DOI https://doi.org/10.30525/978-9934-26-284-5-24

АНОНІМНІСТЬ В МЕРЕЖІ ІНТЕРНЕТ

Токарева В. О.

ВСТУП

Одним із ключових постулатів на первісному етапі розвитку Інтернету та віртуальної реальності називалось, анонімне спілкування та вільне самовираження, яке припускало широкий обсяг права на недоторканність приватного життя у цифровому середовищі. Наразі, погляди на категорію «анонімність», в умовах обов'язкової ідентифікації користувачів в мережі Інтернет як учасників цивільного обігу істотним чином трансформується.

З одного боку, держави, в рамках своїх міжнародних зобов'язань щодо захисту прав і законних інтересів осіб, поступово посилюють контроль за діяльністю в Інтернеті, запроваджується обов'язкова ідентифікацією користувачів. З іншого боку, технологічні гіганти як Facebook, Microsoft, Google, Apple обмежують засади анонімності у правилах користування своїми сервісами, просувають політику єдиної автентичної ідентичності, реальних імень та зацікавлені в отриманні достовірної та якомога повної інформації про користувачів, у тому числі з метою індивідуалізації послуг і таргетованої реклами.

У науці висуваються різні позиції, щодо доречності визнання права на анонімність в якості окремого права людини (М. С. Саліков [1]) та переважна позиція про розгляд анонімності в якості елементу прав людини (права на свободу вираження поглядів; права на отримання інформації; права на недоторканність приватного життя; права брати учать в управління справами, обирати та бути обраним та права збиратися мирно, проводити, збори, мітинги, походи, та демонстрації; та у таких сфер, як комунікація, лікарська таємниці, заявлення про вчинене правопорушення, лікарську таємницю, тощо) (П. М. Сухорольський[2],

[1] Саликов М. С., Несмеянова С. Э., Колобаева Н. Е., Кузнецова С. С., Мочалов А. Н. Право на доступ в Интернет, анонимность и идентификация пользователей (конституционно-правовые проблемы) / под ред. М. С. Саликова – Екатеринбург: Издательство УМЦ УПИ, 2020. 167 с.

[2] Сухорольський П. М. Право на анонімність як суттєвий елемент прав людини. *Правова Інформатика*. 2003. № 1(37). С. 39–47.

В. А. Серьогін[3], Б. А. Ляпунов[4], П. Берналь[5]). З тим, сучасний етап розвитку Інтернету та поширення обов'язкової ідентифікації для участі у цивільних відносинах у мережі Інтернет актуалізує питання дотримання балансу приватних та публічних інтересів. Дослідження питань анонімність стає на часі оскільки в мережі Інтернет відбуваються неминучі зрушення у архітектурі комп'ютерних мереж в умовах пандемій та війн, коли особливо набуває значення дотримання прав людини та доступу до інформації, та зростання ризиків кіберзлочинності, зловживань, воєнних злочинів.

1. Трансформація уявлень про анонімність в мережі Інтернет

Ідея абсолютної анонімності в мережі Інтернет, наразі, ставиться під сумнів, у зв'язку переглядом архітектури комп'ютерних систем, змінами у ідеології існування множинності ідентичності, прагненням компаній запровадження єдиної автентичної ідентичності, визнанням більшістю науковців не можливості існування абсолютної ідентичності в мережі, та потребою ідентифікації суб'єктів цивільних відносин як у фізичному житті, так і у віртуальному просторі.

Уявлення про Інтернет як про простір безмежних можливостей, анонімного спілкування та вільного самовираження, яке припускає широкий обсяг права на приватне життя у цифровому середовищі, де під маскою анонімності може ховатися будь-яка особа, а особиста поведінка жодним чином не контролюється та не фіксується, будучи поширеними в останні роки XX ст. відходить у минуле.

На перших етапах розвитку Інтернет заповнювався контентом, створеним науковцями, інженерами, які дотримувалися принципу свободи інформації, Інтернет розглядався як суспільний електронний ресурс, простір безмежних можливостей для самоідентифікації та справжньої приватності, наразі, характеризується певною мірою девальвацією анонімності та конфіденційності. Інтернет будучи створений для задоволення потреб та інтересів оборонного сектору, характеризувався анонімністю, відсутністю правового регулювання, в подальшому став суспільним явищем, доступним для всього суспільства.

На даному етапі користувачі були наділені правом вільного вибору та зміни масок, зміни ідентичності, псевдонімів під якими вони себе презентували, що створювало ілюзію анонімності в мережі. Вважалося,

[3] Серьогін В. А. Право на анонімність як елемент прайвесі. *Науковий вісник Ужгородського національного університету.* 2014. № 24. С. 154–159.

[4] Ляпунов Б. А. Приватность личности: понятие, сущность и правовая природа. Актуальные проблемы российского права. 2019. № 2. С. 33–42.

[5] Bernal P. Internet Privacy Rights: Rights to Protect Autonomy. N. Y. : Cambridge University Press, 2014. 311.

що користувач має право на власний розсуд вирішувати, чи розкривати йому його справжнє ім'я чи ні. Так, у 90 роки популярним був афоризм, щодо карикатури у журналі «Нью-Йоркер» зображення двох собак, сидячих напроти моніторів, де одна одній говорить, що: «В Інтернеті ніхто не знає, що ви собака»[6]. Зображення майже забулося. Цей підпис до зображення став поширеним, як відображення раннього уявлення про Інтернет як середовище яке гарантує повну анонімність та приватність користувачів та збереження таємниці про їх вчинки.

Винайдення Інтернету описувалося в перші роки прибічниками ліберального підходу до правого регулювання мережі, як глобальний простір в якому обмін думками та поглядами відбувається вільно, незалежно від державних кордонів та анонімно. Один із розробників ідей «вільного Інтернету» Дж. П. Барлоу у «Декларації незалежного кіберпростору» представленій на Давоському формі у лютому 1996 року, стверджував, що традиційне для правової реальності категорія «особа» не можна застосовуватися стосовно Інтернету оскільки: «Наш світ одночасно будь-де та ніде, але не там де живуть наші тіла… Наші індивідуальності не мають тіл, тому мм не можемо досягти порядку за допомогою фізичного примушення »[7] .

Професором права Колумбійського університеті У Сюмін (吳修銘, англ. Tim Wu), був сформульований принцип мережевого нейтралітету[8] для захисту світового високотехнологічного інформаційного простору від будь-яких заборон і спроб примусового регулювання з боку провайдерів, державних відомств; захисту контенту, сайтів, свободи вибору доменних імен, свободу доступу до Інтернету та користування ним вільно від свавілля чиновників і корпорацій[9].

Визнаючи значимість мережевого нейтралітету, притаманного Інтернету від початку та привабливість ідеї анонімності для користувачів [10], необхідно визнати зміни які відбулися з того часу, еволюцію суспільства та інформаційно-комунікаційних технологій. Анонімність, будучи властивістю раннього Інтернету, сприяла можливості

[6] Sarda T., Natale S., Sotirakopoulos N., Monaghan M. Understanding Online Anonymity. Media Cult Soc. 2019. №. 4. P. 557–564.

[7] A Declaration of the Independence of Cyberspace. URL: https://www.eff.org/cyberspace-independence

[8] Network Neutrality FAQ.URL: http://timwu.org/network_neutral- ity.html

[9] Близнец И. А. Авторское право и смежные права : учебник / И. А. Близнец, К. Б. Леонтьев ; под ред. И. А. Близнеца. Москва : Проспект, 2010. 416 с.

[10] Birch D. Putting "identity" on the "blockchain". Part 2: Create an identity model. 2016. CHYP USA, Consalt Hyperion company. URL: http://www.chyp.com/putting-identity-on-the-blockchain

некоректної поведінки в онлайн просторі [11]. Наразі в Інтернеті відбуваються тисячі правопорушень, які не відрізняються від вчинюваних офлайн.

У літературі констатується, що концепція анонімності в мережі виявилася рухливою. Якщо на початку існування мережі анонімність користувачів вважалася однією із ключових ознак Інтернету[12], а протокол не передбачав передання даних про користувачів до кінцевого обладнання, то, сучасний Інтернет характеризується протоколом відкритого, а не конфіденційного спілкування, де анонімність переважно вже ілюзія.

Сучасне ставлення до анонімності трансформується, що обумовлене вимогами ідентифікації та автентифікації, зміною у масштабів персональних даних які збираються та обробляються платформами та сайтами. Сучасні тенденції розвитку ідентичності зводяться до презентації автентичної особи в цифровому просторі [13]. Наразі, для участі у цивільних відносинах та реалізації прав та обов'язків учасниками як у фізичному так і віртуальному світі особам необхідно проходження процедуру автентифікації та ідентифікації

Мочалов А. Н. називає наступні чинники, які трансформували значення анонімності як цінності в Інтернеті. По-перше, можливість вчиняти будь-які дії від імені вигаданої особи призвела до зловживань анонімністю для вчинення злочинних дій, шахрайства, Інтернет торгівлі забороненими речовинами в мережі. Для недопущення правопорушень та встановлення порушників державами були прийняті заходи для правового регулювання діяльності в мережі які передбачали вимогу розкриття автентичної ідентичності під час вступу в юридично значущі відносини. Тому слід поставити під сумнів твердження, що анонімність віртуальної ідентичності, із наділенням відповідними повноваженнями, надає можливість вчиняти практично всі повсякденні операції онлайн, що стимулює, заохочує до вчинення правочинів які б не були б вчинені в іншому випадку[14].

---

[11] Rainie L., Anderson J., Albright J. The Future of Free Speech, Trolls, Anonymity, and Fake News Online. *Pew Research Center*. 2017. 82 p.

[12] Царева А. В. Человек в сети: смена веб-поколений. *Журнал социологии и социальной антропологии.* 2012. № 5 (64). С. 46.

[13] Супрун Г. Г. Ідентичність індивіда в цифрову епоху соціальних комунікацій. *Філософські обрії.* 2020. № 43. С. 85–94; Токарева В. О. Трансформація віртуальної ідентичності: від множинності до єдиної автентичності в мережі Інтернет. *Актуальні проблеми вітчизняної юриспруденції*. 2022. № 3. С. 47–52.

[14] Составляющие цифровой трансформации : монография / Г. С. Сологубова. Москва : Издательство Юрайт, 2019. 147 с.

По-друге, наразі, істотно зросла цінність персональних даних в Інтернеті, як агрегованої інформації у форматі «великих даних» та і персональних даних які стосуються кожної окремої особи. Ці данні дозволяють на підставі аналізу дій користувачів провадити їх профілювання, передбачати їх вірогідні майбутні вчинки та поведінку, направляти, а з тим і маніпулювати, та індивідуалізувати рекламу для підвищення її ефективності. На початковому етапі Інтернету, означені можливості застосування великих даних не були вивчені, то зі спливом часу значення цих даних для економіки стало безперервно зростати та залежати від результатів їх збору, обробки та транскордонної передачі. Вагомий вплив справив розвиток соціальних мереж, де користувачі за власною волею та добровільно розкривають свої персональні дані, інформацію про себе, навіть конфіденційну[15]. Прикладом свідчення невпинно зростаючої цінності персональних даних стали реалізовані проєкти Cambridge Analytica: виборчі перегони на різних континентах, серед яких виборча компанія президента США 2016 року та вихід Великобританії із членства в ЄС.

З огляду на гучні скандали із витоком та маніпулюванням персональними даними, за твердженням вчених, провідною метою регулювання діяльності органів державної влади має стати забезпечення належного захисту персональних даних, які надаються під час реєстрації на сайтах для отримання послуг в мережі, а не спроби введення права на анонімність до абсолюту. А будь-яке примусове надання персональних даних має базуватися на вимогах законодавства або рішенні суду, яке оцінює у конкретному випадку правомірність та пропорційність прийнятого рішення [16].

2. Правове регулювання анонімності в мережі Інтернет

Наразі, правове регулювання права на анонімність в Інтернеті базується переважно на застосуванні правових засобів які направленні на її обмеження, а не встановлення гарантій її реалізації[17].

Наразі, у сучасних умовах розвитку інформаційного суспільства не витримують аргументи прибічників, ідеї вільного поширення інформації в мережі, що під час правового регулювання мають прийматися до уваги

[15] Щербович А. А. Реализация конституционных прав и свобод в Интернете. М. : Теис, 2015. 148 с.

[16] Мылтыкбаев М. Ж. Право на анонимность в сети Интернет: вопросы международно-правовой защиты. *Юридическая наука*., № 4, 2019, С. 42-45.

[17] Кузнецова С. С. Право на анонимность в сети Интернет: актуальные вопросы реализации и защиты. *Российское право: образование, практика, наука*. 2020. №. 5. С. 33–41.

унікальні властивості Інтернет, адже таких очевидних підстав, щоб розглядати Інтернет як особливий правовий простір – не має[18].

Поступово держави розширюють повноваження органів влади щодо контролю за діяльністю користувачів. Законодавчі ініціативи, обумовлені устремлінням держав забезпечити безпеку та протидіяти кіберзлочинності, міжнародному тероризму, відмиванню доходів отриманих злочинним шляхом все більше наділяють правоохоронні та судові органи повноваженнями для доступу до персональних даних користувачів Інтернет, а з тим обмежують їх анонімність.

Задля чого вводяться законодавчі норми які передбачають обов'язок провайдерів надавати інформацію про користувачів за запитом правоохоронних органів, як у Великобританії або В'єтнамі та за запитом судів у Канаді США та Франції. В КНР та Ірані запроваджено вимогу ідентифікації всіх користувачів відповідно до реальних імен. У Південній Кореї діє вимога про обов'язкової ідентифікацію користувачів на сайтах «для дорослих» з метою підтвердження віку та для користування деякими послугами. Хочу 2007 році була невдала спроб запровадити обов'язкова ідентифікацію для всіх користувачів Інтернету, яка була спростована Верховним Судом через несумісність із Конституцією[19].

В Бразилії запроваджено заборону на анонімні висловлювання на рівні Конституції. Анонімність тлумачитися як засіб зловживання вираженням поглядів, а тому метою заборони анонімності є забезпечення покладення на автора публікації юридичних наслідків, викликаних образливою поведінкою (статья 5). Заборона анонімності в Конституції визнається необхідною гарантією захисту недоторканності особистого життя та гідності особи.

У Венесуелі діє заборона анонімності на конституційному рівні. У В'єтнамі з 2013 року діє Закон який забороняє використання псевдонімів. У Еквадорі законодавство передбачає обов'язкову реєстрацію авторів коментарів на сайтах під власними ім'ям.

Для застосування юридичної відповідальності, держави члени ЄС приймають як заходи передбачені національним законодавством та міжнародними актами, так і на рівні ЄС, серед яких Директива 2000/31 ЄС «Про деякі правові аспекти інформаційних послуг, зокрема, електронної комерції, на внутрішньому ринку», прийнята Європейським парламентом та Радою від 8.06.2000 (Далі Директива 2000/31/ЄС «Про

[18] Мироненко Т. В., Куропацкая Е. Г. Проблематика защиты авторских прав в электронной среде: опыт Японии, КНР и России. *Евразийская адвокатура*. 2018. №. 5 (36). С. 84–88.

[19] Михайлов С. В. Анонимность в Интернете. *Журнал Суда по интеллектуальным правам.* 2017. № 17. С. 26–32.

електронну комерцію») яка передбачає обов'язок провайдера надавати компетентним органами доступ до персональних даних користувача, який припускається є суб'єктом незаконної діяльності [20].

ЄСПЛ під час розгляду справ в означеній сфері базується на тлумаченні ст. 10 Конвенції з прав людини та основоположних свобод 1950 року та Конвенції Ради Європи про захист фізичних осіб під час автоматизованої обробки персональних даних 1981 року, яка передбачає принцип невтручання в особисте життя, що передбачено які закріплюють право особи на захист персональних даних та вільне вираження поглядів.

Вагомий вплив на формування практик в даній сфері справило рішення ЕСПЛ Delfi AS v. Estonia. ЄСПЛ відзначив важливість онлайн анонімності для вільного вираження ідей та поглядів, та особливість Інтернеті яка безпрецедентного засобу поширення інформації та дав характеристику ступеням анонімності в мережі Інтернет. Суб'єкт може залишатися анонімним для широкого загалу, але при цьому ідентифікуватися постачальником послуг за допомогою облікового запису, реєстрації або контактних даних, які можуть не перевірятися або підлягати перевірці шляхом повного обмеження верифікації (шляхом активації облікового запису за допомогою адреси електронної пошти або облікового запису соціальної мережі) так і повної автентифікації, використанням національних електронних посвідчень або за допомогою онлайн банкінгу. Поряд з цим постачальник послуг може допускати повну анонімність суб'єктів коли користувач не зобов'язаний ідентифікувати себе загалом та його поведінка може відстежуватися певною мірою через дані які зберігаються провайдером доступу до Інтернету. Означенні персональні данні можуть бути розкритті за умови належного припису уповноважених органів – слідчих або судового органу, а право на анонімність у такому разі може обмежена, коли потребує виявлення та переслідування винних осіб[21].

У справі Delfi AS v. Estonia, суд відхилив посилання заявника на ст. 10 («Свобода вираження переконань») Конвенції з прав людини та основоположних свобод 1950 року. Дане рішення ЄСПЛ було піддано критиці міжнародними правозахисними організаціями, які припустили, що подібні прецеденти можуть привести до прийняття в ЄС законів як

[20] Директива 2000/31 ЄС «Про деякі правові аспекти інформаційних послуг, зокрема, електронної комерції, на внутрішньому ринку». URL: https://zakon.rada.gov.ua/laws/show/994_224#Text

[21] European Court of Human Rights. Case of Delfi AS v. Estonia (Application no. 64569/09). Judgment. Strasbourg. 10 October 2013. URL: http://www.statewatch.org/news/2013/oct/echr-judgment-delfi-AS-v-estonia.pdf

будуть зобов'язувати користувачів реєструватися в Інтернеті під реальними іменами [22].

Означена позиція була покладена в основу наступних рішень ЄСПЛ щодо питань анонімності в Інтернеті та можливості її обмеження. Зокрема, у рішенні ЕСПЛ по справі Benedik v. Slovenia от 24.04.2018 про поширення дитячої порнографії в анонімній мережі, суд визнав право органів поліції на підставі рішення суду отримати доступ до даних IP-адрес користувачів, які використовуються для доступу до Інтернету[23].

Так, Австрійський уряд розробляє законодавством яке зобов'язує проходити обов'язкову ідентифікацію реальних імен користувачів за номером мобільного телефону, який прив'язаний до персональних даних абонентів та позбавить права залишати анонімні коментарі на сайтах. Даний захід покликаний більш ефективно боротися із вираженням нетерпимості. Закон має поширюватися на всі платформи на яких зареєстровано понад 100 тис. осіб на або які мають щорічний обіг понад €500 тис., та платформи які отримають бюджетні гроші на розвиток ЗМІ у понад €50 тис. Таким чином, Закон торкнеться великих газет, сайти новин та Facebook и Twitter. Провайдерів пропонується зобов'язати зберігати дані користувачів та на надавати на запит правоохоронних органів. У разі порушення законодавства провайдери будуть зобов'язані сплатити штраф €500 тис.[24].

Водночас п. 2. ст. 17 Міжнародного Пакта про цивільні та політичні права, покладає обов'язок на уряди держав забезпечувати захист приватного життя від незаконного та свавільного втручання, та посягань, виправдане спробами держав та міжнародних органів та організацій встановити суворе правове регулювання, запровадити порядок для отримання доступу до персональних даних суб'єктів та не допустити неконтрольований збір та обробку персональних даних технологічними компаніями – провайдерами Інтернет послуг.

---

[22] Access intervenes at ECtHR for the right to be anonymous online. URL: https:// www.accessnow.org/access-intervenes-at-ecthr-for-the- right-to-be-anonymous -online; Article 19. Right to Online Anonymity. Policy Brief. June 2015. URL: https:. www.article19.org/data/ files / medialibrary /38006/Anonymity_and_encryption_report_A5_final-web.pdf

[23] European Court of Human Rights. Case of Benedik v. Slovenia (Application no. 62357/14). Judgment. Strasbourg. 24 April 2018. URL: http://www.dirittoegiustizia.it/allegati/ PP_INTERN_18Cedu Privacy_milizia_s.pdf

[24] In Austria in 2020, anonymity on the Internet will be banned. URL: https://tass.ru/ obschestvo/6335723

Козаченко О. В Австрії мають намір заборонити анонімність користувачів великих інтернет-сайтів. Штраф для компаній сягатиме €500 тисяч. URL: https://babel.ua/news/ 29190-v-avstriji-rozglyadayut-zakonoproekt-yakiy-zaboronyaye-zalishati-anonimni-komentari-v-interneti

Зразковими є рішення від 13.06.2014 Верховного суду Канади у справі R. vs. Spencer де, суд зазначив, що визначення ступеня анонімності є властивістю більшості діяльності в мережі Інтернет та залежно від обставин може бути покладена в основу інтересів людини в збереженні приватності, яка припускає конституційний захист від безпідставного спостереження. З огляд на означене, Суд прийшов до висновку, що надання доступу до даних користувачів на запит поліції протирічить положенням Конституції[25]. Адже розкриття подібних даних має відбуватися виключно на підставі судового рішення. Означеними діями держави прагнуть убезпечити права користувачів та протистояти корпораціям у їх намаганнях обмежити анонімність у правилах користування своїми сервісами, запровадження політики реальних імен та єдиної автентичної ідентичності.

З метою боротьби з кіберзлочинністю Проєктом Закону Внесеного до Верховної Ради Про внесення змін до Кримінального процесуального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю та використання електронних доказів 4004 від 01.09.2020 пропонується вдосконалити державно-приватну взаємодію правоохоронців та провайдерів під час проведення оперативно-розшукових заходів, негласних слідчих (розшукових) дій та тимчасового доступу до інформації, речей і документів[26].

Проєктом Закону № 4003[27] пропонується надання доступу співробітниками правоохоронних органів до інформації, що зберігається в електронних інформаційних системах (наприклад, до інформації в смартфоні або персональному комп'ютері), на які не поширюється дозвіл на проведення обшуку, якщо слідчий або прокурор вирішить, що є достатні підстави вважати, що інформація, яка в них міститься, має значення для встановлення обставин у кримінальному провадженні. З огляду на досвід іноземних держав надання постачальниками телекомунікаційних послуг доступу до персональних даних споживачів має відбуватися лише за відповідним рішенням суду.

[25] R. v. Spencer, 2007 1 S. C.R. 500, 2007 SCC 11 SUPREME COURT OF CANADA. URL: https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/2347/index.do

[26] Проєкт Закону Верховної Ради Про внесення змін до Кримінального процесуального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю та використання електронних доказів від 01.09.2020 № 4004. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=69771

[27] Проєкт Закону про внесення змін до Кримінального процесуального кодексу України та Кодексу України про адміністративні правопорушення щодо підвищення ефективності протидії кібератакам від 01.09.2020 № 4003. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=69770

Слід зазначити, що з кожним роком приймаються все більше заходів направлених на прозорість діяльності в мережі, які трансформують уявлення про межі анонімності та приватності. Так, в межах заходів боротьби із поширенням Covid-19 оператори зв'язку зобов'язалися передавати Європейській Комісії данні про геолокацію з мобільних пристроїв своїх абонентів у березні 2020 року. Європейський комісар із захисту персональних даних виявив занепокоєння що передача телекомунікаційними компаніями даних про геолокацію може стати звичною практикою[28].

Так, у травні 2022 року у ФРН було прийнято законодавство для запровадження систем ШІ для розпізнавання віку особи за обличчям для авторизації у соціальних мережах для обмеження впливу контенту на неповнолітніх[29]. Цей захід є істотними кроком для на шляху технічного захисту молоді та вимагає суворе дотримання законодавства при збір та обробці біометричних даних неповнолітніх осіб.

Висувається ідея, що реалізація права на анонімність шляхом приховування персональних даних особи в мережі Інтернет може здійснюватися за допомогою засобів псевдонімізації, шляхом використання додатків та сайтів без реєстрації, обранням псевдоніму при формуванні цифрової ідентичності, поширення в соціальних мережах вигаданої інформації про особу, або використанням технічних засобів шифрування з метою приховування персональних даних (коли провайдер не може встановити точне джерело з'єднання (зокрема, IP-адресу) [30] . анонімного пошуку даних, відвідування веб-сторінок, анонімного поширення інформації або пересилання сповіщень, анонімного створення та оприлюднення творів, тощо[31] .

В умовах потужного розвитку інформаційно-комунікаційних технологій значена теза стає все більш сумнівною. Поряд із правовим регулюванням доступу уповноважених осіб до персональних даних користувачів, законодавство доповнюється нормами щодо забезпечення технічної ідентифікації осіб в Інтернеті, доступу уповноважених органів

[28] Операторы связи будут передавать ЕК геолокационные данные в рамках борьбы с COVID-19. URL: https://www.securitylab.ru/news/506200.php

[29] Kabelka L. German youth protection body endorses AI as biometric age-verification tool. 31.05.2022. URL: https://www.euractiv.com/section/digital/news/german-youth-protection-body-endorses-ai-as-biometric-age-verification-tool/

[30] Саликов М. С., Несмеянова С. Э., Колобаева Н. Е., Кузнецова С. С., Мочалов А. Н. Право на доступ в Интернет, анонимность и идентификация пользователей (конституционно-правовые проблемы) / Под ред. М. С. Саликова. Екатеринбург : Издательство УМЦ УПИ, 2020. 167 с.

[31] Мочалов А. Н. Парадокс Анонимности в Интернете и проблемы ее правового регулирования. *Вестник Сургутского государственного университета.* 2021. № 4 (34). С. 111–121.

до засобів крипто захисту та інших подібних сервісів. В деяких державах впроваджується обов'язкова ідентифікація власників СІМ карток, ідентифікація осіб при використанні суспільних точок онлайн-доступу, зокрема в метро, кафе, ресторані. В КНР, Ірані, Казахстані, Ефіопії та деяких інших державах забороняється та переслідується використання сервісів які дозволяють анонімізувати особу, приховати її реальну IP адресу, наприклад Tor, VPN та тощо.

Слід відмежовувати право на захист персональних даних від доступу третіх осіб та право на вільне поширення інформації від технічної можливості ідентифікувати особу яка поширює інформацію в мережі Інтернет [32] .

Так, характерною властивістю Інтернету є те, що навіть приховуючись під вигаданими ідентифікаційними даними, користувач залишає після кожної дії в Інтернеті «цифрові сліди» (пошукові запити, відвідування сторінок) які аналогічно залишеним у фізичному світ можуть сприяти ідентифікації реальної особи яка стоїть за цифровою ідентичністю. Зокрема, сприяти ідентифікації особи можуть цифрові сліди у поєднання технічних даними (дані про девайс, оператора зв'язку, динамічна або статична IP-адреса, місцезнаходження пристрою, тощо) та індивідуальними даними про властивості взаємодії користувача із пристроями, які збираються більшістю провайдерів (швидкість нажаття клавіатури та миші, куту нахилу телефону, час та тривалість перебування у мережі тощо). У зв'язку з тим, що переконання, думки особи, які традиційно розглядалися правниками як частина внутрішнього світу людини, який не підлягає контролю зовні, в Інтернеті опиняються під суспільним наглядом, оскільки пошукові запити, «лайки» у соціальних мережах, переглянуті відео та інші сліди, ладні розповісти про це. Не сприяє реалізації права на анонімність використання більшістю соціальних мереж, алгоритмів розпізнавання обличчя. Означене ситуація, ставить питання реалізації не лише права на недоторканність приватного життя, а й права особи діяти відповідно до власних переконань. Наступним постає ситуація, що такі технологічні гіганти як Facebook, Microsoft, Google, Apple, а не державні установи визначають вектор політики та правил розкриття персональних даних користувачами про себе[33]. В умовах росту збору та обробки персональних даних, прийняття Регламенту ЄС 2016/679 спрямовано на забезпечення балансу приватних інтересів та публічних.

[32] Митник К. Искусство быть невидимым: как сохранить приватность в эпоху Big Data (пер. с англ.). М. : Эксмо, 2021. 464 с.

[33] Rossi A. Internet Privacy: Who Sets the Global Standard? *The International Spectator*. 2014. №. 1. P. 65–80.

На відміну від фізичних слідів, цифрові слід не зникають зі спливом часу, а залишаються доступними для потенційних учасників Інтернету, таких як уряд, компанії та шахраї. Наприклад, фотографія, розміщена на псевдонімізованій сторінці в соціальній мережі, – навіть якщо на ній не зображені конкретні особи – може містити метадані про пристрій, за допомогою якого було зроблено кадр (у тому числі про серійний номер виробу), про місце та час, коли була зроблена фотографія [34].

За наявності достатніх технічних засобів, за номером виробу та геолокації, можливо визначити абонентський номер та оператора зв'язку, а з тим ідентифікувати володільці не складно. За твердженням фахівців, із застосуванням метаданих фотознімку (дозволяють встановити пристрій та подекуди автоматично визначають геолокацію) розміщеної у Twitter у 2012 році правоохоронними органами США, Беліза та Гватемали було встановлено місцезнаходження розробника першої антивірусної програми Дж. Макафи, який перебував у розшуку по підозрі у вбивстві сусіда. Встановити місцезнаходження можливо завдяки додатку. У 2015 році було встановлено місцезнаходження наркобарона, на ім'я Ель Чапо, завдяки фотознімкам його сина, попри прикрите смайліками зображення обличчя, залишалася видима комплекція батько [35]. Згідно дослідження О. Аквісті з Університету Карнегі Меллон США проведеного 2011 році, володіючи випадковим фото особи, можна встановити номер соціального страхування особи зображеної на фотознімку [36].

ВИСНОВОК

З огляду на тенденцію запровадження єдиної автентичної ідентичності в мережі, боротьби з фейковими шахрайськими аккаунтами, можна розглядати лише відносну анонімність, для широкого загалу користувачів, адже через властивості інформаційних систем, постачальники телекомунікаційних послуг отримують доступ до персональних даних користувачів, які можуть бути передані уповноваженим органам для подальшої ідентифікації осіб які вчинили правопорушення. Користувачі

[34] Мочалов А. Н. Парадокс Анонимности в Интернете и проблемы ее правового регулирования. *Вестник Сургутского государственного университета.* 2021. № 4 (34). С. 111–121.

[35] Митник К. Искусство быть невидимым: как сохранить приватность в эпоху Big Data (пер. с англ.). М. : Эксмо, 2021. 464 с.; P. Roberts 2011. How Facebook and Facial Recognition Are Creating a Minority Report-Style Privacy Meltdown. URL: https://threatpost.com/how-facebook-and-facial-recognition-are-creating-minority-report-style-privacy-meltdown-080511/75514/

[36] Face recognition software, social media sites increase privacy risks, says new carnegie mellon study. URL: https://www.prnewswire.com/news-releases/face-recognition-software-social-media-sites-increase-privacy-risks-says-new-carnegie-mellon-study-126510323.html

кожного разу користуючись Інтернетом, реєструючись на сайтах розкривають персональні данні в обмін на номінальну винагороду, підвищену персоналізацію товарів та послуг.

Як свідчить практика ЄСПЛ та іноземний досвід впровадження обов'язкової ідентифікації, значна кількість цивільних відносин які у фізичному світі для їх реалізації вимагають ідентифікації, наразі, перейшли в Інтернет де вимагається дотримання законодавства, щодо належної ідентифікації учасників цивільних відносин для реалізації їх прав та обов'язків. Поряд із цим, перед постачальникам цифрових послуг ставиться задача забезпечення належного захисту персональних даних від посягань та дотримання вимог щодо їх збору та обробки.

Внесення змін в українське законодавство щодо розкриття постачальниками телекомунікаційних послуг персональних даних користувачів, має відбуватися, з урахуванням досвіду іноземних держав, який передбачає їх розкриття лише за умови відповідного рішення суду.

АНОТАЦІЯ

Розглянуто трансформацію уявлень на категорію «анонімність» в мережі Інтернет. Проведено порівняння поглядів на концепцію віртуальної ідентичності яка існувала на початковому етапі розвитку Інтернету та епохою Web 2.0. у XXI ст. На початковому етапі розвитку Інтернету анонімність називалась невід'ємною властивістю мережі, що підтримувалося протоколом який не передбачав передання даних про користувачів до кінцевого обладнання, то, сучасний етап розвитку Інтернету характеризується протоколом відкритого, а не конфіденційного спілкування, де анонімність переважно вже ілюзія.

З'ясовано, що відсутність абсолютної анонімності, відбувається формування єдиної автентичної ідентичності та учасники мережі прагнуть до прозорості, що знаходить своє відображення у просуванні компаніями відповідних технологічних рішень. Кроком на шляху деанонімізації є просування політики «єдиного аккаунту» та реальних імен, що полегшує технологічним компаніям можливість збирати персональні данні, відстежувати поведінку користувачів та направляти таргетовану рекламу.

Встановлено, що використання засобів псевдонімізації, використання додатків та сайтів без реєстрації, обрання псевдонімів при формуванні цифрової ідентичності, поширення в соціальних мережах вигаданої інформації про особу, не виключають можливість ідентифікувати особу правоохоронними органами у разі вчинення правопорушення. Оскільки, будь-які цифрові сліди дозволяють ідентифікувати особу.

Доведено, що розкриття персональних даних постачальниками телекомунікаційних послуг має відбуватися виключно на підставі судового рішення, що має забезпечити дотримання прав користувачів та недопущення втручання у особисте життя.

Проаналізовані чинники, які трансформують уявлення про категорію «анонімність» та її цінність в мережі Інтернеті.

Доведено, що у сучасних умовах розвитку Інтернету анонімність цифрової ідентичності не наділяє особу можливістю вчиняти операції онлайн та жодним чином не стимулює, не заохочує до вчинення правочинів та інших вчинків. Оскільки держави, в межах своїх міжнародних зобов'язань щодо захисту прав і законних інтересів осіб, поступово посилюють контроль за діяльністю в Інтернеті та запроваджують обов'язкову ідентифікацію користувачів.

Ключові слова: анонімність, право на анонімність, права людини, ЄСПЛ, цифровий слід, цифрова ідентичність, фізична особа, правоздатність, цифрове середовище, персональні дані.

Література

1. Birch D. Putting "identity" on the "blockchain". Part 2: Create an identity model. 2016. Dave Birch. CHYP USA, Consalt Hyperion company / URL: http://www.chyp.com/putting-identity-on-the-blockchain

2. Bernal P. Internet Privacy Rights: Rights to Protect Autonomy. N. Y. : Cambridge University Press, 2014. 311.

3. A Declaration of the Independence of Cyberspace. URL: https:// www.eff.org/cyberspace-independence

4. Network Neutrality FAQ.URL: http://timwu.org/network_neutrality.html

5. *Близнец* И. А. *Авторское право* и смежные права : учебник / И. А. *Близнец*, К. Б. Леонтьев ; под ред. И. А. *Близнеца*. – Москва : Проспект, 2010. – 416 с.

6. Директива 2000/31 ЄС Про деякі правові аспекти інформаційних послуг, зокрема, електронної комерції, на внутрішньому ринку URL: https://zakon.rada.gov.ua/laws/show/994_224#Text

7. Составляющие цифровой *трансформации*: монография / Г. С. *Сологубова*. Москва : Издательство Юрайт, 2019. 147 с. С. 88.

8. Кузнецова С. С. Право на анонимность в сети Интернет: актуальные вопросы реализации и защиты. *Российское право: образование, практика, наука.* 2020. №. 5. С. 33–41.

10. Ляпунов Б. А. Приватность личности: понятие, сущность и правовая природа. *Актуальные проблемы российского права.* 2019. № 2. С. 33–42.

11. Мироненко Т. В., Куропацкая Е. Г. Проблематика защиты авторских прав в электронной среде: опыт Японии, КНР и России. *Евразийская адвокатура.* 2018. №. 5 (36). С. 84–88.

12. Михайлов С. В. Анонимность в Интернете. *Журнал Суда по интеллектуальным правам.* 2017. № 17. С. 26–32.

13. Митник К. Искусство быть невидимым: как со- хранить приватность в эпоху Big Data (пер. с англ.). М.: Эксмо, 2021. 464 с.

14. Мочалов А. Н. Парадокс Анонимности в Интернете и проблемы ее правового регулирования. *Вестник Сургутского государственного университета.* 2021. № 4 (34). С. 111–121.

15. Мылтыкбаев М. Ж. Право на анонимность в сети Интернет: вопросы международно-правовой защиты. *Юридическая наука.* 2019. № 4. С. 42–45.

16. Проєкт Закону Верховної Ради Про внесення змін до Кримінального процесуального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю та використання електронних доказів від 01.09.2020 № 4004 URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=69771

17. Проєкт Закону про внесення змін до Кримінального процесуального кодексу України та Кодексу України про адміністративні правопорушення щодо підвищення ефективності протидії кібератакам від 01.09.2020 № 4003 URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=69770

18. Саликов М. С., Несмеянова С. Э., Колобаева Н. Е., Кузнецова С. С., Мочалов А. Н. Право на доступ в Интернет, анонимность и идентификация пользователей (конституционно-правовые проблемы) / под ред. М. С. Саликова. Екатеринбург : Издательство УМЦ УПИ, 2020. 167 с.

19. Супрун Г. Г. Ідентичність індивіда в цифрову епоху соціальних комунікацій. *Філософські обрії.* 2020. № 43. С. 85–94.

20. Сухорольський П. М. Право на анонімність як суттєвий елемент прав людини. *Правова Інформатика*. 2003. № 1(37). С. 39–47.

21. Серьогін В. А. Право на анонімність як елемент прайвесі. *Науковий вісник Ужгородського національного університету.* 2014. № 24. С. 154–159.

22. Токарева В. О. Трансформація віртуальної ідентичності: від множинності до єдиної автентичності в мережі Інтернет. *Актуальні проблеми вітчизняної юриспруденції.* 2022. № 3. С. 47–52.

23. Царева А. В. Человек в сети: смена веб-поколений. *Журнал социологии и социальной антропологии.* 2012. № 5 (64). С. 46.

24. Rainie L., Anderson J., Albright J. The Future of Free Speech, Trolls, Anonymity, and Fake News Online. *Pew Research Center.* 2017. 82 p.

25. Щербович А. А. Реализация конституционных прав и свобод в Интернете. М. : Теис, 2015. 148 с.

26. Rossi A. Internet Privacy: Who Sets the Global Standard? *The International Spectator.* 2014. Vol. 49, Is. 1. P. 65–80.

27. Sarda T., Natale S., Sotirakopoulos N., Monaghan M. Understanding Online Anonymity. *Media Cult Soc.* 2019. №. 4. P. 557–564.

28. European Court of Human Rights. Case of Delfi AS v. Estonia (Application no. 64569/09). Judgment. Strasbourg. 10 October 2013. URL: http://www.statewatch.org/news/2013/oct/echr-judgment-delfi-AS-v-estonia.pdf (дата обращения: 18.04.2019).

29. European Court of Human Rights. Case of Benedik v. Slovenia (Application no. 62357/14). Judgment. Strasbourg. 24 April 2018. URL: http://www.dirittoegiustizia.it/allegati/ PP_INTERN_18Cedu Privacy_milizia_s.pdf

30. Access intervenes at ECtHR for the right to be anonymous online [Electronic resource]. URL: https://www.accessnow.org/access-intervenes-at-ecthr-for-the- right-to-be-anonymous -online

31. Article 19. Right to Online Anonymity. Policy Brief. June 2015. URL: https: www.article19.org/data/files/medialibrary/38006/Anonymity_and_encryption_report_A5_final-web.pdf

32. In Austria in 2020, anonymity on the Internet will be banned. URL: https://tass.ru/obschestvo/6335723

33. Козаченко О. В Австрії мають намір заборонити анонімність користувачів великих інтернет-сайтів. Штраф для компаній сягатиме €500 тисяч URL: https://babel.ua/news/29190-v-avstriji-rozglyadayut-zakonoproekt-yakiy-zaboronyaye-zalishati-anonimni-komentari-v-interneti

34. R. v. Spencer, [2007] 1 S. C.R. 500, 2007 SCC 11 SUPREME COURT OF CANADA URL: https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/2347/index.do

35. Операторы связи будут передавать ЕК геолокационные данные в рамках борьбы с COVID-19. URL: https://www.securitylab.ru/news/506200.php

36. Kabelka L. German youth protection body endorses AI as biometric age-verification tool. 31.05.2022. URL: https://www.euractiv.com/section/digital/news/german-youth-protection-body-endorses-ai-as-biometric-age-verification-tool/

37. P. Roberts 2011. How Facebook and Facial Recognition Are Creating a Minority Report-Style Privacy Meltdown. URL: https://threatpost.com/

how-facebook-and-facial-recognition-are-creating-minority-report-style-privacy-meltdown-080511/75514/

38. Face Recognition Software, Social Media Sites Increase Privacy Risks, Says New Carnegie Mellon Study. URL: https://www.prnewswire.com/news-releases/face-recognition-software-social-media-sites-increase-privacy-risks-says-new-carnegie-mellon-study-126510323.html

Information about the author:
Tokareva Vira Oleksandrivna,
Ph.D. in Law, Associate Professor,
Lecturer at Civil Law Department
National University "Odessa Law Academy"
9, Academichna str., off. 41, Odessa, Ukraine, 65009
https://orcid.org/0000-0002-8409-1477