

**КАРДАШ А. В.,**  
аспірант кафедри конституційного  
права України  
(Національний юридичний університет  
імені Ярослава Мудрого)

УДК 342.7

## УПОВНОВАЖЕНИЙ ОРГАН У СФЕРІ ЗАХИСТУ ІНФОРМАЦІЇ ПРО ОСОБУ: ЗАРУБІЖНИЙ ДОСВІД

Світова практика у сфері захисту інформаційних прав особи доводить повсюдність створення спеціалізованих уповноважених органів, які б опікувалися цими питаннями. Сфера захисту інформації про особу тісно пов'язана з інформаційною сферою, а також сферою приватного (особистого та сімейного) життя, прайвесі. Саме тому такий уповноважений орган, спеціалізуючись на захисті інформації про особу, може мати ширшу компетенцію, здійснювати захист прайвесі загалом або ж мати також компетенцію у сфері захисту права на доступ до публічної інформації.

**Ключові слова:** права людини, захист інформації про особу, персональні дані, право на приватність, уповноважений орган у сфері захисту інформації про особу.

Мировая практика в сфере защиты информационных прав личности доказывает повсеместность создания специализированных уполномоченных органов, которые бы занимались этими вопросами. Сфера защиты информации о лице тесно связана с информационной сферой, а также сферой частной (личной и семейной) жизни, прайвесі. Именно поэтому такой уполномоченный орган, специализирующийся на защите информации о лице, может иметь более широкую компетенцию, осуществлять защиту прайвесі в целом или же иметь также компетенцию в сфере защиты права на доступ к публичной информации.

**Ключевые слова:** права человека, защита информации о лице, персональные данные, право на приватность, уполномоченный орган в сфере защиты информации о лице.

World practice in the field of protecting information rights of the individual proves the widespread creation of specialized agencies that would handle these issues. The scope of protection of personal information is closely linked to the information sphere, as well as to the sphere of private (personal and family) life, privacy. That is why such a body, specializing in the protection of personal information, may have wider competences, protect the privilege as a whole or have competence in the area of protecting the right to access public information.

**Key words:** human rights, protection of personal data, personal data, right to privacy, data protection authority.

**Вступ.** Світова практика у сфері захисту інформаційних прав особи доводить повсюдність створення спеціалізованих уповноважених органів, які б опікувалися цими питаннями. Якщо говорити про національні підходи зарубіжних і передусім європейських держав до інституціоналізації уповноважених органів щодо захисту інформації про особу (персональних даних), то вони доволі різноманітні.



Варто також наголосити, що сфера захисту інформації про особу тісно пов'язана з інформаційною сферою, а також сферою приватного (особистого та сімейного) життя, прайвесеі. Саме тому такий уповноважений орган, спеціалізуючись на захисті інформації про особу, може мати ширшу компетенцію, здійснювати захист прайвесеі загалом або ж мати також компетенцію у сфері захисту права на доступ до публічної інформації.

**Постановка завдання.** Окремі аспекти зазначеної проблематики відображено в працях таких учених, як О.В. Нестеренко, В.О. Серьогін, Ю.С. Теліна, Н.М. Тимченко й інші. Метою статті є з'ясування зарубіжного досвіду створення та діяльності уповноваженого органу у сфері захисту інформації про особу. Завданнями статті є розкрити стан правового регулювання уповноваженого органу у сфері захисту інформації про особу; порівняти повноваження уповноваженого органу у сфері захисту інформації про особу в зарубіжних країнах; висловити пропозиції щодо подальших змін у законодавстві України щодо вдосконалення інституту уповноваженого органу у сфері захисту інформації про особу.

**Результати дослідження.** Сьогодні інститут уповноважених із захисту персональних даних (наглядних органів) ґрунтується на принципах інституту омбудсмена і являє собою розвинену самостійну незалежну структуру, яка доповнює традиційні інститути державної влади [1, с. 127].

Традиційно існування такого уповноваженого органу у сфері захисту інформації про особу пов'язують із посадою спеціалізованого інформаційного омбудсмена. Посада інформаційного омбудсмена (уповноваженого) у світовій практиці є «наймолодшою», адже потреба у створенні спеціального інституту, що займався б виключно наглядом за дотриманням права людини та громадянина на інформацію, виникла лише наприкінці 70-х років ХХ ст., коли в міру розвитку й упровадження інформаційних технологій інформація перетворилась на окремий вид послуг, товар і навіть на владу. Інформація почала бути не тільки об'єктом правовідносин, а й перетворилась на підставу виникнення у громадян прав та обов'язків. Тому, відповідно, і постала проблема створення якісно нового інституту, який гарантував би забезпечення права на інформацію [2, с. 266]. Те саме можна сказати й про сферу приватного життя громадян (прайвесеі) [3, с. 277].

Загалом, що стосується такого органу, як спеціалізований омбудсман з питань інформації (інформаційний уповноважений), і якщо говорити ширше, спеціалізованих уповноважених, то їх роль і значення в системі захисту прав і свобод людини науковою спільнотою оцінюється неоднозначно [4, с. 206]. Так чи інакше інститут спеціального (інформаційного) омбудсмена вважається одним із дієвих механізмів дотримання прав громадян на інформацію [2, с. 265].

Уперше інститут уповноваженого щодо захисту персональних даних з'явився в 1970 році в Німеччині. Інститут Уповноваженого із питань захисту персональних даних (Bundesbeauftragter für den Datenschutz) почав формуватися в 1970 році, коли в Землі Гессен уперше у світі був прийнятий цільовий Закон «Про захист даних». Закон установив державну посаду Комісара із захисту даних на правах єдиноначальності. Цьому виборному державному службовцю закон надав право повної незалежності від владних структур (жоден орган виконавчої влади не може давати йому вказівки), а також надав право спостереження за діяльністю щодо персональних даних. Як наглядова, незалежна інстанція Комісар не несе прямої відповідальності за оброблення персональних даних. Він тісно співпрацює з Міністром поліції, який повинен доповідати йому про отримання подарунків [5, с. 29]. У 2006 році в ФРН з'явився Федеральний комісар із захисту даних уже на федеральному рівні [4, с. 218], а до цього ж існувала Федеральна комісія із захисту персональних даних (Virtuelles Datenschutzbüro), яка відповідає за виконання Федерального закону про захист даних 2001 року (Bundesdatenschutzgesetz).

Якщо говорити про інші країни, то в 1978 році у Франції створена Національна комісія інформатики і свободи (Commission National de Informatique et des Libertes). У 1979 році в Данії з'явився Danish Data Protection Agency (Datatilsynet) (Данське агентство із захисту даних), а в 1980 році – Datenschutzkommission (Агентство з інформатики та індивідуальних свобод) в Австрії.



Сьогодні практично в усіх державах-членах Ради Європи та Євросоюзу створені національні органи: Уповноважені щодо приватності (праву на недоторканність приватного життя) або спеціальні комісії чи агентства щодо захисту персональних даних, які здійснюють моніторинг застосування й забезпечення дотримання законодавства про захист персональних даних у межах своїх територій.

Кілька держав-членів (наприклад, Австрія, Нідерланди) призначили орган із захисту даних із загальною компетенцією й кілька наглядових органів в інших галузях (наприклад, у галузі охорони здоров'я або телекомунікацій). Деякі із цих країн, що мають федеративний устрій або істотні повноваження на регіональному рівні (наприклад, Німеччина, Іспанія), мають один національний наглядовий орган [1, с. 134] і кілька субрегіональних органів, на які покладено ті самі функції, що й на регіональному або федеральному рівнях. Крім того, необхідно відзначити, що в багатьох країнах (наприклад, Румунії) до створення національних органів із захисту персональних даних обов'язок контролювати дотримання права на недоторканність приватного життя був покладений на інститут омбудсмена, в деяких державах-членах (наприклад, Фінляндія) омбудсмен, як і раніше, підтримує відповідну функцію щодо захисту особистих даних [1, с. 135]. У 2005 році з набранням чинності Закону «Про свободу інформації» у Великій Британії з'явився Комісар з питань інформації [4, с. 218].

Цим особам та органам надано суттєві повноваження: уряд має консультиватися з ними під час розроблення відповідного законодавства, пов'язаного з обробленням інформації персонального характеру, вони також мають право проводити розслідування й отримувати доступ до інформації, що стосується їхнього розслідування, вимагати знищення інформації або забороняти її оброблення, звертатися до суду з позовами, розглядати скарги й вимагати звіти від посадових осіб. На них покладено функції щодо правової освіти населення та підтримання міжнародних зв'язків у галузі захисту й передачі даних. Органи влади, що є операторами баз даних, отримують відповідні ліцензії в уповноважених з питань прайвесі та захисту даних [3, с. 282].

В окремих країнах створено унікальні (нетипові) інституційні форми. Так, в Ізраїлі в структурі Міністерства юстиції створено Реєстраційне бюро баз даних, а в Південній Кореї повноваження щодо контролю за виконанням Закону «Про захист персональної інформації, що перебуває у віданні органів влади» надано Міністерству урядової адміністрації та внутрішніх справ. В Італії створено спеціальний наглядовий орган із питань захисту персональних даних – *Garante*. У Росії уповноваженим органом із захисту прав суб'єктів персональних даних є федеральний орган виконавчої влади, що здійснює функції контролю й нагляду у сфері інформаційних технологій і зв'язку. Сьогодні Уповноваженим органом із захисту прав суб'єктів персональних даних є Федеральна служба з нагляду у сфері зв'язку, інформаційних технологій і масових комунікацій (Роскомнагляд), а саме одне з її управлінь – Управління щодо захисту прав суб'єктів персональних даних. Однак, незважаючи на специфіку таких інституційних форм, майже всі вони позиціонуються в законодавстві як незалежні органи [3, с. 288].

Відповідні національні органи існують в Австралії, Аргентині, Гонконгу (спеціальний адміністративний район КНР), Канаді, Новій Зеландії. В окремих країнах функції щодо захисту інформації про приватне життя особи покладено на один або кілька державних органів, а саме: Міністерство юстиції (Перу), Міністерство зв'язку та комунікацій (В'єтнам) або Агентство з розвитку інформації та комунікацій (Сінгапур), Федеральна торгова комісія (США), Комісія з питань захисту громадян (Чилі) й низка інших.

В Аргентині в основному існують два механізми для забезпечення дотримання права на приватне життя й захист персональних даних:

- в адміністративному порядку через Національну дирекцію щодо захисту персональних даних (NDDP);
- у судовому порядку шляхом видачі судового наказу *Habeas Data* чи виконання інших дій [1, с. 143].



У Канаді на федеральному рівні повноваження з контролю за дотриманням Закону про недоторканність приватного життя й Закону про захист персональної інформації та електронних документах покладені на Комісара щодо конфіденційності Канади (PIPEDA) [1, с. 144–145].

Канадський Уповноважений щодо захисту даних несе відповідальність за дотримання інформаційних прав людини, закріплених у законодавстві, а також за дотримання своїх обов'язків операторами даних. Цей Уповноважений призначається урядом і є незалежним у здійсненні своїх функцій. Особи, які вважають, що їхні права ущемлені, можуть подати скаргу до комісара, який розслідує це питання та може здійснювати будь-які заходи, необхідні для його врегулювання. Уповноважений забезпечує недоторканність приватного життя канадців. До його повноважень належить: а) розслідування скарг, проведення перевірок і подача судових позовів у рамках двох федеральних законів; а) інформування громадськості про практику поведінки державних і приватних організацій з персональними даними; в) підтримка, проведення та публікація результатів досліджень із питань прайвесі; г) підвищення обізнаності громадськості й розуміння наявних проблем щодо інформаційного прайвесі; проведення освітніх семінарів і практикумів [3, с. 283–284].

Він є співробітником парламенту, підзвітним безпосередньо перед Палатою громад і Сенатом. Комісар працює незалежно від будь-якої іншої частини уряду і здійснює розслідування скарг, що надходять від окремих осіб стосовно федеральних органів та організацій як публічного, так і приватного секторів. У публічному секторі окремі особи можуть звернутися зі скаргою до Комісара з будь-яких питань, зазначених у ст. 29 Закону про прайвесі. Цей закон стосується особистої інформації, наявної в урядових установах Канади. З питань, що стосуються особистої інформації в приватному секторі, комісар може розслідувати всі скарги на підставі ст. 11 PIPEDA, за винятком провінцій, у яких прийнято аналогічне за сутністю законодавство щодо прайвесі [3, с. 284].

На рівні провінцій у кожній провінції й території є незалежні Комісаріати щодо конфіденційності, які передусім відповідають за дотримання законів про захист персональних даних, але їх штат і бюджет різноманітні [1, с. 145]. Проте навіть у тих провінціях, де існують аналогічні до федеральних закони з питань прайвесі, PIPEDA продовжує застосовуватися до особистої інформації, що збирається, використовується або розкривається будь-якими федеральними підприємствами, установами та організаціями, у тому числі особистої інформації про працівників. PIPEDA також стосується всіх особистих даних, які передаються через провінційні й федеральні кордони [3, с. 284].

Основні сили цих чиновників зосереджені на тому, аби звернути увагу громадської думки на проблемні зони, навіть якщо вони не мають жодних повноважень для самостійного вирішення проблеми. Вони можуть зробити це шляхом систематизації наявної практики й заохочення промислових асоціацій до прийняття відповідних зводів правил. Вони також можуть використовувати свої щорічні доповіді, аби вказувати на наявні проблеми. Наприклад, федеральний комісар Канади з питань прайвесі в доповіді за 2000 рік заявив про існування великої кількості баз даних, що підтримуються федеральним урядом. Після того, як ця доповідь стала надбанням громадськості, чимало міністерств розформувало свої бази даних [3, с. 286].

Варто зазначити, що реалізація Закону про захист приватного життя належить також до компетенції президента казначейської Ради, який є міністром за цим Законом. Отже, він несе відповідальність за підготовку та розповсюдження директив і настанов щодо виконання закону й регулятивних документів про конфіденційність [1, с. 145].

У Франції Інститут Уповноваженого із питань захисту персональних («номінативних») даних функціонує на основі Закону «Про інформатику, картотеки та свободи» від 06.01.1978. Він поширюється на процеси автоматизованого збирання, оброблення, зберігання й поширення персональних даних.

Закон передбачає створення Національної комісії з інформатики (глава II Закону 1978 року), під контроль якої підпадає близько 120 тисяч електронних баз даних.



Комісія є адміністративним органом з регламентованими повноваженнями, витрати на утримання якого включаються до бюджету міністерства юстиції. Деякі витрати є підставою для стягнення плати за надання послуг (стаття 7 Закону 1978 року).

Комісія складається з 17 чоловік: двох депутатів і двох сенаторів, яких обирає Парламент; двох учасників Економічної й Соціальної ради, яких обирають на її зборах; двох членів Рахункової палати; двох членів Касаційного суду; двох фахівців з інформатики, призначених Декретом голови Національних зборів і Сенату; трьох фахівців, призначених Радою Міністрів. Член Комісії виконує покладені на нього повноваження протягом 5 років (стаття 8 Закону 1978 року).

Комісія зобов'язана:

- інформувати громадськість про вплив інформатики на приватне життя та функціонування демократичних інститутів;
- уносити до Уряду пропозиції щодо захисту персональних даних за умови розвитку інформатики;
- у передбачених Законом 1978 року випадках приймати регламентні акти (постанови) і видавати правила щодо захисту персональних даних;
- приймати й розглядати заяви та скарги;
- попереджати порушників і сповіщати органи прокуратури про порушення Закону 1978 року;
- консультувати приватних і юридичних осіб, органи державної влади та судові органи.

Комісія може вимагати від голів Апеляційних та Адміністративних судів відрядження в її розпорядження відповідних осіб для проведення під її керівництвом нагляду чи перевірки. Особи, що викликані до Комісії для роз'яснень чи надання свідчень, звільняються від дотримання таємниці. Міністри, посадові особи, керівники публічних і приватних організацій (підприємств) повинні всіляко сприяти роботі Комісії.

Рішенням Прем'єр-міністра при Комісії призначається урядовий Комісар із захисту персональних даних. Він бере участь у засіданнях Комісії й може в 10-денний термін призначити повторне слухання з будь-якого питання, що раніше було винесено на розгляд Комісії. Комісар очолює Французьке агентство з питань захисту персональних даних [5, с. 30–31].

Інститут Уповноваженого з питань захисту персональних даних в Угорщині функціонує на підставі Закону «Про захист інформації про особу і доступ до інформації, що становить суспільний інтерес» від 10.11.1992.

Закон визначив виборну посаду Парламентського Комісара із захисту інформації (Омбудсмен), що діє згідно з положеннями Закону про Парламентського Комісара з прав громадян.

Омбудсмен зобов'язаний:

- контролювати виконання положень Закону 1992 року;
- розглядати скарги з питань захисту інформації про особу;
- забезпечувати ведення реєстру щодо захисту інформації [5, с. 31].

В Естонії діє Інспекція із захисту даних, яка є установою державного нагляду, що діє у двох різних напрямках: захист особистих даних (недоторканність особистого життя) і забезпечення дотримання положень закону про публічну інформацію. Інспекція почала свою діяльність у лютому 1999 року. Вона створена при Міністерстві внутрішніх справ (з 1 січня 1997 року до лютого 1999 року цим займався відділ захисту даних Міністерства внутрішніх справ). З лютого 2007 року Інспекція та законодавство із захисту даних входять у сферу відповідальності Міністерства юстиції. Правовий статус Інспекції визначається Законами Естонії «Про захист персональних даних» і «Про публічну інформацію». Очолює цю інституцію голова, якого призначає уряд за поданням міністра юстиції після схвалення цієї кандидатури Конституційною комісією Парламенту Естонії (Рійгікогу) терміном на п'ять років [4, с. 197–198].

Якщо ж звернутися до власне загальноєвропейських стандартів щодо уповноважених органів у сфері захисту інформації, то Конвенція Ради Європи про захист фізичних осіб



під час автоматизованого оброблення персональних даних ETS № 108 указала на необхідність призначення (або створення) одного або декількох органів, що здійснюють функції з реалізації її принципів (ст. 13). При цьому Конвенція не передбачила чіткої регламентації питань, пов'язаних із правовим статусом та обсягом повноважень національних органів, що здійснюють захист прав суб'єктів персональних даних, і реалізації положень прийнятого внутрішнього законодавства [1, с. 124].

Також ст. 10 Конвенції вказує на обов'язок кожної сторони (держави-члена) передбачити відповідні санкції та засоби правового захисту від порушень норм внутрішнього законодавства, що втілюють основні принципи захисту даних, визначені в ній.

Функції зазначених органів, відповідно до положень Конвенції, обмежуються лише наданням інформації про законодавство й адміністративну практику своєї держави в галузі захисту даних, а також про так звану фактологічну інформацію, що стосується конкретного автоматизованого оброблення персональних даних, що здійснюється на території держави. Отже, спочатку функції уповноважених органів були досить обмежені.

Технічний прогрес і збільшення зростання обмінів персональними даними через національні кордони як держав-учасників, так і держав, які не ратифікували цю Конвенцію, поставили на порядок денний нагальну потребу забезпечити ефективний захист права на недоторканність приватного життя під час обміну такими даними.

Зазначені обставини й основоположні принципи, визначені в Конвенції, вимагали розроблення належних засобів правового захисту в національному законодавстві кожної держави в разі порушення вимог законодавства й, відповідно, прав громадян [1, с. 125].

Із цією метою Додатковим протоколом до Конвенції від 08.11.2001 ETS № 181183 визначено необхідність кожній державі-учасниці передбачити один або більше наглядовий орган з покладенням на нього відповідальності за забезпечення виконання заходів у своєму національному законодавстві для застосування принципів, викладених у главах II і III Конвенції та Додаткового протоколу. При цьому статтею 1 Додаткового протоколу до національних наглядових органів покладаються три основні групи повноважень:

1) проведення розслідувань і втручань з правом висувати судові справи або залучити компетентні судові органи під час порушення положень внутрішнього права, що забезпечує виконання вищезазначених міжнародних принципів;

2) розглядання заяв з боку будь-якої особи щодо захисту його/її прав і свобод у зв'язку з обробленням персональних даних у межах своєї компетенції;

3) здійснення співробітництва з іншими наглядовими органами тією мірою, якою це необхідно для виконання своїх обов'язків, зокрема, шляхом обміну необхідною інформацією.

Як можна переконатися, перелік повноважень недостатньо конкретизований, тим самим дає можливість державам самостійно визначати їх обсяг з урахуванням специфіки національного права з метою ефективного здійснення покладених на наглядовий орган завдань, головним із яких є захист права на недоторканність приватного життя під час оброблення персональних даних [1, с. 126].

Основним вихідним документом, який визначив повноваження національних наглядових органів, стала Директива 95/46/ЕС. Між тим положення зазначеної Директиви в частині обсягу повноважень не були повністю реалізовані в усіх державах-членах, створюючи ситуацію, коли окремі національні влади передбачали обмежені інструменти для виконання покладених на національні органи контрольних функцій [1, с. 138–139].

Загалом, аналізуючи повноваження різних національних органів із захисту даних, виділяють дві загальні тенденції, що відображають підходи закордонних країн до захисту персональних даних. Так, у низці країн (наприклад, у Великобританії, Ірландії, Фінляндії, Швеції) підкреслена превентивна та попереджувальна роль наглядових органів у сфері забезпечення персональних даних, в інших державах (наприклад, у Греції, Латвії, Чехії) першочергове значення має реагування правоохоронних органів на вже виявлений факт порушень і функція контролю органу захисту персональних даних за додержанням законодавства про захист персональних даних. У зв'язку з цим і характер повноважень, покладених на ор-



гани контролю, є різнобічним з перевагою «м'яких» профілактичних інструментів у першому випадку та більш «жорстких» заходів у другому випадку [1, с. 151]. Тому під час аналізу ефективності засобів правового захисту, доступних у рамках якоїсь юрисдикції, інструменти правового захисту повинні оцінюватися в їх контексті [6, с. 128].

**Висновки.** Отже, можна дійти висновку, що досвід західних країн свідчить про повсюдність практики існування уповноваженого органу у сфері захисту інформації про особу. При цьому йдеться про діяльність як уповноважених органів за моделлю омбудсмена, так й інших незалежних органів. Обсяг повноважень може бути пов'язаний з усією інформаційною сферою загалом, захисту права на приватність, а також права на доступ до інформації. Існує різниця й у повноваженнях з погляду більшого акценту на превентивній ролі або ж на застосуванні примусових заходів. Щодо України вважаємо, що наша модель має враховувати цей досвід, трансформуючи чинну модель у бік створення спеціалізованого уповноваженого з питань інформації. В інституційному плані варто йти шляхом створення спеціалізованого інформаційного уповноваженого, окремо від Уповноваженого Верховної Ради України з прав людини, який би мав відповідну незалежність. Для цього потрібно внести відповідні зміни до Конституції України.

#### **Список використаних джерел:**

1. Телина Ю.С. Конституционное право гражданина на неприкосновенность частной жизни, личную и семейную тайну при обработке персональных данных в России и зарубежных странах : дисс. ... канд. юрид. наук : спец. 12.00.02 / Ю.С. Телина. – М., 2016. – 266 с.
2. Тимченко Н.М. Перспективи введення в Україні інституту інформаційного омбудсмена / Н.М. Тимченко // Проблеми і перспективи розвитку банківської системи України : збірник наукових праць. – 2012. – Випуск 36. – С. 265–270.
3. Серьогін В.О. Конституційне право особи на недоторканність приватного життя (прайвесі): проблеми теорії та практики : дис. ... докт. юрид. наук : спец. 12.00.01, 12.00.02 / В.О. Серьогін. – Х., 2011. – 415 с.
4. Нестеренко О. Інформація в Україні: право на доступ / О. Нестеренко. – Х. : Акта, 2012. – 306 с.
5. Інформаційне право та правова інформатика у сфері захисту персональних даних / [В. Брижко, М. Гуцалюк, В. Цимбалюк та ін.]. – К. : НДЦП АПрН України, 2006. – 450 с.
6. Посібник з європейського права у сфері захисту персональних даних. – К. : К.І.С., 2015. – 215 с.

