КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ТАРАСА ШЕВЧЕНКА
Філософський факультет
Кафедра етики, естетики та культурології

ЕТИЧНІ ПРИНЦИПИ ЦИФРОВОЇ ПРИВАТНОСТІ
ETHICAL PRINCIPLES OF DIGITAL PRIVACY

Кваліфікаційна робота за спеціальністю 033 філософія
на здобуття освітнього ступеня бакалавра філософії

Студентка-виконавець:
ЗВАРИЧ ХРИСТИНА ВІКТОРІВНА
IV курс
спеціальність 033 «філософія»
ОПП «Філософія»

Науковий керівник:
СОБОЛЄВСЬКА ЛЮБОВ СЕРГІЇВНА
канд. філос.наук,
асистент кафедри
етики, естетики та культурології

Допущено до захисту:
Зав. кафедри_____

Київ-2025

ЗМІСТ

ВСТУП

Чи не кожен наш крок у сучасному світі залишає цифровий слід. Користуючись смартфонами, соціальними мережами та онлайн-сервісами, людина щодня передає інформацію про себе – від геолокації до особистих уподобань. З одного боку це робить життя зручнішим, проте водночас ставить перед суспільством низку питань. Традиційне уявлення про приватність як право на усамітнення або контроль над особистим простором – особливо в інтернет просторі – сьогодні стрімко змінюється під тиском цифрових трансформацій. У цифрову епоху приватність уже не зводиться лише до особистої сфери – вона набуває стратегічного значення. Інформація про людину, її поведінку, переміщення, вподобання, стає ресурсом, який можуть використати не лише з комерційною метою, а й як інструмент впливу, тиску чи навіть у рамках інформаційного протистояння між державами. Саме тому актуальність цього дослідження полягає у спробі осмислити нову ситуацію: коли інформація про особу перетворюється на ресурс, який одночасно є економічним активом, політичним інструментом і потенційною загрозою.

Реакцією на суспільний запит стали законодавчі ініціативи на зразок Загального регламенту захисту даних (GDPR) у ЄС, завдяки яким близько 75% населення світу опинилися під захистом законів про приватність [41]. Сьогодні філософське й етичне осмислення цифрової приватності – тобто захисту персональних даних та інформаційного простору особистості від стороннього або прихованого втручання – набуває особливої актуальності. Мова йде не лише про правові чи технічні інструменти контролю, а насамперед про фундаментальні цінності: гідність, автономію, свободу вибору. Саме етика дозволяє побачити глибше – за межами інструкцій і законів - і сформулювати моральні принципи, які повинні регулювати взаємодію людини з цифровим середовищем. Інакше кажучи, мова йде про необхідність створення культурного простору, в якому людина залишається

суб’єктом, а не лише джерелом даних. «Розуміння поняття приватності у цифровому світі дедалі більше розмивається; відтак украй важливо розробляти етичні принципи, механізми захисту прав користувачів та забезпечити підзвітність у сфері технологій» [26].

Проблематика цифрової приватності знаходиться в полі зору дослідників з різних галузей - від права і комп’ютерних наук до соціології та філософії. Зокрема, у сфері філософії та етики технологій дедалі більше уваги приділяється питанням приватності в інформаційному суспільстві. В українському академічному просторі проблема цифрової приватності поки що не набула настільки широкого висвітлення, проте наявні окремі праці з інформаційної етики та філософії технологій, що закладають підґрунтя для подальших досліджень. Стан наукової розробки теми свідчить про необхідність комплексного підходу: нині питання етичних засад приватності розглядаються фрагментарно, переважно у зв’язку з правовими або технічними аспектами. Отже, бракує саме філософського осмислення, яке б систематизувало базові принципи етики приватності в цифровому вимірі.

Об’єкт дослідження: цифрова приватність в інформаційній етиці.

Предмет дослідження: імплементація етичних принципів цифрової приватності в інформаційну епоху.

Метою дослідження є філософське осмислення поняття цифрової приватності та виокремлення ключових етичних принципів, на яких має ґрунтуватися її захист. Метою є не лише визначення змісту цього поняття в межах сучасного етичного дискурсу, а й розкриття тих базових моральних норм і цінностей, які лежать в його основі. Особлива увага приділяється тому, як ці принципи – зокрема автономія, гідність, прозорість, відповідальність можуть слугувати інструментом досягнення балансу між інтересами окремої людини, суспільства та держави в умовах цифрової трансформації.

Відповідно до поставленої мети, у роботі визначено такі **завдання**:

1. Здійснити аналіз поняття «приватність» у зв’язку з розвитком цифрових технологій.

2. Окреслити сучасні філософські підходи до розуміння цифрової приватності в інформаційній етиці.

3. Визначити та охарактеризувати базові етичні принципи цифрової приватності у їх взаємозв’язку з викликами сучасності.

4. Дослідити моральні дилеми і конфлікти, що виникають у сфері цифрової приватності та окреслити шляхи їх вирішення.

Ступінь наукової розробки теми цифрової приватності демонструє значний інтерес до неї як у вітчизняних, так і зарубіжних дослідників. Серед зарубіжних авторів важливе місце посідають роботи Алана Вестіна, який першим систематизував поняття приватності як контроль людини над інформацією про себе, Гелен Ніссенбаум, що запропонувала концепцію контекстуальної цілісності приватності, та Шошани Зубофф, яка описала феномен «капіталізму спостереження». Філософський аспект приватності та її зв’язок з автономією особистості глибоко досліджувався класичними авторами, такими як Іммануїл Кант, Джон Локк та Джон Стюарт Мілль. Значний внесок у розуміння сучасних аспектів цифрового нагляду та соціального сортування зробили Девід Лайон та Лучано Флоріді.

Українська філософська традиція також активно реагує на ці виклики цифрової доби. Дослідження Валентини Воронкової та Віталіни Нікітенко розкривають філософські проблеми цифрового суспільства, Тетяна Шоріна глибоко аналізує моральні дилеми інформаційної етики, Олександр Дзьобань розглядає цифрову людину як особливу філософську проблему, а Андрій Синиця досліджує етичні виклики штучного інтелекту. Таким чином, наукова розробка теми цифрової приватності має достатньо широку та багаторівневу основу, проте вона залишається відкритою для подальших досліджень через швидкі зміни технологічного середовища та нові етичні виклики.

Дослідження базується на сукупності загальнофілософських та спеціальних **методів**. Застосовано метод аналізу та синтезу, описовий метод

для опрацювання літератури з філософії приватності й технологій, що дозволило виокремити ключові підходи та поняття. Порівняльний метод використано для співставлення різних етичних теорій і підходів до проблеми приватності (наприклад, порівняння деонтологічних та утилітарних оцінок втручання в приватність).

Структура кваліфікаційної роботи відображає поставлені завдання та логіку дослідження. Робота складається зі вступу, трьох розділів, висновків та списку використаних джерел. У першому розділі розглянуто теоретичні засади поняття приватності: аналізується генеза поняття приватності, його трансформація під впливом інформаційних технологій та окреслюються різні концепції приватності (право на приватність, приватність як свобода тощо). Другий розділ присвячено безпосередньому аналізу етичних принципів цифрової приватності: розглянуто основні моральні принципи і норми, що стосуються поводження з персональними даними, а також етичні колізії, які постають у цифровому середовищі, та шляхи їх розв’язання на основі зазначених принципів. Третій розділ роботи має практично-аналітичний характер і присвячений дослідженню конкретних прикладів порушення цифрової приватності. Тут аналізується роль технологічних компаній (Google, Meta, Amazon, TikTok). У висновках підсумовано результати дослідження, сформульовано основні висновки щодо ролі й значення етичних принципів приватності в цифрову добу, а також вказано на перспективи подальших розвідок у цьому напрямі.

РОЗДІЛ 1: ТЕОРЕТИЧНІ ОСНОВИ ПОНЯТТЯ ЦИФРОВОЇ ПРИВАТНОСТІ

1.1. Приватність як об’єкт філософського аналізу

Приватність традиційно розуміється як базове право людини на невтручання у її особисте життя та на контроль над інформацією про себе. В класичній праці Алана Вестіна «Privacy and Freedom» приватність визначена як «домагання індивідів, груп чи інституцій самостійно вирішувати, коли, як і в якій мірі інформація про них передається іншим» [16]. Інакше кажучи, йдеться про можливість особи визначати межі власного особистого простору та інформаційної відкритості. Ще у Загальній декларації прав людини (1948 р.) зафіксовано фундаментальні аспекти приватності: право на невтручання в особисте і сімейне життя, недоторканність житла та таємницю кореспонденції, що загалом позначено як право на конфіденційність [6]. Дотримання конфіденційності пов’язане також із інформаційною безпекою, свободою думки і самовираження. У філософському дискурсі інформаційної етики приватність розглядається поряд із правами людини на доступ до інформації, інтелектуальну власність та безпеку споживачів інформаційних послуг. Таким чином, приватність є комплексним поняттям, що охоплює низку моральних та правових норм, принципів і вимог, і тривалий час виникають дискусії щодо балансу між безпекою, свободою інформації та захистом приватного життя людини [3] .

Поняття права на приватність у філософії часто виводять із більш загальних етичних принципів. Зокрема, в етиці Канта наголошується на повазі до людської гідності та автономії особи, на тому, що неприйнятно використовувати людину лише як засіб - це закладає моральний фундамент непорушності особистого простору, «...Дій так, щоби завжди ставитися до людей і до себе також - як до мети і ніколи - лише як до засобу» [38, с. 429]. Джон Ролз, аналізуючи основоположні свободи справедливого суспільства,

фактично включає приватність до переліку базових свобод, необхідних для забезпечення самоповаги та розвитку особистості. Джудіт Дж. Томсон стверджувала, що право на приватність є не самостійним, а «похідним» від інших прав - воно існує лише остільки, оскільки порушує інші вже визнані права, наприклад власності чи тілесної недоторканості [43]. Попри такі різні підходи до осмислення поняття у філософії та праві панує згода щодо цінності приватності як передумови людської автономії, свободи вибору і розвитку індивідуальності. Недарма ще Іммануїл Кант пов'язував публічність законів з вимогою прозорості влади, тоді як особисте життя громадян мало залишатися захищеним від свавільного нагляду держави.

Із плином часу та зміною суспільних устроїв поділ на приватне та публічне набуває нових значень. У період Просвітництва зокрема в працях Джона Локка - розмежування приватного й публічного стало ключовим для політичної та соціальної філософії [40]. Дж. Локк наголошував на природному праві людини на життя, свободу та власність, яке є приватною сферою, захищеною від втручання держави. Він вважав, що держава та громадська влада легітимні лише тією мірою, якою вони захищають приватну сферу людини від зовнішнього посягання.

Цю ідею далі розвинув Іммануїл Кант, пов'язуючи приватне та публічне з ідеями автономії та свободи особистості. Для Канта приватна сфера - це простір, де особа має право керувати власною волею, без примусу з боку інших, керуючись лише моральним законом всередині себе. Публічна сфера ж виступає простором, де індивідуальні волі зустрічаються і взаємодіють у межах спільних норм і законів. Кантівська ідея «приватної автономії» безпосередньо вплинула на формування сучасних уявлень про приватність, зокрема у розумінні непорушності особистого простору, свободи думки та індивідуального вибору. «Публічне користування свого розуму має завжди залишатися вільним і лише воно спроможне здійснити просвітництво серед людей; приватне ж користування того самого розуму, навпаки, може часто

бути дуже суворо обмежене, не перешкоджаючи при цьому поступові просвітництва» [37, с. 6].

Подальший розвиток поняття приватного і публічного знайшов своє вираження у працях Юргена Габермаса, який висунув концепцію «публічної сфери» (Öffentlichkeit). Для Габермаса публічна сфера - це простір раціональної комунікації, дискусій і формування суспільної думки, де громадяни можуть вільно висловлювати свої погляди, не боячись переслідувань чи тиску з боку влади. Публічна сфера, таким чином, протистоїть закритим сферам, таким як держава або приватні інтереси, і виступає ареною вільного, критичного обговорення суспільно важливих питань. «Під публічною сферою ми насамперед розуміємо сферу нашого суспільного життя, у якій може формуватися щось подібне до громадської думки. Доступ до неї відкритий для всіх громадян. … Громадяни виступають як публічне тіло, коли вони без обмежень - із гарантією свободи зібрань, об’єднань та свободи висловлювати й публікувати свої погляди - обговорюють питання загального інтересу» [34, с. 27].

З розвитком цифрових технологій та інтернету традиційний поділ на приватне і публічне зазнав суттєвої трансформації. Сучасні автори, серед яких Мішель Фуко і Гелен Ніссенбаум, наголошують, що межа між приватним і публічним стає все більш умовною та рухомою. У сучасних умовах приватність дедалі частіше стає предметом маніпуляцій і торгівлі, а публічний простір - предметом комерціалізації та контролю. М. Фуко застосовує поняття «паноптикум», аби описати сучасний стан суспільства, де приватна сфера знаходиться під постійним наглядом. «Людину видно, але вона не бачить; вона стає об’єктом інформації, ніколи - суб’єктом комунікації «Видимість перетворюється на пастку» [31, с. 200]. Натомість Ніссенбаум пропонує концепцію контекстуальної цілісності приватності, яка вказує, що приватне й публічне не є абсолютними, а залежать від конкретного соціального та інформаційного контексту. «Право на приватність - це не право на таємницю і не право на контроль, а право на належний потік

особистої інформації» [45, с. 127]. Поділ на приватне та публічне є ключовим для розуміння людського життя в історичному та філософському аспектах. Сьогодні, у цифрову епоху, ця проблема вимагає нового переосмислення. Міждисциплінарні дослідження допомагають з'ясувати, яким чином цифрові технології трансформують межі приватного та публічного, ставлячи перед філософією завдання по-новому визначити роль особистості, її свободи і межі її взаємодії із суспільством.

Становлення інформаційного суспільства та цифрових технологій радикально змінили контекст реалізації права на приватність. По-перше, сучасні засоби комунікації зумовили безпрецедентну зв'язаність людей у реальному часі: як зазначає Кріс Скіннер, «ось чому я вважаю мережу четвертою епохою людства: ми перейшли від роз'єднаних, кочових спільнот у першій епосі - до поселень, землеробства і міст у другій; до подорожей між країнами й континентами завдяки паровій енергії в третій; і - до світу, який сьогодні з'єднаний глобально, у форматі «один-на-один«. Це колосальна трансформація і вона показує, що людство рухається від окремих племен - до спільнот, від спільнот - до з'єднаних спільнот, і нарешті - до єдиної платформи: інтернету» [48, с. 18]. Ще на початку комп'ютерної ери А. Вестін передбачав виникнення напруги між свободою і контролем, приватністю та автоматизацією [17]. Сьогодні ця напруга проявляється у масовому спостереженні за користувачами з боку як держав, так і корпорацій. Показовим є викриття Едвардом Сноуденом у 2013 році глобальних програм стеження (до прикладу, PRISM), що продемонструвало вразливість приватності перед наглядом спецслужб.

Мішель Фуко, спираючись на ідею Дж. Бентама, показав, що при тотальному спостереженні люди починають дисциплінувати себе самі, усвідомлюючи невидиме око наглядача. В цифрову добу архітектура інтернету та всеприсутність камер, сенсорів і трекерів утворюють своєрідний електронний паноптикум, де межа між публічним і приватним розмивається. Широко вживається і поняття «капіталізму нагляду», запроваджене

Шошанною Зубофф, - для характеристики економічної системи, в якій персональні дані стали новим ресурсом, що експлуатується корпораціями [57]. Авторка пише про технологічних гігантів, які впровадили бізнес-моделі, за яких поведінкові дані користувачів збираються масово і використовуються для прогнозування та спрямування їхніх дій (реклама, контент), ставлячи під сумнів свободу волі і приватність особи. Такий системний нагляд над населенням підриває традиційні уявлення про приватне життя як непорушну сферу: межі приватності тепер визначаються не тільки правовими нормами, але й алгоритмами, комерційними інтересами і державними політиками. У відповідь на це у сфері інформаційної етики з'явилися нові концепції. Зокрема, Гелен Нісенбаум запропонувала теорію контекстуальної цілісності, за якою порушення приватності трапляється, коли інформація про особу поширюється за межі належного соціального контексту та всупереч очікуванням самої особи. Наприклад, дані, надані користувачем медичному закладу, не повинні використовуватися поза медичним контекстом без згоди - інакше контекстуальна цілісність інформації порушується, а отже і приватність. Подібні концепції намагаються віднайти баланс між вільним обігом інформації та дотриманням етичних норм щодо персональних даних, актуалізуючи проблему довіри в цифровому середовищі. Адже без довіри користувачів неможливе повноцінне функціонування цифрової економіки та демократичного суспільства. Недарма підкреслюється, що в умовах інформаційної доби приватність стала однією з нових «цифрових« цінностей людини, яку необхідно захищати на рівні з традиційними правами і свободами [4].

З одного боку, Інтернет дав індивідам анонімність і можливість приміряти на себе різні соціальні ролі. Як зазначає Г. Супрун, «спочатку віртуалізація соціальних контактів дозволила індивіду випробувати на собі соціальні маски анонімності, то в подальшому це надало можливість формувати власні автопортрети віртуальної особистості» [13, с. 85]. Тобто, користувачі спершу отримали свободу приховати своє справжнє ім'я чи

образ (нікнейми, аватари), що могло розглядатися як розширення приватності. Проте згодом ті ж самі люди почали конструювати у соцмережах публічні образи себе - створювати цифрові персональні бренди, що часто переносяться і в офлайн-життя. Виникла парадоксальна ситуація: інтернет одночасно і дає прихисток анонімності, і спонукає до добровільної трансляції приватного (фото, думок, даних про особисте життя) на широкий загал. О. Агарков застерігає: «соціальні мережі можуть впливати на самоідентифікацію та соціальну поведінку особистості. Соціальні мережі впливають на індивідуальність саме у цифрову епоху» [1, с. 74] . Іншими словами, під впливом онлайн-середовища особа ризикує втратити автономність свого «Я», підмінити її конформізмом чи залежністю від зовнішньої оцінки (лайків, трендів). Постають і такі етичні питання: що є допустимим у поводженні з чужими даними, де межа між легітимним моніторингом та маніпуляцією? Інформаційна етика сформувалася саме як реакція на подібні дилеми, намагаючись виробити норми поведінки в цифровому просторі. Так, Т. Шоріна відзначає драматичність і неоднозначність сучасних проблем інформаційної етики та підкреслює необхідність «адекватної моральної регуляції людської практики в інформаційній культурі» [14].

Отже, цифрова приватність - це складне багатовимірне явище, що поєднує правові виміри (права людини, законодавчі гарантії), технічні аспекти (захист даних, кібербезпека) і морально-культурні чинники (цінності автономії, довіри, поваги до особистості). У сучасному цифровому суспільстві приватність трансформується: з одного боку, вона як і раніше служить умовою збереження людської гідності та свободи, а з іншого - потребує нових підходів до свого забезпечення. Феномен «цифрової людини» передбачає усвідомлення того, що приватність стала невід’ємною складовою цифрової культури. Вона інтегрується у систему нових етичних цінностей та правил поведінки онлайн. Захист приватності сьогодні - це не лише питання індивідуального вибору, але й суспільна проблема, що вимагає балансу між

інноваціями та правами людини. Отже, головним викликом сьогодні є спрямування технологічного розвитку так, аби він відповідав фундаментальним цінностям та правам людини. Саме цифрова приватність стає ключовим критерієм гуманного й відповідального поступу інформаційного суспільства- своєрідним показником того, наскільки технології залишаються інструментом у руках людини, а не перетворюють її на власний придаток. Збереження приватності за умов тотального інформаційного середовища є необхідною передумовою для підтримки соціальної довіри, свободи самовираження й збереження індивідуальної ідентичності у світі цифрових взаємодій. Таким чином, сучасне розуміння цифрової приватності поєднує традиційні філософські ідеї про недоторканність особистої сфери із новими викликами інформаційної доби, вимагаючи постійного наукового аналізу та активних практичних заходів для її ефективного захисту.

1.2. Специфіка підходів до визначення цифрової приватності

З позиції утилітаризму моральність будь-яких дій оцінюється відповідно до наслідків, які вони породжують, і головною метою є досягнення максимального добробуту чи щастя для якомога більшої кількості людей. З цього погляду, приватність не сприймається як абсолютне право, а радше як цінність, значення якої визначається тим, наскільки вона сприяє загальному суспільному благу. Іншими словами, право на приватність виправдане рівно тією мірою, наскільки воно приносить позитивні результати для суспільства загалом [47]. Дж. С. Мілль наголошував на важливості особистої свободи як складової загального благополуччя. Він формулює принцип, за яким суспільство може втручатися в дії індивіда лише для запобігання шкоді іншим; в усьому, що стосується лише його самого, «незалежність особи є, по праву, абсолютною. Над собою, над власним тілом і розумом індивід є суверенним« [42]. Сформульований Джоном Стюартом Міллем «принцип

шкоди» передбачає, що доки певна інформація чи дія не завдає шкоди іншим людям, вона повинна залишатися недоторканною сферою індивідуальної автономії. Таким чином, приватність стає невіддільною умовою особистої свободи й самореалізації. Врешті-решт, забезпечення приватності сприяє загальному щастю суспільства, оскільки гарантує кожному простір для вільного й самостійного розвитку без втручання більшості.

Утилітаристський підхід передбачає можливість перегляду значення приватності, якщо цього потребують суспільні інтереси. Ба більше, деякі представники утилітаризму прямо заявляють, що приватність не належить до абсолютних або безумовних прав людини. З їхньої точки зору, приватність-це радше інструмент, який дозволяє досягати важливих суспільних цілей, таких як безпека, здоров'я або загальний добробут. І якщо втручання у приватне життя людини може принести значну суспільну користь, то з моральної точки зору таке втручання можна вважати допустимим. Класичною ілюстрацією такого підходу є дилема між приватністю й безпекою, яка особливо гостро проявляється в ситуаціях кризи або загроз, наприклад, при боротьбі з тероризмом чи пандемією. У таких обставинах утилітаристський погляд допускає широкомасштабний збір персональних даних, посилений нагляд або навіть тотальне відеоспостереження, якщо це реально може захистити людські життя та попередити катастрофу. Під час пандемії COVID-19 деякі країни Східної Азії запровадили жорстке відстеження переміщень громадян за допомогою смартфонів, суттєво обмеживши приватність, але досягнувши високого рівня безпеки і здоров'я населення. З утилітарної позиції таке «обмеження свободи і приватності заради добробуту» може бути виправданим, адже добробут (збережені життя, здоров'я) переважає негатив від втрати приватності. Автори, що аналізували етичні аспекти пандемії, прямо зазначали: для утилітариста добробут важливіший за абстрактні права, тому він «готовий обмежити право на приватність або свободу, щоб захистити благополуччя» [54]. Якщо добровільний підхід на кшталт згоди користувачів ділитися даними не

працює ефективно, утилітаризм схильний підтримати і примусові заходи, ставлячи колективне благо понад індивідуальні переваги.

Підхід утилітаризму до питання приватності може означати, що для досягнення максимальної суспільної користі влада або компанії можуть вдатися до постійного контролю за людьми, систематичного збору інформації або навіть скасування онлайн-анонімності задля ефективної боротьби зі злочинністю. З іншого боку, подібні заходи можуть створювати «суспільство спостереження» (surveillance society)- термін належить канадському соціологу Девіду Лайону (David Lyon). Він вперше широко використав цей термін у своїй книзі: [25] , де люди втрачають почуття автономії та довіри. Критики утилітаризму зауважують, що гонитва за загальним благом може пожертвувати правами меншості: якщо більшості стає трохи краще від порушення приватності окремих осіб, чисто утилітарний розрахунок це дозволяє. У контексті цифрової приватності це означає, що інтереси окремого користувача (скажімо, збереження в таємниці його листування) можуть бути знехтувані, якщо розкриття цих даних принесе користь іншим (запобіжить теракту або покращить сервіс для тисяч людей). Утилітарна перспектива висвітлює головну цінність приватності - її внесок у щастя та добробут - але водночас вказує на межу: коли приватність перестає служити добру, вона може бути обмежена. Таким чином, утилітаризм закликає постійно зважувати благо від захисту даних проти блага від їх відкриття, шукаючи баланс, який дасть максимально моральний результат для суспільства в цілому.

На відміну від утилітаризму, деонтологічна етика стверджує, що деякі дії є морально неприпустимими за будь-яких обставин- незалежно від наслідків. Іммануїл Кант сформулював категоричний імператив, який вимагає ставитися до людської особистості завжди як до мети, і ніколи лише як до засобу [21]. Це принципове положення безпосередньо застосовується до питання приватності: використання чиїхось особистих даних лише як засобу для чужих цілей (навіть благонамірених) порушує гідність та

автономію цієї особи. Кожна людина має невід'ємну цінність, тому вторгнення в її приватне життя потребує морального обґрунтування значно серйознішого, ніж утилітарний підрахунок вигод.

З деонтологічної перспективи, цифрова приватність постає як фундаментальне право особи на автономію, пов'язане з людською гідністю. Кантівський імператив про ставлення до людини як до цілі можна перефразувати так: «слід поважати право кожного самостійно визначати, яку інформацію про себе розкривати, а яку - ні. Порушити приватність - значить зневажити волю і раціональність людини, зробивши її об'єктом маніпуляції». Як зауважує сучасний кантіанський підхід до цифрової етики, ми повинні «поважати здатність людини обирати свій життєвий шлях згідно з власними інтересами і не підпорядковувати чужі інтереси своїм без їхньої згоди» [21]. Особисті дані в цифровому світі - продовження особистості, її «цифровий слід», який заслуговує на такий самий моральний захист, як і фізична автономія людини [21]. Тому з позиції деонтології неприпустимо виправдовувати масове стеження чи продаж приватної інформації користувачів навіть задля корисної мети, якщо при цьому люди перетворюються на засоби. Наприклад, компанія, що збирає персональні дані, зобов'язана робити це лише за вільної згоди клієнта та використовувати дані в межах, на які той погодився - інакше компанія порушує моральний обов'язок не чинити обману і не експлуатувати довіру.

Деонтологічний підхід ставить перед нами серйозну моральну дилему: чи можна допустити винятки в праві людини на приватність? У межах кантівської етики часто постають ситуації, коли один обов'язок вступає в конфлікт з іншим, наприклад: з одного боку - обов'язок говорити правду, а з іншого - обов'язок захищати людське життя. Аналогічні дилеми з'являються сьогодні в цифровій сфері: чи може держава вторгнутися в приватний простір окремого громадянина (наприклад, підозрюваного в злочині), щоб захистити життя і безпеку решти людей? Звісно, сам Кант ніколи прямо не торкався сучасних питань кібербезпеки чи цифрового нагляду. Проте,

виходячи з його філософських принципів, будь-яке рішення в таких ситуаціях повинно максимально обмежити ставлення до людини лише як до засобу досягнення мети. Наприклад, якщо держава хоче отримати прихований доступ до зашифрованих повідомлень громадян (так званий бекдор для спецслужб), то з деонтологічної перспективи постає питання: чи не порушує це фундаментальну автономію та довіру величезної кількості людей, які не мають стосунку до злочинності? Адже у такій ситуації фактично кожного громадянина розглядають як потенційний ресурс у боротьбі з одиничними злочинцями, що є морально дуже сумнівним. З погляду поваги до людської гідності, тотальне спостереження чи постійний аналіз активності людей в мережі здається неприйнятним. Воно перетворює приватне життя людини із захищеного простору свободи на інструмент для задоволення інтересів інших, фактично переводячи громадян у статус контрольованих об’єктів. Це безпосередньо суперечить ключовим принципам Канта щодо поваги до людини як автономної особистості, яка ніколи не може використовуватися лише як засіб для досягнення чиєїсь мети.

Проте й деонтологічний підхід визнає, що права не можуть бути абсолютними: межі свободи однієї людини завжди проходять там, де виникає свобода інших. Це означає, що право людини на приватність не повинно використовуватись як інструмент для уникнення відповідальності або приховування злочинних дій. Наприклад, у ситуації, коли особа зловживає цифровою анонімністю для нанесення шкоди іншим - чи то шляхом кібербулінгу, чи через поширення шкідливих програм - суспільство безумовно має моральне право притягнути її до відповідальності. Але ключовий момент тут полягає у тому, як саме це робити: навіть порушуючи приватність злочинця, ми маємо зберігати повагу до його особистості. Йдеться передусім про суворе дотримання справедливих процедур: законність отримання ордерів на доступ до даних, повагу до презумпції невинуватості та інших фундаментальних гарантій прав людини. Така позиція цілком відповідає кантівському розумінню ролі держави, яка має

виступати гарантом людської автономії та встановлювати єдині для всіх правила, що захищають кожного громадянина від свавілля. Сам Кант прямо наголошував, що держава повинна не лише забезпечувати свободу людей, а й захищати їх від можливих маніпуляцій або використання в якості простих засобів [21]. Сьогодні цю кантівську думку активно переосмислюють у контексті цифрових технологій. Багато дослідників зазначають, що держава повинна стримувати корпорації у їхньому прагненні безконтрольно використовувати особисті дані громадян, а також обмежувати власні можливості для вторгнення в особистий простір. Таким чином, держава має діяти як обережний арбітр, що утримує баланс між суспільною безпекою та приватністю особи, не порушуючи гідність і автономію жодного з учасників суспільного договору.

Принцип справедливості Джона Ролза звучить так: «кожна людина повинна мати рівне право на найбільш широку тотальну систему рівних основних свобод, сумісну з аналогічною системою свобод для всіх» [46]. Хоча Джон Ролз безпосередньо не включав приватність до переліку фундаментальних свобод, запропонованих у своїй теорії, саме його концепція створює ґрунтовне філософське підґрунтя для розуміння цифрової приватності як важливої передумови для реалізації інших свобод, а також збереження людської гідності та самоповаги. Ліберальна традиція, представником якої був Ролз, традиційно розглядає недоторканність особистого життя й родинної сфери як одну із базових свобод - цей принцип, до речі, закріплено і в міжнародних документах, зокрема у статті 12 Загальної декларації прав людини ООН [6]. З погляду контрактуалізму, підхід до приватності є прагматичним: правила щодо збору та використання персональних даних мають бути такими, які раціональні та неупереджені учасники схвалили б, якби укладали спільний соціальний договір.

З погляду теорії суспільного договору, уявімо, що кожен з нас за завісою незнання не знає, ким він буде в цифровому світі - простим користувачем, власником ІТ-компанії, хакером чи жертвою кіберзлочину. За таких умов усі,

ймовірно, погодяться встановити сильні гарантії приватності, щоб убезпечити себе в разі, якщо опинимося серед вразливих сторін (рядових громадян) [55]. Раціонально ми розуміємо, що будь-хто може постраждати від тотального спостереження чи витоку даних - отже, за взаємною згодою слід обмежити збір інформації, забезпечити її захист і дати людям контроль над власними даними. Це узгоджується і з другим принципом Ролза (принципом відмінностей), який вимагає, щоб соціальні та економічні нерівності впорядковувалися на користь найменш привілейованих [46]. У цифровому вимірі це означає: якщо інформаційна асиметрія (нерівність у доступі до даних або в контролі над ними) ставить когось у вразливе становище, суспільство повинно це виправити правилами на користь слабкої сторони. Наприклад, Європейський регламент GDPR можна розглядати як результат соціального консенсусу про те, що громадяни мають право знати, хто і як обробляє їхню інформацію, і вимагати справедливого використання персональних даних. GDPR встановлює саме ті принципи (прозорість, цільове використання, мінімізація даних, згода тощо), які могли б бути виписані в «цифровому суспільному договорі», бо їх раціонально бажав би будь-який індивід, не знаючи, чи буде він простим користувачем чи даними нечесного бізнесу.

Контрактуалістський підхід на практиці базується на поняттях довіри та соціальних очікувань. Люди зазвичай керуються негласними домовленостями, коли йдеться про приватність. Наприклад, ми звикли розраховувати, що наші особисті повідомлення в месенджерах будуть захищені, що історія пошукових запитів не стане інструментом впливу або тиску, а камери відеонагляду, встановлені на вулицях, використовуватимуть для безпеки, а не для тотального контролю. Всі ці очікування можна розглядати як певну негласну угоду між суспільством і кожним окремим громадянином про межі допустимого використання приватних даних. Якщо ці межі порушуються, люди відчувають, ніби їхню довіру було обмануто, а угоду - розірвано без їхнього відома. Яскравий приклад такого порушення -

відомий випадок із компанією Cambridge Analytica. Цей скандал спричинив величезний суспільний резонанс саме тому, що люди, ділячись особистими даними у Facebook, не припускали, що ці дані будуть використані для маніпуляцій їхньою політичною поведінкою. Для багатьох це стало справжнім моральним шоком - мовчазний суспільний договір було грубо порушено, адже ніхто не давав свідомої згоди на таке втручання. З погляду контрактуалізму, ця ситуація вважається несправедливою, оскільки люди не погодилися б добровільно на подібне використання своїх приватних даних. Тому етично правильно було б відновити рівновагу: створити прозорі й чіткі умови використання даних, справедливо покарати винних у зловживаннях, і забезпечити реальні інструменти контролю за інформацією самими користувачами.

Отже, з точки зору контрактуалістської етики, приватність є результатом чесної і прозорої суспільної домовленості між громадянами, державою та бізнесом. Головний етичний ідеал тут - правила цифрової взаємодії, які є прийнятними для всіх сторін, створені на основі взаємоповаги та рівноправності. Практично до цього ідеалу можна наблизитися завдяки відкритим дискусіям, демократично ухваленим законам та міжнародним угодам (наприклад, згаданим у роботі документам ООН або європейським конвенціям). Контрактуалістська позиція підкреслює, що приватність не є приватною справою кожної людини окремо, а виступає спільним суспільним благом. Її рівень залежить від того, на яких умовах ми погоджуємося існувати як єдине суспільство - умовах, що базуються на рівності, взаємній повазі та прагненні до спільного добра.

Розглянуті вище класичні етичні підходи окреслюють фундаментальні принципи і сучасні філософи прагнуть інтегрувати їх для розуміння конкретних викликів цифрової ери. Американська дослідниця Гелен Ніссенбаум запропонувала концепцію «контекстуальної цілісності» приватності, яка поєднує ідеї права, користі та домовленостей у єдину рамку. Г. Ніссенбаум підкреслює, що приватність - це передусім право на належний

потік інформації [45]. Іншими словами, важливо не просто те, що про нас збирають, а як, в якому контексті і з якою метою ці дані передаються. Кожна сфера життя (медична, освітня, сімейна, ділова тощо) має свої норми інформаційного обміну. Те, що прийнято в одному контексті, може бути порушенням в іншому. Приватність порушується не лише тоді, коли дані стали відомі стороннім, а коли вони вийшли за межі належного контексту. Сама Г. Ніссенбаум формулює це так: «недоторканність приватного життя - це не право на секретність чи контроль, а право на належний потік особистої інформації». Тобто, людина вправі очікувати і вимагати, щоб її інформація використовувалася відповідно до соціальних норм конкретної ситуації.

Підсумовуючи перший розділ, варто наголосити, що цифрова приватність є складним, багаторівневим феноменом, що знаходиться на перетині фундаментальних етичних та філософських ідей. Поширення цифрових технологій радикально змінило класичні уявлення про межі приватного і публічного простору, змушуючи нас заново осмислювати поняття особистої захищеності. Якщо раніше приватність насамперед означала свободу від стороннього втручання у приватну сферу, сьогодні вона охоплює значно ширший спектр питань, серед яких особливого значення набувають управління персональними даними, контроль цифрового сліду і захист інформації у віртуальному середовищі. В епоху цифрових технологій приватність перестає бути суто юридичною чи технічною проблемою, вона набуває глибокого морально-філософського виміру. Вона безпосередньо пов’язана з такими базовими цінностями людського існування, як гідність, автономія і свобода - цінностями, які ще в класичній традиції підкреслювали Іммануїл Кант, Джон Стюарт Мілль і Джон Локк. Ці філософи вважали особистий простір необхідною умовою для самореалізації людини та її вільної взаємодії із суспільством.

Таким чином, у першому розділі стає очевидним, що цифрова приватність - це динамічна концепція, яка постійно вимагає глибокого осмислення і адаптації етичних норм до змін у технологіях та суспільстві.

Для того, щоб зберегти приватність як фундаментальну суспільну цінність, необхідно виробляти комплексні рішення, які враховують не лише юридичні або технічні аспекти, але й моральні принципи, що гарантують повагу до особистості, її автономію і людську гідність у сучасному цифровому світі.

РОЗДІЛ 2. СУЧАСНІ ВИКЛИКИ ЦИФРОВОЇ ПРИВАТНОСТІ

2.1. Загрози приватності в епоху великих даних та штучного інтелекту

Обсяг інформації, яка щоденно накопичується про кожну людину, досяг небачених масштабів. Йдеться не лише про кількісні показники - надзвичайно вражає також тематична широта та структурна складність цих даних. Практично кожна дія у цифровому просторі, від вподобання в соціальних мережах до історії покупок чи онлайн-запитів, залишає слід, який може бути зібраний, оброблений і використаний. Паралельно з цим постійно вдосконалюються аналітичні інструменти. Вони стають точнішими, швидшими, здатними виявляти приховані закономірності та формувати профілі особистості з високим ступенем деталізації. У результаті традиційні моделі захисту приватності – як юридичні, так і технічні - виявляються недостатньо ефективними. Вони або не враховують нові ризики, або не встигають адаптуватися до темпів технологічного розвитку. Та попри це, цифрові технології не обов’язково мають деструктивний потенціал. Як влучно зауважив Лучано Флоріді, один із провідних мислителів у сфері інформаційної етики - інформаційні технології можуть не лише загрожувати приватності, а й підтримувати її, посилювати, навіть захищати. Тож ключ - у правильному підході, у закладених принципах, у розумінні того, що цифрове середовище потребує нових рамок - не менш етичних, ніж технологічних. [44]. Іншими словами, Big Data та Штучний Інтелект створюють цілком нові виклики для приватності, яких не існувало в попередні епохи.

Однією з найбільш занепокоєних тем сучасності є те, як глибоко цифрові технології здатні проникати в приватне життя людини. Те, що раніше здавалося несуттєвим - наприклад, історія пошуків у мережі чи звична поведінка в соціальних платформах - тепер може бути перетворене на інструмент вичерпного аналізу особистості. Дані, що окремо видаються

невинними або випадковими, у сукупності дозволяють виявити закономірності поведінки, відчитати емоційний стан, і навіть передбачити індивідуальні реакції. Цифрова слідова інформація перетворюється на багатовимірну мапу приватного простору, доступ до якої дедалі частіше отримують сторонні – без прямої участі самої людини. Алгоритми, які обробляють ці масиви, здатні виявляти неочевидні закономірності в поведінці людини, помічати емоційні зміни та зчитувати психологічні характеристики, які раніше вважались особистими і недоторканними [51]. «Ефект мозаїки - полягає у тому, що окремі елементи інформації, зібрані з різних джерел, об’єднуються і створюють цілісну картину про конкретну особу». При цьому така реконструкція відбувається без відома людини і без її дозволу. Подібна практика суперечить фундаментальному етичному принципу, згідно з яким кожна особа має право контролювати, як саме використовується інформація, що її стосується.

Нуджинг (від англійського слова nudge, що означає підштовхувати) - це сучасний підхід, який прийшов до нас із поведінкової економіки і психології. Головна його ідея полягає в тому, що можна впливати на рішення людей, зовсім не примушуючи їх і не використовуючи прямі фінансові методи стимулювання. Йдеться радше про створення таких умов, у яких людина природно й невимушено схиляється до варіанту, що відповідає її власним потребам та інтересам суспільства загалом. Концепцію детально розробили відомі дослідники Річард Талер і Касс Санстейн у книзі «Nudge: Improving Decisions About Health, Wealth, and Happiness». На думку цих авторів, нудж можна трактувати як будь-яку деталь чи особливість у середовищі, де людина робить свій вибір. Такі деталі можуть майже непомітно, але достатньо прогнозовано змінювати поведінку. При цьому людина, яка обирає, не втрачає жодної зі своїх можливостей, а економічна мотивація рішення практично залишається незмінною. Іншими словами, якщо певні особливості ситуації спонукають людину до передбачуваної дії, але не забороняють їй альтернативні рішення і не створюють значних фінансових

переваг чи втрат, вони цілком відповідають ідеї нуджингу. «Під нуджем ми розуміємо будь-який аспект «архітектури вибору», який змінює поведінку людей передбачуваним чином, не забороняючи жодних опцій і істотно не змінюючи їхніх економічних стимулів». [50]

У сфері цифрової приватності концепцію нуджингу застосовують, щоб непомітно спонукати людей ухвалювати більш обдумані рішення щодо особистих даних. Типовим прикладом є налаштування, які спочатку встановлені з найвищим рівнем конфіденційності (принцип opt-out замість opt-in). Також платформи можуть використовувати ненав'язливі нагадування або короткі попередження про можливі наслідки надмірного відкриття інформації. Основною перевагою такого підходу є те, що він не перевантажує користувачів складними формулюваннями чи тривалими процедурами згоди, а замість цього м'яко й ефективно нагадує про важливість захисту приватних даних. Просте й коротке повідомлення, що з'являється у потрібний момент, може бути набагато дієвішим, ніж детальна політика конфіденційності, яку мало хто читає. Проте існують і серйозні етичні питання щодо використання нуджингу. Якщо підштовхування стає непомітним або недостатньо прозорим для користувача, це може призвести до маніпуляцій і порушення принципу особистої автономії. В такому разі нуджинг перетворюється на інструмент «маніпулятивного дизайну», який не лише підриває довіру користувачів, а й починає слугувати інтересам власників цифрових платформ, а не самих людей.

Окремо слід відзначити загрози приватності з боку корпорацій, бізнес-моделі яких базуються на масовому зборі та монетизації персональних даних. Американська дослідниця Ш. Зубофф описала феномен сучасної цифрової економіки поняттям «капіталізм спостереження», сутність якого-експлуатація приватного життя людей у комерційних цілях. За влучним висловом Зубофф, «капіталізм спостереження односторонньо привласнює особистий досвід людини як безкоштовну сировину для трансформації у поведінкові дані» [57, с. 18]. Наші онлайн-дії, маршрути пересування,

покупки, вподобання - увесь цей особистий досвід перетворюється на сировину, що аналізується алгоритмами та конвертується у прибуток компаній (через таргетовану рекламу, прогнозування поведінки споживачів тощо). Більшість людей навіть не замислюються, як багато їхньої приватної інформації щодня потрапляє до сторонніх рук. При цьому звичайні користувачі майже ніколи не мають можливості втрутитись у цей процес або хоча б зрозуміти, яка інформація збирається та навіщо це потрібно. Ситуація, по суті, така: великі компанії отримують необмежений доступ до даних про життя користувачів, тоді як самі люди лишаються осторонь, не маючи повної картини того, що саме з ними відбувається. Ситуацію можна описати за допомогою наступного образу. Уявіть собі кімнату, стіни якої зроблені з прозорого скла. Ви всередині, а навколо люди, яких ви не бачите. Вони уважно спостерігають за кожним вашим рухом, емоцією чи звичкою. Водночас вам нічого не відомо про цих спостерігачів, ви навіть не впевнені, чи є вони там узагалі. Приблизно так виглядає асиметрія доступу до інформації в сучасному цифровому світі. Це створює потужну інформаційну владу в руках кількох корпорацій. І ця влада несе загрозу, яка виходить далеко за межі особистого життя: вона може підривати свободу особистості, суспільну довіру, право людини на вибір і навіть базові принципи демократії.

Особливу тривогу викликають технології розпізнавання облич, які практично унеможливлюють анонімність у громадських місцях. Завдяки поєднанню відеокамер та баз даних можна легко ідентифікувати будь-якого перехожого чи учасника протестної акції. Це порушує важливе право людини залишатися невпізнаною в публічному просторі, яке лежить в основі таких свобод, як право на протест, вираження думок чи свободу зібрань. Саме тому в Євросоюзі активно тривають дискусії щодо жорстких обмежень або навіть повної заборони технологій автоматичного розпізнавання облич у публічних місцях. Найнебезпечнішим поєднанням великих даних та штучного інтелекту є профілювання людей та персоналізований вплив на їхні рішення. Вже зараз алгоритми визначають, яка інформація, реклама чи новини

відображатимуться користувачеві. Це відкриває можливість тонкої маніпуляції поведінкою не тільки споживачів, але й виборців. Яскравим прикладом тут став скандал Cambridge Analytica, де дані з соцмереж використали для розробки персоналізованих політичних повідомлень, спрямованих на зміну політичних вподобань людей. Штучний інтелект здатен автоматизувати й масштабувати подібні впливи, створюючи оманливе враження нейтральності: мовляв, це лише алгоритм, а не свідома пропаганда. Проте філософи звертають увагу, що це серйозна загроза автономії особистості, адже фактично рішення людини скеровуються за допомогою використання її власних психологічних слабкостей. Як підсумував Ю. Н. Харарі, сьогоднішні технології наближають час, коли «Ми є хакованими тваринами. Поєднання біотехнологій і інформаційних технологій незабаром надасть деяким корпораціям та урядам можливість «зламувати« людей: передбачати наші вибори, маніпулювати нашими бажаннями і навіть замінювати людські почуття штучними механізмами» [36]. Іншими словами, якщо раніше влада над людиною досягалася примусом і переконанням, то в умовах тотального збору даних і всіх можливих алгоритмів виникає ризик «зламування» свободи волі: зовнішні сили можуть знати про нас більше, ніж ми самі, й використовувати це знання, щоб керувати нами без нашої усвідомленої згоди.

Отже, приватність в добу Big Data та ШІ переживає безпрецедентні виклики. Втрата контролю над особистими даними загрожує основоположним цінностям - гідності, автономії та свободі волі людини. Приватність більше не можна розглядати лише як особисте благо чи примху окремої людини; вона стає питанням суспільного інтересу і навіть національної безпеки (в демократичному розумінні). Адже якщо мільйони громадян підлягають невидимому тотальному спостереженню та поведінковому впливу, під загрозою опиняються самі засади вільного суспільства. Недарма Ш. Зубофф наголошує, що нова цифрова реальність «загрожує нашій свободі та демократії, ставлячи під сумнів саму суть

людської природи» [57, с. 17]. Питання приватності сьогодні вже не можна спрощувати до банального аргументу «нічого приховувати». Насправді йдеться про значно глибші речі: про межі допустимого контролю над особистістю, про те, чи залишиться людина повноцінним суб'єктом власного життя в умовах дедалі потужнішого цифрового спостереження. В епоху, коли дані й штучний інтелект здатні проникати у всі сфери нашого існування, виникає необхідність радикально переглянути класичні уявлення про приватність. Ми повинні сформулювати нові етичні підходи, які дозволять захистити людську гідність і автономію перед лицем стрімкого технологічного прогресу.

Такі резонансні випадки, як незаконне отримання даних користувачів Facebook фірмою Cambridge Analytica, викриття Едвардом Сноуденом тотального стеження з боку спецслужб, використання системи розпізнавання облич Clearview AI, зокрема й в Україні, регулярні інциденти з витоком особистих даних і суперечки навколо додатків на кшталт TikTok - усе це ілюструє те, наскільки незахищеною може бути приватність людини в цифрову епоху. Аналіз цих конкретних ситуацій дозволяє зрозуміти, які наслідки мають подібні порушення для свободи особистості, суспільної довіри та демократичних цінностей, а також як ці приклади співвідносяться з ідеями сучасних фахівців з інформаційної етики.

Кейс Cambridge Analytica (Facebook): Одним із найвідоміших прикладів є скандал 2018 року, коли з'ясувалося, що консалтингова фірма Cambridge Analytica нелегально отримала і використала особисті дані мільйонів користувачів Facebook для цілей політичної реклами. За допомогою стороннього додатку компанія зібрала дані 87 мільйонів профілів Facebook - від часових міток оновлень статусів та кількості вподобань до змісту приватних повідомлень [7].Ці дані були застосовані для створення детальних «психографічних» профілів виборців і таргетованого впливу на їхню поведінку, особливо під час виборів у США та референдуму Brexit. Виявлення цього випадку підірвало суспільну довіру до того, що великі

інтернет-платформи здатні відповідально поводитися з нашою інформацією. Як зауважив дослідник Джо Вестбі, скандал поставив незручне запитання: «наскільки ми вразливі до маніпуляцій нашою поведінкою? [5]»З більш широкої перспективи цей інцидент показав небезпечні наслідки економіки, що базується на монетизації даних користувачів. Він підтвердив побоювання щодо того, що особиста інформація може використовуватись для політичних цілей, що загрожує підвалині демократії. З точки зору філософії, ця ситуація демонструє, як легко людина може стати об'єктом прихованого впливу. Це підіймає питання про те, чи залишається в таких умовах особистий вибір справді автономним і вільним, якщо він непомітно скеровується алгоритмами.

Витік даних Cambridge Analytica став можливим не випадково, а внаслідок бізнес-моделі, побудованої на масовому зборі та монетизації інформації про користувачів. Саме так Facebook та інші техногіганти перетворюють наші дії та вподобання на ресурси для отримання прибутку (продаж таргетованої реклами, прогнозування ринкової поведінки тощо). Зубофф застерігає, що капіталізм спостереження створює безпрецедентну асиметрію влади між тими, хто збирає дані, і тими, кого ці дані стосуються. Це становище нагадує ефект однобічного дзеркала: життя користувачів прозоре для корпорацій, тоді як самі ці корпоративні практики лишаються прихованими. У результаті – порушуються базові права, пов'язані з особистою автономією. Як влучно зазначає Зубофф, така система «нівелює елементарні права, пов'язані з автономією особистості, які є суттєво важливими для можливості існування демократичного суспільства». Інакше кажучи, масове комерційне стеження загрожує не лише приватності окремих людей, а й ключовим суспільним цінностям - від гідності й особистісної автономії до плюралізму та демократичної участі [57, с. 16].

Щодо Кейс Clearview AI (розпізнавання облич в Україні), то окрему етичну проблему становлять сучасні технології ідентифікації особи, зокрема системи розпізнавання облич. Яскравий приклад - діяльність компанії

Clearview AI, яка створила глобальну базу зображень із соцмереж і запропонувала інструмент, здатний миттєво впізнавати будь-яку людину за фотографією. В 2022 році Україна почала співпрацювати з Clearview AI, використовуючи її технології для ідентифікації осіб (зокрема, в умовах воєнного стану - для розпізнавання військових злочинців чи жертв війни). Однак впровадження такої системи викликало критику правозахисників та прихильників приватності. Основна претензія полягає в тому, що інструмент Clearview «практично знищує право людини на приватне життя. Технологія може впізнати будь-кого, чиє фото хоча б раз з'явилося в одній із соціальних мереж. Фактично Clearview AI є найбільш досконалим інструментом масового спостереження» [7].

Дійсно, якщо кожен перехожий на вулиці або учасник мітингу може бути негайно ідентифікований за допомогою камер і алгоритмів, то зникає останній прихисток приватності - анонімність у публічному просторі. Це має серйозні наслідки для громадянських свобод: люди можуть боятися виходити на протести або вільно пересуватися, розуміючи, що їхню особу встановлять і, можливо, поставлять на облік. У філософському контексті технології на кшталт Clearview кидають виклик самому поняттю приватності як контролю над інформацією про себе. Самовільне пересування наших фотографій з приватних профілів до поліцейських баз даних порушує «контекстуальну цілісність» інформації: те, що було доречним у контексті соцмереж (обмін фото з друзями), стає загрозливим в контексті стеження. Тому багато країн Заходу вже заборонили або обмежили використання Clearview AI, вбачаючи в ньому непропорційне обмеження права на приватність та ризик для демократичних свобод.

Серйозні побоювання викликає і діяльність соціальних мереж та додатків, які агресивно збирають дані. Зокрема, навколо китайської платформи TikTok точаться дискусії щодо того, чи не передаються дані сотень мільйонів користувачів владним структурам Китаю. Деякі країни вже частково обмежують TikTok з міркувань національної безпеки, оскільки

застосунок підключений до великої екосистеми ByteDance [2] і потенційно може служити каналом масового збору інформації про користувачів без їх згоди. Тут етична проблема приватності переплітається з геополітичними мотивами- страхом перед контролем авторитарної держави над глобальним інформаційним простором. Хоча кінцеві рішення щодо таких додатків ще обговорюються, сам факт цієї «TikTok-паніки» сигналізує: суспільство все більше усвідомлює цінність приватності і готове вимагати обмежень, аби захистити цифровий суверенітет особистості.

Розглянуті випадки яскраво демонструють, що наслідки порушення цифрової приватності глибоко виходять за межі суто технічних чи юридичних питань, зачіпаючи ключові моральні й соціальні цінності. Перш за все, суттєво підривається суспільна довіра - базова умова будь-яких гармонійних соціальних взаємин. Якщо держава та корпорації не здатні забезпечити належного захисту особистих даних громадян, останні почуваються безсилими й незахищеними, що призводить до поступової руйнації фундаментального соціального договору, особливо важливого у цифрову епоху. Не менш серйозно потерпає і демократія. Постійне цифрове спостереження, таргетована інформація та алгоритмічні маніпуляції поведінкою виборців несумісні з відкритим демократичним дискурсом і вільним волевиявленням. У такій ситуації приватність стає необхідною умовою для захисту демократичних свобод, адже тільки в умовах захищеного приватного простору людина може формувати незалежні рішення і висловлювати свою позицію без страху маніпуляції чи репресій. Також виникає гостра загроза для автономії людини як самостійного суб’єкта. Сучасні цифрові системи дозволяють постійно стежити за індивідом, прогнозувати та коригувати його дії через алгоритми. Як наголошує Гелен Ніссенбаум, втрата контролю над персональною інформацією фактично означає втрату контролю над власним життям. Коли особа вже не керує тим, які дані про неї циркулюють у цифровому просторі, вона перестає бути повноцінним суб’єктом свого існування. Зрештою, під серйозним сумнівом

опиняється сама ідея свободи волі. Якщо цифрові технології та великі масиви даних дають змогу не тільки передбачати, але й цілеспрямовано формувати людський вибір, постає важливе питання: чи залишається цей вибір по-справжньому автономним? Шошана Зубофф описує цю проблему через концепцію «ринків поведінкових прогнозів»: інформація про людину перетворюється на потужний інструмент впливу, за допомогою якого можна маніпулювати рішеннями і навіть змінювати моделі поведінки. Внаслідок цього існує реальна небезпека, що людська автономія стає ілюзорною, а поведінка людей дедалі більше підкоряється зовнішнім алгоритмічним впливам та контролю [57].

Таким чином, реальні кейси, такі як скандал із Cambridge Analytica чи ситуація навколо Clearview AI, не просто демонструють нам технічні недоліки чи слабкі місця сучасних систем, але й ставлять гострі філософські питання щодо меж втручання технологій у приватний простір людини. Ці випадки висвітлюють фундаментальне протистояння між безмежними можливостями нових технологій і базовими гуманістичними цінностями. Для того, аби зберегти суспільну довіру, захистити демократичні інституції та поважати автономію людини, сьогодні надзвичайно важливо розробляти чіткі етичні стандарти та юридичні рамки, які б обмежували безконтрольну владу над персональними даними.

2.2. Свобода волі та проблеми збору та обробки персональних даних

Сучасні цифрові технології дозволяють збирати й аналізувати безпрецедентні обсяги персональних даних. Це породжує низку філософсько-етичних проблем, адже збір і обробка даних про особу стосується базових категорій довіри, згоди, автономії, об’єктивації людини, практик спостереження та влади. Приватність як етична цінність постає під загрозою у світі, де майже кожна дія залишає цифровий слід. Як зазначає український дослідник О. Дзьобань, в інформаційну добу приватність стала однією з

нових «цифрових» цінностей людини, яку необхідно захищати на рівні з традиційними правами і свободами [4, с. 9-19]. Водночас цифрове суспільство змінює не тільки те, що ми робимо, а й те, ким ми є і маємо стати [3, с. 108], що виклики у сфері персональних даних є значно глибшими, ніж може здатися на перший погляд. Головним питанням для етики приватності залишається те, наскільки люди можуть реально довіряти тим організаціям, які збирають та обробляють інформацію про них, і чи їхня згода на використання даних є по-справжньому усвідомленою. Це перегукується з класичним визначенням приватності Алана Вестіна, де він особливо підкреслює важливість саме контролю особи над інформацією про себе. Як пише Вестін, «найбільш важливою точкою взаємодії приватності і спостереження є так звана сфера «допустимого відхилення» - тобто дій, які хоча й не є забороненими законом чи не караються жорстко, але розкриття яких може мати негативні соціальні чи економічні наслідки для індивіда.[16] Однак, у сучасному цифровому суспільстві забезпечення такого контролю стає вкрай проблематичним. Користувачі масово погоджуються на обробку персональних даних, зазвичай навіть не знайомлячись детально з політикою конфіденційності, що перетворює цю згоду на чисту формальність, позбавлену реального волевиявлення людини. Фактично, така «згода» перестає бути виразом автономії особистості й більше нагадує ритуальну процедуру, ніж реальне прийняття рішення. Гелен Ніссенбаум звертає увагу на те, що найбільш серйозні порушення приватності виникають саме тоді, коли особисті дані використовуються у спосіб, що не відповідає початковому контексту, в якому вони були надані. Її теорія «контекстуальної цілісності» вимагає, щоб будь-яке збирання чи поширення персональної інформації відбувалося винятково в межах тих соціальних норм та очікувань, в рамках яких ці дані були початково розкриті. Іншими словами, для збереження приватності важливе не просто формальне отримання згоди, а й дотримання контекстних норм, які визначають, як саме можна використовувати інформацію про особу [45, с. 101- 139]. Інакше кажучи, навіть якщо людина

надає дані з певною метою, використання їх у іншому контексті без додаткової згоди підриває довіру. Довіра ж є фундаментальною умовою цифрового суспільства: без неї неможливе повноцінне функціонування ні цифрової економіки, ні демократії. Коли користувачі дізнаються про приховане стеження або витоки даних, це підриває їхню довіру до і державних інституцій, і до бізнесу.

Масштабне збирання персональних даних сьогодні ставить перед нами фундаментальні питання про захист автономії та гідності людини. Персональні дані фактично є цифровим продовженням нашої особистості, і від того, як вони використовуються, залежить, чи посилюється, чи навпаки, послаблюється індивідуальна свобода й самостійність людини. Якщо особа не має можливості контролювати інформацію, яку про неї збирають, і спосіб її подальшого використання, вона неминуче втрачає частину власної автономії. Виникає ризик зведення особистості до набору цифрових характеристик, що створює передумови для об’єктивації - коли людину починають сприймати вже не як самодостатню мету, а лише як засіб для досягнення певних цілей, таких як максимізація прибутку або оптимізація процесів прийняття рішень. У цьому сенсі надзвичайно актуальною стає згадка про фундаментальний моральний принцип Канта, згідно з яким людина ніколи не повинна використовуватися лише як засіб - вона завжди має залишатися кінцевою метою. Однак сучасні алгоритмічні технології дуже часто ігнорують цей принцип: автоматизовані системи оцінки кандидатів при працевлаштуванні або ухвалення рішень щодо кредитоспроможності здебільшого орієнтуються не на індивідуальні характеристики конкретної людини, а на абстрактні алгоритмічні профілі, побудовані на основі аналізу масивів даних. Тим самим людина фактично перетворюється на набір цифр та параметрів, які вирішують її долю без урахування особистих якостей. Відомий соціолог Девід Ліон підкреслює, що сьогодні цифрове спостереження вийшло далеко за рамки простого контролю й перетворилося на потужний механізм «соціального сортування». Ідеться про те, що збір і

аналіз персональних даних тепер не лише загрожує індивідуальній свободі, але й створює умови для довгострокового закріплення соціальних відмінностей. Людей сортують за ризиками, важливістю чи статусом, визначаючи для них місце в суспільстві, часто без можливості оскарження чи навіть розуміння того, як це рішення було ухвалене. Таким чином, приватність стає не просто питанням особистої захищеності, а й важливим фактором соціальної справедливості й людської гідності [25]. Іншими словами, масова обробка даних про людей здатна обмежувати їхню автономію через нав'язування певних ярликів і сценаріїв поведінки. Сама людина може не усвідомлювати, що її життя «під капотом» алгоритмів: якісь аспекти підсвічуються, інші ігноруються, - і в результаті її можливості діяти на власний розсуд звужуються. Водночас цифрова культура породила і добровільну об'єктивацію: в соціальних мережах користувачі самі викладають величезний масив приватної інформації про себе, часто прагнучи схвалення у вигляді вподобань. Це явище вчені називають саморозкриттям або навіть «самоспостереженням», коли особа ніби стає об'єктом спостереження для самої себе, підлаштовуючи свою поведінку під очікування аудиторії. Філософські наслідки такої добровільної передачі даних двозначні: з одного боку, реалізується свобода самовираження, а з іншого - виникає залежність від зовнішньої оцінки, що підточує автономність індивіда. Таким чином, практика збору персональних даних, будь то примусова чи добровільна, ставить питання про межі автономії особи у цифрову епоху.

«Збір даних невіддільний від спостереження (нагляду) за поведінкою людей. Філософ Мішель Фуко, розвиваючи ідею Дж. Бентама, ввів метафору паноптикуму – в'язниці, де наглядач невидимий, зате ув'язнені потенційно постійно спостерігаються і через це дисциплінують себе самі. У цифрову епоху паноптикум набув електронної форми: камери спостереження, інтернет-трекери, смартфони - усе це створює ефект всепроникного ока, за яким особиста сфера прозора, як крізь однобічне дзеркало. Люди починають

поводитися так, наче за ними постійно стежать, що обмежує їхню спонтанність і свободу самовираження» [31, с. 200]. Постійний нагляд (або навіть просто усвідомлення можливості нагляду) може привести до ефекту охолодження, коли особи уникають певних дій або висловлювань із страху бути зафіксованими та оціненими. Це стосується як державного спостереження (через камери, системи розпізнавання облич, стеження за інтернет-трафіком), так і комерційного (відстеження активності користувача в мережі, геолокації, покупок тощо). В обох випадках виникає асиметрія: той, хто спостерігає і збирає дані, набуває влади над тим, за ким спостерігають. Людина ж відчуває себе вразливою і безсилою перед обличчям невидимого цифрового контролю. Ш. Зубофф підкреслює, що в умовах «капіталізму спостереження» користувач фактично перетворюється на об’єкт, з якого непомітно екстрагують дані задля контролю над його поведінкою: «сутність цієї експлуатації - у перетворенні нашого життя на поведінкові дані заради покращеного контролю над нами з боку інших» [57, с. 66]. Отже, тотальне цифрове спостереження веде не лише до порушення приватності, а й до глибшого- трансформації суб’єктивності та волі людини, яка починає підлаштовуватися під очікування системи.

Інформація давно стала джерелом влади, а в цифрову епоху це набуло нового виміру. Ті, хто акумулює персональні дані, отримують однобічну перевагу – знання про людей, яке можна використати для впливу на них. Якщо в руках держави концентруються дані про життя громадян, виникає спокуса застосувати їх для посилення контролю над населенням. Після терактів та інших криз уряди деяких країн розширили практики масового нагляду, аргументуючи це безпекою. Проте філософи застерігають: поступаючись приватністю заради видимого спокою, суспільство ризикує втратити більше. Так, Л. Флоріді критикує підхід «спершу зібрати всі дані, а питання задати потім», називаючи його образою основам ліберальної демократії [44] . Показовим було викриття програм стеження АНБ (PRISM та ін.) Едвардом Сноуденом: воно продемонструвало, що навіть у

демократичних державах масове стеження може вийти з-під громадського контролю. Ю. Н. Харарі попереджає про небезпеку виникнення «цифрових диктатур» і «колонізацію даних». На його думку, якщо уряд чи корпорація матиме тотальний доступ до особистих даних кожного - від медичної історії до потаємних вподобань - то для встановлення контролю вже не потрібні солдати або поліція: «коли в когось є достатньо даних, не треба посилати військо, щоб контролювати країну» [35]. У таких умовах країни, що не володіють відповідними технологіями, ризикують стати просто «колоніями даних» для більш розвинених у цифровому плані держав. Ці застереження підкреслюють: влада, що дають персональні дані, без належних етичних обмежень здатна підірвати самі основи свободи і справедливості. З іншого боку, і приватні корпорації сьогодні володіють масивами даних, співмірними з державами. Виникла ситуація, за якої кілька техно-гігантів мають величезний вплив на життя мільярдів людей - від вибору, що ми читаємо й дивимося, до прогнозування нашої майбутньої поведінки. Етичне осмислення цих практик вимагає балансування між різними цінностями: безпекою і приватністю, інноваціями і повагою до автономії, комерційною вигодою і гідністю особи.

Отже, проблеми збору та обробки персональних даних у цифрову епоху мають комплексний і міждисциплінарний характер. Філософський підхід висвітлює, що на кону - базові принципи людського існування: довіра (без якої неможливий соціальний контракт у цифровому світі), свобода вибору і згода (які ризикують стати фікцією під тиском всевидящої технології), автономія особистості (що розмивається під впливом тотального нагляду та алгоритмічного «наставництва»), а також гідність і неповторність кожної людини (що підважуються, коли індивід редукується до набору даних). Збір даних - це завжди влада, і питання в тому, як забезпечити відповідальне, прозоре і людиноцентричне використання цієї влади. Без цього цифрове суспільство ризикує скотитися до технократичного утилітаризму, де зручність і ефективність ставляться вище за права людини. Подолати ці

загрози можливо лише на основі чітких етичних принципів і норм, що ставлять у центрі людську особистість, її свободу та приватність. У наступних розділах буде розглянуто, як саме світова спільнота намагається відповісти на ці виклики - від розробки міжнародних регуляцій до формування етичних кодексів захисту приватності. Але вже зараз очевидно: проблема персональних даних - це не лише про техніку чи право, це про наше бачення людини і того, яке цифрове майбутнє ми вважаємо прийнятним.

2.3. Вплив цифрових технологій на етику цифрової приватності

Цифрова революція сучасності докорінно змінює не лише повсякденне життя, а й моральні орієнтири суспільства. Новітні технології кидають виклик усталеним етичним принципам, зумовлюючи необхідність їхнього переосмислення. Дедалі більше дослідників відзначають, що інформаційна епоха формує особливу цифрову свідомість, яка трансформує традиційні духовно-моральні цінності [10]. Такі явища, як тотальна прозорість приватного життя, алгоритмічна маніпуляція вибором чи зміна уявлень про особисту ідентичність, оголюють конфлікт між технологічними можливостями та базовими принципами гуманізму. На цьому тлі в етиці набувають популярності постгуманістичні ідеї, що ставлять під сумнів антропоцентризм і пропонують розширити коло моральної відповідальності за межі суто «людського». Цифрові технології вимагають нових підходів до питань добра і зла, справедливості й відповідальності, оскільки вони суттєво впливають на норми поведінки та цінності.

Одним із концептів, що відображає ці зміни, є «цифрова людина» - новий етап розвитку Homo sapiens, тісно пов’язаний із технологіями. О. Дзьобань характеризує цифрову людину як «постмодерний вид людини розумної», здатний опрацьовувати колосальні обсяги інформації та існувати у віртуальних взаємозв’язках [4]. Ця homo digitalis живе в умовах перетину

реального і віртуального, що породжує нові екзистенційні й етичні питання. Передусім, як зауважує Дзьобань, «цифрова людина - це, перш за все, людина нових моральних цінностей, яка занурюється у віртуальну реальність симуляцій і усе більшою мірою сприймає світ як цифрове ігрове середовище…» [4, с. 9]. Отже, ціннісні орієнтири цієї нової людини помітно відрізняються від попередніх: реальність сприймається як пластична і керована, що розширює межі морально припустимого. Постгуманістична перспектива закликає етику врахувати таку трансформацію людської суб'єктності - коли межа між людиною і машиною розмивається, традиційні уявлення про автономію, відповідальність і навіть саму людську природу потребують перегляду.

Етика автономії посідає особливе місце в дискурсі про цифрові технології. Автономія особистості - один із наріжних каменів класичної етики (від Канта до сучасних прав людини) - наразі випробовується всепроникним цифровим середовищем. Практики стеження та мікротаргетингу можуть непомітно обмежувати свободу волі індивіда. Як стверджують деонтологічні підходи, використання людини лише як засобу, зокрема шляхом експлуатації її даних без достатньої згоди, порушує її гідність та автономію. Тож у цифрову добу постає вимога розробки етичних норм, що гарантували б повагу до особистісної автономії в нових умовах (право на контроль над інформацією про себе, свободу від маніпуляції тощо). Деякі філософи навіть говорять про розширення морального статусу на штучні автономні системи, однак першочерговим залишається захист автономії самої людини. Не випадково Ш. Зубофф та інші дослідники «капіталізму спостереження» наголошують, що неконтрольовані технології можуть «руйнувати нашу здатність керувати власними думками, емоціями та бажаннями» [57, с. 22]. Для етики це означає, що принцип поваги до автономії має бути впроваджений у дизайн технологій: від прозорості алгоритмів до забезпечення права на приватність і на opt-out (відказ від розсилки). У відповідь на ці виклики формується окрема інформаційна етика

- галузь прикладної етики, яка аналізує моральні аспекти поводження з інформацією та технологіями. Зокрема, українська дослідниця Т. Шоріна підкреслює, що «розвиток інформаційної етики та ретельне осмислення її драматичних проблем може і має сприяти їхньому подоланню, знаходженню стійких рішень, необхідних для того, щоби дати адекватні відповіді на технологічні виклики інформаційної епохи» [14, с. 74]. Іншими словами, тільки глибоке філософське осмислення безпрецедентних ситуацій, породжених цифровізацією, дозволить виробити нові етичні норми, адекватні часу.

Важливим аспектом впливу технологій на етичні норми є зміна уявлень про ідентичність і приватність. Цифрове середовище суттєво розширює межі самопрезентації особистості, водночас породжуючи ризики фрагментації «Я». У соціальних мережах, де люди конструюють образи себе, норми автентичності та щирості набувають нового значення. Г. Г. Супрун зазначає, що в епоху цифрових комунікацій індивідуальна ідентичність стає динамічною і залежить від віртуальної взаємодії [13]. З одного боку, це відкриває простір для самовираження, з іншого - ставить етичне питання: чи не втрачає особа свою цілісність, підлаштовуючись під цифрові ролі? О. Агарков звертає увагу на небезпеку того, що надмірне занурення у віртуальне життя послаблює унікальність особистості: «надмірне використання соціальних мереж може вести до втрати індивідуальності. Люди перестають розвивати свої власні інтереси та прагнення, і починають діяти відповідно до очікувань, які їм нав’язує соціальна мережа» [1, с. 73]. Втрата автономності суджень та конформізм під тиском цифрових трендів - серйозний виклик для етики особистісного розвитку. Традиційні моральні норми - щирість, відповідальність за свої слова, повага до приватності іншого - потребують оновленого тлумачення у контексті онлайн-взаємодій. Одночасно виникають і нові норми, такі як нетікет (етикет спілкування в інтернеті), правила поводження в кіберпросторі, що поступово оформлюються в спільнотах як негласні етичні стандарти. Українська етична

думка приділяє значну увагу цим явищам: від досліджень інформаційної безпеки особистості до аналізу моральних дилем кіберсоціалізації [13].

Таким чином, цифрові технології докорінно змінюють етичний ландшафт сучасного світу, ставлячи під сумнів усталені моральні принципи та створюючи умови для їх перегляду. Від постгуманістичних концепцій, що відходять від звичного антропоцентризму, до конкретних практичних норм інформаційної етики - всюди простежується необхідність пошуку нових орієнтирів. Традиційні гуманістичні цінності набувають нового звучання: повага до гідності людини тепер немислима без захисту її цифрового простору; свобода вимагає запобігання прихованим алгоритмічним маніпуляціям, а справедливість - недопущення дискримінації, яку можуть породжувати новітні технології. Крім того, формуються зовсім нові цінності, що доповнюють класичну моральну парадигму, зокрема відкритість цифрових даних та ідея цифрової справедливості. Українські дослідники й філософи, зокрема Валентина Воронкова, Олександр Дзьобань та Тетяна Шоріна, відіграють важливу роль у цьому переосмисленні, поєднуючи глибоку гуманістичну спадщину з актуальними глобальними викликами. Саме їхні праці сьогодні стають фундаментом для побудови нової етики цифрового суспільства - етики, яка здатна регулювати стосунки між людиною та цифровими технологіями на основі відповідальності, поваги до автономії та людяності. Основною метою цього етичного переосмислення є спрямування технологічного розвитку на служіння людині, а не навпаки. Іншими словами, етичний контроль має бути постійним супутником цифрового прогресу, щоб запобігти ситуації, коли людина стає додатком до технологій. Лише за такої умови моральні норми збережуть свій гуманістичний зміст і продовжать бути орієнтиром для розвитку, навіть коли змінюються форми людського існування у цифрову добу.

РОЗДІЛ 3. ЕТИКО-ПРАВОВІ АСПЕКТИ РЕГУЛЮВАННЯ ЦИФРОВОЇ ПРИВАТНОСТІ

3.1. Міжнародні стандарти та регламенти у сфері захисту даних

З розвитком інформаційних технологій постало питання специфічних гарантій у сфері обробки персональних даних, що виходять за рамки загальних декларацій і вимагають детального регулювання. Вже наприкінці XX ст. ООН розробила перші універсальні принципи поводження з персональною інформацією: «Керівні принципи щодо регулювання комп'ютеризованих персональних даних» (1990) проголосили, зокрема, принцип законності і сумлінності, за яким «інформація про особу не повинна збиратися чи оброблятися несправедливими або незаконними способами» [8]. Ці керівні принципи, поряд із схожими нормами Організації економічного співробітництва та розвитку, заклали основу для глобального консенсусу щодо стандартів захисту даних.

Важливим кроком стала Рекомендація ОЕСР 1980 р. із восьми принципами приватності (законність, обмеження мети, мінімізація даних тощо), що на багато років наперед визначили стандарт поводження з даними в демократичних державах. Згідно з оцінкою ОЕСР, ці настанови «продовжують уособлювати міжнародний консенсус щодо загальних правил збирання та обробки персональної інформації. Визначаючи основні принципи, Настанови відіграють провідну роль у допомозі урядам, бізнесу і споживачам захищати приватність і персональні дані, водночас уникаючи невиправданих обмежень трансграничних потоків інформації» [33, стр 7]. Інакше кажучи, вже на початку інформаційної доби утвердилася думка, що вільний обіг даних не суперечить приватності, якщо існують чіткі універсальні правила поводження з ними. Цей баланс між захистом даних і вільним інформаційним обміном пізніше ліг в основу багатьох міжнародних документів. Зокрема, в межах Азійсько-Тихоокеанського економічного

співробітництва був ухвалений APEC Privacy Framework (2005, оновлений 2015 р.), який проголосив гнучкий підхід до регулювання: «Рамка приватності АТЕС сприяє гнучким підходам до захисту інформаційної приватності в державах-учасниках, уникаючи створення зайвих бар'єрів для потоків інформації» [18, с. 3]. Таким чином, і Західні, і Азійсько-Тихоокеанські країни визнали необхідність погоджених принципів, що дозволяють одночасно забезпечувати приватність особи та розвиток цифрової економіки.

Найбільш розвинену систему захисту даних створено в Європі, де право на приватність розглядається як невід'ємна складова гідності та автономії особи. Ще 1981 року Рада Європи ухвалила Конвенцію №108 «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних», що стала першим глобальним юридично обов'язковим інструментом у цій сфері. Її сучасна оновлена версія, відома як Конвенція 108+ (протокол 2018 р.), закріплює підвищені стандарти безпеки і права суб'єктів даних. Рада Європи наголошує, що Конвенція 108+ - «віховий інструмент, який полегшує транскордонний обмін даними та водночас поважає людську гідність у цифрову добу», адже «поновлює статус людини як суб'єкта, а не об'єкта алгоритмічного аналізу чи контролю, встановлюючи загальноприйнятний рівень захисту, щоб гарантувати її гідність і приватність та право на інформаційне самовизначення» [23]. Іншими словами, європейський підхід виходить з імперативу розглядати індивіда не як пасивний об'єкт технологій, а як носія невід'ємних прав, що повинні поважатися навіть у цифрових процесах. Цей підхід спирається на глибокі філософські традиції: у кантіанській етиці наголошується на недопустимості трактувати людину лише як засіб для чужих цілей, і саме це лежить в основі принципу недоторканності приватного життя та особистих даних. Як вказує дослідник О. П. Дзьобань, сучасна «цифрова людина» постає одночасно об'єктом і суб'єктом інформаційних відносин, що означає необхідність нових підходів до гарантування її прав в інформаційному суспільстві [4, с. 9].

Європейський Союз, розвиваючи ідеї Конвенції 108, пішов ще далі у закріпленні права на захист даних. Хартія фундаментальних прав ЄС (2000) вперше виділила захист персональних даних як окреме основоположне право (ст. 8) поряд із правом на приватне життя (ст. 7). Це відображає усвідомлення того, що в цифрову епоху простого права на недоторканність приватного життя вже недостатньо, потрібні спеціальні гарантії контролю над інформацією про особу. У 2016 р. в ЄС було прийнято Загальний регламент із захисту даних [32] - нормативний акт прямої дії, який набув чинності у 2018 р. GDPR встановив жорсткі вимоги та принципи обробки даних (законність, прозорість, мінімізація, точність, збереження цілісності тощо) та надав громадянам розширені права - на доступ, виправлення, видалення («право на забуття«), заперечення проти профілювання і т.д. Вперше було впроваджено принцип прозорості і підзвітності, а також запроваджено серйозні санкції за порушення (штрафи до 20 млн євро або 4% обороту компанії). Європейський підхід швидко став орієнтиром для всього світу: як зазначає Європейський інспектор із захисту даних, «європейське законодавство про дані давно вважається «золотим стандартом« у всьому світі» [28, с. 1]. Багато країн поза ЄС прийняли закони, подібні до GDPR, або ж співпрацюють з ЄС у сфері транскордонного обміну даними на основі його вимог. Таким чином, на початку XXI ст. формується глобальна нормативна парадигма, в якій GDPR виконує роль де-факто модельного закону, а Конвенція 108+ - платформи для міжнародного правового співробітництва у сфері приватності [23].

Попри різноманітність підходів (жорсткі регламенти ЄС, гнучкі рамкові принципи APEC тощо), всі ключові міжнародні акти у сфері захисту даних об’єднує спільне розуміння базових цінностей. Йдеться про повагу до приватності, автономії та гідності кожної людини в умовах цифрової революції. Ці цінності мають не лише юридичне, а й глибоке філософське підґрунтя. Приватність розглядається як передумова індивідуальної автономії та свободи самовираження. Недарма в Європі захист даних прямо пов’язують

з охороною людської гідності: як наголошує Європейський інспектор із захисту даних, «приватність є невід'ємною частиною людської гідності, а право на захист даних було задумане в 1970-80-х роках як компенсація можливого підриву приватності та гідності через масштабну обробку інформації» [28, с. 5]. Тобто, у відповіді на сучасні цифрові загрози акцент зроблено на захисті самоцінності особистості: масова слідкувальна і профілююча діяльність не повинна звести людину до «прозорого» об'єкта, позбавленого таємниць і самостійності. Навпаки, міжнародні стандарти прагнуть забезпечити такі умови, за яких технологічний прогрес служить людині, а не принижує її.

Важливо підкреслити, що право на приватність у цифрову епоху тісно пов'язане з підтриманням особистої ідентичності та індивідуальності людини. Сучасні дослідники застерігають, що тотальна відкритість та соціальна підключеність можуть негативно позначитися на самостійності особистості. Наприклад, О. А. Агарков зазначає, що надмірне захоплення соціальними мережами «може спотворювати індивідуальність людей, призводити до залежності… та впливати на їхню соціальну поведінку» [1, с. 74]. Людина ризикує втратити автономність свого «Я», підмінити її конформізмом або залежністю від зовнішніх оцінок. Тому міжнародні нормативні акти щодо захисту даних слугують не лише технічними правилами, а й своєрідними етичними орієнтирами, що мають уберегти особистість від розчинення в цифровому середовищі. Як слушно зауважує Т. Г. Шоріна, масштабність і неоднозначність сучасних інформаційних викликів потребує «адекватної моральної регуляції людської практики в інформаційній культурі» [14, с. 78]. В цьому сенсі міжнародні стандарти захисту даних можна розглядати як матеріалізацію етико-правових ідеалів: вони покликані забезпечити гармонійне поєднання технологічного розвитку і поваги до прав людини. Ключові поняття приватності, автономії та гідності, осмислені в філософському дискурсі, знаходять своє практичне втілення в нормах GDPR, Конвенції 108+, принципах ОЕСР, АТЕС та інших актів.

Завдяки цьому вибудовується цілісна глобальна система, в якій цифрова приватність визнається необхідною умовою збереження людяності в епоху інформаційних технологій.

Філософське осмислення ролі сучасних інституцій у контексті цифрових трансформацій відкриває новий погляд на природу відповідальності. Якщо традиційна етика передусім оцінювала наміри, дії або чесноти окремої людини, то тепер на перший план виходить колективна, розподілена відповідальність. Сучасні технологічні системи є настільки багаторівневими та складними, що їхні наслідки формуються діями багатьох учасників одночасно: від розробників алгоритмів і провайдерів послуг до кінцевих користувачів і державних регуляторів. У результаті виникає феномен так званої «розмитої відповідальності» (diffused accountability), за якої жоден конкретний індивід повністю не контролює кінцевий результат, але організація або інституція в цілому все одно несе моральну відповідальність за впроваджувані технології. Сьогодні багато філософів-етиків наголошують, що в умовах мережевої структури взаємодії майже неможливо чітко визначити індивідуальну відповідальність. Натомість значно ефективніше і логічніше покладати моральні зобов’язання на колективні суб’єкти - команди, компанії, державні установи. Через це інституції все частіше розглядаються як повноцінні моральні агенти, які мають не лише дотримуватися, а й активно втілювати етичні принципи. Від них очікують, наприклад, реалізації кантівського принципу ставлення до людини як мети, а не просто засобу, в усіх алгоритмічних рішеннях. Також вони мають впроваджувати бентамівський ідеал максимальної користі, водночас не допускаючи обмеження прав меншості у своїх цифрових політиках. Інституції повинні нести так звану «відповідальність за майбутнє», як її окреслював Ганс Йонас, тобто передбачати довгострокові наслідки впровадження технологій для людської свободи, автономії та гідності. Саме через спеціальні механізми – етичні комісії, цифрових омбудсменів, міжнародні хартії та угоди – абстрактні моральні принципи стають

реальністю у сучасному цифровому світі. Як наголошують західні дослідники, без чітких стандартів щодо штучного інтелекту та даних поглиблюватиметься суспільна недовіра до демократичних інституцій. Водночас відповідальний розвиток ШІ може стати не лише інструментом захисту людських прав, а й чинником посилення демократичних цінностей: прозорості, підзвітності та відкритості. Відтак, етичні трансформації інституцій, починаючи від локальних українських ініціатив на зразок «Дії» і завершуючи глобальними зусиллями ЮНЕСКО, формують новий інституційний рівень «цифрової моралі». Цей процес охоплює зміни законодавства, етичних норм та державних структур так, щоб технологічний прогрес розвивався у повній відповідності до гуманістичних орієнтирів. Саме інституції мають гарантувати, що в епоху стрімкої цифровізації моральні цінності будуть не лише проголошуватись, але й ефективно реалізовуватись, захищаючи права, свободи і гідність кожної людини в умовах тотального інформаційного середовища.

Перехід від суто декларативного проголошення етичних норм до їх реального застосування потребує суттєвого переосмислення ролі й функцій соціальних інституцій. Саме організації та державні структури виступають важливими посередниками, які перетворюють загальні моральні ідеї у конкретні політики, стандарти й повсякденні практики. Сучасні дослідники наголошують, що цифрова епоха породжує новий тип особистості - «людину нових моральних цінностей», яка постійно перебуває у цифровому просторі й сприймає своє середовище через призму керованих технологічних систем. У зв’язку з цим інституції також повинні пройти трансформацію, щоб ефективно передавати і підтримувати нові етичні орієнтири. Їх завдання - не лише чітко формулювати моральні принципи, але й запроваджувати конкретні механізми їх реалізації, такі як внутрішні етичні кодекси, регулярні етичні аудити, незалежні наглядові органи або комісії з питань цифрових прав. Тільки так інституції зможуть зберегти й посилити моральний порядок

у суспільстві, де технології дедалі глибше проникають у життя кожної людини.

В Україні з'являються приклади інтеграції етичних стандартів у практику як державного, так і приватного сектору. Міністерство цифрової трансформації декларує пріоритет «відповідального розвитку ШІ» у всіх проєктах цифровізації, розуміючи, що довіра громадян залежить від прозорості та безпечності електронних сервісів. Флагманський проєкт «Дія» демонструє, як принципи конфіденційності, зручності та підзвітності можуть бути закладені в основу національної електронної послуги - через захищеність даних, відкритість коду та врахування прав користувачів. У співпраці з європейськими партнерами Україна формує власні стандарти етики даних: так, при Мінцифри створено експертні групи з питань штучного інтелекту, обговорюється впровадження посади офіцера з питань етики даних за аналогією до вимог GDPR (де кожна велика організація має призначити Data Protection Officer). Громадянське суспільство теж відіграє важливу роль. Центр демократії та верховенства права (CEDEM) у своїх аналітичних звітах підкреслює необхідність переходу «від гучних заяв до практики» регулювання ШІ, закликаючи приватний сектор і державу забезпечувати відповідність алгоритмічних систем правам людини та етичним принципам. Зароджується і практика аудиту AI - незалежного оцінювання алгоритмів на упередженість та законність - що поступово впроваджується як інструмент підвищення етичності у діяльності організацій (наприклад, в сфері фінансів і рекрутингу компанії здійснюють зовнішні «етичні аудити» своїх алгоритмів). Українські фахівці усвідомлюють світовий тренд: лише інституційна підзвітність і прозорість можуть гарантувати дотримання прав користувачів у цифровому просторі. Як зауважує О. П. Дзьобань, «цифрова людина» живе у новій реальності, тому і соціальні структури повинні сформувати нові механізми моральної регуляції. Впровадження етичних комітетів, кодексів поведінки для ІТ-спеціалістів та регулярні навчання з інформаційної етики для посадовців - усе це стає частиною організаційної практики в Україні,

особливо в сферах, дотичних до обробки персональних даних або використання ШІ. [4]

Наявність Data Protection Officer у міністерствах, муніципалітетах і корпораціях стала стандартом етичної підзвітності: цей фахівець моніторить обробку даних, проводить оцінки впливу на приватність та навчає персонал етичним правилам поводження з інформацією. Ще одним прикладом є запровадження етичних наглядових рад при технологічних компаніях - так, корпорації Google, Microsoft, SAP та інші у 2018-2020 рр. створили внутрішні AI Ethics Boards для оцінки ризиків нових розробок (хоча ефективність таких рад залежить від реальної підтримки керівництва). У Великій Британії з 2018 р. діє Рамковий кодекс етики даних (Data Ethics Framework) - система принципів і рекомендацій для державних установ щодо прозорого, підзвітного та справедливого використання даних. Цей документ вимагає врахування суспільних інтересів при впровадженні цифрових сервісів і фактично інституціалізує моральні цінності у повсякденну діяльність чиновників. У Канаді на державному рівні введено обов'язкову процедуру оцінювання алгоритмічного впливу (Algorithmic Impact Assessment) перед впровадженням будь-яких систем штучного інтелекту в державних установах. Це означає, що жодна технологічна новація не може бути затверджена без попереднього публічного аналізу потенційних ризиків для людських прав, а також без консультацій із громадськістю. Таким чином, канадський уряд створює важливий прецедент відкритості й залучає громадянське суспільство до процесу етичного контролю над цифровими технологіями. Аналогічно й інші країни, серед яких Німеччина, Франція, Австралія, активно залучають громадськість та експертів до широких консультацій при ухваленні цифрових рішень. Це стосується різних питань - від введення біометричних документів до стратегій розвитку штучного інтелекту на національному рівні. Мета таких консультацій - почути й врахувати етичні застереження громадян, а також їхні очікування та цінності. Цей підхід, який можна назвати демократичним діалогом, стає окремим

етичним принципом управління: рішення щодо впровадження технологій ухвалюються не закритими дверима, а в атмосфері прозорості й з урахуванням суспільної думки та моральних пріоритетів громадян.

3.2. Основні етичні принципи та кодекси захисту цифрової приватності

Основою етичного регулювання цифрової приватності є глибокі моральні принципи, спрямовані на те, щоб у сучасному інформаційному суспільстві зберегти повагу до особистості й гарантувати людині свободу її приватного простору. Як наголошує дослідниця Т. Шоріна, сьогоднішні виклики у сфері інформаційної етики характеризуються значною складністю і конфліктністю, а тому потребують продуманої й відповідної моральної регуляції людської діяльності в умовах цифровізації культури [14, с. 75]. Це означає, що самих лише юридичних засобів захисту приватності вже недостатньо - вони мають бути доповнені етичними рамками, що чітко встановлюють, як саме допустимо поводитися з персональною інформацією, та зобов’язують учасників цифрового середовища дотримуватись базових прав і свобод людини. Цифрова приватність тісно пов’язана з базовими цінностями - автономією особистості, свободою вибору, довірою і повагою до людської гідності. Відтак, у центрі етичного дискурсу знаходяться принципи, що забезпечують баланс між технологічним поступом і захистом приватного життя. Розглянемо ключові з них та відображення цих принципів у міжнародних етичних кодексах.

Автономія особи передбачає її право контролювати власну інформацію та самостійно вирішувати, кому і в який спосіб вона розкривається. Цей принцип лежить в основі вимоги інформованої згоди: збір і використання персональних даних етично виправдані лише за умови, що індивід добровільно і усвідомлено на це погодився. У професійних кодексах ця ідея закріплена як обов’язок поважати приватність. Зокрема, ACM Code of Ethics

містить імператив «Respect privacy» - поважати приватність, наголошуючи, що відповідальність за забезпечення приватності покладається на ІТ-фахівців у особливо сильний спосіб [15]. Технології дають змогу збирати і аналізувати особисті дані в безпрецедентних масштабах, тож професіонали мають бути обізнані з різними аспектами приватності та нести моральний обов'язок захищати конфіденційність даних. Принцип захисту таємниці приватного життя безпосередньо виражає право людини на автономію і свободу у приватному житті, право на захист від вторгнення сторонніх осіб чи держави. Таким чином, етичний імператив автономії вимагає забезпечити, щоби людина залишалася господарем своїх даних, а будь-яка обробка інформації про неї відбувалася з її відома та згоди.

У цифровому середовищі надзвичайно важливо, щоб всі сторони - від розробників програм до посадовців і корпорацій - усвідомлювали свою моральну відповідальність перед особою, чиї дані обробляються. Етичний принцип non-maleficence (не нашкодь) вимагає запобігати діям, які можуть завдати шкоди правам чи свободам людини, в тому числі її праву на приватність. У першому пункті етичного кодексу IEEE інженерам наголошується на необхідності усвідомлювати свою відповідальність за ті рішення, які впливають на життя й благополуччя суспільства. Це означає, що професіонали зобов'язані заздалегідь передбачати потенційні ризики для приватності користувачів і ширших суспільних інтересів, уникаючи будь-яких дій, які можуть призвести до неналежного використання чи розголошення особистої інформації. В усіх глобальних професійних кодексах присутня норма соціальної та особистої відповідальності ІТ-фахівця, а значить - обов'язок діяти етично навіть там, де закон прямо не регулює поведінку. Принцип відповідальності тісно пов'язаний із принципом підзвітності: організації мають бути готові відкрито звітувати про те, як вони збирають, зберігають і використовують дані, та нести реальну відповідальність у разі порушень приватності.

Прозорість (транспарентність) означає відкритість і зрозумілість процесів обробки даних. Щоб забезпечити повагу до автономії, суб'єкти даних повинні знати, які саме їхні дані збираються і з якою метою. Принцип прозорості водночас служить передумовою суспільної довіри: коли діяльність цифрових систем є зрозумілою, менше підстав для підозр у зловживаннях. На міжнародному рівні прозорість дедалі частіше фіксується як етична вимога. Приміром, Європейська етична хартія щодо використання ШІ в правосудді [27] серед п'яти базових принципів містить принцип прозорості, неупередженості та справедливості, згідно з яким «методи обробки даних повинні бути доступними та зрозумілими», забезпечуючи можливість перевірити обґрунтованість та законність автоматизованих рішень. Справедливість у контексті приватності насамперед пов'язана з недискримінацією: дані про особу не мають використовуватися для упередженого ставлення чи порушення рівності можливостей. Етичний принцип справедливості вимагає збалансувати інтереси різних сторін і захистити найбільш уразливих. Зокрема, Хартія Ради Європи щодо етики ШІ підкреслює неприпустимість будь-якої дискримінації осіб чи груп при використанні алгоритмів. Таким чином, прозорість і справедливість доповнюють одна одну: відкритість інформації про алгоритми і практики обробки даних дозволяє виявити та усунути несправедливі або непропорційні впливи на приватне життя людей.

Зазначені принципи- автономія, відповідальність, прозорість, справедливість та інші - знайшли відображення у низці впливових етичних кодексів та декларацій, що регулюють діяльність у сфері ІТ. Кодекс етики ACM (Association for Computing Machinery)[15] прямо проголошує обов'язок поважати приватність і конфіденційність, акцентуючи, що ІТ-професіонал «must maintain the privacy and integrity of individuals' data, guarding it against unauthorized access чи помилкове використання». Кодекс етики IEEE [39] орієнтує на чесність, чесність і турботу про добробут користувачів, що опосередковано включає захист їхньої приватності. У 2021 році Міжнародна

федерація з обробки інформації (IFIP) ухвалила Global Code of Ethics for ICT, який узагальнив універсальні етичні принципи для цифрової сфери. У першому розділі цього кодексу закріплено сім спільних для різних професій принципів, серед яких - повага до прав людини, приватності, доброчесність, справедливість тощо. Цікаво, що всі ці документи, хоч і розроблені різними організаціями, багато в чому перегукуються між собою. Як зауважують українські дослідники, у професійних етичних кодексах для ІТ «фіксуються базові права, що належать кожному учаснику віртуальної комунікації» - і ці права ґрунтуються на дотриманні саме згаданих моральних принципів: приватності (таємниці особистого життя), загальнодоступності інформації та недоторканності власності. Отже, можна говорити про глобальний консенсус щодо ключових цінностей цифрової етики.

В українському академічному дискурсі також наголошується на важливості етичних принципів для захисту приватності. В. Г. Воронкова та ін. у монографії «Філософія цифрової людини і цифрового суспільства: теорія і практика» (2022) підкреслюють, що розвиток цифрового суспільства потребує формування нової системи етичних регулятивів, які б гарантували збереження автономії особистості в умовах тотальної діджиталізації. О.П. Дзьобань зазначає, що поява феномену «цифрової людини» ставить перед нами нові моральні виклики: з одного боку, технології надають небачені можливості, а з іншого - «породжують питання щодо захисту особистої інформації та права на приватність» [4, с. 17]. Тільки спираючись на чіткі етичні принципи, суспільство здатне відповісти на ці виклики. Приміром, проникнення соціальних мереж у повсякденне життя, про яке пише О. А. Агарков [1], вимагає нового розуміння меж приватного і публічного, а відтак-перегляду етичних норм онлайн-комунікації. Саме етичні принципи виступають тим фільтром, що відділяє легітимний моніторинг від неприйнятного стеження, а персоналізований сервіс - від маніпуляції поведінкою користувача.

Таким чином, основні етичні принципи захисту приватності - повага до автономії особи (і пов’язана з нею інформована згода), відповідальність і підзвітність, прозорість і чесність, справедливість і недискримінація, а також дотримання конфіденційності як професійного обов’язку - формують моральний каркас цифрової епохи. Вони закріплені у міжнародних етичних кодексах на кшталт ACM, IEEE, IFIP, у європейських хартіях та деклараціях, і підтримані українськими науковцями. Ці принципи не просто мають теоретичне значення - їх практичне впровадження є запорукою того, що технології служитимуть людині, не порушуючи її прав. Етичні кодекси, що спираються на зазначені цінності, відіграють роль путівника для розробників, політиків і всіх, хто працює з даними. Вони нагадують, що в центрі будь-якої цифрової системи має залишатися людина як самоцінність, а її приватне життя – недоторканним і захищеним на всіх рівнях регуляції.

ВИСНОВКИ

Етичні принципи цифрової приватності виступають не лише нормативними установками, а й глибокими моральними орієнтирами, які формують основу автономії та гідності в умовах стрімкої цифрової трансформації суспільства. Вони зосереджуються на захисті особистості як самодостатнього суб'єкта, здатного контролювати інформаційний простір, що її оточує. У цифрову епоху принципи прозорості та інформованої згоди вже не можна вважати другорядними - вони стають ключовими умовами збереження автономії особистості. Тільки тоді, коли людина чітко розуміє, які саме її дані збираються, з якою метою та за яких умов, можна говорити про справжню згоду, а не формальну «галочку». У свою чергу, принципи відповідальності та справедливості вказують на моральний обов'язок не допускати дискримінації, зловживань і нерівного поводження в інформаційному середовищі.

Приватність сьогодні виходить за межі індивідуального - вона дедалі більше набуває характеру суспільного блага. Вона забезпечує базу для довіри: між громадянином і державою, між користувачем і технологією. Втрата приватності - це не просто витік інформації, а втрата соціального і політичного балансу. Саме тому етичні принципи цифрової приватності можна розглядати як механізми, що утримують тонку рівновагу між свободою та контролем, між технологічним прогресом і людською гідністю. Ідеї на кшталт «privacy by design» чи впровадження етичних аудитів алгоритмів - це спроба зробити цю рівновагу реальною і дієвою, закріпити моральні принципи в інженерній та управлінській практиці.

Власне, у цій роботі я намагалася пройти шлях від філософських підвалин до конкретних етичних і правових рішень. Це був послідовний аналіз - від критики паноптичного суспільства і капіталізму спостереження до вивчення юридичних механізмів і етичних рекомендацій, які дають змогу захистити приватність не лише як право, а як форму поваги до людини в

цифровому світі. Спочатку вивчення еволюції уявлень про приватність від класики Просвітництва до сучасних течій інформаційної етики дозволило усвідомити, що приватність - це не лише право на недоторканість особистого життя, а радше складний феномен, що поєднує свободу автономного вибору, гідність особистості та право на контроль над власними даними. Кантівський імператив став точкою відліку: людина не може бути об'єктом для маніпуляцій, вона має залишатися автономним суб'єктом морального рішення, незалежно від того, чи йдеться про фізичну недоторканність, чи про інформаційну самозахист.

Далі філософське осмислення приватності розширилось через призму «контекстуальної цілісності» Гелен Ніссенбаум, яка вводить у дискурс важливе розрізнення між умовами, у яких інформація виникає, і способами її подальшого використання. Цей підхід розкриває одну з ключових цифрових проблем: дані, передані в одному контексті - наприклад, дружньої розмови чи медичного обстеження - можуть непомітно бути залучені в інший, де їхнє застосування порушує сподівання суб'єкта. Паралельно праці Шошани Зубофф про «капіталізм спостереження» відтворили драматургію сучасного світу даних, у якому людське життя стає сировиною для поведінкової аналітики й алгоритмічної корекції бажань. У цьому світлі приватність розкривається як політична й економічна зброя: її втрата спрощує управління масою, а збереження - уможливлює справжню автономію.

Наступним кроком стало виявлення й розгляд конкретних випадків порушень цифрової приватності: від скандалу Cambridge Analytica, що показав, наскільки легко психологічні профілі можуть бути використані для маніпуляції громадською думкою, до масових витоків персональних даних і систем розпізнавання облич, які поступово руйнують анонімність у публічному просторі. Під час аналізу «мозаїчного ефекту» Big Data було доведено, що навіть невеликі фрагменти інформації можуть, з'єднавшись разом, розкрити досить інтимні подробиці - від стану здоров'я до політичних уподобань. Цей феномен став ілюстрацією нової філософської проблематики:

питання про те, якою мірою людина здатна зберегти своє «Я» у ситуації нескінченного цифрового простору, де вся її поведінка конвертується в дані, що формують «другу її» - data-driven persona.

У рамках дослідження було також проведено детальний огляд міжнародних норм і етичних кодексів, що заклали фундамент для захисту цифрової приватності. GDPR та Конвенція 108+ проголосили автоматизовану обробку даних питанням фундаментальних прав людини, а кодекси ACM, IEEE і IFIP ввели обов'язок етичної відповідальності IT-професіоналів. Українські інституції, зокрема Міністерство цифрової трансформації та сервіс «Дія», продемонстрували готовність адаптувати ці стандарти, закладаючи принцип «privacy by design» в основу своїх проєктів. Водночас громадянське суспільство, представлено аналітичними центрами, наполягало на прозорості й підзвітності: без суспільного контролю навіть найдосконаліші правила залишаться декларативними.

Завершальним етапом стало осмислення моральних дилем і конфліктів, які виникають у процесі впровадження цифрових технологій. З одного боку, нефільтрована безпека може вимагати дедалі більш жорсткого стеження, з іншого - прагнення до абсолютного захисту приватності загрожує інноваціям і суспільному прогресу. Філософи говорять про «розмиту відповідальність» техногенних систем, де ніхто окремо не відповідає за наслідки алгоритмічних рішень, але відповідальність лежить на колективних агентах - організаціях і державах. Ця дилема стає викликом для етики: як побудувати модель, у якій технології служать людині, а не навпаки?

Завдяки послідовному виконанню завдань роботи вдалося поєднати глибокий філософський аналіз із практичною проблематикою цифрової приватності, виявити ключові моральні принципи, обґрунтувати їхню необхідність у сучасних нормах і продемонструвати шляхи втілення - від правових реформ до етичних аудиторій алгоритмів. Найважливіший висновок полягає в тому, що захист цифрової приватності - це не суто технічне завдання, але фундаментальний моральний імператив, без

виконання якого цифрова доба перетвориться на еру контролю й маніпуляції. Лише гармонія між філософією свободи, етикою відповідальності й ефективним регулюванням може забезпечити, що технології розкриватимуть потенціал людини, а не перетворюватимуть її на ресурс для алгоритмів. Збереження приватності стає гарантом людської гідності у світі, де інформація набуває потужності нової стихії, здатної змінювати свідомість і поведінку. Саме тому подальше дослідження має зосередитися на розробці інноваційних підходів до етичного дизайну технологій, культури цифрової відповідальності та вдосконалення правових механізмів, що здатні убезпечити особисту свободу в безмежному цифровому просторі.

Міжнародні декларації та конвенції закріпили приватність як невід'ємне право. Найбільш системною відповіддю став Загальний регламент із захисту даних ЄС (GDPR), який установив вимоги щодо прозорості, добровільної усвідомленої згоди, мінімізації даних та відповідальності при обробці інформації. Ці норми відображають важливі етичні імперативи і орієнтують цифрову індустрію на повагу до особи. Паралельно набувають поширення професійні етичні кодекси та принцип «privacy by design», що вимагають враховувати приватність ще на етапі розробки технологій. На національному рівні, зокрема в Україні, впроваджуються законодавчі зміни для гармонізації з міжнародними стандартами. Українські реалії - від законів про захист персональних даних до суспільних дискусій навколо впровадження систем спостереження - віддзеркалюють глобальну потребу знайти рівновагу між безпекою та правами особи. Отже, етико-правове регулювання формується як відповідь на техногенні загрози і прагне підпорядкувати цифрову силу даних гуманістичним цінностям.

Саме філософія цифрової етики сьогодні виконує роль того морального компаса, що дозволяє зрозуміти: де проходять межі припустимого втручання технологій у людське життя. Вона не просто реагує на зміни - вона змінює сам спосіб мислення про свободу, відповідальність і гідність у світі алгоритмів. У цьому контексті особливо важливими постають ідеї

справедливості та автономії - не як абстрактні категорії, а як принципи, що мають бути вплетені у саму структуру цифрових рішень. З’являються нові ключові поняття - «цифрова гідність», «інформаційне самовизначення» - які формують нову моральну мову. Пріоритетом залишається одне: технології мають створюватися так, щоби в їхньому центрі залишалась не система, а людина - зі своїм правом бути вільною, непроникною, людяною навіть у цифрі. Ця робота ще раз засвідчує: в умовах, коли інформація перетворилася на потужний інструмент впливу, саме поняття приватності потребує глибокого переосмислення. Йдеться вже не лише про захист персональних даних, а про збереження простору для автономії, внутрішньої свободи та гідності. Лише за умови поєднання філософського бачення, етичних орієнтирів і чітких правових механізмів можна забезпечити, щоб цифрова епоха не зруйнувала основу людяності, а навпаки - сприяла її розвитку.

У першому розділі дипломної роботи було здійснено філософське осмислення поняття приватності крізь призму класичних і сучасних етичних вчень. Починаючи від кантівського імперативу поваги до особистості як цілі самої по собі - до утилітаристських міркувань про баланс індивідуального блага і суспільної безпеки, приватність розглядається як фундамент людської гідності, автономії та свободи. У цьому контексті концепція «контекстуальної цілісності» Гелен Ніссенбаум відкрила нові горизонти для етики приватності в інформаційному суспільстві. Погляд Ніссенбаум дозволив переосмислити приватність не як абсолютну замкнутість, а як право на належний потік інформації у відповідному соціальному контексті.

У другому розділі було розглянуто сучасні виклики, з якими стикається приватність у світі великих даних, алгоритмів і штучного інтелекту. Коли розглядаєш такі кейси, як скандал з Cambridge Analytica чи використання систем розпізнавання облич компанією Clearview AI, стає очевидно: загрози приватності давно вже вийшли за межі звичних уявлень про контроль і нагляд. Те, що раніше здавалося справою лише права або моралі, сьогодні стало полем конфлікту – водночас політичного, економічного й

технологічного. І це добре видно у працях Шошани Зубофф, яка описує логіку «капіталізму спостереження», а також у теорії Девіда Лайона про «суспільство нагляду», де приватність дедалі більше перетворюється на ресурс, яким намагаються володіти. Автономія особи все більше піддається дії алгоритмів, що скеровують її рішення, прогнозують поведінку й формують уподобання. Особистість у цифровому середовищі - це вже не стільки суб'єкт волевиявлення, скільки масив даних, що підлягає аналізу та оптимізації.

У третьому розділі дипломної роботи було приділено увагу етико-правовим механізмам регуляції цифрової приватності. Міжнародні стандарти, зокрема GDPR та Конвенція 108+, закріплюють приватність як самостійну цінність і гарантують права на інформовану згоду, забуття, обмеження обробки даних. Аналіз кодексів етики (ACM, IEEE, IFIP) свідчить про глобальний консенсус у сфері цифрової відповідальності: автономія, справедливість, прозорість, підзвітність - ці принципи трансформуються у професійну і правову практику. Українські дослідники - Воронкова, Дзьобань, Шоріна, Агарков - наголошують, що цифрове суспільство формує нову моральну архітектоніку, в якій інституції, такі як Мінцифра, «Дія», громадські аналітичні центри, повинні не лише адаптувати норми, а й конструювати етичну інфраструктуру цифрової держави.

Таким чином, приватність у цифрову епоху - це не стільки захист минулого, скільки захист можливості мати майбутнє як моральна істота. Людина має залишатися не лише об'єктом аналізу, а насамперед суб'єктом права, гідності та свободи. І тому завдання філософії - бути сторожем цієї суб'єктності, її останнім захисником перед обличчям машин, що не знають сумніву, сорому і співчуття.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ ТА ДЖЕРЕЛ

1. Агарков О. А. Індивідуальність в цифрову епоху: як соціальні мережі впливають на самоідентифікацію. *Дніпровський науковий часопис публічного управління, психології, права*. 2023. № 1. С. 73-78.

2. Американська тікток паніка, українські тренди та нові виклики. URL: https://www.ukrinform.ua/rubric-world/3951967-amerikanska-tiktokpanika-ukrainski-trendi-ta-novi-vikliki.html#:~:text=на%20загрози%20національній%20безпеці%20саме,TikTok%20із%20кит

3. Воронкова В. Г., Нікітенко В. О. Філософія цифрової людини і цифрового суспільства: теорія і практика. Запоріжжя: Гельветика, 2022. 460 с.

4. Дзьобань О. П. Цифрова людина як філософська проблема. *Інформація і право.* 2021. № 37. С. 9-19.

5. «Джо Вестбі. Великий злам»: Cambride Analytica - тільки вершина айсберга. URL: https://www.amnesty.org.ua/velykyj-zlam/#:~:text=поведінку,та%20навіть%20змістом%20приватних%20повідо

6. Загальна декларація прав людини. ООН, 1948. Режим доступу: https://www.un.org/uk/universal-declaration-human-rights

7. Кейс Clearview AI. URL: https://tyzhden.ua/clearview-ai-znaty-voroha-v-lytse/#:~:text=17%20%D0%91%D0%B5%D1%80%D0%B5%D0%B7%D0%BD%D1%8F%202022%2C%2019%3A19

8. Міжнародний пакт про громадянські і політичні права. ООН, 1966. Режим доступу: https://www.un.org/uk/civil-political-rights.

9. Петрів О. Від гучних заяв до практики: реалії регулювання штучного інтелекту. CEDEM, 2024.

10. Роганов М. Л. Морально-етичні аспекти інформаційно-комунікаційних технологій. *Духовність особистості: методологія, теорія і практика.* 2020. № 95. С. 169-178.

11. Синиця А. С. Вступ до філософії штучного інтелекту. Львів: ЛНУ імені Івана Франка, 2023. 292 с.

12. Синиця А. С. Проблема розуміння в контексті критики комп'ютаціоналізму. *Філософські студії.* 2021. № 14. С. 5-25. URL:https://eprints.oa.edu.ua/id/eprint/2418/1/Synytsya_Filosof_Vyp_14.pdf

13. Супрун Г. Г. Ідентичність індивіда в цифрову епоху соціальних комунікацій. *Філософські обрії*. 2020. № 43. С. 85- 94.

14. Шоріна Т. Г. Філософський аналіз дискурсу інформаційної етики та її морально-практичних дилем. *Вісник Національного авіаційного університету. Серія: Філософія. Культурологія.* 2021. № 33. С. 74-79.

15. ACM Code of Ethics and Professional Conduct. URL: https://www.acm.org/code-of-ethics#:~:text=1

16. Alan F. Westin. Privacy and Freedom. New York: Atheneum, 1967. 384 p.

17. Alan F. Westin. Privacy And Freedom. *Washington and Lee Law Review*. 1968. Vol. 25, No. 1. P. 166-170.

18. APEC Privacy Framework. APEC Secretariat, 2015.

19. Bentham J. Panopticon: Or The Inspection House. - London, 1791.

20. Bletchley Declaration. United Kingdom, 2023. URL: https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration

21. Chapter 9. Kant's ethics in the age of online surveillance: An appeal to autonomy. Casey Rentmeester. URL: https://www.diva-portal.org/smash/get/diva2:1746832/FULLTEXT01.pdf#:~:text=For%20Kant%20,the%20vein%20of%20Marshall%20McLuhan

22. Charter of Fundamental Rights of the European Union. *Official Journal of the EU*. 2000. C 364/1.

23. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108). Council of Europe, 1981.

24. Data Ethics Framework. Government Digital Service (UK), 2020.

25. David Lyon. The Electronic Eye: The Rise of Surveillance Society. Minneapolis: University of Minnesota Press, 1994.

26. Ethics of Data Sharing and Digital Privacy. Mary Karapetyan. 2024. URL : https://vce.usc.edu/volume-7-issue-2/ethics-of-data-sharing-and-digital-privacy/#:~:text=Privacy%20is%20becoming%20a%20blur,and%20fairness%20in%20data%20ethics

27. European Commission for the Efficiency of Justice (CEPEJ). Evaluation Report on the Use of Artificial Intelligence in Judicial Systems. Council of Europe, 2022.

28. European Data Protection Supervisor. The History of the General Data Protection Regulation. EDPS Website. - 2018.

29. Facts and Figures 2024 URL: https://www.itu.int/itu-d/reports/statistics/2024/11/10/ff24-internet-use/#:~:text=In%202024%20fully%205,connectivity%20remains%20a%20distant%20prospect

30. Fitz-Gerald A. M., Padalko H. Restoring Trust in Democratic Institutions through AI Standards. Centre for International Governance Innovation, 2023.

31. Foucault M. Discipline and Punish: The Birth of the Prison / Translated by Alan Sheridan. New York: Vintage Books, 1977.

32. GDPR - General Data Protection Regulation, EU Regulation 2016

33. Guidelines for the Regulation of Computerized Personal Data Files. United Nations General Assembly Resolution 45/95. 1990.

34. Habermas J. The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society / Translated by Thomas Burger, with the assistance of Frederick Lawrence. Cambridge, MA: MIT Press, 1989.

35. Harari Y., Davos Speech, 2020 URL: https://www.weforum.org/stories/2020/01/yuval-hararis-warning-davos-speech-future-predications/#:~:text=produce%20textiles%20or%20cars%20in,colony

36. Harari Yuval N. 21 Lessons for the 21st Century. Spiegel & Grau, 2018.

37. Immanuel Kant. Beantwortung der Frage: Was ist Aufklärung? *Akademie-Ausgabe, Bd. 8*, 1784.

38. Immanuel Kant. Grundlegung zur Metaphysik der Sitten. *Akademie-Ausgabe, Bd. 4*, 1785.

39. Institute of Electrical and Electronics Engineers (IEEE). IEEE Code of Ethics. IEEE, 2020.

40. John Locke. Two Treatises of Government. URL: https://standardebooks.org/ebooks/john-locke/two-treatises-of-government

41. Joseph D'Souza. Data Privacy Statistics and Facts. 2024. URL: https://electroiq.com/stats/data-privacy-statistics/

42. J.S. Mill's great principle was that «over himself, over his own body and mind, the individual is sovereign« (1859) | Online Library of Liberty. URL: https://oll.libertyfund.org/quotes/j-s-mill-s-great-principle-was-that-over-himself-over-his-own-body-and-mind-the-individual-is-sovereign-1859#:~:text=that%20the%20sole%20end%20for,mind%2C%20the%20individual%20is%20sovereign

43. Judith J. Thomson. The Right to Privacy. *Philosophy & Public Affairs*. 1975. Vol. 4, No. 4.

44. Luciano Floridi. The Ethics of Information. Oxford: Oxford University Press, 2013.

45. Nissenbaum H. Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford: Stanford University Press, 2010.

46. Original Position (Stanford Encyclopedia of Philosophy) URL : https://plato.stanford.edu/entries/original-

position/#:~:text=First%20Principle%3A%20“Each%20person%20has,”%20%28TJ%20266

47. Privacy as a Utilitarian Value. Paul Rosenzweig. 2024. URL: https://www.lawfaremedia.org/article/privacy-utilitarian-value#:~:text=instrumental%20value%2C%20one%20that%20acts,Let%20me

48. Skinner C. Digital Human: The Fourth Revolution of Humanity Includes Everyone. London: Penguin Business, 2020.

49. Sunstein C. R. Nudging: A Very Short Guide. *Journal of Consumer Policy*. 2014. Vol. 37, No. 4.

50. Thaler R. H., Sunstein C. R. Nudge: Improving Decisions About Health, Wealth, and Happiness. New Haven & London: Yale University Press, 2008.

51. The Cambridge Handbook of Surveillance Law, David Gray, Stephen E. Henderson. URL: https://assets.cambridge.org/97811087/22100/frontmatter/9781108722100_frontmatter.pdf

52. Thompson J. J. The Right to Privacy. *Philosophy & Public Affairs*. 1975. Vol. 4, No. 4.

53. Turing A. M. Computing Machinery and Intelligence. *Mind*. 1950. Vol. 59, No. 236.

54. Utilitarianism and the pandemic. Julian Savulescu. URL : https://pmc.ncbi.nlm.nih.gov/articles/PMC7276855/#:~:text=1,rights%20and%20liberty

55. View of The ethics of unbreakable encryption. URL: https://firstmonday.org/ojs/index.php/fm/article/view/7006/5860#:~:text=,contextual%20integrity%20within%20informational

56. Wu T. The Attention Merchants: The Epic Scramble to Get Inside Our Heads. New York: Vintage Books, 2017.

57. Zuboff S. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. New York: PublicAffairs, 2019.