

Бліхар М. М.,*докторка юридичних наук, професорка,
завідувачка кафедри адміністративного та інформаційного права
Національного університету «Львівська політехніка»*

ПРАВОВІ ОСНОВИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В ІНТЕРНЕТІ

Анотація. У статті проаналізовано наявні правові основи захисту персональних даних в Інтернеті. Сьогодні захист персональних даних саме в інтернеті є актуальним як ніколи; цьому сприяє, перш за все, діджиталізація суспільства, отримання людиною можливостей вчинення чималої кількості необхідних у щоденному житті дій через інтернет, у найпростішому значенні – використання інтернету – здатність комунікувати з людьми по всьому світу. Однак поряд із отриманням нових можливостей, перед людиною виникають і нові загрози, що з'явилися у процесі розвитку людського суспільства як негативна реакція на ті чи інші нововведення. Однією з таких загроз є несанкціоноване розповсюдження та використання персональних даних в мережі інтернет, що окрім моральних, може мати й негативні правові наслідки для того, чий персональні дані було поширено або використано. Попри наявність законодавчої бази, одержувачі персональних даних не завжди або не в повному обсязі або вибірково дотримуються вимог закону. Саме тому проблема захисту персональних даних в мережі інтернет стосується як суб'єкта персональних даних, одержувача персональних даних, так і держави. Щобільше, поряд із технічними можливостями захисту персональних даних особа також має знати свої права та обов'язки, пов'язані з захистом персональних даних та відновлення своїх порушених прав юридичним шляхом. Обумовлено, що суб'єкти відносин, пов'язаних із персональними даними, зобов'язані забезпечити захист цих даних від незаконної обробки, а також від незаконного доступу до них. Обґрунтовано, що дуже частою причиною такої ситуації слугує найперше низький рівень цифрової обізнаності користувачів мережі інтернет щодо наявних правових та технічних способів захисту власних персональних даних. У багатьох людей відсутні елементарні знання щодо способів та засобів захисту персональних даних з метою недопущення їх використання без особистої на те згоди. Насамперед людина – користувач інтернету, чітко має знати, що таке персональні дані, та які є законодавчі гарантії захисту персональних даних та способи їх забезпечення. Відповідальність за захист персональних даних лежить як на користувачеві інтернету, так і на одержувачі персональних даних. Роль держави у цьому процесі полягає у створенні нормативно-правової бази та забезпеченні її ефективного функціонування для захисту персональних даних в інтернеті.

Ключові слова: гарантії захисту персональних даних, закон, персональні дані, правові засоби захисту персональних даних, цифрові технології.

Постановка проблеми. Розвиток суспільства сприяє щоразу більшому залученню людини до мережі інтернет. Чимало необхідних та іноді і юридично значимих дій сьогодні

можна зробити в мережі. Однак поряд із цим зростає і рівень небезпеки для користувачів інтернету, а найбільшою загрозою постає недостатній рівень захисту персональних даних користувачів.

Означена проблема не стосується лише безпосередньо користувача інтернету як володільця персональних даних, які можуть бути несанкціоновано використані та мати негативні морально-психологічні та юридичні наслідки для особи. Вона повинна вирішуватися комплексно: володільцем персональних даних, який має володіти необхідним мінімумом знань про персональні дані та технічно захистити їх у своїх персональних кабінетах чи акаунтах; одержувачами персональних даних – компаніями, з якими «комунікує» володільць персональних даних і надає їм згоду на обробку та використання в межах, визначених законодавством. Вони повинні забезпечити максимальний захист баз персональних даних осіб від несанкціонованого поширення; держава – як гарант захисту персональних даних, який створює правовий механізм захисту персональних даних та відновлення порушених прав, пов'язаних із несанкціонованим їх поширенням або використанням.

Стан дослідження. Досягнення поставленої мети передбачає аналіз праць дослідників, тих хто тією чи іншою мірою вивчав проблематику різних механізмів захисту персональних даних. Посилання на їхні праці та розробки будуть подані у тексті наукової розвідки з обґрунтуванням основ, що стали теоретико-методологічним підґрунтям цієї статті. З огляду на це, *мета статті* полягає у дослідженні правових основ захисту персональних даних в Інтернеті.

Виклад основного матеріалу. Сьогодні, попри певні напрацювання у цій сфері, у кожній з груп є чимало проблем, пов'язаних із захистом персональних даних. У пересічних користувачів мережі інтернет відсутні часто елементарні знання про можливості захисту своїх персональних даних. Компанії та організації різних форм власності, які володіють базами персональних даних, часто не використовують усі наявні механізми для їх захисту від несанкціонованого використання або відкрито ними нехтують. Держава ж як гарант захисту персональних даних має формувати більш актуальні норми законодавства, покликані ефективніше реагувати на виклики, що з'являються з розвитком суспільства та відповідних інформаційних технологій.

Так, у 2021 році було проведено дослідження двадцяти провідних технологічних компаній, які працюють на ринку України, на предмет захисту персональних даних їх клієнтів [1]. Дослідники вивчили сайти таких компаній, як: ПрАТ «Київстар» – Kyivstar.ua; ТОВ «Лайфселл» – Lifecell.ua; ПрАТ «ВФ Україна» – Vodafone.ua ПрАТ «ДАТАГРУП» – DataGroup.ua; ТОВ

«ТРИОЛАН» – Triolan.com; ТОВ «РОЗЕТКА.УА» – Rozetka.com.ua; ТОВ «УАПРОМ» – Prom.ua; ТОВ «ЄМАРКЕТ УКРАЇНА» / OLX Global BV – Olx.ua; Український інтернет-холдинг ТОВ «Укрнет» – Ukr.net; ТОВ «Нова Пошта» – NovaPoshta.ua; ТОВ «КОМФІ ТРЕЙД» – Comfy.ua; ТОВ «ГК «ФОКСТРОТ»» – Foxtrot.ua; ТОВ «ІД ЕЛЬДОРАДО» – Eldorado.ua; ТОВ «ЗТ-ІНВЕСТ» – Citrus.ua; ТОВ «АЛЛО» – Allo.ua; MAKEUP GLOBAL/ТОВ «Мейкап» – Makeup.com.ua; ТОВ «КАСТА ГРУП» – Kasta.ua; ТОВ «СІЛЬПО-ФУД» – Silpo.ua; ТОВ «Заказ Юкрейн» – Zakaz.ua; ТОВ «ЛАНЕТ ТЕЛЕКОМ» – Lanet.ua. Метою дослідження став аналіз політики компаній щодо дотримання цифрових прав користувачів з акцентом на захисті персональних даних.

Висновки дослідження є наступними: «1. Найкращі результати серед 20 досліджуваних компаній продемонстрували Olx.ua з показником 77,5%, Ukr.net та Foxtrot.ua з показником 70% балів кожна з максимально можливих 100% як відображення стану корпоративної політики приватності та захисту персональних даних користувачів.

2. Водночас навіть для Olx.ua, Ukr.net та Foxtrot.ua є простір для вдосконалення своєї корпоративної політики, зокрема в аспектах дотримання принципу мінімізації даних, які вони збирають про користувачів (Olx.ua), публікації попередніх версій політики конфіденційності на сайтах (Olx.ua, Ukr.net), надання можливості користувачам отримати копію своїх персональних даних, зазначення часових меж відповідей на запити користувачів (Ukr.net).

3. Щонайменше 50% максимальної кількості балів отримали 12 із 20 приватних компаній за критерієм захисту персональних даних. Корпоративну політику цих компаній оцінюють як середнього та вищого від середнього рівня в контексті забезпечення дієвого захисту персональних даних своїх клієнтів. До цих компаній увійшли Kyivstar.ua, Comfy.ua, Allo.ua, Kasta.ua, Prom.ua, NovaPoshta.ua, Vodafone.ua, Zakaz.ua, Citrus.ua та вже згадані Olx.ua, Ukr.net та Foxtrot.ua.

4. Згаданим компаніям варто звернути увагу на дотримання принципу мінімізації даних, які вони збирають про користувачів, на публікацію політики конфіденційності в простій та доступній формі на своєму сайті, на чітке прописання процесу передавання даних третім особам тощо.

5. 8 із 20 компаній, обраних для дослідження, набрали менше ніж 50% балів з максимально можливих, що свідчить про нижчий за середній рівень захисту персональних даних, відображених у корпоративній політиці. Серед них – Eldorado.ua, DataGroup.ua, Lifecell.ua, Rozetka.com.ua, Makeup.com.ua, Silpo.ua, Lanet.ua і Triolan.com.

6. Більшість із зазначених компаній мають значні недоліки в чотирьох категоріях дослідження – від дотримання вимог національного законодавства до зручності користування сайтом та інклюзивності. Менеджменту цих компаній варто переглянути корпоративну політику приватності та захисту персональних даних, розробити й реалізувати план з посилення політики конфіденційності.

7. На сайтах 4 компаній (Vodafone.ua, Silpo.ua, Triolan.com, Lanet.ua) немає відмітки для користувача про надання дозволу на оброблення його персональних даних, хоча це одна з вимог законодавства.

8. 10 досліджуваних компаній не інформують своїх користувачів, впродовж якого часу ці компанії зберігатимуть інформацію про користувача.

9. На сайтах 4 компаній (Triolan.com, Makeup.com.ua, Silpo.ua, Lanet.ua) користувачі не мають можливості видалити свої збережені особисті дані.

10. 15 досліджуваних компаній не описують умов видалення аккаунту користувача після припинення договору / за умов некористування аккаунтом.

11. 10 досліджуваних компаній не вказують, де та як вони зберігають дані користувачів (розташування серверів)» [1].

Таблиця 1

Індекс захисту персональних даних

Назва компанії	Дотримання вітчизняного законодавства про персональні дані, %	Дотримання європейських стандартів щодо персональних даних, %
ПрАТ «Київстар»	60	33,3
ТОВ «Лайфселл»	50	3,8
ПрАТ «ВФ Україна»	40	33,3
ПРАТ «ДАТАГРУП»	50	58,3
ТОВ «ТРИОЛАН»	10	0
ТОВ «РОЗЕТКА.УА»	50	41,6
ТОВ «УАПРОМ»	90	75
ТОВ «ЄМАРКЕТ УКРАЇНА» / OLX Global BV	80	83,3
Український інтернет-холдинг ТОВ «Укрнет»	100	75
ТОВ «Нова Пошта»	80	41,6
ТОВ «КОМФІ ТРЕЙД»	70	41,6
ТОВ «ГК «ФОКСТРОТ»»	80	75
ТОВ «ІД ЕЛЬДОРАДО»	50	50
ТОВ «ЗТ-ІНВЕСТ»	80	50
ТОВ «АЛЛО»	70	66,7
MAKEUP GLOBAL/ТОВ «Мейкап»	70	50
ТОВ «КАСТА ГРУП»	70	50
ТОВ «СІЛЬПО-ФУД»	30	25
ТОВ «Заказ Юкрейн»	80	66,7
ТОВ «ЛАНЕТ ТЕЛЕКОМ»	20	16,7

Отже, дані дослідження демонструють проблеми компаній одержувачів персональних даних у сфері захисту персональних даних в інтернеті, які сьогодні наявні. Попри наявність законодавчої бази, одержувачі персональних даних не завжди або не в повному обсязі або вибірково дотримуються вимог закону. Саме тому проблема захисту персональних даних в мережі інтернет стосується як суб'єкта персональних даних, одержувача персональних даних, так і держави.

Найперше саме особа, котра надає свої персональні дані стороннім фізичним чи юридичним особам, має попіклуватися про їх елементарний захист. Користувач інтернету (суб'єкт персональних даних) з метою захисту своїх персональних даних повинен: знати, що відноситься до персональних даних; ставити надійні паролі на свої особисті кабінети чи аккаунти; користуватися тільки перевіреними сайтами, на яких передбачено проставлення відмітки на згоду про обробку персональних даних; завжди уважно читати документ про надання згоди на обробку персональних даних (обов'язково має бути зазначено, яка саме інформація збирається та як буде використовуватися; умови, за яких інформація може бути передана третім особам; передбачена можливість видалення своїх даних користувачем; стислий та зрозумілий опис політики конфіденційності компанії).

Найбільше часу користувачі інтернету проводять у соціальних мережах, де розповідають про себе та знаходять чимало інформації про інших. Ця інформація також відноситься до персональних даних. Тому завжди варто розуміти, що опублікована інформація може бути використана іншими особами. Сьогодні усі соціальні мережі та месенджери мають функцію збереження інформації з інших аккаунтів чи облікових записів. Тобто навіть після видалення тих чи інших своїх публікацій, записів ви не можете бути впевнені, що дана інформація видалена назавжди, адже хтось міг її зберегти (хоча у соціальних мережах зараз розроблені відповідні інструменти, де можна переглянути, хто зберігав ті чи інші публікації, фото- та відеоматеріали).

При встановленні нових програм на свій комп'ютер або телефон доцільно завжди перевіряти розділ «Налаштування», де можна обмежити обсяг даних для збору та опрацювання, заборонити перегляд матеріалів певній категорії користувачів соціальних мереж чи месенджерів.

Якщо людина не планує більше користуватися певною соціальною мережею, персональним кабінетом на сайті конкретної компанії, необхідно повністю видалити свій обліковий запис. Також при зміні пристрою потрібно видалити свої персональні дані, щоб вони не потрапили до наступного власника пристрою.

Усі ці поради є скоріше технічними моментами, яких необхідно дотримуватися з метою захисту персональних даних. Це той необхідний мінімум дій, який необхідно здійснити суб'єкту персональних даних для збереження персональних даних від несанкціонованого використання.

У 2019 та 2021 роках було проведено загальнонаціональне опитування рівня цифрової грамотності населення України [7]. Що стосується рівня обізнаності про можливості захисту своїх даних в інтернеті, то: з 2019 року почастишали випадки шахрайських дій в мережі Інтернет (у середньому на 11% збільшилась кількість людей, які за останні 12 місяців зазнавали проблем, пов'язаних із безпекою, через використання Інтернету);

найпоширенішими неправомірними діями в мережі Інтернет, з якими стикаються люди, як і у 2019 році залишаються отримання шахрайських повідомлень, перенаправлення на підблені веб-сайти із запитом особистої інформації та шахрайське використання кредитної чи дебетової карти; серед базових курсів підвищення рівня цифрової грамотності найбільшим попитом користуються: онлайн безпека; швидкий та якісний пошук інформації в мережі Інтернет; розрізнення надійних та ненадійних джерел інформації; користування послугами Інтернет-банкінгу. Тобто українці бажають підвищити свій рівень цифрової грамотності найперше з метою безпеки – захисту своїх даних від несанкціонованого використання.

Поряд із технічними можливостями захисту персональних даних особа також має знати свої права та обов'язки, пов'язані з захистом персональних даних та відновлення своїх порушених прав юридичним шляхом.

В Україні правовими основами захисту персональних даних в мережі інтернет є Конституція України, Закон України «Про захист персональних даних», Кримінальний кодекс України, Цивільний кодекс України, рішення Конституційного Суду України, міжнародні нормативно-правові акти, згода на обов'язковість використання яких надана Верховною Радою України, зокрема Регламент Європейського Парламенту і Ради (ЄС) 216/679 від 27.04.2016 р. про захист фізичних осіб при обробці персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних).

У статтях 21, 31, 32 Конституції України йдеться, що усі люди є вільні і рівні у своїй гідності та правах. Права і свободи людини є невідчужуваними та непорушними. ... Ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України. Не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини [2]. Кожному гарантується право на захист від втручання в особисте життя, таємницю листування, телефонних розмов, кореспонденції (також і електронних листів). Дія цих правових норм поширюється також і на відносини в мережі інтернет та виступає базою для подальшої розробки та вдосконалення вітчизняного законодавства у сфері захисту персональних даних в мережі інтернет.

Закон України «Про захист персональних даних» [3] є основним нормативно-правовим актом, який регулює правові відносини, пов'язані із захистом і обробкою персональних даних, і спрямований на захист основоположних прав і свобод людини і громадянина, зокрема права на невтручання в особисте життя, у зв'язку з обробкою персональних даних.

У Законі наголошено, що особисті немайнові права на персональні дані, які має кожна фізична особа, є невід'ємними і непорушними. Кожному гарантується право на захист своїх персональних даних від незаконної обробки та випадкової втрати, знищення, пошкодження у зв'язку з умисним приховуванням, ненаданням чи несвоєчасним їх наданням, а також на захист від надання відомостей, що є недостовірними чи ганьблять честь, гідність та ділову репутацію фізичної особи. Особа має право звертатися з питань захисту своїх прав щодо персональних даних до органів державної влади, органів місцевого самоврядування, до повноважень яких належить здійс-

нення захисту персональних даних, а також застосовувати засоби правового захисту в разі порушення законодавства про захист персональних даних.

Кримінальний кодекс України [4] містить норми закону щодо захисту персональних даних в мережі інтернет. Так, статтею 163 передбачено кримінальну відповідальність за порушення таємниці кореспонденції, зокрема і такої, що передається через комп'ютер. Стаття 182 Кодексу визнає злочином незаконне збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди або поширення цієї інформації у публічному виступі, творі, що публічно демонструється, чи в засобах масової інформації. Особі, щодо якої було вчинено дії, визначені у цих статтях, гарантовано право на судовий захист.

У Цивільному кодексі України [5] персональні дані віднесено до особистих немайнових прав та визначено спосіб їх захисту від протиправних посягань у судовому порядку. Зміст особистого немайнового права становить можливість фізичної особи вільно, на власний розсуд визначати свою поведінку у сфері свого приватного життя.

Міжнародним нормативно-правовим актом у сфері захисту персональних даних у мережі інтернет згода на обов'язковість застосування якого надана Верховною Радою України, є Регламент Європейського Парламенту і Ради (ЄС) 216/679 від 27.04.2016 р. про захист фізичних осіб при обробці персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних) [6]. Розробники цього документа наголошують: «Стрімкий технологічний розвиток і глобалізація призводять до виникнення нових труднощів для захисту персональних даних. Масштаби збирання та спільного використання персональних даних суттєво зросли. Технології дозволяють як приватним компаніям, так і публічним органам користуватися персональними даними в безпрецедентних масштабах з метою реалізації своєї діяльності. Фізичні особи дедалі частіше надають доступ до персональної інформації для громадськості та в глобальному масштабі. Технології змінили як економіку, так і суспільне життя і повинні надалі стимулювати вільний рух персональних даних у межах Союзу та передавання їх до третіх країн і міжнародних організацій, забезпечуючи при цьому високий рівень захисту персональних даних. Такі зміни вимагають наявності міцних та більш узгоджених засад щодо захисту даних у Союзі, із запровадженням належного механізму виконання, беручи до уваги важливість формування довіри, що дозволить розвиток цифрової економіки на рівні внутрішнього ринку. Фізичні особи повинні мати контроль щодо власних персональних даних. Необхідно зміцнити правову та практичну визначеність для фізичних осіб, суб'єктів господарювання і органів публічної влади» [6].

Даний Регламент є реакцією європейської спільноти на актуальні виклики, що постали перед нею у зв'язку з розвитком інформаційних технологій та зростанням їх ролі в житті особи. Це є ще одним свідченням визнання людини, її прав та свобод найвищою цінністю для європейської правової сім'ї та пріоритетність їх забезпечення.

Висновки. Держава гарантує захист персональних даних, тобто створює всі умови для ефективного захисту та якнайшвидшого відновлення порушених прав особи, що пов'язані із персональними даними. Суб'єкти відносин, пов'язаних із персональними даними, зобов'язані забезпечити захист цих даних

від незаконної обробки, а також від незаконного доступу до них. Такі суб'єкти мають вчиняти сукупність правозначущих та технічних дій, спрямованих на максимально високий рівень захисту персональних даних в інтернеті. Врешті решт, сукупність аналізованих вище нормативно-правових актів складає правові основи захисту персональних даних в мережі інтернет. Разом вони покликані сформувати та гарантувати ефективний механізм для забезпечення інформаційної безпеки людини, мінімізації можливостей несанкціонованого використання персональних даних та швидкого відновлення порушених прав людини, пов'язаних із поширенням її персональних даних.

Література:

1. Індекс захисту персональних даних 2021. URL: <https://uadigital.report/index-of-personal-data-protection-2021.pdf> (дата звернення 03.05.2023).
2. Конституція України. URL: <https://zakon.rada.gov.ua/laws/show/254k/96-вр#Text>
3. Про захист персональних даних: Закон України від 1 червня 2010 р. № 2297-VI. URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text> (дата звернення 03.05.2023).
4. Кримінальний кодекс України. URL: <https://zakon.rada.gov.ua/laws/show/2341-14#Text> (дата звернення 03.05.2023).
5. Цивільний кодекс України. URL: <https://zakon.rada.gov.ua/laws/show/435-15#Text> (дата звернення 03.05.2023).
6. Регламент Європейського Парламенту і Ради (ЄС) 216/679 від 27.04.2016 р. про захист фізичних осіб при обробці персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних). URL: <https://ips.ligazakon.net/document/MU16144> (дата звернення 03.05.2023).
7. Цифрова грамотність населення України: звіт за результатами загальнонаціонального опитування. 2021. URL: https://osvita.dia.gov.ua/uploads/0/2625-doslidzenna_2021_ukr.pdf (дата звернення 03.05.2023).

Blikhar M. Legal basis of protection of personal data on the Internet

Summary. The article analyzes the available legal bases for the protection of personal data on the Internet. Today, the protection of personal data on the Internet is more relevant than ever; this is facilitated, first of all, by the digitalization of society, the ability of a person to perform a considerable number of actions necessary in daily life via the Internet, in the simplest sense – the use of the Internet – the ability to communicate with people all over the world. However, along with the acquisition of new opportunities, people face new threats that appeared in the course of the development of human society as a negative reaction to certain innovations. One of such threats is the unauthorized distribution and use of personal data on the Internet, which, in addition to moral ones, may have negative legal consequences for the person whose personal data was shared or used. Despite the existence of a legal framework, the recipients of personal data do not always or not fully or selectively comply with the requirements of the law. That is why the problem of protecting personal data on the Internet concerns both the subject of personal data, the recipient of personal data, and the state. At most, along with the technical possibilities of personal data protection, a person should also know his rights and obligations related to the protection of personal data and the restoration of his violated rights by legal means. It is stipulated that the subjects of relations related to personal data are obliged to ensure the protection of this data from illegal processing, as well as from illegal access to it. It is substantiated that the very frequent cause of such a situation

is, first of all, the low level of digital awareness of Internet users regarding the available legal and technical methods of protecting their personal data. Many people lack elementary knowledge about ways and means of protecting personal data in order to prevent their use without personal consent. First of all, a person – an Internet user – must clearly know what personal data is, and what are the legal guarantees of personal

data protection and ways to ensure them. Responsibility for the protection of personal data lies both on the Internet user and on the recipient of personal data. The role of the state in this process is to create a legal framework and ensure its effective functioning for the protection of personal data on the Internet.

Key words: personal data protection guarantees, law, personal data, legal means of personal data protection, digital technologies.