DOI https://doi.org/10.30525/978-9934-26-331-6-32

ІНФОРМАЦІЙНА ПРИВАТНІСТЬ ЗА ЗАКОНОДАВСТВОМ ЄС: ВИКЛИКИ ТА ПЕРСПЕКТИВИ

Токарева В. О.

ВСТУП

У зв'язку із стрімким розвитком Інтернету, цифрових платформ, зростає цінність персональних даних які стали «новою нафтою», ресурсом для розвитку платформ автоматизованих систем та систем штучного інтелекту у суспільстві виникають побоювання через зростання обсягів збору, обробки персональних даних та загроз порушення приватність як провідного ризику інформаційного суспільства[1].

Поширюється застосування автоматизованих технологій, штучного інтелекту, відеоспостереження із дистанційним біометричним розпізнаванням або віддаленої біометричної ідентифікації особи актуалізує питання впливу технологій та приватне життя та встановлення правових гарантій захисту прав особи на недоторканність приватного життя, адже наразі, існуючі технології дозволяють створити диктатуру на зразок Дж. Орвелла та авторів інших антиутопій. Поширення використання даних систем державними органами обумовлюється метою забезпечення національної безпеки: запобігання, розкриття та розслідування злочинів, предикативної аналітики вчинення правопорушень, оплати громадського транспорту, державних послуг тощо. У діяльності комерційних організацій технологія (транспортних організацій, банків, супермаркетів, кафе), використовується для гарантування безпеки, полегшення доступу до фінансових продуктів і підвищуватимуть продажі.

Верховний комісар ООН за прав людини у звіті наголошує, що право людей на приватність зазнає дедалі більшого тиску через використання сучасних мережевих цифрових технологій, властивості яких роблять їх потужними інструментами для стеження, контролю та пригнічення[2]. Оскільки при сучасному рівні розробки автоматизованих технологій та

[1] Ken D. Kumayama A right to pseudonymity. Arizona Law Review. 2009. Vol. 51. P. 427–464.

[2] Report of the Office of the United Nations High Commissioner for Human Rights. The right to privacy in the digital age 4 August 2022 № A/HRC/51/17. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G22/442/29/PDF/G2244229.pdf?OpenElement

штучного інтелекту, призупинити неможливо, постає потреба розробки оптимальних шляхів правового регулювання застосування технології, яке засноване на стандартах та принципах прав людини.

1. Концепція інформаційної приватності в доктрині та законодавстві ЄС

Закріплення права на недоторканність приватного життя отримало своє поширення в конституціях держав континентальної правової системи, які були прийняті після Другої світової війни. Так, ФРН характеризується сталою традицією захисту недоторканності приватного життя та верховенства права. У 1983 р. Федеральний Конституційний суд ФРН ухвалив рішення, яким визнав, право на вільний розвиток особи та на інформаційне самовизначення за всіма фізичними особами (можливість встановлювати форм використання даних про особу)[3]. Внаслідок перепису населення в згідно із Законом «Про перепис 1983 року», провідною метою якого було зазначено отримання найбільш актуальної інформації про населення, яка мала б скласти базу для прийняття рішень федеральними, регіональними та муніципальними органами в області економічної та соціальної політики. Закон передбачав, що результати перепису можуть бути співставленні із даними інших державних баз для цілей правозастування. Саме дане положення викликало дискусії та призвело до чисельних звернень до Конституційного суду ФРН.

Спираючись на ст. 2.1 та ст. 1.1 Конституції ФРН Конституційний суд прийняв рішення про неконституційність зазначеного положень. Суд зазначив, що тогочасні, станом на 1983 рік, технології обробки даних дають змогу зберігати інформацію про громадян і легко отримувати до них доступ. У разі поєднання даних із різних баз виникає можливість створити профіль особи, не надаючи особі можливості перевірити правильність зазначеної в цьому профілі інформації або контролювати її використання. Така ситуація розширює можливості для маніпулювання особою, поведінка якої може змінюватися через психологічний вплив через побоювання, про розкриття публічного доступу до його персональних даних. Суд зазначив, що за відсутності у особи даних про те, хто та якими саме даними володіє про нього, особи можуть утримуватимуться від певної поведінки, побоюючись, про майбутніх ризики обмеження їх самовизначення. Таке самообмеження, на думку Конституційного суду ФРН, несумісне з положеннями ст. 2.1 і 1.1

[3] Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court] Dec. 15, 1983, 65 Entscheidungen des Bundesverfassungsgerichts [BVerfGE] 1 (F.R.G.). URL: http://www.servat.unibe.ch/dfr/bv065001.html

Конституції, що захищають право на гідність особи та може спричинити шкоду і суспільним інтересам, оскільки самовизначення є споконвічною передумовою для функціонування вільного демократичного суспільства, що ґрунтується на свободі дії та участі його учасників[4].

Зазначивши це протиріччя, суд вказав, що в контексті сучасних технологій обробки даних, вільний розвиток особи передбачає, захист осіб від необмеженого збору, зберігання, обробки та передачі їх персональних даних, що належить до фундаментальних прав, передбачених ст. 1.1, 2.1 Конституції. Дане фундаментальне право на захист осіб від необмеженого збору, зберігання, обробки та передачі їх персональних даних гарантує особам можливість самостійно ухвалювати рішення щодо розкриття та використання їх персональних даних. Обмеження права на інформаційне самовизначення особи допускається лише за умови існування істотних суспільних інтересів. Суд наголосив, що випадки обмеження цього права, повинні мати законодавчі закріпленні межі[5] .

Як зазначає Е. Фіалова визначення інформаційного самовизначення дана Судом є близьким до визначення приватності як права особи, груп чи організацій на власний розсуд визначати, коли та в якій мірі персональні данні про них передаються іншим особам[6].

Т. Хохімстра визначає право на інформаційне самовизначення як можливість особи в принципі визначати межі, в яких їх персональну інформацію використовують і поширюють, з метою досягнення життя, заснованого на самовизначенні[7].

А. Флюкігер зазначає, що право на самовизначення у сфері персональних даних є наріжним каменем захисту приватної сфери в цифрову епоху. Воно гарантує кожному право ухвалювати рішення щодо поширення та використання його персональних даних[8].

Право на інформаційне самовизначення відображене у ст. 8 Хартії ЄС про основні права від 07.12.2000 р., яка безпосередньо визнає право кожної людини на охорону даних які її стосуються, передбачає право

---

[4] Bennett C. Regulating Privacy: Data Protection and Public Policy in Europe and the United States. Ithaca, NY : Cornell University Press, 1992. P. 20.

[5] Там само.

[6] Fialová E. Data Portability and Informational Self-Determination. *Masaryk University Journal of Law and Technology.* 2014. № 1. Vol. 8. P. 47.

[7] Hooghiemstra T. Informational Self-Determination, Digital Health and New Features of Data Protection. *European Data Protection Law Review.* 2019. № 2. Vol. 5. P. 161–162.

[8] Flückiger A. L'autodétermination en matière de données personnelles: un droit (plus si) fondamental à l'ère digitale ou un nouveau droit de propriété? *Pratique juridique actuelle.* 2013. № 6. Vol. 22. P. 837.

вирішувати, кому, за яких обставини та які данні про себе розкривати, обізнаність про передання персональних даних та їх обробку (прозорість процедури обробки персональних даних), свободу вибору при передані персональних даних для обробки. Такі дані повинні використовуватися належним чином для певних цілей та на підставі згоди фізичної особи чи інших підстав, встановлених законом. Кожен має право на доступ до персональних даних та право несення виправлень в них через неточності[9].

Таким чином, право на інформаційне самовизначення в цілому розуміється як право особи визначати: хто, яким чином, згідно із якими цілями може обробляти персональні дані про фізичну особи та іншу персональну інформацію про особу. Право на самовизначення пронизане ідеєю конституційної заборони на втручання у приватне життя особи, насамперед у її інформаційному вимірі (яке формується за допомогою засобів цифрового зв'язку), без його згоди.

О.Б. Братасюк, Н.Ф. Ментух висувають позицію, що під правом на цифрове самовизначення розуміється не лише право на власний розсуд визначати інформацію про особу яку вона буде використовувати в системі, а й право на відключення від онлайну або право бути забутим в Інтернеті[10].

На думку Дж. Рейденберг такий підхід європейського законодавця, допомагає прояснити різницю у позиціях до правового регулювання недоторканності приватного життя та захисту персональних даних в ЄС та США[11].

Слід констатувати, що право на недоторканність приватного життя перетинається із правом на захист персональних даних, разом з цим у доктрині висуваються різні підходи до питання співвідношення недоторканності приватного життя та персональних даних.

Відповідно до Інструкції Європейського дорадчого органу із захисту персональних даних та приватності 4/2007 «Щодо концепції персональних даних»[12], правила захисту персональних даних виходять за межі широкого поняття права на повагу приватного та сімейного життя. Доцільно зазначити, що Хартія основних прав ЄС закріплює захист

[9] Хартії основних прав Європейського Союзу від 07.12.2000 р. URL: https://ips.ligazakon.net/document/MU00303

[10] Братасюк О.Б., Ментух Н.Ф. Поняття та класифікація цифрових прав в Україні. *Юридичний науковий електронний журнал.* 2021. № 10. С. 58–61.

[11] Joel R. Reidenberg Resolving Conflicting International Data Privacy Rules in Cyberspace. *Stanford* Law Review. 2000. № 52 (5). P. 1330–31.

[12] Opinion 4/2007 on the concept of personal data. European Advisory dody on data protection and privacy URL: http://ec.europa.eu/justice_home/fsj/privacy /index_en.htm

персональних даних в ст. 8 як автономне право поряд із правом на приватне життя, передбачене у статті 7. Це відповідає умовам статті 1.1, спрямованої на захист «основних прав і свобод фізичних осіб, зокрема, але не виключно, їх права на недоторканність приватного життя». Відповідно, у Регламенті та Директиві мітиться особливе посилання на обробку персональних даних за межами дому та сім'ї, як обробка передбачена трудовим законодавством, обробка рішень у судочинстві або прямий маркетинг. Означений підхід виходить з того, що захист персональних даних поширюється на різні сфери не лише приватного життя людини, з тим персональні дані є значно ширшою категорією та виходять за межі приватної життя.

Слід зазначити, що ЄСПЛ не вбачає доцільним розробку єдиного та вичерпного тлумачення поняття приватне життя. Завдяки практиці застосування ст. Європейської конвенції про захист прав та основних свобод людини (1950 р.)[13] поняття приватного життя набуло широкого тлумачення ЄСПЛ яке не є вичерпним, охоплює фізичну та психологічну цілісність людини і тому може передбачати заборону на будь-яке втручання в аспекти приватного та особистого життя, яке охоплює широке коло питань, як визнання батьківських прав, право на розлучення, право на домашні роди, ім'я або елементи, що належать до права людини на власний образ тощо[14].

Огляд на рішень ЄСПЛ дає розуміння категорії недоторканність приватного життя як досить широкої категорії, яка за містом виходить за межі особистого та сімейного життя[15]. Із означеного підходу випливає, що питання збору, обробки персональних даних та реалізація особою право доступу до них є елементом який охоплюються категорією недоторканність приватного життя.

Позиція з віднесення питань збору, обробки персональних даних та реалізації особою права на їх доступ як складової категорії приватного

[13] Європейська Конвенція з прав людини Рим, 4.XI.1950. URL: https://zakon.rada.gov.ua/laws/show/995_004#Text

[14] Case of Niemietz v. Germany (Application № 13710/88) 16 December 1992. *European Court of Human Rights.* URL: http://hudoc.echr.coe.int/eng?i=001-57887; Case of Axel Springer AG v. Germany (Application № 39954/08) 7 February 2012. *European Court of Human Rights.* URL: http://hudoc.echr.coe.int/eng?i=001-109034

[15] Кулініч О.О. Загальні положення про інформацію з обмеженим доступом в цивільному праві : монографія. Одеса : Видавництво «Букаєв Вадим Вікторович», 2008. 243 с.

Гуйван П.Д. Особливості цивільного захисту інформаційного приватного права особи. *Південноукраїнський правничий часопис.* 2019. № 3. С. 100–104.

життя переважає у роботах вітчизняних науковців Т.В. Бачинського, Р.І. Радейко, О.І. Харитонова[16], П.Д. Гуйвана[17].

Недоторканність персональних даних фізичної особи пов'язують із таким різновидом недоторканності приватного життя, як інформаційна приватність.

А. Бернард відносить до інформаційної складової приватного життя: будь-якого роду фактичні данні про події пов'язанні із тілом особи (обставини про хвороби фізичної особи, які складають медичну таємницю); відомості про терапевтичне або хірургічне лікування; відомості про смерть та долю людських останків; фактичні відомості, які торкаються сімейного життя (персональні даних за виключенням загальнодоступних даних цивільного стану, про факт народження, укладення шлюбу, смерті, таємниці всиновлення); відомості про факти особистих відносин поза сім'єю або розірвання відносин; відомості про внутрішні переконання особи (політичні або філософські погляди)[18].

Враховуючи викладене, визнаючи існування різноманітнх підлодів до розуміння інформаційної приватності ми солідаризуємося із позицією за якою інформаційна приватність розуміється як право особи контролювати обсяг, та зміст інформації, мету, способи пов'язаної зі збором, обробкою та використанням персональних даних, незалежно від того, які дані збираються про фізичну особу приватними та державними установами.

При розкритті права на інформаційну приватність, необхідно враховувати, що зміст суб'єктивного права будучи сукупністю можливостей (правомочностей) складає правомочність на власні дії, тобто можливість самостійно здійснювати юридично та фактично значущі дії; правомочність вимагати, тобто можливість вимагати від зобов'язаного суб'єкта виконання покладених на нього обов'язків; правомочність на захист тобто можливість використання чи можливість вимагати використання державно-примусових заходів у разі порушення суб'єктивного права.

Відповідно положень ст. 27 ЦК України зміст особистого немайнового права становить можливість фізичної особи вільно, на власний розсуд визначати свою поведінку у сфері свого приватного

[16] Основи ІТ-права:навч.посіб./ Т. В. Бачинський, Р. І. Радейко, О. І. Харитонова і інші. К. : Юрінком Інтер, 2017. 208 с.

[17] Гуйван П.Д. Недоторканність даних про особисте життя людини як елемент її права на приватність. *Часопис Київського університету права*. 2019. 4. С. 179–183.

[18] Bernard A. La protection de l'intimité par la droit privé: eloge du ragot ou comment vices exposes engendrent vertu. Les For Interieur. P. 153–179. URL: http://www.u-picardie.fr/labo/curapp/ revues/root/35/alain_bernard. pdf

життя. Одним з основоположних прав кожної людини є право отримувати, збирати, поширювати та використовувати інформацію. Кожна із зазначених вище правомочностей передбачає свої особливості регулювання, які встановлюються залежно від умов їхньої реалізації та спрямованості на задоволення потреб людини у використанні такого блага. Так, пошук інформації як процес визначається у теорії шляхом вчинення дій із звернення особи до певного органу, установи чи іншого суб'єкта за отриманням необхідної інформації. Одержанням особистих чи публічних відомостей вважається перехід до такого запитувача у володіння та утримання необхідних йому даних від персони, яка володіє ними, на законних підставах.

На наш погляд, при розкритті змісту права на інформаційну приватність слід враховувати положення ст. 8 Закону України «Про захисту персональних даних» та Регламенту ЄС 2016/679 (ст. 13, 14, 15, 16, 17, 18, 20, 21, 22), який передбачає низку прав якими наділено суб'єктів персональних даних та кореспондуючі ним обов'язки контролера або процесора, серед яких: право на інформацію про обробку персональних даних та право на доступ до персональних даних; право на уточнення даних; право на видалення даних або право бути забутим; право на обмеження обробки персональних даних; право на перенесення персональних даних; право не бути об'єктом автоматизованого прийняття рішення та право на захист від автоматизованого рішення яке має правові наслідки; право на заперечення проти обробки персональних даних; право знати механізм автоматизованої обробки персональних даних. Як нам уявляється, означені правомочності складають зміст права на інформаційну приватність, можна розглядати як самостійні права.

Відтак зміст права на інформаційну приватність можна визначити, як право особи контролювати обсяг та зміст інформації, пов'язаної зі збором, обробкою, поширенням та використанням персональних даних; правомочність вимагати від суб'єктів господарювання та органів державної влади виконання їх обов'язків щодо реалізації суб'єктом його правомочності доступу до персональних даних, правомочності на уточнення даних, правомочності на видалення даних, право на обмеження обробки персональних даних, правомочності право на перенесення персональних даних; правомочності не бути об'єктом автоматизованого прийняття рішення, правомочності право на заперечення проти обробки та обмеження обробки персональних даних, правомочність знати механізм автоматизованої обробки даних; право на захист у разі незаконного збору, обробки, зберігання персональних даних та вимагати застування державно-примусових заходів у разі порушення суб'єктивного права. Тож, кожний випадок реалізації права на

інформаційну приватність може бути розглянутий за трьома критеріями і трьома можливостями поведінки.

2. Дистанційна біометрична індентифікація та дотримання приватності в ЄС

Наразі, лідером використання технології відеоспостереження із дистанційним біометричним розпізнаванням є КНР, де системи відеоспостереження із функцією розпізнавання обличчя не лише активно застосовуються, а й експортується до різних держав світу[19]. Технологія передбачає привоєння особі рейтингу в соціальній системі та може відправляти необхідні данні правоохоронним органам про те, що особа має неоплачені штрафи, ухиляється від сплати аліментів або перебуває в розшуку[20]. Технологія дозволяє уряду КНР збирати великі обсяги даних про громадян.

Наразі, технологія відеоспостереження із дистанційним біометричним розпізнаванням допомагає правозахисним організаціям виявляти жертв работоргівлі, визначати їхнє місцезнаходження, заощаджуючи час фахівців, як, наприклад, компанія Marinus Analytics використовує програм у сервісі Amazon Rekognition[21].

У зв'язку із повномасштабною російською агресією, Україна отримала доступ до приватної бази даних розпізнавання обличчя – Clearview AI, яка містить майже десять мільярдів фотографій, що має надати можливість перевіряти фізичних осіб при перетині кордону[22]**.** Правоохоронні органи США використовували технологію Clearview AI для встановлення учасників масових заворушень під час протестів Black Lives Matter та штурму Капітолію у Вашингтоні[23]. Clearview AI, відома

[19] У Китаї камера розпізнала підозрюваного серед 60 тисяч людей 14 квітня 2018. URL: https://volynonline.com/u-kitayi-kamera-rozpiznala-pidozryuvanogo-sered-60-tisyach-lyudey/

[20] Сканування за ходою і формою тіла: у Китаї запускають систему тотального стеження 11 листопада 2018. URL: https://konkurent.ua/publication/32528/skanuvannya-za-hodou-i-formou-tila-u-kitai-zapuskaut-sistemu-totalnogo-stezhennya/

[21] Kaiser Larsen Marinus Analytics fights human trafficking using Amazon Rekognition09 AUG 2018 URL: https://aws.amazon.com/blogs/machine-learning/marinus-analytics-fights-human-trafficking-using-amazon-rekognition/

[22] 10 мільярдів фото і система розпізнавання: Україна отримала доступ до бази Clearview AI 14.03.2022 07:33 URL: https://www.ukrinform.ua/rubric-technology/3429032-10-milardiv-foto-i-sistema-rozpiznavanna-ukraina-otrimala-dostup-do-bazi-clearview-ai.html

[23] Года М. Clearview AI збирає базу фотографій всіх жителів планети: для чого це потрібно компанії. URL: https://24tv.ua/tech/clearview-ai-zbiraye-bazu-fotografiy-vsih-zhiteliv-novini-tehnologiy_n1870807

тим, що свої послуги надає державним органам та його представникам, а база фотографій зібрана із відкритих джерел в Інтернеті та соціальних мережах, зокрема громадян ЄС, порушує європейське законодавство, законний збір та обробку персональних даних про фізичних осіб.

Відтак, використання технології покликано нести позитивний вплив, разом з цим, на конференції під назвою «Орвеллівське передбачення: обговорення небезпек біометричного спостереження» проведеного Європейською Радою з питань захисту персональних даних зазначається, що шкода від застосування технологій розпізнавання обличчя може значно перевищувати потенційні переваги[24]. Адже не можна нехтувати впливом повсюдного відеоспостереження на добробут та психіку людей, та потребу дотримання вимог законодавства при захист персональних даних під час оброки. Поширення застосування технології ставить питання етико-правових засад її розповсюдження.

Слід зазначити, що використання систем відеоспостереження вимагає дотримання принципу законності та ставить питання щодо ефективності застосування таких систем, оскільки відеоспостереження не запобігло вчиненню терористичних актів у громадському транспорті у Лондоні[25], терористичних актів 2001 року в США. К. Веліз підтверджує, що використання систем відеоспостереження не ефективне в попередженні терористичних актів, оскільки є не закономірними вчинками, а умисними порушенням законодавства. До того, ж втручання у приватне життя яке справляє відеоспостереження також призводить до смерті людей[26].

Крім того, залишаються ризики пов'язані із можливістю вторинного використання даних зібраних системами відеоспостереження із дистанційним біометричним розпізнаванням з порушенням мети, для якої вони були отримані та зібрані. Тому використання технології відеоспостереження із біометричною ідентифікацією потребує суворої регламентації.

Тому, поряд із позитивним ефектом використання технології, наразі, відзначається тенденція у правовому регулювання на обмеження

[24] Trainees Conference Recording – An. An Orwellian Premonition: a discussion on the perils of biometric surveillance URL: https://edps.europa.eu/press-publications/press-news/videos/trainees-conference-recording-orwellian-premonition-discussion_en

[25] Токарева В.О. Страхування ризику тероризму. *Традиції та новації юридичної науки: минуле, сучасність, майбутнє* : матеріали Міжнародної науково-практичної конференції (м. Одеса, 19 травня 2017 р.) У 2-х т. Т. 2 / відп. ред. Г.О. Ульянова. Одеса: Видавничий дім «Гельветика», 2017. С. 530–533.

[26] The Power of BigTech and Ethics, Carissa Veliz. GRC World Forums1 April 2021. URL: https://www.grcworldforums.com/on-demand-content/the-power-of-bigtech-and-ethics-carissa-veliz/1185.article

повсюдного використання систем відеоспостереження із дистанційним біометричним розпізнаванням та розробка чітких правових засад використання технології. Навіть, в КНР поступово запроваджуються законодавчі обмеження використання технології. Згідно зі ст. 26 Закону КНР Про захист персональної інформації, що набрав чинності 1 листопада 2021 р., передбачено, що встановлення обладнання для збору зображень або розпізнавання обличчя у громадських місцях повинно здійснюватися у випадках, коли це вимагається засадами національної та громадської безпеки та згідно із законодавством про, що має бути чітко зазначено. Збір зображень та відмінних ідентифікаційних ознак може здійснюватися тільки з метою національної безпеки, та не може здійснюватися для іншої мети, за виключенням окремої згоди суб'єкта даних[27].

ЄКПЛ у ч. 2 ст. 8 наголошує, що органи державної влади не можуть порушувати недоторканність приватного життя, інакше як: на підставі закону; якщо це необхідно в демократичному суспільстві в інтересах національної безпеки, громадської безпеки та економічного добробуту держави, для запобігання або припинення злочину, захисту здоровє'я чи моралі або захисту прав і свобод інших осіб.

У ч. 1 ст. 52 Хартії фундаментальних прав ЄС міститься аналогічне формулювання, однак, його доповнює принцип пропорційності, під яким розуміється пропорційність між характером запроваджуваних обмежень та їхнім впливом на права суб'єктів, з одного боку, і важливістю та масштабом переслідуваних цілей, з іншого.

Європарламент у Резолюції від 6 жовтня 2021 р., визнає певний позитивний вплив від застосування систем віддаленої біометричної ідентифікації в області правозастосування, підвищення якості методів роботи правоохоронних та судових органів, ефективністю боротьби із злочинами у фінансовій сфері, відмиванню доходів отриманих злочинним шляхом, фінансуванню тероризму, насильницькими злочинами та експлуатацією дітей в Інтернеті, окремими видами кіберзлочинів, водночас може призвести до зростання числа випадків використання систем віддаленої ідентифікації для масового спостереження. Водночас застосування систем з метою масового спостереження буде невідповідним[28].

[27] Personal Information Protection Law of the People's Republic of China, PIPL URL: https://digichina.stanford.edu/news/translation-personal-information-protection-law-peoples-republic-china-effective-nov-1-2021

[28] European Parliament resolution of 6 October 2021 on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters (2020/2016(INI)) 6 October 2021UR: https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_EN.html

Законопроект ЄС про штучний інтелект від 18 червня 2021 р. відносить технології розпізнавання обличчя до категорії технологій із високим рівнем ризику для прав і свобод людини та встановлення загальної заборони на використання таких технологій, за виключенням чітко визначених випадків.

Відповідно до Висновку Європейської Ради із захисту персональних даних та Європейського наглядового органу із захисту персональних даних на Законопроект ЄС про штучний інтелект зазначено, що дистанційна біометрична ідентифікація осіб у загальнодоступних місцях несе високий ризики втручання у приватне життя осіб, а можливість бути визначеною або класифікованою програмо зачіпає людську гідність[29]. У Висновку зазначається, що використання систем штучного інтелекту може створити проблеми із дотриманням пропорційності, оскільки це може призвести до обробки даних невибіркової та невідповідної кількості суб'єктів даних для ідентифікації лише декількох осіб (наприклад, пасажирів в аеропортах та вокзалах). Безконтактний характер систем відеоспостереження із дистанційним біометричним розпізнаванням може створити проблеми прозорості та дотримання правових підстав для обробки даних відповідно до законодавства ЄС. До того ж постає питання щодо способу належного інформування фізичних осіб про відеоспостереження із застосуванням віддаленої біометричної ідентифікації та обробки, для ефективного здійснення прав фізичних осіб, а саме здійснення свободи вираження поглядів, зібрань, асоціацій, свободи пересування. Адже застосування подібних систем істотно впливає на дотримання засад (розумного) очікування населення на анонімність в громадських місцях та може негативно впливати на реалізацію прав та свобод людини.

Визнаючи, що Законопроекту ЄС про штучний інтелект містить значний перелік виключних випадків, коли віддалена біометрична ідентифікація в режимі реального часу в публічних місцях допускається для цілей правозастосування, проте Європейська Рада із захисту персональних даних та Європейського наглядового органу закликають запровадити загальну заборону на будь-яке використання ШІ для автоматичного розпізнавання людських рис у загальнодоступних місцях – як обличчя, хода, відбитки пальців, ДНК, голос, натискання клавіш та інших біометричних або поведінкових сигналів – у будь-якому контексті. Оскільки подібна практика як така не може відповідати вимогам

[29] EDPB-EDPS Joint Opinion 03/2021 on the Proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act) URL: https://edps.europa.eu/data-protection/our-work/publications/opinions/joint-opinion-edps-edps-proposal-regulation-european_en

необхідності та пропорційності, що в решті випливає з розуміння допустимого втручання у фундаментальні права, як це тлумачить Європейського суду Справедливості та ЄСПЛ. У Висновку пропонується встановити суворі випадки дозволеного використання коли технології.

Аналогічна позиція висловлена Європейським парламентом у Резолюції Про штучний інтелект у кримінальному провадженні та його використанні поліцією та судовими органами у кримінальних справах від 6 жовтня 2021 р. де зазначено, що підхід, прийнятий у деяких державах, не членах ЄС, до розробки, впровадження та використання технологій масового спостереження, непропорційно обмежує основні права, і тому має не застосовуватися в ЄС. У Резолюції також зазначено, що Європейський парламент закликає запровадити постійну заборону на використання автоматизованого аналізу та/або розпізнавання в публічно доступних місцях характеристик людини, таких як хода, відбитки пальців, ДНК, голос та інші біометричні та поведінкові сигнали.

За твердженням Європейського парламенту використання правоохоронними органами та спецслужбами приватних баз даних розпізнавання обличчя, таких як Clearview AI викликає занепокоєність, а факт використання технології Clearview AI та еквівалентних технологій має розкриватися правоохоронними органами. Європейський парламент загалом закликає заборонити використання приватних баз даних розпізнавання обличчя правоохоронними органами. Європарламент висловлює стурбованість з приводу проведення дослідницьких проектів таких, як iBorderCtrl. Європарламент також вважає необхідним та закликає Комісію запровадити заборону на будь-яку обробку біометричних даних, включно із зображеннями обличчя, у правоохоронних цілях, що призводить до масового спостереження в загальнодоступних місцях та закликає Комісію припинити подальше фінансування на проведення біометричних досліджень, що можуть призвести до невибіркового масового спостереження в громадських місцях.

ВИСНОВКИ

Слід зазначити, що остаточних законодавчих рішень в ЄС щодо застування відеоспостереження з дистанційним біометричним розпізнаванням обличчя не прийнято та проводяться лише окремі поодинокі законодавчі обмеження використання технології масового дистанційного розпізнавання людей у громадських місцях у законодавстві, проте не повної заборони законодавством.

Неможливо, прийняти рішення про відмову від використання біометричних технологій, включаючи системи розпізнавання осіб, через вірогідні порушення фундаментальних прав людини та невдоволення

суспільства. Таке рішення не зупинить розвитку технологій науково-технічного прогресу.

З огляду на потребу боротьби з терористичними діями, злочинністю та з урахуванням позиції Європейського парламенту, потребу створення відповідальних, антропоцентричних та заслуговуючих довіри систем штучного інтелекту застосування систем віддаленої біометричної ідентифікації має бути обмеженим та включати такі складові, як: заборона на використання систем розпізнавання приватним компаніями у громадських місцях; заборона на невибіркове розпізнавання осіб та обмеження лише особами, яких розшукують, встановлення підстав і процедури внесення людей до переліків розшукуваних; визначення місць розміщення засобів систем розпізнавання, інформування людей про спостереження і механізми реалізації та захисту своїх прав особами та заборона прихованого відеоспостереження; встановлення строків зберігання таких даних і механізмів їх захисту; Чітке визначення відповідальності, обмеження державних органів, які мають повноваження щодо використання систем розпізнавання.

АНОТАЦІЯ

Досліджені доктринальні та нормативні джерела ЄС в області приватності та застосування автоматизованих технологій відеоспостереження із дистанційним біометричним розпізнаванням обличчя. Застосування систем віддаленої біометричної ідентифікації справляє позитивний вплив в галузі правозастосовчої практики, підвищення якості діяльності судових та правоохоронних органів, ефективності боротьби із злочинами у фінансовій сфері, відмиванню доходів отриманих злочинним шляхом, фінансуванню тероризму, розкриттю насильницьких злочинів, експлуатацією дітей та інших видів кіберзлочинів. Встановлено, що використання таких технологій як Clearview AI приватними компаніями може порушувати законодавство про законний збір та обробку персональних даних, оскільки до суб'єкт даних не може бути належним чином поінформований про таку обробку. Крім того, залишаються ризики пов'язані із можливістю вторинного використання зібраних даних системами відеоспостереження з порушенням мети, для якої вони були отримані та зібрані.

Встановлено, що поряд із безспірними позитивним ефектом використання технології, наразі, відзначається тенденція у правовому регулюванні на обмеження повсюдного використання систем відеоспостереження із дистанційним біометричним розпізнаванням та розробка чітких правових засад використання технології. Обмеження застосування систем відеоспостереження із дистанційним біометричним розпізнаванням, збір та обробка зображень та відмінних

ідентифікаційних ознак виключно з метою національної та громадської безпеки, за виключенням окремої згоди суб'єкта даних запроваджено Законом КНР Про захист персональної інформації.

ЛІТЕРАТУРА

1. Ken D. Kumayama A right to pseudonymity. *Arizona Law Review.* 2009. Vol. 51. p. 427–464.
2. Report of the Office of the United Nations High Commissioner for Human Rights. The right to privacy in the digital age 4 August 2022 № A/HRC/51/17. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G22/442/29/PDF/G2244229.pdf?OpenElement
3. Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court] Dec. 15, 1983, 65 Entscheidungen des Bundesverfassungsgerichts [BVerfGE] 1 (F.R.G.). URL: http://www.servat.unibe.ch/dfr/bv065001.html.
4. Bennett C. Regulating Privacy: Data Protection and Public Policy in Europe and the United States. Ithaca, NY: Cornell University Press, 1992. P. 20.
5. Bernard A. La protection de l'intimité par la droit privé: eloge du ragot ou comment vices exposes engendrent vertu. Les For Interieur. P. 153–179. URL: http://www.u-picardie.fr/labo/curapp/ revues/root/35/alain_bernard. pdf
6. Fialová E. Data Portability and Informational Self-Determination. Masaryk University Journal of Law and Technology. 2014. Vol. 8. № 1. P. 47.
7. Hooghiemstra T. Informational Self-Determination, Digital Health and New Features of Data Protection. *European Data Protection Law Review.* 2019. № 2. Vol. 5. P. 161–162.
8. Flückiger A. L'autodétermination en matière de données personnelles: un droit (plus si) fondamental à l'ère digitale ou un nouveau droit de propriété? *Pratique juridique actuelle.* 2013. № 6. Vol. 22. P. 837.
9. Хартії основних прав Європейського Союзу від 07.12.2000 р. URL: https://ips.ligazakon.net/document/MU00303
10. Братасюк О. Б., Ментух Н. Ф. Поняття та класифікація цифрових прав в Україні. *Юридичний науковий електронний журнал.* 2021. № 10. С. 58–61.
11. Joel R. Reidenberg Resolving Conflicting International Data Privacy Rules in Cyberspace. *Stanford* Law Review. 2000. № 52 (5). P. 1330–31.
12. Opinion 4/2007 on the concept of personal data. European Advisory dody on data protection and privacy URL: http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm
13. Європейська Конвенція з прав людини Рим, 4.XI.1950. URL: https://zakon.rada.gov.ua/laws/show/995_004#Text

14. Case of Niemietz v. Germany (Application № 13710/88) 16 December 1992 / *European Court of Human Rights.* URL: http://hudoc.echr.coe.int/eng?i=001-57887

15. Case of Axel Springer AG v. Germany (Application № 39954/08) 7 February 2012 / *European Court of Human Rights.* URL: http://hudoc.echr.coe. int/eng?i=001-109034

16. Кулініч О.О. Загальні положення про інформацію з обмеженим доступом в цивільному праві: монографія. Одеса: Видавництво «Букаєв Вадим Вікторович», 2008. 243 с.

17. Гуйван П.Д. Особливості цивільного захисту інформаційного приватного права особи. *Південноукраїнський правничий часопис.* 2019. № 3. С. 100–104.

18. Основи ІТ-права:навч.посіб. / Т. В. Бачинський, Р. І. Радейко, О. І. Харитонова і інші. К. : Юрінком Інтер, 2017. – 208 с.

19. Гуйван П.Д. Недоторканність даних про особисте життя людини як елемент її права на приватність. *Часопис Київського університету права*. 2019. 4. С. 179–183.

20. У Китаї камера розпізнала підозрюваного серед 60 тисяч людей 14 Квітня 2018. URL: https://volynonline.com/u-kitayi-kamera-rozpiznala-pidozryuvanogo-sered-60-tisyach-lyudey/

21. Сканування за ходою і формою тіла: у Китаї запускають систему тотального стеження 11 листопада 2018. URL: https://konkurent.ua/publication/32528/skanuvannya-za-hodou-i-formou-tila-u-kitai-zapuskaut-sistemu-totalnogo-stezhennya/

22. Kaiser Larsen Marinus Analytics fights human trafficking using Amazon Rekognition09 AUG 2018 URL: https://aws.amazon.com/blogs/machine-learning/marinus-analytics-fights-human-trafficking-using-amazon-rekognition/

23. 10 мільярдів фото і система розпізнавання: Україна отримала доступ до бази Clearview AI 14.03.2022 07:33 URL: https://www.ukrinform.ua/rubric-technology/3429032-10-milardiv-foto-i-sistema-rozpiznavanna-ukraina-otrimala-dostup-do-bazi-clearview-ai.html

24. Года М. Clearview AI збирає базу фотографій всіх жителів планети: для чого це потрібно компанії. URL: https://24tv.ua/tech/clearview-ai-zbiraye-bazu-fotografiy-vsih-zhiteliv-novini-tehnologiy_n1870807

25. Trainees Conference Recording – An. An Orwellian Premonition: a discussion on the perils of biometric surveillance URL: https://edps.europa.eu/press-publications/press-news/videos/trainees-conference-recording-orwellian-premonition-discussion_en

26. Токарева В.О. Страхування ризику тероризму. *Традиції та новації юридичної науки: минуле, сучасність, майбутнє* : матеріали

Міжнародної науково-практичної конференції (м. Одеса, 19 травня 2017 р.) У 2-х т. Т. 2 / відп. ред. Г.О. Ульянова. Одеса : Видавничий дім «Гельветика», 2017. С. 530–533.

27. The Power of BigTech and Ethics, Carissa Veliz. GRC World Forums1 April 2021 URL: https://www.grcworldforums.com/on-demand-content/the-power-of-bigtech-and-ethics-carissa-veliz/1185.article

28. Personal Information Protection Law of the People's Republic of China, PIPL URL: https://digichina.stanford.edu/news/translation-personal-information-protection-law-peoples-republic-china-effective-nov-1-2021

29. European Parliament resolution of 6 October 2021 on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters (2020/2016(INI)) 6 October 2021. URL: https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_EN.html

30. EDPB-EDPS Joint Opinion 03/2021 on the Proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act) URL: https://edps.europa.eu/data-protection/our-work/publications/opinions/joint-opinion-edps-edps-proposal-regulation-european_en

Information about the author:
Tokareva Vira Oleksandrivna,
Ph.D. in Law, Associate Professor,
Lecturer at the Department of Civil Law
National University "Odesa Law Academy"
23, Fontanska doroha str., Odesa, 65009, Ukraine
https://orcid.org/0000-0002-8409-1477