рішення [15]).

Аналіз не є еквівалентом прогнозних висновків, а скоріше міркуванням (логікою), яка веде до висновку. Таке міркування можна сприймати як когнітивний процес, тоді як "аналіз даних" – це записаний результат міркування. Важко уявити міркування чи логіку "правового аналізу", який не передбачає створення висновків щодо справи заявника. Необхідно розрізняти факти та процес їх аналізу. "Факти" можна описати "об'єктивними" показниками (наприклад, кілограми) або "суб'єктивними" критеріями (наприклад, важкий). Самі оцінки, оскільки їх можна вважати суб'єктивним вираженням факту, можуть вважатися персональними даним, оскільки вони "стосуються" фізичної особи [15].

Але це не означає, що через право доступу до процесу прийняття рішення, у поєднанні з правом на виправлення даних, суб'єкт може вказати на неточності в аналізі фактів, чи попередніх висновків у юридичному аналізі. Відтак, потенційна незгода, з висновками про результат обробки даних, є предметом судового розгляду, і оскарження дій чи бездіяльності державних органів, а не підміни функції суду і процесу доказування через право доступу та виправлення даних.

Тому, при визначенні, чи поширюється на певні дані правовий режим "персональних даних", необхідно визначити:

1. Чи можуть дані використовуватись для оцінки суб'єкта (наприклад, його поведінки).

2. Чи впливають такі дані на результат поведінки і дії суб'єкта даних.

При такому підході проблемним аспектом є невизначеність конкретних критеріїв, в якому випадку проаналізовані дані виражені суб'єктивними критеріями, а коли результати проведеного аналізу даних конкретно ґрунтуються на фактах.

Отже, при формулюванні правових підходів для реалізації права на результати обробки даних необхідно розрізняти факти або результати процесу оцінки (тобто "оцінка" або "думка"), а також сам процес (тобто "міркування") і конкретний метод обробки даних.

Важливо відзначити, що закон про захист даних, і зокрема право на доступ, не створено для надання доступу до результатів обробки або точності процесів прийняття рішень. У практиці Суду ЄС зустрічається аналіз сфери застосування двох інших Регламентів, які мають сприяти реалізації прав громадян у процесі адміністративної практики:

1. Регламент (ЄС) № 1049/2001 Європейського Парламенту та Ради від 30 травня 2001 року щодо доступу громадськості до документів Європейського Парламенту, Ради та Комісії [16]. Він покликаний забезпечити якомога більшу прозорість процесу прийняття рішень органами державної влади та інформації, на основі якої вони ґрунтують свої рішення. Таким чином, цей Регламент має сприяти, здійсненню права на доступ до документів і сприяти належній адміністративній практиці.

2. Регламент (ЄС) № 45/2001 Європейського Парламенту та Ради від 18 грудня 2000 року "Про захист осіб щодо обробки персональних даних установами та органами Співтовариства, та про вільний рух таких даних" [17], який призначений для забезпечення захисту свобод і основних прав осіб, зокрема їхнього приватного життя, під час обробки ПД. Але вони не призначені для забезпечення максимально можливої прозорості процесу прийняття рішень органами державної влади для належної адміністративної практики шляхом сприяння здійсненню права доступу до документів (п. 47 рішення [15]).

Таким чином, законодавство про захист даних загалом, і право на доступ зокрема, не розроблено для забезпечення повної прозорості у прийнятті рішень, що стосуються ПД, або для гарантування "належної адміністративної практики".

Такі підходи до практики застосування норм Регламентів і Директив, відображених в практиці Суду ЄС, викликають занепокоєння щодо правових та етичних стандартів прийняття рішень.

По-перше, правовий аналіз містить попередні висновки, припущення або думки, які лежать в основі остаточних висновків і рішення органу державної влади. Виключення права доступу та перегляду такого аналізу зі сфери дії законодавства про захист даних означає, що суб'єкти даних не можуть оцінити, наскільки потенційно впливові попередні висновки отримує державний орган до основного рішення щодо суб'єкта даних [18].

По-друге, практика надання суб'єкту даних лише короткого викладу (резюме в зрозумілій формі) ПД, які обробляються, суттєво обмежує сферу дії права на доступ та можливість суб'єкта даних оцінити законність обробки даних та достовірність своїх ПД, які використовуються для прийняття рішення.

По-третє, обмежена сфера дії закону про захист даних у сфері прийняття рішень в державному секторі, не сприятиме формуванню культури поводження і обробки даних в приватному секторі. Адже компанії можуть формулювати власні правила і політику конфіденційності, у яких ще більше будуть обмежувати право доступу та виправлення, або надмірно ускладнювати такі процедури.

Поширення аналітики Великих Даних і, як наслідок, збільшення можливостей контролерів даних отримувати інформацію про приватне життя людей, змінювати їх особистість через поведінкові шаблони, а також впливати на їх репутацію, свідчить про те, що потрібні додаткові категорії прав, які сприятимуть реалізації прав суб'єкта даних, з урахуванням особливостей розвитку технологій [15]. У сукупності з практикою правозастосування, можемо побачити, що спеціальних прав суб'єкта ПД, передбачених GDPR, не достатньо для захисту від прогнозних висновків за результатами аналізу Великих Даних технологіями ШІ.

Таким чином, згідно з рішеннями Суду ЄС, коли приватна компанія робить прогнозні висновки на основі зібраних даних, або приймає рішення на їх основі, навіть якщо остаточні висновки або рішення розглядаються як персональні дані, суб'єкти даних не можуть виправити їх відповідно до законодавства про захист даних. Суб'єкти даних також не мають доступу до аргументації, що лежить в основі рішень, яка не вважається персональними даними, а також засобів для виправлення аналізу відповідно до законодавства про захист даних [19, с. 531].

Цікаво проаналізувати і інше рішення, де Європейський Суд відступив від висновків по справах "YS, M і S".

У справі "Peter Nowak v. Data Protection Commissioner" [20] заявник попросив скористатися своїм правом доступу і "виправлення" його оціненого бланку відповідей на іспит. При визначенні питання, чи є персональними даними відповіді на питання іспиту, а також коментарі екзаменатора, Суд встановив:

- письмові відповіді, подані кандидатом на професійному іспиті, являють собою інформацію, яка "стосується" заявника як суб'єкта даних (п. 36) [20].
- зміст цих відповідей відображає ступінь знань і компетентності кандидата в певній галузі, а в деяких випадках і його інтелект, процеси мислення та здатність до міркування. У випадку рукописного тексту відповіді містять інформацію про його почерк (п. 37) [20].
- метою збору цих відповідей є оцінка професійних здібностей кандидата та його придатності до практики у відповідній професії (п. 38) [20].
- коментарі екзаменатора відображають думку або оцінку екзаменатора індивідуальних результатів іспиту кандидата, зокрема його знань і компетенцій у відповідній галузі. Крім того, мета цих коментарів полягає саме в тому, щоб зафіксувати оцінку екзаменатором роботи кандидата, і ці коментарі мають конкретні наслідки для кандидата (п. 43) [20].

Отже, якщо відповіді та зміст коментарів є персональними даними, це означає не тільки виникнення обов'язків контролера щодо обробки таких даних, а відповідно і виникнення у заявника прав на доступ, виправлення, чи заперечення.

Звичайно, право на виправлення не може дозволити кандидату "виправити" відповіді, які є "не правильними" (п. 52.) [20]. З іншого боку, виправлення можливе, у ситуації зміни титульного аркушу і помилкового приписування відповідей іншій особі (п. 54) [20].

Описані у рішеннях особливості реалізації права доступу та виправлення доводять, що законодавство про захист даних не поширюється на процеси забезпечення точності у процесі прийняття рішень. На перший погляд, у справі Nowak Суд розширив сферу дії норм про захист ПД, поширивши їх на думки та оцінки, іншого суб'єкта (екзаменатора), як такі, що "стосуються" заявника і мають на нього безпосередній вплив. Однак, висновки по справі описують обсяг даних, що обробляються, можливість поширення режиму ПД на результати обробки даних, формулювання оцінки щодо законності обробки. Оцінка точності результатів обробки та процесів прийняття рішень залишається поза сферою дії норм про захист ПД.

Ці два рішення відрізняються визначенням ПД. У справах "YS, M і S" Суд ЄС чітко тлумачить персональні дані обмежено. Ім'я, стать та подібні "факти" про особу, вважаються персональними даними, а думки, міркування та оцінки, які лежать в основі рішень, не є такими. У справі "Nowak", Суд ЄС навпаки встановив, що думки та оцінки (тобто коментарі екзаменатора) є персональними даними за критерієм "стосуються" фізичної особи.

Обидва судові рішення залишають відкритим питання про те, чи є результат оцінювання (наприклад, остаточний висновок, оцінка) і подальше рішення (наприклад, незадовільно оцінити когось на іспиті, відмовити в наданні адміністративної послуги) персональними даними. Незважаючи на розширення сфери визначення ПД у справі "Nowak", рішенню бракує повторюваності такого ж підходу в інших справах.

Вважається, що формування прогнозних висновків та похідних оцінок на основі аналізу ПД виходить за межі передбаченої мети законодавства про захист даних. Однак, якщо права в GDPR (наприклад, статті 15 – 17) не застосовуються до похідних даних (прогнозних висновків) одночасно з охороною ПД, то прогнозні висновки, які "стосуються" суб'єкта даних, та можуть вплинути на його поведінку, і отримані за результатом аналізу ПД, залишаються за межами правового захисту GDPR.

Можна звісно припустити, що на результати обробки може розповсюджуватись широка класифікація ПД за критерієм "стосується", однак в контексті обробки Великих Даних ШІ, ефекту "чорної скриньки" видається проблематичним ідентифікувати, які саме дані суб'єкта були оброблені, яким може бути ступінь визначення суб'єктом даних щоб оцінити точність або обґрунтованість отриманих висновків.

З урахуванням проведеного аналізу сформулюємо два поняття:

***Прогнозні висновки*** *– це дані, отримані у результаті аналізу Великих Даних технологіями штучного інтелекту*.

***Право на результати обробки даних*** *– це право суб'єкта персональних даних отримувати прогнозні висновки, які були отримані у результаті обробки комбінованих наборів даних, у тому числі псевдонімізованих.*

Окремою проблемою є корпоративний інтерес в обробці даних. Якщо результат прогнозних висновків у процесі надання адміністративної послуги можна оскаржити, оскільки існує зв'язок: "суб'єкт даних – заява в адміністративний орган – незаконне рішення (бездіяльність) – скарга суб'єкта даних – суд". То суб'єкти приватного сектору захищені положеннями Хартії ЄС про свободу підприємництва та нормами про захист наборів даних в режимі комерційної таємниці. Таким чином, суб'єкти господарювання самостійно встановлюють, критерії, за якими вони будуть оцінювати отримані висновки, і довести факт незаконності цих критеріїв оцінки буде дуже проблематично.

**Висновки.**

1. Великі Дані можуть включати в себе комбінований набір персональних і не ПД. Результат обробки Великих Даних у формі прогнозних висновків створює конкурентні переваги для компанії, оскільки дозволяє змоделювати поведінку особи, а інколи і безпосередньо вплинути на її рішення.

2. У випадку, якщо набір Великих Даних містив персональні дані, навіть у псевдонімізованій формі, отримані прогнозні висновки можуть мати безпосередній вплив на суб'єкта даних. Прогнозні висновки впливають на сферу приватності особи, через особливі категорії даних, які були проаналізовані для отримання висновків.

3. Права передбачені GDPR (доступу до даних, право на виправлення, стирання, обмеження опрацювання) застосовуються до обробки даних отриманих на підставі згоди, однак суб'єкт персональних даних позбавлений правової можливості захистити свої дані, оскільки не має правових інструментів виявлення, що його дані включені до набору Великих Даних.

4. Прогнозні висновки є окремим результатом обробки даних, які знаходяться за межами правового регулювання законодавства про захист ПД.

5. Право доступу до ПД не призначене для забезпечення прозорості процесу обробки даних, процесу прийняття рішення та формування прогнозних висновків. Це

позбавляє суб'єкта даних можливості оцінити, наскільки впливовими можуть бути прогнозні висновки, отримані за результатом обробки даних.

6. Право на результат обробки даних повинно передбачати можливість суб'єкта даних отримати прогнозні висновки з метою оцінки ступеню їх впливу на поведінку суб'єкта даних.

7. Вбачається, що використання комбінованого набору даних у псевдонімізованій формі, для отримання прогнозних висновків, не допоможе суб'єкту даних встановити, чи були оброблені саме його персональні дані, чи це були дані іншої особи. Однак, це не має бути універсальною підставою для відмови в наданні таких висновків, оскільки, право на результат обробки даних має забезпечувати окреме право суб'єкту даних, а саме: можливість самостійно оцінити ступінь впливу на його поведінку (дії, бездіяльність) через використання компаніями прогнозних висновків, а не їх точність та обґрунтованість по відношенню до конкретного суб'єкта даних.

8. Право на результат обробки даних не має тлумачитись у вузькому сенсі – як окремий спосіб реалізації права на виправлення неточних даних у контексті обробки Великих Даних технологіями ШІ.

9. Право на результат обробки даних повинно мати самостійне значення. Якщо його розглядати у системі прав, передбачених законодавством про захист ПД, існує ризик відмови у наданні результатів обробки даних, оскільки до комбінованого набору Великих Даних можуть не включатись персональні дані. Отже, компанії не будуть зобов'язані надавати такі результати обробки.

10. З урахуванням поставленої юридичної проблеми у роботі [21, с. 90] про "необхідність створення багаторівневої і багатооб'єктної системи захисту ПД та формування нової системи правового забезпечення" зазначимо, що норми GDPR, які широко регламентують права суб'єкта даних, у контексті особливостей їх обробки технологіями ШІ не охоплюють прогнозні висновки, які впливають на майбутню поведінку і дії суб'єкта права, а право на результат обробки даних, може вважатись окремим елементом такого багаторівневого і багатооб'єктного правового забезпечення і повинно мати самостійне значення у системі інформаційних відносин.

## Використана література

1. Regulation (EU) 2016/679 Of The European Parliament And Of The Council on General Data Protection Regulation. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A 32016 R0679&qid=1684155858687

2. Дубняк М.В. Економіка даних: правовий та етичний аспект. *Інформація і право.* № 3(46)/2023. С. 64-74.

3. Graef I., Gellert R., Husovec, M. (2018). Towards a Holistic Regulatory Approach for the European Data Economy: Why the Illusive Notion of Non-Personal Data is Counterproductive to Data Innovation. Cybersecurity. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3256189

4. Charter of Fundamental Rights of the European Union (2016/C 202/02). URL: http://data. europa.eu/eli/treaty/char_2016/oj

5. Kennedy G. (2017) Asia Pacific News. *Computer Law and Security Review,* 33, 6, 896-904. URL: https://doi.org/10.1016/j.clsr.2017.09.006.

6. Scism L. (2019) New York Insurers Can Evaluate Your Social Media Use – If They Can Prove Why It's Needed, WALL ST. J. URL: https://www.wsj.com/articles/new-york-insurers-can-evaluate-your-social- media-useif-they-can-prove-why-its-needed-11548856802 (on file with the Columbia Business Law Review).

7. Altenburger K., Ugander J. (2018) Monophily in Social Networks Introduces Similarity among Friends-of-Friends. *Nature human behaviour,* at 284.

8. Cook J. (2018) Amazon Patents New Alexa Feature That Knows When You're Ill and Offers You Medicine, *TELEGRAPH*. URL: https://www.telegraph.co.uk/technology/2018/10/09/amazon-patents-new- alexa-feature-knows-offers-medicine [https://perma.cc/V346-HFWE

9. Adobe AI Ethics Principles (2021) URL: https://www.adobe.com/about-adobe/aiethics.html

10. Ethical Norms for the New Generation Artificial Intelligence (2021) National Governance Committee for the New Generation Artificial Intelligence, China. URL: https://ai-ethics-and-governance.institute/2021/09/27/the-ethical-norms-for-the-new-generation-artificial-intelligence-china

11. Samsung AI principles (2018). URL: https://www.samsung.com/us/about-us/digital-responsibility/ai-ethics

12. Baidu Four principles of AI ethics (2018). URL: https://www.fonow.com/view/208592.html

13. Google AI principles (2018). URL: https://ai.google/responsibilities/responsible-ai-practices/?category=general

14. Sage Ethics of Code: Developing AI for Business with Five Core Principles (2017). URL: https://www.sage.com/investors/investor-downloads/press-releases/2017/06/27/sage-shares-core-principles-for-designing-ai-for-business

15. YS v Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v M and S: Judgment of the Court (Third Chamber), 17 July 2014. ECLI identifier: ECLI:EU:C:2014:2081. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=ecli%3AECLI%3AEU%3AC%3A2014%3A2081

16. Regulation (EC) № 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents. URL: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32001R1049

17. Regulation (EC) № 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32001R0045

18. Korff D. (2014) The Proposed General Data Protection Regulation: Suggested Amendments to the Definition of Personal Data, EU LAW ANALYSIS. URL: http://eulawanalysis.blogspot.com/2014/10/the- proposed-general-data-protection

19. Wachter S., Mittelstadt B.D. (2018). A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI. *Columbia Business Law Review*, 494-620. DOI: https://doi.org/10.7916/cblr.v2019i2.3424.

20. Peter Nowak v Data Protection Commissioner : Judgment of the Court (Second Chamber) of 20 December 2017, ECLI identifier: ECLI:EU:C:2017:994. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62016CJ0434

21. Баранов О.А., Брижко В.М. Захист персональних даних в сфері Інтернет речей. *Інформація і право.* № 2(17)/2016. С. 85-91.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~