УДК 341.231.14

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ У СУЧАСНОМУ СВІТІ

PROTECTION OF PERSONAL DATA IN THE MODERN WORLD

Прохазка Г.А.,
кандидат юридичних наук,
асистент кафедри теорії та історії держави і права
Полтавського юридичного інституту
Національного юридичного університету імені Ярослава Мудрого

Захист персональних даних належить до правил, які стосуються регулювання, зберігання та використання особистої конфеденційної інформації про осіб, яка може збиратися щодо них державними або приватними організаціями або іншими особами. Право на захист персональних даних розглядається у контексті права людини на приватне життя або у виправданих очікуваннях захисту конфіденційності.
Ключові слова: право на приватне життя, міжнародне право, права людини, особиста конференційна інформація, інтернет.

Защита персональных данных относится к правилам, которые касаются регулирования, хранения и использования личной конфиденциальной информации о лицах, которая может собираться о них государственными или частными организациями или другими лицами. Право на защиту персональных данных рассматривается в контексте права человека на личную жизнь или в оправданных ожиданиях защиты конфиденциальности.
Ключевые слова: право на личную жизнь, международное право, права человека, личная конфиденциальная информация, интернет.

Privacy law refers to the laws that deal with the regulating, storing, and using of personally identifiable information of individuals, which can be collected by governments, public or private organizations, or other individuals. Privacy laws are considered within the context of an individual's privacy rights or within reasonable expectation of privacy.
Key words: individual's privacy rights, international law, human right, personally identifiable information, internet.

Забезпечення доступу до інтернету і підтримання свободи використання інтернет-ресурсів є одним із показників зрілості суспільства і якості демократичних інститутів сучасної держави. Поширення новітніх технологій поступово замінюють собою звичайні способи зв'язку, що, своєю чергою, вимагає детальної правової регламентації і є сучасною проблемою глобалізованого світу.

Наявність права доступу до інтернету, свободи обміну інформацією в сучасному світі ніхто не заперечує. З іншого боку, враховуючи наявні ризики, загрозу терористичних атак, цілком очевидно, що державами будуть здійснюватися кроки, спрямовані на обмеження цього права, у будь-якому разі, недопущення його абсолютизації. Проблема захисту персональних даних в Україні є малодослідженою і представлена в працях В. Лутковської [1], О. Золотар [5], а також М.В. Бема, І.М. Городиського, Г. Саттона, О.М. Родіоненка [15]. Саме тому метою статті є подальша теоретична розробка сутності захисту персональних даних, з'ясування взаємозв'язку відповідного права і загальних інтересів суспільства і держави.

Світова мережа інтернету давно втратила свою ознаку, як тільки результату технологічного прориву XX ст. Це, насамперед, соціальна мережа, яка поєднує мільйони людей і досі будується за стихійним принципом. Ще кілька років тому ніхто не думав про можливість появи інтернету речей і інших благ інтернет-технологій.

Здійснюючи пошук інформації, ми з огляду на технічні особливості програм, які використовуємо, з огляду на специфіку законодавства інших країн, в яких перебуває постачальник послуг, змушені поширювати інформацію про своє місцеперебування, стать, вік, інтереси, уподобання. Цю інформацію, яка складається фактично із персональних даних, провайдери мають право збирати й обробляти, а в окремих випадках − передавати третім особам. Зрозуміло, що правовими актами держав можуть встановлюються обмеження із поширення персональних даних, проте довести незаконне використання цієї інформації надзвичайно складно, особливо в Україні. Широка судова практика в нашій державі відсутня.

Разом із тим заслуговують на окрему увагу приклади, які були наведені Уповноваженим Верховної Ради України В. Лутковською про зафіксовані випадки порушення права на приватність в мережі Інтернет, коли сайтом «Миротворець» оприлюднювалися персональні дані журналістів вітчизняних і закордонних засобів масової інформації, нібито акредитованих незаконними збройними формуваннями, включаючи адреси, номери мобільних телефонів, місця роботи. На запит Уповноваженого Верховної Ради з прав людини Національною поліцією тільки було повідомлене, що триває досудове розслідування в кримінальному провадженні за ст. 182 КК України [1, с. 80−82].

Приклади можливого неправомірного використання персональних даних наведені у прийнятій 07.03.2018 р. Комітетом Міністрів Ради Європи Рекомендації CM/Rec (2018) 2 державам-учасницям про роль і зобов'язання інтернет-посередників, в якій,

зокрема, зазначалося, що інтернет сприяє збільшенню ризиків і порушень, пов'язаних з особистим життям, стимулює поширення певних видів переслідування, ненависті, підбурювання до насилля, зокрема на основі статі, раси, релігії, які складно долаються виправним і судовим переслідуванням. На думку Комітету Міністрів Ради Європи, через зловживання з'явилися серйозні проблеми щодо підтримання суспільного порядку, національної безпеки, запобігання злочинності, діяльності правоохоронних органів, а також для захисту інших осіб, включаючи захист права інтелектуальної власності [2].

Свобода вираження поглядів і інформації в сучасному міжнародному праві прав людини розуміється як можливість для індивіда без будь-яких обмежень шукати, отримувати та поширювати відомості поза будь-якими формами втручання держави в особі уповноважених нею органів. Саме свобода поширення поглядів і інформації має тільки ті обмеження, які випливають із реалізації прав і свобод інших суб'єктів.

Так, обмеженню на законодавчому рівні підлягають заклики до будь-яких проявів насилля, створення загрози національній безпеці та чинному правопорядку, порушення прав інтелектуальної власності, авторського права. Також певні обмеження можуть встановити власники або розпорядники інтернет-ресурсів, оскільки вони мають права на володіння або використання послуг. В останньому разі провайдери мають зобов'язання поінформувати споживачів інтернет-ресурсу про встановлені обмеження щодо контенту.

Вищезазначене пов'язується з тим, що в мережі Інтернет провайдерами було створену середовище, яке можна персоніфікувати через специфіку наданих послуг, а інтернет виступає як віртуальна платформа для таких послуг. На спілкування, пересилання кореспонденції, інтернет речей поширюються норми національного права держав щодо захисту права власності або права розпорядження такими ресурсами, а також міжнародні угоди, директиви, рекомендації щодо захисту персональних даних.

З позиції дотримання права на обмеження доступу до персональних даних найскладнішими є ситуації, за яких такі дані обробляються регулярно і поза відомом власників. Наприклад, це складно проконтролювати під час використання браузерів, електронної пошти, передачі голосових повідомлень через використання різних пошукових систем. Практично неможливо визначити, яка інформація обробляється і кому може бути передана через особливості роботи самих ресурсів, обсяги обробленої інформації, недостатню обізнаність з особливостями роботи в інтернеті самих користувачів. До того ж постачальники інтернет-послуг можуть розташовувати своє технічне обладнання на території інших держав, з іншою специфікою національного права і за відсутності ратифікації міжнародних угод щодо зобов'язань із захисту персональних даних.

Про складність поставленої задачі із забезпечення захисту персональних даних свідчить розроблена Радою Європи Стратегія гендерної рівності на 2018−2023 рр., у п. 44 якої визначена важливість медіа і соціальних мереж щодо обміну інформації, проте підкреслено, як ці мережі можуть бути неправомірно спрямовані проти дотримання прав жінок і дівчат, у плані різних форм насильства, і свобода поглядів там часто використовується для зловживань і прикриття неприйнятної та образливої поведінки щодо жіночої статі [3].

Одним із профільних міжнародно-правових документів щодо захисту персональних даних в інтернет-мережі є Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних, прийнята Радою Європи 28 січня 1981 р., і, до речі, ратифікована Україною 6 липня 2010 р., у ст. 6 якої зазначається, що персональні дані, які свідчать про расову приналежність, погляди або переконання, дані, що стосуються здоров'я або статевого життя, не можуть піддаватися автоматизованій обробці, якщо внутрішнє законодавство не забезпечує відповідних гарантій. Додається, що зазначене правило також застосовується до персональних даних, які стосуються засудження в кримінальному злочині [4].

Найбільш небезпечними у плані обмеження права на захист персональних даних є можливе поширення зловживань із боку правоохоронних органів, з огляду на необхідність підвищення протидії терористичним актам. Такі зловживання стають можливими через бажання влади контролювати інтернет-ресурси і здійснювати моніторинг інформації, яка підпадає під ознаки приватної.

Певні кроки у цьому напрямі були зроблені через діяльність ENFOPOL (Enforcement Police) – системи електронного співробітництва держав-країн ЄС внаслідок прийняття резолюцій ENFOPOL-98 і ENFOPOL-19. Останні передбачали, починаючи з 1995 р., встановлення контролю за комунікаціями через отримання доступу до інформації, яку ми зазвичай вважаємо персональною (наприклад, статичні і динамічні IP-адреси, номери кредитних карток, електронні адресі тощо). Серед засобів отримання інформації також передбачалася змога встановити спеціальні програми, які б передавали необхідну інформацію правоохоронним органам.

Загалом уся система захисту персональних даних ЄС ґрунтувалася на Директиві 95/46/ЄС «Про захист фізичних осіб під час обробки персональних даних і про вільне переміщення таких даних» Європейського парламенту та Ради від 24.10.1995 р. та окреслювала межі правової регламентації захисту персональних даних у державах-членах ЄС. У подальшому країнами ЄС та США були розроблені нові нормативні акти щодо особливостей отримання, зберігання та поширення персональних даних.

Залежно від особливостей власного національного права державами напрацьовувалися норми, які і обмежують доступ до персональних даних, і закріплюють винятки правомірного поширення цих даних без волевиявлення власника.

Наприклад, із-поміж західних країн найбільш активно ідею обмеження захисту персональних даних підтримують США з причин як безпекового,

так і економічного характеру. Зокрема, О. Золотар у своїй монографії зазначає, що протягом історії США постійно опікувалися забезпеченням інформаційної безпеки країни, адже перший закон «Про захист інформації» був прийнятий США у далекому 1906 р., а інтенсивний розвиток відповідного законодавства розпочався тільки після появи комп'ютерної техніки. В подальшому у США було прийнято низку нормативних актів із цієї проблеми. Так, у 1974 р. у США прийнятий Акт про охорону персональних даних, який визначив категорію «право на приватність» як особисте і фундаментальне право, яке охороняється Конституцією США. О. Золотар зазначає, що повноваження поліції і федеральних агентств у подальшому були розширені Актом про боротьбу з тероризмом (Combating Terrorism Act) 2001 р., коли було скасовано необхідність отримання дозволу суду для прослуховування приватних переговорів і моніторингу мережі Інтернет. А з 2009 р., внаслідок прийняття кількох Актів про кібербезпеку, зокрема, передбачене повноваження Президента США відключати доступ до мережі Інтернет на всій території США у надзвичайних випадках через загрозу національної безпеки. О. Золотар додає, що у США завжди існувала певна перевага національних інтересів над приватними, хоча право на приватні дані в США підлягають належному захисту. Разом із тим із 2001 р. та у період 2009–2015 рр. було прийнято низку актів, які суттєво розширили повноваження органів державної влади та надавали доступ до приватної інформації семи державним органам, включаючи поліцію. Загалом у США було прийнято понад 300 актів щодо інформаційної безпеки здебільшого на федеральному рівні [5, с. 331–339].

Так, наприклад, у 2017 р. Палата представників Конгресу США в межах національного права скасувала закон, за яким інтернет-провайдери мали отримувати дозвіл на використання особистих даних користувачів, включаючи такі, які розкривали місце перебування користувача, історії його відвідування інтернет-ресурсів. Це було зроблено в інтересах великих компаній і викликало хвилю занепокоєння в американському суспільстві [6].

Про відмінності у нормативному підході США і ЄС до розуміння захисту персональних даних свідчать зміни в 2015 р., коли Суд Європейського Союзу скасував угоду «Безпечна гавань» (Safe Harbor). Вона давала змогу зберігати персональні дані і передавати їх США, оскільки саме там перебуває більшість серверів. У редакції угоди від 2016 р. між США та ЄС щодо трансатлантичного обміну даними спостерігається підвищення вимог до якості контролю за передачею спецслужбам такого типу інформації.

Приблизно з цього часу в ЄС починається робота зі зменшення ризиків порушення права на захист персональних даних, і з 25.05.2018 р. на території ЄС діє прийнятий 27.04.2016 р. Регламент Європейського Союзу про захист фізичних осіб стосовно обробки персональних даних та про вільне переміщення таких даних (General Data Protection Regulation), який став підтвердженням цінностей, що сповідує міжнародна спільнота після Другої світової війни.

Цікавою особливістю Регламенту є те, що його положення можуть бути поширені і на держави, які не входять до ЄС. Зокрема, це стосується суб'єктів господарювання, які здійснюють свою діяльність на території ЄС, не будучи там зареєстрованими, або отримали через таку діяльність доступ до персональних даних громадян ЄС чи дані інших осіб, якщо вони знаходяться на території ЄС.

Разом із тим у цьому документі (п. 19) зазначається, що за особливих обставин Регламентом державам може бути надана змога вводити обмеження щодо окремих обов'язків і прав у випадку, коли такі обмеження є необхідними і пропорційними для захисту особливо важливих інтересів у демократичному суспільстві, наприклад, для громадської безпеки, запобігання, виявлення та переслідування за скоєння кримінальних злочинів або виконання кримінальних покарань, у тому числі у разі запобігання загрозам громадської безпеки [7].

Разом із тим більш спеціалізованою, з точки зору наявності правової регламентації проблеми доступу до персональних даних саме представниками правоохоронних органів, є Директива (ЄС) 2016/680 «Про захист фізичних осіб у зв'язку з обробкою персональних даних компетентними органами з мметою попередження, розслідування, виявлення або переслідування кримінальних злочинів або виконання кримінальних покарань, та про вільне переміщення таких даних, і скасування Рамкового Рішення Ради 2008/977/ПВД» від 27.04.2016 р. [8], а також Директива (ЄС) 2016/681 «Про використання даних записів реєстрації пасажирів (PNR) для профілактики, виявлення, розслідування і судового переслідування злочинів терористичного характеру і тяжкого злочину від 27.04.2016 р. [9]. Зазначені Директиви, підкреслюючи права громадян на приватність, разом із тим визначають напрями обмеження цього права у зв'язку із потребами захисту інтересів суспільства від злочинних дій.

В Україні проблеми захисту персональних даних також потребують подальшої правової регламентації, зокрема у світлі збройного конфлікту на сході держави. Основу правової регламентації в державі становить ЗУ «Про захист персональних даних» від 01.07.2010 р., а також інші національні і, зокрема, міжнародні нормативно-правові акти, які ратифіковані Україною, і, за законом, останнім надається перевага відповідно до ч. 1 ст. 6 та ч. 2 ст. 29 цього Закону. В цьому є свої переваги і недоліки. З одного боку, нам відкривається доступ до напрацювань міжнародної спільноти, з іншого, застосовувати його ми можемо зі значними обмеженнями.

Наприклад, у ст. 7 Закону детально перераховані випадки щодо особливих вимог до обробки персональних даних, адже відповідно до ч. 7 обмеження захисту персональних даних поширюється на вироки суду, виконання завдань оперативно-розшукової або контррозвідувальної діяльності, боротьби з тероризмом та здійснення державним органом у межах його

повноважень, визначених законом. Законом визначені й інші особливі випадки обробки персональних даних, наприклад, у зв'язку зі згодою суб'єкта, станом його здоров'я у сфері трудових правовідносин тощо [10].

Ці питання значно детальніше врегульовані хоча б тим самим Регламентом ЄС від 27.04.2016 р. Проте і Регламент, і інші Директиви ЄС і США є внутрішніми документами цих суб'єктів і можуть бути застосовані Україною тільки за умови адаптації нашого національного права до європейських стандартів, що є справою часу. Це, своєю чергою, вимагає більш детальної регламентації захисту персональних даних на рівні національного права України, оскільки сама проблема є надзвичайно широкою, вона зачіпає проблеми протидії злочинності, захисту інформації в соціальних мережах, захисту інтересів окремих соціальних груп, забезпечення протидії дискримінації, трудові, соціальні, пенсійні, культурні, політичні і громадянські права людини та ін.

Складність порушеного питання може бути проілюстрована, зокрема, положеннями пп. 52−54 Регламенту ЄС від 27.04.2016 р. щодо опрацювання персональних даних у сфері охорони здоров'я людини. Наприклад, Регламентом ЄС закріплене поняття «суспільного здоров'я» і його складників, як-от стан здоров'я, включаючи захворюваність і недієздатність, потребу в послугах з охорони здоров'я, надання та універсальний доступ до охорони здоров'я, витрати на послуги з охорони здоров'я та їх фінансування, причини смертності. А опрацювання даних щодо стану здоров'я людини заради суспільних інтересів не має призводити до опрацювання персональних даних з іншою метою третіми сторонами, такими як працедавці або страхові компанії чи банківські установи [7].

З урахуванням широти проблеми і часу прийняття представляється, що застосування в Україні Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних та Додаткового протоколу до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних стосовно органів нагляду та транскордонних потоків даних від 28.01.1981 р., ратифікованої Україною 06.07.2010 р., для сучасних потреб є явно недостатніми [11]. Це відчувають і самі законотворці, намагаючись наздогнати ЄС через нормативне регулювання різних сфер застосування мережі Інтернет. Наприклад, через прийняття редакції ЗУ «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 р. [12].

Певна поверхневість національного права з цього питання може стати підставою для різних зловживань, використання персональних даних із метою отримання неправомірної вигоди, вчинення різних правопорушень і зловживань. Поява соціальних мереж і збільшення кількості населення, яке має доступ до інтернету, загострила проблему обізнаності наших громадян із правилами поведінки, як із власними персональними даними, так і з обробкою цих даних із боку юридичних осіб і органів державної влади. Право людини знати, як і де її персональні дані обробляються і хто з третіх осіб буде їх використовувати, в нашій державі не захищено повноцінно, що є однією з актуальних проблем сучасності України.

На нашу думку, доцільно було б на національному рівні розробити рекомендації фізичним особам щодо поводження в інтернеті, хоча б за зразком Рекомендації NR (99) 5 Комітету Міністрів державам-членам Ради Європи «Про захист недоторканності приватного життя в Інтернеті» від 23.02.1999 р., в якій викладені принципи забезпечення недоторканності приватного життя для користувачів та постачальників послуг інтернету [13].

До речі, великі компанії в Україні, у тому числі телемедійні, вже нині на своїх сайтах встановлюють політику конфіденційності та захисту персональних даних, визначають обсяги та характер інформації, яка обробляється, а також цілі, терміни зберігання її, умови передачі третім особам, місце зберігання інформації і права суб'єктів персональних даних, за практикою, що є поширеною в країнах Західної Європи і тільки починає отримувати визнання в Україні [14].

На думку М.В. Бема, І.М. Городиського, Г. Саттона, О.М. Родіоненка, обмеження обробки персональних даних у світлі статей Закону України «Про захист персональних даних» від 01.07.2010 р. загалом можливе, тільки якщо: 1) передбачене законом; 2) необхідне/пропорційне; 3) переслідує одну з легітимних цілей – національної безпеки, економічного добробуту або захисту прав і свобод суб'єктів персональних даних чи інших осіб [15, с. 99].

На підставі вищевикладеного ми можемо зробити висновки, що з усіх інформаційних джерел саме Інтернет-мережа є найбільш масштабним ресурсом поширення інформації, яка містить конференційні дані про особу. З огляду на правові і технічні особливості функціонування Інтернет-мережі оператори отримують і зберігають персональні дані своїх користувачів на серверах, що подекуди розташовані на території інших держав і підпорядковані їхньому національному праву. Разом із поширенням таких явищ, як кіберзлочинність, використання Інтернет-мережі для вчинення інших тяжких злочинів, злочинів, які посягають на функціонування державних установ, приватних компаній, життя, свободу, власність і особисту безпеку фізичних осіб, принижують їх людську гідність або передбачають вчинення терористичних атак, на такі види інформації державами можуть бути встановлені обмеження щодо захисту персональних даних.

Встановлення обмежень на захист персональних даних мали бути в розумних межах на підставі санкціонованого рішення повноважного судді. Представляється небезпечним надання такого доступу до персональних даних у позасудовому порядку, навіть правоохоронним органам. Розширене тлумачення права на доступ цієї інформації може бути використане для невиправданого втручання в приватне життя людини. Україна має визначити, яку модель захисту персональних даних вона готова обрати −

країн ЄС чи США і будувати власне законодавство у гармонії з нормами міжнародного права і власних зобов'язань. Адаптація норм права ЄС із питань захисту персональних даних разом із тим вимагає більш досконалого його опрацювання на національному рівні, оскільки низка Директив ЄС не поширюється на інші країни, а обсяги правової регламентації охоплюють політичні, економічні, соціальні, культурні аспекти дотримання прав людини, спільнот, юридичних осіб і держав.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Лутковська В. Щорічна доповідь Уповноваженого Верховної Ради України з прав людини про стан дотримання прав і свобод людини і громадянина в Україні. Права людини. Київ, 2017. 627 с.

2. Recommendation CM/Rec (2018) 2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries (Adopted by the Committee of Ministers on 7 March 2018 at the 1309th meeting of the Ministers' Deputies). URL: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=0900001680790e14.

3. Стратегія гендерної рівності Ради Європи на 2018−2023 рр. 51 с. URL: https://rm.coe.int/strategy-en-2018-2023/16807b58eb

4. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних від 28.01.1981 р. URL: http://zakon.rada.gov.ua/laws/show/994_326.

5.Золотар О. Інформаційна безпека людини: теорія і практика: монографія. Київ: «Тов. Видавничий дім «АртЕк», 2018. 446 с.

6. Конгресс США отменил закон о защите данных в интернете. BBC NEWS. Русская служба. URL: https://www.bbc.com/russian/news-39428662.

7. Регламент Європейського парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних) [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/984_008-16

8. On the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data and repealing Council Framework Decision 2008/977/JHA: Directive (EU) 2016/680 of the European Parliament and of the Council, of 27 April 2016. URL: https:///eur-lex.europa.eu/legalcontent/en/TXT/%3Furi%3DCELEX%253A32016L0680&prev=search.

9. On the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime: Directive (EU) 2016/681 of the European Parliament and of the Council, of 27 April 2016. URL: https://consilium.europa.eu/en/ press/press-releases/2016/04/21-council-adopts-eu-pnr-directive/&prev=search.

10. Про захист персональних даних: Закон України від 1.07.2010 р. URL: http://zakon.rada.gov.ua/laws/show/2297-17

11. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних та Додатковий протокол до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних стосовно органів нагляду та транскордонних потоків даних від 28.01.1981 р. URL: http://zakon.rada.gov.ua/laws/show/994_326

12. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. URL: http://zakon.rada.gov.ua/laws/show/2163-19

13. Рекомендація NR(99) 5 Комітету Міністрів державам-членам Ради Європи «Про захист недоторканності приватного життя в Інтернеті» від 23.02.1999 р. URL: http://zakon.rada.gov.ua/laws/show/994_357

14. ТСН. Політика конфіденційності та захисту персональних даних. URL: https://tsn.ua/privacy-policy

15. Захист персональних даних: Правове регулювання та практичні аспекти: науково-практичний посібник / М.В. Бем, І.М. Городиський, Г. Саттон, О.М. Родіоненко. К.: К.І.С., 2015. 220 с.