

# МІЖНАРОДНЕ ПРАВО ПРАВ ЛЮДИНИ

---

---

УДК 347.2/3  
DOI

**ГУЙВАН П. Д.,**  
кандидат юридичних наук, професор,  
заслужений юрист України,  
докторант  
Національного юридичного університету імені Ярослава Мудрого

## МІЖНАРОДНИЙ ДОСВІД ЗАХИСТУ ЧУТЛИВИХ КАТЕГОРІЙ ПЕРСОНАЛЬНИХ ДАНИХ

**Анотація.** Ця робота присвячена науковому аналізу стану міжнародного та національного законодавства в сфері регулювання обробки та захисту чутливих персональних даних. Дано визначення вказаної категорії особистої інформації. В роботі підкреслюється, що оскільки обробка таких специфічних відомостей може нанести значної матеріальної і моральної шкоди суб'єктові даних, вона можлива у виняткових випадках, коли держава запроваджує певні гарантії, прописані у законі. Досліджено міжнародні та зарубіжні національні правові акти у цій галузі юридичної регламентації. Встановлено, що міжнародне законодавство детально напрацювало, а правозастосовна практика Європейського суду з прав людини ефективно використовує юридичний інструментарій здійснення основних процедур щодо обробки інформації особистого характеру. Особливо ретельно регламентовано порядок передачі даних іншим особам, у тому числі транскордонного характеру, а також під час здійснення правоохоронної діяльності. При цьому міжнародне законодавство виходить із принципу, що поширення даних про приватне життя фізичної особи, тобто передання її іншим особам без узгодження з людиною, яка є суб'єктом інформації, припускається лише у чітко встановлених законом випадках. Ретельно досліджене законодавство Європейського Союзу в частині застосування принципу, згідно з яким обробка чутливих персональних даних, таких як відомості про здоров'я громадян, про підозру у скоєнні злочину, про наявність звинувачень та застосування запобіжних заходів, а також здійснення операцій стосовно оцінки здібностей, поведінки людини або щодо обмеження її прав, у тому числі за договором, становить певну загрозу правам і свободам особи. В статті зроблений правовий аналіз конкретних правозастосовних рішень у досліджуваній сфері, які винесені Європейським судом з прав людини щодо застосування ст. 8 Конвенції про

захист прав людини і основоположних свобод 1950 року. Вказані конкретні недоліки українського правотворення та правозастосування, розроблені рекомендації стосовно удосконалення діяльності української правової системи у даній царині.

**Ключові слова:** чутливі персональні дані, обробка і захист особистої інформації.

**Постановка проблеми.** Основним правовим актом у галузі обороту та захисту персональних даних є міжнародна Конвенція про захист осіб стосовно автоматизованої обробки даних особистого характеру. Даний документ обов'язковий для усіх країн, що ратифікували його, у тому числі України. У ньому персональні дані визначаються як будь-яка інформація про визначену або таку, що може бути визначеною, особу (суб'єкта даних) (ст. 2). Вказане формулювання закріплене у практично такому ж вигляді в усіх внутрішніх законодавчих актах країн-учасників у цій сфері регулювання. Знайшло воно своє відтворення і у Законі України «Про захист персональних даних» 2010 року (далі Закон). Цей національний Закон визначає вичерпний перелік умов, за яких уповноваженими особами може здійснюватися обробка персональних даних суб'єкта. Лише у вказаних випадках обробка даних матиме легітимний характер, в іншому разі – вона вважатиметься незаконною. Власне, за позицією Закону, який, зокрема, встановлює зміст основних дефініційних понять, обробка персональних даних – це будь-яка дія або сукупність дій, таких як збирання, реєстрація, накопичення, зберігання, адаптування, зміна, поновлення, використання і поширення (розповсюдження, реалізація, передача), знеособлення, знищення персональних даних, у тому числі з використанням інформаційних (автоматизованих) систем (ст. 2). Як бачимо, згідно з позицією цього закону поняття «захист персональних даних» не охоплюється визначенням їхньої обробки, а розглядається як окрема правова категорія. Певні проблеми виникають, коли слід надати юридичну характеристику таким процесам, як поновлення, використання і поширення (розповсюдження, реалізація, передача), знеособлення, знищення персональних даних, у тому числі з використанням інформаційних систем. В національному правовому полі їх прийнято кваліфікувати як різновиди обробки приватної інформації про особу. Водночас наразі відсутні конкретні правові механізми здійснення вчинків у кожній із цих операцій. Однак міжнародне законодавство детально напрацювало, а правозастосовна практика Європейського суду з прав людини ефективно використовує юридичний інструментарій здійснення кожної із названих процедур щодо інформації особистого характеру. Особливо ретельно регламентовано порядок передачі даних іншим особам, у тому числі транскордонного характеру [1, ст. 7]. При цьому міжнародне законодавство виходить із принципу, що поширення даних про приватне життя фізичної особи, тобто передання її іншим особам без узгодження з людиною, яка є суб'єктом інформації, припускається лише у чітко встановлених законом випадках.

Обробка даних про приватне життя конкретної особи повинна здійснюватися у такий спосіб, аби в процесі виключалася можливість несанкціонованого доступу чи використання та втрати або знищення інформації. В значній кількості випадків, коли персональні дані стосуються особливо важливих аспектів життєдіяльності людини, після використання їх задля досягнення відповідної легітимної мети вони мають знищуватися володільцем і ні в якому разі не використовуватися для інших цілей всупереч інтересам особистості. На сьогоднішній день персональні дані є інформацією у електронно-орієнтованій чи каталоговій формі, яка містить відомості про приватне життя індивідуума, що може бути ідентифікований на основі цієї інформації. При цьому суб'єкт даних зі стандартною чутливістю повинен усвідомлювати, що ці дані про нього мають конфіденційний характер і не призначені для публічного поширення [2, с. 6].

**Аналіз останніх досліджень і публікацій.** Питанням дослідження правової природи обробки персональних даних присвятили свої праці такі науковці, як К. Беляков, Р. Калюжний, І. Городиський, Р. Чанишев, О. Волков, А. Чернобай, А. Тунік, В. Брижко, І. Забара, А. Пазюк, В. Цимбалюк, М. Швець та інші. У вказаних роботах розглядаються різні аспекти обробки та захисту персональних даних, аналізується міжнародний досвід правового регулювання даних відносин, проблематика належної організації інформаційного суспільства в Україні, здійснення державної та міжнародної інформаційної політики тощо. Проте у національних та зарубіжних доктринальних дослідженнях ще недостатньо уваги приділяється питанням специфічності обробки окремих персональних даних, зокрема, в контексті їхньої підвищеної важливості для гарантування невіддільного права особи на приватність. Отже, **метою статті** є вивчення чинного українського та міжнародного законодавства у сфері регламентації правового інструментарію обробки та передачі окремих видів інформації про особу, а також аналіз наявної правозастосовної практики. Буде запропоновано необхідні кроки для подальшого поступу нашого суспільства в напрямку справедливого захисту найбільш вразливих даних про людину.

**Виклад основного матеріалу.** Вже у 1981 році у статті 6 Конвенції Ради Європи Про захист осіб у зв'язку з автоматизованою обробкою персональних даних була започаткована диференціація окремих видів персональних даних за ознакою їхньої важливості для суб'єкта та ризиків і загроз йому у разі їх неправомірного поширення. Таким чином, з'явилося поняття чутливих персональних даних, збір, обробка, використання та передача яких або взагалі заборонена, або вимагає спеціальних заходів безпеки і захисту. Інакше кажучи, у разі відсутності прямої заборони обробка цих категорій персональних даних здійснюється в спеціальному порядку, який окремо регламентується законом. Зокрема, Конвенція встановила, що персональні дані, які належать до расової належності, політичних поглядів або релігійних та інших переконань, не можуть підлягати автоматизованій обробці, якщо внутрішнє законодавство не встановлює відповідних гарантій. Тобто,

оскільки обробка таких специфічних відомостей може нанести значної матеріальної і моральної шкоди суб'єктові даних, їхня обробка можлива у виняткових випадках, коли держава запроваджує певні гарантії, прописані у законі.

Надалі, внаслідок прийняття Директиви 95/46/ЄС Європейського Парламенту і Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» 1995 року, із загального переліку персональних даних були виділені спеціальні групи так званих чутливих особистих відомостей, обробка яких має значну специфіку і дозволяється лише у чітко визначених випадках [3, ст. 8]. До категорії даних, обробка яких взагалі заборонена, вказані правові акти відносять персональні дані про расове або етнічне походження, політичні, релігійні або філософські переконання. Спеціальний правовий режим обороту особистої інформації із забезпеченням ефективних державних гарантій застосовується під час обробки і поширення даних про членство в політичних партіях та професійних спілках, засудження до кримінального покарання, а також даних, які стосуються здоров'я, статевого життя, а також біометричні або генетичні дані. Ця позиція також відображена у Положенні (ЄС) 2016/679 Європейського Парламенту та Ради від 27 квітня 2016 року про захист фізичних осіб стосовно обробки персональних даних та щодо вільного переміщення таких даних та скасування Директиви 95/46 / ЄС [4]. Вказана концепція також імплементована до українського національного Закону (ст. 7).

Загальні принципи обробки чутливих даних у Європейському Союзі конкретизуються у численних підзаконних актах, які регулюють правила відповідної діяльності у різних галузях. Важливим актом, який регулює особливості взаємин між учасниками в сфері поширення персональних даних, є Рекомендація Комітету Міністрів ЄС № R (91) 10 «Щодо передачі третім особам інформації особистого характеру, яка знаходиться в розпорядженні органів влади» [5]. Цей акт ґрунтується на принципі поваги до приватного життя та захисту даних. При цьому наголошується, що повідомлення, зокрема засобами електронного зв'язку, даних особистого характеру чи файлів з даними особистого характеру третім сторонам має супроводжуватися гарантіями, що приватне життя суб'єкта даних не буде порушуватися в незаконному порядку. Зокрема, дані особистого характеру та файли з такими даними не повинні повідомлятися третім сторонам, окрім випадків, коли: а) це передбачено спеціальним законом; або б) громадськість має доступ до них відповідно до правових положень, що регулюють доступ до інформації публічного сектору; або с) повідомлення здійснюється відповідно до національного законодавства про захист інформації; або d) суб'єкт даних вільно та поінформовано надав свою згоду. Якщо нормами національного права не передбачено забезпечення належних гарантій суб'єкта даних, дані особистого характеру або файли з даними особистого характеру не можуть повідомлятися третім сторо-

нам для цілей, що не відповідають тим, для яких ці дані були зібрані (п. 2). При цьому особлива увага надається застереженням, які повинні враховуватися під час поширення даних чутливого характеру. Вони не мають зберігатися у файлі чи частині файлу, загальнодоступних третім сторонам. Будь-які винятки з цього принципу мають бути чітко передбачені законом із забезпеченням відповідних гарантій суб'єктові даних (п. 3).

Окремі Рекомендації КМ ЄС присвячені питанням врегулювання відносин щодо збору та обробки персональних даних під час здійснення правоохоронної діяльності. До прикладу, можемо назвати Рекомендацію № R(87)15 Комітету Міністрів державам-членам, що регулює використання персональних даних у секторі поліції [6] (схвалена 17 вересня 1987 на 410-й зустрічі заступників Міністрів). Згідно з цим актом збір персональних даних у цілях поліції повинен обмежуватися тією мірою, яка необхідна для відвернення реальної небезпеки чи припинення кримінального правопорушення особливого характеру. Будь-який виняток з цього положення повинен бути предметом спеціального національного законодавства. Якщо дані про індивіда були зібрані і зберігаються без його відома, і якщо дані не знищені, він повинен бути поінформований, у разі доцільності, що інформація про нього тримається як тільки предмет діяльності поліції більше не цікавить її (п. 2.2). Збір даних за допомогою технічних чи інших автоматизованих засобів може здійснюватися лише відповідно до правових положень, збір даних про осіб лише на тій підставі, що вони мають особливе расове походження, особливі релігійні переконання, сексуальну поведінку чи політичні погляди або належать до особливих рухів чи організацій, які не оголошені поза законом, повинен заборонятися. Збір даних, що торкаються цих питань, може здійснюватися у разі виняткової потреби для цілей конкретного розслідування (Принцип 2).

Власне, у законодавстві Європейського Союзу вже давно напрацьований та застосовується принцип, згідно з яким обробка чутливих персональних даних, таких як відомості про здоров'я громадян, про підозру у скоєнні злочину, про наявність звинувачень та застосування запобіжних заходів, а також здійснення операцій стосовно оцінки здібностей, поведінки людини або щодо обмеження її прав, у тому числі за договором, становить певну загрозу правам і свободам особи. Тож, усі подібні операції підлягають попередній перевірці Уповноваженим ЄС з повідомленням Офіцера із захисту даних [7, с. 101]. У зарубіжних національних законодавствах про захист та охорону персональних даних критерій чутливості використовується задля віднесення деяких видів особистої інформації до категорій даних, взагалі заборонених до обробки, або тих, що потребують під час обробки підвищених заходів захисту. При цьому внутрішній закон або містить пряму вказівку на віднесення конкретної групи даних до певної категорії, або наділяє представників влади (зазвичай міністра, котрий курує національний орган із захисту даних, іноді прем'єр-міністра) повноваженнями щодо прийняття оперативних рішень з цього питання [8, с. 164].

Перелік особистих даних, що вважаються чутливими і потребують особливого ретельного захисту у площині їхнього збирання, обробки та поширення у різних країнах визначається національними традиціями, менталітетом населення, культурними та релігійними звичаями тощо. Тож, він може бути неоднаковим у різних суспільствах. Водночас є загальні правила, які діють у всіх країнах демократичної орієнтації, які визначені конвенційними принципами та включають до вразливої інформації дані про расове та етнічне походження, релігійну та гендерну самоідентифікацію, політичні уподобання, участь у професійних та соціальних організаціях, кримінальну історію, включаючи давно минулі часи, стан здоров'я та сексуальну поведінку.

Оскільки чинні нормативні акти, як національного, так і міжнародного характеру, не в змозі детально встановити винятковий перелік найбільш вразливих блоків інформації про особисте життя людини (тим більше, що в конкретних ситуаціях одна і та ж інформація для окремих суб'єктів може бути чутливою, чи ні), в науковій літературі напрацьовані певні бачення з цього питання. Так, на загальнотеоретичному рівні чутливими персональними даними прийнято зазначати інформацію про арешти, кредитні історії та звіти, трудову діяльність в частині оцінки професійних здібностей і ділових якостей працівника, банківську інформацію, медичні та податкові дані. Найбільш вдало критерій чутливості персональних даних сформульовано оксфордським науковцем Раймондом Уексом: «Персональна інформація могла б визначатися як ті факти, повідомлення чи думки, які пов'язані з даною особою та стосовно яких можна було б чекати, що суб'єкт вважає їх інтимними чи конфіденційними, і, відповідно, бажає зупинити або принаймні обмежити їхню циркуляцію» [9, с. 31].

Окремі дослідники, виходячи з критеріїв чутливості особистої інформації, поділяють її на номінативну та іншу. При цьому як номінативні постулюються відомості, що дозволяють ідентифікувати конкретну особу (прізвище, ім'я, по батькові, стать, серія та номер паспорта, дата і місце народження тощо). Серед номінативних даних особливе місце займає вразлива інформація про біометричні персональні дані, тобто відомості, що характеризують фізіологічні та біологічні особливості людини, на основі яких можна встановити її особистість. До неномінативних даних належить персональна інформація, що має додатковий, факультативний характер і може також залежно від обставин та особистого сприйняття її важливості суб'єктом бути віднесеною до чутливої чи ні. Це відомості про доходи, місце роботи, політичні погляди, медичні захворювання, наявність судимості тощо [10, с. 18]. Як бачимо, у цілій низці практичних ситуацій віднесення персональної інформації до розряду чутливої вирішальним чином залежить від суб'єктивного сприйняття її такою конкретною людиною та від усвідомлення нею факту можливого порушення права на приватність внаслідок обробки та поширення цих відомостей. Такий підхід вважаємо досить виваженим та справедливим, отже, він має враховуватися під час

конструювання відповідного нормативного механізму і особливо під час судового правозастосування.

Виходячи із викладеного вище, дуже важлива роль у юридичному опосередкуванні обороту чутливих персональних даних належить правозастосовній практиці. Позаяк українська правова система у плані судової практики щодо вирішення спорів даної спрямованості нічим не може похвалитися, мусимо взяти до уваги міжнародні правозастосовні рішення, зокрема ті, що винесені Європейським судом з прав людини щодо застосування ст. 8 Конвенції про захист прав людини і основоположних свобод 1950 року. Так, у рішеннях по конкретних справах ЄСПЛ вказує, що такі поняття, як гендерна ідентифікація, ім'я, сексуальна орієнтація та статеве життя, потрапляють до сфери, що захищається статтею 8 Конвенції [11, п. 47; 12, п. 57]. До особливо вразливих елементів приватного життя належить інформація щодо стану здоров'я особи [13, п. 71]. Суд вважає, що до них також належать відомості щодо етнічного походження особи [14, п. 41].

Показовою в сенсі гарантування особі судового захисту щодо недоторканості її права на приватність в частині охорони персональних даних є справа «Авілкіна та інші проти Росії» [15], розглянута Європейським судом з прав людини 6 червня 2013 року. У ній заявниці стверджували, що прокуратура вимагала від лікарів надати відомості, які містяться в їхніх медичних документах без їх згоди і за відсутності розслідування за кримінальною справою, яке могло б обґрунтувати одержання таких відомостей. Під час розгляду справи Суд наголосив, що захист персональних даних, у тому числі медичних відомостей, має фундаментальне значення для реалізації особою свого права на повагу до приватного і сімейного життя – права, гарантованого статтею 8 Конвенції. Дотримання конфіденційності відомостей про здоров'я є особливо важливим принципом правових систем всіх Держав – учасниць Конвенції. Передача таких відомостей може серйозно вплинути на приватне та сімейне життя громадян, а також на їхнє соціальне становище та трудову зайнятість, оскільки це робить їх об'єктом наруги та можливих гонінь. Дотримання конфіденційності даних про здоров'я має ключове значення не тільки для захисту приватного життя пацієнта, але й для збереження його довіри до медичних працівників і системи охорони здоров'я загалом. За відсутності таких гарантій захисту особи, які потребують медичної допомоги, можуть утриматися від звернення за необхідним лікуванням, піддаючи тим самим своє здоров'я небезпеці (п. 45). При цьому зазначено, що за компетентними державними органами повинна зберігатися певна свобода розсуду стосовно встановлення справедливого балансу між громадськими та приватними інтересами, які суперечать один іншому. Та ця свобода розсуду супроводжується європейським наглядом (п. 46), і її рамки залежать від таких факторів, як характер і значимість порушених інтересів, а також серйозність втручання.

Як було встановлено під час розгляду справи, заявниці не були підозрюваними або обвинуваченими за жодним кримінальним розслідуванням. Прокуратура лише проводила перевірку діяльності релігійної організації заявниць за одержаними зверненнями. Медичні установи, в яких заявниці проходили лікування, не повідомляли прокуратуру про жодні випадки стверджуваної злочинної поведінки. З урахуванням цих обставин Суд не побачив гострої соціальної потреби, яка б вимагала передачі відомостей, що становлять лікарську таємницю, про заявниць. Таким чином, Суд визнав, що заходи, вжиті прокуратурою під час проведення перевірки, не обов'язково повинні були мати настільки суворий характер відносно заявниць. Крім запиту про надання відомостей, які становлять лікарську таємницю, у прокуратури були й інші можливості для проведення перевірки за одержаними зверненнями. Наприклад, прокурор міг спробувати отримати згоду заявниць на передачу таких відомостей та/або з'ясувати думку заявниць з цього питання (див. вище, пункти 23 і 24 цього рішення). Незважаючи на це, прокуратура вирішила вимагати надання відомостей, які становлять лікарську таємницю, не повідомивши про це заявниць та не забезпечивши їм можливість висловити свою згоду або незгоду (п. 48). Суд також не побачив у тексті національних судових рішень, якими було відмовлено заявницям у задоволенні їхніх вимог, жодних вказівок на те, що національні органи влади спробували встановити справедливий баланс між правом заявниць на повагу до їхнього приватного життя та діяльністю прокуратури, спрямованою на захист здоров'я населення та прав громадян у цій сфері. Державні органи також не навели відповідних та достатніх мотивів у якості обґрунтування передачі конфіденційних відомостей. Вищевказаних міркувань достатньо для того, щоб Суд дійшов висновку, що збір прокуратурою відомостей, які становлять лікарську таємницю, щодо заявниць, не супроводжувався належним захистом, що дозволяє запобігти передачі цих даних, у порушення принципу поваги до приватного життя заявниць. Відповідно, мало місце порушення статті 8 Конвенції з огляду на надання медичних документів заявниць для цілей прокурорської перевірки (п. 51, 53).

У справі «С та Марпер проти Сполученого Королівства» [14] ЄСПЛ під час вирішення спору використав правило національного закону – Акту про захист персональних даних Великої Британії [Data Protection Act] (був прийнятий 16 липня 1998 р.) [16] стосовно того, що «вразливі персональні дані» означають відомості особистого характеру, які включають, серед іншого, дані про расову або національну приналежність суб'єкта даних, скоєння (ймовірне скоєння) ним будь-якого злочину або про провадження за справою, відкритою за фактом скоєного (ймовірно скоєного) ним злочину, про завершення такого провадження або про покарання, призначене судом за скоєння цього злочину (ст. 2), а також керувався положеннями доповіді Наффілдської ради з біоетики (Nuffield Council on Bioethics) від 2007 року під заголовком «Використання біологічної інформації у судовій



експертизі: етичні проблеми» [17]. Це дало можливість Суду дійти висновку, що, беручи до уваги можливе подальше використання, серед іншого, зразків клітин, їх систематичне зберігання достатньо сильно зачіпає інтереси людини та може потягти за собою втручання держави у реалізацію права на повагу до приватного життя. Тож, Суд вважає побоювання людини стосовно можливого подальшого використання інформації приватного характеру, яка зберігається, правомірними та вважає, що вони повинні враховуватися під час вирішення питання про наявність втручання держави у реалізацію конвенційних прав. Дійсно, беручи до уваги швидкі темпи розвитку генетики та інформаційних технологій, Суд не може виключити ймовірність того, що в майбутньому стане можливим втручання держави в приватне життя шляхом використання генетичної інформації по-новому або такими способами, які сьогодні неможливо точно передбачити (п. 70, 71). З урахуванням викладеного ЄСПЛ дійшов висновку, що зберігання зразків клітин та профілів ДНК свідчить про втручання держави в права заявників на повагу до їхнього приватного життя за змістом положень частини 1 статті 8 Конвенції.

У чинному українському Законі про захист персональних даних також є норма, присвячена загальним засадам обробки чутливих відомостей про особу. У ч. 2 ст. 7 Закону передбачена обробка чутливих категорій даних, якщо вона, зокрема: 1) здійснюється за умови надання суб'єктом персональних даних однозначної згоди на обробку таких даних; 2) необхідна для здійснення прав та виконання обов'язків володільця у сфері трудових правовідносин відповідно до закону із забезпеченням відповідного захисту; 3) необхідна для захисту життєво важливих інтересів суб'єкта персональних даних; 5) необхідна для обґрунтування, задоволення або захисту правової вимоги; 6) необхідна в цілях охорони здоров'я, встановлення медичного діагнозу, для забезпечення піклування чи лікування або надання медичних послуг за умови, що такі дані обробляються медичним працівником або іншою особою закладу охорони здоров'я, на яку покладено обов'язки щодо забезпечення захисту персональних даних та на якого поширюється законодавство про лікарську таємницю; 7) стосується вироків суду, виконання завдань оперативно-розшукової діяльності, боротьби з тероризмом та здійснюється державним органом в межах його повноважень, визначених законом.

Сама наявність даних положень у національному законодавстві є позитивним чинником. Але для того, аби вони практично запрацювали, слід продовжувати правотворчу діяльність у напрямку конкретизації та деталізації правил обробки та поширення чутливих персональних даних. У такий спосіб має бути усунена двозначність та розмитість загальних правил ч. 2 ст. 7 Закону. Наприклад, навіть попри те, що він передбачає для обробки наявність однозначної згоди особи, наразі не визначені ні форми такої згоди, ні порядку та строку її отримання. Також потребує додаткового детального нормативного тлумачення правило про

віднесення до складу чутливих відомостей, необхідних для обґрунтування, задоволення або захисту правової вимоги. Таке «гумове» визначення може застосовуватися різнобічно і містить реальні можливості для зловживань з боку, наприклад, слідчих органів або суду під час прийняття рішення про залучення певної інформації до матеріалів справи в ході провадження.

З проведеного дослідження можемо зробити наступні **висновки**. Національне законодавство, принаймні в частині нормування обробки чутливих персональних даних, страждає декларативністю, фрагментарністю, недостатньою чіткістю, конкретністю та не узгоджується з європейським правовим регулюванням. Основними напрямками вдосконалення національного законодавства у цій сфері повинні бути його конкретизація та деталізація. Правові приписи стосовно підвищеного захисту персональних даних чутливого характеру мають узгоджуватися з принципами європейського регулювання у цій царині та вдосконалюватися, наближаючись до положень міжнародних стандартів.

Крім заходів юридичної регламентації вчинення конкретних дій щодо обробки чутливих даних, необхідно також напрацювати заходи технічної та організаційної охорони таких відомостей, які перебувають у державних та недержавних інформаційних системах для запобігання несанкціонованому доступу, пошкодженню чи знищенню чутливих даних або використанню їх в протизаконних цілях. Мають бути також запроваджені досить жорсткі санкції за подібні порушення у зв'язку з підвищеною важливістю для особи та необхідністю більш прискіпливої уваги з боку законодавця та усвідомленням державою серйозності суспільної небезпеки порушення правил обробки вразливої інформації.

#### *Література:*

1. Регламент (ЄС) №45/2001 Європейського Парламенту і Ради від 18 грудня 2000 року стосовно захисту осіб з точки зору обробки персональних даних установами та органами Спільноти та вільного руху таких даних. URL: <https://www.dst.dk/ext/454209204/0/>.
2. Иванский В.П. Теоретические проблемы правовой защиты частной жизни в связи с использованием информационных технологий : автореф. дисс. ... канд. юрид. наук. Москва, 1998. 26 с.
3. Директива 95/46/ЄС Європейського Парламенту і Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» від 24 жовтня 1995 року. URL: [http://zakon3.rada.gov.ua/laws/show/994\\_242](http://zakon3.rada.gov.ua/laws/show/994_242).
4. Положення (ЄС) 2016/679 Європейського Парламенту та Ради від 27 квітня 2016 року про захист фізичних осіб стосовно обробки персональних даних та щодо вільного переміщення таких даних та скасування Директиви 95/46 / ЄС (Загальні положення про захист даних) URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN>.
5. Рекомендація № R (91) 10 Щодо передачі третім особам інформації особистого характеру, яка знаходиться в розпорядженні органів влади Схвалено Комітетом міністрів 9 вересня 1991 року. URL: <http://cedem.org.ua/>

- library/rekomendatsiya-r-91-10-shhodo-peredachi-tretim-osobam-informatsiyi-osobystogo-harakteru-yaka-znahodytsya-v-rozporyadzhenni-organiv-vlady/.
6. Рекомендацію № R(87)15 Комітету Міністрів державам-членам, що регулює використання персональних даних у секторі поліції від 17 вересня 1987 року. URL: [http://cyberpeace.org.ua/files/rekomendacia\\_km\\_radi\\_evropi\\_sodo\\_vikoristanna\\_personal\\_nih\\_danih\\_sektori\\_policii.pdf](http://cyberpeace.org.ua/files/rekomendacia_km_radi_evropi_sodo_vikoristanna_personal_nih_danih_sektori_policii.pdf)
  7. Кашкин С.Ю. Право Европейского Союза. Москва : Проспект, 2005. 331с.
  8. Иванский В.П. Правовое регулирование персональных данных в законодательстве зарубежных государств. *Вестник РУДН, серия Юридические науки*, 2012, № 1. С. 156–168.
  9. Wacks Raymond Protection of Privacy. *Modern Legal Studies*. London : Sweet & Maxwell, 1980. 205 p.
  10. Братановский С.Н. Специальные правовые режимы информации. Саратов : Научная книга, 2010. 172 с.
  11. Рішення ЄСПЛ від 6 лютого 2001 року (остаточне від 6 травня 2001 року) у справі «Бенсаїд проти Сполученого Королівства» (Bensaid v. the United Kingdom), заява № 44599/98, URL: <http://www.asylumlawdatabase.eu/sites/www.asylumlawdatabase.eu/files/aldfiles/Bensaid%20v%20United%20Kingdom%20%28Application%20no.%2044599-98%29.pdf>.
  12. Рішення ЄСПЛ від 28 січня 2003 року (остаточне від 28 квітня 2003 року) у справі «Пек проти Сполученого Королівства» (Peck v. the United Kingdom), заява № 44647/98, URL: <https://www.juridice.ro/wp-content/uploads/2016/07/Peck-v-UK-ECHR-28-Jan-03.pdf>.
  13. Рішення ЄСПЛ від 25 лютого 1997 року у справі «З проти Фінляндії» (Z v. Finland), заява № 22009/93. URL: <https://swarb.co.uk/z-v-finland-echr-25-feb-1997/>.
  14. Рішення ЄСПЛ від 4 грудня 2008 року у справі «С і Марпер проти Сполученого Королівства» (S. and Marper v. The United Kingdom), заяви № 30562/04 і 30566/04. URL: <https://rm.coe.int/168067d216>.
  15. Рішення ЄСПЛ від 26 травня 2016 року у справі «Авілкіна та інші проти Росії», заява № 1585/09. URL: <https://www.garant.ru/products/ipo/prime/doc/70431012/>.
  16. Акт про захист персональних даних Великої Британії (Data Protection Act), прийнятий 16 липня 1998 року. URL: <https://www.legislation.gov.uk/ukpga/1998/29/contents>.
  17. Доповідь Наффільдської ради з біоетики (Nuffield Council on Bioethics) від 8 вересня 2007 року «Використання біологічної інформації у судовій експертизі: етичні проблеми». The forensic use of bioinformation: ethical issues. Published by Nuffield Council on Bioethics 28 Bedford Square London WC1B 3JS. 139 p.

#### **Guyvan P. International experience in protecting sensitive categories of personal data**

**Summary.** This paper deals with the scientific analysis of the state of international and national legislation in the field of regulation of processing and protection of sensitive personal data. The definition of the specified category of personal information is given. The paper emphasizes that, since the processing of such specific information can cause significant material and moral damage to the data subject, it is possible only in cases where the state imposes certain guarantees prescribed by law. International and foreign national legal acts in the field of legal regulation are investigated. It has been established that international law has worked in detail, and the case law

of the European Court of Human Rights has effectively used the legal tools to carry out basic procedures for the processing of personal information. The procedure for transferring data to other persons, including cross-border ones, as well as for the implementation of law enforcement activities is particularly carefully regulated. However, international law proceeds from the principle that the dissemination of data on the private life of an individual, that is, transfer to other persons without consent with the person who is the subject of information, is only allowed in clearly defined cases by law. European Union law has been thoroughly investigated regarding the application of the principle that the processing of sensitive personal data, such as public health information, suspicion of a crime, the existence of charges and the use of precautionary measures, and the conduct of ability assessment operations, the conduct of a person or the restriction of his rights, including by contract, poses a certain threat to the rights and freedoms of the individual. The article makes a legal analysis of the specific enforcement decisions in the research area, made by the European Court of Human Rights regarding the application of Art. 8 of the 1950 Convention on the Protection of Human Rights and Fundamental Freedoms. The specific shortcomings of the Ukrainian law-making and law-enforcement are indicated, the recommendations on improvement of activity of the Ukrainian legal system in this field are developed.

**Key words:** sensitive personal data, processing and protection of personal information.