DOI https://doi.org/10.51647/kelm.2021.5.1.37

MIĘDZYNARODOWE STANDARDY I ZAGRANICZNE DOŚWIADCZENIA PRAWNE REGULUJĄCE OCHRONĘ DANYCH OSOBOWYCH I ICH WDRAŻANIE NA UKRAINIE

Julia Samoilenko
aspirant Katedry Prawa Administracyjnego, Postępowania i Działalności Administracyjnej
Dniepropetrowskiego Państwowego Uniwersytetu Spraw Wewnętrznych (Dniepr, Ukraina)
ORCID ID: 0000-0001-5020-4966
e-mail: samoylenko11@gmail.com

Adnotacja. W artykule dokonano analizy międzynarodowych standardów ochrony danych osobowych, określono sposoby ewentualnego wprowadzenia zagranicznych doświadczeń w zakresie regulacji prawnych i praktyki organów administracji publicznej w zakresie wdrażania mechanizmów ochrony danych osobowych w krajowym modelu ochrony danych osobowych.

W szczególności zaproponowano i uzasadniono: 1) wprowadzenie procedury licencjonowania baz danych w zakresie ochrony danych osobowych, która powinna być zapewniona przez organ wykonawczy, któremu powierzono funkcje ochrony praw w zakresie ochrony danych osobowych; 2) ujednolicenie procedur rejestracji baz danych osobowych, co zapewnia ich rejestrację i umożliwia informowanie obywateli o możliwości dostępu do ich danych osobowych; 3) wprowadzenie rejestru administratorów danych osobowych; 4) wprowadzenie certyfikacji zautomatyzowanych systemów informatycznych przeznaczonych do przetwarzania danych osobowych, mających na celu stworzenie niezbędnego poziomu ochrony danych osobowych; 5) nałożenie na Ministerstwo Transformacji Cyfrowej Ukrainy obowiązku monitorowania zasobów internetowych w celu wykrycia naruszeń przepisów o ochronie danych osobowych i postawienie przed Osobą uprawnioną pytania o zastosowanie odpowiednich środków oddziaływania na przestępców.

Słowa kluczowe: dane osobowe, ochrona danych osobowych, międzynarodowe standardy ochrony danych osobowych, doświadczenie zagraniczne, kierunki wdrażania doświadczeń zagranicznych.

INTERNATIONAL STANDARDS AND FOREIGN EXPERIENCE OF LEGAL REGULATION OF PERSONAL DATA PROTECTION AND ITS IMPLEMENTATION IN UKRAINE

Julia Samoilenko
Postgraduate Student at the Department of Administrative Law,
Process and Administrative Activities
Dnipropetrovsk State University of Internal Affairs (Dnipro, Ukraine)
ORCID ID: 0000-0001-5020-4966
e-mail: samoylenko11@gmail.com

Abstract. The article analyzes the international standards of personal data protection, identifies ways to implement foreign experience of legal regulation and practice of public administration in implementing mechanisms for personal data protection in the domestic model of personal data protection.

In particular, it is proposed and substantiated: 1) to introduce a procedure for licensing databases on personal data protection, which should be provided by the executive body, which is entrusted with the functions of protection of rights in the field of personal data protection; 2) unify the procedures for registration of personal databases, which ensures their accounting and allows to inform citizens about the possibilities of access to their personal data; 3) introduce a register of personal data controllers; 4) introduce certification of automated information systems designed for personal data processing, which aims to create the necessary level of personal data protection; 5) impose on the Ministry of Digital Transformation of Ukraine the obligation to monitor Internet resources to identify violations of legislation on personal data protection and raise before the Commissioner on the application of appropriate measures to influence violators.

Key words: personal data, personal data protection, international standards of personal data protection, foreign experience, directions of implementation of foreign experience.

МІЖНАРОДНІ СТАНДАРТИ Й ЗАКОРДОННИЙ ДОСВІД ПРАВОВОГО РЕГУЛЮВАННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ І ЙОГО ВПРОВАДЖЕННЯ В УКРАЇНІ

Юлія Самойленко
аспірант кафедри адміністративного права,
процесу та адміністративної діяльності
Дніпропетровського державного університету внутрішніх справ (Дніпро, Україна)
ORCID ID: 0000-0001-5020-4966
e-mail: samoylenko11@gmail.com

Анотація. У статті здійснено аналіз міжнародних стандартів захисту персональних даних, виокремлено шляхи можливого впровадження зарубіжного досвіду правового регулювання та практики діяльності органів публічної адміністрації щодо реалізації механізмів захисту персональних даних у вітчизняну модель захисту персональних даних.

Зокрема, запропоновано й обґрунтовано: 1) запровадити процедуру ліцензування баз даних із захисту персональних даних, яка повинна надаватися органом виконавчої влади, на який покладені функції захисту прав у сфері захисту персональних даних; 2) уніфікувати процедури реєстрації баз персональних даних, що забезпечує їх облік і дає змогу інформувати громадян про можливості доступу до своїх персональних даних; 3) запровадити реєстр розпорядників персональних даних; 4) запровадити сертифікацію автоматизованих інформаційних систем, призначених для обробки персональних даних, що має на меті створення необхідного рівня захисту персональних даних; 5) покласти на Міністерство цифрової трансформації України обов'язок здійснювати моніторинг інтернет ресурсів на предмет виявлення порушень законодавства про захист персональних даних і порушувати перед Уповноваженим питання про застосування відповідних заходів впливу на порушників.

Ключові слова: персональні дані, захист персональних даних, міжнародні стандарти захисту персональних даних, зарубіжний досвід, напрямки впровадження зарубіжного досвіду.

Вступ. Вироблення дієвих правових механізмів захисту персональних даних в Україні має здійснюватися також з урахуванням міжнародних стандартів захисту прав і свобод особи в інформаційній сфері, а також на підставі аналізу зарубіжного досвіду законодавчого забезпечення та практики захисту персональних даних у передових країнах світу в цілому і Європейських країн, зокрема які мають багаторічну практику реалізації стандартів і механізмів захисту персональних даних.

Виходячи з вищезазначеного, метою дослідження в межах наукової статті є виокремлення шляхів можливого впровадження зарубіжного досвіду правового регулювання та практики діяльності органів публічної адміністрації щодо реалізації механізмів захисту персональних даних у вітчизняну модель захисту персональних даних, завданням дослідження на виконання його мети є аналіз міжнародних стандартів і практики діяльності органів публічної адміністрації передусім європейських країн щодо захисту персональних даних.

Основна частина. Аналіз міжнародних актів, які тим чи іншим чином регулюють питання захисту персональних даних, дає можливість виокремити ключові з них. Так, необхідність створення міжнародної системи правового регулювання обробки й передачі даних порушена на засіданні Організації з економічного співробітництва і розвитку (далі – ОЕСР) у 1978 р., у результаті чого заснована експертна група із завданням розробити набір базових принципів захисту приватного життя й індивідуальних свобод у зв'язку з обробкою персональних даних і транскордонними потоками даних. За підсумками дворічної роботи експертної групи, включаючи процес узгодження принципів з усіма державами-членами, Рада ОЕСР прийняла Настанови «Про базові принципи захисту недоторканності приватного життя і транскордонних потоків персональних даних», які складаються з п'яти частин: перша – містить дефініції й визначає сферу дії базових принципів; друга – установлює вісім базових принципів захисту у зв'язку з обробкою персональних даних на національному рівні; третя – присвячена принципам міжнародного застосування, тобто взаємодії між державами-членами ОЕСР; четверта – визначає заходи для здійснення на практиці вищезгаданих принципів і, зокрема, установлює, що вони повинні застосовуватися в «недискримінаційній манері»; п'ята – присвячена організації співробітництва держав-членів ОЕСР (за допомогою обміну інформації й запобігання несумісним національним процедурам для захисту персональних даних) (1). Положення базових принципів розроблені з метою досягнення державами-членами ОЕСР мінімальних стандартів захисту персональних даних; зменшення нормативно-правових розходжень між відповідними нормами національного законодавства різних країн; гарантії того, що при захисті персональних даних на національному рівні будуть братися до уваги інтереси інших країн, зокрема не допускатися неналежне втручання при передачі персональних даних між країнами; усунення причин, що могли б спонукати країни обмежити або заборонити транскордонні потоки персональних даних через можливі ризики, асоційовані з такими потоками.

Першим міжнародним нормативним актом, у якому офіційно закріплено принципи, засади й механізми захисту персональних даних, є Конвенція Ради Європи «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних» (відома як Конвенція № 108 згідно з порядком у серії Європейських договорів), прийнята 28 січня 1981 року (2). Держава-член Конвенції Ради Європи № 108 має право визначати види персональних даних, які підлягають захисту (стаття 3 Конвенції). Кожна держава-член Конвенції Ради Європи № 108 коригує національне законодавство в частині втілення її основних принципів і поставленої мети забезпечення на території держави-члена поваги до прав та основних свобод кожної особи незалежно від її громадянства або місця проживання (стаття 4). Конвенцією до захисту персональних даних висуваються певні вимоги: їх отримання й обробка мають здійснюватися законним шляхом; вони повинні зберігатися та використовуватися у визначених і законних цілях, бути точними й поновлюваними, допускати ідентифікацію фізичної особи; персональні дані, що свідчать про расову належність, політичні, релігійні чи інші переконання, а також дані, що стосуються здоров'я або статевого життя, не можуть піддаватися автоматизованій обробці, якщо внутрішнє законодавство країни не забезпечує відповідних гарантій (це правило застосовується також до персональних даних, що стосуються засудження в кримінальному порядку; засоби та заходи, що застосовують до таких даних, повинні передбачати безпеку персональних даних від випадкового й несанкціонованого доступу, знищення, модифікації, блокування, розповсюдження та випадкової втрати (статті 5–7)). Важливими положеннями Конвенції є ті, які стосуються використання персональних даних. Так, збирання, накопичення, зберігання й поширення персональних даних може здійснюватися лише

з дозволу особи, дані про яку обробляються (цій особі надано право знати місце роботи та проживання розпорядника бази персональних даних (відповідального за обробку даних)), а також право отримувати відповідні дані без затримки й у зрозумілій формі. У разі відмови зацікавлена особа може звернутися до суб'єкта нагляду за дотриманням законодавства в державі, який повинен забезпечити припинення порушень положень, що зазначені в національному законодавстві (статті 8 і 13).

Для захисту персональних даних Конвенція Ради Європи № 108 зобов'язує кожну державу-члена призначити один або більше Уповноважених органів нагляду й направити відповідне повідомлення Генеральному секретарю Ради Європи. Завдання інституту Уповноваженого передбачають створення належного організаційно-правового регулювання діяльності щодо захисту персональних даних у країні (стаття 13). Нині Уповноважені органи з питань захисту персональних даних діють більше ніж у двадцяти країнах Європи. Їхня діяльність свідчить, що вони є ефективним засобом, здатним забезпечити баланс інтересів людини, суспільства й держави. У Німеччині, наприклад, за участі цього інституту вдалося оформити право на захист персональних даних як основне право фізичних осіб і розглядати його як конституційну норму (Брижко, 2006: 23). Для вирішення питань, що пов'язані з узгодженням позицій держав-членів Конвенції Ради Європи № 108, створено Консультативний комітет, який може вносити пропозиції з метою сприяння або покращення застосування Конвенції; може вносити пропозиції щодо внесення змін і доповнень до Конвенції; надає свій висновок щодо пропозиції про внесення змін і доповнень до Конвенції; на прохання держави-члена може робити висновок з будь-якого питання, що стосується застосування положень Конвенції.

З метою уніфікації вимог щодо захисту персональних даних окремі країни Сходу (Австралія, Гонконг, Нова Зеландія), Південної Африки, Америки (Канада) прийняли відповідні закони з питань захисту даних, нині близько 40 країн світу мають закони з питань захисту персональних даних (Проценко, 2012: 45). Разом із тим варто зазначити, що інформаційне законодавство багатьох із них має суттєві недоліки, навіть у найбільш демократичних країнах поширеним є несанкціоноване прослуховування й інші порушення законів, які визначають порядок доступу до даних, що поширюються за допомогою електронних каналів зв'язку. Виходячи з економічних інтересів щодо потреби вільної транскордонної передачі персональних даних, 24 жовтня 1995 р. була ухвалена Директива 95/46/ЄС Європейського парламенту та Ради «Про захист осіб у зв'язку з обробкою персональних даних та вільним обігом цих даних» (5), а 15 грудня 1997 р. – Директива 97/66/ЄС Європейського парламенту та Ради «Про обробку персональних даних і захист прав осіб у телекомунікаційному секторі» (6). Ці документи деталізують положення Конвенції Ради Європи № 108 і вводять обмеження на передачу персональних даних як до Європи, так і з Європи в країни, де ще не прийняті закони з адекватним рівнем захисту персональних даних. Міжнародні стандарти гарантують країнам, які дотримуються європейського режиму захисту персональних даних, вільний обмін такими даними.

Найбільш важливими положеннями Директиви 95/46/ЄС є такі: положення застосовують до обробки персональних даних за допомогою повного чи часткового використання автоматизованих засобів, а також до обробки неавтоматичними засобами персональних даних, що є частиною картотеки чи призначені для внесення до картотеки (вона не застосовується, якщо обробка персональних даних проводиться фізичною особою під час її діяльності виключно особистого чи побутового характеру (стаття 3)); обробка персональних даних має здійснюватися лише за згодою зацікавленої фізичної особи (під обробкою персональних даних уважаються будь-які дії чи сукупність дій, які здійснюють або не здійснюють за допомогою автоматизованих систем, вона включає збирання, реєстрацію, накопичення, зберігання, модифікацію, комбінування, компіляцію, поширення та будь-яку іншу форму дій, що дає змогу мати доступ до персональних даних, а також їх блокування та знищення на носіях інформації (стаття 2)); фізична особа має бути повідомлена про факт обробки, про передачу її персональних даних третім особам, а також має право на точну та повну інформацію про обставини такої передачі (статті 10 і 11); кожній особі гарантується право отримати від контролера підтвердження того, обробляються чи ні дані, які її стосуються, й інформацію принаймні про цілі обробки, категорії даних і про одержувачів чи категорії одержувачів, яким надаються дані (стаття 12); суб'єкт даних має право заперечувати в будь-який час проти обробки його даних, пов'язаних із конкретною ситуацією, за винятком випадків, коли інше передбачено національним законодавством (стаття 14); кожна особа має право на те, щоб стосовно неї не приймалося рішення, яке ґрунтується виключно на автоматизованій обробці даних (стаття 15); захист персональних даних передбачає використання технічних та організаційних засобів з моменту створення системи їх обробки (стаття 17); наглядовий орган повинен вести реєстр операцій з обробки персональних даних (стаття 21); кожній людині передбачено право на судовий захист від будь-якого порушення прав, гарантованих національним законодавством, що застосовується до відповідної обробки (стаття 22), і на одержання компенсації за завдану шкоду (стаття 23) тощо.

Окремим питанням, яке потребує міжнародного правового регулювання, є захист персональних даних у міжнародних інформаційних системах, зокрема в глобальній комунікаційній інформаційній системі Інтернет, що відображено в Рекомендаціях Ради Європи «Основні напрями захисту прав фізичних осіб у зв'язку з обробкою персональних даних в інформаційних супермагістралях» від 9 грудня 1997 року. Особливість Інтернет полягає в тому, що йому властива екстериторіальність, а захист прав осіб, зокрема захист персональних даних, визначається територіальною юрисдикцією. Більше того, у світі відсутні механізми аналізу потоків даних, що циркулюють в Інтернет. В Україні Інтернет не підпадає під жодний із законів, тому що не віднесений ні до електронних засобів масової інформації, ні до будь-якого іншого, поки що не є широковживаним комерційним інструментом. Вивчення можливостей і спроб регулювання на національному

рівні інформаційних потоків в електронному вигляді шляхом ліцензування інформаційної діяльності щодо надання послуг вже здійснюється у Великобританії, Франції, Німеччині, США, Японії, Китаї. Так, у Великобританії не дозволяється публікувати матеріали, що містять випади персонально на чиюсь адресу чи державну таємницю. У Німеччині влада прагне захистити персональні дані своїх громадян і відгородити їх від пропаганди неонацизму, хоча подібне може розміщуватися далеко від неї на веб-вузлах, наприклад, у Канаді, на законних підставах. Уряд Німеччини вважає за необхідне розглядати Інтернет просто як ще один вид засобів масової інформації, а не місце розміщення електронних видань і порнографії. Міністр з технологій заявив: «Мережа Інтернет не повинна перетворюватися на законодавчий вакуум. Наша країна не готова терпіти деякі явища, що виникають в Інтернет». У свою чергу, стосовно контролю над Інтернет голова корпорації Microsoft Білл Гейтс зазначив: «Нам потрібен розумний баланс – відкритість цієї системи та захист її від зловживань. ... Ми наполягаємо на праві публікувати в електронному вигляді всі ті матеріали, що на законних підставах продаються в кіосках, друкуються в газетах чи загальнодоступні в бібліотеках» (Пилипчук, 2016: 66). Не заглиблюючись і не дискутуючи про форми та способи обмеження інформації, яка поширюється через Інтернет, з позиції правника звернемо увагу на деякі положення Рекомендацій щодо врегулювання питання захисту персональних даних, які використовуються в Інтернет мережі.

Рекомендації визначають основні положення щодо захисту персональних даних у мережі Інтернет. Зокрема, користувачі та провайдери послуг Інтернет повинні враховувати особливість захисту персональних даних у цій мережі у зв'язку з можливістю несанкціонованого їх використання та нанесення шкоди людині, суспільству або державі. Користувачі Інтернет мають ураховувати таке: Інтернет не є безпечною мережею, варто використовувати всі засоби для захисту персональних даних, такі як дозволене законодавством шифрування конфіденційної е-пошти, а також паролі доступу до персонального комп'ютера; після кожної операції на вузлах Інтернет, які були відвідані, залишаються електронні сліди, що можуть бути використані для збирання різних відомостей щодо відвідувача; якщо дозволено законом, необхідно використовувати псевдонім, при цьому ідентифікуюча інформація буде відома лише провайдеру послуг Інтернет; необхідно надавати провайдеру послуг Інтернет чи будь-якій іншій особі лише ті персональні дані, які слугують потребам забезпечення комунікації; адреса е-пошти також є персональними даними, вона може бути включена до різних каталогів чи списків користувачів, користувач Інтернет-послугами повинен запитувати про призначення каталогів і вимагати виключення своїх персональних даних із них, якщо не бажає в них фігурувати; необхідно бути уважним та обережним із веб-вузлами, які вимагають надання більше відомостей, ніж це необхідно для доступу до вузла. Користувач Інтернет-послугами може нести юридичну відповідальність за персональні дані, які передає третім особам. Натомість провайдер послуг Інтернет несе відповідальність за правильне використання персональних даних, час від часу варто з'ясовувати: які персональні дані він збирає, зберігає й поширює, яким чином і з якою метою. Він зобов'язаний виправляти дані, якщо вони помилкові, чи знищити їх, якщо вони надлишкові чи застаріли. У тому випадку, коли користувач не вдоволений способом, яким збираються, зберігаються та поширюються персональні дані, необхідно перейти до іншого провайдера.

Для провайдерів послуг Інтернет є такі рекомендації: необхідно використовувати всі доступні процедури й нові технології, що забезпечують захист персональних даних; необхідно інформувати користувачів про ризики, яким вони можуть піддаватися при використанні мережі Інтернет; необхідно надавати користувачам можливість застосування псевдоніма й інформувати про технічні засоби захисту, можливості шифрування; не читайте, не змінюйте і не знищуйте повідомлення; не дозволяйте нікому чинити будь-який вплив на зміст повідомлень (це може здійснюватися тільки державним органом, що уповноважений на це законом); сприяйте державним органам у встановленні походження зловмисних та образливих повідомлень, про порушення законодавства про захист персональних даних; збирайте і зберігайте персональні дані користувачів тільки у випадках, якщо це вкрай необхідно; не зберігайте персональні дані довше, ніж це потрібно для досягнення мети обробки (наприклад, не варто зберігати рахунки довше визначеного терміну, якщо це не передбачено податковим, цивільним чи карним законодавством), тощо.

Нижче на виконання завдань дослідження в межах статті доцільно з'ясувати особливості законодавчого й інституційних механізмів захисту персональних даних в окремих країнах. Варто зазначити, що нижче мова буде йти передусім про інституційні форми захисту персональних даних у європейських країнах сталої демократії, на які варто орієнтуватися Україні в побудові ефективного механізму захисту персональних даних.

Так, відповідно до статті 13 Конвенції Ради Європи № 108, для захисту персональних даних «кожна Сторона (держава-член Конвенції № 108) призначає один чи більше органів», «призначений орган є наглядовою інстанцією за діяльністю у сфері захисту персональних даних, забезпечує організацію законодавчої й адміністративної роботи на національному рівні і становить основу інституту Уповноваженого з питань захисту персональних даних у країні». У площині дослідження розглянемо відповідне законодавство окремих європейських країн.

У Німеччині Інститут Уповноваженого з питань захисту персональних даних почав формуватися в 1970 році, коли в Землі Гессен уперше у світі був прийнятий цільовий Закон «Про захист даних», яким запроваджено 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 обробку персональних даних. Він тісно співпрацює з міністром поліції, який повинен доповідати йому про отримання подарунків.

Захист персональних даних у країні визначається положеннями Федерального Закону «Про подальший розвиток обробки і захисту даних» від 20.12.1990. Положення Закону про інститут Уповноваженого підтвердили його правовий статус і конкретизували порядок виборності, контрольні функції, можливості оскарження незаконних дій з персональними даними тощо.

Основними нормативно-організаційними елементами системи захисту персональних даних у Німеччині є ведення реєстру файлів і баз персональних даних у державних і недержавних структурах; ведення переліку пристроїв і нагляд за застосуванням програм обробки персональних даних; здійснення контролю (перевірки) діяльності з персональними даними в різних організаціях, оскарження порушень щодо положень Закону (Василенко, 2010: 130).

Інститут Уповноваженого з питань захисту персональних даних Великобританії функціонує на основі Закону «Про захист даних» від 12.07.1984. Закон визначив посади міністра із захисту даних, реєстратора із захисту даних та утворив Суд із захисту даних. Таким чином, окреслена сфера захисту персональних даних. Міністр має право змінити чи доповнити положення Закону з метою надання додаткових гарантій щодо захисту персональних даних. Проект розпорядження, правила чи наказу повинен бути схвалений постановою кожної палати Парламенту. Реєстратор призначається грамотою Її Величності королеви. На нього покладені такі обов'язки: ведення реєстру осіб, які збирають і зберігають персональні дані, а також осіб, які мають комп'ютерні бюро й надають послуги щодо персональних даних; вручення повідомлень про порушення Закону, про скасування реєстрації або про заборону передачі даних; розгляд скарг про порушення Закону.

Будь-яка особа вправі звернутися з апеляцією до Суду із захисту даних у разі відмовлення реєстратора розглянути скаргу про порушення Закону. Основними нормативно-організаційними елементами системи захисту персональних даних у Великобританії є ведення реєстру користувачів даних, баз персональних даних і осіб, які надають послуги у сфері захисту персональних даних; перевірка й контроль діяльності з персональними даними; вручення повідомлення про порушення, про скасування реєстрації, про заборону передачі даних; адміністративне й судове оскарження у зв'язку із захистом даних.

Інститут Уповноваженого з питань захисту персональних даних Франції функціонує на основі Закону «Про інформатику, картотеки та свободи» від 06.01.1978 (9). Він поширюється на процеси автоматизованого збирання, обробки, зберігання й поширення персональних даних. Закон передбачає створення Національної комісії з інформатики, 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. Комісія складається із 17 чоловік: двох депутатів і двох сенаторів, яких обирає Парламент; двох учасників Економічної та 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. Комісія зобов'язана інформувати громадськість про вплив інформатики на приватне життя й функціонування демократичних інститутів; уносити до Уряду пропозиції про захист даних за умов розвитку інформатики; у передбачених Законом 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; консультувати приватних і юридичних осіб, органи державної влади та судові органи.

Основними нормативно-організаційними елементами системи захисту персональних даних у Франції є таке: 1) ведення Національного реєстру ідентифікації фізичних осіб (ведення Реєстру здійснює Національний інститут статистики й економічних досліджень); 2) видача дозволу на доступ до Національного реєстру й обробку персональних даних на передачу даних за кордон; 3) нагляд і контроль (перевірка рекламацій, заяв, скарг) за дотриманням вимог щодо захисту даних, перевірка документів; 4) видання розпорядження про порушення, попередження й звернення до прокуратури, оскарження неправомірних дій у суді. Особи, що винні в порушенні Закону про інформацію, можуть бути притягнуті до адміністративної відповідальності.

Висновки. Аналіз міжнародних стандартів і практики діяльності органів публічної адміністрації передусім європейських країн щодо захисту персональних даних дає можливість нам зробити певні висновки. Так, за останні 20 років у більшості європейських країн прийняті базові закони про захист персональних даних, створюються передумови розвитку їх вільного обміну й гармонізації національних законодавств із законодавством ЄС, не є винятком й Україна, яка у 2010 році прийняла Закон України «Про захист персональних даних», основні положення якого в цілому відповідають міжнародним стандартам захисту персональних даних, адже в процесі розробки цього Закону орієнтирами слугувало законодавство про захист персональних даних країн Західної Європи (Франції, Німеччини, Польщі тощо) (10). Незважаючи на розходження правових систем, в основу всіх законів про захист персональних даних покладено однакові основоположні принципи, ці принципи залишаються незмінними дотепер, навіть якщо саме законодавство в деяких країнах (у Німеччині, наприклад) оновилося. Усі вони мають однакову структуру, однакову мету й відрізняються лише в деталях. Захист персональних даних передбачає обов'язкову реєстрацію баз даних і ліцензування діяльності щодо персональних даних відповідними уповноваженими органами. Відмова від реєстрації чи ліцензування розглядається як порушення національного законодавства. Загалом усіма прогресивні державні

механізми захисту персональних даних базуються на дотриманні загальних стандартів, до яких можна віднести таке: системи обробки персональним даних є відкритими; особу має бути повідомлено про обробку та використання її персональних даних; особі повинна бути забезпечена можливість знати, яку інформацію містять її персональні дані, з якою метою їх обробляють і як використовують, вона повинна мати можливість запобігти використанню чи поширенню персональних даних для цілей, що з нею не узгоджені; особі повинна бути надана можливість уносити виправлення чи доповнення до своїх персональних даних; усі організації, що обробляють чи використовують дані у формі, яка допускає ідентифікацію особи, зобов'язані вживати заходи проти зловживання персональними даними; персональні дані варто використовувати тільки для тієї мети, для якої вони зібрані.

Вищенаведений аналіз дав змогу виокремити окремі шляхи можливого впровадження зарубіжного досвіду правового регулювання та практики діяльності органів публічної адміністрації щодо реалізації механізмів захисту персональних даних у вітчизняну модель захисту персональних даних, зокрема доцільно:

1. Запровадити процедуру ліцензування дій (робіт) із захисту персональних даних, яка повинна надаватися органом виконавчої влади, на який покладені функції захисту прав у сфері захисту персональних даних, що є основною формою державного контролю за діяльністю в цій сфері. Зокрема, мова має йти не про будь-яку діяльність, яка передбачає обробку персональних даних, а стосується лише утримувачів (адміністраторів) систематизованих баз даних, наприклад, автоматизованих баз даних медичних установ, науково-дослідних установ, реєстру виборців, поліцейських баз даних, баз фінансових і банківських установ.

2. Уніфікувати процедури реєстрації баз персональних даних, що забезпечує їх облік і дає змогу інформувати громадян про можливості доступу до своїх персональних даних. Бази персональних даних мають підлягати обов'язковій реєстрації в органах виконавчої влади, на які покладені функції захисту персональних даних. При реєстрації баз персональних даних має фіксуватися найменування баз персональних даних; перелік даних, що збирають, мета їх одержання й використання; категорії чи групи суб'єктів, що отримують персональні дані; термін зберігання персональних даних.

3. Запровадити реєстр розпорядників персональних даних, до якого вносяться відомості про мету, способи одержання й використання персональних даних, режим і термін їх зберігання; категорії чи групи суб'єктів, що отримують персональні дані; джерела персональних даних; порядок повідомлення суб'єктів про внесення їхніх персональних даних до баз персональних даних; заходи щодо зберігання персональних даних і конфіденційності дій з ними; осіб, які відповідальні за роботу з персональними даними; наявність сертифікатів на інформаційні системи, що призначені для обробки захисту персональних даних.

4. Запровадити сертифікацію автоматизованих інформаційних систем, призначених для обробки персональних даних, що має на меті створення необхідного рівня захисту персональних даних. Сертифікацію мають здійснювати відповідні органи із сертифікації, згідно із національним законодавством, зокрема, наприклад, структурний підрозділ Міністерства цифрової трансформації України, повноваження якого доцільно визначити в відповідному положенні про міністерство (11), а контроль за дотриманням умов сертифікації покласти на Уповноваженого Верховної Ради України з прав людини, прописати відповідні повноваження в положенні (12).

5. Покласти на Міністерство цифрової трансформації України обов'язок здійснювати моніторинг інтернет ресурсів на предмет виявлення порушень законодавства про захист персональних даних і порушувати перед Уповноваженим питання про застосування відповідних заходів впливу на порушників.

Список використаних джерел:

1. Про базові принципи захисту недоторканності приватного життя і транскордонних потоків персональних даних : Директива ОЕСР (Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data). Париж, 1981. URL: www.oecd.org/dsti/sti/it/secur/prod /PRIV-EN.HTM; //www.gdf.ru/books/books/defence/index.shtml.
2. Про захист осіб у зв'язку з автоматизованою обробкою персональних даних : Конвенція Ради Європи № 108 (Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data; Amendment to Convention ETS No.108 allowing the European Communities to accede). Страсбург, 28.01.1981. Серія «Європейські угоди». № 108. URL: www.convention. coe.int/treaty/en/Treaties/Html/108.htm.
3. Брижко В.М., Радянська А.І., Швець М.Я. Порівняльно-правове дослідження відповідності законодавства України законодавству ЄС у сфері персональних даних. Київ : Тріумф, 2006. 256 с.
4. Проценко В.А. Особливості механізмів захисту персональних даних в законодавстві ЄС. *Правова інформатика*. 2012. № 2 (34). С. 45–47.
5. Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних : Директива 95/46/ЄС Європейського парламенту та Ради від 24.10.1995. URL: www.evropa.eu.int/ISPO/legal/en/dataprot /directiv/directiv.html.
6. Про обробку персональних даних і захист права осіб на невтручання в особисте життя в телекомунікаційному секторі : Директива 97/66/ЄС Європейського парламенту та Ради від 15.12.1997. URL: www.evropa.eu.int/ISPO/legal /en/dataprot/protection.html.
7. Пилипчук В.Г., Брижко В.М. Інформаційна безпека та приватність у сфері захисту персональних даних. *Інформація і право*. 2016. № 4 (19). С. 60–70.
8. Василенко Д.П., Маслак В.І. Законодавство провідних країн світу в сфері захисту інформації. *Вісник КДУ імені Михайла Остроградського*. 2010. № 2 (61). Ч. 1. С. 128–132.

9. Об административной ответственности за нарушения некоторых положений Закона № 78-17 от 06.01.1978 г. «Об информатике, картотеках и свободах : Декрет Франции от 23.12.1981 № 81-1142 (Iournal official de la Republique Fracaise, 26 decembre 1981).
10. Про захист персональних даних : Закон України від 1 черв. 2010 р. № 2297-VI. *Відомості Верховної Ради України*. 2010. № 34. Ст. 481.
11. Положення про Міністерство цифрової трансформації України, затверджене Постановою Кабінету Міністрів України від 18 вересня 2019 р. № 856. *Офіційний вісник України*. 2019. № 80. Ст. 2736. С. 7.
12. Про Уповноваженого Верховної Ради України з прав людини : Закон України від 23 грудня 1997 року № 776/97-ВР. *Відомості Верховної Ради України.* 1998. № 20. Ст. 99.

References:

1. OECD Directive «On Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data». Paris, 1981. URL: www.oecd.org/dsti/sti/it/secur/prod /PRIV-EN.HTM; //www.gdf.ru/books/books/defence/index.shtml [in Ukraine].
2. Convention № 108 of the Council of Europe on the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data; Amendment to Convention ETS No.108 allowing the European Communities to access). Strasbourg, January 28, 1981. European Agreements Series, № 108. URL: www.convention. coe.int/treaty/en/Treaties/Html/108.htm [in Ukraine].
3. V.M. Bryzhko, A.I. Radyanska, M.Y. Shvets. (2006) Porivnialno-pravove doslidzhennia vidpovidnosti zakonodavstva Ukrainy zakonodavstvu YeS u sferi personalnykh danykh. [Comparative legal study of compliance of Ukrainian legislation with EU legislation in the field of personal data]. K .: Triumph, 2006. 256 p. [in Ukraine].
4. Protsenko V.A. (2012) Osoblyvosti mekhanizmiv zakhystu personalnykh danykh v zakonodavstvi YeS [Features of personal data protection mechanisms in EU legislation. Legal informatics]. № 2 (34). 2012. pp. 45–47 [in Ukraine].
5. Directive 95/46 / EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data of 24.10.1995. URL: www.evropa.eu.int/ISPO/legal/en/dataprot /directiv/directiv.html [in Ukraine].
6. Directive 97/66 / EC of the European Parliament and of the Council on the processing of personal data and the protection of individuals' right to privacy in the telecommunications sector of 15.12.1997.URL: www.evropa.eu.int/ISPO/legal / en / dataprot / protection.html [in Ukraine].
7. V.G. Пилипчук, B.M. Carefully. (2016) Informatsiina bezpeka ta pryvatnist u sferi zakhystu personalnykh danykh. [Information security and privacy in the field of personal data protection. Information and law]. № 4 (19). 2016. pp. 60–70.
8. Vasilenko D.P., Maslak V.I. (2010) Zakonodavstvo providnykh krain svitu v sferi zakhystu informatsii. [Legislation of the world's leading countries in the field of information protection]. Bulletin of KSU named after Mykhailo Ostrogradsky. 2010. № 2 (61). Ch. 1. S. 128–132 [in Ukraine].
9. Decree of France № 81-1142 of 23.12.1981 «On administrative liability for violations of certain provisions of the Act № 78-17 of 06.01.1978 «On computer science, files and freedoms» (Iournal official de la Republique Fracaise, December 26, 1981) [in Ukraine].
10. On personal data protection: Law of Ukraine of June 1. 2010 № 2297-VI. Information of the Verkhovna Rada of Ukraine. 2010. № 34. Ст. 481 [in Ukraine].
11. Regulations on the Ministry of Digital Transformation of Ukraine, approved by the Resolution of the Cabinet of Ministers of Ukraine of September 18, 2019 № 856. Official Gazette of Ukraine official publication. 2019. № 80. p. 7. Art. 2736 [in Ukraine].
12. On the Commissioner for Human Rights of the Verkhovna Rada of Ukraine: Law of Ukraine of December 23, 1997 № 776/97-VR. Information of the Verkhovna Rada of Ukraine. 1998. № 20. P. 99 [in Ukraine].