УКРАЇНСЬКА ГЕЛЬСІНСЬКА СПІЛКА З ПРАВ ЛЮДИНИ

МІЖНАРОДНИЙ ФОНД ВІДРОДЖЕННЯ

ПРЯМУЄМО РАЗОМ

# ШТУЧНИЙ ІНТЕЛЕКТ ТА ПРАВА ЛЮДИНИ:

## ОРІЄНТИРИ ТА ОБМЕЖЕННЯ У КОНТЕКСТІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ ТА ОБОРОНИ

Київ. 2024

**Штучний інтелект та права людини: орієнтири та обмеження у контексті національної безпеки та оборони.**

Автори дослідження:

**Юлія Коваленко,** доктор філософії, адвокат, юрист Центру стратегічних справ Української Гельсінської спілки з прав людини

**Максим Войнов,** юрист Центру стратегічних справ Української Гельсінської спілки з прав людини

**Українська Гельсінська спілка з прав людини** (УГСПЛ) – найбільша асоціація правозахисних організацій України. Спілка об'єднує 26 правозахисних недержавних організацій. Метою діяльності УГСПЛ є захист прав людини.

УГСПЛ вважає себе частиною гельсінського руху і продовжувачем традицій та діяльності Української Гельсінської групи сприяння виконанню Гельсінських угод – УГГ.

**Міжнародний фонд «Відродження»** – одна з найбільших благодійних фундацій в Україні, що з 1990-го року допомагає розвивати в Україні відкрите суспільство на основі демократичних цінностей. За час своєї діяльності Фонд підтримав близько 20 тисяч проектів на суму понад 350 мільйонів доларів США.
Сайт: www.irf.ua
Facebook: www.fb.com/irf.ukraine

**Європейський Союз** складається з 27 держав-членів та їхніх народів. Це унікальне політичне та економічне партнерство, засноване на цінностях поваги до людської гідності, свободи, рівності, верховенства права і прав людини. Понад п'ятдесят років знадобилось для створення зони миру, демократії, стабільності і процвітання на нашому континенті. Водночас нам вдалось зберегти культурне розмаїття, толерантність і свободу особистості. ЄС налаштований поділитись своїми цінностями та досягненнями з країнами-сусідами ЄС, їхніми народами, та з народами з-поза їхніх меж.

УКРАЇНСЬКА ГЕЛЬСІНСЬКА СПІЛКА З ПРАВ ЛЮДИНИ

МІЖНАРОДНИЙ ФОНД ВІДРОДЖЕННЯ

ПРЯМУЄМО РАЗОМ

# Зміст

# УМОВНІ СКОРОЧЕННЯ

| | |
|---|---|
| **АСО** | автоматичні системи озброєння |
| **БПЛА** | безпілотні літальні апарати/безпілотники/дрони |
| **ЄКПЛ/Конвенція** | Конвенція про захист прав людини і основоположних свобод 1950 року |
| **ЄС** | Європейський Союз |
| **ЄСПЛ** | Європейський суд з прав людини |
| **Женевські конвенції** | Женевські конвенції про захист жертв війни 1949 року |
| **ІПсО** | інформаційно-психологічна спецоперація |
| **ЛАСО** | летальна автономна система озброєнь |
| **МГП** | Міжнародне гуманітарне право |
| **МПГПП** | Міжнародний пакт про громадянські та політичні права 1966 року |
| **МППП** | Міжнародне право прав людини |
| **НАТО** | Організація Північноатлантичного договору, Північноатлантичний альянс |
| **ОЕСР** | Організація економічного співробітництва та розвитку |
| **ООН** | Організація Об’єднаних Націй |
| **ШІ** | штучний інтелект |

# ВСТУП

Технології є частиною світу, в якому ми живемо, і важливим елементом майже кожного аспекту нашого життя. Цей феномен призводить до стрімкого розвитку та активного впровадження технологій штучного інтелекту (ШІ) у різні сфери та галузі, не є виключенням і військова справа. На думку експертів, війна в Україні – це своєрідна «перша світова війна з використанням технологій». ШІ активно застосовується для ведення війни за допомогою програмного забезпечення, використання дронів, для розпізнавання і розшифрування супутникових знімків, розпізнавання цілей на полі бою і прогнозування засобів, якими вони можуть бути уражені, для розпізнавання облич та ідентифікації військових злочинців або виявлення, ідентифікації жертв війни та повернення тіл загиблих їхнім сім'ям тощо.

Україна, як і інші країни, стикається з викликами регулювання використання ШІ у військовій сфері, особливо в контексті триваючої збройної агресії. Відтак важливо знайти баланс між використанням новітніх технологій для захисту країни та забезпеченням дотримання прав людини.

Безумовно, застосування технологій ШІ надає широкий спектр можливостей і має низку переваг, адже ШІ може покращити та оптимізувати процес прийняття рішень на полі бою, поглибити обізнаність та розуміння поля бою, забезпечити перевагу, адаптивність планування сил та підвищити точність і швидкість прийняття рішень, зокрема й щодо виявлення, ідентифікації, оцінки загроз та реагування на них. Впровадження ШІ у військовій сфері може передбачати, серед іншого, розробку БпЛА, антидронових рушниць, систем управління боєм, тренувальних модулів, систем кібербезпеки. Завдяки ШІ стає можливою й розробка новітнього озброєння, впровадження автономних систем озброєнь (АСО), тобто бойових систем, що здатні самостійно ідентифікувати та вражати ціль, а також летальних автономних систем озброєнь (ЛАСО), тобто таких систем зброї, які можуть виявляти, визначати цілі та атакувати їх без прямої участі людини у прийнятті рішення про момент та об'єкт атаки. Однак використання ШІ у військових цілях нерідко викликає й певні етичні та моральні занепокоєння, особливо у контексті використання летального автономного озброєння. Відтак використання військового ШІ ставить низку питань – чи може ШІ приймати рішення про застосування сили? хто нестиме відповідальність за такі рішення? чи існують запобіжники щодо помилкової ідентифікації цілей, упередженості чи непрозорості алгоритмів?

Вочевидь, стрімкий розвиток технологій ШІ та їх широке впровадження у різні галузі свідчить про те, що вони мають подвійну природу, адже можуть застосовуватися як у мирному житті, так і у військовій справі. Відповідно, впровадження та застосування таких технологій у нових сферах може створювати певні ризики для основоположних прав та свобод людини, а тому потребує належного правового регулювання і розробку та впровадження безпечних систем ШІ, орієнтованих на дотримання прав людини, а також їх відповідальне використання.

# I. СУЧАСНІ ПІДХОДИ ЩОДО ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ (ШІ) У БЕЗПЕКОВІЙ СФЕРІ

Темпи розвитку штучного інтелекту (ШІ) у сучасному світі вражають. Технології ШІ, серед іншого, використовуються для розпізнавання мови, біометричної автентифікації, навігаційних систем, транспортування і контролю за дорожнім рухом, менеджменту, виробництва, управління ланцюгами постачання, збору даних і контролю за цільовим онлайн-маркетингом. Стрімкий розвиток цієї технології дозволяє поступово адаптувати її до різних галузей сучасного життя, включаючи економічну сферу, промисловість, медицину, освіту та науку, судочинство, правоохоронну діяльність тощо. Відтак не викликає здивування активне впровадження систем ШІ у сфері національної безпеки та оборони, що є важливим напрямом розвитку військових технологій.

ШІ у військовій сфері (або ж військовий ШІ) має великий потенціал і може бути застосований для різних цілей. Нижче наведено деякі приклади використання ШІ в цьому контексті:

- **Автономні системи озброєння (АСО)**. Збройні системи з ШІ можуть самостійно ідентифікувати, відстежувати і вражати цілі з мінімальною участю людини, щоб мінімізувати ризики супутньої шкоди і одночасно підвищити ефективність військових операцій.

- **Спостереження та розвідка.** Алгоритми ШІ можуть використовувати величезні обсяги даних спостереження, такі як зображення, аудіопотоки і радіолокаційні сигнали, щоб виявляти закономірності, відхилення і відстежувати цілі для інформування військового командування в режимі реального часу.

- **Розпізнавання та класифікація цілей.** ШІ може бути використаний для ідентифікації і класифікації об'єктів, таких як озброєння, бойова, боєприпаси, бойова та інша техніка і особовий склад, для більш швидкого і точного виявлення і ураження цілей.

- **Аналіз і прогнозування загроз.** Системи ШІ можуть використовувати історичні дані, поточну інформацію, враховувати інформацію про навколишнє середовище для точного прогнозування потенційних загроз або вразливостей і вжиття превентивних кроків для протидії ризикам.

- **Логістика та управління ланцюгами постачання.** Технології ШІ можуть допомогти логістичним операціям, оптимізуючи планування маршрутів, контроль запасів, розподіл ресурсів, підвищуючи ефективність і знижуючи витрати.

- **Кібербезпека.** Системи кібербезпеки на основі ШІ можуть виявляти і нейтралізувати кібератаки, захищаючи критично важливу військову інфраструктуру і мережі.

- **Радіоелектронна боротьба.** Технології ШІ дозволяють аналізувати перехоплені сигнали з каналів зв'язку та інші форми електронного зв'язку, щоб визначити місцезнаходження ворожих позицій, вивести з ладу ворожі комунікаційні мережі та отримати тактичну перевагу над противником.

- **Симуляція й навчання.** Симуляції на основі ШІ створюють реалістичні умови для тренувань військових, дозволяючи їм відпрацьовувати бойові сценарії і набувати нових навичок.

- **Системи підтримки прийняття рішень.** Технології ШІ можуть використовуватися для аналізу складних масивів даних і надання рекомендації військовим командирам для стратегічного планування та прийняття рішень.

Зауважимо, що у звіті Організації НАТО з науки і технологій (NATO Science & Technology Organization) «Тенденції у науці й технологіях: 2020-2040», були окреслені тенденції розвитку технологій впродовж наступних 20 років. Так, у зазначеному звіті досліджені напрями розвитку науки й технологій, які потенційно матимуть вплив на розвиток колективної безпеки й оборони, що включають технології великих даних, технології штучного інтелекту, автономні системи, квантові, космічні та гіперзвукові технології й біотехнології.[1]

Для використання можливостей технологій ШІ більшість провідних країн розробили національні та наднаціональні стратегії в цій сфері. Подібні документи були затверджені в Європейському Союзі, а також у США, Канаді, Китаї, Японії, Південній Кореї та інших країнах. На міжнародному рівні першою спробою унормувати стандарти використання ШІ стала Рекомендація Організації економічного співробітництва та розвитку (ОЕСР) з питань штучного інтелекту, прийнята 22 травня 2019 року.[2]

В Україні питання регулювання технологій ШІ були закріплені у затвердженій Кабінетом Міністрів України Концепції розвитку штучного інтелекту в Україні.[3] Згадана Концепція визначила дев'ять пріоритетних сфер розвитку галузі ШІ, що включає: освіту, науку, економіку, кібербезпеку, оборону, інформаційну безпеку, державне управління, правове регулювання та етику, правосуддя. Основними принципами розвитку та використання технологій ШІ, дотримання яких є обов'язковим для реалізації цієї Концепції, та які повністю відповідають принципам ОЕСР з питань штучного інтелекту, є наступні:

- ШІ має приносити користь людям і планеті, сприяючи інклюзивному зростанню, сталому розвитку та добробуту;

- системи ШІ розробляються та використовуються лише за умови дотримання верховенства права, основоположних прав і свобод людини і громадянина, демократичних цінностей, а також їх використання має забезпечуватися відповідними гарантіями, зокрема, можливістю безперешкодного втручання людини у процес функціонування системи ШІ;

- забезпечення прозорості та відповідального розкриття інформації про системи ШІ;

- системи ШІ повинні функціонувати надійно та безпечно протягом усього їх життєвого циклу, а оцінка та управління потенційними ризиками має здійснюватися на постійній основі;

---

[1] NATO Science & Technology Organization. Science & Technology Trends 2020-2040. Available at: https://securitydelta.nl/media/com_hsd/report/406/document/190422-ST-Tech-Trends-Report-2020-2040.pdf

[2] OECD. Recommendation of the Council on Artificial Intelligence, adopted on 22.05.2019. Available at: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449

[3] Концепція розвитку штучного інтелекту в Україні, затверджена розпорядженням КМУ від 02.12.2020 року 1556-р. Доступно за посиланням: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text

- організації та особи, які розробляють, впроваджують або використовують системи ШІ, несуть відповідальність за їх належне функціонування відповідно до вищезазначених принципів.

Примітно, що у грудні 2023 року було ухвалено дорожню карту з регулювання ШІ в Україні, яка спрямована на забезпечення балансу між інноваціями, безпекою та захистом прав людини від ризиків розробки та використання систем з ШІ, а також імплементацію відповідних норм права ЄС у цій сфері.

Важливим історичним етапом розвитку ШІ стало схвалення Європейським Парламентом 13 березня 2024 року Закону про штучний інтелект (AI Act), який є першим у світі правовим актом, що регулює питання використання штучного інтелекту та водночас спрямований на захист демократії, верховенства права та основоположних прав людини.[4] Закон про ШІ передбачає «горизонтальний» підхід, який запроваджує правила ШІ для всіх секторів та галузей, встановлює правила відповідального використання ШІ з урахуванням потенційних ризиків, а також встановлених стандартів безпеки та прозорості. Закон про ШІ також встановлює обмеження для різних рівнів ризику технологій ШІ, поділяючи їх на: 1) системи ШІ з обмеженим та мінімальним ризиком (до яких належать більшість систем ШІ), 2) системи ШІ з високим ступенем ризику, тобто такі, що становлять значну загрозу здоров'ю, безпеці чи основоположним правам людини та вимагають постійної оцінки їх відповідності, 3) заборонені практики, до прикладу, використання біометричних систем, що працюють у режимі реального часу і віддалено, зокрема, сканування для розпізнавання обличчя.

Паралельно з розробкою та прийняттям Закону ЄС про ШІ в рамках Ради Європи впродовж останніх трьох років проводилася робота над Рамковою конвенцією про штучний інтелект, права людини, демократію та верховенство права, остаточний текст якої було оприлюднено 27 березня 2024 року.[5] Згаданий міжнародно-правовий акт, на відміну від Закону ЄС про ШІ, закріплює загальні принципи та підходи до регулювання ШІ, які поширюються, перш за все, на публічний сектор, залишаючи питання поширення відповідних норм на приватний сектор на розсуд держав, які можуть зробити відповідну декларацію. Водночас питання, які стосуються національної оборони, не підпадають під сферу дії Рамкової конвенції. Що стосується використання ШІ у сфері національної безпеки, то держави не зобов'язані застосовувати Рамкову конвенцію, але використання ШІ у цій сфері повинно відповідати нормам міжнародного права, включаючи міжнародні зобов'язання щодо прав людини.

Водночас у НАТО також приділяється значна увага технологіям штучного інтелекту та практичним аспектам їх використання з точки зору розвитку національних та спільних спроможностей, а також всебічного врахування можливих проблем та викликів, пов'язаних із масовим поширенням відповідних технологій у світі.

У жовтні 2021 року НАТО було офіційно ухвалено стратегію ШІ, яка покликана прискорити впровадження ШІ, зосереджуючись на ключових аспектах співпраці у контексті розробки і впровадження ШІ, адаптації політики, включаючи принципи відповідального ви-

[4] European Parliament. Press Release "Artificial Intelligence Act: MEPs adopt landmark law" of 13.03.2024. Available at: https://www.europarl.europa.eu/news/en/press-room/20240308IPR19015/artificial-intelligence-act-meps-adopt-landmark-law

[5] Draft Framework Convention on artificial intelligence, human rights, democracy and the rule of law. Available at: https://rm.coe.int/-1493-10-1b-committee-on-artificial-intelligence-cai-b-draft-framework/1680aee411

користання ШІ в цілях оборони і безпеки та захист від загроз зловмисного використання ШІ державними та недержавними акторами[6] Це підкреслює глобальну тенденцію до інтеграції ШІ у військові стратегії та необхідність міжнародної співпраці та регулювання.

Питання застосування ШІ у військовій сфері спонукає держави до обговорення та ухвалення спільних рішень щодо рекомендаційних норм у цій сфері. Зокрема, на саміті «Відповідальний штучний інтелект у військовій сфері» (REAIM 2023), що відбувся у лютому 2023 року в Гаазі, було ухвалено Політичну декларацію про відповідальне використання ШІ та автономії у військових цілях, спрямовану на формування міжнародного консенсусу щодо відповідальної поведінки та державного управління розробленням, розгортанням і використанням військового ШІ. Станом на 12 лютого 2024 року зазначену декларацію підтримали 54 держави, зокрема країни G7 (США, Японія, Німеччина, Велика Британія, Франція, Італія, Канада) та Україна.[7]

Понад те, 21 березня 2024 року Генеральна Асамблея ООН прийняла Резолюцію A/78/L.49 «Використання можливостей безпечних, надійних і таких, що заслуговують на довіру, систем штучного інтелекту для сталого розвитку», якою закликала держави до розробки міжнародних принципів для розв'язання ризиків та збільшення переваг використання штучного інтелекту (ШІ). Це перша в історії резолюція, прийнята ООН з питань штучного інтелекту (ШІ), і тому вона є важливою віхою в його регулюванні. Резолюція підкреслює загрози, які несе в собі ця технологія, коли вона використовується з метою заподіяння шкоди, а також визнає, що за відсутності гарантій ШІ ризикує призвести до порушення прав людини, посилити упередження і поставити під загрозу захист персональних даних. Відтак, державам-членам та зацікавленим сторонам варто «утримуватися або припинити використання систем штучного інтелекту, які не можуть функціонувати відповідно до міжнародного права прав людини або які створюють надмірні ризики для реалізації прав людини».[8]

Підсумовуючи зазначимо, що використання технологій ШІ безумовно має низку переваг. Водночас існують певні ризики, пов'язані з неналежним, неконтрольованим або недобросовісним (зловмисним) використанням систем ШІ, та їхнім негативним впливом на права людини. Зазначені ризики жодним чином не применшують переваг і цінності технологій ШІ, а лише підкреслюють необхідність подальшої міжнародної співпраці та формування глобального консенсусу щодо майбутньої розробки та впровадження безпечних систем ШІ, орієнтованих на дотримання прав людини. Це є актуальним питанням й в контексті розробки та впровадження ШІ в оборонній сфері, оскільки ця сфера наразі ще розвивається, а тому точні зобов'язання та обмеження щодо використання ШІ все ще залишаються неконкретизованими та нечіткими. З іншого боку відсутність чіткої регламентації створює ризики недотримання ключових принципів та гарантій використання ШІ у військовій справі.

---

6 NATO. «Summary of the NATO Artificial Intelligence Strategy» of 22.10.2021. Available at: https://www.nato.int/cps/en/natohq/official_texts_187617.htm

7 US Department of State. Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy. Available at: https://www.state.gov/political-declaration-on-responsible-military-use-of-artificial-intelligence-and-autonomy/

8 United Nations General Assembly, Resolution A/78/L.49 "Seizing the opportunities of safe, secure and trustworthy artificial intelligence systems for sustainable development". Available at: https://documents.un.org/doc/undoc/ltd/n24/065/92/pdf/n2406592.pdf?token=61ndADmJNZ37qDDjhG&fe=true

# II. ШТУЧНИЙ ІНТЕЛЕКТ (ШІ) ТА ПРАВА ЛЮДИНИ

Системи ШІ здатні аналізувати та обробляти велику кількість інформації, автономно приймати рішення, розпізнавати загрози та застосовуватися для інших завдань. Водночас використання технологій ШІ, не зважаючи на низку переваг, несе й певні ризики у контексті гарантування прав людини. В цілому, технології ШІ можуть негативно впливати на право на життя, право на приватне життя та право на свободу вираження поглядів, а також інші основоположні права людини. Відтак важливим завданням є забезпечення належних гарантій, які б унеможливили порушення прав людини при використанні таких технологій, в тому числі у військовій справі.

Незважаючи на відсутність специфічного правового регулювання у контексті використання військового ШІ, потрібно зважати на те, що використання будь-яких новітніх технологій, які мають вплив на основоположні права та свободи людини, має відповідати міжнародним стандартам та низці критеріїв, які застосовуються для оцінки будь-якого втручання в права людини.

При розгляді справ про порушення прав людини під час збройного конфлікту[9] разом з міжнародним правом прав людини (МППП) підлягає застосуванню міжнародне гуманітарне право (МГП), яке виступає як *lex specialis*, тобто як спеціальні норми по відношенню до міжнародних стандартів у галузі прав людини, що доповнюють, але водночас не замінюють їх. Це корелює й з декларацією (застереженням) Мартенса[10] – положенні, яке відсилає до принципів гуманності і моралі, вимог суспільної свідомості.

Зауважимо, що Конвенція про захист прав та основоположних свобод (ст. 15), як і Міжнародний пакт про громадянські та політичні права (ст. 4) дозволяють певною мірою обмежувати окремі права під час війни або іншої надзвичайної ситуації, що «загрожує життю нації», проте будь-яке обмеження прав під час надзвичайної ситуації має носити винятковий та тимчасовий характер і бути обмеженим «тими межами, яких вимагає гострота становища». Водночас деякі права, серед іншого, право на життя чи заборона катувань, нелюдського чи такого, що принижує гідність, поводження або покарання, не підлягають обмеженням.

Нижче розглянемо на які права людини може впливати використання технологій ШІ в безпековій сфері.

---

[9] У міжнародному праві використовується юридичний термін «збройний конфлікт», який не передбачає обов'язкового формального акту оголошення війни та може бути як міжнародного, так і неміжнародного характеру. Міжнародний збройний конфлікт виникає коли одна держава застосовує свої збройні сили проти іншої держави. Норми МГП застосовуються від початку збройного конфлікту, при цьому не має значення чи було формально оголошено війну, факт її визнання/невизнання, а також інтенсивність чи тривалість збройного протистояння.

[10] Декларація Мартенса відображена в Гаазьких конвенціях про закони та звичаї сухопутної війни 1899 та 1907 років

## і. **Право на життя.**

Право на життя є абсолютною цінністю і передумовою здійснення всіх інших прав. Ключові міжнародно-правові акти наголошують на тому, що право на життя є невід'ємним правом кожної людини, ніхто не може бути свавільно позбавлений життя.[11] Важливість права на життя, необхідність його захисту, гарантування та реалізації є беззаперечною і відступ від цього права не допускається навіть під час війни чи іншої надзвичайної ситуації. Водночас за певних обставин право на життя все ж може бути правомірно обмежено, втім це не виключає обов'язку держави дотримуватися своїх зобов'язань щодо захисту права на життя навіть в умовах збройного конфлікту.

Питання щодо захисту права на життя під час збройних конфліктів перш за все нормами МГП, хоч норми МППП не перестають застосовуватися. МГП становить певні мінімальні стандарти в області прав людини у контексті збройних конфліктів, відступ від яких є неприпустимим за жодних обставин. Варто зауважити, що МГП покладає низку зобов'язань на обидві сторони збройного конфлікту, а тому не залежно від того, хто є державою агресором, обидві сторони повинні дотримуватися МГП.

Одними з основних принципів МГП при плануванні військових операцій є ***принцип пропорційності*** при визначенні цілі та ***принцип розрізнення*** цивільного населення та цивільних об'єктів від військових об'єктів. Відповідно, щоб визначити чи мало місце порушення права на життя під час при застосуванні сили в умовах збройного конфлікту, потрібно оцінити:

- пропорційність застосування сили у конкретній ситуації і мету, яку прагнула досягти держава,
- межі необхідності застосування сили та можливість застосування інших, більш безпечних способів для досягнення однієї і тієї ж мети,
- використання державою всіх доступних засобів для мінімізації ризиків під час використання сили.

Варто звернути увагу й на відповідну практику ЄСПЛ. При розгляді справ, що стосуються збройних конфліктів чи застосування сили, ЄСПЛ враховує контекст і норми міжнародного гуманітарного права при тлумаченні та застосуванні Конвенції.[12] Зауважимо, що ЄСПЛ бере до уваги статтю 1 Конвенції, згідно з якою держави-члени повинні відповідати за порушення прав і свобод, які захищає Конвенція, вчинених проти осіб, що перебувають під їхньою юрисдикцією.[13] До того ж ЄСПЛ був сформульований принцип, згідно з яким державні органи зобов'язані планувати операції, пов'язані із застосуванням сили, не тільки з урахуванням принципу пропорційності, але й таким чином, щоб мінімізувати ризик як для життя осіб, проти яких спрямована операція, так і цивільних осіб, випадкових свідків подій. Крім того, варто враховувати й те, чи була застосована сила «абсолютно необхідною» для досягнення відповідних цілей.[14] Тягар доказування «абсолютної

[11] Стаття 3 Загальної декларації прав людини 1948 року, стаття 2 Конвенції про захист прав людини і основоположних свобод 1950 року, стаття 6 Міжнародного пакту про громадянські та політичні права 1966 року

[12] Hanan v. Germany [GC], no.4871/16, §199, 16 February 2021

[13] Ilaşcu and Others v. Moldova and Russia [GC], no. 48787/99, § 311, ECHR 2004-VII

[14] McCann and Others v. the United Kingdom, 27 September 1995, §§ 194, 201, Series A no. 324; Andronicou and Constantinou v. Cyprus, 9 October 1997, § 171, Reports of Judgments and Decisions 1997-VI

необхідності» застосування сили перекладається на державу. Крім того, розглядаючи справу щодо застосування сили державою зі смертельними наслідками, держава зобов'язана вжити адекватних і необхідних заходів для того, щоб дослідити власні дії з точки зору дотримання гарантій статті 2 ЄКПЛ та провести ефективне розслідування у випадку ймовірного порушення права на життя. Розслідування має бути ефективним у тому сенсі, що воно здатне привести до визначення того, чи була застосована сила виправданою за конкретних обставин, а також до виявлення та покарання винних.[15]

Отже, ЄСПЛ наголошує на важливості врахування таких аспектів:

- **Відповідальність держав за ЄКПЛ**. У разі якщо держава діє поза межами власної території, ЄСПЛ розглядає питання юрисдикції держав і концепцію "ефективного контролю" над певною територією.
- **Планування та підготовка воєнних операцій**. ЄСПЛ аналізує, як держави планують та контролюють воєнні операції, звертаючи увагу на пропорційність та необхідність застосування сили зі смертельними наслідками, захист мирного населення, а також недбалість у виборі вжитих заходів.
- **Обов'язок розслідування порушень ЄКПЛ**. ЄСПЛ вимагає проведення ефективного розслідування випадків порушень прав людини, включаючи випадки застосування непропорційної сили, які могли відбутися в умовах збройного конфлікту.

Беззаперечно, впровадження технологій ШІ у військовій сфері надають перевагу на полі бою і здатні суттєво змінювати хід воєнних дій. Водночас розвиток технологій ШІ сприяє використанню пристроїв, обладнаних камерами для сканування місцевості чи розпізнавання цілей, а також технологій, що дозволяють системі автономно прийняти рішення щодо обрання цілей, включаючи ураження живої сили, техніку, склади тощо. Окрім того, можлива й розробка баражуючих боєприпасів (дронів-камікадзе), при використанні яких оператор бере участь у знищенні об'єктів до того моменту, як ціль виявлена і підтверджена, після чого баражуючий боєприпас починає працювати в автономному режимі та вражає ціль, а також баражуючих боєприпаси на основі ШІ, які можуть передбачати «розумний» вибір напрямку удару без використання координат, а лише на основі спеціальних алгоритмів. Відтак під час дослідження застосування технологій ШІ у оборонній сфері важливим елементом, який слід розглянути, є те, чи відповідна система насправді автономна або просто автоматизована. Різниця полягає у тому, яким є ступінь контролю з боку людини при використанні відповідних систем.

Водночас використання роботизованих систем, автономних/напівавтономних систем озброєнь (як от БПЛА, дрони з машинним зором, рої дронів), а також летальних автономних систем озброєння (ЛАСО), які запрограмовані на ураження цілей без необхідності передачі даних між оператором і боєприпасом, підіймають низку правових та етичних міркувань щодо гарантування права на життя. У цьому аспекті постає ключове питання – чи може рішення про позбавлення життя прийматися автономними системами озброєння?

[15] Al-Skeini and Others v. the United Kingdom [GC], no. 55721/07, §§ 163-167, ECHR 2011, Hanan v. Germany, cited above, §§198-201

Подібні ситуації порушують питання щодо правомірності використання автономних летальних систем при здійсненні атак, дотримання принципу розрізнення та пропорційності. До прикладу, у звіті Ради безпеки ООН у Лівії (2021) було згадано, що автономний дрон самостійно, без будь-якого втручання оператора, вбив людину. У цій ситуації безпілотник Kargu-2, що використовує бортові камери та ШІ для ідентифікації цілей, «стежив» за солдатами, коли вони відступали, та завдав удару без спеціального наказу. Варто зауважити, що у звіті нічого не сказано про те, чи використовувалися ударні безпілотники Kargu-2 незаконно, хоча в ньому й зафіксовані різні порушення МГП та МППП в інших контекстах (§§32-55).[16]

Частково питання використання летальної автономної зброї врегульовано як нормами МГП, згідно з яким право сторін збройного конфлікту обирати методи або засоби ведення війни не є необмеженим, так і МППП, що обмежує можливість застосування озброєння, яке може призвести до порушення прав людини.

З одного боку, МГП встановлює заборони та обмеження у виборі методів і засобів ведення воєнних дій для сторін, що воюють. Серед іншого, це заборона вбивати та завдавати поранення супротивнику, якщо він полонений, втратив бойову спроможність, склав зброю і не становить загрози (hors de combat), заборона вдаватися до нападів невибіркового характеру,[17] заборона використовувати зброю, яка може призвести до надмірних ушкоджень чи зайвих страждань, а також заборона використовувати таку зброю та методи ведення бойових дій, що можуть призвести до невиправданих втрат.

Вагоме значення у контексті розробки нового озброєння, зокрема й автономного озброєння, має стаття 36 Першого додаткового протоколу до Женевських конвенцій, яка передбачає, що *«при дослідженні, розробці, придбанні або прийнятті на озброєння нової зброї, засобів або методів ведення війни Висока Договірна Сторона зобов'язана визначити, чи не буде її застосування за деяких або за всіх обставин заборонено цим Протоколом або будь-якою іншою нормою міжнародного права, що застосовується до Високої Договірної Сторони».*

Тож створюючи будь-яке новітнє озброєння держави повинні оцінити чи її розробка, створення, впровадження і застосування не призведе до порушення МГП, зокрема чи має вона антигуманні вражаючі властивості, чи не призведе вона до надмірних ушкоджень чи зайвих страждань, чи має вона невибіркову дію, чи може призвести до неминучої смерті. Водночас при оцінці відповідності принципам пропорційності та розрізнення варто визначити наскільки точно системи озброєння здатні ідентифікувати законні цілі та їх типи, відрізняти комбатантів від некомбатантів, а також розрізняти об'єкти, що використовуються у військових цілях від цивільних об'єктів.

---

[16] UN Security Council, Final report of the Panel of Experts on Libya established pursuant to Security Council resolution 1973 (2011), S/2021/229, 8 March 2021. Available at: https://www.securitycouncilreport.org/un-documents/document/s-2021-229.php ICRC. Case study "Libya, The Use of Lethal Autonomous Weapon Systems". Available at: https://casebook.icrc.org/case-study/libya-use-lethal-autonomous-weapon-systems

[17] До нападів невибіркового характеру належать напади, які не спрямовані на конкретні військові об'єкти; при яких застосовуються методи або засоби ведення воєнних дій, які не можуть бути спрямовані на конкретні військові об'єкти; або при яких застосовуються методи або засоби ведення воєнних дій, наслідки яких не можуть бути обмежені, як це вимагається згідно з Додатковими протоколами до Женевських конвенцій від 12 серпня 1949 року; напад невибіркового характеру, який може спричинити такі втрати серед цивільного населення та такий збиток цивільним об'єктам, що будуть непорівнянними з досягненням необхідної військової переваги над противником.

В основі більшості правових, моральних та інших кодексів лежить припущення, що коли на кону стоїть рішення позбавити життя або піддати людей іншим тяжким наслідкам, право приймати рішення має належати людині. Декларація Мартенса, як одна з ключових норм МГП, безпосередньо вимагає застосування «принципу гуманності» у збройних конфліктах до всіх ситуацій, не врегульованих міжнародним правом, а також відсилає до загальнолюдських моральних вимог і цінностей, які регулюють поведінку сторін під час війни, розробки нових видів зброї та використанні засобів і методів ведення війни. Водночас Гаазька конвенція (IV) про закони і звичаї війни на суходолі передбачає, що комбатанти знаходяться під командуванням особи, відповідальної за своїх підлеглих. Отже, військові командири, які планують військові операції, завжди несуть відповідальність за застосування засобів чи методів ведення війни, в тому числі при використанні АСО, які працюють без нагляду і контролю людини, у разі якщо їх застосування призвело до порушення МГП.[18] Водночас оператори АСО при розгортанні, налаштуванні та використанні таких систем несуть всі ті ж самі зобов'язання за МГП, що і при використанні будь-якого іншого озброєння, серед іншого, скеровувати атаки лише на військові об'єкти та мінімізувати очікувану шкоду для цивільного населення.

Поява новітніх типів зброї завжди викликає занепокоєність та має наслідком спроби обмежити чи заборонити її застосування. В контексті автономного озброєння варто пам'ятати, що його особливість полягає не в застосуванні нового методу чи засобу ураження цілі, а саме у застосуванні нового способу прийняття рішення про ураження певних цілей, ступеню і типу взаємодії з оператором. Водночас ШІ можливо запрограмувати так, щоб він діяв відповідно до принципів МГП, хоч це і не виключає всіх потенційних ризиків при використанні автономної зброї. Ймовірно спроби повністю заборонити автономну зброю навряд чи матимуть успіх, але серед держав та міжнародної спільноти поступово формується розуміння того, що ризики, пов'язані з військовим ШІ, вимагають від людини-оператора збереження активного (позитивного) контролю над застосуванням АСО, що забезпечить етичне та відповідальне застосування такої зброї.

## ii. **Заборона катувань.**

Заборона катувань є однією з абсолютних, імперативних норм міжнародного права, що відображена у багатьох міжнародно-правових актах та договорах, включаючи Загальну декларацію прав людини, МПГПП, ЄКПЛ, Конвенцію проти катувань та інші. Заборона катувань також виступає одним з основних принципів МГП та закріплена у статті 3 кожної із чотирьох Женевських конвенцій 1949 року. Використання військового штучного інтелекту (ШІ) повинно відповідати міжнародним стандартам прав людини, включаючи заборону катувань, яка не має винятків і застосовується в усіх обставинах, включаючи війну чи надзвичайний стан.

Як було зауважено вище, сторони конфлікту не є необмеженими у виборі засобів та методів ведення воєнних дій і розробка та впровадження новітнього озброєння має відповідати забороні використовувати зброю, яка може призвести до надмірних ушкоджень чи зайвих страждань. У цьому аспекті слід констатувати, що машинний розум не має (або ж має вкрай обмежені) можливості для розпізнавання емоцій людини, а тому зали-

[18] З урахуванням статті 57 (2) (a) Додаткового протоколу до ЖК 1949 року, ті хто планують напад або приймає рішення про його здійснення, несуть за нього пряму відповідальність.

шається відкритим питання чи може система ШІ, яка використовується у нових видах зброї, виміряти або оцінити рівень «надмірних ушкоджень чи зайвих страждань». Це питання вкотре підкреслює необхідність збереження контролю над АСО з боку оператора. Водночас відповідальність за дотримання прав людини лежить не тільки на операторах ШІ, але й на розробниках та військовому командуванні, яке використовує ці технології. Саме вони повинні забезпечити, що використання ШІ відповідає етичним стандартам та відповідним міжнародним зобов'язанням, включаючи заборону катувань.

Варто звернути увагу й на те, що технології ШІ теоретично можуть бути застосовані для моніторингу за порушенням прав людини, адже ШІ може аналізувати великі обсяги даних, включаючи відео- та аудіозаписи, щоб виявляти випадки катувань або нелюдського чи такого, що принижує гідність поводження або покарання, якому в умовах збройного конфлікту в Україні піддаються як військовополонені, так і цивільні.

## iii. **Заборона дискримінації.**

Використання озброєння на основі ШІ безумовно має низку переваг, серед іншого, при розпізнаванні, обранні та враженні цілей, а також у контексті прогнозування та моніторингу загроз. Втім класифікація об'єктів зазвичай відбувається за допомогою машинного навчання, тобто здатності реагувати на зміну обставин і цілей, вживати певних дій та корегувати поведінку відповідно до накопиченого досвіду. При створені система на основі ШІ завжди має перевірятись на відповідність основоположним принципам, одним із яких є заборона дискримінації. Однак можуть траплятися випадки, коли система буде наповнюватись упередженою інформацією, а її результати призводитимуть до алгоритмічної дискримінації, тобто прийняте рішення буде несправедливо впливати на певні групи людей. Крім того, при здійснені прогнозування за допомогою ШІ, відповідні алгоритми можуть не враховувати дискримінаційні фактори, а тому можуть посилити існуючі несправедливості чи упередження або створити нові.

Таким чином, використання помилкового алгоритму або програмного забезпечення, що призводить до дискримінації та упередженості за будь-якою ознакою, матиме наслідком порушення прав людини.

Що стосується використання автономних озброєнь, то ключовим питанням є здатність такого озброєння відрізняти легітимні військові цілі від захищених цивільних осіб та цивільних об'єктів, проводити оцінку пропорційності атаки, яка не повинна призводити до дискримінаційних атак. До прикладу, автономні системи озброєння можуть заподіяти шкоду захищеним об'єктам, як от цивільним особам, адже система наведення ідентифікуватиме їх не як захищену ціль, а як дозволену.

Тож аби відповідати принципу пропорційності автономна зброя повинна оцінювати потенційну побічну шкоду від застосування зброї та порівняти її з очікуваною військовою перевагою, яку можна отримати у разі здійснення атаки. Така оцінка має враховувати відповідний контекст, а тому потребує розробки відповідних алгоритмів машинного навчання, які б уміли визначати стратегічну цінність певних об'єктів на полі бою на основі наявної інформації.

Крім того, варто пам'ятати, що зброя, яка не здатна розрізняти або обмежувати наслідки своїх атак, заборонена міжнародним звичаєвим правом.[19] Відповідно, як командири, так і оператори зобов'язані робити все можливе, щоб переконатися, що певні цілі є законними військовими об'єктами. Більше того, вони повинні скасувати або призупинити атаку, якщо стає очевидним, що певна ціль не є військовим об'єктом.

Окремо варто зауважити і на існуванні операційних ризиків, які виникають через питання надійності, вразливості та безпеки систем ШІ. У цьому аспекті вкрай важливим є забезпечення належного рівня кібербезпеки.

## iv. Право на приватне життя (право на приватність).

У контексті гарантування права на приватне життя варто звернути увагу на системи та технології розпізнавання обличчя. У повсякденному житті такі системи широко впроваджуються та використовуються, як, наприклад, Європейська система спостереження за кордонами (Eurosur), яка використовується для посилання охорони державних кордонів шляхом боротьби з нелегальною міграцією і транскордонною злочинністю.

Зауважимо, що однією із законних підстав втручання у право на приватність є забезпечення інтересів національної безпеки. Дійсно, у багатьох випадках захист інтересів національної безпеки виправдовуватиме втручання в права людини, однак межі розсуду держав при втручанні у права людини не є безмежними і держава має забезпечити справедливий баланс між правами особи та інтересами національної безпеки. Тому розглядаючи *«національну безпеку»* як багатоаспектне явище, що відображає стан захищеності життєво важливих інтересів особи, суспільства і держави від реальних та потенційних загроз, та *«інтереси національної безпеки»* як підставу для обмеження прав людини, варто пам'ятати про так званий трискладовий тест, вироблений у практиці ЄСПЛ, який передбачає, що втручання у основоположні права та свободи людини повинно мати законну підставу, переслідувати законні цілі та бути необхідним у демократичному суспільстві та пропорційним до цілей, що переслідуються.

У цьому аспекті ЄСПЛ наголошував, що таємний нагляд за громадянами, у відповідних випадках, є необхідним в демократичному суспільстві в інтересах національної безпеки та/або запобігання бунтів або злочинів, тобто розглядається як необхідний засіб оборони для захисту демократичної держави. Втім незалежно від прийнятої системи нагляду, мають існувати адекватні та ефективні гарантії проти зловживань.[20] До того ж у справі *Big Brother Watch and Others v the United Kingdom*, ЄСПЛ, розглядаючи питання використання технологій масового спостереження, вказав, що будь-які заходи спостереження повинні бути належним чином обґрунтовані та повинні впроваджуватися лише компетентним органом у чітко визначених випадках, підлягати незалежному нагляду, а відповідна особа повинна бути повідомлена про застосування таких технологій.[21] У справі *Škoberne v. Slovenia* ЄСПЛ також дійшов висновку, що систематичний, загальний та невибірковий спосіб зберігання, доступу та обробки персональних даних, зокрема да-

[19] Customary IHL. Rule 71. Weapons That Are by Nature Indiscriminate. Available at: https://ihl-databases.icrc.org/en/customary-ihl/v1/rule71
[20] *Klass and Others v. Germany*, 6 September 1978, §§ 42-50, Series A no. 28
[21] Big Brother Watch and Others v the United Kingdom, [GC], nos. 58170/13 and 2 others, §§ 332-339, 25 May 2021

них про зв'язок, порушує статтю 8 Конвенції.[22] У цьому аспекті Суд ЄС дійшов подібних висновків, наголосивши, що загальна та невибіркова передача персональних даних, зокрема даних про трафік і даних про місцезнаходження, є забороненою, навіть якщо це здійснюється з метою захисту національної безпеки.[23]

Примітно, що у нещодавній справі ***Glukhin v. Russia*** ЄСПЛ зауважив, що використання технологій розпізнавання обличчя може за певних обставин призводити до порушення статті 8 Конвенції, яка гарантує право на захист приватного та сімейного життя.[24]

Відповідно, при впровадженні технологій ШІ держава повинна створити належні гарантії проти ризику зловживання та дотримуватися конкретних правил та принципів у використанні нових технологій, включаючи технології масового спостереження, перехоплення даних та розпізнавання облич, які б запобігали свавільному втручанню у права людини. Відсутність чітких орієнтирів та вимог щодо правомірного застосування технологій ШІ призводитиме до порушення принципу законності як однієї з підстав втручання у право людини на приватність та інші основоположні права.

Також ШІ може використовуватись для виявлення та протидії дезінформації. Втім, варто пам'ятати, що на сьогодні інформаційна війна стала невід'ємною складовою сучасних збройних конфліктів, які за своєю природою є гібридними і включають не тільки використання конвенційної зброї, але й, серед іншого, застосування новітніх засобів боротьби, включаючи кібертехнології, агресивну пропаганду, інформаційно-психологічні операції й вплив на громадську думку тощо. Відповідно, існує ризик недобросовісного використання технологій ШІ для інформаційних атак, поширення дезінформації та/або пропаганди.

Від початку повномасштабного вторгнення російська пропаганда неодноразово запроваджувала інформаційно-психологічні спецоперації (ІПсО) з дискредитації військового керівництва ЗСУ, а також поширювала відео з використанням технологій діпфейку (англ. deepfake), яка за допомогою алгоритмів машинного навчання здатна повністю відтворити зовнішній вигляд певної людини. До прикладу, неодноразово були використані ІПсО, в тому числі з відео, де президент України В. Зеленський нібито анонсує капітуляцію чи закликає українців припинити боротьбу та скласти зброю. Крім того, 7 листопада 2023 року було опубліковано відео, в якому чинний на той час головнокомандувач Збройних сил України В. Залужний нібито звинувачував українську владу у тому, що В. Зеленський намагається його ліквідувати, що він здає Україну та провалив контрнаступ.[25]

Водночас ШІ використовується й для виявлення та протидії кібератакам, що дозволяє автоматизуючи виявлення та реагування на кібератаки і забезпечує більш ефективний захист інформаційних систем. Втім, знову ж таки, у сучасних збройних конфліктах технології ШІ можуть застосовуватися й недобросовісно – задля здійснення кібератак, виявлення вразливостей у мережах або навіть для розробки нових шкідливих програм. До прикладу, у грудні 2023 року російські хакери здійснили кібератаку на систему оператора зв'язку «Київстар». Стверджується, що ця атака спричинила «катастрофічні» руйнування

---

[22] Škoberne v. Slovenia, no. 19920/20, §§ 141-147, 15 February 2024

[23] Court of Justice of the European Union, Case C-623/17, *Privacy International v. Secretary of State for Foreign and Commonwealth Affairs and Others*, **§§ 80-82,** Judgment of the Court (Grand Chamber) of 6 October 2020

[24] Glukhin v. Russia, no. 11519/20, §§ 74-77, 04 July 2023

[25] Центр протидії дезінформації. Стаття «Для чого російська пропаганда використовує діпфейк В.Залужного» від 09.11.2023. Доступно за посиланням: https://cpd.gov.ua/main/dlya-chogo-rosijska-propaganda-vykorystovuye-dipfejk-v-zaluzhnogo/

та мала на меті завдати психологічного удару й отримати розвідувальну інформацію. Водночас ця кібератака хоч і не мала серйозного ефекту на військові комунікації, але значно вплинула на цивільне населення, адже на декілька днів унеможливила користування послугами мобільного зв'язку та інтернету для близько 24 млн абонентів. Британська розвідка охарактеризувала цю кібератаку як одну з найбільш руйнівних, адже кібератака порушила роботу сирен повітряної тривоги та деяких банків, банкоматів, терміналів торгових точок, а також постраждали державні ресурси та екстрені служби України.[26]

Відтак важливо приділяти належну увагу розвитку заходів захисту від кіберзагроз для систем з використанням ШІ чи кіберзагроз у військових мережах, а також захисту інформації та даних від кібератак та кібершпигунства, що можуть призвести до неправомірного витоку інформації та персональних даних.

[26] Forbes. Стаття «Хакери перебували в системі «Київстару» з травня 2023 року. СБУ розкрила деталі кібератаки» від 04.01.2024. Доступно за посиланням: https://forbes.ua/news/khakeri-perebuvali-v-sistemi-kiivstar-z-travnya-2023-roku-sbu-04012024-18307 Стаття «Якою була атака хакерів на «Київстар» та як відновлювалась компанія» від 19.03.2024. Доступно за посиланням: https://dou.ua/lenta/news/kyivstar-cyber-attack-restoration/ Ministry of Defence of the United Kingdom. Intelligence update on the situation in Ukraine, 16 December 2023. Available at: https://twitter.com/DefenceHQ/status/1735993232247476720

# III. ПРАКТИЧНІ АСПЕКТИ, ПОВ'ЯЗАНІ З ВИКОРИСТАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ (ШІ) У ВІЙСЬКОВІЙ СПРАВІ

**«…Вже сьогодні в Україні Штучний інтелект активно використовують у різних напрямах. Особливо важливим є використання ШІ у сфері військових технологій. Він допомагає фіксувати переміщення техніки та особового складу окупантів, збивати ворожі ракети, ефективніше наводити БПЛА на цілі тощо…»** - *Михайло Федоров, Міністр цифрової трансформації України*

На думку експертів, війна в Україні – це своєрідна «перша світова війна з використанням технологій». ШІ активно застосовується для ведення війни за допомогою програмного забезпечення, використання дронів, для розпізнавання і розшифрування супутникових знімків, розпізнавання цілей на полі бою і прогнозування засобів, якими вони можуть бути уражені, для розпізнавання облич та ідентифікації військових злочинців або виявлення, ідентифікації жертв війни та повернення тіл загиблих їхнім сім'ям тощо.

Дійсно, Збройні Сили України задіюють технології біометричної ідентифікації, роботів-саперів, інструменти пошуку підозрілих осіб та інструменти для аналізу супутникових знімків, технології автоматизованого розпізнавання облич, транспортних засобів, об'єктів із зображень, що отримуються з дронів або відеоспостереження тощо.

Відоме американське видання National Defense, яке займається висвітленням питань розвитку військово-промислового комплексу США, оцінило збройний конфлікт в Україні як «живу лабораторію для війни штучного інтелекту».[27]

Українські ударні безпілотники великої дальності «Лютий» наводяться на ціль з високою точністю завдяки системі «машинного зору». Такі дрони у реальному часі можуть коригувати напрямок польоту, знаходити та вражати ворожі об'єкти. ШІ також робить українські безпілотники нечутливими до систем радіоелектронної боротьби, які здатні збивати дрони з завданого курсу. ШІ-дрони можуть стежити за великими територіями, виявляти підозрілі дії та відстежувати людей або транспортні засоби в режимі реального часу.

Іншим прикладом використання ШІ у військовій справі є програмний комплекс **Griselda**, який використовується для збору розвідувальних даних – система збирає, аналізує, перевіряє на вірогідність і робить звіти на основі даних та інтегрована з системами «Дельта», «Кропива», «Броня», якими користуються українські військові. Варто звернути увагу й на одну з ключових розробок **UA Dinamics**, які створили БпЛА Punisher, а саме – балістичний калькулятор. Це спеціально розроблене програмне забезпечення, який на основі завантажених у нього даних про точку розміщення цілі, набір метеоданих та інших параметрів здійснює скидання боєзапасу, коригуючись штучним інтелектом.[28]

---

[27] National Defence Magazine. Article "Ukraine A Living Lab for AI Warfare" of 24.03.2023. Available at: https://nationaldefensemagazine.org/articles/2023/3/24/ukraine-a-living-lab-for-ai-warfare

[28] Ucluster. "Рої дронів: Тренди українських БпЛА". Доступно за посиланням: https://ucluster.org/blog/2023/09/roji-droniv-trendy-ukrajinskyh-bpla/

Понад те, технологія розпізнавання облич **Clearview AI** стала «таємною зброєю» України у війні проти Росії. На початку повномасштабного вторгнення рф на територію України, розробники американського сервісу **Clearview AI** запропонували українським урядовцям спробувати цю технологію в дії. Система має доступ до бази з понад 30 млрд. зображень, зокрема близько 2 млрд. фото зібрані з російської соціальної мережі «ВКонтакте». На даний час цим сервісом користуються близько 18 українських відомств, в тому числі Державна прикордонна служба України і Національна поліція України.[29]

Система розпізнавання обличчя – це технологія, яка здатна ідентифікувати особу на цифровому зображенні та порівняти риси обличчя заданого зображення з обличчями, які зберігаються в базі даних. Система **Clearview AI** використовується в Україні для виявлення російських воєнних злочинців, зловмисників на контрольно-пропускних пунктах, переслідування членів проросійських формувань і українських колабораціоністів, і навіть для пошуку депортованих дітей.

Після деокупації українських регіонів ШІ використовували для ідентифікації загиблих. За словами міністра цифрової трансформації Михайла Федорова, - «Україна використовує програмне забезпечення **Clearview AI** для розпізнавання облич, щоб ідентифікувати тіла російських солдатів, які загинули в бою, та інформувати їхні сім'ї про їх загибель».

Проте використання ШІ, зокрема у воєнний час, може привести до порушення фундаментальних прав людини, закріплених в основних міжнародно-правових актах. Технології ШІ, подібні **Clearview AI**, здійснюють збір персональних даних особи автоматично, без її інформування про цей процес та за відсутності згоди на обробку даних, що є порушенням права особи на приватність, яке захищається національним і міжнародним правом.

Крім того, масовий моніторинг, збір, зберігання, аналіз конфіденційних персональних і біометричних даних особи і використання матеріалів без обґрунтованої підозри у вчиненні кримінального правопорушення можна вважати невибірковим масовим наглядом. База даних **Clearview AI**, наприклад, постійно та в автоматичному режимі акумулює зображення з усіх доступних джерел, тобто користувачі сервісу можуть відстежувати діяльність, пересування, соціальні зв'язки та інші конфіденційні дані стосовно запитуваної особи.

Деякі країни, зокрема Велика Британія, Канада, Франція, Італія та Австралія, визнали незаконним збір персональних, біометричних та геолокаційних даних за допомогою системи **Clearview AI**, внаслідок чого компанія мала сплатити значні суми штрафів через порушення правил захисту персональних даних і конфіденційності. Великі компанії, в тому числі YouTube, Facebook, Google та Twitter відмовляються співпрацювати з цим стартапом, тому що для ідентифікації особи система **Clearview AI** збирає величезну кількість зображень з соціальних мереж, що призводить до ризиків порушення конфіденційності.

Американська корпорація **Palantir –** ще одна технологічна компанія, яка розробляє системи для аналітики даних за допомогою штучного інтелекту і використовує ШІ у військових цілях. Основним продуктом компанії є модульна система Palantir Edge AI – набір універсальних алгоритмів, які налаштовуються під окремі завдання з різними наборами даних.

[29] **Портал МВС. Повідомлення «CEO американської компанії Clearview AI, продукт якої ідентифікував окупантів та зрадників, продовжить співпрацювати з МВС» від 13.04.2022. Доступно за посиланням:** https://mvs.gov.ua/uk/news/ceo-amerikanskoyi-kompaniyi-clearview-ai-produkt-iakoyi-identifikuvav-okupantiv-ta-zradnikiv-prodovzit-spivpraciu-z-mvs

Для візуалізації місцевості та розпізнавання цілей на полі бою система **Palantir** кожного дня обробляє великий масив супутникових зображень певної місцевості, після чого її особливості відображаються на картах. Це дає змогу відслідкувати, де знаходиться ворог і яку зброю найбільш ефективно застосовувати проти позицій противника. При OSINT-розслідуваннях (Open Source Intelligence – збір інформації з відкритих джерел), штучний інтелект **Palantir** може допомогти при викритті воєнних злочинів і воєнних злочинців.

«Щоб уявити, як це працює на практиці, подумайте про успіх України у відвоюванні Херсону на узбережжі Чорного моря. Українці мали точні розвідувальні дані про те, куди рухаються росіяни, і змогли завдати точного удару вогнем з великої відстані. Це стало можливим завдяки розвідданим про місцезнаходження ворога, які оброблялись за межами країни, а потім передавались командирам на місцях...», – написано у статті «Як алгоритм перехилив чашу терезів в Україні»,[30] яка розміщена на сайті The Washington Post.

В березні 2024 року Міністерство економіки України підписало угоду з технологічною компанією **Palantir** щодо гуманітарного розмінування території України.[31] За словами представників Мінекономіки, наразі потенційно забрудненими є 156 000 квадратних кілометрів землі, а в зоні ризику перебуває понад 6 млн. українців. Угода про розмінування регіонів України містить конкретні положення щодо оцифрування операцій гуманітарного розмінування, автоматизації процесів, розширення цифрових можливостей для координації вивільнення та оцінки земель, управління ризиками в протимінній діяльності, прийняття рішень на базі платформи штучного інтелекту **Palantir AI**.

«Платформа **Palantir AI** аналізуватиме інформацію та надаватиме рекомендації щодо оптимізації процесів. Наприклад, зможе порадити, враховуючи всі дані, як найбільш ефективно провести очищення конкретної території — за допомогою нових методів розмінування (дрони), чи використовуючи традиційні методи (підрозділи спеціалістів). Кінцева мета — розміновувати території швидше та з меншими витратами», — повідомили у Мінекономіки.

### Що важливіше: приватність чи безпека?

Право на приватність (right to privacy) належить до основоположних прав і свобод людини. Проте потужне програмне забезпечення **Palantir**, система розпізнавання облич **Clearview AI** і інші подібні технології ШІ можуть призводити до порушення права на приватність і використовуватись в сумнівних цілях. Такі системи не мають бути технологіями тотального спостереження, а їх використання по факту події, яку потрібно проаналізувати, повинні зберігати право особи на приватність та захист персональних даних.

У 2019 році газета The Post писала, що програмне забезпечення **Palantir** застосовувалось державними службами для відстеження нелегальних іммігрантів, внаслідок чого виникає питання: чи не може компанія «бачити занадто багато» за допомогою своїх інструментів?

---

[30] The Washington Post. "How the algorithm tipped the balance in Ukraine" of 19.12.2022. Available at: https://www.washingtonpost.com/opinions/2022/12/19/palantir-algorithm-data-ukraine-war/

[31] Офіційний сайт Міністерства економіки України. «Автоматизація процесів розмінування та використання ШІ». Доступно за посиланням: https://www.me.gov.ua/News/Detail?lang=uk-UA&id=f8007eec-0057-4ef1-8205-3b1e370e0a4d&title=MinisterstvoEkonomikiTaPalantirPidpisaliUgoduProPartnerstvo

Хоча закони про захист персональних даних прийняті вже в більшості країн Європи, в Україні досі немає належного регулюючого законодавства і якісного підходу до роботи зі штучним інтелектом, зокрема з технологіями ШІ, які застосовуються у військових цілях.

Основним законом в сфері захисту персональних даних осіб залишається Закон України «Про захист персональних даних» (далі - Закон),[32] який встановлює вичерпний перелік підстав щодо обробки персональних даних, і однією з найбільш поширених підстав є саме наявність згоди суб'єкта персональних даних як обов'язкова умова для збору та обробки таких даних. Це є вкрай важливим в аспекті збору персональних даних в воєнних цілях за допомогою технологій ШІ, оскільки такий збір даних проводиться автоматично, без згоди особи.

Відповідно до згаданого Закону, органи державної влади, місцевого самоврядування, установи, організації та інші володільці та розпорядники персональних даних зобов'язані забезпечити захист цих даних від випадкової втрати, знищення, незаконної обробки, незаконного доступу до персональних даних. Оброблятися повинні лише ті персональні дані, використання яких необхідно для досягнення конкретної законної мети.

Водночас допускається обробка персональних даних без згоди особи в інтересах національної безпеки. Це передбачено статтею 25 Закону, згідно з якою обмеження дії статей 6, 7 і 8 цього Закону, які стосуються вимог щодо обробки персональних даних та прав суб'єкта даних, може здійснюватися у випадках, передбачених законом, наскільки це необхідно у демократичному суспільстві в інтересах національної безпеки, економічного добробуту або захисту прав і свобод суб'єктів персональних даних чи інших осіб. Тобто, як було зауважено у розділі II вище, втручання у права людини на приватність та захист персональних даних, що пов'язані й із використанням технологій ШІ, повинні мати законну підставу, переслідувати законну мету, якою у контексті військової справи виступає національна безпека та оборона, та бути необхідним і пропорційним до мети, що переслідується. Крім того, законодавство повинно передбачати належні гарантії від свавілля та зловживань у цьому контексті, що можуть призвести до порушення відповідних прав людини.

Варто також звернути увагу на проєкт Закону №8153 «Про захист персональних даних» від 25.10.2022 року, який наразі перебуває на розгляді Верховної Ради України. Згаданим законопроєктом пропонується удосконалення положень щодо обробки персональних даних відповідно до сучасних стандартів захисту персональних даних, що містяться в оновленій Конвенції Ради Європи №108 (так звана Конвенція №108+) та Загальному регламенті про захист даних, що діє в ЄС. У законопроєкті запропоновано закріпити випадки, коли обробка біометричних даних суб'єктами владних повноважень є правомірною, наприклад, у разі якщо така обробка здійснюється з метою забезпечення національної безпеки, оперативно-розшукової та контррозвідувальної діяльності, протидії злочинності, підтримання громадської безпеки і порядку, економічного добробуту та прав людини. Примітно, що у проєкті Закону №8153 також надається визначення обробки даних в правоохоронних цілях, тобто обробка персональних даних правоохоронними органами, спрямована на розслідування кримінальних правопорушень, виконання кримінальних покарань; забезпечення охорони прав і свобод людини, протидії злочинності, підтри-

[32] Закон України «Про захист персональних даних» від 01.06.2010 року. Доступно за посиланням: https://zakon.rada.gov.ua/laws/show/2297-17#Text

мання публічної безпеки і порядку; відкриття та проведення досудового розслідування; **здійснення розвідувальної діяльності та забезпечення національної безпеки**. Окремо в ст. 56, 57 законопроєкту пропонується врегулювати вимоги до обробки персональних даних правоохоронними та розвідувальними органами, а також особливості реалізації прав суб'єкта даних.

Важливим у контексті гарантування права на приватність та захисту персональних даних є також забезпечення належних умов зберігання даних. До прикладу, відповідно до Постанови Кабінету Міністрів України № 263 від 12.03.2022 року «Деякі питання забезпечення функціонування інформаційно-комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів в умовах воєнного стану», відповідно до якої на період дії воєнного стану для збереження персональної і конфіденційної інформації, що міститься в державних інформаційних ресурсах і публічних електронних реєстрах, мають вживатися додаткові заходи захисту.

Відомості з реєстрів повинні розміщуватись на хмарних ресурсах або в центрах обробки даних, що розташовані за межами України; дія таких реєстрів має бути обмежена чи зупинена на територіях активних бойових дій і на тимчасово окупованих територіях тощо. На період дії воєнного стану також категорично заборонено використання хмарних ресурсів або центрів обробки даних, розташованих на тимчасово окупованій території України.

Мешканцям регіонів України, які перебувають під тимчасовою окупацією, слід бути особливо обережними при передачі конфіденційної інформації та своїх персональних даних представникам окупаційної влади. Центр протидії дезінформації РНБО України повідомляє про дії окупантів, які полягають у зборі персональних даних громадян під виглядом «перепису населення» або під час роздачі гуманітарної допомоги. Зібрані відомості можуть бути використані для залякування і переслідування українців на тимчасово окупованих територіях, зокрема це може стосуватись військовослужбовців, членів їх сімей, громадських активістів і діячів, журналістів та інших осіб.

Що стосується застосовування ШІ, то 07 жовтня 2023 року Міністерство цифрової трансформації України презентувало Дорожню карту з регулювання штучного інтелекту в Україні,[33] яка допоможе українським компаніям підготуватись до ухвалення закону – аналога AI Act Європейського Союзу, а громадянам – навчитися захищати себе від ризиків, пов'язаних з використанням ШІ. За словами Міністра цифрової інформації Михайла Федорова, - в основі впровадження регулювання ШІ лежить bottom-up підхід, який передбачає рух від меншого до більшого: спочатку бізнесу надаються інструменти для підготовки до майбутніх вимог, а після цього буде ухвалено відповідний закон. Такий підхід враховує інтереси всіх ключових стейкхолдерів і дає змогу знайти баланс між інтересами бізнесу та захистом прав громадян. Зокрема, наразі бізнес може впроваджувати добровільні кодекси поведінки щодо етичного використання ШІ. Крім того, Міністерство цифрової інформації планує публікувати рекомендації, як загальні, так і секторальні, щодо впровадження та використання ШІ.

[33] Міністерство цифрової інформації України. «Регулювання штучного інтелекту в Україні: презентуємо дорожню карту». Доступно за посиланням: https://thedigital.gov.ua/news/regulyuvannya-shtuchnogo-intelektu-v-ukraini-prezentuemo-dorozhnyu-kartu

Повертаючись до питання застосування технології **Clearview AI**, варто зауважити, що використання цієї системи, не зважаючи на переваги, які вона надає в контексті збройного конфлікту, все ж порушує норми законодавства Європейського Союзу щодо захисту персональних даних усіх осіб у межах Європейського Союзу та Європейської економічної зони, викладені у Загальному регламенті про захист даних (General Data Protection Regulation, GDPR; Regulation (EU) 2016/679)[34] щодо:

- прозорого інформування суб'єктів персональних даних про процедуру збору їх персональних даних, тобто компанія не інформує користувачів про те, що вона робить з їхніми фотографіями;
- цілей використання, тобто дані користувачів використовуються не в тих цілях, у яких вони були опубліковані в інтернеті;
- порушення права на збереження даних користувачів і гарантії приватності таких даних.

У цьому аспекті Загальний регламент про захист даних передбачає, серед іншого, що персональні дані особи повинні оброблятися законним, справедливим і прозорим чином по відношенню до суб'єкта даних; збиратися для визначених, чітких і законних цілей; оброблятися у спосіб, що забезпечує належну безпеку персональних даних, включаючи захист від несанкціонованої або незаконної обробки та від випадкової втрати (стаття 5).

Водночас занепокоєння викликає і використання систем масового відеоспостереження, як от система «Безпечне місто». У цьому контексті варто зауважити, що 20 лютого 2024 року Верховна Рада України зареєструвала *проєкт Закону №11031, спрямований на запровадження єдиної системи відеомоніторингу стану публічної безпеки*, основною метою якого є забезпечення безпеки у публічних місцях, виявлення та запобігання правопорушенням, а також встановлення осіб, підозрюваних у вчиненні злочинів або які переховуються.[35] Згаданий законопроєкт має низку дискусійних положень та проблемних аспектів, на які звертають увагу правозахисники.[36] Серед іншого, використання систем масового відеоспостереження потребує значної кількості ресурсів, а також належного рівня забезпечення безпеки та гарантій від ризику витоку персональних даних, включаючи й чутливі дані (як от біометричні дані), що є вкрай важливим в умовах триваючої збройної агресії. Крім того, хоч використання подібних систем переслідує законні цілі завжди залишається актуальним питання пропорційності втручання у права людини, що пов'язане з категоріями персональних даних, які обробляються, строками зберігання даних, вимоги інформувати особу про здійснення відеоспостереження та доволі широкої дискреції органів влади у цій сфері, що потребує належних гарантій від зловживань та ефективного механізму контролю.

Зрозуміло, що використання ШІ у військовій справі та у воєнний час надає значні переваги, такі як можливість збирати, обробляти, зберігати та аналізувати великий масив ін-

---

[34] Регламент Європейського Парламенту та Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних). Доступно за посиланням: https://zakon.rada.gov.ua/laws/show/984_008-16#Text [Текст українською]

[35] Офіційний сайт Верховної Ради України. Проект Закону про єдину систему відеомоніторингу стану публічної безпеки. Доступно за посиланням: https://itd.rada.gov.ua/billInfo/Bills/Card/43733

[36] Лабараторія цифрової безпеки. «Законопроєкт про відеомоніторинг: захист публічної безпеки чи ліцензія на масове стеження?» від 09.03.2024. Доступно за посиланням: https://dslua.org/publications/zakonoproiekt-pro-videomonitorynh-zakhyst-publichnoi-bezpeky-chy-litsenziia-na-masove-stezhennia/

формації. Технології ШІ досить прості та зручні у використанні і можуть застосовуватись для розпізнавання й розшифрування супутникових знімків і цілей, використання БпЛА для ураження завданих цілей, що може надати військову перевагу на полі бою, ідентифікації воєнних злочинців і жертв війни тощо.

Проте, на думку експертів, використання інструментів штучного інтелекту на кшталт **Clearview AI** може привести до масового спостереження чи інших зловживань після закінчення війни. Також, розробка повністю автономного озброєння на основі штучного інтелекту може надати ШІ повноваження щодо ухвалення рішень про летальне застосування сили. Неправильне використання та несправності технологій ШІ у військових умовах можуть привести до непередбачуваних наслідків і завдати шкоди цивільним особам і об'єктам. Відповідно, потрібно дотримуватись рівноваги між перевагами ШІ та потенційними ризиками при застосуванні ШІ, зокрема під час воєнного стану в Україні.

Таким чином, використання технологій ШІ як у мирний, так і воєнний час повинно забезпечувати справедливий баланс між основоположними правами особи та потребами держави у сфері безпеки та оборони.

# ВИСНОВКИ ТА РЕКОМЕНДАЦІЇ

Кожне явище, яке є новим та ще не повністю вивченим, має свої переваги та недоліки. Інтеграція ШІ у військову справу безумовно має великий потенціал і переваги впровадження ШІ у цій сфері має беззаперечно вагомі результати, адже ШІ допомагає збільшити точність та ефективність військових операцій, зменшує ризик для військового персоналу, дозволяє швидко реагувати та виявляти загрози та прогнозувати дії противника.

Втім, як і будь-яка новітня технологія, ШІ несе певні потенційні ризики для основоположних прав людини. Важливим аспектом є проблема упередженості та справедливості в системах ШІ, адже технології ШІ повинні допомагати у відповідних сферах діяльності та водночас залишатися контрольованими людиною. Відтак системи на основі ШІ повинні розроблятися та використовуватися відповідно до національного та міжнародного права.

Використання технологій ШІ має забезпечувати дотримання основоположних прав людини, а також відповідати певним принципам, які здатні усунути потенційні ризики, пов'язані з їх використанням, таким як:

- **Відповідальність**. Технології ШІ у військовій сфері повинні використовуватися відповідально, тобто з урахуванням основоположних принципів міжнародного гуманітарного права та прав людини. Автономні системи озброєння не повинні бути запрограмовані на виконання дій, які б суперечили принципам міжнародного гуманітарного права, зокрема, вони не повинні мати автономну можливість атакувати цивільних осіб чи об'єкти. Крім того, відповідальність за використання військового ШІ повинна бути чітко визначена. Також має бути врегульовано питання зловмисного використання технологій ШІ.

- **Контроль.** Забезпечення контролю за застосуванням, відповідність принципам справедливості та підзвітності при використанні технологій ШІ, зокрема через наявність активного контролю з боку оператора при прийнятті остаточних рішень.

- **Пропорційність.** Розробка та впровадження законодавчого регулювання щодо застосування технологій ШІ в безпековій сфері, що забезпечувало б справедливий баланс між використанням ШІ, інтересами національної безпеки та оборони, а також правами людини. Використання ШІ має сприяти виконанню військових завдань, підвищуючи ефективність та здатність до ведення операцій та водночас має бути пропорційним, відповідати оборонним цілям та не призводити до свавільного порушення прав людини.

- **Безпека та надійність.** Системи ШІ мають бути безпечними та надійними, здатними до виявлення та усунення помилок, а також захищеними від несанкціонованого доступу, кібератак та стороннього впливу. Створення запобіжників на етапі розробки, розгортання і впровадження відповідних систем із використанням ШІ, має сприяти зменшенню ризиків алгоритмічної дискримінації, пом'якшувати можливість настання непередбачуваних наслідків та запобігати помилковій ідентифікації цілей, упередженості чи непрозорості алгоритмів.

- **Прозорість та підзвітність.** Використання військового ШІ характеризується рівнем секретності, однак розробка та використання ШІ у військовій сфері має бути прозорою настільки, щоб забезпечити довіру й розуміння його можливостей та обмежень. Варто забезпечити розуміння логіки прийняття рішення системою, що використовує технології ШІ, а також забезпечення балансу між прозорістю та конфіденційністю.

- **Захист цивільного населення.** Системи ШІ у військовій справі повинні використовуватися з урахування необхідності забезпечення безпеки цивільного населення. Такі системи повинні бути налаштовані на мінімізацію цивільних жертв та запобігання непередбачуваним наслідкам для мирного населення.

- **Запобігання автономному застосуванню сили.** Варто уникати автономного використання технологій ШІ у військових цілях, оскільки це може призвести до непередбачуваних наслідків та порушень міжнародного гуманітарного права.

- **Етичні міркування.** Розробка та застосування військового ШІ має враховувати етичні міркування, зокрема питання автономності, справедливості та впливу на цивільне населення. Має залишатися достатній етичний контроль над розробкою і застосуванням ШІ, щоб забезпечити його відповідальне використання.

Перелічені вище принципи та ключові аспекти використання технологій ШІ не є вичерпними, але вони відображають певні міркування, що стосуються використання ШІ в цілому, підкреслюючи необхідність регулювання та контролю за використанням ШІ у військовій сфері, щоб забезпечити його етичне, відповідальне та безпечне впровадження і застосування з урахуванням необхідності гарантування основоположних прав людини.