

УДК 347.772.3

DOI <https://doi.org/10.24144/2307-3322.2024.81.1.35>

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ ДІТЕЙ У СОЦІАЛЬНИХ МЕРЕЖАХ В КОНТЕКСТІ ПРАВА НА ЗАБУТТЯ

Садовська Д.І.,
аспірантка,

Львівський національний університет імені Івана Франка

ORCID: 0000-0001-7598-6394

e-mail: Diana.S12777@gmail.com

Садовська Д.І. Захист персональних даних дітей у соціальних мережах в контексті права на забуття.

Стаття присвячена правовому аналізу захисту конфіденційності особистих даних дітей у соціальних мережах в контексті права на забуття та Загального регламенту про захист даних. Встановлено, що більшість соціальних мереж мають власні правила користування, проте вони спрямовані на можливість залучення більшої кількості користувачів і прибуток, а не на безпеку особистих даних користувачів. Правові механізми реалізації та захисту прав людини в цифровому середовищі знаходяться на стадії формування та удосконалення. Доведено, що застосування права на забуття стало одним зі способів захисту персональних даних у соціальних мережах та в Інтернеті загалом. І хоча спершу право на видалення виникло лише на рівні судової практики Суду справедливості ЄС (далі Суд – ЄС), зараз створений досить дієвий механізм захисту права особи видалити застарілу інформацію про себе з урахуванням балансу між правом на приватність та правом на свободу вираження поглядів. Унаслідок психологічної незрілості та обмеженого життєвого досвіду діти та підлітки можуть легковажно розкривати чутливу особисту інформацію, що збільшує ймовірність зловживання такою інформацією як соціальними мережами, так і третіми особами. Тому неповнолітні користуються особливим захистом як вразливі категорії користувачів відповідно до Загального регламенту про захист даних. Обґрунтовано, що закріплення права на забуття в законодавстві ЄС допомагає усунути небажані наслідки від шерентінгу та повертає неповнолітнім можливість контролювати свій цифровий слід. Доведено, що Умови надання послуг більшості соціальних мереж гарантують додатковий захист даних неповнолітніх та кілька варіантів видалення вже поширеної інформації. Встановлено такі перешкоди для застосування права на забуття у соціальних мережах, як відсутність розробленого механізму видалення фото чи відео з неповнолітніми, що опубліковані без згоди дитини чи її батьків іншим користувачем; обмежена можливість користувачів до 13 років звернутися з запитом на видалення без посередництва; обмежена відповідальність соціальних мереж за втрату інформації, даних та прямі чи побічні збитки від таких дій.

Ключові слова: право на забуття, неповнолітні, соціальні мережі, Інтернет, цифрове середовище, цифрові права.

Sadovska D.I. Protection of children's personal data in social networks in the context of the right to be forgotten.

The article is devoted to a legal analysis of the protection of the confidentiality of children's personal data on social networks in the context of the right to be forgotten and the General Data Protection Regulation. It is established that most social networks have their own usage rules, but their priority is to attract more users and company profit rather than the security of users' personal data. Legal mechanisms for the implementation and protection of human rights in the digital environment are in the process of formation and improvement. It is proven that the application of the right to be forgotten has become one of the forms of personal data protection in social networks and on the Internet in general. Although initially the right to erasure emerged only at the level of the judicial practice of the Court of Justice of the EU, an effective mechanism has now been created to protect the individual's right to delete

outdated information about themselves, taking into account the balance between the right to privacy and the right to freedom of expression. Due to psychological immaturity and limited life experience, children and adolescents may casually disclose sensitive personal information, increasing the likelihood of abuse by both social networks and third parties. Therefore, minors receive special protection as vulnerable user categories according to the General Data Protection Regulation. It is argued that the incorporation of the right to be forgotten into EU legislation helps eliminate undesirable consequences of oversharing and restores minors' ability to control their digital footprint. The terms of service of most social networks ensure additional protection of minors' data and provide several options for deleting already disseminated information. Obstacles to the application of the right to be forgotten in social networks are identified, such as the lack of a developed mechanism for deleting photos or videos with minors published without the consent of the child or their parents by another user, the limited ability of users under 13 years old to request deletion without intermediaries, and the limited liability of social networks for the loss of information, data, and direct or indirect damages from such actions.

Key words: right to be forgotten, minors, social networks, Internet, digital environment, digital rights.

Постановка проблеми. За останнє десятиліття соціальні мережі щільно вкоренилися в наше життя. Лише в Україні за даними звіту компанії GlobalLogic [1] понад 76,6% населення зареєстровані та хоча б раз на тиждень використовують соціальні мережі. Тому зрозуміло, що у такому диджиталізованому світі соціальні платформи стали невіддільною частиною життя не лише дорослих, але й дітей. Алгоритми соціальних мереж налаштовані так, щоб зібрати якомога найбільше персональних даних про користувачів для потреб налаштування реклами, створення аналітики тощо. Зокрема, Центр конфіденційності компанії Meta у політиці конфіденційності вказує [2], що для персоналізованої взаємодії компанія збирає та обробляє інформацію з трьох основних джерел: публічного контенту (ім'я користувача у Facebook та Instagram, основна світлина, активність на публічних сторінках Facebook), контенту про користувача, який поширюють інші особи та контенту створеного самим користувачем. Неповнолітні користувачі через довірливість та брак досвіду можуть не розуміти повною мірою наслідки публікації персональних даних у соціальних мережах. А такі дані можуть залишатися загальнодоступними навіть через десятиліття, коли стають застарілими та неактуальними.

Персональна інформація про дітей в соціальних мережах часто також поширюється через їх батьків. Шерентінг – відносно нове явище, яке полягає в тому, що батьки без дозволу і без розуміння того, як працюють правила приватності, викладають у соцмережі фотографії, відео зі своїми дітьми чи діляться іншою персональною інформацією про них. Іронічним в такій ситуації є те, що Умови надання послуг більшості соціальних мереж вказують вікове обмеження у 13 років для реєстрації та створення акаунту. Тобто ті діти, які дотримуються цих правил, можуть бути неприємно здивовані тою тією кількістю інформації, яку можна знайти про них в Інтернеті.

Одним з варіантів часткового розв'язання проблеми захисту користувачів, в тому числі й неповнолітніх, від надмірної, застарілої інформації про них в цифровій мережі може стати застосування права на забуття. Воно належить до так званого покоління «нових прав» та полягає у тому, що особа за певних визначених законодавством підстав може звернутися до контролера даних з вимогою видалити особисту інформацію, яка є правдивою, але яку б особа хотіла вилучити.

Стан дослідження. Дослідженням теми права на забуття займалися різні правники-науковці, серед них Калітенко О.М., Спасибо-Фатєєва І.В., Тарасенко Л.Л., Сухорольський П.М. та інші. Водночас значна кількість правових нюансів, зокрема щодо застосування права на видалення у соціальних мережах практично не розглядаються у публікаціях та потребують подальших досліджень.

Метою цієї статті є правовий аналіз захисту персональних даних неповнолітніх у соціальних мережах в контексті права на забуття, а також дослідження юридичних перешкод при зверненні до контролерів даних з запитами на видалення.

Виклад основного матеріалу. Не можна заперечувати той факт, що сьогодні діти є активними користувачами соціальних мереж. Час їх перебування в мережі Інтернет з об'єктивних та з суб'єктивних причин збільшується. А якщо правові механізми реалізації прав людини в реальному житті вже достатньо розроблені, то їх аналоги для цифрового світу поки лише формуються, законодавча база більшості країн не встигає за розвитком технологій [3].

Через відсутність міжнародного регулювання більшість соціальних мереж вибудували власну систему правил користування, основа яких – національне законодавство, здебільшого США – штату Каліфорнія, де знаходяться штаб-квартири більшості з них, зокрема МЕТА (Facebook, Instagram), Twitter та інших. Такі правила мають на меті захистити соціальну мережу від ймовірних ризиків та створити безпечне середовище для користувачів. Але, звичайно, оскільки вони розроблені самими платформами пріоритет йде на забезпеченні можливості залучати більше користувачів та отримувати прибуток, а не на безпеку персональних даних користувачів.

Проаналізувавши Умови надання послуг трьох найпопулярніших платформ в Україні (Instagram – 16,1 млн користувачів, Facebook – 15,45 млн користувачів, TikTok – 10,55 млн користувачів [4]), можемо зазначити, що всі вони вказують мінімальне вікове обмеження у 13 років для створення акаунту. Такий віковий ценз бере свій початок з американського Закону про захист конфіденційності дітей в Інтернеті (COPPA), який забороняє компаніям збирати особисту інформацію дітей віком до 13 років без згоди батьків або збирати більше особистої інформації, ніж їм потрібно для роботи служби, призначеної для дітей віком до 13 років. На практиці, це означає, що діти вже з 13 років можуть без контролю дорослих самостійно створювати та ділитися власним контентом, зокрема фотографіями, відео та іншою персональною інформацією. Попри те, що молодші користувачі легко адаптуються до цифрового середовища та майже з народження «зі смартфоном в руках», не всі з них мають достатньо умінь та навичок, які необхідні для безпечного та ефективного використання соціальних мереж. Окрім цього підлітки часто через брак досвіду не можуть передбачити всі потенційні наслідки від поширеного ними контенту.

Батьки також часом створюють цифровий слід дітей, про який ті можуть навіть не здогадуватися. Це несе матеріальні ризики як для здорового розвитку дитини, так і для її фізичної безпеки. Через поширеність такого явища в англійській спільноті навіть виник новий термін «шерентінг» (sharenting) [5]. Він утворений від англійських слів parenting (виховувати) і to share (ділитися, розміщувати в інтернеті), і описує ситуацію, коли батьки та інші старші родичі викладають у соцмережі фотографії своїх дітей і публічно розповідають про ситуації з їхнього життя. Через вищезазначені фактори діти заслуговують на особливий захист своїх даних.

Світова спільнота активно почала обговорювати можливість видалити правдиву інформацію про себе з мережі Інтернет ще у 2014 році, після рішення Суду ЄС у справі Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González [6]. У цій справі Суд зобов'язав компанію Google видалити з пошукової системи посилання на дві сторінки каталонської газети La Vanguardia 1998 року випуску на тему примусового продажу нерухомості у зв'язку з заборгованістю по соціальному забезпеченню, де були розкриті персональні дані заявника – громадянина Іспанії Маріо Костея Гонсалеса. Рішенням було створено прецедент застосування права на забуття, згідно з яким пошукові системи та інші контролери даних за певних підстав мають видалити персональні дані після запиту суб'єкта даних.

Програвши у справі, компанія Google була змушена, з метою мінімізації судових позовів, запустити спеціальну онлайн-форму для подання запитів на видалення приватної інформації про себе користувачами. Був розроблений так званий тест на баланс інтересів, тобто стандартизовані критерії, за допомогою яких контролер зважує інтерес (публічний чи приватний) під час обробки запиту на видалення.

Подальший розвиток та закріплення багатьох ключових пунктів з рішення по справі Google Spain v AEPD and Mario Costeja González можемо спостерігати у Загальному регламенті про захист даних (General Data Protection Regulation). Документ був ратифікований Європейським парламентом 14.04.2016 року та набрав чинності 25 травня 2018 року. Документ закріплює додатковий захист для персональних даних дітей. Водночас у цьому питанні важливо зазначити хто є «дитиною» відповідно до Регламенту. Адже на відміну від Конвенції ООН про права дитини, яка містить конкретне визначення, що за загальним правилом дитиною вважається кожна людська істота до досягнення 18-річного віку, в Регламенті вік згадується лише стосовно згоди дитини у сфері послуг інформаційного суспільства.

В цілому документ пропонує кілька положень, які прямо (стаття 8,12, 40 Регламенту) або непрямо стосуються дітей (стаття 17 Регламенту). Зокрема у статті 8 Регламенту вказано, що для того, щоб у сфері пропозиції послуг інформаційного суспільства безпосередньо дитині опрацювання даних вважалось законним контролер повинен докласти розумних зусиль для перевірки надання згоди на таке опрацювання дитиною чи санкціонування такого надання носієм батьківської відповідальності щодо дитини, з урахуванням наявних технологій. Розуміємо, що таке фор-

мулювання викликає багато практичних питань щодо його виконання. По-перше, незрозуміло, що означає «безпосередньо пропонована дитині» [7]. Тобто це положення застосовується лише до послуг, спеціально орієнтованих на дітей (наприклад, YouTube для дітей) або це стосується платформ, якими користуються діти, хоча вони не націлені спеціально на них (наприклад, Facebook, Tik Tok). По-друге, «деклараційні» зобов'язання перевірки згоди та віку дитини є недостатніми для ефективного захисту малолітніх осіб в соціальних мережах. Для того, щоб обійти правила платформ дітям частіше за все потрібно при створенні облікового запису підтвердити, що їм є 18 років. Деякі платформи взагалі досить довгий час не вимагали навіть такої формальності. Так Instagram до 2019 року не запитував у нових користувачів дату їхнього народження [8], не кажучи вже про спробу перевірити цю інформацію. Також незрозумілим є і те, як платформи перевіряють, що особа, що санкціонує згоду є опікуном дитини.

Важливим елементом, який містить Регламент є пункт 1 статті 12, який закріплює обов'язок контролера вжити необхідних заходів для надання будь-якої інформації, спеціально призначеної для дитини у стислій, прозорій, доступній для розуміння формі. Хоча ці прикметники здаються такими, що не потребують пояснень, але вони заслуговують на ближчий розгляд, щоб прояснити їх фактичне значення в контексті законів про захист даних. Так, стислість як зазначає юрист Квебекської Колегії адвокатів Луї-Філіп Граттон в коментарі до Регламенту означає, інформація має бути подана коротко, але також вичерпно [9]. Прозорість як один із ключових принципів обробки персональних даних взагалі включає в себе зобов'язання компаній не приховувати інформацію та не намагатися заховати важливі деталі від споживачів. Діти зможуть надати усвідомлену згоду лише якщо будуть чітко розуміти на що вони погоджуються. Головна ідея принципу зрозумілості в тому, щоб стиль та форма написання були простими та доступними. Повідомлена інформація має бути однозначною та адаптованою до аудиторії.

Стаття 17 Регламенту хоча і стосується не лише дітей, містить окрему підставу на підставі якої неповнолітні можуть вимагати у контролера стирання своїх персональних даних. Важливим є і те, що загалом зобов'язання щодо видалення інформації Регламент покладає на контролерів даних, тобто на соціальні мережі, а не на батьків, що робить акцент на інтересах дитини, а не на звинуваченні чи покаранні батьків за їхні дії та рішення.

Звичайно, неповнолітні користувачі можуть зіштовхнутися з певними складнощами у реалізації права на забуття. Так діти молодшого віку (які не досягли мінімального вікового порогу, 13 років) не можуть звертатися самостійно до більшості соціальних мереж щодо видалення даних про себе. Цим можуть користуватися батьки чи інші опікуни, які створюють та ведуть соціальні мережі від імені дитини чи монетизують контент з дітьми. Той факт, що діти часто надто малі для доступу до технологій, не означає, що використання дорослими цих інструментів та платформ не може зашкодити їм.

Зрештою важливо у кожній окремій ситуації намагатися знайти баланс між правом батьків на свободу вираження поглядів та правом дитини на розвиток (стаття 6 Конвенції), недоторканність приватного життя (стаття 16 Конвенції), приватне та сімейне життя (стаття 8 Конвенції). Вразливість дітей як суб'єкта даних є багатомірною, але, мабуть, найбільше занепокоєння викликає ризик того, як на психічний розвиток дітей впливатиме підвищена соціальна тривога та дискомфорт. Крім того, слід зазначити, що право на забуття не є абсолютним. Законна потреба захищати приватне життя, видаляти особисту інформацію про себе не повинна суперечити таким умовам демократії та політичної свободи як: свободі ЗМІ та праву шукати, отримувати й передавати інформацію, що становить суспільний інтерес.

Наразі дія Регламенту прямо розповсюджується на 27 країн Європейського Союзу та 3 країни Європейської Економічної зони. Проте документ одночасно є проявом глобальної тенденції та прокладає шлях до міжнародного законодавства, спрямованого на захист персональних даних в Інтернеті. Україна підписавши Угоду про асоціацію з ЄС також взяла на себе зобов'язання «забезпечити належний рівень захисту персональних даних відповідно до найвищих європейських та міжнародних стандартів, зокрема відповідних документів Ради Європи» [10]. Зараз головним законом, який регулює відносини, пов'язані із захистом персональних даних під час їх обробки є ЗУ «Про захист персональних даних». І хоча в ньому як і в інших законодавчих актах України поки не закріплене право на забуття, можна прослідкувати тенденцію до посилення передачі контролю над особистою інформацією до суб'єктів даних. Наприклад, згідно з пунктом 4 частини 2 статті 15 персональні дані підлягають видаленню або знищенню, зокрема, в разі набрання законної сили рішенням суду щодо видалення або знищення персональних даних. Крім того, додаткові гарантії

захисту персональних даних дітей можна прослідкувати у Законі України «Про охорону дитинства», зокрема у статті 10, яка забороняє розголошення чи публікацію будь-якої інформації про дитину, якщо оприлюднення цих даних може завдати неповнолітньому шкоди.

Досліджуючи політику конфіденційності компанії Meta локалізовану для українців, бачимо, що користувач від 13 років може видалити поширену ним інформацію двома способами: знайти й видалити конкретний допис чи фото або видалити обліковий запис назавжди. Стандарти спільноти Facebook [11] гарантують також додатковий захист даних неповнолітніх, зокрема за запитом користувача, уряду, правоохоронних органів або зовнішніх експертів з безпеки дітей соціальна мережа може видалити контент, створений з метою ідентифікації неповнолітнього приватної особи, якщо існує ризик для її безпеки. Серйозним недоліком є те, що не має розробленого механізму видалення фото чи відео з неповнолітніми опублікованих без згоди дитини іншим користувачем. Виходом в цій ситуації може бути лише скарга на такий контент, що не означає надійний захист. На додаток, більшість соціальних мереж в умовах надання послуг прямо зазначають, що їх «відповідальність обмежена у максимальному ступені, дозволеному чинним законодавством» [5]. А отже вони не несуть відповідальність втрату інформації, даних та прями чи побічні збитки.

Висновки. Розвиток технологій, доступність цифрового середовища частково змінюють світ дітей, породжуючи додаткову потребу контролювати персональні дані. Діти через свій вік часто не можуть усвідомлювати ризики, пов'язані з розкриттям їхньої особистої інформації в онлайн середовищі, а тому стають найбільш вразливою групою користувачів.

В більшості країнах нормативне регулювання використання соціальних мереж підлітками не встигає за стрімким розвитком технологій. Такі платформи при розробці правил користування орієнтуються здебільшого на законодавство США, а саме штату Каліфорнія, де знаходяться штаб-квартири багатьох технологічних компаній та регіональне регулювання. Документи як Загальний регламент про захист даних здійснюють великий вплив на розвиток внутрішніх правил соціальних мереж не лише в межах тої території на яку, вони поширюють свою дію, а й на увесь світ підвищуючи стандарти захисту. Закріплене у статті 17 Регламенту право на забуття допомагає збалансувати конкуруючі інтереси батьків та дітей, забезпечуючи одночасно батькам право на свободу вираження поглядів та захищаючи переважну можливість дітей захистити своє право на приватність. Можливість реалізації права бути забутим хоча і не усуває первинної шкоди, яку дитина може зазнати через необдумане поширення нею чи її батьками особистої інформації, проте збільшує можливість обмеження рівня наслідків від поширення даних в довгостроковій перспективі. Дорослі мають право змінити свою думку та видалити інформацію, яку вони опублікували про себе, якщо вона негативно вплине на них, діти повинні мати такий самий привілей.

Звичайно, забезпечення безпеки діяльності дітей в соціальних мережах є комплексним завданням. Воно не може обмежуватися лише безпекою персональних даних чи забезпеченням права на забуття. Варто поступово відходити від правила автоматичного звільнення соціальних мереж від відповідальності та на державному рівні розробляти програми для підвищення рівня цифрової грамотності молодших користувачів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. 28 млн в YouTube, 10 млн у TikTok: як війна змінила українські соцмережі. AIN.UA. URL: <https://ain.ua/2022/08/06/yak-vijna-zminyla-soczmerezhi/> (дата звернення: 15.12.2023).
2. Політика конфіденційності. Центр конфіденційності компанії Meta. URL: <https://uk-ua.facebook.com/privacy/policy/> (дата звернення: 15.12.2023).
3. Право на забуття: зб. ст. / за ред. І.В. Спасибо-Фатєєвої. – Харків: Видавництво «ЕКУС», 2021. – 172 с.
4. Якими соцмережами користуються українці під час війни: статистика. SPEKA. URL: <https://speka.media> (дата звернення: 20.12.2023).
5. Understanding the Ramifications of ‘Sharenting’: Children’s “Right to be forgotten”. Humanium. URL: <https://www.humanium.org/en/understanding-the-ramifications-of-sharenting-childrens-right-to-be-forgotten/> (дата звернення: 20.12.2023).
6. Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González. EUR-Lex. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131> (дата звернення: 15.12.2023).

7. Загальний регламент про захист даних (GDPR). GDPR TEXT. URL: <https://gdpr-text.com/uk/> (дата звернення: 25.12.2023).
8. Інстаграм тестує функцію, яка визначатиме вік користувача за фото. Детектор медіа. URL: <https://ms.detector.media/sotsmerezhi/post/29722/2022-06-23-instagram-testuie-funktsiyu-ya-ka-vyznachatyme-vik-korystuvacha-za-foto/> (дата звернення: 25.12.2023).
9. The General Data Protection Regulation and children's rights: questions and answers for legislators, DPAs, industry, education, stakeholders and civil society. Better Internet for kids. URL: https://www.betterinternetforkids.eu/documents/167024/2013511/GDPRRoundtable_June2017_FullReport.pdf (дата звернення: 15.12.2023).
10. Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони. Верховна Рада України. Офіційний вебпортал парламенту України. Зконодавство України. URL: https://zakon.rada.gov.ua/laws/show/984_011#top (дата звернення: 17.12.2023).
11. Додатковий захист неповнолітніх. Стандарти спільноти Facebook. URL: <https://transparency.fb.com/uk-ua/policies/community-standards/additional-protection-minors/> (дата звернення: 17.12.2023).