

УДК 342.7:347.12

DOI <https://doi.org/10.32837/pyuv.v0i2.1020>*Д. О. Колодін**orcid.org/0000-0001-6368-0849**кандидат юридичних наук, доцент,**декан факультету цивільної та господарської юстиції**Національного університету «Одеська юридична академія»**А. І. Веретільник**orcid.org/0000-0003-4168-4077**студентка II курсу магістратури факультету цивільної та господарської юстиції**Національного університету «Одеська юридична академія»*

## ПРАВА ЛЮДИНИ В ЦИФРОВУ ЕПОХУ: ПРОБЛЕМИ ТЕОРІЇ І ПРАКТИКИ

У 2014 році Суд Європейського союзу виніс рішення у справі «Google (Іспанія) проти AEPD & Mario Costeja González» [1], згідно з яким оператор пошукової системи несе відповідальність за обробку персональної інформації, яка з'являється на веб-сторінках, опублікованих третіми сторонами, і суб'єкт даних має право видалити свої дані з пошукової системи, якщо його попросять зробити це, наприклад, у разі незаконної обробки та зберігання даних або якщо дані є неправильними та нерелевантними. Таке рішення суд прийняв на підставі тлумачення Хартії основних прав ЄС, яка гарантує громадянам право на приватність (стаття 7) і безпеку персональних даних (стаття 8) [2]. Водночас це спровокувало суспільну дискусію, яка зосередилася на взаємозв'язку між правом на інформацію, з одного боку, та правом на недоторканність приватного життя, конфіденційність і захист особистої інформації, з іншого [3]. Наприклад, Shoor [4] у своєму дослідженні негативно оцінила зазначене вище судове рішення та зазначила, що надмірне регулювання призведе до того, що компанії, які контролюють пошукові системи, автоматично видалятимуть контент, оскільки це зробити простіше, ніж сплачувати штрафи і вирішувати проблеми у судових процесах щодо скарги кожного користувача [5]. Крім того, постає питання: що робити, якщо особа, інформація про дії якої має суспільне значення, вимагає видалення цієї інформації [6]? У той час як посилення захисту прав людини, зокрема, права на приватність в мережі Інтернет, є очевидною перевагою, що впливає зі змісту судового рішення, забезпечення балансу суспільних і приватних інтересів стає проблемним питанням у контексті так званого «Права на забуття», активне обговорення якого зумовлене зазначеним знаковим рішенням у справі «Google v. Costeja» [1].

Згадане вище судове рішення стало правовою основою для запровадження Загального регламенту захисту даних ЄС (GDPR), який набув чинності 25 травня 2018 року в Європейському Союзі. Серед особливостей документа є згадка «права на

доступ» та «права на забуття». Наприклад, керуючись ст. 15 цього регламенту суб'єкт даних має право вимагати інформацію щодо цілей, порядку збору, обробки його персональних даних та доступу до них у разі їх збору оператором. Неправильні персональні дані повинні бути виправлені на вимогу суб'єкта даних (стаття 16). Право на забуття означає, що на вимогу суб'єкта оператор зобов'язаний без невиправданої затримки видалити персональні дані суб'єкта за наявності підстав, передбачених ст. 17 (1), наприклад, у разі порушення порядку збору та обробки даних, якщо суб'єкт відкликає свою згоду на обробку даних, якщо мета збору та обробки даних досягнута та зберігання інформації не має значення, нарешті, якщо збір та обробка відбувалися з порушенням законодавства. У разі подання скарги обробка даних суб'єкта може бути призупинена відповідно до ст. 18 регламенту. «Право на мобільність даних» (ст. 20) передбачає, що на вимогу суб'єкта йому повинні бути надані його персональні дані, які легко зчитуються автоматично, передані іншому оператору, і загалом це буде зручно для проведення комп'ютерних операцій. Простіше кажучи, суб'єкт має право отримати персональні дані в зручній формі. Слідуючи ст. 12 (1), оператор зобов'язаний надати інформацію про персональні дані суб'єкта у зрозумілій, стислій, чітко сформульованій формі, яка може бути підтверджена в майбутньому посиланням на лист, зокрема, електронну пошту, або усно, якщо це можна підтвердити, наприклад, голосовим повідомленням [7].

У травні 2017 року французький кіберрегулятор CNIL наклав штраф на Facebook за маніпулювання персональними даними користувачів [8]. Компанію визнали винною у використанні конфіденційних даних громадян для показу їм цільової реклами на основі їхніх сексуальних уподобань. Маніпуляції передбачали відстеження за допомогою файлів cookie, про які користувачі не були достатньо поінформовані.

7 грудня 2018 року в Іспанії набув чинності Ley Organica 3/2018 – Закон, згідно з яким Іспанія

прийняла GDPR, і попередній Закон Ley Organica 15/1999 про захист персональних даних втратив чинність, за винятком ст. 22-24.

У 2019 році Суд ЄС у Люксембурзі визнав «право на забуття» лише в країнах-членах ЄС, задовольнивши таким чином позов Google LLC проти французького кіберрегулятора CNIL, у якому позивач просив визнати едісним «право на забуття» за межами ЄС, де вони також використовуються пошукова система Google [9;10].

Наступна проблема, яка пов'язана із порушенням прав людини у мережі інтернет, – це мова ворожнечі в соціальних мережах [11, 12]. Для початку, розглянемо, що означає мова ворожнечі на прикладі Facebook. Відповідно до частини III, пункту 12 стандартів спільноти Facebook [13], прояви ворожнечі у Facebook заборонені. Це стосується дискримінації конкретної особи або групи осіб за низкою характеристик, таких як раса, етнічна приналежність, стан здоров'я, стать, зовнішній вигляд тощо. Такі напади та переслідування в Інтернеті є неприйнятними. Ознаками мови ворожнечі є жорстокі та образливі висловлювання, засновані на порівнянні так званих захищених характеристик, до яких належать зазначені вище стать, гендер, мова, національність, етнічна приналежність, раса, колір шкіри тощо. Адміністрація Facebook зберігає за собою дискреційні повноваження ідентифікувати висловлювання як мову ненависті, модерувати та обмежувати користувачів на цій основі. Варто додати, що мова ворожнечі може бути використана для критики або спонукання інших не поширювати її, але адміністрація не буде видаляти такі публікації, лише якщо особа має чітко сформульований намір процитувати мову ворожнечі (ознаки того, що особа насправді не підтримує мовна ворожнеча і її метою є її критика або спонукання інших не поширювати мову ворожнечі).

Вже певний час років спостерігається все більший прогрес у спробах регулювати мову ненависті в Інтернеті [14, 15, 12]. Наприклад, 30 червня 2017 року парламент Німеччини схвалив закон, який вимагає від соціальних мереж реагувати на ворожнечу користувачів і видаляти такий контент протягом 24 годин [6]. В іншому випадку соцмережу чекає значний штраф.

Оскільки кожна людина має право використовувати мережу інтернет та бути в безпеці в Інтернеті, не завдаючи шкоди собі, своїм родичам і близьким, поширення мови ненависті в Інтернеті становить поточну загрозу для реалізації цього права [17, 12]. Використання соціальних мереж тісно пов'язане з цим явищем [18]. Наприклад, у 2018 році в доповіді ООН про репресії проти етнічної групи рохінджа в М'янмі зазначено, що соціальна мережа Facebook сприяє зростанню ворожнечі в суспільстві [19]. Тоді голова Facebook

визнав, що мова ненависті в м'янманському секторі Facebook сприяла етнічним вбивствам у країні [20]. Дослідження Whitten-Woodring, Kleinberg, Thawngmung і Thitsar (2020) робить висновок, що Facebook справді сприяв поляризації поглядів у М'янмі [22, 23]. Проте за достатнього рівня інформаційної та цифрової культури цьому можна було запобігти. Так чи інакше, оскільки в М'янмі немає розвинутих демократичних інституцій, неможливо було домогтися неконтрольованого споживання контенту, який радикалізував погляди ворожої влади та населення на народ рохінджа [21]. У 2021 році Френсіс Хауген, колишня співробітниця і обвинувач Facebook, підтвердила у своїх свідченнях у Сенаті США, що компанія проявила необережність, не регулюючи контент за межами США, що призвело до неконтрольованого поширення мови ненависті та етнічних чисток у М'янмі [24].

Далі варто зосередитися на алгоритмах і персональних даних. Алгоритми онлайн-реклами запам'ятовують, що цікавило користувача, які сайти він відвідував. На основі історії пошуку користувачеві показуються релевантні оголошення, що іноді створює відчуття, ніби за ними спостерігають. На жаль, це не просто ілюзія, адже при використанні пошукової системи за замовчуванням дані перегляду зберігаються та передаються компанії для «покращення надання послуг». Таким чином, за рахунок постійного вдосконалення таргетингу, тобто адресної доставки інформації користувачу, забезпечуються актуальність і максимальна ефективність реклами та пропозицій, які працюють на основі алгоритмів Google і Facebook. Однак побічні ефекти полягають у тому, що людині може бути показана інформація, яка для неї небажана. З іншого боку, реклама може бути нав'язливою. У цьому випадку мати математичну схему, яка, здається, знає краще за вас, чого ви хочете, пригнічує.

Інший приклад сумнівний підбір контенту алгоритмами TikTok. Сама компанія описує це як потік персоналізованого відеоконтенту [25]. Існують дослідження [26], за результатами яких респонденти вказують, що, незважаючи на всі свої зусилля, щоб «приручити» алгоритми TikTok і «одомашнити» канал (свою стрічку), їм це не вдається і це призводить до появи контенту небажаного або тривожного вмісту. Справа в тому, що алгоритм стрічки TikTok підлаштовується під особисті уподобання користувачів, щоб те, що їм подобається, з'являлося частіше. Простіше кажучи, «сигнал», який посилає штучний інтелект TikTok, постійно посилюється, що може призвести до радикалізації поглядів і думок. Наприклад, якщо користувач має консервативні погляди, з часом алгоритм може запропонувати йому більш радикальний контент. Або якщо

людині стає сумно, на її стрічці можуть з'явитися відео, які навіюють смуток, загострюють депресію. З іншого боку, коли людині дійсно потрібна допомога або вона має недіагностоване психічне захворювання, їй може допомогти освітній контент або інші користувачі TikTok можуть допомогти їй дізнатися більше про свій стан, що може мати позитивні наслідки. Проте неоднозначність підбору контенту призводить до появи складного питання: як алгоритми впливають на нашу ідентичність і вільний вибір нашої поведінки [28]. Занепокоєння викликає той факт, що незважаючи на те, що алгоритм TikTok здатний передбачити, яке відео може сподобатися, а яке не сподобатися, ми, як спільнота, не можемо передбачити, до чого це призведе в кожному окремому випадку, що є предметом ширшої дискусії щодо наслідків майбутніх алгоритмів штучного інтелекту та їх впливу на права людини.

У січні 2022 року австрійський інспектор із захисту даних постановив, що використання Google Analytics порушує GDPR [29]. Це рішення посилює напруженість щодо передачі даних між Європою та Сполученими Штатами, оскільки, за словами Google, дані європейських користувачів зберігаються та обробляються в Сполучених Штатах через використання Google Analytics. Рішення, прийняте в Австрії, може бути поширене на інші європейські країни, оскільки вони співпрацюють з Австрією в Європейській раді із захисту даних.

20 січня 2022 року Європарламент прийняв попередню редакцію Закону про цифрові послуги (DSA). Законопроект пропонувався обмежити загальний моніторинг користувачів в Інтернеті та обмежити адміністрацію сайту тотальною цензурою небажаного контенту, з точки зору модераторів сайту. Законопроект передбачав обов'язок власників інтернет-платформ інформувати користувачів щодо особливостей збору даних та модерування контенту. Веб-сайти мають надавати інформацію та дані дослідникам, наприклад некомерційним організаціям, для дослідження та підвищення прозорості та безпеки використання Інтернету [30]. Як зазначається у статті Human Rights Watch (2022), серед аспектів, які залишаються поза увагою законопроекту, – таргетована реклама, загроза розширення державного контролю над Інтернетом, особливості онлайн-роботи, як-от неврегульованість соціальних гарантій для модераторів контенту тощо.

Згідно з попередньою редакцією закону, ухваленого Європарламентом 21 січня 2022 року, буде обмежена таргетована реклама для неповнолітніх, а також заснована на релігійних, сексуальних і політичних переконаннях користувачів. Meta (ex-Facebook) внесла такі зміни до своєї політики наприкінці 2021 року [31], але тепер вони будуть

відображені в законодавстві ЄС. Відмова від обробки персональних даних не повинна ускладнюватися відключенням функцій сайту згідно з новими правилами. Буде посилено відповідальність онлайн-ринків за забезпечення прозорості та репутації продавців. Крім того, пропонується обмежити маніпуляції з отриманням згоди на обробку даних. Це стосується використання так званих «темних шаблонів», коли за допомогою відображення контенту (нових вікон браузера, зображень, підказок тощо) особа спонукається дати згоду на обробку її персональних даних.

Варто додати, що подібні правові ситуації виникають у таких країнах, як Німеччина, Франція, Аргентина, Індія та Південна Корея. В першу чергу, це пов'язано з технологічним розвитком, оскільки громадяни цих країн користуються соціальними мережами, як і всі інші люди на планеті. Водночас, слід зазначити різницю в доктринальному рівні розуміння свободи слова, преси та конфіденційності, характерну для Сполучених Штатів Америки. Справа не тільки в тому, що Google є американською компанією і, враховуючи її репутацію, повинна протестувати проти судових рішень, які посилюють підзвітність і відповідальність за збір і обробку даних і використання алгоритмів. Як зазначає Вітмен (2003) [32], наївно очікувати, що стандарти конфіденційності будуть такими ж значущими для Сполучених Штатів, як і для європейців. Цьому передувала довга культурна, історична та правова традиція, яка ставить свободу слова вище приватності як такої, як це відображено в конституційному праві США, наприклад у Першій поправці. Історія показала, що Вітмен мав рацію у своїх прогнозах щодо реагування на конфлікт приватності та свободи слова, оскільки саме в англосаксонській правовій родині існувала різка критика «права на забуття» [33].

Razmetaeva (2017) [34] підтверджує цю думку, але на прикладі європейських країн. Зокрема, вона наводить приклад Національного реєстру громадян Нідерландів, який використовувався під час нацистської окупації для пропаганди расової, етнічної, релігійної, сексуальної тощо ненависті [35, 36, 37, 38].

Отже, проблема забезпечення захисту прав людини в мережі інтернет потребує свого вирішення як на національному, так і на міжнародному рівні. Зокрема, необхідно прийняти низку нормативно-правових актів, які б регламентували особливості використання персональних даних в мережі інтернет, а також особливості функціонування інтернет-платформ, що запроваджують алгоритми з використанням штучного інтелекту. Крім того, Україна має уніфікувати власне законодавство у досліджуваній сфері із законодавством Європейського союзу, яке наразі є більш прогресивним.

*Література*

1. European Court of Justice. (May 13, 2014). Google Spain SL & Google Inc. v. AEPD & M.C. González.
2. European Parliament. (December 18, 2000). Charter of Fundamental Rights of The European Union (2000/C364/01). Official Journal of the European Communities, C364/3.
3. Leatherwood, E. (September 9, 2014). Why Google's Removal of News Links in the EU Is a Good Thing.
4. Shoor, E.A. (2014). Narrowing the right to be forgotten: why the European Union needs to amend the proposed data protection regulation. *Brook. J. Int'l L.*, 39, 487. In <https://ssrn.com/abstract=2410240> (access date: 21.01.2022)
5. Mason, R. (July 25, 2014). Right to be forgotten: Wikipedia chief enters internet censorship row. *The Guardian*. In
6. Harper, T., & Owen, J. (May 30, 2014). Google privacy law 'means total rethink of basic freedoms'. *The Independent*.
7. Data Privacy Office LLC. (2022). General data protection regulations [UKR].
8. Deutsche Welle. (May 16, 2016). France fines Facebook over 'targeted advertising'.
9. Androschuk, G. (October 9, 2019). Court of Justice: Google has won the dispute over the right to forget.
10. European Court of Justice. (September 24, 2019). *Google LLC v. CNIL*.
11. Del Vigna, F. et al. (2017). Hate me, hate me not: Hate speech detection on Facebook. In *Proceedings of the First Italian Conference on Cybersecurity (ITASEC17)* (pp. 86-95).
12. O'Regan, C. (2018). Hate speech online: An (intractable) contemporary challenge? *Current Legal Problems*, 71(1), 403-429.
13. Facebook. (January 16, 2022). Community standards. Unacceptable content.
14. Alkiviadou, N. (2017). Regulating Hate Speech in the EU. In *Online hate speech in the European Union: A discourse-analytic perspective*, 6-10.
15. Alkiviadou, N. (2019). Hate speech on social media networks: towards a regulatory framework? *Information & Communications Technology Law*, 28(1), 19-35.
16. Shatalin, W. (June 30, 2017). The Bundestag has approved the Facebook law.
17. Willard, N.E. (2007). *Cyber-safe kids, cyber-savvy teens: Helping young people learn to use the Internet safely and responsibly*. John Wiley & Sons.
18. Mathew, B., Dutt, R., Goyal, P., & Mukherjee, A. (2019, June). Spread of hate speech in online social media. In *Proceedings of the 10th ACM Conference on Web Science* (pp. 173-182).
19. UN. (September 28, 2018). *Report of the Detailed Findings of the Independent International Fact-Finding Mission in Myanmar*.
20. TSN News UA. (April 11, 2018). Facebook will block "hate speech" that promotes ethnic killings in Myanmar.
21. Whitten-Woodring, J., Kleinberg, M.S., Thawngmung, A., & Thitsar, M.T. (2020). Poison if you don't know how to use it: Facebook, democracy, and human rights in Myanmar. *The International Journal of Press/Politics*, 25(3), 407-425.
22. Fink, C. (2018). Dangerous speech, anti-Muslim violence, and Facebook in Myanmar. *Journal of International Affairs*, 71(1.5), 43-52.
23. Lee, R. (2019). Extreme speech in Myanmar: The role of state media in the Rohingya forced migration crisis. *International Journal of Communication*, 13, 22.
24. Akinwotu, E. (October 7, 2021). Facebook's role in Myanmar and Ethiopia under new scrutiny.
25. TikTok. (June 18, 2020). How TikTok recommends videos #ForYou.
26. Simpson, E., Hamann, A., & Semaan, B. (2022). How to Tame "Your" Algorithm: LGBTQ+ Users' Domestication of TikTok. In *Proceedings of the ACM on Human-Computer Interaction*, 6(GROUP), 1-27.
27. Schellewald, A. (2021). On getting carried away by the TikTok algorithm. Paper presented at AoIR 2021: The 22nd Annual Conference of the Association of Internet Researchers. Virtual Event: AoIR.
28. Brownell, B. (May 29, 2019). Yuval Noah Harari and Fei-Fei Li on Artificial Intelligence: Four Questions that Impact All of Us.
29. Noyan, O. (January 13, 2022). Use of Google Analytics violates EU law, Austrian authority rules.
30. Human Rights Watch. (January 7, 2022). EU: Put Fundamental Rights at Top of Digital Regulation.
31. MediaSapiens. (November 11, 2021). Facebook and Instagram will ban ads targeting race, sexual orientation and religion.
32. Whitman, J.Q. (2003). The Two Western Cultures of Privacy: Dignity versus Liberty. *Yale Law Journal*, 113, 1151.
33. Mayes, T. (March 18, 2011). We have no right to be forgotten online. *The Guardian*.
34. Razmetaeva, Yu. (October 28-29, 2017). Leave me alone, or the right to be forgotten. Human rights: philosophical, theoretical, legal and political dimensions, 221-235.
35. Moore, B. (1998). *Victims and Survivors: the Nazi Persecution of the Jews in the Netherlands 1940 - 1945*. Oxford: Arnold
36. Deak, I. (2009). *The Politics of Retribution in Europe*. Princeton: Princeton University Press
37. Presser, J. (2010). *Ashes in the wind: the destruction of Dutch Jewry*. Londen: Souvenir Press
38. Griffioen, P., & Zeller, R. (n.d.). *The Netherlands: the greatest number of Jewish victims in Western Europe*.

**Анотація**

**Колодін Д. О., Веретельник А. І. Права людини в цифрову епоху: проблеми теорії і практики.** – Стаття.

У статті досліджено стан захисту прав людини в мережі інтернет. Автори статті дійшли висновку щодо наявності проблеми співвідношення приватних і публічних інтересів у досліджуваній сфері. Зокрема, йдеться про необхідність захисту права на інформацію в мережі інтернет, з одного боку, та права на недоторканність приватного життя, з іншого боку. У статті, зокрема, проаналізовано Загальний регламент захисту даних ЄС, в якому зроблено спробу упорядкування використання персональних даних користувачів мережі інтернет на території Європейського союзу. Серед іншого, в регламенті захисту даних вперше використано концепцію «право на забуття». Право на забуття означає, що на вимогу суб'єкта оператор зобов'язаний без невинуватої затримки видалити персональні дані суб'єкта за наявності певних визначених регламентом підстав. Серед проблемних аспектів забезпечення і захисту прав у мережі інтернет автори статті називають також маніпулювання даними і використання персональних даних для таргетування реклами. При цьому, судова практика в цій

сфері складається на користь приватних осіб, втім на законодавчому рівні чіткі норми, які б забороняли використовувати таргетування контенту в залежності від уподобань конкретного користувача мережі інтернет, поки що не запроваджені. Таргетування контенту також пов'язане з можливим поширенням ворожнечі, оскільки алгоритм платформи може формувати більш радикальний контент з метою утримання уваги користувача і виходячи з його уподобань. Зокрема, стрічка TikTok підлаштовується під особисті уподобання користувачів, щоб те, що їм подобається, з'являлося частіше. Простіше кажучи, «сигнал», який посиляє штучний інтелект TikTok, постійно посилюється, що може призвести до радикалізації поглядів і думок. Наприклад, якщо користувач має консервативні погляди, з часом алгоритм може запропонувати йому більш радикальний контент. Автори статті роблять висновок, що проблема забезпечення захисту прав людини в мережі інтернет потребує свого вирішення як на національному, так і на міжнародному рівні. Зокрема, необхідно прийняти низку нормативно-правових актів, які б регламентували особливості використання персональних даних в мережі інтернет, а також особливості функціонування інтернет-платформ, що запроваджують алгоритми з використанням штучного інтелекту.

*Ключові слова:* права людини, право на забуття, право на мобільність інформації, персональні дані, штучний інтелект.

### Summary

**Kolodin D. O., Veretelnyk A. I. Human rights in the digital era: problems of theory and practice.** – Article.

The article examines the state of human rights protection on the Internet. The authors of the article came to a conclusion regarding the existence of a problem of the balance of private and public interests in the researched area. In particular, it is about the need to protect the right to information on the Internet, on the one hand,

and the right to inviolability of private life, on the other. The article, in particular, analyzes the EU General Data Protection Regulation, which attempts to regulate the use of personal data of Internet users on the territory of the European Union. Among other things, the concept of "right to be forgotten" was used for the first time in the data protection regulations. The right to be forgotten means that at the request of the subject, the operator is obliged to delete the subject's personal data without undue delay, if there are certain grounds defined by the regulation. Among the problematic aspects of ensuring and protecting rights on the Internet, the authors of the article also mention data manipulation and the use of personal data for advertising targeting. At the same time, judicial practice in this area is in favor of private individuals, however, at the legislative level, clear rules that would prohibit the use of content targeting depending on the preferences of a particular Internet user have not yet been introduced. Content targeting is also associated with the possible spread of hostility, as the platform's algorithm can generate more radical content in order to keep the user's attention and based on their preferences. In particular, the TikTok feed is adjusted to the personal preferences of users so that what they like appears more often. Simply put, the "signal" sent by TikTok's artificial intelligence is constantly amplified, which can lead to radicalization of views and opinions. For example, if a user has conservative views, over time the algorithm can offer him more radical content. The authors of the article conclude that the problem of ensuring the protection of human rights on the Internet needs to be solved both at the national and international levels. In particular, it is necessary to adopt a number of legal acts that would regulate the specifics of using personal data on the Internet, as well as the specifics of the functioning of Internet platforms that introduce algorithms using artificial intelligence.

*Key words:* human rights, the right to be forgotten, the right to information mobility, personal data, artificial intelligence.