

Токарева В. О.,

кандидат юридичних наук,

доцент кафедри цивільного права

Національного університету «Одеська юридична академія»

ПРАВО НА ВИДАЛЕННЯ ТА ПРАВО НА ЧИСТИЙ ЦИФРОВИЙ ЛИСТ

У науці піддається критиці право на видалення або «право на забуття» передбачене Регламентом ЄС 2016/679 (далі Регламент ЄС 2016/679) відомого як GDPR, через обмеженість реалізації права на видалення даних або «права на забуття», адже допускає лише можливість видалення персональних даних за дотриманням визначених умов та певних ситуацій [1]. Оскільки ст. 17 Регламенту ЄС 2016/679 передбачає виключення із права на видалення даних, які покликані врівноважити інтереси контролерів даних та суб'єктів даних, на думку Б. Кастерса право на видалення не є основним правом, по-перше, тому, що воно міститься у вторинному, а не в основному законодавстві, і, по-друге, тому, що воно не є абсолютним правом та передбачає виключення із застосування.

М. Фазліоглу підтримує тезу, про те, що реалізація права на видалення даних є досить обмеженим та контролери не завжди зобов'язані співпрацювати із запитом суб'єктів даних [2].

З огляду на зазначене, поряд із законодавчим закріпленням права на видалення даних у доктрині висувається ідея про існування права почати все з чистого (цифрового) листа, яке покликане дозволити особам дійсно розпочати абсолютно нову (цифрову) ідентичність. Оскільки алгоритми збирання та профілювання великих даних є механізмами які з часом самопосилуються, про що зазначає винахідник Гугл Р. Курцвейл [3], то навіть незначні відхилення, невірні або неповні дані, можуть в подальшому призвести до ще більших значних не точних результатів у висновках та профілях. Наприклад, спостереження правоохоронними органами в більшій мірі, будучи зосередженим у неблагополучних районах міста, може призвести з часом до упередженого та суб'єктивного заповнення баз даних та профілювання мешканців цих районів, навіть за відсутності їх девіантної поведінки, з огляду на ризики пов'язані із районом проживання.

За твердженням Т. Калдерса та Б. Кастерса, оскільки алгоритми та інструменти профілювання ризику у подальшому можуть

застосовуватися для отримання профілів осіб які можуть потенційно схильними до правопорушень з поліцейських баз даних, результати будуть свідчити [4], що поліції слід зосередити спостереження за цими районами, водночас данні від початку містили упередженість. Таким чином мешканці навіть без ознак девіантної поведінки будуть під прихильним наглядом правоохоронних органів. Посилення поліцейського нагляду може призводити до стигматизації цих районів, зниження вартості нерухомості в цих районах та ускладнити можливість позбавитися від профілів та стереотипів, які стануть перешкодою подальшому переїхати в інший район. Такі результати профілювання можуть залишитися з особою на все життя.

Можна порівняти із ситуацією коли особа повернувшись після відбуття покарання у закладах позбавлення волі, повинна мати можливість розпочати життя з чистого аркуша. Незважаючи на те, що в деяких юрисдикціях заборонено відмовляти будь-кому в прийомі на роботу через судимість, насправді реінтеграція може бути складною для колишніх засуджених. Саме з цієї причини в деяких штатах США, наприклад штаті Нью-Йорк, ухвалено закон, який забороняє дискримінацію при прийомі на роботу з посиленням та на підставі судимості (CBED) [5]. В цьому прикладі антидискримінаційного законодавства начебто повинно бути достатньо, для переконання у необхідності розробки прав на цифровий лист та з тим, на думку прибічників запровадження даного права, воно має охоплювати більш широке коло питань, які не можуть бути розв'язані та вирішенні в межах норм антидискримінаційного законодавства.

Водночас, слід зазначити, що практика ЄСПЛ певний проміжок часу формувалася з огляду на потребу врахування значущості тяжкості злочину та суспільного інтересу в отриманні доступу до інформації про особу та про вчинений злочин при прийнятті рішення про можливість видалення такої інформації із інформаційних систем. У справах *V.V. v. France* [6] та *Gardel v. France* [7] постало питання, чи слід вважати порушенням ст. 8 Конвенції Ради Європи 1981 року Про захист осіб у зв'язку з автоматизованою обробкою персональних даних, включення у національну систему бази даних інформації про осіб які вчинили злочини сексуального характеру. Відповідно до обставин справ зберігання даних мало відбуватися впродовж 20–30 років залежно від тяжкості злочину. ЄСПЛ прийняв до уваги тяжкість злочинів та зацікавленість суспільства в існуванні таких баз даних та прийшов до висновку, про те, що у даних справах не відбулося порушення ст. 8, з огляду на існування процедури пред'явленн я вимоги про вилучення інформації із бази даних.

У справі *M.M. v. the United Kingdom* заявниця скаржилася на зберігання та розкриття попередження поліції про викрадення дитини, яке не біло вилучене із її матеріалів справи які зберігаються у поліції [8].

У справі *Dalea v. France* [9] заявник скаржився, що зберігання інформації про нього в інформаційній системі держав Шенгенської домовленості призвело до того, що йому не дозволялися поїздки в межах Шенгенської зони та відмовлялося у видачі відповідних віз, в особистих та професійних цілях. Його скарга була визнана неприйнятною за ст. 8 та ЄСПЛ зазначив, що заявник міг оскаржити пропорційність цих заходів у різних національних органах.

Слід зазначити, що з огляду на зростання потреби у транс-кордонному обміні даними, актуальність питань пов'язаних із зберіганням та обробкою даних у національних та європейських системах даних у практиці національних судів та ЄСПЛ, буде зростати. Так, відповідно до даних Європейського наглядового органу захисту інформації, за останні десять років також відмічається збільшення міжнародної активності поліції та судів у боротьбі з терористичною діяльністю та іншими формами міжнародної організованої злочинності, що забезпечується значними обміном інформацією з метою здійснення правоохоронної діяльності.

Крім того, з метою визнання 58 державами світу електронних версій українських документів вебпорталу «Дія» та надання можливості використовувати громадянами України електронного відображення інформації, що міститься у документах, передачі електронних копій відповідних документів, отримання публічних послуг за межами України за допомогою засобів Єдиного державного вебпорталу електронних послуг «Дія», іноземних суб'єктів відносин пов'язаних з персональними даними має бути підключено до інформаційних систем України [10].

Слід констатувати, що наразі концепція права суб'єкта заперечувати проти подальшої обробки його/її особистих даних та обов'язок контролера даних видаляти інформацію негайно після того, як вона перестає бути необхідною для цілей обробки стає дуже актуальною та набуває свого розвитку, водночас реалізація цього права відбувається з урахуванням дотримання потреб суспільних інтересів про, що свідчать практика ЄСПЛ останнього двадцяти років.

Поряд зі правом суб'єктів персональних даних заперечувати проти подальшої обробки персональних даних, пов'язано право на виправлення неточних персональних даних зібраних у електронних базах даних, передбачене у ст. 16 Регламенту ЄС 2016/679 та потреба

у закріпленні якого було зазначено, ще у Резолюції Ради Європи Про захист конфіденційності фізичних осіб по відношенню електронних баз даних у недержаному секторі від 26.09.1973.

Регламент ЄС 2016/679 наділяє суб'єктів даних правом вимагати від контролера, без невинуватих зволікань, виправити неточні персональні дані щодо нього. Правом на уточнення особа може скористатися у разі доповнення або виправлення неповної інформації у випадку профілювання, коли компанія складає профілі співробітників або користувачів за різними підставами (виробничість труда, маркетинг тощо). Тобто ситуація коли компанія здійснює профілювання, застосовує автоматизовану обробку персональних даних для прийняття рішень, аналізу або прогнозування особистих переваг, поведінки чи установок (згідно ст. п. 24 Преамбули Регламенту ЄС 2016/679).

Припускається, що особа яка піддається профілюванню може скористатися своїм правом на доступ до даних за ст. 15, щоб дізнатися які дані щодо неї були використані для складання профілю та зміст профілю, а у разі виявлення невідповідності оскаржити неточність профілю та коректність використання персональних даних. Відповідно до Керівництва із автоматизованого прийняття індивідуального рішення та профілювання право на виправлення наділяє суб'єкта можливістю виправити або внести зміни у неточності у профілюванні, у разі включення особи до категорії яка не відповідає її здібностям або категорію яка не відповідає стану здоров'я.

З урахуванням зазначеного, як нам уявляється, з урахуванням значущості суспільних інтересів та права на доступ до публічної інформації, подолати певні прогалини які можуть виникати під час реалізації права на видалення або «право на забуття», виникненні ситуації помилок та неточностей у профілюванні, суб'єкти можуть подолати шляхом реалізації права на виправлення неточних персональних даних зібраних у електронних базах даних.

Список використаних джерел:

1. Custers B.H.M. New digital rights: Imagining additional fundamental rights for the digital era. *Computer Law & Security Review*. № 44. 2022. P. 1–13.
2. Fazlioglu, M. Forget me not: the clash of the right to be forgotten and freedom of expression on the Internet, *International Data Privacy Law*. № 3. 2013. P. 149–157.
3. Calders T. & Custers B.H.M. What is data mining and how does it work? In: Custers B.H.M., Calders T., Schermer B., Zarsky T. (eds.) *Discrimination and Privacy in the Information Society*. 2013. Heidelberg: Springer.

4. Criminal Record-Based Employment Discrimination (CBED) URL: <https://dhr.ny.gov/protections-people-arrest-and-conviction-records>
5. Case *B.B. v. France* від 17 декабря 2009 г. Application no. 5335/06,
6. Case *Gardel v. France* від Application no. 16428/05, Постановление от 17 декабря 2009 г.
7. Case *M.M. v. the United Kingdom* від Application no. 24029/07, коммуніцирована 6 октября 2010 г.)
8. Case *Dalea v. France* від Application no. 964/07, Постановление от 2 февраля 2010г.)
9. Деякі питання передачі персональних даних за межі України засобами Єдиного державного вебпорталу електронних послуг Постанова Кабінету Міністрів України від 16 серпня 2022 р. № 910 URL: <https://www.kmu.gov.ua/npas/deiaki-pytannia-peredachi-personalny-a910>