

ПРАВО НА ПРИВАТНІСТЬ В УМОВАХ СУЧАСНИХ КОМУНІКАЦІЙ

THE RIGHT TO PRIVACY IN THE CONDITIONS OF MODERN COMMUNICATIONS

Коваленко О.О., студентка VI курсу юридичного факультету

*Навчально-науковий інститут інформаційної безпеки**Національної академії Служби безпеки України*

Тихомиров О.О., к.ю.н., доцент,

*доцент кафедри цивільно-правових дисциплін**Національна академія Служби безпеки України*

У статті висвітлюється сутність права на приватність в умовах сучасних комунікацій. Приділено увагу видам права на приватність та виокремлено основні складники цього права. Проведено порівняння між інформаційною приватністю та приватністю комунікацій. Зазначено про доцільність невіддільного розгляду вказаних видів права на приватність та наведені причини такої необхідності. Продемонстрований процес трансформації розуміння права на приватність до його сучасного значення. Виділені нові ознаки, які притаманні відносинам осіб у світовій мережі Інтернет та які безпосередньо вплинули на модернізацію розуміння права на приватність. У роботі згадана триада вимог, дотримання яких забезпечує реалізацію права на приватність. У зв'язку зі швидкими темпами розвитку інформаційних технологій було акцентовано увагу на групі технологій та методів Big Data, які тим чи іншим чином впливають на стан захищеності права на приватність в Інтернеті. Встановлено передумови можливого втручання в інформаційну приватність особи та виділено дві найбільш актуальні натеper. Наведено приклади ситуацій виникнення передумов можливого порушення права на приватність. Акцентовано увагу на існуючих загрозах інформаційної приватності, які є найбільш поширеними у наш час. На основі даних світових експертів виявлені найпоширеніші транснаціональні загрози праву на приватність. Проаналізовано норми міжнародних документів, які регулюють вказану проблематику. З урахуванням нормативно-правових актів було досліджено практичний стан реалізації права на приватність в умовах сучасних комунікацій. У статті також згадувалось про порушення права на приватність українською неурядовою організацією. Розроблено можливі варіанти надійної реалізації права на приватність в умовах інформаційної глобалізації.

Ключові слова: право на приватність, право на приватність в умовах сучасних комунікацій, інформаційна приватність, приватність технологій, загрози праву на приватність, обробка персональних даних, сучасні комунікації, право комунікацій, Big Data, триада вимог до права на приватність.

The article deals with the essence of the right to privacy in modern communications. In the first section of the paper, the author describes types of the right to privacy. A comparison is made between information privacy and communication privacy. Additionally, the text explores expediency of separate consideration of the specified types of the right to privacy and describes the reasons of such necessity of separation. The purpose of this paper is to demonstrate the process of transformation the understanding of the right to privacy to its modern meaning. New features have been identified that are inherent in human relationships on the World Wide Web and that have directly influenced the modernization of the understanding of the right to privacy. The article mentions a triad of requirements, compliance which ensures the realization of the right to privacy with. Due to the rapid development of the information technology, attention is also focused on a group of technologies and methods of Big Data, which in one way or another affect the state of protection of the right to privacy in the Internet. In the middle of the work, the author gives preconditions for possible interference with a person's information privacy and identifies the two most relevant ones for today. The author demonstrates examples of situations of preconditions for possible violations of the right to privacy. Emphasis is placed on the existing threats to information privacy, which are the most common today. Based on data from global experts, the article provides the most common transnational threats to the right to privacy. The final points are focused on the norms of international documents that regulate this issue. Taking into account the normative legal acts, the paper highlights the practical state of realization of the right to privacy in the conditions of modern communications. The article also mentioned the violation of the right to privacy by a Ukrainian non-governmental organization. In conclusion, possible options for reliable implementation of the right to privacy in the context of information globalization have been developed.

Key words: right to privacy, right to privacy in modern communications, information privacy, privacy of technologies, threats to the right to privacy, processing of personal data, modern communications, right to communications, Big Data, triad of requirements for the right to privacy.

Постановка проблеми. У зв'язку з розвитком суспільних відносин та стрімкою інформаційною глобалізацією всіх сфер життєдіяльності особи право на приватність зазнало змін відповідно до нових умов. Зокрема, це пов'язано з появою та розвитком Інтернету як невіддільного компоненту сучасної дійсності, як основного засобу поширення та обміну інформацією.

Раніше під правом на приватність розуміли захист від фізичного посягання на життя і власність, від заподіяння шкоди *vi et armis* (лат. силою зброї) [1]. Таке розуміння приватності ототожнювало його з «правом бути залишеним у спокої» [2]. З часом під впливом різних факторів виникла потреба в розширенні змісту цього права. Стали виділяти такі види приватності: фізичну, територіальну, інформаційну і приватність комунікацій [3].

Сучасні інформаційні технології надали людству нові комунікативні можливості, чим сприяли побудові нових взаємовідносин, іманентними ознаками яких є довіра та прозорість. Це зумовило поступову модернізацію розуміння права на приватність, зокрема виділення та осмислення таких своєрідних складників приватності, як інформаційна приватність та приватність комунікацій. Обидва

вказані складники права на приватність перебувають у тісному взаємозв'язку.

Під інформаційною приватністю розуміють передусім установлення належного захисту персональних даних під час їх обробки від несанкціонованого та нецільового використання. У цьому контексті науковці виокремлюють такі правові можливості людини, як: а) бути захищеною від втручання в її особисте і сімейне життя та стосунки через опублікування інформації; б) знати, ким, коли, яким чином і в яких межах інформація про неї може бути або буде використовуватися іншими особами [4]. Що стосується приватності комунікацій, то її зміст полягає в безпечному для особистого життя поширенні, отриманні та інших діях, пов'язаних з інформацією, які здійснюються з використанням технічних засобів.

Слід акцентувати увагу на тому, що визначені вище види приватності та реалізація відповідних прав в умовах програмно-технологічного прогресу суспільства повинні розглядатися невіддільно, оскільки особливості поширення інформації в цифровому вигляді виключає можливість розмежування інформаційної і комунікаційної приватності.

Підтвердженням цього є ситуація, коли індивід оприлюднив інформацію у своєму обліковому записі для обмеженого кола осіб, однак із часом вирішив змінити налаштування конфіденційності таким чином, що відомості стали доступні широкому загалу. І навпаки, коли доступність інформації була обмежена лише згодом, однак певний час була можливість її використання необмеженим колом осіб.

Наведені приклади демонструють важливість проблеми права на приватність в інформаційному просторі та глибину його правового забезпечення, що підтверджується і відповідними міжнародними актами. Так, у резолюції Генеральної Асамблеї Організації Об'єднаних Націй «Право на приватність у цифрову епоху» від 18 грудня 2013 року акцентовано увагу на тому, що «ті ж права, що люди мають в оффлайн-режимі, також повинні бути захищені онлайн, зокрема право на приватність» [5].

Актуальність досліджуваної тематики полягає передусім у тому, що інформатизація суспільних відносин створює істотну небезпеку реалізації та захисту права людини на приватність. У своїй щорічній доповіді за 2019 рік Уповноважений Верховної Ради України з прав людини зазначив, що ним було розглянуто 1061 повідомлення про порушення права на приватність; здійснено 36 перевірок щодо додержання законодавства про захист персональних даних; складено 10 протоколів про адміністративні правопорушення [6]. Тому потреба створення дієвої системи захисту приватного життя в час, коли технологічні засоби значно випереджають правові механізми регулювання інформаційних відносин, є очевидною.

Аналіз останніх досліджень і публікацій. Правам людини, зокрема праву на приватність у його різних інтерпретаціях, присвячені численні праці зарубіжних і українських дослідників. Не применшуючи важливості наукових здобутків інших, у контексті досліджуваної теми інтерес авторів привернули передусім наукові роботи таких учених, як Дж. В. ДеКью, С.Д. Воренн, Л.Д. Брандейс, О.А. Баранов, В.М. Брижко, О.В. Гронь, А.В. Пазюк.

Метою статті є розвиток уявлень про право людини на недоторканність особистого життя в умовах сучасних комунікацій.

Виклад основного матеріалу. Відповідно до низки міжнародних та національних нормативно-правових актів право на приватність є одним із фундаментальних прав людини. Його первинний зміст відображено у ст. 12 Загальної декларації прав людини і ст. 8 Конвенції про захист прав та основоположних свобод [7; 8].

Вважаємо за доцільне погодитись із концепцією Дж. В. ДеКью, що структура аналізованої можливості людини виявляється в дотриманні тріади вимог: інформаційна вимога – здійснення контролю над особистою інформацією індивіда; приватність доступу, фізична недоторканність; приватність вираження, зокрема самоідентичність або індивідуальність особи [4, с. 75–77].

Із розвитком сучасних комунікацій кожен із вказаних елементів зазнає негативного впливу в інформаційному просторі. З кожним роком комунікаційні канали вдосконалюються швидкими темпами, й дедалі більше соціальні мережі стають невід'ємною частиною приватного життя особи. Це несе із собою істотні ризики, наприклад необережне ставлення до використання різних веб-ресурсів може стати передумовою порушення інформаційного права особи на приватність, оскільки користувач залишає за собою «інформаційний слід» у вигляді операційних даних (IP-адресу, тип комп'ютера, інформацію про відвідані веб-сторінки тощо). Аналіз цих даних дає змогу сформулювати інтернет-портрет користувача: звички, смаки, погляди, мотиви пошуків в Інтернеті.

Окрім цього, сьогодні вже стала звичною автоматизована обробка інформації про особу під час учинення правочинів, зокрема купівлі-продажу, оплати надання різного

роду послуг. Або ж нерідко люди готові «обмінювати» свої персональні дані на дисконтні знижки в магазинах.

Проте слід зауважити, що вся інформація про нас, яка так чи інакше опиняється в Інтернеті, не потрапляє в безодню, а зберігається і накопичується різними інформаційними системами. Обробці та аналізу такої великої кількості інформації сприяє група технологій та методів Big Data. Це феноменальне прискорення нагромадження даних та їх ускладнення, в результаті чого під загрозою опиняються особисті дані та захист конфіденційності, забезпечення анонімності в спілкуванні тощо [9].

Вважаємо за необхідне виділити дві передумови можливого втручання в інформаційну приватність особи:

1) неадекватна чи помилкова самостійна попередня оцінка ризиків використання власних персональних даних або її відсутність;

2) легковажне ставлення осіб до публікації інформації про інших.

Прикладом першої передумови ймовірного виникнення загрози праву на приватність в інформаційному просторі є ігнорування змісту повідомлень про політику конфіденційності веб-ресурсу, які користувач отримує в разі необхідності отримання доступу до ресурсу. Однією з умов цієї політики є надання користувачем згоди на обробку своїх персональних даних з метою подальшого користування сайтом. Вказана дія врегульована такими міжнародними договорами, як Конвенція Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних [10] та Загальний регламент захисту персональних даних Європейського Союзу (General Data Protection Regulation, далі – GDPR) [11]. У глобальній мережі Інтернет згоди на обробку персональних даних притаманний формальний характер виконання. У більшості випадків користувач автоматично ставить галочку про згоду з політикою конфіденційності, не звертаючи увагу на інформаційне наповнення сповіщень про неї.

Видається, що вказаній дії доцільно приділити більше уваги, зокрема сприяти підвищенню рівня усвідомлення користувачем змісту повідомлень. Наприклад, запровадити покрокове ознайомлення з політикою конфіденційності, без чого користувач не зможе продовжити користування веб-ресурсом. Підтвердженням того, що особа дійсно прочитала правила, може бути, зокрема, питання щодо змісту повідомлення наприкінці меседжа. Однак не заперечуємо того факту, що така форма вираження згоди може викликати незадоволення у користувача. Ця проблема лежить у контексті необхідності підвищення такої нової складової частини правової культури, як культура інформаційно-правова [12, с. 262–263].

Яскравим підтвердженням впливу другої передумови втручання в інформаційну приватність є порушення, розглянуте Коломийським міськрайонним судом Івано-Франківської області від 14 лютого 2017 року. Зокрема, було встановлено, що секретар Коломийської міської ради вчинив адміністративне правопорушення, а саме розмітив у вільному доступі в мережі Інтернет на сайті www.facebook.com в групі «Типова Коломия» публікацію щодо ОСОБА_1 з фотографією звернення ОСОБА_1 на урядову гарячу лінію, яке містить відомості про ОСОБА_1: прізвище, ім'я, по батькові, адресу проживання, номер мобільного телефону, текст звернення. У судовому засіданні секретар міської ради заперечував свою причетність до вказаного діяння, допускаючи, що його сторінку могли зламати і надрукувати дану інформацію. Проте, незважаючи на це, якби не оперативність ОСОБА_1 та використання ним відповідного ресурсу, він і не підозрював би, що інформація, яка його ідентифікує, розміщена в Інтернеті без його згоди [13].

У світлі судового захисту права на приватність варто згадати, що одним із перших прецедентів стало рішення Верховного Суду штату Джорджія у справі «Павесіч

vs. Нью Ігланд Лайф Іншуранс Ко.» (1905 р.). Задовольняючи позов чоловіка, зображеного без його згоди в рекламному оголошенні, суд визначив об'єкт і мету правового захисту таким чином: «Той, хто бажає жити життям відносного усамітнення, має право вибрати час, місце та способи, в які він буде піддавати себе громадському спостереженню» [14].

Як видно, наведені рішення датовані різними століттями, але містять близькі за змістом порушення. Тобто у зв'язку з розвитком новітніх технологій, які, з одного боку, сприяють полегшенню нашого спілкування, а з іншого – створюють загрозу поширенню персональних даних за допомогою цих комунікацій, захист «право бути залишеним у спокої» не тільки не втрачає актуальності, а й набуває нового змісту.

Окрім передумов можливого порушення права особи на приватність, у кіберпросторі утворюється й низка специфічних загроз, серед яких доцільно виокремити такі: 1) кібератаки; 2) недосконалість системи захисту персональних даних.

Поширеними є випадки незаконної обробки персональних даних у глобальній мережі Інтернет шляхом застосування, зокрема, шкідливих програм. За даними щорічної доповіді про глобальні ризики у світі «Global Risks Report 2017», підготовленої експертами Всесвітнього економічного форуму в Давосі, на третьому місці за важливістю для світової спільноти перебувають технологічні ризики – крадіжки персональних даних, махінації з ними, масштабні кібератаки та кіберзлочинність [15]. Вказаний вид злочинності є транснаціональним та може завдати великої шкоди як окремій особі, так і державі загалом. Тому наявна потреба створення та ефективного захисту від злочинців-хакерів, які можуть отримати доступ до особистих даних користувачів.

Однак не тільки інформаційні технології як такі створюють загрози праву на приватність. Ще одним джерелом небезпек слід вважати недосконалість наявної системи захисту персональних даних у контексті її нормативно-правового регулювання. Безперечно, в авангарді правового захисту персональних даних іде Європейський Союз (далі – ЄС). Але європейський регіон насичений різними комунікативними зв'язками між різними державами, зокрема й тими, які не є членами ЄС, що значно ускладнює визначення територіальної дії GDPR. Так, пункт 2 статті 3 GDPR передбачає застосування екстериторіального принципу (зокрема, в Україні) у разі, якщо діяльність з обробки пов'язана з: а) пропонуванням товарів чи послуг незалежно від того, чи потрібно платити суб'єкту даних таким суб'єктам даних у Союзі; б) моніторингом їхньої поведінки, наскільки їхня поведінка відбувається в межах Союзу [11]. Така ситуація вимагає особливої уваги з боку володільців (контролерів) персональних даних та відповідних юридичних консультацій.

Як приклад спробуємо змоделювати таку ситуацію. Українське медіаагентство містить інформаційний контент українською мовою та націлене лише на аудиторію користувачів з України, зокрема й на тих, хто подорожує світом. На цьому інформаційному ресурсі щотижня розміщується стаття з порадами щодо подорожей у країнах ЄС. Разом із тим веб-сайт має вільний доступ для здійснення обробки інформації користувачів, які зареєстровані на ньому. У своїй

політиці конфіденційності сайт передбачив право отримувати інформацію, зокрема про тривалість відвідування та дії користувача. Враховуючи вищезазначене положення GDPR, можна зробити висновок, що його дія не поширюватиметься на це медіаагентство, а саме його правила не діятимуть на користувачів, які подорожують за кордоном, оскільки обробка персональних даних безпосередньо не здійснюється на території ЄС і не має на меті надавати свої послуги, передавати товари за валютою ЄС, здійснювати моніторинг поведінки фізичних осіб за межами України. Проте не слід забувати, що сайт можуть використовувати не лише громадяни України, тому власнику цього агентства потрібно переглянути відповідність своєї діяльності згідно з останніми змінами у правовому полі.

Іншою важливою ознакою системи правового захисту права на приватність є те, що вона майже завжди базується на необхідності дотримання балансу приватного права і публічного інтересу, який може бути неочевидним. У цьому контексті звернемо увагу на контент сайту «Миротворець», який виступає інтернет-представництвом Центру досліджень ознак злочинів проти національної безпеки України, миру та безпеки громадян і міжнародного правопорядку. Керуючись цілями забезпечення національної безпеки України, яка є очевидним публічним інтересом, та посиляючись на положення законодавства України і міжнародних актів у сфері обробки персональних даних, представники зазначеного сайту збирають і поширюють інформацію щодо осіб, у діях яких виявлено ознаки відповідних протиправних діянь. Водночас згаданий Центр не є уповноваженим державним органом, не надає конкретних даних про перевірку достовірності інформації, її документального підтвердження тощо, що разом зі сприянням протидії злочинності може спричинити й ситуації, в яких право на приватність буде порушуватися.

Також проблему забезпечення балансу прав демонструє і сучасна ситуація з реалізацією так званого «права на забуття» в Інтернеті. За сучасною європейською практикою це право не має очевидної переваги перед потребою осіб у доступі до інформації, а тому рішення щодо вилучення контенту наразі приймається в кожному окремому випадку індивідуально в судовому порядку [16].

Висновки і пропозиції. Право на недоторканність особистого життя має комплексний характер, зумовлений наявністю в його структурі варіативного переліку можливостей, який змінюється разом із науково-технічним та соціальним розвитком суспільства. У зв'язку з цим право на приватність особи в умовах інформаційної глобалізації може бути забезпечено за умови побудови виваженої системи правового захисту. По-перше, це пов'язано з удосконаленням системи чинних нормативно-правових актів, які регламентують право на приватність в інформаційній сфері; по-друге – з розробленням нормативно-методичних документів із питань забезпечення захисту персональних даних із застосуванням сучасних засобів спілкування; по-третє – з формуванням елементів правової культури в інформаційній сфері, тобто мотиваційних, психологічних установок суб'єктів щодо безпечного поширення особистої інформації в глобальній мережі Інтернет. Останнє може бути забезпечене шляхом проведення тренінгів та семінарів для людей різних вікових категорій залежно від рівня їх обізнаності у вказаній сфері.

ЛІТЕРАТУРА

1. Warren S.D., Brandeis L.D. The right to privacy. *Harvard law review*. 1890. Vol. 4. P. 193–220.
2. Серьогін В.О. Прайвесі як право «бути залишеним у спокої». *Право і Безпека*. 2010. № 3. С. 6–9. URL: http://nbuv.gov.ua/UJRN/Pib_2010_3_3 (дата звернення: 07.08.2020).
3. Privacy & Human Rights. Privacy International and Electronic Privacy Information Center, 1999. URL: <http://gilc.org/privacy/survey/intro.html> (дата звернення: 07.08.2020).
4. DeCew J.W. In Pursuit of Privacy: Law, Ethics, and the Rise of Technology. Ithaca, N.Y. : Cornell University Press, 1997. 208 p.
5. General Assembly Resolution "The right to privacy in the digital age", A/RES/68/167. URL: <https://undocs.org/en/A/RES/68/167> (дата звернення: 07.08.2020).

6. Щорічна доповідь Уповноваженого Верховної Ради України з прав людини про стан дотримання прав і свобод людини і громадянина. URL: <file:///C:/Users/o.kovalenko/Downloads/zvit-za-2019.pdf> (дата звернення: 07.08.2020).
7. Загальна Декларація прав людини ООН від 10 грудня 1948 року. URL: https://zakon.rada.gov.ua/laws/show/995_015 (дата звернення: 07.08.2020).
8. Конвенція про захист прав та основоположних свобод від 4 листопада 1950 року. URL: https://zakon.rada.gov.ua/laws/show/995_004 (дата звернення: 07.08.2020).
9. Великі перспективи індустрії Big Data. Український суперкомп'ютерний інтернет-дайджест. URL: <http://supercomputer.com.ua/ua/266-veliki-perspektivi-industriji-big-data.html> (дата звернення: 16.11.2019).
10. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних від 28 січня 1981 року. URL: https://zakon.rada.gov.ua/laws/show/994_326 (дата звернення: 07.08.2020).
11. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL> (дата звернення: 07.08.2020).
12. Теорія держави і права : навч. посіб. для підгот. фахівців з інформ. безпеки / О.О. Тихомиров та ін. ; за заг. ред. Л.М. Стрельбицької. Київ : Кондор-Видавництво, 2016. 332 с.
13. Постанова Коломиїського міськрайонного суду Івано-Франківської області 14.02.2017 р., справа № 346/200/17. URL: <http://reyestr.court.gov.ua/Review/64723526> (дата звернення: 07.08.2020).
14. Pavesich vs. New England Life Ins. Co., 50 S.E. 68 (Ga. 1905)). Information privacy law : Textbook / D.J. Solove, M. Rotenberg. New York : Aspen Publishers, 2003. 795 p.
15. Эксперты Давоса назвали главные риски для человечества в 2017. URL: http://www3.weforum.org/docs/GRR17_Report_web.pdf (дата звернення: 07.08.2020).
16. Гугл згадає все! Право суспільства на інформацію визнане важливішим за захист особистих даних. *Закон і бізнес*. 08.08–14.08.2020. № 32 (1486). URL: <https://zib.com.ua/ua/pda/143946.html> (дата звернення: 08.08.2020).