

БЛІНОВА Г. О.,
кандидат юридичних наук,
завідувач кафедри цивільно-правових
дисциплін
(ВНПЗ «Дніпропетровський
гуманітарний університет»)

УДК 342.95

ДЕРЖАВНИЙ КОНТРОЛЬ ЗА ДОТРИМАННЯМ ЗАКОНОДАВСТВА ПРО ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ

Досліджуються правові норми, що визначають основні положення контролю за дотриманням законодавства про захист персональних даних, та питання притягнення до адміністративної відповідальності за його порушення.

Ключові слова: *контроль, персональні дані, адміністративна відповідальність.*

Исследуются правовые нормы, определяющие основные положения контроля за соблюдением законодательства о защите персональных данных, и вопросы привлечения к административной ответственности за его нарушение.

Ключевые слова: *контроль, персональные данные, административная ответственность.*

We investigate the legal rules governing the substantive provisions of compliance with the law on protection of personal data and the issue of bringing to administrative responsibility for any breach.

Key words: *control, personal data, administrative responsibility.*

Вступ. З прискоренням тенденцій інформатизації суспільного життя громадян України та діяльності системи державних органів усе більшої актуальності набуває забезпечення права громадян на невторчання в їх особисте й сімейне життя, передбачене ст. 32 Конституції України. У час відсутності технічних перепон щодо отримання, зберігання й використання інформації єдиними стримуючими юридичними факторами та гарантіями захисту права на приватність для фізичних осіб є правовий режим персональних даних.

Проблематиці правових режимів інформації з обмеженим доступом у науці адміністративного права приділялася увага такими вченими, як В.Ю. Баскаков, О.А. Городов, Ю.О. Дмитрієв, М.Ю. Костенко, В.М. Лопатін, Н.М. Попова, О.С. Соколова, Г.О. Шлома. Водночас окреме дослідження питань контролю за дотриманням законодавства про захист персональних даних комплексно не проводилось.

Постановка завдання. Мета статті – з'ясування нормативно-правових актів, що визначають основні положення контролю за дотриманням законодавства про захист персональних даних, підстави й порядок притягнення до адміністративної відповідальності за його порушення, а також історію їх становлення. Предмет розгляду цього наукового дослідження – правові норми та наукові теорії, що визначають статус контролюючих суб'єктів, їх повноваження, основні елементи контролю в цій сфері, адміністративну відповідальність за порушення законодавства про захист персональних даних та історичні етапи їх становлення.



Результати дослідження. Сучасний стан захисту персональних даних в Україні швидко змінюється. Так, 1 січня 2014 року набули чинності зміни до чинного законодавства про захист персональних даних відповідно до Закону України «Про внесення змін до деяких законодавчих актів України щодо удосконалення системи захисту персональних даних» [13]. Відповідно до цих змін може зовсім зникнути така держструктура, як Держслужба України із захисту персональних даних (далі – ДСЗПД). Її повноваження щодо реєстрації баз персональних даних і ведення відповідного реєстру, на думку деяких юристів, можуть перейти до Державної реєстраційної служби, яка, на відміну від ДСЗПД, має досить розгалужену структуру в усій Україні [14].

Проте нині переважна більшість повноважень ДСЗПД, включаючи проведення перевірок, покладаються на омбудсмена – Уповноваженого Верховної Ради України з прав людини, якому передано Державний реєстр баз персональних даних, що функціонує з 1 липня 2011 року [15].

Відповідно до Порядку здійснення Державною службою України з питань захисту персональних даних державного контролю за додержанням законодавства про захист персональних даних, за неререєстрацію баз персональних даних законом не передбачено автоматичне настання відповідальності з 1 січня 2012 року. Порушення вимог закону «Про захист персональних даних» могли бути виявлені в ході перевірок Державною службою з питань захисту персональних даних, графік яких (планових і позапланових) оприлюднювався на офіційному сайті цього державного органу. Наприклад, План проведення перевірок володільців та (або) розпорядників баз персональних даних щодо дотримання ними вимог законодавства у сфері захисту персональних даних на IV квартал 2011 року [6], План проведення перевірок володільців та (або) розпорядників баз персональних даних щодо дотримання ними вимог законодавства у сфері захисту персональних даних на IV квартал 2012 року [8] та План проведення перевірок володільців та (або) розпорядників баз персональних даних щодо дотримання ними вимог законодавства у сфері захисту персональних даних на III квартал 2013 року [7].

Слід відмітити, що План проведення перевірок володільців та (або) розпорядників баз персональних даних щодо дотримання ними вимог законодавства у сфері захисту персональних даних на IV квартал 2011 року ще не містив розділу «Підстава перевірки», на відміну від такого плану на IV квартал 2012 року. З аналізу підстав проведення перевірки в останньому зазначеному плані з'ясовано, що в 90% випадків це є скарги, а в 10% – ухилення від надання відповіді.

У проекті наказу Міністерства юстиції України «Про затвердження Положення про порядок здійснення Державною службою України з питань захисту персональних даних державного контролю за додержанням законодавства про захист персональних даних» ішлося про те, що одну юридичну особу перевірятимуть 1 раз на 5 років. До 1 січня 2014 року Державна служба з питань захисту персональних даних могла проводити й позапланові перевірки, за умови отримання цим контролюючим органом обґрунтованої скарги щодо порушення права особи на збір або захист її персональних даних. У разі виявлення порушень Державна служба з питань захисту персональних даних спочатку виносила припис про їх усунення у визначений термін, у випадку невиконання якого складала протокол про адміністративне правопорушення та направляла його до суду. Слід звернути увагу на те, що штрафи за порушення у сфері захисту персональних даних могли бути призначені виключно за рішенням суду, і жоден інший орган, окрім Державної служби з питань захисту персональних даних (наприклад, податкова служба), не мав права проводити контролюючі заходи у сфері захисту персональних даних. Порушенням могло бути визнане свідоме ухилення від реєстрації бази персональних даних, неповідомлення особи про збір її персональних даних до бази, про мету створення відповідної бази та права особи у цьому зв'язку, у випадку неналежного захисту бази персональних даних, а також у випадку передачі без згоди особи її персональних даних третім особам.



Заступник голови Державної служби з питань захисту персональних даних Л.В. Олесюк повідомляла, що до 2014 року в Державній службі з питань захисту персональних даних працювала 51 особа, з яких 7 займалися саме контролем. Таким чином, на думку заступника голови Державної служби з питань захисту персональних даних Л.В. Олесюк, проведення регулярних, ґрунтовних перевірок не лише в Києві, а й у регіонах із такою кількістю контролерів видається нереальним. Ця ситуація пояснюється кількістю зареєстрованих баз даних. Так, лише за перший квартал 2013 року ДСЗПД зареєструвала 10939 баз персональних даних та внесла 351 зміну відомостей до реєстру баз персональних даних.

Відповідно до звіту ДСЗПД за 2013 рік про виконану роботу було визначено такі основні показники контролю й нагляду за законністю використання баз персональних даних:

1. Видача володільцям та (або) розпорядникам персональних даних приписів щодо усунення виявлених порушень законодавства про захист персональних даних (за результатами перевірок): протягом цього року їх було видано 25.

2. Складення адміністративних протоколів про виявлені порушення законодавства у сфері захисту персональних даних: за результатами перевірок протягом року складено 5 адміністративних протоколів про виявлені порушення.

3. Протягом року здійснено 14 планових виїзних перевірок володільців (розпорядників) баз персональних даних на додержання вимог законодавства у сфері захисту персональних даних та 15 позапланових [5].

Порушенням під час таких перевірок визнавалося свідоме ухилення від реєстрації бази даних, неповідомлення особи про збір її персональних даних до бази, про мету створення відповідної бази та права особи у зв'язку із цим, у випадку неналежного захисту бази персональних даних, а також у випадку передачі без згоди особи її персональних даних третім особам. Лише в разі невиконання вимог припису або в разі виявлення серйозних порушень ДСЗПД складала адміністративний протокол, форма якого була передбачена Порядком здійснення Державною службою України з питань захисту персональних даних державного контролю за додержанням законодавства про захист персональних даних та який направлявся до суду. Основним суб'єктом, що мав право складати протоколи про ці правопорушення на цей період, відповідно до ст. 255 КУпАП, були уповноважені на те посадові особи спеціально уповноваженого центрального органу виконавчої влади з питань захисту персональних даних – ДСЗПД. Документи, які могли складатися за необхідності, складалися під час проведення перевірки, а саме: акт про неможливість проведення перевірки через відсутність юридичної або фізичної особи за місцезнаходженням або за місцем її проживання; акт перевірки додержання законодавства у сфері захисту персональних даних; журнал обліку результатів перевірки додержання законодавства про захист персональних даних; протокол про адміністративне правопорушення; журнал обліку матеріалів про адміністративні правопорушення; акт огляду електронного документа.

Штрафи за порушення у сфері захисту персональних даних призначались виключно за рішенням суду на підставі протоколів про адміністративне правопорушення, складених за результатами перевірки Державною службою захисту персональних даних.

Водночас практика притягнення до адміністративної відповідальності осіб, винних у порушенні вимог законодавства про захист персональних даних, є дуже незначною. Існує декілька пояснень цього: по-перше, зовсім незначний період часу діяли в незмінному вигляді ст. ст. 188-39 та 188-40 КУпАП (лише півтора року); по-друге, відсутність чітких критеріїв ознак правопорушення, що підпадає під дію цих норм; по-третє, несформованість суспільного розуміння про неможливість вільного обігу персональних даних.

Незважаючи на потенційну загрозу незаконного використання персональних даних ДСЗПД протягом 2013 року здійснила 14 планових перевірок та 15 позапланових



виїзних перевірок володільців (розпорядників) баз персональних даних на дотримання вимог законодавства у сфері захисту персональних даних, за результатами яких було складено 5 адміністративних протоколів про виявлені порушення законодавства у сфері захисту персональних даних [5]. Тому, на жаль, практика застосування ст. ст. 188-39 та 188-40 КУпАП за період їх існування в тогочасному вигляді не була поширеною. Єдиний державний реєстр судових рішень надає нам інформацію лише за двома справами за ст. 188-39 «Порушення законодавства у сфері захисту персональних даних».

У першому випадку Постановою Подільського районного суду м. Києва від 7 лютого 2013 року ОСОБА_2 визнано винним у вчиненні правопорушення, передбаченого ч. 2 ст. 188-39 КУпАП, та стягнуто з нього в дохід держави штраф у розмірі 200 неоподатковуваних мінімумів доходів громадян, що становить 3 400 гривень. Згідно із цією постановою суду, 2 січня 2013 року під час проведення перевірки діяльності ТОВ «Видавництво «Рідерз Дайджест», розташованого в м. Києві по вул. Сагайдачного, 25-Б, було виявлено порушення його директором ОСОБА_2 законодавства у сфері захисту персональних даних, так як фактично база персональних даних ТОВ «Видавництво «Рідерз Дайджест» знаходиться за адресою, про яку у визначений законом строк не було повідомлено Державну службу України з питань захисту персональних даних [10].

У другій справі від 21.03.2013 року до Вознесенського міськрайонного суду Миколаївської області від Державної служби України з питань захисту персональних даних надійшов адміністративний протокол про притягнення до адміністративної відповідальності ОСОБА_1 за ч. 5 ст. 188-39 КУпАП. З протоколу вбачається, що під час проведення позапланової безвізної перевірки дотримання вимог законодавства про захист персональних даних КП «Санітарна очистка міста» було виявлено порушення, допущене начальником відділу збуту послуг зі збору, вивозу та утилізації твердих побутових відходів КП «Санітарна очистка міста» ОСОБА_1, зокрема, незабезпечення володільцем персональних даних належного захисту персональних даних під час їх обробки, що призвело до незаконного доступу до них, чим порушено ст. 24 Закону України «Про захист персональних даних» від 01.06.2010 року. Проте в цьому випадку провадження у справі щодо ОСОБА_1, було закрито у зв'язку з відсутністю в її діях події та складу адміністративного правопорушення, передбаченого ч. 5 ст. 188-39 КУпАП [11].

ДСЗПД була уповноважена лише складати адмінпротоколи про виявлені порушення законодавства у сфері захисту персональних даних, що нині, відповідно до ст. 255 КУпАП, протоколи про правопорушення, передбачені ст. ст. 188-39 та 188-40, складають уповноважені на те посадові особи секретаріату Уповноваженого Верховної Ради України з прав людини [2]. Проте вони не мають права розглядати справи про адмінпротипорушення, накладати стягнення й установлювати критерії малозначності вчинених правопорушень. Протокол про адмінпротипорушення разом з іншими матеріалами у триденний строк із дня його складання надсилається до місцевого загального суду за місцем вчинення правопорушення.

Правовою підставою для притягнення до адміністративної відповідальності за порушення законодавства про захист персональних даних є норми Кодексу України про адміністративні правопорушення, передбачені ст. ст. 188-39 та 188-40, якими було доповнено КУпАП відповідно до Закону України «Про внесення змін до деяких законодавчих актів України щодо посилення відповідальності за порушення законодавства про захист персональних даних» від 2 червня 2011 року [12]. Після набрання ним чинності з 1 липня 2012 року були внесені відповідні зміни до КУпАП [3]. Після дії в незмінному вигляді лише до 31.12.2013 року їх було значно перероблено. Такі зміни пов'язані з набуттям чинності 1 січня 2014 року Закону України «Про внесення змін до деяких законодавчих актів України щодо удосконалення системи захисту персональних даних», відповідно до якого основні повноваження Держслужби України із захисту персональних даних були передані, включаючи проведення перевірок, Уповноваженому Верховної Ради України



з прав людини, а також змінено сам механізм державного контролю за використанням персональних даних.

Виходячи із зазначеного, на наш погляд, можна виокремити три історичні етапи законодавства України, що передбачає адміністративну відповідальність за порушення порядку використання персональних даних. Перший період є найбільшим, коли від часу проголошення України незалежною державою адміністративна відповідальність за порушення порядку використання персональних даних не передбачалась до 01.07.2012 року. Відповідно до тогочасного рівня розвитку правових інститутів та пріоритету державних інтересів і колективних інтересів над особистими персональні дані включались до складу інформації з обмеженим доступом, за порушення режимів якої й наступала адміністративна відповідальність. Другий період тривав з 01.07.2012 року до 31.12.2013 року, у цей період встановлено адміністративну відповідальність за ст. ст. 188-39 «Порушення законодавства у сфері захисту персональних даних» та 188-40 «Порушення законодавства у сфері захисту персональних даних» КУпАП, напроцьовується незначна практика їх застосування. Третій період становлення законодавства про адміністративну відповідальність за порушення законодавства про захист персональних даних розпочався 01.01.2014 року з набранням чинності Законом України «Про внесення змін до деяких законодавчих актів України щодо удосконалення системи захисту персональних даних», наданням Уповноваженому Верховної Ради України з прав людини функцій контролю за дотриманням вимог законодавства в Україні у сфері захисту персональних даних та внесенням відповідних змін до ст. ст. 188-39, 188-40, 255 КУпАП.

У зв'язку із цим ДСЗПД може зовсім зникнути як держструктура. І на сучасному етапі функціонування механізму контролю й нагляду за захистом персональних даних має переважно консультативні повноваження, які реалізує в тому числі й у процесі розробки проекту національного стандарту «Інформаційні технології. Методи захисту. Основні положення щодо забезпечення невтручання в особисте життя (ISO/IEC 29100:2011, MOD)» [1].

Проект національного стандарту повністю гармонізований із міжнародним стандартом ISO/IEC 29100:2011 Information technology – Security techniques – Privacy framework. На сьогодні вже завершено експертизу остаточної редакції проекту національного стандарту. Прийняття й застосування в Україні гармонізованого з ISO/IEC 29100:2011 національного стандарту у сфері захисту персональних даних створює базу для забезпечення відповідності управлінських процесів в організаціях та на підприємствах України до вимог міжнародних стандартів у цій сфері. Цей стандарт передбачає систему таких контрольних і наглядових заходів щодо дотримання законодавства щодо захисту персональних даних:

- 1) перевірки й доведення того, що управлінські процеси відповідають вимогам, які стосуються захисту даних і недоторканості приватного життя, шляхом періодичного проведення аудитів внутрішніми аудиторами або довіреними зовнішніми аудиторами;
- 2) розробки необхідних внутрішніх заходів і механізмів незалежного нагляду, що гарантують сумісність із законодавством про недоторканість приватного життя та процедурами забезпечення інформаційної безпеки;
- 3) розробка й застосування засобів оцінювання ризиків порушення недоторканості приватного життя, які дадуть можливість оцінити внутрішні процедури на їх відповідність до встановлених вимог.

На цей час втратив чинність Наказ Міністерства юстиції України від 22 червня 2012 року № 947/5 «Про затвердження Порядку здійснення Державною службою України з питань захисту персональних даних державного контролю за додержанням законодавства про захист персональних даних», відповідно до Наказу Міністерства юстиції України «Про визнання таким, що втратив чинність, наказу Міністерства юстиції України від 22 червня 2012 року № 947/5» від 10.01.2014 року № 13/5 [4].



Третій період становлення законодавства про адміністративну відповідальність за порушення законодавства про захист персональних даних розпочався 01.01.2014 року, коли набрав чинності Закон України «Про внесення змін до деяких законодавчих актів України щодо удосконалення системи захисту персональних даних» [13]. Згідно з нововведеннями, з 1 січня 2014 року Уповноважений Верховної Ради України з прав людини наділяється повноваженням здійснювати контроль за дотриманням вимог законодавства в Україні у сфері захисту персональних даних, наданням рекомендацій щодо практичного застосування законодавства у сфері захисту персональних даних тощо.

Верховна Рада суттєво змінила існуючу процедуру реєстрації баз персональних даних. Так, законом передбачено скасування процедури державної реєстрації баз персональних даних. Натомість із 1 січня 2014 року запроваджено новий порядок – повідомлення Уповноваженого. При цьому таке повідомлення здійснюється лише щодо певних категорій дій з обробки персональних даних – лише тих даних, які становлять особливий ризик для суб'єктів персональних даних.

Відповідно до Порядку здійснення Уповноваженим Верховної Ради України з прав людини контролю за дотриманням законодавства про захист персональних даних [9] передбачені окремі процедурні питання. Так, виїзна перевірка проводиться Уповноваженим та (або) на підставі виданого ним іменного доручення такими посадовими особами: керівником Секретаріату та його заступником; представниками Уповноваженого; керівниками структурних підрозділів Секретаріату та їх заступниками; працівниками Секретаріату Уповноваженого. Доручення видається в письмовій формі на визначений у ньому строк. До участі в перевірці в установленому законодавством порядку можуть бути залучені працівники органів державної влади, у тому числі органів державного управління, органів виконавчої влади та правоохоронних органів. У разі залучення вказаних осіб вони дають письмове зобов'язання про нерозголошення персональних даних, які стануть їм відомі в результаті проведення перевірки.

До документів, які складаються під час перевірки, належать такі: припис про усунення порушення вимог законодавства у сфері захисту персональних даних, виявленого під час перевірки; акт огляду електронного документа; акт перевірки дотримання законодавства про захист персональних даних; протокол про адміністративне правопорушення.

Висновки. Водночас чинні зміни законодавства про захист персональних даних, які наділяють Уповноваженого з прав людини здійснювати контроль і нагляд за використанням персональних даних, не визначають порядок формування планів проведення перевірок володільців баз персональних даних, не встановлюють методик проведення перевірок, як планових, так і позапланових, не передбачають структуру звіту та критерії оцінки якості роботи Уповноваженого з прав людини у сфері захисту персональних даних, кількісний склад апарату Уповноваженого з прав людини не дозволяє достатньо якісно здійснювати контроль і нагляд за законністю використання персональних даних, не встановлені показники роботи Уповноваженого щодо контролю в цій сфері. Усе зазначене створює передумови для вдосконалення нормативно-правових актів, які регулюють діяльність Уповноваженого з прав людини щодо захисту персональних даних.

Список використаних джерел:

1. Інформаційні технології. Методи захисту. Основні положення щодо забезпечення невторчання в особисте життя (ISO/IEC 29100:2011, MOD) : підготовлено Технічним комітетом зі стандартизації «Інформаційні технології» (ТК-20) та Інститутом кібернетики імені В.М. Глушкова НАН України за участю Державної служби України з питань захисту персональних даних та Науково-дослідного інституту інформатики і права Національної академії правових наук України [Електронний ресурс]. – Режим доступу : <http://minjust.gov.ua>.



2. Кодекс України про адміністративні правопорушення : Закон України від 7 грудня 1984 року № 8073-Х // Відомості Верховної Ради УРСР. – 1984. – № 51. – Ст. 1122.
3. Кодекс України про адміністративні правопорушення : Закон України від 7 грудня 1984 року № 8073-Х в редакції від 01.07.2012 року (підстава 3454-17) // Відомості Верховної Ради УРСР. – 1984. – № 51. – Ст. 1122.
4. Наказ Міністерства юстиції України «Про визнання таким, що втратив чинність, наказу Міністерства юстиції України від 22 червня 2012 року № 947/5» від 10.01.2014 року № 13 [Електронний ресурс]. – Режим доступу : <http://minjust.gov.ua>.
5. Отчет о выполнении годового плана работы Государственной службы Украины по вопросам защиты персональных данных на 2013 год в первом квартале [Електронний ресурс]. – Режим доступу : <http://zpd.gov.ua/dszpd/uk/publish/article/54827;jsessionid=85A3D5E0192578C5B2B4C66F6022653F>.
6. План проведення перевірок володільців та (або) розпорядників баз персональних даних щодо дотримання ними вимог законодавства у сфері захисту персональних даних на IV квартал 2011 року : Наказ Державної служби України з питань захисту персональних даних від 28 вересня 2011 року № 61 [Електронний ресурс]. – Режим доступу : <http://zpd.gov.ua/dszpd/uk/publish/article33812>.
7. План проведення перевірок володільців та (або) розпорядників персональних даних щодо дотримання ними вимог законодавства у сфері захисту персональних даних на III квартал 2013 року : Наказ Державної служби України з питань захисту персональних даних від 25.06.2013 року № 200 [Електронний ресурс]. – Режим доступу : <http://zakon.nau.ua/doc/?uid=1041.54452.0>.
8. План проведення перевірок володільців та (або) розпорядників баз персональних даних щодо дотримання ними вимог законодавства у сфері захисту персональних даних на IV квартал 2012 року : Наказ Державної служби України з питань захисту персональних даних від 24.09.2012 року № 74 [Електронний ресурс]. – Режим доступу : <http://zpd.gov.ua/dszpd/uk/publish/article/44185>.
9. Порядок здійснення Уповноваженим Верховної Ради України з прав людини контролю за додержанням законодавства про захист персональних даних [Електронний ресурс]. – Режим доступу : http://www.ombudsman.gov.ua/index.php?option=com_content&view=article&id=3412%3A2014-01-10-09-55-09&catid=202%3A2011-11-25-14-59-08&Itemid=202.
10. Постанова Апеляційного суду м. Києва від 5 березня 2013 року на постанову Подільського районного суду м. Києва від 7 лютого 2013 року у справі № 33/796/393/2013 [Електронний ресурс]. – Режим доступу : <http://www.reyestr.court.gov.ua>.
11. Постанова Вознесенського міськрайонного суду Миколаївської області від 1 квітня 2013 року у справі № 473/1160/13-п [Електронний ресурс]. – Режим доступу : <http://court.gov.ua>.
12. Про внесення змін до деяких законодавчих актів України щодо посилення відповідальності за порушення законодавства про захист персональних даних : Закон України від 2 червня 2011 року № 3454-VI // Голос України. – 2011. – № 116. – Ст. 12.
13. Про внесення змін до деяких законодавчих актів України щодо удосконалення системи захисту персональних даних : Закон України від 3 липня 2013 року № 383-VII // Урядовий кур'єр. – 2013. – № 136. – Ст. 10.
14. Степанец А. Штрафы за правонарушения в сфере защиты персональных данных могут вырасти до 34 000 грн / А. Степанец [Електронний ресурс]. – Режим доступу : <http://dinai.com.ua/overview/285>.
15. Висновок Головного науково-експертного управління 18.06.2013 року на пропозиції Президента України до Закону України «Про внесення змін до деяких законодавчих актів України щодо удосконалення системи захисту персональних даних» (№ 2836 від 06.06.2013 року) [Електронний ресурс]. – Режим доступу : http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=46647.

