

ЦИФРОВА БЕЗПЕКА ДІТЕЙ: МІЖНАРОДНО-ПРАВОВИЙ ВИМІР ЗАХИСТУ ПРАВ ДИТИНИ В ЕПОХУ МЕТАВСЕСВІТІВ ТА ШТУЧНОГО ІНТЕЛЕКТУ

Зверева К. С.

ВСТУП

Цифрова трансформація суспільства суттєво вплинула на життя дітей, відкриваючи їм нові можливості для навчання, спілкування та творчості, але одночасно наражаючи на нові ризики. Сьогодні близько третини користувачів інтернету у світі – це діти та молодь¹. Пандемія COVID-19 та перехід до онлайн-освіти ще більше загострили актуальність питань цифрової безпеки дітей. Діти стикаються з різноманітними загрозами у цифровому просторі: контентом, що шкодить їхньому розвитку (насилницьким, порнографічним, таким, що пропагує ненависть або самоушкодження), кібербулінгом, сексуальною експлуатацією, онлайн-грумінгом (домаганнями) тощо². Окрім цього, надмірна комерціалізація цифрового середовища ставить під ризик приватність дітей – їхні персональні дані збираються і використовуються для таргетованої реклами, профілювання, що діти не завжди можуть усвідомити³.

Міжнародна спільнота розуміє необхідність адаптації існуючих механізмів захисту прав дитини до нових реалій цифрової епохи. У 2021 році Комітет ООН з прав дитини прийняв Загальний коментар № 25, яким офіційно визнав, що всі права дитини повною мірою застосовуються і в цифровому середовищі, зобов'язавши держави

¹ Livingstone S. Children's rights apply in the digital world! Parenting for a Digital Future.: 24.03.2021. URL: <https://blogs.lse.ac.uk/parenting4digitalfuture/2021/03/24/general-comment-25/> (дата звернення: 20.06.2025).

² Національна стратегія з захисту дітей в цифровому середовищі на період до 2025 року. URL: https://thedigital.gov.ua/storage/uploads/files/normative_document/2020/77%D0%9D%D0%90%D0%A6%D0%86%D0%9E%D0%9D%D0%90%D0%9B%D0%AC%D0%9D%D0%90_%D0%A1%D0%A2%D0%A0%D0%90%D0%A2%D0%95%D0%93%D0%86%D0%AF_%D0%97_%D0%97%D0%90%D0%A5%D0%98%D0%A1%D0%A2%D0%A3_%D0%94%D0%86%D0%A2%D0%95%D0%98%CC%86_%D0%92_%D0%A6%D0%98%D0%A4%D0%A0%D0%9E%D0%92%D0%9E%D0%9C%D0%A3_%D0%A1%D0%95%D0%A0%D0%95%D0%94%D0%9E%D0%92%D0%98%D0%A9%D0%86_%D0%9D%D0%90.pdf (дата звернення: 20.06.2025). (thedigital.gov.ua)

³ Niestadt M. Protecting children in virtual worlds (the metaverse). Epthinktank.: 26.04.2024. URL: <https://epthinktank.eu/2024/04/26/protecting-children-in-virtual-worlds-the-metaverse/> (дата звернення: 20.06.2025)

вживати заходів для реалізації цих прав онлайн⁴. Рада Європи ще у 2018 році видала докладні Керівні принципи щодо дотримання прав дитини в цифровому середовищі (Recommendation CM/Rec(2018)7), наголосивши на необхідності комплексної політики у цій сфері за участі всіх зацікавлених сторін⁵. Україна, як частина європейського простору, також розробляє власні стратегії: зокрема, затверджено Національну стратегію з захисту дітей в цифровому середовищі на період до 2025 року, яка визначає основні загрози та заходи протидії їм⁶.

Важливим аспектом проблематики є поява нових технологічних явищ – метавсесвітів (занурених віртуальних світів) та систем штучного інтелекту (ШІ). Метавсесвіти обіцяють дітям безпрецедентні можливості для навчання і розваг у VR/AR-середовищах⁷. Водночас, як зазначають дослідники, ці віртуальні світи вже демонструють випадки переслідувань, домагань та контакту дітей з неприйнятним контентом⁸. Штучний інтелект, у свою чергу, використовується в контент-фільтрах, чат-ботах, персональних асистентах тощо, і може як допомагати модерувати середовище, так і створювати нові ризики – від проривів у приватність (розпізнавання облич, профілювання) до генерування шкідливого або нелегального контенту. Зокрема, набули розголосу випадки використання генеративних моделей ШІ для створення фейкових зображень сексуального характеру за участю дітей – так званого штучно згенерованого CSAM (child sexual abuse material). Такі матеріали, хоч і не відображують реальну дитину, фактично

⁴ Livingstone S. Children's rights apply in the digital world! Parenting for a Digital Future.: 24.03.2021. URL: <https://blogs.lse.ac.uk/parenting4digitalfuture/2021/03/24/general-comment-25/> (дата звернення: 20.06.2025).

⁵ Комітет Міністрів Ради Європи. Рекомендація CM/Rec(2018)7 про принципи дотримання, захисту та реалізації прав дитини в цифровому середовищі.: 04.07.2018. URL: https://mvs.gov.ua/upload/file/rekomendac_ua_schodo_zahistu_d_tey_u_cifrovomu_seredovis_ch_2018.pdf (дата звернення: 20.06.2025)

⁶ Національна стратегія з захисту дітей в цифровому середовищі на період до 2025 року. URL: https://thedigital.gov.ua/storage/uploads/files/normative_document/2020/7/%D0%9D%D0%90%D0%A6%D0%86%D0%9E%D0%9D%D0%90%D0%9B%D0%AC%D0%9D%D0%90_%D0%A1%D0%A2%D0%A0%D0%90%D0%A2%D0%95%D0%93%D0%86%D0%AF_%D0%97_%D0%97%D0%90%D0%A5%D0%98%D0%A1%D0%A2%D0%A3_%D0%94%D0%86%D0%A2%D0%95%D0%98CC%86_%D0%92_%D0%A6%D0%98%D0%A4%D0%A0%D0%9E%D0%92%D0%9E%D0%9C%D0%A3_%D0%A1%D0%95%D0%A0%D0%95%D0%94%D0%9E%D0%92%D0%98%D0%A9%D0%86_%D0%9D%D0%90.pdf (дата звернення: 20.06.2025). (thedigital.gov.ua)

⁷ Niestadt M. Protecting children in virtual worlds (the metaverse). Epthinktank.: 26.04.2024. URL: <https://epthinktank.eu/2024/04/26/protecting-children-in-virtual-worlds-the-metaverse/> (дата звернення: 20.06.2025)

⁸ Niestadt M. Protecting children in virtual worlds (the metaverse). Epthinktank.: 26.04.2024. URL: <https://epthinktank.eu/2024/04/26/protecting-children-in-virtual-worlds-the-metaverse/> (дата звернення: 20.06.2025)

відтворюють сцени злочину і можуть стимулювати попит на реальну експлуатацію ⁹. Відтак законодавці постають перед необхідністю оновлювати правові норми з урахуванням цих новітніх викликів.

Метою даної статті є дослідити міжнародно-правовий вимір захисту прав дитини в цифровому середовищі, приділивши увагу базовим міжнародним стандартам, зобов'язанням держав, аналізу нових явищ (метавесвіт, ШІ) та порівнянню підходів різних країн.

1. Міжнародно-правові стандарти захисту дітей у цифровому середовищі

Права дітей у цифровому просторі спираються на загальні міжнародні стандарти прав людини та дитини, адаптовані до специфіки інформаційної доби. Базовим глобальним інструментом є Конвенція ООН про права дитини 1989 року, що ратифікована 196 державами (в тому числі Україною) і закріплює широкий спектр прав дитини. Попри те, що Конвенція ухвалена задовго до появи масового Інтернету, її норми повністю поширюються на цифровий вимір життя дитини ¹⁰. Зокрема, стаття 13 гарантує право дитини на висловлення думки та отримання інформації; стаття 16 – право на приватне життя, недоторканність кореспонденції та захист честі і гідності; стаття 19 – право на захист від будь-яких форм насильства, образ чи недбалого поводження; стаття 34 – захист від сексуальної експлуатації та розбещення тощо. Конвенція зобов'язує держави вживати всі необхідні законодавчі, адміністративні, соціальні та освітні заходи для реалізації цих прав, у тому числі стосовно запобігання експлуатації дітей та їхньому захисту від жорстокого поводження ¹¹. У 2021 році Комітет ООН з прав дитини спеціально роз'яснив ці зобов'язання у контексті цифрового середовища, ухваливши Загальне зауваження № 25 «щодо прав дитини у зв'язку з цифровим середовищем». Це авторитетне тлумачення підтверджує, що держави повинні забезпечити дотримання всіх прав дітей онлайн, приділяючи увагу, зокрема, рівному доступу дітей до цифрових технологій, захисту їх від шкідливого контенту та кіберзагроз, дотриманню приватності дітей в мережі, їх освітнім і

⁹ Lory G., Armangau R. EU Parliament to criminalise AI-generated child abuse material. Euronews.: 17.06.2025. URL: <https://www.euronews.com/my-europe/2025/06/17/eu-parliament-to-criminalising-ai-generated-child-abuse-material> (дата звернення: 20.06.2025).

¹⁰ Niestadt M. Protecting children in virtual worlds (the metaverse). Epthinktank.: 26.04.2024. URL: <https://epthinktank.eu/2024/04/26/protecting-children-in-virtual-worlds-the-metaverse/> (дата звернення: 20.06.2025).

¹¹ Niestadt M. Protecting children in virtual worlds (the metaverse). Epthinktank.: 26.04.2024. URL: <https://epthinktank.eu/2024/04/26/protecting-children-in-virtual-worlds-the-metaverse/> (дата звернення: 20.06.2025).

культурним правам у цифровому просторі тощо ¹². Комітет наголосив, що права дітей мають бути пріоритетом при розробці державами цифрових політик, а бізнес-сектор та інші залучені сторони теж несуть відповідальність за повагу прав дитини (в дусі Керівних принципів ООН з бізнесу і прав людини) ¹³.

На регіональному рівні важливу роль відіграють стандарти Ради Європи та Європейського Союзу. Рада Європи ще в 2016 році визначила права дитини в цифровому середовищі одним із пріоритетів своєї Стратегії з прав дитини ¹⁴. У 2018 році Комітет міністрів Ради Європи ухвалив Рекомендацію CM/Rec(2018)7, яка містить «Керівні принципи щодо дотримання, захисту та реалізації прав дитини в цифровому середовищі». Цей документ узагальнює сучасні міжнародні стандарти і надає державам-членам детальні орієнтири політики. Зокрема, Рекомендація підтверджує, що діти повинні користуватися всіма правами людини в цифровому середовищі так само, як офлайн ¹⁵. Держави зобов'язані забезпечити, щоб розвиток технологій не вів до ущемлення прав дитини, а навпаки – використовувався на благо дітей ¹⁶. Принцип «безпечного, надійного, відкритого та сприятливого для дітей інтернету» декларується одним із цілей ¹⁷. Рекомендація охоплює різні аспекти: право дітей на доступ до інформації та цифрової участі; право на свободу вираження поглядів онлайн; захист приватності і персональних даних дітей; захист від кібербулінгу, експлуатації,

¹² Livingstone S. Children's rights apply in the digital world! Parenting for a Digital Future.: 24.03.2021. URL: <https://blogs.lse.ac.uk/parenting4digitalfuture/2021/03/24/general-comment-25/> (дата звернення: 20.06.2025).

¹³ Комітет Міністрів Ради Європи. Рекомендація CM/Rec(2018)7 про принципи дотримання, захисту та реалізації прав дитини в цифровому середовищі.: 04.07.2018. URL: https://mvs.gov.ua/upload/file/rekomendac_ya_schodo_zahistu_d_tey_u_cifrovomu_seredovis_ch_2018.pdf (дата звернення: 20.06.2025).

¹⁴ Комітет Міністрів Ради Європи. Рекомендація CM/Rec(2018)7 про принципи дотримання, захисту та реалізації прав дитини в цифровому середовищі.: 04.07.2018. URL: https://mvs.gov.ua/upload/file/rekomendac_ya_schodo_zahistu_d_tey_u_cifrovomu_seredovis_ch_2018.pdf (дата звернення: 20.06.2025).

¹⁵ Комітет Міністрів Ради Європи. Рекомендація CM/Rec(2018)7 про принципи дотримання, захисту та реалізації прав дитини в цифровому середовищі.: 04.07.2018. URL: https://mvs.gov.ua/upload/file/rekomendac_ya_schodo_zahistu_d_tey_u_cifrovomu_seredovis_ch_2018.pdf (дата звернення: 20.06.2025).

¹⁶ Комітет Міністрів Ради Європи. Рекомендація CM/Rec(2018)7 про принципи дотримання, захисту та реалізації прав дитини в цифровому середовищі.: 04.07.2018. URL: https://mvs.gov.ua/upload/file/rekomendac_ya_schodo_zahistu_d_tey_u_cifrovomu_seredovis_ch_2018.pdf (дата звернення: 20.06.2025).

¹⁷ Комітет Міністрів Ради Європи. Рекомендація CM/Rec(2018)7 про принципи дотримання, захисту та реалізації прав дитини в цифровому середовищі.: 04.07.2018. URL: https://mvs.gov.ua/upload/file/rekomendac_ya_schodo_zahistu_d_tey_u_cifrovomu_seredovis_ch_2018.pdf (дата звернення: 20.06.2025).

шкідливого контенту; освіту і підвищення цифрової грамотності; спеціальні обов'язки батьків, шкіл, інтернет-провайдерів, платформи та інших стейкхолдерів у забезпеченні безпеки дітей онлайн¹⁸. Державам рекомендується розробляти національні стратегії захисту дітей у цифровому середовищі, удосконалювати законодавство, співпрацювати з приватним сектором та громадянським суспільством. Україна, як член Ради Європи, бере до уваги ці стандарти; зокрема, переклад рекомендації CM/Rec(2018)7 був доведений до відома відповідних органів¹⁹.

Слід також відзначити міжнародні договори, спрямовані на боротьбу з найбільш небезпечними явищами, що загрожують дітям у цифровому середовищі, – такими як дитяча порнографія та сексуальна експлуатація. До них належать: Факультативний протокол до Конвенції ООН про права дитини щодо торгівлі дітьми, дитячої проституції і дитячої порнографії (2000 р.)²⁰, а на європейському рівні – Конвенція Ради Європи про захист дітей від сексуальної експлуатації та сексуального насильства 2007 р.²¹ (так звана Ланцаротська конвенція). Ці договори зобов'язують держави криміналізувати виготовлення, розповсюдження та зберігання матеріалів, що зображують сексуальне насильство над дітьми (CSAM), притягувати винних до відповідальності, співпрацювати міжнародно для виявлення і покарання злочинців, а також проводити превентивну роботу та допомагати потерпілим дітям. Україна ратифікувала обидва зазначені документи (у 2003 р. та 2012 р. відповідно), імплементувавши їх норми в національне законодавство (зокрема, статті 301 та 156 Кримінального кодексу України щодо обігу дитячої порнографії та розбещення неповнолітніх).

На рівні національного законодавства України охорона прав дітей в інформаційній сфері забезпечується низкою актів. Конституція України проголошує, що дитинство перебуває під охороною держави, а

¹⁸ Комітет Міністрів Ради Європи. Рекомендація CM/Rec(2018)7 про принципи дотримання, захисту та реалізації прав дитини в цифровому середовищі.: 04.07.2018. URL: https://mvs.gov.ua/upload/file/rekomendac_ia_schodo_zahistu_d_tey_u_cifrovomu_seredovis_ch_2018.pdf (дата звернення: 20.06.2025).

¹⁹ Комітет Міністрів Ради Європи. Рекомендація CM/Rec(2018)7 про принципи дотримання, захисту та реалізації прав дитини в цифровому середовищі.: 04.07.2018. URL: https://mvs.gov.ua/upload/file/rekomendac_ia_schodo_zahistu_d_tey_u_cifrovomu_seredovis_ch_2018.pdf (дата звернення: 20.06.2025).

²⁰ Факультативний протокол до Конвенції про права дитини щодо торгівлі дітьми, дитячої проституції і дитячої порнографії ООН; Протокол, Міжнародний документ від 01.01.2000. URL : https://zakon.rada.gov.ua/laws/show/995_b09#Text

²¹ Конвенція Ради Європи про захист дітей від сексуальної експлуатації та сексуального насильства Рада Європи; Конвенція, Міжнародний документ від 25.10.2007. URL : https://zakon.rada.gov.ua/laws/show/994_927#Text

наси́льство над дитино́ю та її експлуата́ція забороняються (ст. 52) ²². Базовим спеціальним законом є Закон України «Про охорону дитинства» (2001 р.) ²³, який встановлює правові засади захисту інтересів дитини. Цей закон, зокрема, гарантує право дитини на інформацію, що відповідає її віку, і забороняє розголошення чи публікацію будь-якої інформації про дитину, яка може завдати їй шкоди, без згоди її законних представників ²⁴. Також законом передбачено захист дитини від усіх форм експлуатації, у тому числі сексуального насильства, використання дитини у створенні та розповсюдженні порнографічних матеріалів, втягнення у азартні ігри, екстремістські угруповання тощо ²⁵. Для захисту приватності дітей діє Закон України «Про захист персональних даних» (2010 р.) [10], який гарантує недоторканність особистих даних кожної особи, включно з дитиною. Хоч цей закон і не містить спеціальних положень про дітей, загальні норми (про згоду суб'єкта даних, цільове використання, безпеку даних) поширюються і на дані неповнолітніх. У сфері кібербезпеки рамковий Закон «Про основні засади забезпечення кібербезпеки України» (2017 р.) ²⁶ визначає об'єктами кібербезпеки, зокрема, конституційні права і свободи людини і громадянина у кіберпросторі. Це означає, що заходи з кібербезпеки (захист від кіберзагроз) також мають враховувати і захист прав дитини онлайн.

²² Конституція України Верховна Рада України; Конституція України, Конституція, Закон від 28.06.1996 № 254к/96-ВР. URL : <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text>

²³ Про охорону дитинства Закон України від 26.04.2001 № 2402-III. URL : <https://zakon.rada.gov.ua/laws/show/2402-14#Text>

²⁴ Національна стратегія з захисту дітей в цифровому середовищі на період до 2025 року. URL: https://thedigital.gov.ua/storage/uploads/files/normative_document/2020/7/%D0%9D%D0%90%D0%A6%D0%86%D0%9E%D0%9D%D0%90%D0%9B%D0%AC%D0%9D%D0%90_%D0%A1%D0%A2%D0%A0%D0%90%D0%A2%D0%95%D0%93%D0%86%D0%AF_%D0%97_%D0%97%D0%90%D0%A5%D0%98%D0%A1%D0%A2%D0%A3_%D0%94%D0%86%D0%A2%D0%95%D0%98%D0%98%D0%92_%D0%A6%D0%98%D0%A4%D0%A0%D0%9E%D0%92%D0%9E%D0%9C%D0%A3_%D0%A1%D0%95%D0%A0%D0%95%D0%94%D0%9E%D0%92%D0%98%D0%A9%D0%86_%D0%9D%D0%90.pdf (дата звернення: 20.06.2025). (thedigital.gov.ua)

²⁵ Національна стратегія з захисту дітей в цифровому середовищі на період до 2025 року. URL: https://thedigital.gov.ua/storage/uploads/files/normative_document/2020/7/%D0%9D%D0%90%D0%A6%D0%86%D0%9E%D0%9D%D0%90%D0%9B%D0%AC%D0%9D%D0%90_%D0%A1%D0%A2%D0%A0%D0%90%D0%A2%D0%95%D0%93%D0%86%D0%AF_%D0%97_%D0%97%D0%90%D0%A5%D0%98%D0%A1%D0%A2%D0%A3_%D0%94%D0%86%D0%A2%D0%95%D0%98%D0%98%D0%92_%D0%A6%D0%98%D0%A4%D0%A0%D0%9E%D0%92%D0%9E%D0%9C%D0%A3_%D0%A1%D0%95%D0%A0%D0%95%D0%94%D0%9E%D0%92%D0%98%D0%A9%D0%86_%D0%9D%D0%90.pdf (дата звернення: 20.06.2025). (thedigital.gov.ua)

²⁶ Про основні засади забезпечення кібербезпеки України Закон України від 05.10.2017 № 2163-VIII. URL : <https://zakon.rada.gov.ua/laws/show/2163-19#Text>

Окремо варто згадати нещодавно ухвалений Закон України «Про медіа» (2023 р.)²⁷, який встановлює вимоги щодо захисту неповнолітніх від шкідливої інформації в аудіовізуальних медіа та онлайн-платформах (класифікація контенту за віковими категоріями, обмеження показу сцен насильства, порнографії тощо) – цей закон гармонізований з правом ЄС (Директива про аудіовізуальні медіапослуги)²⁸. Таким чином, в Україні сформовано базові правові механізми для захисту дітей у цифровому середовищі, хоча їх розвиток триває і потребує врахування новітніх викликів.

Міжнародно-правові стандарти також включають прецеденти і тлумачення, вироблені міжнародними судовими та квазі-судовими органами. Так, Європейський суд з прав людини (ЄСПЛ) у своїй практиці неодноразово стикався з питаннями захисту приватного життя та безпеки дітей в інтернеті. Важливою є справа «K.U. проти Фінляндії» (K.U. v. Finland, заява №2872/02, рішення від 2 грудня 2008 р.), де 12-річний хлопчик став жертвою оголошення сексуального характеру, розміщеного невідомою особою на сайті знайомств²⁹. Фінське законодавство того часу не дозволяло провайдеру розкрити особу автора оголошення, і національні суди відмовили в доступі до цих даних, посилаючись на захист конфіденційності комунікацій. ЄСПЛ визнав, що держава не виконала позитивного обов'язку із захисту права дитини на приватне життя (ст. 8 ЄКПЛ), оскільки не забезпечила наявності правового механізму для ідентифікації та притягнення винної особи³⁰. Суд наголосив, що діти та інші вразливі особи мають право на державний захист у формі ефективного стримування від таких тяжких посягань на їхнє приватне життя. Сама лише наявність кримінальної заборони (наприклад, наклепу) є недостатньою, якщо відсутній спосіб встановити винуватця і притягнути його до відповідальності. Цей прецедент утвердив принцип, що держава повинна активно забезпечувати правові інструменти для боротьби з онлайн-насильством щодо дітей, навіть якщо це вимагає обмеженого втручання у

²⁷ Про медіа Закон України від 13.12.2022 № 2849-IX. URL : <https://zakon.rada.gov.ua/laws/show/2849-20#Text>

²⁸ Директива Європейського Парламенту і Ради 2010/13/ЄС від 10 березня 2010 року про координацію певних положень, встановлених законами, нормативно-правовими або [...] Європарламент, Рада ЄС; Директива, Міжнародний документ від 10.03.2010 № 2010/13/ЄС. URL : https://zakon.rada.gov.ua/laws/show/984_022-10#Text

²⁹ European Court of Human Rights. Case of “K.U. v. Finland”: judgment of 02.12.2008 (application no. 2872/02). URL: <https://hudoc.echr.coe.int/eng?i=001-89964> (accessed: 22.06.2025)

³⁰ European Court of Human Rights. Case of “K.U. v. Finland”: judgment of 02.12.2008 (application no. 2872/02). URL: <https://hudoc.echr.coe.int/eng?i=001-89964> (accessed: 22.06.2025)

приватність потенційних правопорушників (розкриття їхніх даних провайдерами) задля захисту прав і свобод інших осіб – у даному разі дитини ³¹.

Окрім ЄСПЛ, варто згадати й Суд Європейського Союзу (ЄСЄ), який у рішеннях останніх років торкнувся питань «права на забуття» та захисту персональних даних, що мають значення і для дітей. Хоча відомі рішення на кшталт *Google Spain v. AEPD* (2014) стосувалися дорослих, запроваджене ЄСЄ «право на видалення» інформації з пошуковиків однаково важливе для неповнолітніх, чия необережна онлайн-активність або персональні дані, оприлюднені батьками («шерентинг»), можуть завдати шкоди їх репутації в майбутньому ³². Загальний регламент ЄС із захисту даних 2016/679 (GDPR) прямо визнає дітей вразливою категорією суб'єктів даних, що потребує особливого захисту (Recital 38 GDPR). Зокрема, встановлено більш високі стандарти згоди для обробки персональних даних дітей: послуги інформаційного суспільства не можуть збирати дані дитини до 16 років без батьківської згоди (держави ЄС можуть знизити цей вік до 13 років) – ст. 8 GDPR. В Україні право на забуття та інші положення GDPR поступово імплементуються; як зазначає Д. Садовська, неповнолітні користуються особливим захистом як вразливі категорії користувачів відповідно до Загального регламенту про захист даних ³³. Діти через психологічну незрілість часто не усвідомлюють наслідків публікації особистої інформації, тому право дитини на видалення інформації про себе є важливим механізмом відновлення контролю над своїм цифровим слідом.

Підсумовуючи, фундаментальні міжнародно-правові стандарти – від універсальних договорів ООН до регіональних європейських конвенцій і «м'якого права» – одностайно стверджують: права дитини повинні бути захищені в цифровому середовищі не менш ефективно, ніж у реальному житті. Держави несуть обов'язок оновлювати законодавство і практику, залучати бізнес до співрегулювання, надавати батькам і дітям знання та інструменти для безпечного користування інтернетом.

³¹ European Court of Human Rights. Case of “K.U. v. Finland”: judgment of 02.12.2008 (application no. 2872/02). URL: <https://hudoc.echr.coe.int/eng/?i=001-89964> (accessed: 22.06.2025)

³² Court of Justice of the European Union. Judgment of the Court (Grand Chamber) of 13.05.2014 in Case C-131/12 *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62012CJ0131> (accessed: 22.06.2025).

³³ Садовська Д. І. Захист персональних даних дітей у соціальних мережах в контексті права на забуття. Науковий вісник Ужгородського національного університету. Серія: Право. 2024. Вип. 81, ч. 1. С. 225–230. URL: <https://visnyk-juris-uzhnu.com/wp-content/uploads/2024/03/37.pdf> (дата звернення: 22.06.2025)

Наступні розділи розглянуть, як ці загальні принципи застосовуються до новітніх викликів – метавсесвіту та ШІ – та як різні країни впроваджують їх на практиці.

2. Нові виклики цифрової епохи: метавсесвіти та штучний інтелект

Метавсесвіт (англ. metaverse) – це поняття, що використовується для опису колективних віртуальних просторів, часто доступних через технології VR (віртуальна реальність) та AR (доповнена реальність), де користувачі можуть взаємодіяти один з одним у режимі реального часу. Для дітей метавсесвіти відкривають нові горизонти: освітні програми з повним зануренням, віртуальні подорожі в космос чи минулі епохи, інтерактивні ігри, творчі майданчики тощо ³⁴. Такі платформи, як Roblox, Minecraft, Fortnite та інші, уже еволюціонують у бік метасвітів, де мільйони дітей проводять час, спілкуючись і створюючи власний контент. Існують успішні приклади використання VR у терапії та освіті дітей з особливими потребами або при реабілітації ³⁵. Отже, потенціал технології для реалізації права дитини на розвиток, освіту, доступ до культури – значний.

Однак, поряд із можливостями, віртуальні світи несуть і множинні ризики. Багато загроз, притаманних «традиційному» інтернету, проявляються у метавсесвіті ще гостріше через ефект присутності та псевдо-анонімності аватарів. Діти у VR-середовищах можуть ставати об'єктами домагань, булінгу, зіткнутися з агресивною поведінкою або непристойними пропозиціями з боку інших користувачів. У 2023 році дослідження Центру протидії цифровій ненависті (CCDH) зафіксувало регулярні випадки сексуальних домагань неповнолітніх у популярних VR-чатах ³⁶. Репортажі журналістів теж виявляли, що діти у VR-світах (на кшталт Meta Horizon Worlds) можуть зазнавати вербальних образ, переслідувань та навіть віртуальних «домагань» у формі небажаного дотику аватарів. Це ставить питання про ефективну модерацію в реальному часі тривимірних просторів, що є технічно складнішим, ніж фільтрація текстового контенту в соціальних мережах.

³⁴ Niestadt M. Protecting children in virtual worlds (the metaverse). Epthinktank.: 26.04.2024. URL: <https://epthinktank.eu/2024/04/26/protecting-children-in-virtual-worlds-the-metaverse/> (дата звернення: 20.06.2025)

³⁵ Niestadt M. Protecting children in virtual worlds (the metaverse). Epthinktank.: 26.04.2024. URL: <https://epthinktank.eu/2024/04/26/protecting-children-in-virtual-worlds-the-metaverse/> (дата звернення: 20.06.2025)

³⁶ Niestadt M. Protecting children in virtual worlds (the metaverse). Epthinktank.: 26.04.2024. URL: <https://epthinktank.eu/2024/04/26/protecting-children-in-virtual-worlds-the-metaverse/> (дата звернення: 20.06.2025)

Ще одним викликом є відсутність належної верифікації віку. Більшість VR-платформ номінально встановлюють мінімальний вік (наприклад, 13 років), але на практиці діти молодшого віку можуть отримати доступ, просто поставивши «плюсик» при питанні про вік. Виробники устаткування починають усвідомлювати проблему: наприклад, компанія Meta (Facebook) знизил офіційний вік користування VR-гарнітурами Oculus Quest з 13 до 10 років, намагаючись розширити аудиторію ³⁷. Це викликає занепокоєння, адже молодші діти ще менш готові до потенційно травматичного досвіду у віртуальних світах. Європейський Союз у своїй Стратегії щодо Web 4.0 і віртуальних світів (2023) особливо наголошує на потребі надійних механізмів верифікації віку та безпечного дизайну платформ з урахуванням присутності дітей. Так, обговорюється впровадження загальноєвропейської цифрової ідентичності, що дозволила б підтверджувати вік користувача онлайн без розкриття його особистості.

Приватність і захист даних – окрема сфера ризику у метавесвітах. Якщо традиційні сайти збирають історію переглядів, то VR/AR-платформи можуть збирати біометричні та поведінкові дані: траєкторію рухів, вираз обличчя, частоту серцебиття, напрям погляду користувача тощо ³⁸. Ці дані надзвичайно чутливі, адже дозволяють робити висновки про емоційний стан, інтереси, реакції дитини. Комерційне використання таких даних (наприклад, для таргетованої реклами у віртуальних світах) створює етичні і правові питання. Звіт Лондонського університету (LSE) показав, що діти можуть усвідомлювати факт відстеження їх активності онлайн, але далеко не повністю розуміють обсяг зібраної про них інформації та наслідки профілювання ³⁹. Відтак принцип «privacy by design» (приватність за дизайном) є критично важливим при розробці метавесвітів: за замовчуванням повинні стояти найвищі налаштування приватності для неповнолітніх, мінімізація збору даних, чіткі вікові межі для доступу до різних зон контенту.

На глобальному рівні поки бракує спеціальних правових актів, що регулювали б безпеку у метавесвітах. Втім, застосовуються загальні

³⁷ Niestadt M. Protecting children in virtual worlds (the metaverse). Epthinktank.: 26.04.2024. URL: <https://epthinktank.eu/2024/04/26/protecting-children-in-virtual-worlds-the-metaverse/> (дата звернення: 20.06.2025)

³⁸ Niestadt M. Protecting children in virtual worlds (the metaverse). Epthinktank.: 26.04.2024. URL: <https://epthinktank.eu/2024/04/26/protecting-children-in-virtual-worlds-the-metaverse/> (дата звернення: 20.06.2025)

³⁹ Niestadt M. Protecting children in virtual worlds (the metaverse). Epthinktank.: 26.04.2024. URL: <https://epthinktank.eu/2024/04/26/protecting-children-in-virtual-worlds-the-metaverse/> (дата звернення: 20.06.2025)

норми. Так, у ЄС Акт про цифрові послуги (Digital Services Act, 2022) ⁴⁰ установлює, що онлайн-платформи (включно з віртуальними світами) забороняється таргетувати рекламу на основі персональних даних неповнолітніх ⁴¹. DSA також посилює вимоги до модерації контенту: дуже великі платформи повинні проводити оцінку системних ризиків, зокрема ризиків для прав дітей, та вживати заходів для їх мінімізації. Загальний регламент захисту даних (GDPR) прямо поширюється на метавсесвіт-платформи, змушуючи їх отримувати явну згоду на обробку персональних даних і забезпечувати права суб'єктів даних (наприклад, право на видалення) У 2022 р. Єврокомісія внесла пропозицію Регламенту щодо запобігання та боротьби з сексуальним насильством над дітьми онлайн, який, серед іншого, має зобов'язати провайдерів проактивно виявляти і видаляти CSAM зі своїх платформ (включаючи VR-середовища). Ця ініціатива наразі дискутується: критики вказують на ризики для приватності через сканування повідомлень користувачів. Проте політична воля до жорсткіших заходів є: у червні 2025 р. Європарламент схвалив нову директиву, що криміналізує створення і поширення CSAM, згенерованого штучним інтелектом (дії прирівнюються до поведінки з реальними матеріалами), а також розширює відповідальність за онлайн-грумінг, сексторшин та трансляцію насильства ⁴². Це новаторський крок, що покликаний закрити лакуни у законі: адже раніше фейкові зображення чи анімація з «на вигляд» дітьми могли не підпадати під визначення порнографії з участю реальних дітей.

Іншим визначальним чинником цифрової ери є штучний інтелект. Системи ШІ все ширше застосовуються як у продуктах, орієнтованих на дітей (від «розумних» іграшок до адаптивних освітніх платформ), так і «за лаштунками» цифрового середовища, визначаючи, який контент побачить юний користувач, з ким він встановить контакт тощо. Використання алгоритмів рекомендаційного відбору контенту викликало чимало нарікань: відомо, що діти можуть швидко «затягуватися» у споживання відео чи ігор через механізми, що експлуатують психологічні вразливості (наприклад, нескінченна

⁴⁰ European Parliament and Council of the European Union. Regulation (EU) 2022/2065 of 19.10.2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act). Official Journal of the European Union.: 27.10.2022. URL: <https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng> (дата звернення: 20.06.2025).

⁴¹ Niestadt M. Protecting children in virtual worlds (the metaverse). Epthinktank.: 26.04.2024. URL: <https://epthinktank.eu/2024/04/26/protecting-children-in-virtual-worlds-the-metaverse/> (дата звернення: 20.06.2025)

⁴² Lory G., Armangau R. EU Parliament to criminalise AI-generated child abuse material. Euronews.: 17.06.2025. URL: <https://www.euronews.com/my-europe/2025/06/17/eu-parliament-to-criminalising-ai-generated-child-abuse-material> (дата звернення: 20.06.2025)

стрічка TikTok чи автопрогравання відео на YouTube). Такі алгоритми можуть ненавмисно підсовувати дітям шкідливий або травматичний контент, оскільки оптимізовані на утримання уваги, а не на благо користувача. Крім того, чат-боти зі штучним інтелектом (як-от популярні нині генеративні моделі) в деяких випадках можуть виступати «співрозмовниками» дітей. Тут виникають і питання безпеки (чи не отримає дитина небезпечну пораду, чи не буде схилена до протиправних дій), і приватності (чат-бот може непомітно зібрати особисту інформацію про дитину), і навіть ризики емоційного здоров'я (надмірна прив'язаність до віртуального співрозмовника або дезорієнтація щодо реального та віртуального).

Міжнародні організації в останні роки активно працюють над принципами «дитячоцентричного» ШІ. Так, Дитячий фонд ООН (UNICEF) у 2020 р. розробив Політичні керівні настанови щодо ШІ для дітей, які пропонують урядам та компаніям сім ключових вимог: 1) захист – безпека та приватність дітей, 2) добробут і вигода – ШІ має сприяти розвитку дитини, 3) справедливість та недискримінація – уникати упередженості щодо дітей, 4) прозорість – зрозумілість роботи алгоритмів для дітей і батьків, 5) відповідальність розробників, 6) підготовка дітей – освіта про ШІ, 7) участь дітей – залучення дитячої думки у дизайн AI-систем. Ці принципи носять рекомендаційний характер, але вже проходять апробацію в ряді країн та компаній (пілотні проекти за підтримки ЮНІСЕФ у 2021–2022 рр.).

Європейський Союз наближається до ухвалення першого у світі комплексного закону про ШІ – Акту про штучний інтелект (AI Act). У цьому законопроекті враховано і аспекти, релевантні для дітей. Зокрема, забороняються AI-системи, які експлуатують вразливості дітей або інших вразливих груп у спосіб, що може завдати шкоди (ст. 5(1)(b) AI Act)⁴³. Це означає, що, наприклад, ігри чи застосунки, які приховано маніпулюють психологією дитини з метою змусити її зробити покупки (through loot box механізми тощо), будуть поза законом. Також Акт класифікує системи ШІ, що застосовуються у сферах освіти чи професійної орієнтації дітей, як високоризикові – вони потребуватимуть обов'язкової сертифікації, прозорості та нагляду. Окремо, як уже згадувалося, ЄС рухається до криміналізації певних дій, пов'язаних з ШІ: генерація дитячої порнографії прирівнюється до

⁴³ 5Rights Foundation. EU AI Act enters into force: A crucial step for child protection.: 01.08.2024. URL: <https://5rightsfoundation.com/eu-ai-act-enters-into-force-a-crucial-step-for-child-protection/> (дата звернення: 20.06.2025).

реальної експлуатації ⁴⁴, розробляються підходи до автоматизованого моніторингу за ознаками грумінгу у мережах.

Держави також впроваджують національні ініціативи. У Великій Британії регулятор (ICO) видав Кодекс для дизайну, враховувального найкращі інтереси дітей (Age-appropriate design code, 2020), який, серед іншого, стосується й алгоритмів: від постачальників онлайн-сервісів вимагається мінімізувати профілювання дітей, вимкнути нотифікації в нічний час, якщо це можливо, і взагалі проєктувати сервіси так, щоби вони не заохочували дітей до перегляду шкідливого контенту. Цей підхід «безпека дітей за замовчуванням» підтримується й на рівні ЄС – Європарламент у 2024 р. прямо закликав, щоб онлайн-сервіси і продукти, якими переважно користуються діти, були безпечними за дизайном і за замовчуванням. Досягти цього планується, зокрема, через кодекс поведінки щодо віково-адекватного дизайну для ІТ-індустрії, який нині розробляється за сприяння Єврокомісії та експертів ⁴⁵.

Поза країнами Заходу, свої особливі підходи. Наприклад, Китай запровадив драконівські обмеження на ігровий час неповнолітніх – діти до 18 років можуть грати онлайн лише з 20:00 до 21:00 у вихідні та святкові дні, а доступ до ігор вимагає реєстрації під справжнім ім'ям. Це радикальний приклад того, як держава намагається захистити дітей від ігрової залежності та небажаного контенту, хоч і за рахунок жорсткого контролю. В Європі та США такий підхід навряд чи можливий через міркування пропорційності та прав людини, але деякі елементи (реєстрація, верифікація віку) обговорюються і там.

Отже, поява метавесвітів та ІІІ ставить нові комплексні питання перед правозахисниками та законодавцями. Необхідно виробити баланс між стимулюванням інновацій, що можуть приносити користь дітям, та превенцією зловживань. Міжнародне право дає базові орієнтири – принцип пріоритетності найкращих інтересів дитини (ст. 3 Конвенції ООН про права дитини), який повинен застосовуватися і у цифровому вимірі. Застосування цього принципу означає, що у центрі розробки нових технологій повинна бути безпека, приватність і добробут дітей, а не лише бізнес-цілі. У наступному розділі розглянемо, як різні країни світу, опираючись на згадані стандарти, впроваджують правові та політичні заходи для забезпечення цифрової безпеки дітей.

⁴⁴ Lory G., Armangau R. EU Parliament to criminalise AI-generated child abuse material. **Euronews.**: 17.06.2025. URL: <https://www.euronews.com/my-europe/2025/06/17/eu-parliament-to-criminalising-ai-generated-child-abuse-material> (дата звернення: 20.06.2025).

⁴⁵ Niestadt M. Protecting children in virtual worlds (the metaverse). **Ephthinktank.**: 26.04.2024. URL: <https://epthintktank.eu/2024/04/26/protecting-children-in-virtual-worlds-the-metaverse/> (дата звернення: 20.06.2025).

3. Порівняльний аналіз підходів до цифрової безпеки дітей (ЄС, США та інші країни)

Підходи різних країн до регулювання цифрової безпеки дітей історично різнилися, відображаючи правові традиції, культуру та ступінь залучення держави в інтернет-сферу. Розвинуті демократії конвергують у розумінні цілей захисту дітей онлайн, однак засоби їх досягнення варіюються. Розглянемо для порівняння, з одного боку, підхід Європейського Союзу (як наднаціонального об'єднання, чий норми впливають і на Україну), а з іншого – Сполучених Штатів Америки, де діють інші правові рамки. Також побіжно згадаємо деякі приклади інших юрисдикцій.

Європейський Союз. Як уже зазначалося, ЄС поступово формує комплексну нормативну базу для захисту дітей у цифровому середовищі. В її основі – регламенти прямої дії та директиви, обов'язкові для держав-членів. Основні елементи європейського підходу такі:

Захист даних та приватності дітей. Загальний регламент із захисту даних (GDPR, чинний з 2018 р.) встановив високий стандарт для обробки персональних даних дітей. Він зобов'язує отримувати встановлену згоду батьків для дітей до певного віку (13–16 років) при користуванні інформаційними послугами⁴⁶. GDPR також визнає право на забуття: якщо дитина сама або її батьки вимагають видалити особисті дані – компанія повинна це зробити (ст. 17), за винятком окремих випадків (суспільний інтерес, свобода вираження). Багато країн ЄС, наприклад Франція, додатково ввели в національне право норму про «право на забуття для дітей», що спрощує видалення інформації, розміщеної про особу в дитинстві.

Контент-модерація і безпечність сервісів. Директива ЄС про аудіовізуальні медіапослуги (AVMSD) в редакції 2018 р. поширила ряд вимог щодо захисту неповнолітніх і на платформи спільного використання відео (типу YouTube, TikTok). Вони зобов'язані вживати заходів для захисту неповнолітніх від контенту, що може зашкодити їх фізичному, психічному чи моральному розвитку (напр. порнографія, насильство), зокрема шляхом систем вікового маркування і батьківського контролю. Новітній Акт про цифрові послуги (DSA) доповнив цей підхід: великі онлайн-платформи мають оцінювати ризики для неповнолітніх, що випливають з функціонування їхніх сервісів (розповсюдження забороненого контенту, вплив на психіку

⁴⁶ Federal Trade Commission. Children's Online Privacy Protection Rule (COPPA). URL: <https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa> (дата звернення: 22.06.2025)

тощо), та впроваджувати дизайн-рішення для зменшення цих ризиків. DSA також закріпив заборону таргетованої реклами на основі профілів дітей як важливий крок для зменшення комерційного тиску на дитячу аудиторію ⁴⁷.

Принципи «безпечного інтернету» та просвіта. В Європі значна увага приділяється просвітницьким програмам: діє мережа національних центрів Better Internet for Kids, щорічно проводиться День безпечного Інтернету, фінансуються дослідження дитячої поведінки онлайн (наприклад, пан'європейське опитування EU Kids Online). Це «м'який» вимір політики, покликаний підвищити обізнаність дітей, батьків, педагогів про кібербезпеку. В рамках Стратегії ЄС з прав дитини (2021–2024) одним із пріоритетів визначено «цифрову та інформаційну грамотність дітей».

Правоохоронний і судовий вимір. ЄС має спільні інструменти боротьби зі злочинами проти дітей онлайн: Європол координує діяльність кіберполіції країн-членів, функціонує гаряча лінія INHOPE для повідомлення про випадки CSAM. Директива 2011/93/ЄС зобов'язує криміналізувати низку діянь (від виготовлення порнографії до «хазяїнгу» сайтів з нею), полегшує блокування таких сайтів ⁴⁸. Зараз на заміну цій директиві напрацьовується вищезгаданий Регламент проти сексуального насильства над дітьми онлайн, який може зобов'язати сервіси сканувати матеріали на наявність відомих CSAM та повідомляти органи. Це дискусійний крок, адже він торкається питання шифрування приватних повідомлень, але він підкреслює готовність ЄС пожертвувати частиною приватності дорослих заради виявлення злочинів проти дітей.

Отже, європейський підхід можна охарактеризувати як проактивний і комплексний: поєднання жорстких норм (обов'язкових для бізнесу) з м'якими заходами (освіта, співрегулювання), акцент на «design & default»-принципах, щоб сервіси за змовчуванням були дружніми до

⁴⁷ Національна стратегія з захисту дітей в цифровому середовищі на період до 2025 року.

URL: https://thedigital.gov.ua/storage/uploads/files/normative_document/2020/7/%D0%9D%D0%90%D0%A6%D0%86%D0%9E%D0%9D%D0%90%D0%9B%D0%AC%D0%9D%D0%90_%D0%A1%D0%A2%D0%A0%D0%90%D0%A2%D0%95%D0%93%D0%86%D0%AF_%D0%97_%D0%97%D0%90%D0%A5%D0%98%D0%A1%D0%A2%D0%A3_%D0%94%D0%86%D0%A2%D0%95%D0%98CC%86_%D0%92_%D0%A6%D0%98%D0%A4%D0%A0%D0%9E%D0%92%D0%9E%D0%9C%D0%A3_%D0%A1%D0%95%D0%A0%D0%95%D0%94%D0%9E%D0%92%D0%98%D0%A9%D0%86_%D0%9D%D0%90.pdf (дата звернення: 20.06.2025). (thedigital.gov.ua)

⁴⁸ European Parliament and Council of the European Union. Directive 2011/93/EU of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography (Ukrainian translation). Jurfem.: 26.09.2023. URL: <https://jurfem.com.ua/dyrektyva-2011-92-eu-pereklad/> (accessed: 22.06.2025). (jurfem.com.ua)

дітей. ЄС також активно експортує ці стандарти: країни, що прагнуть інтеграції (як Україна), імплементують їх у своє право.

У США підхід історично більш сегментарний. Немає єдиного всеосяжного закону про цифрові права дітей, натомість діють кілька цільових актів і галузевих правил, а також велика роль відведена саморегуляції індустрії під загрозою державного нагляду. Ключові елементи:

Центральним є федеральний закон COPPA (Children's Online Privacy Protection Act, ухвалений ще в 1998 р.)⁴⁹. COPPA забороняє збору персональної інформації дітей віком до 13 років без підтвердженої згоди батьків. Він накладає вимоги на операторів вебсайтів і онлайн-сервісів, призначених для дітей або таких, що свідомо збирають дані про дітей: публікувати політику конфіденційності, отримувати згоду, надавати батькам право видалити дані дитини тощо. Виконання COPPA контролює Федеральна торгова комісія (FTC), яка періодично штрафує порушників – від великих компаній (як Google у справі YouTube, штраф \$170 млн у 2019 р. за незаконний трекінг дітей) до дрібних розробників додатків. COPPA не охоплює користувачів 13–17 років, залишаючи цю категорію поза спеціальним захистом – за них «боролися» лише загальні закони про приватність, яких до недавнього часу не було (проте з 2023 р. низка штатів – Каліфорнія, Юта, Арканзас – ухвалили свої акти, що поширюють деякі вимоги на підлітків до 18 років). Також у 2022 р. було представлено в Конгресі двопартійний законопроект KOSA (Kids Online Safety Act), який пропонує на федеральному рівні запровадити для платформ обов'язок «обережності» щодо неповнолітніх, але його прийняття поки невизначене.

Американське право традиційно більше покладається на саморегуляцію. В США відсутні законодавчі вимоги щодо вікового рейтингування онлайн-контенту або обов'язкового фільтрування. Навпаки, провайдерам надається широкий захист від відповідальності за дії користувачів згідно з Section 230 Закону про пристойність в комунікаціях (1996), що довгі роки стримувало втручання держави. Це призвело до того, що такі гіганти, як Facebook, Twitter, YouTube, самостійно виробляли стандарти спільноти і механізми модерації (з різним ступенем суворості), а держава мінімально регулювала процес. Однак останнім часом, на тлі скандалів про шкоду соціальних мереж для психічного здоров'я підлітків, у США почалися зрушення: кілька штатів (Юта, Арканзас) у 2023 р. ухвалили закони, що вимагають письмової згоди батьків для користування соцмережами дітьми до 18 і вводять комендантську годину у застосунках. Ці закони ще не набули

⁴⁹ Federal Trade Commission. Children's Online Privacy Protection Rule (COPPA). URL: <https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa> (дата звернення: 20.06.2025). (ftc.gov)

чинності і вже оскаржуються компаніями та правозахисниками (через цензурні ризики), проте вони свідчать про зміну настроїв.

На федеральному рівні діє ряд законів проти сексуальної експлуатації дітей (напр. PROTECT Act 2003 р.⁵⁰, що криміналізував віртуальну дитячу порнографію, попередньо легальну після рішення Верховного суду 2002 р.). Ведеться активна діяльність силових органів (ФБР, ICE) зі виявлення педофілів онлайн, часто в співпраці з міжнародними партнерами. Але законодавчо примусити технологічні компанії до проактивного моніторингу контенту в США складно через конституційні гарантії свободи слова та відсутність загального обов'язку цензурувати користувацький контент. Натомість компанії добровільно (частково під тиском) впроваджують механізми типу PhotoDNA для пошуку відомих фото CSAM. У Конгресі тривають дебати навколо закону EARN IT Act, що намагався б зняти з платформ захист Section 230, якщо ті не дотримуються певних «найкращих практик» щодо боротьби з CSAM – але він також наштотхнувся на критику як загрозливий для шифрування.

У США важливою рушійною силою є НУО та коаліції батьків. Наприклад, організація Common Sense Media активно просуває ідеї «діджитал благополуччя», видає вікові рекомендації щодо медіаконтенту, лобіює закони про захист дітей. FiveRights Foundation (заснована у Британії) також впливає глобально, у тому числі на американську дискусію, особливо в частині «design code» для продуктів з III і інтернету речей. Це демонструє, що незважаючи на повільність формального регулювання, суспільний запит у США на безпечніше цифрове середовище для дітей зростає.

У державах, що розвиваються, а також у пострадянських країнах, законодавство часто перебуває на початкових стадіях. Наприклад, багато країн Східної Європи (включно з Україною) прийняли або розробляють стратегії безпечного інтернету для дітей, спираючись на європейські моделі. В деяких державах Азії сильний акцент на цензурі контенту: у Південній Кореї свого часу існувала вимога «game curfew» (заборона нічних онлайн-ігор для підлітків), яка згодом була скасована на користь гнучкішого «choice permit system» (батьки самі встановлюють ліміти часу). Австралія запровадила посаду e-Safety Commissioner, що має повноваження наказувати платформам видаляти кібербулінговий контент щодо неповнолітніх протягом 48 годин, а у випадку відмови – штрафувати. ЄС наразі випереджає багато країн за комплексністю підходу, але його норми поступово стають де-факто глобальними стандартами – міжнародні корпорації часто впроваджують

⁵⁰ United States Congress. PROTECT Act of 2003 (S. 151, 108th Congress). Congress.gov.: 30.04.2003. URL: <https://www.congress.gov/bills/108th-congress/senate-bill/151> (accessed: 22.06.2025).

GDPR-комплаєнс і child-safety by design глобально, щоб не робити окремих версій для різних регіонів.

Для України, яка інтегрується до європейського правового поля, актуальним є перейняття найкращих практик ЄС у цій сфері. Вже нині наша країна виконує План дій Ради Європи щодо прав дитини в цифровому середовищі, впроваджує європейські директиви згідно з Угодою про асоціацію (наприклад, новий Закон «Про медіа» врахував положення AVMSD щодо захисту неповнолітніх). Проте є і власні ініціативи: запущено платформу «Дія.Цифрова освіта», де серед інших є курси з digital hygiene для батьків і дітей; працює онлайн-платформа «Stop Sexting», що займається просвітою та допомогою щодо секстингу, грумінгу. У співпраці з ЮНІСЕФ та ІТ-бізнесом реалізуються проекти з безпечного дизайну веб-сервісів (наприклад, модуль батьківського контролю в мобільних операторах).

Європейський підхід більше регуляторно орієнтований (багато законів, правил для компаній), американський – більш ринковий і фрагментарний, але нині їх тенденції зближуються. В обох випадках визнається, що діти потребують спеціального захисту онлайн, який виходить за межі загального регулювання інтернету. Ключові напрямки – це обмеження збору та використання даних дітей, обмеження шкідливого контенту та взаємодій (через вікові перевірки, фільтри, модерацію), підвищення цифрової компетентності дітей та їхніх опікунів, а також ефективне переслідування злочинів (від кібербулінгу до сексуальної експлуатації). Жодна країна поки що не вирішила всі проблеми, але обмін досвідом (через платформи типу Глобального альянсу WePROTECT, форумів ООН тощо) сприяє виробленню кращих практик.

Україна, зі свого боку, має можливість використати напрацювання інших, аби не «винаходити колесо». Завдяки співпраці з ЄС та Радою Європи вже вдалося модернізувати законодавство (криміналізація кібергрумінгу у 2021 р., оновлення законів про медіа і персональні дані, розробка стратегії безпечного інтернету). Попереду – імплементація нових європейських актів (DSA, потенційно регламенту про CSAM, AI Act тощо), що підвищить стандарти захисту. Водночас український контекст має свою специфіку: зокрема, російська агресія супроводжується інформаційними атаками і використанням цифрових платформ для пропаганди, що теж впливає на дітей (поширення сцен насильства, мова ворожнечі). Тому держава мусить врахувати й цей аспект, комбінуючи цілі безпеки із загальними правами дитини.

ВИСНОВКИ

Захист прав дитини в цифровому середовищі сьогодні став невід'ємною частиною міжнародного порядку денного у сфері прав людини. Проведені дослідження показало, що на глобальному рівні

формується консенсус щодо ключових принципів: діти мають ті самі права онлайн, що й офлайн, і держави зобов'язані забезпечити ці права перед обличчям нових технологічних викликів. ООН, Рада Європи, Європейський Союз та інші міжнародні інституції розробили нормативні орієнтири – від всеосяжних (Конвенція ООН про права дитини і Загальний коментар № 25 Комітету ООН) до спеціалізованих (рекомендації Ради Європи CM/Rec(2018)7, директиви і регламенти ЄС тощо). В центрі цих документів – принцип пріоритету найкращих інтересів дитини, який повинен визначати як державну політику, так і підходи бізнесу до дизайну цифрових продуктів.

Новітні феномени – метавесвіти та штучний інтелект – одночасно відкривають нові можливості для дітей і створюють безпрецедентні ризики. Метавесвіт вимагає переосмислення питань безпеки в умовах повного занурення і псевдоанонімності: потрібні ефективні механізми контролю контенту і поведінки, перевірки віку, захисту приватних даних (включно з біометричними) та запобігання експлуатації дітей у віртуальному просторі. Штучний інтелект, зі свого боку, ставить питання відповідальності алгоритмів: від заборони використання ШІ для завдання шкоди дітям (маніпуляції, генерація протиправного контенту) до вимоги прозорості та етичності AI-систем, що взаємодіють з дітьми. Міжнародне співтовариство вже робить перші кроки у відповідь – як нормативні (заборона AI-генерованого CSAM у ЄС, положення AI Act про вразливих користувачів), так і рекомендаційні (керівництва ЮНІСЕФ, ініціативи 5Rights Foundation). Важливо продовжувати дослідження цих сфер та обмін найкращими практиками, щоб правове регулювання встигало за технологічним прогресом.

Порівняння національних підходів (ЄС, США та ін.) продемонструвало, що, хоча юридичні інструменти відрізняються, цілі захисту спільні. Європейський досвід корисний своєю системністю та превентивним підходом (законодавче встановлення стандартів «безпеки за замовчуванням»), американський – прикладами інновацій саморегуляції та ролі громадянського суспільства. Для України, яка прагне забезпечити своїм дітям безпечне і сприятливе цифрове середовище, пріоритетними завданнями є: імплементація актуальних міжнародних норм (що відбувається в рамках євроінтеграції); розвиток національних програм цифрової освіти дітей і батьків; стимулювання IT-індустрії до впровадження добровільних стандартів захисту дітей; посилення спроможності правоохоронних органів реагувати на кіберзлочини проти дітей; міжвідомча координація (освіта, соцслужби, кіберполіція) у вирішенні проблем, які виникають у дітей онлайн (кібербулінг, секстинг, шахрайство тощо). Не менш важливо залучати самих дітей до розробки рішень – враховувати їхню думку про те, яким має бути безпечний і дружній до дитини інтернет.

АНОТАЦІЯ

Проаналізовано міжнародно-правові підходи до забезпечення цифрової безпеки дітей в умовах стрімкого розвитку інтернет-технологій, зокрема метавесвітів та штучного інтелекту. Визначено актуальні проблеми захисту прав дитини в цифровому середовищі та нові виклики, що постають із появою віртуальних світів та алгоритмів штучного інтелекту. Досліджено міжнародні стандарти та зобов'язання держав у цій сфері, включно з нормами ООН та Ради Європи. Розглянуто судову практику, зокрема позиції Європейського суду з прав людини щодо позитивних обов'язків держав із захисту дітей онлайн. Проведено порівняльний аналіз підходів у різних країнах (ЄС, США та ін.) стосовно регулювання цифрової безпеки дітей, зокрема щодо захисту персональних даних неповнолітніх, боротьби з онлайн-експлуатацією та впровадження принципів «безпечності за дизайном». У висновках подано рекомендації щодо вдосконалення правових механізмів захисту прав дитини в цифровому середовищі з урахуванням новітніх технологічних реалій.

Ключові слова: права дитини; цифрова безпека; цифрове середовище; метавесвіт; штучний інтелект; міжнародне право; захист дітей онлайн; персональні дані; право на забуття.

ЛІТЕРАТУРА:

1. Livingstone S. Children's rights apply in the digital world! Parenting for a Digital Future.: 24.03.2021. URL: <https://blogs.lse.ac.uk/parenting4digitalfuture/2021/03/24/general-comment-25/> (дата звернення: 20.06.2025).

2. Національна стратегія з захисту дітей в цифровому середовищі на період до 2025 року. URL: https://thedigital.gov.ua/storage/uploads/files/normative_document/2020/7/%D0%9D%D0%90%D0%A6%D0%86%D0%9E%D0%9D%D0%90%D0%9B%D0%AC%D0%9D%D0%90_%D0%A1%D0%A2%D0%A0%D0%90%D0%A2%D0%95%D0%93%D0%86%D0%AF_%D0%97_%D0%97%D0%90%D0%A5%D0%98%D0%A1%D0%A2%D0%A3_%D0%94%D0%86%D0%A2%D0%95%D0%98%CC%86_%D0%92_%D0%A6%D0%98%D0%A4%D0%A0%D0%9E%D0%92%D0%9E%D0%9C%D0%A3_%D0%A1%D0%95%D0%A0%D0%95%D0%94%D0%9E%D0%92%D0%98%D0%A9%D0%86_%D0%9D%D0%90.pdf (дата звернення: 20.06.2025). (thedigital.gov.ua)

3. Niestadt M. Protecting children in virtual worlds (the metaverse). Epthinktank.: 26.04.2024. URL: <https://epthinktank.eu/2024/04/26/protecting-children-in-virtual-worlds-the-metaverse/> (дата звернення: 20.06.2025).

4. Комітет Міністрів Ради Європи. Рекомендація CM/Rec(2018)7 про принципи дотримання, захисту та реалізації прав дитини в цифровому середовищі.: 04.07.2018. URL: <https://mvs.gov.ua/>

upload/file/rekomendac_ia_schodo_zahistu_d_tey_u_cifrovomu_seredovish_ch_2018.pdf (дата звернення: 20.06.2025).

5. Lory G., Armangau R. EU Parliament to criminalise AI-generated child abuse material. Euronews.: 17.06.2025. URL: <https://www.euronews.com/my-europe/2025/06/17/eu-parliament-to-criminalising-ai-generated-child-abuse-material> (дата звернення: 20.06.2025).

6. Факультативний протокол до Конвенції про права дитини щодо торгівлі дітьми, дитячої проституції і дитячої порнографії ООН; Протокол, Міжнародний документ від 01.01.2000. URL : https://zakon.rada.gov.ua/laws/show/995_b09#Text

7. Конвенція Ради Європи про захист дітей від сексуальної експлуатації та сексуального насильства Рада Європи; Конвенція, Міжнародний документ від 25.10.2007. URL : https://zakon.rada.gov.ua/laws/show/994_927#Text

8. Конституція України Верховна Рада України; Конституція України, Конституція, Закон від 28.06.1996 № 254к/96-ВР.URL. : <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text>

9. Про охорону дитинства Закон України від 26.04.2001 № 2402-III. URL : <https://zakon.rada.gov.ua/laws/show/2402-14#Text>

10. Про захист персональних даних Закон України від 01.06.2010 № 2297-VI. URL : <https://zakon.rada.gov.ua/laws/show/2297-17#Text>

11. Про основні засади забезпечення кібербезпеки України Закон України від 05.10.2017 № 2163-VIII. URL : <https://zakon.rada.gov.ua/laws/show/2163-19#Text>

12. Про медіа Закон України від 13.12.2022 № 2849-IX. URL : <https://zakon.rada.gov.ua/laws/show/2849-20#Text>

13. Директива Європейського Парламенту і Ради 2010/13/ЄС від 10 березня 2010 року про координацію певних положень, встановлених законами, нормативно-правовими або [...] Європарламент, Рада ЄС; Директива, Міжнародний документ від 10.03.2010 № 2010/13/ЄС. URL: https://zakon.rada.gov.ua/laws/show/984_022-10#Text

14. European Court of Human Rights. Case of “K.U. v. Finland”: judgment of 02.12.2008 (application no. 2872/02). URL: <https://hudoc.echr.coe.int/eng?i=001-89964> (accessed: 22.06.2025).

15. Court of Justice of the European Union. Judgment of the Court (Grand Chamber) of 13.05.2014 in Case C-131/12 *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62012CJ0131> (accessed: 22.06.2025).

16. Садовська Д. І. Захист персональних даних дітей у соціальних мережах в контексті права на забуття. Науковий вісник Ужгородського національного університету. Серія: Право. 2024. Вип. 81, ч. 1.

C. 225–230. URL: <https://visnyk-juris-uzhnu.com/wp-content/uploads/2024/03/37.pdf> (дата звернення: 22.06.2025)

17. European Parliament and Council of the European Union. Regulation (EU) 2022/2065 of 19.10.2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act). *Official Journal of the European Union*.: 27.10.2022. URL: <https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng> (дата звернення: 20.06.2025).

18. Lory G., Armangau R. EU Parliament to criminalise AI-generated child abuse material. *Euronews*.: 17.06.2025. URL: <https://www.euronews.com/my-europe/2025/06/17/eu-parliament-to-criminalising-ai-generated-child-abuse-material> (дата звернення: 20.06.2025).

19. 5Rights Foundation. EU AI Act enters into force: A crucial step for child protection.: 01.08.2024. URL: <https://5rightsfoundation.com/eu-ai-act-enters-into-force-a-crucial-step-for-child-protection/> (дата звернення: 20.06.2025).

20. Federal Trade Commission. Children's Online Privacy Protection Rule (COPPA). URL: <https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa> (дата звернення: 22.06.2025)

21. European Parliament and Council of the European Union. Directive 2011/93/EU of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography (Ukrainian translation). *Jurfem*.: 26.09.2023. URL: <https://jurfem.com.ua/dyrektyva-2011-92-eu-pereklad/> (accessed: 22.06.2025). (jurfem.com.ua)

22. Federal Trade Commission. Children's Online Privacy Protection Rule (COPPA). URL: <https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa> (дата звернення: 20.06.2025). (ftc.gov)

23. United States Congress. PROTECT Act of 2003 (S. 151, 108th Congress). *Congress.gov*.: 30.04.2003. URL: <https://www.congress.gov/bill/108th-congress/senate-bill/151> (accessed: 22.06.2025).

Information about the author:

Zvierieva Kateryna Serhiivna,

PhD in International Law,

Senior Lecturer of the Department of International, Civil

and Commercial Law

State University of Trade and Economics

19, Kyoto str., Kyiv, 03100, Ukraine