УДК 342.7

ІСАКОВ М.Г.
ПАРКУЛАБ В.Г.

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ У МЕРЕЖІ ІНТЕРНЕТ: ЗАГАЛЬНОТЕОРЕТИЧНІ ПИТАННЯ

Стаття присвячена з'ясуванню правових механізмів захисту персональних даних у мережі Інтернет, визначенню сфери реалізації права людини на шифрування інформації й анонімність у мережі Інтернет, оскільки перевищення меж втручання будь-якого суб'єкта в приватне життя особи створює можливості для зловживань її суб'єктивними правами.

Ключові слова: *права людини, персональні дані, анонімність особи, конфіденційність інформації, кіберзлочинність.*

Статья посвящена анализу правовых механизмов защиты персональных данных в сети Интернет, установлению сферы реализации права человека на шифрование информации и анонимность в сети Интернет, поскольку превышение пределов вмешательства любого субъекта в частную жизнь лица создает возможности для злоупотреблений его субъективными правами.

Ключевые слова: *права человека, персональные данные, анонимность лица, конфиденциальность информации, киберпреступность.*

The article is devoted to the clarification of legal mechanisms for the protection of personal data on the Internet, the definition of the scope of the implementation of human rights for information encryption and anonymity on the Internet, since the excess of the limits of the interference of any subject in the private life of a person creates opportunities for abuse of its subjective rights.

Key words: *human rights, personal data, anonymity of a person, confidentiality of information, cybercrime.*

Вступ. Як відомо, право на недоторканність приватного життя в Інтернеті включає свободу від спостережень, право на використання шифрування, право на онлайн-анонімність. Кожна особа має право на захист персональних даних у процесі збереження, оброблення, утилізації та розкриття інформації. Як і у випадку з багатьма іншими правами людини, право на недоторканність приватного життя не є абсолютним і, як зазначено у Європейській конвенції прав людини й основоположних свобод, може обмежуватися з метою запобігання порушень правопорядку та злочинних діянь. Обмеження права на захист персональної інформації та недоторканості приватного життя в мережі Інтернет (незаконне спостереження за спілкуванням, прослуховування, незаконний збір особистих даних) порушують право людини на недоторканність приватного життя і свободу думки і можуть привести до обмежень права на свободу вираження поглядів.

Постановка завдання. Метою статті є з'ясування правових механізмів захисту персональних даних у мережі Інтернет, визначення сфери реалізації права людини на шифрування інформації й анонімність у мережі Інтернет, оскільки перевищення меж втручання в приватне життя створює можливості для зловживань суб'єктивними правами.

Вивчення окресленої проблематики та досягнення поставленої мети не можливе без звернення до наявних наукових напрацювань, представлених роботами Г. Андрощука, С.В. Демченка, В.І. Гриценко, К.І. Задираки, Г. Козіна, О.Б. Ломаги, Б.В Романюка, В.А. Серьогіна, М.П. Сухорольского та ін.

© ІСАКОВ М.Г. – доктор юридичних наук, адвокат, президент (Юридична фірма «Глобус»)
© ПАРКУЛАБ В.Г. – кандидат юридичних наук, адвокат, керуючий партнер (Юридична фірма «Глобус»)

Результати дослідження. У ст. 17 Міжнародного пакту про громадянські і політичні права йдеться про захист від посягань на таємницю кореспонденції, що охоплює усі форми комунікації як в Інтернеті, так і поза ним. Незаконний доступ урядових структур і приватних компаній до особистих даних негативно впливає на свободу вираження думки, оскільки змушує менше користуватися електронними комунікаційними технологіями [1].

Можливості інформаційно-комунікаційних технологій дозволяють широко використовувати їх як для захисту, так і для обмеження права людини на недоторканність приватного і сімейного життя (прайвесі). Так, технології шифрування можуть зробити спілкування між приватними особами конфіденційним або, навпаки, надати можливість зацікавленим особам (наприклад, із боку уряду) перехоплювати цю інформацію. Так само технології спостереження можуть як охороняти приватне життя, так і використовуватися з іншою метою, порушуючи принцип недоторканності приватного життя. Цифрові технології можуть забезпечити анонімність, дозволяючи людям почуватися в безпеці, обмінюючись думками, які вони ніколи б не озвучили, якби їх імена асоціювалися з цими ідеями [2].

Континентальна традиція захисту особистих прав людини виходить з інституту римського права actio iniuriarum (у римському праві – позов за звинуваченням в особистій образі), що забезпечує захист не тільки від тілесних ушкоджень, а й від моральної шкоди. Таким чином, особисті права можна вважати джерелом приватноправових інтересів та еквівалентом прав людини. Так, захист від наклепу і порушень інших особистих прав на європейському континенті має давні традиції, тоді як в англо-американському праві аналогами поняття «наклеп» є поняття libel і slander [3].

Загальне право захисту особистого життя пов'язане з низкою різноманітних питань, таких як свобода поведінки і можливість визначення приватного простору, щоб захистити себе від небажаного втручання і контролювати доступ до особистої інформації з метою запобігання її несанкціонованому поширенню. Крім того, право на захист особистого життя пов'язане з концепціями особистісних характеристик і конфіденційності, а також анонімності і недоторканості людської гідності.

У межах ЮНЕСКО сформоване поняття недоторканності особистого життя, що спирається на такі принципи ООН, як популяризація в Інтернет-мережі політики і практики поваги права на недоторканність особистого життя; сприяння відкритості та транспарентності з урахуванням недоторканності особистого життя; визнання того, що недоторканність особистого життя та її захист є основою довіри в мережі Інтернет; використання багатосторонніх угод для забезпечення недоторканності особистого життя поряд з іншими правами людини – такими, як права на свободу вираження поглядів, права на життя, права на свободу й особисту безпеку.

Потенційні суперечності між правами людини і загальнолюдськими цінностями можуть вимагати їх врівноваження у конкретних ситуаціях. Наприклад, заклики до транспарентності з боку держави і корпорацій в окремих випадках не відповідають вимогам права на недоторканість особистого життя. З одного боку, політика свободи інформації вимагає від державних органів надавати наявну в їх розпорядженні інформацію про ту чи іншу людину і навіть сприяти доступу до такої інформації, що забезпечує підтримку свободи вираження думки, дозволяючи людям шукати й отримувати, а також вільно поширювати будь-яку інформацію. А з іншого боку, за подібних обставин виникає необхідність врахувати і захищати права інших осіб.

Шифрування персональних даних використовується для захисту відомостей про особу і має криптографічний характер, роблячи неможливим доступ до цієї інформації без прихованих ключів. Персональні дані людини можна розглядати як її проекцію, тому шифрування відіграє важливу роль як інструмент захисту від зловживань у використанні контенту користувача, забезпечує більший ступінь захисту інформації про особисте життя й анонімності передачі даних, оскільки доступ до контенту комунікацій має тільки одержувач. Деякі фахівці вважають шифрування одним із найкращих способів забезпечення конфіденційності і ключовим методом особистого та комерційного захисту і пропонують використовувати шифрування за мовчазною згодою. Інші висловлюють більш обережну позицію, проте практично усі фахівці визнають, що певний рівень шифрування може запобігти більшості порушень у сфері конфіденційності [4].

Турбота про громадську безпеку у зв'язку зі зростанням екстремізму і терористичними погрозами призвела до нових закликів відмовитися від шифрування (або принаймні зробити повідомлення такими, що можуть бути дешифровані) або зобов'язати користувачів Інтернету розкривати свої шифрувальні ключі за наявності встановлених умов і процедур, які забезпечують законність такого обмеження конфіденційності.

Політика конфіденційності щодо усіх сервісів в Інтернеті повинна бути доступна для користувача. Управління системами налаштування приватності має бути необмеженим і здійснюватися в режимі безперервної оптимізації, причому головним критерієм такої оптимізації повинна бути

зручність у користуванні. Крім того, право на недоторканність приватного життя має бути захищене стандартами конфіденційності і цілісності інформаційних систем, які повинні включати захист від несанкціонованого доступу до відповідних даних (тільки сам користувач повинен давати на це згоду).

На думку Є. Горного, поняття «віртуальна особистість» у широкому сенсі, як і її англомовний аналог virtual identity, є багатозначним і має низку синонімів, значення яких перетинається лише частково. Основні з них: ідентифікатор для входу в комп'ютерну систему (login, user name); прізвисько або псевдонім (user name, nickname), що використовується для ідентифікації користувача в комунікативних електронних середовищах (таких як чат), розраховане на велику кількість користувачів, рольові ігри, блоги і т. п.; псевдонім або інший замінник імені людини (наприклад, номер або особистий код), що використовується для соціальної репрезентації. Сюди належать такі різнорідні явища, як номер ідентифікаційної карти, картки соціального страхування або мобільного телефону, DNA, відбитки пальців, псевдонім тощо. Комп'ютеризація суспільства призвела до того, що дедалі більша кількість способів соціальної ідентифікації мають цифровий характер. Саме цим пояснюється стрімке поширення віртуальної (або цифрової) ідентичності у правових термінах [5].

Віртуальна особистість – це об'єкт, котрому приписуються якості суб'єкта, статус існування якого залишається не визначеним. Термін «віртуальний» позначає щось середнє між «реальним» і «нереальним». Віртуальна особистість відрізняється від реальної тим, що вона не має матеріального виразу і складається виключно зі знаків і дій (а також із образів, думок і почуттів, які вона породжує у психіці спостерігачів). У вузькому розумінні віртуальна особистість – це комплекс знаків, що існують в електронному середовищі, носієм яких є певна особа. Однак реалізація змісту цих знаків відбувається виключно в людській свідомості. Таким чином, слід розуміти різницю між природою середовища та її сутністю. Можна назвати дві фундаментальні якості віртуальної особи – власне ім'я і здатність до автономних дій. Всі інші якості віртуальної особи є похідними [6]. Поступово межа між віртуальною і реальною дійсністю може стати настільки прозорою, що буде невідомо, хто є суб'єктом реальних суспільних відносин – віртуальна особа або реальна людина. Для того, щоб юридична норма здійснювала фактичний регулятивний вплив на суспільні відносини нового типу, необхідно чітко формулювати, хто саме буде суб'єктом цих відносин, чітко визначати зміст прав і обов'язків суб'єктів правовідносин нового типу.

В умовах сучасного інформаційного суспільства концептуально змінюються поняття «суб'єкт права» і «суб'єкт правовідносин» як елементів механізму правового регулювання, і на етапі реалізації юридичних норм в інформаційному просторі стає неможливою ідентифікація «віртуальної особистості» з реальним суб'єктом конкретних правовідносин, тому виникає проблема визначення меж правового регулювання суспільних відносин в Інтернет-мережах за допомогою закріплених у законодавстві механізмів і процедур [7, с. 14–24]. Сучасні засоби програмування дозволяють створювати комп'ютерні програми-роботи (т. зв. «боти»), які можуть здійснювати певні функції без участі людини. Згодом такі програми можуть виконувати більш складний комплекс дій, у т. ч. на основі аналізу стану навколишнього віртуального середовища. У перспективі можлива постановка питання про створення особливої програми, що б здійснювала юридично значущі дії в кіберпросторі без безпосередньої команди «власника».

Дотепер не врегульованим залишається питання про долю результатів мережевої активності особи після її смерті. Електронні гаманці, електронні поштові скриньки, акаунти в соціальних мережах та інших сервісах можуть зберігатися нескінченно довго. Необхідно враховувати той факт, що доступ до них можуть отримати зловмисники, які від імені померлої особи вчинятимуть дії правого характеру. Та обставина, що «мережеве майно» особи може мати реальну ринкову вартість, зумовило розвиток Інтернет-економіки. Паролі від електронних гаманців і акаунтів у соціальних мережах включають до заповіту багато жителів Великої Британії для того, щоб після смерті людини члени її родини або друзі змогли отримати доступ до сторінок і профілів померлої особи на поштових сервісах, у соціальних мережах та інших сайтах. Дослідники з Лондонського університету стверджують, що кожен десятий житель Сполученого Королівства включає інформацію про паролі у свій заповіт [8].

Під анонімністю (від грец. anynimos – не має імені) в Інтернеті маються на увазі різні способи залишитися непоміченим у Всесвітній мережі. Якщо говорити про причини, які спонукають користувачів приховувати свої дії на Інтернет-сайтах, то вони досить різноманітні – скільки користувачів, стільки і причин, від законного використання права на приватність, зафіксованого в ст. 32 Конституції України, до бажання приховати особисту інформацію, маючи протиправну мету. Крім того, частішають випадки незаконного стеження в мережі Інтернет і кіберзлочинності.

Питання використання анонімності в мережі Інтернет постало наприкінці 80-х рр. XX ст., коли для її досягнення почали використовуватися псевдоніми й унікальні імена. На початку 90-х рр.

XX ст. з розвитком цифрових технологій почали з'являтися перші методи забезпечення анонімності в Інтернеті, наприклад, сервери-ремейлери, які пересилали отримані від відправників повідомлення електронною поштою і в процесі переадресації знищували всю інформацію про відправника. Сьогодні для забезпечення більш високого рівня анонімності в Інтернеті використовуються т. зв. анонімайзери – різні технічні засоби приховування інформації про Інтернет-користувача і його дії в Мережі. Це, зокрема, і проксі-сервери (до яких вдаються за необхідності приховати джерело Інтернет-запиту або відобразити неправдиву інформацію про користувача), і VPN-сервіси (що дозволяють користувачеві приховати реальну IP-адресу і самостійно обирати віртуальне місце розташування), і мережа I2P (яка працює поверх мережі Інтернет і використовує шифрування, що дозволяє зберігати анонімність сервера). Одним із найбільш надійних анонімайзерів вважається вільне (відкрите) програмне забезпечення Tor (системи проксі-серверів, що дозволяє встановлювати анонімне мережеве з'єднання, захищене від прослуховування) [9].

З погляду деяких дослідників, свобода передавати інформацію включає право на анонімне висловлювання думки; право утворювати групи, не розкриваючи імен членів цієї групи; право отримувати інформацію в приватному порядку. Вони вважають, що захист анонімності «життєво необхідний» для формування збалансованої громадської думки в країнах із низьким рівнем розвитку демократії. На їхню думку, можливість приховати свою особистість, якою користуються в Мережі т. зв. дисиденти, дозволяє їм висловлювати погляди меншості, «критично важливі для інформованого демократичного дискурсу». В іншому разі побоювання, що особистість може бути розкрита і що людина може піддатися переслідуванням за свої висловлювання, може змусити її взагалі відмовитися від висловлювань у політичних, етнічних, релігійних або інших міноритарних групах, а це позбавляє людину права на свободу власної думки [9].

Європейський суд з прав людини у рішенні від 16 червня 2015 р. у справі «Компанія DelfiAS проти Естонії» (скарга № 64569/09) зазначає, що в Інтернеті можливі різні градації анонімності. Інтернет-користувач може бути анонімним для широкого загалу, але відомим постачальникам послуг за даними облікового запису або контактної інформації про нього, що може або залишатися непідтвердженою, або підлягати певному контролю – від обмеженої перевірки (наприклад, шляхом активації облікового запису за адресою електронної пошти або через сторінку у соціальних мережах) до безпечної аутентифікації з використанням національних електронних посвідчень особи або даних про онлайн-ідентифікації клієнта банку, що дозволяє з більшою впевненістю встановити особу користувача. Постачальник послуг може також передбачити вищий ступінь анонімності для своїх користувачів. У цьому разі від користувачів не потрібно вимагати ніяких відомостей, їх можна встановити обмежено тільки за даними, що збереглися в Інтернет-провайдера. Зазвичай такі дані повідомляються лише на вимогу слідчих або судових органів, коли це необхідно для встановлення особи правопорушника та притягнення його до відповідальності [3].

Верхня палата французького парламенту прийняла закон про свободу спілкування, в якому позитивно оцінила анонімність діяльності суб'єктів в Інтернеті. Ще на стадії обговорення проекту зазначений закон викликав бурхливі дискусії, оскільки користувачі під час реєстрації у провайдера або у хостінговій компанії зобов'язувалися вказувати про себе лише правдиві відомості. У проекті закону передбачалося, що за достовірність цієї інформації повинні нести відповідальність як користувач, так і компанія, яка реєструє користувача. Під тиском правозахисних організацій до закону були внесені поправки, згідно з якими провайдер або хостінгова компанія повинні вимагати від користувача зазначати правдиві дані про себе, але не зобов'язані перевіряти їх достовірність [10].

Протилежної думки – про необхідність заборони анонімності в Інтернеті – дотримується Парламент Ізраїлю. Кнесет прийняв закон, який вимагає від власників Інтернет-сайтів не давати користувачам можливості залишати коментарі без попередньої реєстрації. Депутати вважають, що заборона анонімних коментарів дозволить скоротити кількість судових розглядів про захист честі, гідності та ділової репутації [10]. Противники анонімності в Інтернеті вважають, що її слід тримати під суворим державним і громадським контролем і ставитися до неї як до «інтелектуальної отруйної речовини» найвищого рівня небезпеки, «призначаючи» її тільки «за життєвими показаннями». Зважаючи на те, що анонімність і загальнолюдські цінності є несумісними явищами, оскільки анонімність за своєю сутністю – це відхід від відповідальності, а використання анонімності як засобу захисту персональних даних, в т. ч. таємниці приватного життя, є підміною моральних орієнтирів, видається, що в майбутньому акценти світової спільноти в оцінці анонімності повинні зміщатися у бік її постійного обмеження [11].

Аналітики дослідницької групи Deloitte регулярно публікують результати досліджень про основні тенденції поширення інформації в галузі телекомунікацій, вважаючи, що необмежена

«свобода» в Інтернеті, яка породжується анонімністю користувачів, «провокує шахрайство, різні форми якого зустрічаються в Мережі все частіше. Тому в майбутньому авторизація користувачів для проведення транзакцій через Інтернет повинна стати обов'язковою» [12].

Величезні «можливості» цифрових технологій із безповоротним входженням Інтернету в життя людини, на жаль, допомагають кіберзлочинцям втручатися в приватне життя, порушуючи право на недоторканність приватного життя, тому варто звернути особливу увагу на такий вид незаконних дій в Інтернеті, як кіберпереслідування. Сучасні програми-шпигуни дозволяють відстежувати будь-які дії людини, що здійснюються на комп'ютері або в мобільному телефоні, надаючи переслідувачам величезні можливості й інформацію. Основними видами кіберпереслідувань є: стеження, погрози, крадіжки, знищення або зміна ідентифікаційних даних, а також експлуатація неповнолітніх осіб, включаючи сексуальні домагання. Кіберпереслідування можуть набувати різних форм – публікацій у соцмережах викривлених, наклепницьких або приватних відомостей, недоречного звернення, настирливого вторгнення в життя людини і членів її сім'ї з використанням електронної пошти, SMS-повідомлень, телефонних дзвінків, крадіжок, несанкціонованого використання відомостей про особисте життя людини і багато іншого, але загальна ознака, незалежно від форми переслідування, – це небажані, часто нав'язливі і завжди незаконні дії. Наслідки таких дій є руйнівними для особи, яка стала жертвою кіберпереслідування (знищені сімейні і дружні відносини, зруйнована кар'єра, зіпсована репутація, підірваний авторитет). Часто переслідування тривають і в реальному житті, тоді людині може навіть загрожувати фізична небезпека.

Висновки. У сучасному глобалізованому суспільстві більшість відносин здійснюються засобами Інтернету, тому саме правове регулювання повинно стати базовим соціальним регулятором, основою якого є визнання принципів пріоритету прав і свобод людини, адекватного і виправданого державного контролю, забезпечення вибору опцій, що дозволяють захистити конфіденційність та анонімність інформації, забезпечити мінімізацію збору й обробки персональних даних, реалізація яких не дозволить створити глобальну інформаційну базу, де об'єктами нагляду будуть не тільки злочинці.

Список використаних джерел:

1. Руководство ЕС по правам человека в области свободы выражения мнений в интернете и вне его. Документ SN 10232/14 от 18 мая 2014 г. URL: https://eeas.europa.eu/sites/eeas/files/eu_human_rights_guidelines_on_freedom_of_expression_online_and_offline_ru.pdf.

2. Всестороннее исследование проблемы киберпреступности. Проект. Организация Объединенных Наций, февраль 2013 г. URL: https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime_Study_Russian.pdf.

3. Рішення ЄСПЛ від 16 червня 2015 р. у справі «Компанія «Делфі АС» (Delfi AS) проти Естонії» (скарга № 64569/09). URL: http://unba.org.ua/assets/uploads/publications/publikacii/2016-03-10.echr.internet.drozdov.pdf.

4. Основные аспекты укрепления инклюзивных обществ знаний. Доступ к информации и знаниям, свобода выражения мнений, неприкосновенность личной жизни и этические аспекты глобального Интернета. Заключительное исследование. Париж, ЮНЕСКО, 2015. URL: http://unesdoc.org/images/0023/002325/232563r.pdf.

5. Горный Е. Виртуальная личность как жанр. Лаборатория сетевой литературы. URL: http://ww.netslova.ru/gorny/vl.html.

6. Сухорольський М.П. Право на анонімність як суттєвий елемент прав людини. Правова інформатика. 2013. № 1 (37). С. 39–48.

7. Перчаткина С.А., Черемисинова М.Е., Цирин А.М., Цирина М.А., Цомартова Ф.В. Социальные интернет-сети: правовые аспекты. Журнал российского права. 2012. № 5. С. 14–24.

8. Середа В.Н., Середа М.Ю. Защита прав и свобод человека и гражданина в сети Интернет: монография. Воронеж: Издательско-полиграфический центр «Научная книга», 2013. 252 с.

9. Рандл М., Конли К. Задачи инфоэтики в области нейтральных технологий. Этические аспекты новых технологий: обзор. Изд. на рус. яз. М.: «Права человека», 2007. 100 с.

10. Рішення ЄСПЛ від 16 червня 2015 р. у справі «Компанія Delfi AS проти Естонія» скарга № 64569/09). URL: https://cedem.org.ua/library/delfi-as-proty-estoniyi-delfi-as-v-estonia/.

11. Жарова А.К. Право и информационные конфликты в информационно-телекоммуникационной сфере: монография. М: Янус-К, 2016. 248 с.

12. Серьогін В.А. Право на анонімність як елемент прайвесі. Науковий вісник Ужгородського національного університету. 2014. Вип. 24. Т. 1. С. 154–159.