

Der aktuelle Stand des Systems des Schutzes personenbezogener Daten und neue Herausforderungen für seine Stärkung

Volodymyr Olexandrovych Krut

Leitender Spezialist der Abteilung

für die Zusammenarbeit mit internationalen

Organisationen und Protokoll im

Sekretariat des Menschenrechtsbeauftragten

der Verchovna Rada der Ukraine

In diesem Beitrag werden die Wirkungen des ukrainischen Systems des Datenschutzes in der Phase seiner Einführung untersucht. Der Autor beleuchtet die Entwicklungstendenzen und die Besonderheiten der Feinangleichung an die Standards des Europarates. Beispiele illustrieren die Unzulänglichkeiten der rechtlichen Ausgestaltung, die aus der Heranziehung wegen Verstößen gegen die Datenschutzvorschriften nach Straf- und Ordnungswidrigkeitenrecht resultieren.

Anlass für diesen Beitrag ist die Erkenntnis, dass der Schutz personenbezogener Daten ein vollkommen neues Rechtsphänomen in der Ukraine ist, die Absicherung einer leistungsfähigen staatlichen Datenschutzverwaltung aber die Beziehungen zwischen Staat und Bürger auf hohem Niveau gewährleistet, da Letztere in ihren Persönlichkeitsrechten und Privatleben unangetastet bleiben.

Es wird ein Akzent darauf gesetzt, dass im System der Staatsverwaltung eine große Anzahl staatlicher Organe und Beamten auf die eine oder andere Weise mit der Datenverarbeitung befasst sind, was die Sammlung, Registrierung, Speicherung, Aufbewahrung, Anpassung, Änderung, Aktualisierung, Nutzung und Verbreitung personenbezogener Daten umfasst. Da die staatlichen Behörden und ihre Beamten im Zusammenhang mit den ihnen eingeräumten Befugnissen personenbezogene Daten über einzelne Personen oder Gruppen von Personen anhäufen, tragen sie eine große Verantwortung dafür, dass keine rechtswidrige Verbreitung dieser Daten oder deren zufällige Veränderung geschieht.

Im Ergebnis zeigt diese Untersuchung, dass die Notwendigkeit von Vorschlägen für eine Feinkorrektur der ukrainischen Gesetzgebung besteht um ein effektives Funktionieren des ukrainischen Systems des Schutzes personenbezogener Daten zu befördern.

**Становлення національної системи захисту персональних даних
та нові виклики на шляху її удосконалення**

Крут Володимир Олександрович

Головний спеціаліст відділу співробітництва з міжнародними

Організаціями та протокольного забезпечення Управління

міжнародного співробітництва Секретаріату

Уповноваженого Верховної Ради України з прав людини

Стрімкий розвиток інформаційних технологій наприкінці ХХ століття та пов'язане із ним транскордонне розповсюдження інформації поклато початок виникненню нових відносин, пов'язаних із захистом персональних даних. В результаті технологічного прогресу людства відбуваються спостереження та перехоплення інформації, фактів, ідей, поглядів, здійснюється зберігання даних, що створює значні виклики для державно-правового регулювання у сфері захисту персональних даних.

Оскільки захист персональних даних є абсолютно новим явищем для України, забезпечення ефективної системи захисту персональних даних гарантуватиме високий рівень відносин між державою та громадянином, в основі яких знаходитиметься непорушність права особи на недоторканність до приватного життя. Однак, з огляду на свою новизну, в українському суспільстві спостерігається

доволі невисокий рівень знань та розуміння законодавства України та Ради Європи у сфері захисту персональних даних.

Питання, пов'язані із захистом персональних даних, досліджувались такими вітчизняними науковцями, як: О. Кохановська, Г. Блінова, В. Брижко, І. Бойко, В. Ліпкан, Р. Калюжний, Т. Костецька, М. Щербатюк та іншими, проте динамічний розвиток законодавства про захист персональних даних, внесення до нього змін, зумовлюють детально зупинитись на особливостях функціонування системи захисту персональних даних в Україні.

Відповідно метою нашої статті стане дослідження становлення національної системи захисту персональних даних, тенденції її розвитку, а також вдосконалення процедури притягнення до відповідальності за порушення законодавства із наведенням окремих прикладів. На думку автора

статті, розуміння громадянами, державними органами та посадовими особами, а також юридичними особами, що здійснюють свою діяльність на території України, основних вимог законодавства та особливостей функціонування системи захисту персональних даних сприятиме підвищенню рівня дотримання права кожного на повагу до особистого і сімейного життя, що гарантується статтею 32 Конституції України¹.

Ключовим стрижнем у становленні інформаційного суспільства, у врегулюванні правовідносин в інформаційній сфері та захисті прав і свобод людини та громадянина є держава. Саме держава виступає координатором поведінки учасників інформаційних відносин, законодавцем, що забезпечує правові засади розвитку відповідних правовідносин, юридичним гарантом реалізації права на інформацію, здатним захистити суб'єктів права від несанкціонованого доступу до інформації, забезпечити недоторканність приватного життя людини, реалізацію права на інтелектуальну власність в інформаційній сфері, а також забезпечити умови конкурентоздатності в інформаційній

індустрії, правила функціонування інформаційних систем. Роль держави полягає також у встановленні балансу між розвитком конкуренції в інформаційній галузі та її врегулюванням, свободою слова, вільним вираженням своїх поглядів і переконань та захистом суспільних інтересів, національної безпеки, репутації або права конкретної людини².

В Україні розвиток інформаційних технологій як правило випереджав державу у її спроможності до своєчасного та ефективного врегулювання відносин в інформаційній сфері. Динаміка розвитку суспільних відносин, пов'язаних із збиранням, зберіганням, використанням та поширенням інформації про особу, так само «підштовхнула» державу до активних дій щодо удосконалення нормативно-правової бази із забезпечення захисту персональних даних в контексті виконання положень статей 3, 32, 34 Конституції України. Свідченням цього стало внесення у 2008 році групою народних депутатів України Шевчуком О. Б., Литвиним В. М., Полохалом В. І., Самойлик К. С. проекту Закону України «Про захист персональних даних», які у своїй пояснювальній записці до законопроекту вказували на наявність «більш ніж двох десятків законів України

¹ Конституція України [Електронний ресурс]. – Режим доступу: <http://zakon5.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80>.

² Бойко І. Наукова стаття: «Охорона й захист персональних даних адміністративно-правовими заходами» // Вісник Академії правових наук України – 2011. – № 4. – с. 146.

у цій сфері, однак всі вони не мали чіткого та скорельованого з європейським законодавством визначення персональних даних»³.

В результаті розгляду цього питання 01.07.2010 Верховна Рада України прийняла Закон України «Про захист персональних даних»⁴ і вже 06.07.2010 ратифікувала Конвенцію Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних (далі – Конвенція Ради Європи 108)⁵. Такі кроки законодавчого органу нашої держави поклали початок функціонування нової правової бази державного регулювання відносин людини, суспільства та держави у сфері захисту персональних даних.

Особливістю цього процесу стало одночасне набуття чинності Закону України «Про захист персональних даних» та Конвенції Ради Європи 108, а саме обидва документа вступили в силу 01 січня 2011 року. На нашу думку, одночасність таких дій є не випадковою, і була направлена законодавчим органом на

³ Пояснювальна записка до проекту закону України про захист персональних даних [Електронний ресурс]. – Режим доступу: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=32124.

⁴ Закон України «Про захист персональних даних». // Офіційний вісник України. – 2010. – № 49 – С. 199.

⁵ Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/994_326.

гармонізацію та подальше удосконалення національного законодавства до європейських стандартів у цій галузі.

Однак, незважаючи на це, уникнути недоліків, неточностей та неузгодженостей при прийнятті Закону не вдалось, що насамперед пов'язане із браком досвіду нормотворчості у галузі захисту персональних даних і новизною самих відносин в українському суспільстві. І вже 22.04.2011 року Указом Президента України № 494/2011 був затверджений Національний план з виконання Плану дій щодо лібералізації Європейським Союзом візового режиму для України, пункт 36 якого зобов'язував визначені державні органи вжити заходів щодо удосконалення законодавства про захист персональних даних та забезпечення функціонування державного органу з питань захисту персональних даних⁶.

Поряд з цим, у 2012 році експерти Європейського Союзу надали свої висновки щодо необхідності перегляду положень Закону та приведення їх у відповідність до стандартів Європейського Союзу⁷, де одним із основоположних

⁶ Указ президента України «Про Національний план з виконання Плану дій щодо лібералізації Європейським Союзом візового режиму для України» від 22.04.2011 № 494/2011 // Офіційний вісник України. – 2011. – № 32 – С. 12.

⁷ Впровадження Європейської політики сусідства в Україні. Досягнення 2012 року й

документів у цій сфері є Директива №95/46/ЄС від 24.10.1995 «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних». З метою приведення у відповідність законодавства про захист персональних даних до вимог Конвенції Ради Європи 108 у період з 2011 по 2015 роки до Закону України «Про захист персональних даних» були внесені суттєві зміни, якими, серед іншого, змінено сферу дії Закону, уточнено визначення термінів, розширено підстави обробки персональних даних, передано повноваження контрольних функцій від Державної служби України з питань захисту персональних даних до компетенції Уповноваженого Верховної Ради України з прав людини, а також вилучено норму про створення спеціального Державного реєстру баз персональних даних – єдиної державної інформаційної системи збору, накопичення та обробки відомостей про зареєстровані бази персональних даних.

Закладаючи європейські цінності прав людини, Україна зобов'язується не лише втілювати у своє законодавство норми і принципи Конвенції Ради Європи 108, удосконалювати його відповідно до рішень Європейського Суду з прав

людини, а й очевидно, що нашій державі потрібно буде розширювати та поглиблювати національну систему захисту персональних даних у відповідності до законодавства Європейського Союзу, в основі якого закладений принцип забезпечення однаково високого рівня захисту прав і свобод людини і громадянина для всіх держав-членів ЄС.

Важливим позитивним кроком на шляху розвитку української системи захисту персональних даних стало прийняття Закону України «Про внесення змін до деяких законодавчих актів України щодо удосконалення системи захисту персональних даних», коли з 01.01.2014 повноваження контрольних функцій за дотриманням законодавства були передані до компетенції Уповноваженого Верховної Ради України з прав людини та удосконалено порядок притягнення до адміністративної відповідальності за його порушення.

Такий крок не лише забезпечив дотримання Україною принципу незалежності наглядового органу, але й дозволив упорядкувати повноваження Уповноваженого з прав людини за здійсненням контролю. Власне тому автор статті вважає, що дата 01.01.2014 стала завершенням формування основи української системи захисту персональних

рекомендації по-дальших дій [Електронний ресурс]. – Режим доступу: http://euroosvita.net/prog/data/attach/2576/ukraine_ukr_enp_implemenetation.pdf

даних та з цього моменту розпочався етап реалізації, застосування, дотримання та виконання норм і принципів, пов'язаних із збиранням, зберіганням, використанням та поширенням інформації про особу.

Проведені Україною зміни знайшли позитивний відгук у шостій доповіді Європейської Комісії від 18.12.2015, пункт 2.3.4 якої вказує на виконання критеріїв щодо захисту персональних даних⁸. Однак, не дивлячись на те, що законодавство України про захист персональних даних у переважній більшості його положень приведені у відповідність до стандартів Ради Європи, це не означає, що воно не потребує подальшого удосконалення, а тому це питання і у майбутньому буде залишатись предметом досліджень вітчизняних науковців та експертів.

В щорічних доповідях Уповноваженого Верховної Ради України з прав людини про стан додержання та захисту прав і свобод людини і громадянина в Україні за 2014 рік⁹ та за

⁸ Шоста доповідь Європейської Комісії про хід виконання Україною Плану дій щодо лібералізації ЄС візового режиму COM(2015) 905 від 18.12.2015 [Електронний ресурс]. – Режим доступу: http://www.kmu.gov.ua/control/publish/article?art_id=247754429

⁹ Щорічна доповідь Уповноваженого Верховної Ради України з прав людини про стан додержання та захисту прав і свобод людини і громадянина в Україні за 2014 рік, с. 225-226 [Електронний ресурс]. – Режим доступу: [file:///C:/Users/User/Downloads/Dopovid_2015_10b%20\(4\).pdf](file:///C:/Users/User/Downloads/Dopovid_2015_10b%20(4).pdf).

2015 рік¹⁰ Омбудсмен звертає увагу на значну кількість скарг, яку він отримує від громадян та юридичних осіб, пов'язаних із обробкою персональних даних у фінансовій сфері, освіті, у сфері житлово-комунальних послуг та мережі Інтернет. Якщо у перших трьох – фінанси, освіта, ЖКП – порушників вимог Закону можна встановити шляхом проведення відповідних перевірок та притягти їх до відповідальності, то незаконне поширення персональних даних у мережі Інтернет в українському суспільстві залишається практично безкарним.

Безкарність, насамперед, пов'язана із тим, що особу, яка поширила персональні дані, може бути складно встановити, оскільки доменне ім'я сайту, де незаконно поширені персональні дані, зареєстроване в іншій державі, а інформація, надана хостинг-провайдером щодо особи, яка зареєструвала доменне ім'я, може не відповідати дійсності.

Для боротьби з такими випадками законодавство інших держав передбачає механізм здійснення блокування доступу до веб-сторінки або її видалення. Для

¹⁰ Щорічна доповідь Уповноваженого Верховної Ради України з прав людини і громадянина в Україні за 2015 рік, с. 118-120 [Електронний ресурс]. – Режим доступу: [file:///C:/Users/User/Downloads/Dopovid_2016_final%20\(1\).pdf](file:///C:/Users/User/Downloads/Dopovid_2016_final%20(1).pdf).

цього наглядовий орган спочатку звертається до адміністрації сайту з вимогою (приписом) видалити інформацію, що порушує права суб'єкта на захист персональних даних. У випадку відсутності реакції наглядовий орган або самостійно блокує доступ до сторінки, де містяться незаконно поширені персональні дані або звертається з цією метою до суду, який приймає відповідне рішення. При цьому, якщо наглядовий орган здійснює блокування самостійно, особа, яка розмістила відповідну інформацію на веб-сайті має право оскаржити такі дії до суду¹¹.

У цьому зв'язку, з метою забезпечення захисту права особи на приватність, нашій державі варто взяти за приклад подібну практику європейських держав та внести відповідні зміни до Закону України «Про захист персональних даних».

Наглядовим прикладом незаконного поширення персональних даних у мережі Інтернет в українському суспільстві є оприлюднення у 2015 році веб-сайтом «Миротворець» (<https://psb4ukr.org/>) інформації про персональні дані великої кількості громадян України, а саме фактично

адреси їх проживання, телефонних номерів, реєстраційних номерів облікової картки платника податків, адрес електронних скриньок, які звинувачуються авторами сайту в сепаратизмі та сприянні іноземній агресії на території України.

Така діяльність представників веб-сайту «Миротворець» підпадає під дію статті 182 Кримінального кодексу України, яка передбачає відповідальність за порушення недоторканості приватного життя.

Незважаючи на звернення Уповноваженого Верховної Ради України з прав людини до Служби безпеки України та Національної поліції України щодо встановлення та притягнення до кримінальної відповідальності осіб, причетних до незаконного зберігання, використання та поширення на сайті персональних даних, досягти відчутних зрушень у справі так і не вдалось. Більше того, на думку автора, бездіяльність правоохоронних органів у 2015 році призвела до того, що у травні 2016 року сайт «Миротворець» оприлюднив персональні дані журналістів українських та іноземних засобів масової інформації, які, як стверджується, отримували акредитацію незаконних збройних формувань для здійснення діяльності на тимчасово окупованій території. Бездіяльність правоохоронних органів та

¹¹ Бем М. В., Городинський І. М., Саттон Г., Родіоненко О. М. Науково-практичний посібник: «Захист персональних даних: правове регулювання та практичні аспекти» – К.:К.І.С., 2015. – С. 158.

системність оприлюднення персональних даних сайтом «Миротворець» спричинили не лише серйозний резонанс в українському суспільстві, але й привернули увагу світової спільноти, у зв'язку з чим Посли країн G7 оприлюднили заяву, якою висловили глибоке занепокоєння діями представників інтернет-ресурсу «Миротворець» та закликали українську владу до забезпечення захисту свободи засобів масової інформації в Україні.

З огляду на продовження діяльності згаданого інтернет-ресурсу, можна припустити, що подальші звернення Уповноваженого з прав людини до Служби безпеки України та Голови Національної поліції України щодо вжиття заходів для припинення незаконного збору та поширення персональних даних осіб на інтернет-сайті «Миротворець» та забезпечення блокування доступу до зазначеного сайту на території України, позитивних результатів знову не надали.

Приклад із веб-сайтом «Миротворець» яскраво демонструє той факт, що для уникнення подібних ситуацій в майбутньому в національному законодавстві має бути посилена спроможність державних органів забезпечити захист персональних даних у всесвітній мережі. Так, погоджуючись з думкою Бем М. В., Городинського І. М.,

Саттон Г. та Родіоненко О. М.¹², слід чітко визначити органи, які матимуть право приймати рішення про блокування контенту, які контролюватимуть законність таких рішень, а які будуть уповноважені ці рішення виконувати. Виходячи з цього, такий стан речей можливо виправити шляхом внесення змін до Закону України «Про захист персональних даних», згідно із якими уповноважити Омбудсмена приймати рішення про блокування контенту в частині персональних даних, Службу безпеки України приймати рішення про блокування сайтів в частині захисту національної безпеки, суди уповноважити контролювати законність таких рішень, а Державну службу спеціального зв'язку та захисту інформації уповноважити виконувати прийняті рішення.

Ефективне функціонування системи захисту персональних даних залежить з однієї сторони від спроможності державних органів забезпечити захист самих відносин, а з іншої сторони від фахового та професійного виконання обов'язків самими володільцями персональних даних, тобто фізичними або юридичними особами, які визначають мету обробки

¹² Бем М. В., Городинський І. М., Саттон Г., Родіоненко О. М. Науково-практичний посібник: «Захист персональних даних: правове регулювання та практичні аспекти» – К.:К.І.С., 2015. – С. 159

персональних даних, встановлюють склад цих даних та процедури їх обробки. Так, і на фізичних осіб, і на юридичних осіб, які здійснюють обробку персональних даних, що включає в себе збирання, реєстрацію, накопичення, зберігання, адаптування, зміну, поновлення, використання і поширення (розповсюдження, реалізацію, передачу), знеособлення та знищення персональних даних, покладається визначена відповідальність. Однак, особливістю відповідальності юридичної особи є те, що вона зобов'язується вживати організаційних та технічних заходів з метою запобігання випадковій втраті, знищенню та незаконній обробки персональних даних, а на фізичну особу (працівника) покладається обов'язок недопущення розголошення персональних даних, які стали відомі їй під час виконання службових обов'язків.

Пункт 2 статті 23 Закону України «Про захист персональних даних» визначає повноваження Уповноваженого Верховної Ради України з прав людини, до яких належить проведення виїзних та безвиїзних, планових, позапланових перевірок володільців або розпорядників персональних даних (фізичних та/або юридичних осіб), які здійснюються за власною ініціативою Омбудсмена або на підставі відповідного звернення. У цьому зв'язку серед інших важелів запобігання

або усунення порушень законодавства про захист персональних даних, в контексті нашого дослідження варто сфокусувати увагу на двох основних складових контролю, які передбачені пунктами 5 та 10 статті 23 Закону. Перший, – це видання Омбудсменом за підсумками перевірки або розгляду звернення відповідних вимог (приписів), які обов'язкові для виконання, а другий, – складання протоколів про притягнення до адміністративної відповідальності та направлення їх до суду у випадках, передбачених законом.

Отже, аналізуючи пункти 2, 5 та 10 цієї статті впливає, що приписи можуть виписуватись як з метою усунення та виправлення вже виявлених недоліків, так і з метою запобігання порушенню законодавства, тобто для уникнення порушення у майбутньому. Для виконання цих цілей припис може містити, у тому числі вказівки або вимоги до володільців або розпорядників змінити, видалити або знищити персональні дані, забезпечити доступ до них, надати чи заборонити передати їх третій особі, зупинити чи припинити обробку персональних даних.

На відміну від припису, який може бути виписаний на підставі розгляду звернення або проведення перевірки володільця або розпорядника персональних даних, протокол про притягнення до адміністративної

відповідальності складається виключно на підставі результатів перевірки, при проведенні якої були встановлені ознаки адміністративного правопорушення.

Статистика Уповноваженого Верховної Ради України з прав людини, яка наводиться у його щорічних доповідях^{13 14} вказує, що протягом 2014 року за зверненням було видано 59 приписів, за підсумками перевірок – 30 приписів, тобто всього виписано 89 приписів про усунення правопорушень та недопустимості повторення подібних випадків у майбутньому. У 2014 році уповноваженими особами здійснено 59 перевірок та складено 8 протоколів про адміністративні правопорушення. А от у 2015 році відбулось зростання зазначених показників, коли володільцям персональних даних було виписано 141 припис та здійснено 62 перевірки, за підсумками яких складено 3 протоколи про адміністративні правопорушення. Хоча за першими двома роками діяльності

Уповноваженого Верховної Ради України з прав людини в контексті здійснення ним контролю за додержанням законодавства про захист персональних даних зарано робити висновки та давати певні прогнози, наведені статистичні дані можуть свідчити про зростання кількості приписів і проведення перевірок у найближчих роках. Проте, незначна кількість складених протоколів про адміністративні правопорушення пов'язана, на думку автора, з відсутністю в законодавстві про захист персональних даних норми про притягнення до адміністративної відповідальності юридичних осіб. Так, Кодекс України про адміністративні правопорушення, зокрема статті 188-39, 188-40 визначає підстави притягнення лише фізичних осіб до адміністративної відповідальності за порушення законодавства у сфері захисту персональних даних, і не містить положень про відповідальність юридичних осіб¹⁵.

Частина четверта статті 188-39 Кодексу України про адміністративні правопорушення визначає, що недодержання встановленого законодавством про захист персональних даних порядку захисту персональних даних, що призвело до незаконного

¹³ Щорічна доповідь Уповноваженого Верховної Ради України з прав людини про стан додержання та захисту прав і свобод людини і громадянина в Україні за 2014 рік, С. 225-226, [Електронний ресурс]. – Режим доступу: [file:///C:/Users/User/Downloads/Dopovid_2015_10b%20\(4\).pdf](file:///C:/Users/User/Downloads/Dopovid_2015_10b%20(4).pdf).

¹⁴ Щорічна доповідь Уповноваженого Верховної Ради України з прав людини про стан додержання та захисту прав і свобод людини і громадянина в Україні за 2015 рік, с. 118-120, [Електронний ресурс]. – Режим доступу: [file:///C:/Users/User/Downloads/Dopovid_2016_final%20\(1\).pdf](file:///C:/Users/User/Downloads/Dopovid_2016_final%20(1).pdf).

¹⁵ Бем М. В., Городинський І. М., Саттон Г., Родіоненко О. М. Науково-практичний посібник: «Захист персональних даних: правове регулювання та практичні аспекти» – К.:К.І.С., 2015. – С. 159.

доступу до них або порушення прав суб'єкта персональних даних, тягне за собою накладення штрафу на громадян від ста до п'ятисот неоподатковуваних мінімумів доходів громадян і на посадових осіб, громадян – суб'єктів підприємницької діяльності – від трьохсот до однієї тисячі неоподатковуваних мінімумів доходів громадян. Тобто, коли за підсумками перевірки щодо незаконного поширення персональних даних буде встановлено, що причиною їх витоку у відкритий доступ стали не дії фізичних осіб, а низька організаційна складова діяльності юридичної особи або ж неналежне забезпечення технічних заходів захисту персональних даних з боку установи, накласти на неї адміністративний штраф за порушення порядку захисту персональних даних буде неможливо через невключення до цієї статті норми про відповідальність юридичних осіб.

Поряд з цим, порушення порядку захисту персональних даних фізичними особами або юридичними особами може спричинити висунення потерпілими особами обґрунтованих вимог щодо отримання компенсації у зв'язку з порушенням їх права на недоторканість приватного життя. З огляду на те, що українське законодавство у такому випадку не передбачає будь-якої

компенсації, на що теж варто звернути увагу при удосконаленні законодавства, потерпіла особа або її представник мають право подати позов про відшкодування шкоди, завданої порушенням її права на захист персональних даних.

Підбиваючи остаточний підсумок, можна констатувати, що законодавство України про захист персональних даних послідовно наближається до європейських стандартів та в цілому відповідає вимогам та положенням Конвенції Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних. Проте, наведені у статті прогалини та недоліки свідчать, що національна система захисту персональних даних далека від досконалості. Для підвищення спроможності держави ефективно і вчасно відповідати на виклики, які виникають в ході розвитку системи захисту персональних даних, варто досконаліше проводити нормотворчу діяльність, а також ефективніше застосовувати існуючу нормативно-правову базу.

З огляду на новизну самих відносин та необхідність у цьому зв'язку підвищити рівень знань громадськості щодо правових засад захисту персональних даних, важливою складовою удосконалення функціонування системи є посилення співпраці Уповноваженого Верховної Ради України з прав людини з

представниками органів державної влади, підприємств, організацій та установ державної та приватної форм власності на предмет дотримання ними вимог законодавства про захист персональних даних. У цьому зв'язку забезпечення співпраці пропонується реалізовувати в рамках діяльності відповідної Експертної ради при Уповноваженому з прав людини, до якої залучатимуться науковці, експерти, представники громадськості та органів державної влади. Ще одним важливим елементом співпраці має бути поширення серед громадськості та державних органів інформації про права та обов'язки, які виникають у зв'язку із обробкою персональних даних. Поряд з цим володільці персональних даних теж мають приділяти більше уваги самоорганізації та відповідальності, ознайомлюватись з доступною на сайті Омбудсмена інформацією, а також з власної ініціативи звертатись до нього за роз'ясненнями з метою запобігання допущенню помилок при обробці персональних даних. Практика проведення семінарів та інших навчальних заходів, які організовує Секретаріат Уповноваженого з прав людини за участю експертів Ради Європи, має з кожним роком збирати все більше учасників та охоплювати ширше коло питань, що безумовно сприятиме підвищенню рівня знань та розуміння стандартів Ради Європи, особливо, коли

мова йде про захист права на невтручання в особисте життя.

В рамках наступного етапу удосконалення системи захисту персональних даних варто приділити більше уваги таким її ключовим елементам, як адміністративна відповідальність та контроль за дотриманням законодавства. Таким чином, автор статті пропонує визначити в статті 188-39 Кодексу України про адміністративні правопорушення адміністративну відповідальність юридичних осіб за незаконне поширення персональних даних, а також шляхом внесення змін до Закону України «Про захист персональних даних» передбачити механізм блокування доступу до веб-сторінки, визначивши органи, які прийматимуть, контролюватимуть та виконуватимуть такі рішення. Поряд з цими пропозиціями, ще одним кроком на шляху до удосконалення має стати запровадження в українському законодавстві моральної компенсації за неправомірне поширення персональних даних.