Київський національний торговельно-економічний університет

Т. О. Гуржій, А. Л. Петрицький

ПРАВОВИЙ ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ

Монографія

Київ 2019

УДК 340.13
Г 95

Автори: Т. О. Гуржій, д-р юрид. наук, проф.,
А. Л. Петрицький, канд. юрид. наук

Рецензенти: О. Н. Ярмиш, д-р юрид. наук, проф., член-кореспондент Національної академії правових наук України;
О. І. Миколенко, д-р юрид. наук, проф., завідувач кафедри адміністративного та господарського права Одеського національного університету імені І. І. Мечнікова;
Н. О. Армаш, д-р юрид. наук, доц. Навчально-наукового Юридичного інституту Національного авіаційного університету;
О. В. Олійник, д-р юрид. наук, проф. Київського національного торговельно-економічного університету

Рекомендовано до друку вченою радою Київського національного торговельно-економічного університету
(протокол № 6 від 25 січня 2018 р.)

Гуржій Т. О.

Г 95 Правовий захист персональних даних : монографія / Т. О. Гуржій, А. Л. Петрицький. – Київ : Київ. нац. торг.-екон. ун-т, 2019. – 216 с.

ISBN 978-966-629-941-6

DOI: http://doi.org/10.31617/m.knute.2019-343

Монографія присвячена дослідженню правових та організаційних засад захисту персональних даних. На основі досягнень вітчизняної юриспруденції, зарубіжного досвіду, аналізу чинного законодавства, нормотворчої та правозастосовної практики сформовано комплекс теоретичних положень і практичних рекомендацій, спрямованих на підвищення ефективності правового регулювання та організаційного забезпечення захисту персональних даних.

Видання призначене викладачам, аспірантам, студентам юридичних навчальних закладів. Може бути корисною фахівцям у галузі інформаційного права, а також усім, кому не байдужа проблематика інформаційних прав людини.

УДК 340.13

ISBN 978-966-629-941-6

ЗМІСТ

ВСТУП

Інституціоналізація захисту персональних даних як складової вітчизняного права та напряму державної інформаційної політики актуалізує питання розроблення досконалого організаційно-правового базису, котрий би гарантував стабільність правовідносин, ефективність нормотворення й правозастосування, баланс між правом людини на конфіденційність особистого життя та суспільними інтересами в інформаційній сфері.

Від стану правового та організаційного забезпечення залежить передусім інформаційна безпека людини, суспільства, держави. Досконала організація та надійне правове підґрунтя зміцнює сферу інформаційних відносин, роблячи її толерантною до внутрішніх і зовнішніх загроз. Натомість вади правової регламентації та організаційного забезпечення чинять потужну деструктивну дію. Вони дестабілізують кореспондуючі соціальні зв'язки, провокують конфлікти між їх суб'єктами, створюють передумови для маніпуляцій, зловживань та утисків.

Саме в площині організаційно-правового забезпечення слід шукати витоки численних проблем функціонування та системних збоїв механізму захисту персональних даних. Рік у рік зростає кількість випадків несанкціонованого доступу та використання конфіденційної інформації, збільшується число нелегальних інформаційних баз, зростає кількість правопорушень. Вочевидь, ці тенденції матимуть місце доти, доки не буде усунуто системні недоліки правового регулювання та організаційного забезпечення у сфері захисту персональних даних.

Усвідомлюючи масштаби проблеми та загрозу її ескалації з подальшим розвитком електронних технологій, держава розглядає захист персональних даних як пріоритетний напрям інформаційної політики. Протягом кількох останніх років в Україні реалізовано широкий комплекс правових та організаційних заходів, спрямованих на побудову ефективного механізму захисту персональних даних.

Однак попри наявність загальних позитивних тенденцій, доводиться констатувати, що існують проблеми, які виникають фактично на всіх рівнях нормативно-правового регулювання та правозастосовної діяльності у сфері захисту

персональних даних. Кардинального оновлення потребує тематичне законодавство, яке характеризується неузгодженістю, колізійністю, фрагментарним регулюванням суспільних відносин і багатьма іншими недоліками. Система публічного адміністрування в цій сфері виявилися малоефективною, а її нинішнє реформування відбувається надто мляво. Окремі складові цієї системи функціонують розрізнено, без належної взаємодії й координації. Їх робота ускладнена недостатньою визначеністю правового статусу, перетином сфер відповідальності, браком кадрових та матеріально-технічних ресурсів. Ці проблеми чинять негативний вплив на держану політику у сфері захисту персональних даних, знижуючи її ефективність, нівелюючи здобутки.

Викладене вище зумовлює необхідність удосконалення правових та організаційних засад захисту персональних даних. З цією метою доцільно провести ґрунтовний аналіз інформаційного законодавства та правозастосовної практики, висвітлити пов'язану з ними проблематику, окреслити перспективні напрями її вирішення.

Стрімкий розвиток інформаційних відносин, кардинальне оновлення інформаційного законодавства та нещодавня реорганізація системи контролю за додержанням законності у сфері захисту персональних даних актуалізували широкий комплекс проблем, які потребують невідкладного розв'язання. Це неможливо зробити на основі наявних наукових напрацювань, більшість яких не враховує специфіки новел правового та організаційного забезпечення захисту персональних даних.

У світлі викладеного постає необхідність проведення комплексного дослідження проблематики захисту персональних даних на основі останніх теоретичних напрацювань, аналізу сучасної нормотворчої та правозастосовної практики, новел вітчизняного та міжнародного законодавства. Спробою саме такого дослідження є представлена монографія. Наскільки вона вдалася – судити тобі, читачу. Плекаємо надію, що монографія буде не лише цікавою широкому загалу, а й корисною для подальшого розвитку правового регулювання та організаційного забезпечення захисту персональних даних.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

PHAEDRA	– Improving Practical and Helpful Cooperation between Data Protection Authorities – Міжнародний науковий проект з налагодження ефективної міжурядової взаємодії у сфері захисту персональних даних, організований під егідою Ради Європи
УПЗПД	– Управління з питань захисту персональних даних секретаріату уповноваженого Верховної Ради України з прав людини
ДСУПЗПД	– Державна служба України з питань захисту персональних даних
ЄС	– Європейський Союз
КАС України	– Кодекс адміністративного судочинства України
КЗпП України	– Кодекс законів про працю України
КК України	– Кримінальний кодекс України
КУпАП	– Кодекс України про адміністративні правопорушення
КПК України	– Кримінальний процесуальний кодекс України
МВС	– Міністерство внутрішніх справ України
НПА	– нормативно-правовий акт
РНБО України	– Рада національної безпеки і оборони України
Секретаріат	– секретаріат уповноваженого Верховної Ради України з прав людини
ЦК України	– Цивільний кодекс України

РОЗДІЛ 1. ТЕОРЕТИКО-ПРАВОВІ ОСНОВИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

1.1. Захист персональних даних як об'єкт науково-правових досліджень

Одним з головних пріоритетів України є прагнення побудувати орієнтоване на інтереси людей, відкрите для всіх і спрямоване на сталий розвиток інформаційне суспільство, в якому кожен міг би створювати й накопичувати інформацію та знання, мати до них вільний доступ, користуватися і обмінюватися ними, щоб надати можливість кожній людині повною мірою реалізувати свій потенціал, сприяючи суспільному й особистому розвитку, підвищуючи якість життя.

Україна має власну історію розвитку базових засад інформаційного суспільства. Вагомим здобутком останніх десятиліть стали: діяльність всесвітньо відомої школи кібернетики, розроблення національної програми інформатизації, новітніх інформаційно-комунікаційних технологій, створення загальнодержавних електронних інформаційно-аналітичних систем різного рівня та призначення.

Сформовано правові засади побудови інформаційного суспільства шляхом ухвалення нормативно-правових актів, які регулюють суспільні відносини у сфері сприяння розвитку громадянського суспільства, створення інформаційних електронних ресурсів, захисту прав інтелектуальної власності на такі ресурси, гарантій та механізму доступу до публічної інформації, електронного документообігу, інформаційної безпеки тощо.

Суб'єкти господарювання інтенсивно запроваджують сучасні інформаційно-комунікаційні технології та рішення щодо створення інформаційних ресурсів і запровадження електронних технологій. Активізується робота із запровадження новітніх інформаційно-комунікаційних технологій у публічному секторі, зокрема в освіті, науці, охороні здоров'я, культурі [1].

Проте бурхливий розвиток інформаційних мереж, розширення технічних можливостей у сфері накопичення, обробки й передачі інформації, розгалуження електронних комунікаційних мереж, збільшення швидкості, місткості та функціональності електронних баз даних – це не тільки чинники суспільного прогресу, а й джерело різноаспектних загроз для інформаційної безпеки та конфіденційності приватного життя громадян. Адже потужні інформаційні ресурси, які відкривають широкі можливості щодо збирання, обробки та використання конфіденційної інформації, одночасно можуть слугувати важелем психологічного тиску на людину, засобом втручання в її особисте життя, інструментом її дискредитації в очах найближчого оточення та суспільства загалом.

Для сучасної України ця проблема більш ніж актуальна. Сьогодні на вітчизняних теренах є сотні тисяч баз персональних даних. І далеко не завжди їх функціонування характеризується неухильним дотриманням закону та максимальним ступенем захисту конфіденційної інформації. У багатьох випадках обробка персональних даних супроводжується різноманітними порушеннями, які зумовлюють просочення конфіденційної інформації, несанкціонований доступ до неї, її використання в неправомірний спосіб та з неправомірною метою.

Дуже поширеним явищем у наші дні стало несанкціоноване використання конфіденційної інформації про особу в ході передвиборних кампаній, маркетингових заходів, соціальних опитувань. Нерідко така інформація використовується з метою шантажу, зведення особистих і політичних рахунків. Злонавмисне чи безвідповідальне ставлення до наслідків її оприлюднення часто шкодить національним, політичним та економічним інтересам, слугує джерелом особистих проблем, стає причиною багатьох конфліктів і негараздів.

Ситуація диктує необхідність розроблення широкого комплексу правових, організаційних, технічних та інших заходів, спрямованих на посилення контролю за обігом інформації, захист персональних даних, забезпечення права на конфіденційність приватного життя. Однак першочерговим кроком у цьому напрямі має стати створення надійного науково-правового підґрунтя.

Вивчаючи право як універсальний регулятор соціальних відносин, правова наука відшукує оптимальні форми організації всіх царин суспільного життя (політичної, економічної, адміністративної, інформаційної, технічної тощо) і через закономірний вплив на законодавство детермінує процеси їхнього розвитку. Сфера захисту персональних даних – не виняток. Її функціонування завжди відбувається у рамках, окреслених правом, отже великою мірою зумовлюються станом науково-правових досліджень. Вони сприяють удосконаленню її правового базису, формують модель її адміністрування, визначають її принципи, цілі і завдання, розробляють форми та методи її системної організації.

В умовах, коли питання захисту персональних даних набувають дедалі більшої соціальної гостроти, постає нагальна потреба узагальнення й систематизації знань, накопичених вітчизняною правовою наукою. При цьому, з огляду на швидкоплинність науково-технічного прогресу та соціально-політичних перетворень (упродовж останніх десятиліть інформаційна проблематика набула якісно нових обрисів) особливий інтерес становлять дослідження нового часу, відлік якого розпочинається з набуття державної незалежності.

Як свідчить бібліографічний аналіз, до середини 90-х років XX ст. правових та організаційних засад захисту персональних даних у вітчизняній науці ґрунтовно не досліджували. З одного боку, це пояснюється концентрацією наукового потенціалу на розв’язання глобальних проблем розбудови національної правової системи. З іншого – проблематика захисту персональних даних тоді ще не мала великої соціальної актуальності: тогочасний рівень інформатизації

суспільства був вельми низьким, обробка персональних даних здійснювалась переважно у механічний спосіб, а відповідні інформаційні бази були нечисленними й легко контрольованими. Відповідно на певному історичному відтинку техніко-технологічні аспекти накопичення, обробки та передачі даних мали значно більший науковий резонанс, аніж питання їх правового захисту.

Із часом ситуація змінилася. Стрімкий розвиток електронних технологій і комунікацій, зростання їх технічних можливостей разом з масовим поширенням та використанням потужних обчислювальних пристроїв оголили проблему захисту людини від втручання у приватне життя. Стало очевидним, що наявний рівень контролю за обробкою персональних даних не відповідає ні темпам технологічного розвитку, ні міжнародним правовим стандартам, ані нагальним потребам соціуму. Тож питання захисту прав громадян у зв'язку з обробкою персональних даних почали виходити на передній план.

Одним з перших до їх системного аналізу вдався В. Брижко, який з 1997 року виступив автором та співавтором наукових праць з питань правового забезпечення захисту персональних даних [2; 3; 4; 5; 6; 7; 8]. Об'єктом прискіпливої уваги цього дослідника стали галузеві аспекти захисту персональних даних, зокрема конституційно-правовий, міжнародно-правовий, цивільно-правовий та інші.

Узагальнюючи теоретичні напрацювання, положення міжнародного інформаційного законодавства та зарубіжний досвід, В. Брижко сформулював концептуальні висновки щодо сутності захисту персональних даних і механізмів його забезпечення. Це висновки про те, що:

будь-яка особа має природне виключне право власності на відомості про неї (це означає, що вона може володіти, користуватися та розпоряджатися відомостями про себе, як вважає за потрібне, з урахуванням чинного законодавства та норм суспільної моралі, а також право забороняти іншим суб'єктам використовувати свої персональні дані, крім винятків, передбачених законом) [3, с. 64];

право власності на персональні дані потребує обов'язкового юридичного закріплення та надійного захисту, однак в умовах активного розвитку процесів інформатизації такий захист неможливо забезпечити самими лише заходами організаційного й техніко-технологічного характеру без створення спеціального інституту права [4, с. 179, 180];

функціонування цього інституту об'єктивно може і повинно ґрунтуватися на принципах регулювання приватних майнових відносин, сам же він є складовою загальної системи захисту прав і свобод людини та громадянина [5, с. 154–156];

недостатня ефективність механізмів захисту персональних даних приховує чималі ризики для безпеки людини, суспільства, держави, тож їх нейтралізація має бути визнана важливим напрямом державної діяльності та першочерговим завданням національної інформаційної політики [4, с. 94];

основні пріоритети цієї політики: забезпечення нормативно-правової регламентації при роботі з персональними даними всіх учасників процесу інформаційної взаємодії; забезпечення захисту персональних даних від несанкціонованого доступу [4, с. 187];

правова регламентація захисту персональних даних має здійснюватися на основі міжнародного інформаційного законодавства шляхом ухвалення окремого закону, натомість конкретизація механізмів практичного регулювання має відбуватись у підзаконних нормативних документах [4, с. 165].

Незважаючи на те що деякі з наведених положень характеризуються певною дискусійністю (такі, на наш погляд, теза про цивільно-правовий характер захисту персональних даних, а також зведення пріоритетів інституціональної політики виключно до нормотворення й технічної безпеки), теоретичні погляди В. Брижка сформували плідне підґрунтя для подальших досліджень у сфері правового та організаційного забезпечення захисту персональних даних.

Етапною віхою наукових пошуків автора стала дисертація «Організаційно-правові питання захисту персональних даних» (2004), в якій на базі сучасної європейської практики та міжнародних стандартів прав людини розглянуто перспективи розвитку вітчизняного інформаційного законодавства в частині регулювання відносин безпеки конфіденційної інформації [9].

Поряд із вирішенням важливих теоретичних питань (як-то: класифікація баз даних, визначення принципів захисту від неправомірного збирання, обробки, зберігання та поширення інформації, формулювання авторських дефініцій «персональні дані», «власник персональних даних», «володілець персональних даних тощо) у дисертації В. Брижка подано багато пропозицій для практичного забезпечення захисту персональних даних на правовому та організаційному рівнях.

Фактично вперше до уваги широкої громадськості було запропоновано проект рамкового закону «Про захист персональних даних», яким пропонувалося гарантувати право власності на персональні дані, окреслити коло суб'єктів правовідносин у сфері захисту персональних даних, встановити загальні вимоги до операцій з даними, запровадити спеціальний режим доступу, передбачити юридичну відповідальність за порушення законодавства про захист персональних даних, визначити підстави, форми та напрями міжнародного співробітництва в сфері їх захисту. [9, с. 221–236].

На тлі більшості тогочасних досліджень, які обґрунтовували доцільність повної кодифікації інформаційного законодавства та введення норм про захист персональних даних до єдиного Інформаційного кодексу, ідея ухвалення окремого спеціалізованого закону вирізнялась істотною новизною. І подальший розвиток подій засвідчив її обґрунтованість. Через деякий час (2010) вона втілилась у Законі України «Про захист персональних даних», структура та зміст якого мають багато спільного з проектом В. Брижка.

Чималий практичний інтерес становить авторське бачення системи адміністрування сферою персональних даних. У дисертації В. Брижко обґрунтував доцільність створення незалежного від держави органу, який би провадив дозвільну діяльність у сфері обробки персональних даних, забезпечував реєстрацію відповідних інформаційних баз, розглядав звернення фізичних і юридичних осіб з питань захисту персональних даних в адміністративно-правовому порядку, репрезентував країну на міжнародному рівні, зокрема в Консультативному комітеті Ради Європи та інших міжнародних організаціях з питань захисту персональних даних.

Глибина опрацювання цієї пропозиції справляє чимале враження. Поряд з детальним описом функцій і повноважень органу захисту персональних даних автор змоделював його організаційну структуру, здійснив точні розрахунки його матеріально-технічного забезпечення, виклав алгоритм реалізації основних напрямів його діяльності (дозвільної, реєстраційної, контрольної тощо), запропонував багаторівневу схему його нормативно-правового забезпечення [9, с. 237–250].

Тепер, через десяток років, є всі підстави вважати, що своєчасне втілення цих новел істотно наблизило б Україну до міжнародних стандартів організації захисту персональних даних та сприяло б помітному прогресу у захисті права людини на конфіденційність приватного життя. Однак подібно до багатьох інших прогресивних наукових ідей, викладені пропозиції тривалий час залишалися незатребуваними.

Фактично від доктринального оформлення цієї концепції до її практичного втілення минуло десять років. За цей період були марно витрачені значні ресурси, а головне – згаяно час на шляху до інтеграції в європейське інформаційне суспільство, імплементації міжнародного законодавства та переходу на світові стандарти захисту приватного життя.

Викладене свідчить як про прогресивність вітчизняної правової думки, так і про відсутність ефективних механізмів її втілення у життя. Залишається сподіватися, що нако-

пичений досвід дасть змогу уникнути помилок у майбутньому, а між наукою та практикою організації інформаційних відносин буде налагоджено дієвий зворотний зв'язок.

Ключова роль у формуванні теоретико-правових основ захисту персональних даних належить професору Р. Калюжному, який став не лише автором, а й науковим керівником багатьох тематичних досліджень. Під керівництвом Р. Калюжного написано десятки наукових праць, які охоплюють найважливіші аспекти захисту персональних даних, висвітлюють нагальні проблеми практики, пропонують ефективні шляхи їхнього розв'язання [6; 10; 11; 12; 13; 14].

Широке визнання в наукових і практичних колах отримали сформульовані ним ідеї про кодифікацію вітчизняного інформаційного законодавства, визнання захисту персональних даних складовою інформаційної безпеки, пошук балансу між правом на інформацію та правом на захист від втручання у приватне життя, вдосконалення правових та інституційних механізмів захисту персональних даних, запровадження юридичної відповідальності за делікти в сфері обробки та використання персональної інформації про особу.

Внесок Р. Калюжного у розбудову теорії інформаційного права не вичерпується самим лише літературним доробком. Під орудою цього наставника зросла ціла генерація правників, котрі продовжують його наукові пошуки та успішно працюють над питаннями правового забезпечення обігу інформації. У цьому контексті варто згадати Д. Красікова, Н. Новицької, О. Тихомирова та інших представників сучасної школи інформаційного права.

Особливе місце в правничих дослідженнях з питань інформаційної безпеки та захисту персональних даних посідають наукові праці І. Арістової [15; 16; 17; 18; 19; 20; 21]. Констатуючи значні прогалини в інформаційному законодавстві, недосконалість механізмів реалізації конституційного права на захист персональних даних та відсутність дієвої системи контролю за його дотриманням, І. Арістова дійшла

висновку про комплексний характер наявних проблем та необхідність їхнього вирішення у рамках державної інформаційної політики.

Проблематика інформаційного права є міжгалузевою і міжрегіональною, вона потребує вирішення складних організаційних і техніко-технологічних питань, значних витрат і не може бути здійснена в одну вмить. Потрібне всебічне урахування соціально-економічних, правових і політичних аспектів інформатизації суспільства, активне використання організаційного, технологічного й технічного досвіду провідних країн. Необхідне також розроблення комплексу організаційно-правових заходів та проведення гнучкої політики інформаційної безпеки, заснованої на балансі публічних і приватних інтересів, оптимальному співвідношенні права людини на інформацію та права на недоторканність особистого життя.

Особливе значення такий баланс має у сфері обробки персональних даних, адже саме тут актуалізується загроза недоторканності особистого життя, обмеження права на особисту, сімейну і комерційну таємницю як у разі надмірного втручання держави, так і внаслідок несанкціонованої діяльності недержавних структур [15, с. 130, 230, 396, 397].

Слушність цих висновків незаперечна. Проблеми захисту персональних даних зумовлені широким колом політичних, правових, організаційних чинників. Вони проявляються у різних сферах інформаційної діяльності та нерозривно пов’язані між собою, що потребує системного підходу до їх розв’язання. Забезпечити його може тільки цілеспрямована державна політика, яка має комплексний міжгалузевий характер, спрямована на вирішення конкретних цілей, підкріплюється дієвим механізмом реалізації, реалізується на всіх рівнях публічного адміністрування та у всіх сферах інформаційної діяльності.

Розроблення і втілення такої політики – першочергове завдання держави, для якої захист персональних даних – це не тільки питання додержання прав людини, а й національної

безпеки. Важливим кроком на цьому шляху стало визначення І. Арістовою пріоритетів державної діяльності у сфері захисту персональних даних: запобігання випливу, втраті і підробленню інформації, загрозі інформаційної небезпеки особистості, суспільства, держави; несанкціонованим діям щодо знищення, модифікації, перекручування, копіювання, блокування інформації; іншим формам незаконного втручання в інформаційні ресурси та системи, забезпечення правового режиму існування інформації та документації як об'єктів власності; захист конституційних прав громадян щодо зберігання особистої таємниці й конфіденційності персональних даних [17, с. 361–362].

Окреслені пріоритети знайшли широке відображення в багатьох актах інформаційного законодавства, концепціях, планах і програмах інформаційного розвитку і так лягли в основу національної інформаційної політики.

Неабиякою значущістю характеризуються й інші наукові напрацювання І. Арістової, велика частина яких успішно втілена в практику правового, організаційного, методичного та інформаційного забезпечення захисту персональних даних.

Всезростаюча актуалізація проблем правового та організаційного забезпечення захисту персональних даних зумовила підвищений інтерес до міжнародних стандартів та зарубіжного досвіду у сфері захисту права людини на конфіденційність приватної інформації. Так уже склалося, що і самі інформаційні відносини, і питання правового забезпечення їх безпеки набули найбільшого розвитку в провідних (з точки зору економічного, політичного та соціального розвитку) країнах. І вони й заклали фундамент міжнародно-правового регулювання захисту персональних даних на засадах верховенства права, законності, рівності й демократизму.

Можливості використання їхніх здобутків і напрацювань, урахування накопиченого ними досвіду, застосування апробованих ними інструментів правового забезпечення неможливо переоцінити. А саме вони дають змогу побудувати оптимальну

модель захисту персональних даних та скерувати її розвиток у прогресивне русло. Крім того, невідповідність національного законодавства міжнародно-правовим стандартам гальмує темпи євроінтеграційних процесів, створюючи величезні перешкоди для міжнародного співробітництва у всіх сферах, пов'язаних з обміном персоніфікованою інформацією.

Зважаючи на це, міжнародно-правовий аспект захисту персональних даних неодноразово потрапляв у поле зору вітчизняних правників. У різні роки його вивчали Ю. Гелич, Д. Красіков, О. Шевчук та інші [22; 23; 24; 25]. Однак доводиться визнати, що більшість тематичних досліджень позбавлені фундаментального характеру й охоплюють лише окремі напрями (інститути, сфери) гарантування безпеки персональних даних.

Чи не єдиним зразком комплексного розгляду міжнародно-правових питань захисту персональних даних є дисертація А. Пазюка «Міжнародно-правовий захист права людини на приватність персоніфікованої інформації» [26]. У цій роботі на підставі аналізу міжнародного інформаційного законодавства, галузевого законодавства окремих країн та зарубіжної правозастосовної (зокрема судової) практики сформульовано пропозиції, покликані забезпечити гармонійний перехід України до сучасної моделі захисту конфіденційної інформації про особу.

Систематизувавши ознаки національних систем захисту персональних даних у провідних країнах, А. Пазюк виділив три світові моделі забезпечення конфіденційності персоніфікованої інформації: соціальну (більшість європейських країн), ліберальну (США), змішану (Канада, Австралія). Для соціальної моделі властиве поширення правил правового захисту персоніфікованих даних, а також наглядових повноважень не тільки на публічні, а й однаковою мірою на приватноправові відносини. В основу ліберальної моделі покладено принцип невтручання держави у відносини між приватними особами, що зумовлює її суто публічну спрямованість. Змішана модель хоч і спирається на засоби приватного та публічного права,

ключову роль у забезпеченні захисту персональних даних відводить саме останнім.

На думку А. Пазюка (і з нею важко не погодитись), ідея про запровадження в Україні ліберальної або змішаної моделі правового захисту персональних даних позбавлена практичного підґрунтя. Засновані на принципах прецедентного права, обидві моделі характеризуються слабким рівнем правового регулювання, нормативними прогалинами та вузькістю регуляторного охоплення, тому їх упровадження в національну правову систему видається неперспективним.

З огляду на це А. Пазюк обґрунтував необхідність взяття за зразок європейської (соціальної) моделі захисту персональних даних, пріоритетом якої є повага до прав людини, а не ринкові чинники. У цьому контексті на особливу увагу заслуговують його висновки щодо систематизації та правового закріплення загальноєвропейських принципів захисту персональних даних, імплементації ключових актів інформаційного законодавства ЄС в національне законодавство України, посилення контролю за виконанням міжнародних зобов'язань України у сфері захисту персональних даних, розширення правової бази регулювання кореспондуючих суспільних відносин, всебічне задіяння в механізмі захисту інформаційних прав громадян (зокрема права на захист персональних даних) інституту омбудсмена та інші.

Актуальність цих висновків підтверджується їх широким практичним втіленням, зокрема, під час ратифікації деяких міжнародних конвенцій і директив, ухвалення Закону України «Про захист персональних даних», створення спеціалізованих інститутів адміністрування та контролю за додержанням законності тощо. Фактично перехід до соціально орієнтованої моделі захисту персональних даних нині ввійшов у завершальну фазу, що, з одного боку, свідчить про правильний вектор наукового пошуку, а з іншого – дає змогу підкреслити роль міжнародно-правових досліджень у вирішенні стратегічних питань інформаційної безпеки.

Як показав аналіз, на певному етапі розвитку інституту захисту персональних даних присвячені йому правничі дослідження почали набувати вузькоспрямованого, галузевого характеру. У деяких дослідженнях осібне місце займають наукові праці А. Чернобай та С. Ясечко, які розглядають кореспондуючу проблематику крізь призму відповідно трудового та цивільного права [27; 28; 29; 30; 31; 32; 33].

Виходячи з того що у сфері трудових відносин здійснюється накопичення та обробка найбільшого масиву персональних даних, А. Чернобай констатувала необхідність вжиття комплексу правових, організаційних і технічних заходів, спрямованих на захист працівників підприємств, закладів, установ, організацій від несанкціонованого використання (розголошення) пов'язаної з ними інформації.

«У трудовому законодавстві України треба закріпити право працівника на конфіденційність і захист від вторгнення в особисте життя, а також передбачити юридичний механізм його забезпечення, – пише авторка, – працівникам і кандидатам на посаду слід гарантувати свободу самостійно вирішувати, чи потрібно надавати роботодавцю інформацію особистого характеру, тобто контролювати інформацію про себе. Цю свободу можна обмежити лише законними інтересами роботодавців, держави, третіх осіб» [34, с. 175].

У рамках поставленої мети А. Чернобай визначила першочергові кроки на шляху до інтеграції інституту захисту персональних даних у структуру вітчизняного трудового права, а саме: законодавче закріплення індивідуальних та колективних прав працівників у сфері захисту персональних даних; визначення принципів захисту персональних даних працівника з урахуванням міжнародних трудових стандартів; встановлення загальних вимог щодо обробки персональних даних працівника на засадах верховенства права, законності, рівності, добровільності та публічного контролю; гарантування права працівників на безперешкодний і безкоштовний доступ до будь-яких відомостей про себе; запровадження юридичної (зокрема

дисциплінарної) відповідальності за порушення норм, які регулюють обробку та захист персональних даних працівника [34, с. 69–71, 142–147, 173–179].

Визначальною рисою наукового підходу С. Ясечко став акцент на питаннях юридичної відповідальності за порушення права на інформацію та захист персональних даних. На відміну від більшості цивілістів, які ототожнюють право на володіння інформацією із правом на її захист, С. Ясечко провела між ними чітку межу: «Право на захист інформації має інші підстави виникнення, зміст і форми, ніж право власності: воно виникає внаслідок загрози порушення або ж фактичного порушення суб'єктивних прав на інформацію, має загальний характер, здебільшого не може бути здійснене поза юрисдикційною формою і охоплює певні процесуальні дії. Тож право на захист інформації слід розглядати окремо» [35, с. 193].

На цій підставі зроблено висновок про принципову відмінність порушень інформаційного законодавства (зокрема пов'язаних з поширенням конфіденційної інформації) та порушень інформаційних зобов'язань, що зумовлює необхідність законодавчого розмежування їх юридичних складів, а також встановлення різних санкцій за їх учинення.

У наукових працях С. Ясечко особливу увагу приділено компенсаторним механізмам цивільної відповідальності (компенсації моральної шкоди, заподіяної внаслідок незаконного поширення конфіденційної інформації), а також підставам для звільнення від цивільної відповідальності за інформаційні делікти. Вона довела, що через специфіку цього виду правопорушень звільнення від відповідальності за їх учинення може відбуватися за наявності обмеженого кола підстав, як-то: дія непереборної сили, відсутність вини, крайня необхідність і заподіяння шкоди правомірними діями.

У зв'язку з цим істотний теоретичний інтерес становить авторська теза про розмежування категорій «підстави для звільнення від відповідальності» та «підстави, які виключають притягнення до відповідальності». Така постановка питання видається цілком слушною, оскільки звільнення від відповідальності за порушення законодавства про захист персональ-

них даних може мати місце тільки там, де є підстави для такої відповідальності. В іншому разі має йтися про підстави, котрі виключають відповідальність.

І хоч далеко не всі положення, сформульовані А. Чернобай та С. Ясечко, видаються настільки ж беззаперечними, їхній науковий доробок заслуговує на дуже високу оцінку, оскільки він дав потужний імпульс для розгляду проблем захисту персональних даних на рівні галузевих правових наук.

У числі правничих досліджень з питань захисту персональних даних помітною новизною та глибиною опрацювання емпіричного матеріалу вирізняються праці А. Туніка [36; 37; 38; 39; 40]. Узагальнивши великий масив теоретичних напрацювань, позитивний зарубіжний досвід та вітчизняну практику регулювання інформаційних відносин, А. Тунік вибудував концептуальну модель державної політики захисту персональних даних. Ключові елементи цієї моделі: спрямованість на забезпечення міжнародних правових стандартів захисту прав людини, наявність досконалого з точки зору юридичної техніки та практичних потреб нормативно-правового підґрунтя, гармонійне поєднання державних і громадських механізмів контролю, цільове програмування організаційних заходів, посилення відповідальності за делікти проти безпеки персональних даних та ін.

Характерною рисою авторського підходу А. Туніка стало обґрунтування двох альтернативних сценаріїв розвитку національної системи захисту прав громадян в інформаційній сфері. Перший із запропонованих сценаріїв передбачає забезпечення пріоритету права на доступ до інформації, гарантування особистої інформаційної безпеки шляхом створення мережі спеціалізованих організацій та укладення спеціальних договорів, максимальну прозорість механізмів обробки персональних даних в органах державної влади. Другий сценарій характеризується такими аспектами й вимогами: збільшення технічної безпеки інформаційних систем, удосконалення відповідного програмного забезпечення, створення додаткових мереж технічного контролю, постійний моніторинг інформаційної безпеки, обмежений доступ до персональних баз даних тощо.

Котрий із пропонованих сценаріїв має більше шансів на реалізацію – покаже майбутнє. Нині ж можемо констатувати, що між ними немає нездоланних суперечностей. Це вказує на можливість їх узгодження, комбінування та вироблення на цій основі єдиної стратегії розвитку в сфері захисту персональних даних.

З огляду на багатоаспектний характер захисту персональних даних вітчизняні дослідники не обмежуються розглядом перерахованих вище питань. Об'єктом сталого наукового інтересу також слугують:

гарантії права людини на захист від втручання у приватне життя (Ю. Гелич, В. Сивухін, В. Серьогін) [41; 42; 43; 44; 45];

роль держави в організації захисту персональних даних (О. Тихомиров) [46];

правові засади отримання конфіденційної інформації органами державної влади (І. Сопілко) [47; 48];

проблеми правового захисту інформаційних ресурсів (О. Олійник) [49; 50];

кримінально-правова охорона інформаційного аспекту приватності (О. Горпинюк, Ю. Дем'яненко) [51; 52; 53; 54];

правовий режим захисту інформації та персональних даних (В. Баскаков) [55; 56];

адміністративно-правове забезпечення захисту персональних даних (І. Березовська, Г. Линник, О. Шевчук) [25; 57; 58; 59; 60].

Загалом огляд правових досліджень з питань захисту персональних даних справляє неоднозначне враження. З одного боку, ці питання слугують предметом активної наукової розробки. Їм приділяють увагу багато вчених, щодо них точиться жвава полеміка. На їх вирішення спрямовані зусилля провідних закладів освіти та науково-дослідних установ.

З іншого – чимало важливих аспектів захисту персональних даних лишається без належної уваги. Це і питання про галузеву належність кореспондуючих юридичних норм, і питання захисту персональних даних окремих категорій осіб (неповнолітніх, державних службовців, співробітників право-

охоронних органів тощо), і питання обробки персональних даних в окремих галузях (правоохоронній, освітній, комунікаційній), і проблематика формування та реалізації відповідного напряму державної політики, і багато інших.

Упровадження результатів наукових досліджень у нормотворчу й правозастосовну практику відбувається дуже мляво. Більшість конструктивних пропозицій, внесених сучасними правниками, втілюється у життя з великою затримкою. Деякі вже упродовж багатьох років не можуть знайти практичного втілення. І річ тут зовсім не в низькій якості наукового продукту. Навпаки, як засвідчив проведений аналіз, досягнення вітчизняної науки є вагомими, обґрунтованими та актуальними. Відповідні наукові розробки провадяться з урахуванням провідних зарубіжних досліджень та світових тенденцій гарантування безпеки персональних даних. Наочне свідчення їх наукової новизни та практичної значущості – велика кількість цитувань в роботах іноземних вчених.

Видається, що витоки наявних проблем слід шукати у великому розриві між наукою та практикою. Наразі ні держава, ні громадські інституції не мають дієвих механізмів моніторингу, планування, організації та впровадження наукових досліджень з питань захисту персональних даних. Це спричиняє не тільки необізнаність, а й відсутність зацікавленості в інноваційному розвитку на перспективу. Через брак зворотного зв’язку потужний науковий потенціал працює надаремно, а генеровані ним ідеї залишаються незатребуваними. Водночас уповноважені суб’єкти публічної адміністрації змушені діяти навмання. Не маючи ґрунтовної наукової підтримки, вони припускаються доволі серйозних помилок.

Наочним прикладом стало створення наприкінці 2010 року центрального органу виконавчої влади, покликаного забезпечувати реалізацію державної політики у сфері захисту персональних даних, – Державної служби України з питань захисту персональних даних (ДСУЗПД). Фактично цей крок

було зроблено всупереч висновкам провідних вітчизняних вчених, котрі наполягали на необхідності мінімізації державного втручання у сферу захисту персональних даних, створенні не залежної від держави системи адміністрування, чіткому дотриманні відповідних рекомендації ЄС. Зрештою він вкрай негативно позначився на євроінтеграційних перспективах країни, що зумовило подальшу передачу повноважень ДСУЗПД уповноваженому Верховної Ради України з прав людини.

Ситуація змушує констатувати широкий комплекс проблем, пов'язаних із безсистемністю наукових досліджень, відсутністю механізмів упровадження наукових здобутків у практику, слабкою підтримкою науково-правового забезпечення захисту персональних даних з боку держави. Першочерговими кроками на шляху до їх подолання мають стати:

посилення ролі провідних наукових організацій, задіяних у комплексному розв'язанні проблем інформаційної безпеки та захисту персональних даних;

введення питань наукового забезпечення захисту персональних даних до змісту державних цільових програм і планів інформаційного розвитку;

активізація діяльності Координаційного бюро з інформаційного права та інформаційної безпеки НДІ інформатики і права в частині моніторингу наукових (в тому числі науково-правових) досліджень з питань захисту персональних даних;

визначення пріоритетних напрямів наукових досліджень у сфері захисту персональних даних, розвиток системи їх цільового фінансування, всебічне розроблення охопленої ними тематики;

забезпечення постійного інформування суб'єктів державної політики у сфері захисту персональних даних про наукові дослідження та перспективи їх практичної реалізації;

стимулювання дослідницької активності у сфері захисту персональних даних шляхом надання персональних і колективних грантів, проведення конкурсів, організації науково-практичних стажувань;

підтримка відповідних наукових шкіл, молодих учених (визначення рівня бюджетних видатків на наукові школи в законі про державний бюджет);

розроблення та втілення комплексу заходів, спрямованих на комерціалізацію наукових досліджень з питань захисту персональних даних.

Як видається, пропоновані кроки сприятимуть зближенню науки та практики, раціональному використанню наукового потенціалу, підвищенню якості науково-дослідних робіт та загальному розвитку правового, організаційного і технічного забезпечення захисту персональних даних.

1.2. Поняття та сутність захисту персональних даних

У світлі формування національної політики інформаційної безпеки та актуалізації питань гарантування конфіденційності особистого життя людини неабиякого значення набуває проблематика захисту персональних даних. Рік у рік вона дедалі жвавіше обговорюється в засобах масової інформації, колах істеблішменту, громадських структурах та науковому середовищі. Їй присвячують сотні публіцистичних і наукових праць, тематичних конференцій, диспутів, обговорень. У її вирішенні задіяні фактично всі суб'єкти публічної влади, незалежно від статусу, підпорядкування й напряму діяльності. З цією метою ухвалюють закони та підзаконні нормативно-правові акти, створюють спеціалізовані органи адміністрування, розробляють концепції державних цільових програм.

Здавалося б, така широта суспільного резонансу має передбачати чітку визначеність у розумінні засадничих питань щодо природи та сутності захисту персональних даних, принципів, на яких він ґрунтується, завдань, на які він спрямовується. Проте детальне вивчення нормативної бази, правозастосовної практики та наукових джерел дає підстави для протилежного висновку. Як засвідчив проведений аналіз, багато концептуальних питань захисту персональних даних

досі лишаються невизначеними. Більш того, ні чинне законодавство, ні правова наука не пропонують чіткої однозначної та незаперечної дефініції відповідного поняття.

І це дуже велика прогалина. Адже саме наявність всебічно обґрунтованої дефініції служить запорукою ясності змісту того чи іншого поняття. Не в останню чергу саме вона гарантує розуміння предмета дискусії, однозначний підхід до тлумачення змісту юридичних норм, відсутність різнобою в нормотворенні та правозастосуванні. Дефініції надають кожному зацікавленому користувачеві можливість ознайомитися не тільки з понятійним апаратом права, а й краще зрозуміти зміст певних лексичних одиниць, глибше проникнути в їх суть [61, с. 45]. Визначення понять, якими оперує право, – обов'язкова умова ефективності його норм [62, с. 194].

Парадоксально, але факт: попри загальне визнання значущості дефініцій, незважаючи на важливість проблематики захисту персональних даних, тільки окремі галузеві дослідники роблять спроби проникнути в сутність цього явища, детально проаналізувати відповідне поняття, систематизувати його ознаки та сформулювати його авторське визначення.

Зокрема, В. Брижко визначає поняття захисту персональних даних як «захист відомостей про особу, що ідентифікована, або таку, що може бути ідентифікованою» [9, с. 51, 90]. На думку А. Возінцева, захист персональних даних являє собою «регламентовану законом діяльність уповноважених суб'єктів державної влади, спрямованих на забезпечення безпеки конфіденційної інформації персонального характеру» [63, с. 72].

З точки зору В. Козака, захист персональних даних – це обробка персональних даних лише з метою, для якої вони були зібрані; мінімізація даних, обробка яких необхідна для конкретної мети; обмеження строку зберігання та обробки даних, забезпечення актуальності персональних даних [64, с. 2 з 4]. А. Волокітін, В. Копилов та С. Волошенюк під захистом персональних даних розуміють комплекс заходів реагування на факти їх порушення та оспорювання [65, с. 11–14; 66, с. 9–12]. О. Соколова трактує це поняття набагато ширше,

а саме: «заходи, спрямовані на попередження неправомірних дій з персональними даними, а також на захист і відновлення порушених прав» [67, с. 79].

Розглядаючи захист персональних даних крізь призму трудових відносин, А. Чернобай вбачає в ньому сукупність організаційно-правових, інженерно-технічних, криптографічних та інших заходів, яких вживає власник цих даних або інші особи на його замовлення, для запобігання заподіянню шкоди інтересам власника та особи, якої вона стосується, її неконтрольованому поширенню. На її думку, захист персональних даних працівника містить передбачену законодавством діяльність відповідних державних органів щодо визнання, поновлення прав, а також усунення перешкод, що заважають реалізації прав та законних інтересів суб'єктів права у сфері персональних даних [34, с. 125].

І. Вельдер та О. Федосін доводять, що захист персональних даних – це самостійний інститут галузі інформаційного права. Причому перший розглядає його як сукупність правових норм, спрямованих на регламентацію суспільних відносин, що виникають під час збирання, використання, зберігання, обробки, видалення, передавання та розкриття інформації, пов'язаної з ідентифікуючою чи ідентифікованою особами [68, с. 36]. Другий пропонує розуміти під ним «систему юридичних норм, котрі регулюють суспільні відносини з приводу забезпечення прав особи при обробці її персональної інформації, реалізації прав і обов'язків їх учасників, повноважень контролюючих органів» [69, с. 60].

Деякі правники визначають поняття «захист персональних даних» не прямо (тобто шляхом побудови авторської дефініції), а опосередковано – через докладний опис його визначальних ознак.

У цьому аспекті чималий інтерес становлять міркування А. Туніка, який стверджує: а) захист персональних даних як діяльність здійснюють певні суб'єкти (державні і недержавні), він має цілеспрямований характер та втілюється в певному результаті – захищеності персональних даних;

б) така діяльність зумовлена конкретно історичними та соціально-культурними умовами, отже залежить від рівня розвиненості держави та інститутів громадянського суспільства; в) така діяльність регулюється насамперед правом (різними його галузями: кримінальною, цивільною, адміністративною), а також іншими соціальними засобами, вибір яких залежить від специфіки об'єкта, суб'єкта, мети діяльності тощо [40, с. 35–37].

До описової характеристики явища вдаються О. Баранов, В. Брижко та Ю. Базанов. На підставі аналізу зарубіжної та вітчизняної практики вони сформулювали певні узагальнювальні висновки стосовно захисту персональних даних як сфери діяльності, суб'єктивного права та інституту. Зокрема, на увагу заслуговують авторські тези про те, що захист персональних даних являє собою фундаментальне право, яке може бути захищене законодавством; передбачає здійснення технічних та організаційних заходів з моменту створення системи їх обробки та на весь час її функціонування; забезпечується не тільки заходами організаційного та техніко-технологічного характеру, а й заходами, заснованими на принципах регулювання відносин на майно, річ, шляхом створення особливого інституту права власності людини на свої персональні дані; має ґрунтуватися на спеціальному методі регулювання, а також на принципах права власності на матеріальні об'єкти й виключного права на нематеріальні об'єкти; технічний захист персональних даних – це окрема сфера діяльності, яку має регламентувати спеціальний закон [70, с. 116, 122, 184, 187, 188, 218].

Аналіз наведених дефініцій, уявлень та висновків про природу й сутність захисту персональних даних змушує констатувати їх еклектичність, неповноту та концептуальну неузгодженість.

Недостатньо інформативними (тож малокорисними з точки зору наукового і практичного застосування) видаються дефініції, в яких захист персональних даних визна-

чений як «захист відомостей», «захист інформації», «заходи, спрямовані на захист даних» тощо. Цілком очевидно, що вони розкривають суть персональних даних, але не їх охорони. Вони лише дублюють термін «персональні дані» і не дають відповіді на ключові запитання: що таке захист персональних даних?, в чому він полягає?, на що він спрямований? і т.ін.

Крім того, в усі подібні дефініції закладена логічна помилка, іменована «колом у визначенні». Остання має місце під час спроби роз'яснити суть певного поняття за допомогою цього ж таки поняття або його частини [71, с. 55]. За загальним визнанням, такі дефініції не розкривають змісту кореспондуючих понять, отже, не можуть вважатися істинними [72, с. 51; 73, с. 42; 74, с. 49].

Окремим авторським визначенням відчутно бракує чіткості й повноти. Це зокрема стосується дефініцій, що тлумачать захист персональних даних як комплекс заходів, однак не роз'яснюють їх змісту; у яких ідеться про захист будь-яких особистих відомостей (а не тих, за допомогою яких особу може бути ідентифіковано); котрі, ведучи мову про захист, охорону та відновлення порушених прав, не конкретизують сферу їх реалізації; де взагалі не розкрито сутності захисту як специфічного стану персональних даних; у яких за надлишком другорядних ознак поняття приховано відсутність ознак першочергових.

Поряд з недоліками форми викладення деяких авторських дефініцій призвертають увагу кардинальні розбіжності в уявленнях про природу, сутність та межі захисту персональних даних.

Як неважко помітити, одні вчені (В. Брижко, В. Козак, А. Волокітін, В. Копилов, С. Волошенюк, А. Чернобай) розглядають це явище в розрізі діяльнісного підходу. Захист персональних даних ідентифікується ними як прояв людської активності, спрямованої на гарантування безпеки конфіденційної інформації про особу (відповідно для розкриття змісту кореспондуючого поняття вони використовують діяльнісну термінологію: «операції», «заходи», «комплекс заходів», «сукупність заходів» і т.ін.).

Друга група науковців (І. Вельдер, О. Федосін та ін.) виходить з позицій інституціоналізму, вбачаючи в захисті персональних даних самостійний інститут права, покликаний забезпечити системне регулювання відповідної сфери суспільних відносин. Таким чином, вони розуміють під ним систему юридичних норм, об'єднаних загальною метою, спільним предметом та методом регулювання.

Серед представників обох згаданих концепцій теж відчувається дефіцит єдності наукових ідей. Здебільшого вони демонструють неабияке розмаїття поглядів на стрижневі, визначальні характеристики захисту персональних даних: на його функціональне призначення, основні цілі, сферу реалізації, коло суб'єктів, форми та методи здійснення, джерела регулювання тощо.

Зокрема, деякі прибічники діяльнісного підходу (А. Волокітін, В. Копилов, С. Волошенюк та ін.) розглядають категорію захист суто в аспекті реагування на фактичні загрози для визначеного об'єкта (читай – персональних даних). З цієї точки зору механізм захисту персональних даних активується тільки у разі фактичного посягання на їх цілісність і безпеку. І лише в таких випадках захист персональних даних проявляється в об'єктивній дійсності, тобто існує.

Окремі фахівці (В. Козак) обстоюють протилежну позицію. Логіка їхніх міркувань ґрунтується на тому, що захист персональних даних – це профілактична діяльність, ефективність якої забезпечується шляхом неухильного дотримання встановленого режиму обробки (збирання, реєстрації, накопичення, зберігання, адаптування, зміни, поновлення, використання, поширення, знеособлення та знищення) персональної інформації про особу.

Інші правники (В. Брижко, О. Соколова, А. Чернобай) вкладають у це поняття значно ширший зміст. Вони обстоюють думку, згідно з якою функціональне призначення захисту персональних даних полягає як у припиненні фактичних посягань на їх безпеку, так і в усуненні причин, умов

та шкідливих наслідків вчинення таких посягань. Під цим кутом захист персональних даних вони розглядають як інтегральний комплекс профілактичних, юрисдикційних та правовідновлюючих заходів, покликаних забезпечити стабільне функціонування відповідної сфери правовідносин.

Серед прибічників діяльнісної концепції захисту персональних даних немає згоди і з інших принципових питань. Деякі з них вважають, що захист персональних даних – це виключна прерогатива органів держави. Інші стверджують, що функція захисту персональних даних первинно покладається на їх володільця і може бути реалізована тільки з його ініціативи. Решта ж виходить з того, що даний напрям діяльності реалізовує широке коло державних і недержавних суб'єктів, зокрема суб'єкт публічної адміністрації, суд, володільці та розпорядник персональних даних, треті особи.

Із наведених дефініцій і суджень випливає неабияка розбіжність поглядів на природу джерел регулювання відносин у сфері захисту персональних даних. На думку одних вчених, ця сфера впорядкована різними соціальними регуляторами – як правовими, так і позбавленими правового характеру. З точки зору інших, вона служить об'єктом виключно правової регламентації. А хтось висловлює думку про те, що діяльність із захисту персональних даних (отже, й відповідна сфера суспільних відносин) може регулювати тільки закон.

За інших обставин такий плюралізм думок можна сприймати як цілком позитивне явище, позаяк «завжди більше шансів на те, що єдино вірне рішення викристалізується в горнилі наукової полеміки, аніж на те, що воно народиться знічев'я» [75, с. 248]. Однак в умовах невизначеності деяких фундаментальних питань захисту персональних даних він анітрохи не сприяє формуванню цілісної стрункої концепції їх розуміння.

Не можуть похвалитися згуртованістю й апологети інституційного підходу до визначення захисту персональних даних. Якщо одні (І. Вельдер) поширюють дію однойменного інституту права на всі відносини у сфері обробки персональних даних, незалежно від їхнього типу й спрямованості,

то інші (О. Федосін) звужують його межі до регулювання лише тих відносин, котрі складаються з приводу захисту основоположних прав і свобод людини та громадянина, зокрема права на невтручання в особисте життя, у зв'язку з обробкою відомостей персонального характеру. Таким чином, і в межах цієї концепції існує необхідність узгодження авторських поглядів та консолідації наукових ідей за єдиним напрямом.

У світлі викладеного вище доцільно проаналізувати найбільш дискусійні аспекти розуміння захисту персональних даних та сформулювати на цій основі вихідні положення, необхідні для формування єдиного уявлення про цей суспільно-правовий феномен, а також для побудови науково обґрунтованої дефініції відповідного поняття.

Отже, перша проблема, котра привертає увагу в ході вивчення тематичних наукових праць, – це обмежене сприйняття захисту персональних даних як явища, що перебуває в одній площині об'єктивної дійсності – діяльнісній (функціональній) чи суто правовій. Сучасні вчені вбачають у ньому або діяльність, спрямовану на захист конфіденційності приватного життя, або ж систему юридичних норм, котрі регламентують відповідну сферу суспільних відносин. Причому мало хто припускає, що обидва підходи можуть гармонійно співіснувати, розкриваючи різні грані досліджуваного явища, збагачуючи наукове знання про його природу, зміст та іманентні властивості.

Проте сприйняття певного явища як галузі людської діяльності та одночасно як комплексу норм об'єктивного права для вітчизняної юриспруденції не є чимось екстраординарним. Більше того, сьогодні в ній домінує саме багатоаспектний підхід до розуміння сутності суспільно-правових явищ і процесів. Свідчення цього – величезна кількість науково-правових праць, у яких ці явища розглядаються одразу під кількома кутами: діяльнісним, інституційним, правовим, нормативно-технічним і т.ін.

Зокрема, такий підхід властивий для адміністративного права, представники якого розглядають адміністративну від-

повідальність і як реакцію держави на делікт, і як однойменний інститут адміністративного права [76, с. 332; 77, с. 15, 51]. З аналогічних позицій виходять сучасні цивілісти, котрі визначають дарування, спадкування, купівлю-продаж і міну не лише як правочини, а й як самостійні цивільно-правові інститути [78, с. 28–47; 79, с. 3, 117]. Багатоаспектне сприйняття явищ об'єктивної дійсності демонструють також фахівці з інших галузей права: кримінального, трудового, земельного та ін. [80, с. 3–8; 81, с. 101–115; 82, с. 10–21].

З нашої точки зору, дослідник, який претендує на глибину розуміння та всебічність аналізу захисту персональних даних, повинен виходити з того, що це явище характеризується багатоаспектністю. Його суть не можна і недоцільно зводити до окремих проявів. Його вичерпна характеристика неможлива без застосування комплексного підходу, системного вивчення усіх аспектів його об'єктивізації.

У світлі викладеного вище постає питання про те, які ж саме аспекти захисту персональних даних слід вважати ключовими з точки зору формування узагальненої наукової концепції. Навряд чи хтось може заперечити, що захист персональних даних – це прояв цілеспрямованої людської діяльності, котра має певну соціальну мету та втілюється в конкретних суспільних відносинах. Не викликає сумніву й те, що впорядкованість цих відносин забезпечується за допомогою функціонування спеціального правового інституту, тобто цілісного комплексу юридичних норм, об'єднаних спільною метою та предметом регулювання.

Отже, варто визнати, що формування всебічного уявлення про захист персональних даних потребує обов'язкової систематизації його функціональних та інституційних ознак. Та чи тільки в цих аспектах (діяльнісному й інституційно-правовому) втілюється суть цього явища? Чи тільки в цих двох площинах воно існує та проявляється в навколишній дійсності? Видається, що ні.

Аналіз положень міжнародного, зарубіжного та вітчизняного законодавства з питань інформації переконливо свідчить, що захист персональних даних має ще один надзвичайно важливий аспект – аспект права людини.

Протягом останніх десятиліть однією з основних тенденцій міжнародно-правової регламентації захисту персональних даних стало його декларування як невід'ємної частини фундаментальних прав людини та гарантії права на конфіденційність приватного життя [83].

Зокрема, Страсбурзька конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних ставить за мету «забезпечення для кожної особи, незалежно від її громадянства або місця проживання, дотримання її прав й основоположних свобод, зокрема її права на недоторканність приватного життя, у зв'язку з автоматизованою обробкою персональних даних, що її стосуються» *(див. ст. 1 Конвенції)* [84]. Директива Європейського парламенту і Ради ЄС від 24.10.1995 № 95/46/ЄС «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» покладає на країни ЄС обов'язок захищати фундаментальні права та свободи фізичних осіб, в тому числі право на недоторканність приватного життя в частині захисту персональних даних [85].

Ідея захисту персональних даних як невід'ємного права людини червоною ниткою проходить крізь законодавство більшості європейських країн таких як Великобританія, Польща, Франція тощо [86; 87; 88]. Знайшла вона відображення і в законодавстві сучасної України.

Так, з моменту набуття чинності Закону України від 6 липня 2010 року «Про ратифікацію Страсбурзької конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних» [89] усі положення останньої (зокрема й ті, що розкривають суб'єктивно-правовий аспект захисту персональних даних) були імплементовані в систему вітчизняного законодавства. Закон України «Про захист персональних даних» не тільки декларує ідею захисту персональних даних як основоположного права людини й громадянина (ст. 1), а й наділяє функцією контролю за його дотриманням уповноваженого Верховної Ради України з прав людини (ст. 22, 23) [90].

Таким чином, законодавча парадигма захисту персональних даних вимагає розглядати їх не тільки як напрям людської діяльності чи інститут юридичних норм, а і як елемент правового статусу людини, природну можливість індивіда, що забезпечує його гідність, свободу і безпеку в усіх сферах суспільного життя.

Усебічний аналіз захисту персональних даних неможливий без з'ясування його функціональної спрямованості. Уже зазначалося, що з цього приводу в науці сформовано два підходи. Якщо одні вчені вважають, що захист персональних даних спрямований суто на протидію реальним (фактичним) негативним впливам та запобігання (мінімізацію) їх шкідливим наслідкам, то інша підкреслює системотворчу роль захисту персональних даних, вбачаючи його мету у створенні правових, організаційних і технічних умов, які б гарантували конфіденційність приватного життя людини.

Як видається, така розбіжність поглядів зумовлена неоднозначним розумінням базової категорії «захист» у сучасній теорії права. Більшість правників тлумачить її достатньо вузько: як сукупність заходів, спрямованих на виявлення та припинення правопорушень, притягнення винних до відповідальності, визнання порушених прав і відновлення правовідносин [91, с. 280; 92, с. 18–19; 93, с. 124, 125; 94, с. 9–13]. При цьому майже всі вони розглядають захист як складову широкого поняття (явища) – охорони. «Охорона та захист права чи інтересу – це не одне й те саме, – вказує М. Матузов: Охороняються вони постійно, а захищаються тільки тоді, коли порушуються. Захист – це момент охорони, одна з її форм» [95, с. 130, 131]. Охорона – це загальний правовий режим, натомість захист – це заходи, які застосовуються в разі порушення чи оспорювання права», – додає І. Гаврилов [96, с. 217].

Однак частина науковців не погоджується з таким підходом, доводячи, що захист права полягає не тільки в протидії правопорушенням та відновленні правовідносин, а й у забезпеченні режиму їх стабільного і безпечного

функціонування. Деякі з них вважають охорону окремим проявом захисту [97, с. 217–225], а деякі взагалі не вбачають між ними різниці [98, с. 528, 529].

Далеко не останньою причиною такої розбіжності думок стала недостатньо послідовна позиція законодавця, який у різних нормативно-правових актах наділяє поняття «захист» та «охорона» принципово різним значенням. Інколи ці поняття він інтерпретує як тотожні, інколи – як частину і ціле або навпаки.

Не заглиблюючись у деталі термінологічних розбіжностей, зауважимо, що, попри дещо меншу наукову підтримку в контексті вирішення практичних питань забезпечення прав людини, пов'язаних з обробкою інформації, більш обґрунтованим і доцільним видається широкий підхід до розуміння захисту персональних даних.

По-перше, саме цей підхід лежить в основі інформаційної політики ЄС, заснованої на тому, що: «принципи захисту персональних даних мають бути відображені, з одного боку, у зобов'язаннях, що накладаються на осіб, державні органи влади, підприємства, агентства чи інші органи, які відповідають за обробку, зокрема в тому, що стосується якості даних, технічної безпеки, повідомлення наглядових органів, і обставин, за яких може проводитися обробка, а також у праві, яким наділені фізичні особи, чиї дані підлягають обробці, знати, що обробка дійсно проводиться, звертатися до даних, вимагати внесення змін і заперечувати проти обробки за певних обставин» [85].

По-друге, саме на ньому ґрунтується вітчизняне інформаційне законодавство, зокрема Закон України «Про захист персональних даних». І хоча у цьому законі дефініція поняття «захист персональних даних» немає, узагальнений аналіз його положень свідчить, що захист персональних даних в розумінні законодавця передбачає не тільки протидію порушенням, але й широкий комплекс організаційних та забезпечувальних заходів, а саме: встановлення загальних та

особливих вимог щодо обробки персональних даних, запровадження спеціальної процедури такої обробки, обмеження доступу до персональних даних, створення механізмів контролю та ін. [90].

Євроінтеграційний вектор зовнішньополітичного курсу держави та об'єктивний стан правового регулювання інформаційних відносин дають підстави розглядати захист персональних даних як сферу, котра охоплює широкий спектр правовідносин регулятивного, забезпечувального та охоронного характеру.

Як засвідчив огляд тематичних наукових праць, для формування об'єктивного уявлення про захист персональних даних необхідно чітко визначитись у питаннях про коло суб'єктів такого захисту, а також про те, які саме дані виступають його об'єктом.

Захист персональних даних – вельми складне і багатогранне явище. Хоч би про який його аспект ішлося і хоч би в якому сенсі його розглядали (чи то як напрям діяльності, чи то як право людини, чи то як інститут інформаційного права), незаперечно, що його ефективність залежить від дуже широкого кола суб'єктів. Це і вищі державні структури, які формують нормативно-правову базу та закладають підвалини інформаційної політики, і органи виконавчої влади, котрі провадять захист персональних даних як шляхом реалізації зовнішніх (контрольних, наглядових тощо) повноважень, так і на внутрішньоорганізаційному рівні як володільці відповідних інформаційних баз. Це і уповноважений Верховної Ради України як суб'єкт парламентського контролю за додержанням конституційних прав і свобод людини та громадянина. Це і суди, на яких, поряд із здійсненням правосуддя, покладено функцію контролю за додержанням законодавства про захист персональних даних. Це всі фізичні і юридичні особи, задіяні в процесі обробки персональних даних. І, звичайно ж, це самі володільці персональних даних – не в останню чергу саме від них залежить безпека і конфіденційність інформації персонального характеру.

Зважаючи на викладене вище, не можна визнати обґрунтованою тезу, що захист персональних даних належить до виключної компетенції суб'єктів державної влади [63, с. 72]. Неможливо погодитись і з тими, хто, абсолютизуючи роль володільця персональних даних, стверджує, що їх захист здійснює тільки він особисто або ж за його ініціативою [34, с. 125]. Адже більшість суб'єктів, задіяних у механізмі захисту персональних даних, здійснюють такий захист з огляду на функціональні обов'язки і законні повноваження, а не з волі конкретних осіб.

Таким чином в основі наукового розуміння сутності захисту персональних даних має лежати ідея про його полісуб'єктний характер.

Що ж стосується джерел регулювання відповідної сфери суспільних відносин, то, вочевидь, такими є не тільки норми права, як стверджують деякі науковці, а й інші соціальні регулятори. Захист персональних даних – це явище, що існує на перетині соціальної, правової й технічної сфер людського життя. Воно проявляється не тільки в праві і об'єктивно не тільки ним упорядковується. Нарівні з правом помітну роль у його регулюванні відіграють техніко-технологічні норми (адже, як відомо, першочерговим об'єктом захисту є персональні дані, що піддаються автоматичній обробці). Не варто відкидати можливість впливу норм моралі й корпоративної етики. У перспективі можливе формування звичаїв інформаційного обігу і т.ін.

На цьому тлі будь-які твердження про суто правову природу відносин у сфері захисту персональних даних, а тим більше про їх виключно законодавчу регламентацію, видаються недостатньо обґрунтованими.

Слід, однак, пам'ятати, що саме право впорядковує основний масив суспільних відносин у сфері захисту персональних даних. Саме воно передає цій сфері сутнісну визначеність і системну організацію, гарантує її стабільність у мінливому соціально-технічному середовищі.

Регулятивний вплив права на сферу захисту персональних даних є визначальним, масштабним та всепроникним. І це обов'язково слід врахувати під час формулювання кореспондуючих визначень, доктринальних концепцій і законодавчих положень.

Узагальнюючи викладені міркування та враховуючи багатоаспекність захисту персональних даних, пропонуємо на розгляд широкого загалу такі дефініції:

захист персональних даних як фундаментальне право – це гарантована суспільством можливість збереження конфіденційності й недоторканності приватного життя людини у зв'язку з обробкою даних, котрі її стосуються;

захист персональних даних як інститут права – це виокремлена в рамках галузі інформаційного права система норм, спрямованих на регулювання суспільних відносин з приводу забезпечення прав людини в сфері обробки інформації персонального характеру (тобто інформації, яка дає змогу ідентифікувати конкретну особу);

захист персональних даних як напрям діяльності – це комплекс правових, організаційних, технічних та інших заходів, спрямованих на забезпечення точності, цілісності та конфіденційності персональних даних в ході їх системної обробки (збирання, накопичення, зберігання, використання, поширення, знищення тощо) юридичними та фізичними особами.

1.3. Детермінанти та критерії правової інституціоналізації захисту персональних даних в Україні

Стрімкі темпи інформатизації суспільства та невпинний розвиток інформаційно-комунікаційних технологій відкрили перед людиною нові можливості у сфері накопичення, обробки та використання інформації. Глобальні електронні

мережі, швидкісні комп'ютерні пристрої, мультизадачні операційні системи – ще півстоліття тому ці явища вважались мало не фантастичними. Сьогодні ж вони виступають невід'ємним атрибутом повсякденного життя.

Без належного інформаційного забезпечення не мислиться прогрес у жодній суспільно значущій сфері: економічній, політичній, адміністративній, науковій та інших. Широкий доступ до інформаційних потоків є свідченням сталих демократичних процесів, гарантією свободи слова, непорушності права на інформацію, що передбачає можливість вільного одержання, використання, поширення та зберігання інформації, необхідної для реалізації своїх прав, свобод і законних інтересів.

Однак безконтрольне поширення інформації здатне призвести до негативних наслідків. За певних умов воно може створити загрозу національним інтересам країни, дезорганізувати роботу державних структур, спровокувати масштабні соціальні конфлікти, порушувати громадянські, політичні, економічні, соціальні, духовні, екологічні та інші права, свободи і законні інтереси людей, права та інтереси юридичних осіб.

У світлі викладеного з неабиякою гостротою постає проблема захисту персональних даних, тобто відомостей про фізичну особу, на підставі яких її можна ідентифікувати. Історія знає чимало прикладів, коли збирання, систематизація та використання відомостей персонального характеру здійснювалися з намірами, далекими від ідей суспільного чи особистого блага. Потрапивши у брудні руки, інформація про особу нерідко ставала потужним інструментом впливу на її волю, рішення і вчинки, силою, що руйнувала приватність її життя, чинником тиску на її найближче оточення.

Усвідомлюючи масштаби проблеми та загрозу її ескалації з подальшим розвитком електронних технологій, європейська спільнота розглядає захист персональних даних як пріоритетний напрям інформаційної політики. На сьогодні в більшості країн Європи ухвалено спеціалізовані закони про

захист персональних даних, створено інститути незалежних контролерів із їх захисту, визначено принципи та умови обробки у публічному та приватному секторах.

Не лишається осторонь цих процесів і наша держава. Протягом кількох останніх років в Україні реалізовано широкий комплекс правових та організаційних заходів, спрямованих на побудову ефективного механізму захисту персональних даних. Це зокрема ратифікація низки важливих актів міжнародного інформаційного законодавства, ухвалення національного закону про захист персональних даних, створення системи контролю за станом дотримання законності у відповідній сфері, залучення до цієї системи уповноваженого з прав людини, і впорядкування процедур автоматизованої обробки персональних даних, запровадження Стратегії розвитку інформаційного суспільства, яка визнала захист персональних даних пріоритетом державної діяльності в галузі гарантування інформаційної безпеки, і багато інших [89; 90; 99].

Сучасний стан і тенденції розвитку сфери захисту персональних даних дають змогу констатувати невпинне розширення її меж, урізноманітнення охоплених нею відносин та збільшення ступеня її правової регламентації, яке втілилось у формуванні вельми обширного масиву юридичних норм. Цей масив постійно збагачується та набуває дедалі більшої соціальної ваги, що зумовлює необхідність його поглибленого вивчення.

Дивно, але попри значний науковий інтерес до захисту персональних даних, його місце у вітчизняній системі права ґрунтовно не досліджували. З одного боку, це можна пояснити тим, що основна увага науковців зосереджена на вивченні функціонального аспекту цього явища (більшість учених вбачає у ньому певний напрям діяльності та елемент державної системи захисту інформації). З іншого – система правового захисту персональних даних перебуває у фазі становлення, тож вітчизняна наука просто не встигла напрацювати необхідний теоретичний багаж.

Лише окремі правники (А. Баранов, В. Брижко, Ю. Казанов, А. Чернобай) намагаються розглянути захист персональних даних під кутом об'єктивного права та ідентифікувати його як цілісну систему правових норм. Однак при цьому вони здебільшого обмежуються констатацією його інституційної природи, не вдаючись до детального аргументування своїх висновків.

Як наслідок, маємо тимчасову невизначеність критеріїв правової інституціоналізації захисту персональних даних та принципові розбіжності в поглядах на його галузеву належність.

Наприклад, А. Марущак вбачає у захисті персональних даних окремий суб'інститут інформаційного права, який виділяється в рамках інституту захисту інформації, поряд із суб'інститутами технічного захисту інформації, технічного захисту інформації в автоматизованих системах та іншими [100, с. 97].

У наукових працях В. Брижка обстоюється думка про цивільно-правову природу захисту персональних даних. Свою позицію автор обґрунтовує тим, що «персональні дані в статусі інформації через свою унікальність, зміст рис і делікатність в поводженні з ними розміщуються, так би мовити, на стику (на межі) двох відомих юридичних інститутів – права власності та права використання… Сумісність негативного і позитивного статусу (змісту) повноважень людини на свої персональні дані щодо зазначених інститутів дозволяє запропонувати нову юридичну категорію і створити новий правовий інститут державного упорядкування суспільних інформаційних відносин у сфері захисту персональних даних» [9, с. 82].

А. Чернобай пропонує виокремити інститут захисту персональних даних у системі трудового права в межах такого її структурного елемента, як індивідуальне трудове право [34, с. 4].

Аналогічна розбіжність думок спостерігається й серед представників російської правової науки. Здебільшого вони розглядають питання захисту персональних даних або з позицій інформаційного права (як особливий інститут захисту права на недоторканність), або виключно з позицій трудового законодавства, оскільки «належність інформації до конкретного суб'єкта правовідносин (працівника) є домінантним чинником, що визначає специфіку трудового правовідношення в контексті з інформаційною складовою» [101, с. 5, 6], або ж як комплексний міжгалузевий інститут, сформований на базі одразу кількох галузей права.

Зокрема, А. Дворецький, аналізуючи захист персональних даних в розрізі трудових правовідносин, наголошує, що виокремлення цього інституту в трудовому праві обумовлене потребами індивідуалізації правового статусу працівника, захисту конституційного права на захист приватного сфери, відображенням міжнародних тенденцій щодо посилення захисту особистих прав [102, с. 41].

Виокремлюючи однойменний інститут у структурі галузі інформаційного права, І. Вельдер визначив його як сукупність правових норм, спрямованих на регламентацію суспільних відносин, що виникають під час збирання, використання, зберігання, обробки, вилучення, передачі та розкриття інформації, пов'язаної з особою, що ідентифікована чи може бути ідентифікована [68, с. 36].

О. Федосін вважає це трактування не зовсім правильним, оскільки «вона не в повній мірі розкриває суспільні відносини, врегульовані правовим інститутом захисту персональних даних, ігноруючи їх правозахисний характер. Означені відносини хоч і належать до інформаційної сфери, мають конституційно-правову основу та пов'язані із забезпеченням права особи на недоторканність приватного життя, а також суміжних із ним прав в умовах розвитку технологій автоматизованої обробки інформації» [69, с. 59]. На думку цього автора, положення інституту захисту персональних даних

містяться в нормах конституційного, інформаційного, адміністративного, трудового права, що дає підстави констатувати його міжгалузевий характер [69, с. 60, 70].

У деяких принципових моментах поділяє цю думку А. Маркевич, стверджуючи, однак, що інститут захисту персональних даних утворюють не тільки норми різних галузей права, а й доктринальні положення відповідних галузевих правових наук [101, с. 7].

Попри відсутність консолідованої позиції щодо розуміння галузевої належності правового захисту персональних даних, здобутки російських правників достатньо вагомі. На сьогодні їм вдалося досягти помітного прогресу в питаннях визначення принципів захисту персональних даних, з'ясування підстав його інституціоналізації, окреслення пріоритетів його розвитку та ін. Проте й у вітчизняній, і в російській правовій науці ці питання все ще далекі від остаточного розв'язання.

Більшість сучасних дослідників презюмують інституційну природу захисту персональних даних, вбачаючи в ньому новий інститут права, тобто відносно відокремлену сукупність правових норм, які регулюють певну сферу суспільних відносин [103, с. 315, 316].

З такою точкою зору важко не погодитися. Поява нових інститутів права – це абсолютно закономірний процес, зумовлений соціально-економічним розвитком, науково-технічним прогресом, загальним рівнем правосвідомості, генезисом законодавства та регульованих ним суспільних відносин. І цілком очевидно, що сьогодні в деяких країнах пострадянського простору (зокрема Україні, Білорусі, Росії) сформувалися передумови для інституційного відокремлення норм, спрямованих на регламентацію сфери захисту персональних даних. У них чинні спеціалізовані закони та підзаконні нормативно-правові акти, створено кореспондуючу ланку дер-

жавного управління, сформовано доктринальну концепцію захисту персональних даних як особливого напряму діяльності, окремої сфери суспільних відносин та осібної системи правових норм.

Однак лише поодинокі вчені роблять спроби обґрунтувати свою позицію та визначити критерії, за якими захист персональних даних визнається самостійним інститутом права. До того ж, і ці спроби не завжди вдалі.

Прикладом може слугувати висновок про те, що «для повноцінного функціонування інституту захисту персональних даних в країні потрібне розроблення і введення в дію не менш як 20 підзаконних нормативно-організаційних актів» [9, с. 76].

Обґрунтованість такого критерію, а тим більше науковість визначення його кількісних параметрів викликають серйозні сумніви. Дійсно, без створення нормативно-правового підґрунтя інститут права існувати не може, оскільки саме нормативно-правові акти є головним вмістилищем його норм. Однак це стосується не тільки інститутів, а й національної системи права загалом. Нормативно-правовий акт – її основне джерело та форма, поза якими не мислиться ні вона сама, ні її окремі складові: галузі, підгалузі, інститути тощо. Таким чином, нормативно-правова база виступає об'єктивною передумовою існування права, але в жодному разі не критерієм його інституційної структуризації.

Що ж до кількості нормативно-правових актів, необхідних для створення певного інституту, то її точне визначення *a priori* неможливе. Нині існує чимало сфер правового регулювання, які попри більш ніж детальну нормативну регламентацію, не зумовили появи самостійних інститутів. І навпаки – багато визнаних інститутів права охоплюють відносно незначну кількість норм та мають вельми значну нормативну базу. На цьому тлі будь-які точні розрахунки видаються непереконливими. «Думається, кількісний критерій тут незастосовний, – пише О. Керімова, – теоретично пра-

вовий інститут може складатись навіть з однієї норми, якщо вона забезпечує самостійний регуляторний вплив на певну ділянку суспільних відносин» [104, с. 15].

Загалом проблема визначення критеріїв правової інституціоналізації захисту персональних даних доволі складна. Адже у вітчизняній правничій думці досі не сформоване єдине уявлення про підстави для окреслення структурних елементів права. Виняток становить хіба що поділ права на галузі, підстави якого отримали певну доктринальну визначеність. Водночас на підгалузевому (інституційному) рівні такі підстави залишаються малодослідженими.

Як засвідчив проведений аналіз, в основу виокремлення інститутів права здебільшого покладаються предметна відокремленість та специфіка способу (методу) впливу на суспільні відносини [105, с. 62, 63; 106, с. 314]. Крім того, до критеріїв інституціоналізації правових норм прийнято зараховувати їх здатність самостійно впорядковувати певну сферу суспільних відносин, наявність спільної мети й загальних принципів функціонування [107, с. 26–35]. Погоджуємось також і з тими вченими, які зараховують до ознак інституту права створення «власної», специфічної термінології [104, с. 14].

Чи наділені цими ознаками норми, спрямовані на регламентацію суспільних відносин у сфері захисту персональних даних? Для відповіді на це запитання проаналізуємо їх об'єктивний стан та системні характеристики.

Цілком очевидно, що ця група норм регламентує осібне коло суспільних відносин, яке рельєфно окреслилось у світовій та вітчизняній суспільно-правовій практиці. Кореспондуючі відносини функціонують у різних галузях, але водночас зберігають риси системної єдності. Вони складаються навколо одного предмета, мають спільні цілі. Між ними існують багатогранні взаємозв'язки. Вони взаємообумовлені та взаємозалежні в плані стабільності, повноти й ефективності.

Ці відносини якісно однорідні, вони виконують єдину соціальну функцію, виникають з однорідних підстав, мають вельми подібну структуру. Однак їм властива певна міра автономності. Існуючи в рамках окремого напряму соціально-технічної діяльності, вони утворюють відносно ізольовану сферу суспільного життя, що передбачає системну відокремленість норм, спрямованих на їх регулювання.

На підставі викладеного можемо констатувати, що захист персональних даних як система юридичних норм характеризується наявністю специфічного предмета регламентації, який, з одного боку, займає особливу нішу в загальній системі соціальних зв'язків, з іншого – чітко окреслює межі її функціонування та регуляторного впливу.

Щодо специфіки способів (методу) впливу цих норм на суспільні відносини слід сказати таке. Як відомо, метод правового регулювання – це ніщо інше, як прийом регуляторного впливу, властивий більшості норм певної групи. Відповідно його суть визначається тим, які саме норми (дозвільні, заборонні або наказові) в цій групі домінують.

З огляду на відносно невелику кількість норм, спрямованих на регулювання суспільних відносин у сфері захисту персональних даних, встановити їх домінантний тип нескладно. Цілком очевидно, що здебільшого вони мають зобов'язальний характер. А це дає підстави констатувати ознаки імперативного методу правового регулювання.

Слід мати на увазі, що, на відміну від предмета регулювання, метод – суто допоміжний критерій інституціоналізації захисту персональних даних. За цим критерієм можуть бути розмежовані лише інститути публічного та приватного права (адміністративного і цивільного, інформаційного й господарського і т.ін.). Проте якщо цей критерій досить добре спрацьовує на рівні різних галузевих груп, то всередині них спостерігається зовсім інша ситуація.

Оскільки більшість інститутів права використовують метод кореспондуючої материнської галузі, то розрізнити за цим критерієм інститути однієї галузі або ж кількох споріднених майже неможливо. Зважаючи на це, в нашому випадку цей критерій свідчить не стільки про структурну відокремленість системи норм, спрямованих на захист персональних даних, скільки про її змістову однорідність, функціональну єдність та внутрішню узгодженість.

Як вже було зазначено, у вітчизняній теорії права одним із критеріїв інституціоналізації нормативно-правових утворень вважається наявність у них спільної мети. З таким підходом важко не погодитись. Адже передусім саме ознака цілеспрямованості дає підстави вбачати у певному наборі елементів цілісну функціональну систему, орієнтовану на вирішення складних комплексних завдань.

Аналіз чинного законодавства та практики застосування норм про захист персональних даних свідчить, що кожна з них, виконуючи окреме локальне завдання, неодмінно спрямована на загальну соціальну мету – забезпечення конфіденційності приватного життя людини під час обробки пов'язаної з нею інформації. Ця мета не просто зумовлює їх спрямованість та фактичний зміст, вона детермінує необхідність їх системної взаємодії в рамках окремого підрозділу вітчизняного права.

Водночас ця мета і сама підпорядковується глобальним цілям правового регулювання у сфері гарантування інформаційної безпеки людини, суспільства, держави. Тож у цьому аспекті її можна розглядати як один із критеріїв визначення галузевої належності захисту персональних даних.

У рамках питання про інституційну природу норм про захист персональних даних важливо з'ясувати їх здатність самостійно врегульовувати кореспондуючу сферу суспільних відносин. Адже саме ця ознака свідчить про функціональну єдність того чи іншого нормативного блоку. І саме вона дає змогу вбачати у ньому відносно ізольовану систему, котра не просто спрямована на певну мету, а й наділена достатнім потенціалом її реалізації.

Аналіз правового забезпечення захисту персональних даних дає змогу зробити висновок про те, що ця група норм функціонує автономно, забезпечуючи максимальне охоплення кореспондуючої сфери суспільних відносин. Зокрема, нею визначаються загальні та особливі вимоги щодо обробки персональних даних, встановлюється порядок їх збирання, накопичення, зберігання та поширення, окреслюються умови доступу до їх змісту, впорядковується організація їхнього захисту, запроваджуються механізми контролю за додержанням законності. Фактично на рівні цієї нормативної групи врегульовано більшість аспектів захисту персональних даних (інституційний, організаційний, правосуб'єктний, процедурний та інші), що дає змогу говорити про самостійний характер та повноту її регуляторного впливу.

Однак у цьому контексті не йдеться про абсолютну самостійність і вичерпність правового регулювання. Навряд чи у вітчизняній системі права знайдеться бодай один інститут або галузь, які б цілком самостійно, за рахунок тільки свого нормативного інструментарію забезпечували вичерпну регламентацію певної сфери суспільних відносин. «Не існує підсистем права, цілковито відокремлених, – пише О. Черданцев. У суспільстві не буває абсолютно ізольованих сфер відносин, тож і їх правове регулювання, і їх охорона не можуть провадитись у відриві від інших норм, інститутів, галузей» [108, с. 66].

Сфера захисту персональних даних – не виняток. У ній, а також навколо неї складаються найрізноманітніші за характером суспільні відносини, які потребують усебічного правового регулювання, правової охорони та правового захисту. Деяка їх частина через специфіку природи та змісту належить до предметів (читай – сфери регламентації) традиційних галузей права: адміністративного, кримінального, трудового та інших. І саме на ці галузі та їх окремі інститути покладається функція їх регламентації.

З огляду на викладене було б помилкою стверджувати, що сфера захисту персональних даних цілком і повністю впорядко-

вується засобами окремого нормативного блоку. В її регламентації задіяно низку галузей та інститутів вітчизняного права, і це очевидно. Але не менш очевидно й те, що з точки зору загального функціонування цієї сфери роль традиційних правових утворень далека від провідної. Вони регулюють тільки окремі аспекти захисту персональних даних і не визначають його фундаментальних засад: цілей, принципів, напрямів, форм, організації тощо. Натомість впорядкування ключових правовідносин у сфері захисту персональних даних забезпечується якісно та функціонально осібною системою правових норм.

Викладене дає підстави для висновку, що система норм про захист персональних даних самостійно регламентує кореспондуючу сферу правовідносин, але таку самостійність слід вважати відносною – вона проявляється не у впливі на всі відносини, а в здатності регулювати їх основний масив.

За визнанням авторитетних правників, ще одним свідченням юридичної однорідності та системної єдності норм права є наявність «специфічної групи понять, загальних положень і термінів, які використовуються для розкриття змісту їх приписів» [109, с. 121–124]. Екстраполюючи цей критерій на систему правового регулювання захисту персональних наданих, доходимо висновку, що на сьогодні відповідна група правових норм має достатньо міцний термінологічний фундамент.

Упродовж останніх років міжнародне та національне законодавство про захист персональних даних запровадило в обіг багато спеціальних понять, які відображають специфіку кореспондуючої сфери правовідносин. Це зокрема такі поняття: персональні дані, обробка персональних даних, володілець персональних даних, розпорядник персональних даних, вразливі персональні дані та багато інших. Усі вони пов’язані між собою у стрункy формально-логічну систему. Вони взаємообумовлені, взаємодоповнювані та взаємозалежні. У сукупності вони утворюють стійкий понятійний

апарат, наділений ознаками смислової єдності та загальної спрямованості.

Звісно, деякі елементи (поняття) цього апарату використовують інші інститути й галузі права, що цілком закономірно. Адже всі складові системи права функціонують у тісному взаємозв'язку, і жодна з них не може претендувати не ексклюзивність використовуваної термінології. Проте ця обставина нітрохи не впливає на уявлення про термінологію захисту персональних даних як про цілісний, концептуально відокремлений комплекс понять. Навпаки – вона свідчить про здатність відповідного блоку правових норм взаємодіяти з різними галузями (інститутами) права на первинному, понятійному рівні. І це ще один аргумент на користь його інституційної природи.

Важливим свідченням системної єдності норм про захист персональних даних є наявність спільних принципів функціонування. Сьогодні не викликає жодних сумнівів той факт, що захист персональних даних як регламентована правом діяльність здійснюється на основі фундаментальних положень (ідей, принципів), вироблених правовою доктриною та конкретизованих у міжнародному законодавстві. Наявність іманентних принципів захисту персональних даних констатують фактично всі галузеві дослідники. Вважаємо цей висновок правильним, обґрунтованим і підтвердженим практикою. З одного боку, він відображає об'єктивні закономірності захисту персональних даних, з іншого – свідчить про системність його правової регламентації та інституційну природу відповідного комплексу юридичних норм.

Здавалося б, в умовах загальновизнаності принципів захисту персональних даних визначення їх суті не має становити проблеми. Насправді ситуація інша. Попри одностайне визнання факту існування цих принципів, вітчизняні науковці по-різному інтерпретують їх природу, зміст і спрямованість.

Наприклад, В. Серьогін пропонує вважати такими: а) принцип законності; б) принцип цільової визначеності; в) принцип мінімальності; г) принцип якості інформації; ґ) принцип участі суб'єкта даних та здійснення ним контролю; д) принцип обмеження розкриття персональних даних; е) принцип інформаційної безпеки; є) принцип урахування чутливості інформації [110, с. 199].

З точки зору А. Чернобай, до основних принципів захисту персональних даних належать: конфіденційність одержуваних персональних даних, обмеження доступу до них інших осіб; достовірність і повнота персональної інформації, а також заборона включення в персональні дані недостовірних фактів; цільовий характер персональної інформації; вільний доступ суб'єкта до своїх персональних даних і право на повну інформацію про них [34, с. 145, 146].

В. Брижко наголошує, що, «в умовах активного розвитку процесів інформатизації захист персональних даних може і повинен бути забезпечений правовими засобами, *які базуються на принципах упорядкування суспільних відносин щодо майна, авторського чи патентного права* шляхом створення особливого інституту права власності людини на свої персональні дані» [111, с. 97] *(курсив мій. – А.П.)*. Крім того, в роботах цього автора виділяються: принципи поділу персональних даних за критерієм чутливості, окремого збереження персональних даних, обов'язкової згоди на обробку персональних даних, а також об'єктивності, згідно з яким персональні дані не можна обробляти виключно з метою виявлення фактів, котрі характеризують людину лише негативно [9, с. 126, 197, 198].

Не заглиблюючись у специфіку різних наукових підходів (це питання варте окремого дослідження), зауважимо, що розбіжності, які існують між ними, вносять чималий розлад у формування єдиної концепції захисту персональних даних як специфічного напряму діяльності й елемента системи права. З нашої точки зору, головним орієнтиром при визначенні принципів захисту персональних даних мають стати положення міжнарод-

ного законодавства, котре акумулювало багатий світовий досвід у сфері регулювання інформаційних відносин та захисту права на конфіденційність приватного життя.

Як цілком справедливо підкреслює знаний грецький дослідник Спірос Сімітіз (Σπύρος Σημίτης), проблема захисту персональних даних в індустріальних країнах має однакове походження і потребує однакового розв'язання. У демократичному суспільстві воно покликане підтримувати оптимальний баланс прав людини, суспільства і держави. Засобом встановлення цього балансу виступає правовий режим захисту персональних даних, заснований на визначених принципах, єдиних для всіх демократичних держав, незалежно від особливостей їхніх правових систем [112, с. 49].

На сьогодні такі принципи знайшли відображення в багатьох міжнародних правових документах: Керівних настановах, що регулюють захист приватності й транскордонні потоки персональних даних від 23 вересня 1980 року Організації економічного співробітництва та розвитку, Страсбурзькій конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних від 28 січня 1981 року, директиві Європейського парламенту і Ради ЄС від 24.10.1995 № 95/46/ЄС «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних», директиві Європейського парламенту і Ради ЄС від 12 липня 2002 року № 2002/58/ЄС «Про обробку персональних даних та захисту права на недоторканість особистого життя у сфері електронних комунікацій», пропозиціях Європейської комісії стосовно захисту прав людини у зв'язку з обробкою та поширенням персональних даних від 25 січня 2012 р. С7-0025/2012 та інших [84; 85; 113; 114; 115].

Попри наявність деяких незначних відмінностей, зумовлених розвитком сфери обробки персональних даних та конкретизацією її правового регулювання, на підставі актів міжнародного законодавства можна сформулювати достатньо чіткий концептуально цілісний перелік принципів захисту персональних даних. До нього входять:

принцип законності – полягає у тому, що обробку персональних даних можна здійснювати тільки на законних підставах, для законних цілей, добросовісним і законним способом;

принцип відкритості – не може бути систем обробки персональних даних, існування яких є таємницею;

принцип доцільності – означає, що обробка персональних даних можна здійснювати тільки для чітко визначених законних цілей, а також у спосіб, що відповідає їм;

принцип адекватності – персональні дані можна обробляти в кількості, мінімально необхідній для досягнення поставлених цілей (персональні дані не можуть бути надлишковими стосовно цілей їх обробки);

принцип достовірності – персональні дані мають бути точними, достовірними та оновлюватися в міру потреби; неточні дані з урахуванням цілей їх обробки підлягають виправленню або знищенню;

принцип обґрунтованості – персональні дані не можна зберігати та обробляти довше, ніж це зумовлено цілями їх обробки;

принцип конфіденційності – доступ до персональних даних може бути надано тільки уповноваженому персоналу у визначеному законом порядку та лише в законних цілях;

принцип збереження персональних даних – персональні дані мають бути захищені від випадкового чи незаконного знищення, втрати та змін, несанкціонованого доступу, незаконного зберігання, обробки та розкриття;

принцип заборони на обробку вразливих персональних даних – заборонено обробку персональних даних, що вказують на расове чи етнічне походження, політичні погляди, релігійні чи філософські переконання, профспілкове членство, а також даних, що стосуються здоров'я чи статевого життя людини;

принцип свободи волевиявлення – не допускається обробка даних про фізичну особу без її недвозначної згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини; кожен суб'єкт має право на законних підставах заперечувати про обробку пов'язаних з ним персональних даних, відкликати раніше надану згоду на обробку таких даних, а також вимагати їх зміни або знищення;

принцип обов'язкового інформування – якщо дані не було отримано від суб'єкта даних, його слід проінформувати про обробку таких даних, цілі такої обробки, оператора обробки та одержувачів персональних даних, крім випадків, передбачених законом;

принцип вільного доступу до власних персональних даних – кожному гарантується доступ до його персональних даних, а також до пов'язаної з ними інформації, зокрема про особу контролера персональних даних, цілі обробки, її логіку, одержувачів (категорій одержувачів) тощо.

Ці принципи не просто фундують ідеологічну базу захисту персональних даних, а й мають самостійну нормативну силу. Викладені у формі чітких нормативних приписів, вони обов'язкові для врахування та виконання всіма уповноваженими суб'єктами захисту персональних даних, в тому числі суб'єктами нормотворчої й правозастосовної діяльності. Цілком слушно наголошує В. Серьогін: «Ці принципи є зразком для наслідування при творенні інформаційного законодавства технологічно розвинених країн та базисом для розробки нових положень з питань інформаційної безпеки, захисту прайвесі» [110, с. 199].

Це стосується й нашої держави, яка на вищому політичному рівні задекларувала курс зближення з ЄС на основі спільних цінностей, уніфікації законодавства, посилення взаємодії у сфері юстиції, безпеки, захисту прав і свобод людини та громадянина. Поза всяким сумнівом, загально-

визнані принципи захисту персональних даних мають знайти максимально повне і точне відображення у вітчизняному інформаційному законодавстві, зокрема, в Законі України «Про захист персональних даних».

У контексті аналізу системно-функціональних аспектів правової регламентації захисту персональних даних чималий інтерес становить питання про галузеву належність кореспондуючих юридичних норм. Як уже зазначалося, в цьому питанні сучасна наука ще не дійшла однозначного висновку. Констатуючи важливе значення та непересічну роль захисту персональних даних в тій або іншій сфері правового регулювання, різні вчені вносять його у структуру різних галузей права. Хтось вважає його складовою цивільного права, хтось – конституційного, хтось – трудового, а хтось – інформаційного (і це попри те, що галузева парадигма інформаційного права на пострадянському просторі концептуально не сформована).

Захист персональних даних – і як діяльність, і як система правових норм – реалізується в багатьох царинах суспільного життя, охоплює різноманітні сфери суспільних відносин, інтегрується в різні галузі правового регулювання. Зважаючи на це, відповідний нормативний блок має тісні взаємопроникні зв'язки з кількома галузями права. Його першочергова мета – захист конституційного права людини на конфіденційність приватного життя. В основі предмета його регламентації лежать цивільно-правові відносини власності та користування. Кореспондуюча група правових норм акумульована в актах інформаційного законодавства. Провідною сферою їх застосування виступають трудові відносини.

У світлі викладеного включення норм про захист персональних даних до структури окремої галузі права видається необґрунтованим. Ця група норм регламентує відносини на стику регулювання різних юридичних галузей, забезпечує вирішення їх завдань, несе відбиток їх іманентних властивостей, тож має комплексний міжгалузевий характер.

Узагальнюючи проведений аналіз, можемо констатувати, що правові норми з питань захисту персональних даних являють собою цілісну інтегральну систему, яка:

– спрямована на регламентацію визначеної, чітко окресленої сфери суспільних відносин, тобто характеризується наявністю специфічного предмета регулювання;

– впливає на суспільні відносини переважно шляхом встановлення правових зобов'язань, отже використовує імперативний метод регламентації;

– має єдину (загальну) соціальну мету – забезпечення конфіденційності приватного життя людини у разі обробки пов'язаної з нею інформації;

– забезпечує комплексне регулювання основного масиву правовідносин у сфері захисту персональних даних;

– зумовила розробку та нормативне закріплення спеціального термінологічного апарату;

– ґрунтується на єдиних ідеологічних засадах (принципах), вироблених правовою доктриною, верифікованих практикою, формалізованих у міжнародному, зарубіжному та вітчизняному законодавстві;

– перебуває в тісному взаємозв'язку та системній взаємодії з провідними галузями права: конституційним, цивільним, трудовим, адміністративним та ін.

Наявність перелічених ознак дає змогу розглядати систему норм про захист персональних даних як комплексний міжгалузевий інститут, який реалізує важливу соціальну функцію та посідає окреме місце у структурі вітчизняного права.

***

Аналіз сучасних правових досліджень свідчить про постійне зростання інтересу до питань захисту персональних даних. Дедалі частіше вони стають предметом ґрунтовного вивчення та широкого наукового обговорення. Їм присвячені десятки міжнародних і загальнодержавних конференцій. Вони знаходять відображення на сторінках численних науко-

вих (в тому числі капітальних) праць. При цьому особлива активізація їх наукової розробки мала місце упродовж останнього часу: якщо протягом 2003–2005 рр. питання захисту персональних даних лягли в основу чотирьох дисертацій з юридичних наук, то в 2009–2012 рр. таких дисертацій було захищено втричі більше – 12.

Загалом науковий доробок з питань правового захисту персональних даних характеризується високим рівнем актуальності, наукової новизни та практичної значущості. Більшість тематичних досліджень здійснено на основі передового зарубіжного досвіду, з урахуванням міжнародних стандартів і світових тенденцій забезпечення інформаційної безпеки. Їх висновки та пропозиції знайшли широке практичне втілення, зокрема в нормотворчій і правозастосовній діяльності. Первинно саме на доктринальному рівні було обґрунтовано доцільність ухвалення Закону «Про захист персональних даних», юридичної відповідальності за порушення правил обробки конфіденційної інформації, створення недержавної системи інституціонального контролю, а також багатьох інших кроків, здійснених у ході реалізації національної інформаційної політики.

Однак сучасний стан науково-правового забезпечення захисту персональних даних неможливо визнати досконалим. За браком дієвого зв’язку між наукою та практикою широкий спектр нагальних проблем залишається нерозв’язаним. Спеціальні дослідження провадяться безсистемно та переважно з ініціативи самих науковців. Практичне впровадження їх результатів надто повільне, іноді вони роками не знаходять реалізації.

Для розв’язання проблем необхідно внести питання наукового забезпечення захисту персональних даних до державних цільових програм і планів інформаційного розвитку; визначити коло проблем, які потребують першочергового наукового роз-

в'язання; окреслити пріоритетні напрями досліджень у сфері захисту персональних даних, забезпечити їх цільове фінансування та ґрунтовну розробку охопленої ними тематики; здійснювати постійне інформування суб'єктів захисту персональних даних про наявні наукові дослідження та перспективи їх практичної реалізації; всебічно стимулювати розробку малодосліджених аспектів інформаційної безпеки; налагодити тісну взаємодію між профільними навчальними закладами (науково-дослідними установами) та суб'єктами правовідносин у сфері захисту персональних даних.

Цілком очевидно, що ефективне правове забезпечення захисту персональних даних неможливе без створення надійного теоретичного підґрунтя, зокрема, без вирішення питань про його природу, сутність, визначальні ознаки та принципи.

Аналіз провідних доктринальних концепцій, положень інформаційного законодавства та сучасної правозастосовної практики дає змогу розглядати захист персональних даних у трьох аспектах: а) як фундаментальне право людини; б) як напрям діяльності; в) як інтегральну систему юридичних норм.

Правові норми з питань захисту персональних даних характеризуються наявністю загального предмета регулювання, використовують імперативний метод регламентації, спрямовані на досягнення єдиної мети, забезпечують комплексне регулювання правовідносин у сфері захисту персональних даних, формують спеціальний термінологічний апарат, перебувають в тісному взаємозв'язку та системній взаємодії з провідними галузями права, ґрунтуються на спільних принципах.

Перелічені ознаки дають підстави для висновку, що норми про захист персональних даних являють собою комплексний міжгалузевий інститут, який реалізує важливу соціальну функцію та посідає особливе місце у структурі вітчизняного права.

РОЗДІЛ 2. ОРГАНІЗАЦІЙНО-ПРАВОВИЙ МЕХАНІЗМ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

2.1. Нормативно-правове регулювання захисту персональних даних

Інституціоналізація захисту персональних даних як складової системи права та напряму державної інформаційної політики актуалізує питання розроблення досконалої нормативної бази, яка гарантувала б стабільність правовідносин, ефективність правозастосування, баланс між правом людини на конфіденційність особистого життя та суспільними інтересами в інформаційній сфері.

Передусім від якості правового забезпечення залежить стан інформаційної безпеки людини, суспільства, держави. Досконала правова база оптимізує та зміцнює сферу інформаційних відносин, роблячи її толерантною до внутрішніх і зовнішніх загроз. Натомість вади правової регламентації чинять деструктивний вплив. Вони дестабілізують кореспондуючі соціальні зв'язки, провокують конфлікти між їх суб'єктами, створюють передумови для маніпуляцій, зловживань та утисків.

Саме в площині правового регулювання слід шукати витоки численних організаційних проблем та системних збоїв механізму захисту персональних даних. Рік у рік зростає кількість випадків несанкціонованого доступу та використання конфіденційної інформації, збільшується число нелегальних інформаційних баз, зростає кількість правопорушень. Вочевидь, ці тенденції матимуть місце доти, доки не буде усунуто системні вади законодавства про захист персональних даних. Адже на хиткому правовому фундаменті неможливо побудувати (і тим більше реалізувати) успішну стратегію інформаційної безпеки.

Усе це зумовлює необхідність удосконалення правового захисту персональних даних. З цією метою доцільно провести ґрунтовний аналіз галузевого законодавства, висвітлити пов'язану з ним проблематику, окреслити перспективні напрями його розвитку.

Зважаючи на велике розмаїття суспільних відносин у сфері захисту персональних даних, їх регламентація забезпечується широким колом правових актів: Конституцією, законами України, підзаконними актами Президента, Кабінету Міністрів, центральних і місцевих органів виконавчої влади, інших державних органів, а також міжнародними договорами України, згоду на обов'язковість яких надала Верховна Рада.

Як і будь-який інший напрям державної інформаційної політики, захист персональних даних провадиться на засадах, визначених Основним Законом – *Конституцією України*. Норми Конституції слугують наріжним каменем галузевого законодавства, нормотворчої та правозастосовної практики. Втілювані ними ідеї пронизують усі аспекти інформаційної діяльності. Вони гарантують право громадянина на захист від втручання в особисте та сімейне життя, на спростування недостовірної інформації про себе та членів своєї сім'ї, на відшкодування матеріальної і моральної шкоди, завданої збиранням, зберіганням, використанням та поширенням недостовірної інформації. Через вплив на систему правових, державних та суспільних інститутів Конституція закладає підвалини гарантування інформаційної безпеки та реалізації інформаційних інтересів.

Конституційне регулювання сфери захисту персональних даних здійснюється як на загальному рівні (шляхом встановлення фундаментальних засад життєдіяльності людини, суспільства і держави), так і на рівні конкретних суспільних відносин.

Зокрема, ст. 32 Конституції проголошує: «Ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України. Не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини. Кожний громадянин має право знайомитися в органах державної влади,

органах місцевого самоврядування, установах і організаціях з відомостями про себе, які не є державною або іншою захищеною законом таємницею». У ст. 34 Основного Закону поряд із правом вільно збирати, зберігати, використовувати та поширювати інформацію визначено, що його здійснення може бути обмежене законом для запобігання розголошенню інформації, одержаної конфіденційно [116].

Слід зауважити, що до останнього часу в колі науковців і практиків єдиного розуміння наведених положень фактично не існувало. Найбільша кількість дискусій точилися навколо трьох питань: «Що саме потрібно розуміти під інформацією про особисте і сімейне життя?», «Чи належить така інформація до конфіденційної інформації про особу (читай – до персональних даних)?» та «Чи вважається збирання, зберігання, використання й поширення інформації про особу втручанням в її особисте і сімейне життя?». Невизначеність цих питань вносив різнобій у діяльність публічної адміністрації, стояла на заваді справедливому правосуддю, провокувала конфлікти в реалізації конституційних прав на інформацію та невтручання в особисте і сімейне життя людини.

Однак на початку 2012 року дискусіям про конфіденційну природу особистої інформації було покладено край. Розглянувши справу за поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України, Конституційний Суд України визначив:

– інформацією про особисте та сімейне життя особи є будь-які відомості та/або дані про відносини немайнового та майнового характеру, обставини, події, стосунки тощо, пов’язані з особою та членами її сім’ї, за винятком передбаченої законами інформації, що стосується здійснення особою, яка обіймає посаду, пов’язану з виконанням функцій держави або органів місцевого самоврядування, посадових або службових повноважень;

– така інформація про особу є конфіденційною;

– збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди державою, органами місцевого самоврядування, юридичними або фізичними особами є втручанням у її особисте та сімейне життя, що допускається виключно у випадках, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини [117].

Нині саме цей підхід покладено в основу правового регулювання відносин у сфері захисту персональних даних. Його врахування обов'язкове під час розробки та застосування актів галузевого законодавства.

Ключову роль у системі правового захисту персональних даних відіграють *законодавчі акти України*. Передусім законами визначаються засади обробки та захисту інформації. Лише на підставі, в межах повноважень та у спосіб, що передбачені законами України, зобов'язані діяти органи державної влади, суб'єкти місцевого самоврядування, їхні посадові та службові особи. Закони наділені вищою юридичною силою стосовно інших нормативно-правових актів з інформаційних питань, тож завжди й у всьому зумовлюють їх зміст і спрямованість. Зрештою, тільки закони можуть визначати підстави юридичної відповідальності за правопорушення у сфері захисту персональних даних.

Нині суспільні відносини у сфері захисту інформації регламентуються більш як двома десятками законодавчих актів: законами «Про захист персональних даних» [90], «Про інформацію» [118], «Про міліцію» [119], «Про захист прав споживачів» [120], «Про всеукраїнський перепис населення» [121], «Про платіжні системи та переказ коштів в Україні» [122], «Про електронний цифровий підпис» [123], «Про телекомунікації» [124], «Про свободу пересування та вільний вибір місця проживання в Україні» [125], «Про державний реєстр виборців» [126], «Про державний земельний кадастр» [127], «Про державну службу» [128], «Про систему гарантування вкладів фізичних осіб» [129], «Про охоронну діяльність» [130], «Про громадські об'єднання» [131], «Про

адвокатуру та адвокатську діяльність» [132], «Про екстрену медичну допомогу» [133], «Про зайнятість населення» [134], «Про адміністративні послуги» [135], а також Кримінальним кодексом, Цивільним кодексом, Кодексом України про адміністративні правопорушення – в частині відповідальності за делікти у сфері інформації та відшкодування заподіяних ними збитків [136; 137; 138].

На перший погляд, така велика кількість законодавчих джерел мала б свідчити про повноту й усебічність правового регулювання. Однак при детальному розгляді стає очевидним, що більшість законів упорядковують лише окремі аспекти захисту персональних даних. Це і не дивно, оскільки без стрижневого законодавчого акта (Закон України «Про захист персональних даних» було ухвалено влітку 2010 року) регламентація кореспондуючого сектору суспільних відносин здійснювалася спорадично – в контексті розв'язання інформаційних проблем тієї чи іншої галузі.

Певною мірою ця тенденція збереглася і донині. Так, Закон України «Про державну службу» (2011) декларує право служб персоналу державних органів та органів влади Автономної Республіки Крим на обробку персональних даних фізичних осіб, Закон «Про систему гарантування вкладів фізичних осіб» (2012) визначає повноваження Фонду гарантування вкладів фізичних осіб у сфері обробки персональної інформації, а Закон «Про адміністративні послуги» (2012) покладає в основу державної політики надання адміністративних послуг принцип захищеності персональних даних.

За великим рахунком, лише закони України «Про інформацію» та «Про захист персональних даних» охоплюють глибокі пласти інформаційних відносин, регламентуючи їх на загальному, надгалузевому рівні.

Закон «Про інформацію» врегульовує відносини щодо створення, збирання, одержання, зберігання, використання, поширення, охорони та захисту інформації. Свого часу (2 жовтня 1992 року) ухвалення цього закону стало знаковою подією в організації безпечного інформаційного простору.

Фактично вперше на вищому законодавчому рівні ним були визначені (конкретизовані): поняття інформації, її види та галузі; принципи інформаційних відносин; пріоритетні напрями державної інформаційної політики; гарантії права на інформацію; основні види інформаційної діяльності; режими доступу до інформації; процедура інформаційного запиту; коло учасників інформаційних правовідносин, їхні права та обов'язки; питання охорони інформації; підстави відповідальності за делікти в інформаційній сфері; правові форми міжнародного співробітництва в галузі інформації; гарантії інформаційного суверенітету України.

Однак як засвідчила практика, первинна редакція Закону України «Про інформацію» виявилася далекою від досконалості. Вона не охоплювала багатьох важливих аспектів інформаційної діяльності (в тому числі діяльності журналістів, засобів масової інформації та їхніх працівників), не регулювала питань поширення суспільно необхідної інформації з обмеженим доступом, містила колізійні положення. Багатьма недоліків характеризувався її понятійно-категоріальний апарат, передбачені нею класифікації були суперечливими та неповними.

Вади закону мали місце і в частині регулювання відносин з приводу обробки та захисту персональних даних. Зокрема, під персональним даними пропонували розуміти лише документовані або публічно оголошені відомості. Джерелами персональних даних про особу було визнано тільки видані на її ім'я або підписані нею документи та відомості, зібрані органами влади. Крім того, закон забороняв збирання будь-яких (!) відомостей про особу без її попередньої згоди, але не стояв на заваді зберіганню, використанню та поширенню конфіденційної інформації.

Тому 13 січня 2011 року була ухвалено нову (чинна дотепер) редакцію закону, покликану забезпечити надійне правове підґрунтя для формування та реалізації державної інформаційної політики, функціонування інформаційного середовища, здійснення різних форм інформаційної

діяльності, забезпечення публічного доступу до інформації, зміцнення інформаційної безпеки, вдосконалення механізмів контролю за дотриманням законності.

Оновлений закон на якісно новому рівні врегулював кореспондуючу сферу суспільних відносин, скерувавши її розвиток у русло прогресивних світових тенденцій. Утім, і нова редакція закону виявилася далеко не бездоганною як з точки зору повноти регуляторного охоплення, так і з точки зору юридичної техніки.

Чимало запитань викликає вже сам термін «інформація», який у ст. 1 закону визначається так: «будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді». По-перше, не враховано, що різноманітні відомості/дані можуть існувати поза матеріальними носіями і не мати електронної форми. Зокрема, їх можна передавати (і досить часто передають) шляхом коливань електромагнітного поля. По-друге, наведене визначення внесло сум'яття в регулювання правовідносин з приводу інформації як нематеріального блага, яке не зводитися до матеріальних об'єктів фіксації (наприклад, під час реалізації права на захист честі та гідності фізичної особи, а також ділової репутації фізичної або юридичної особи). По-третє, базова категорія «інформація» (в оновленій редакції) вельми погано корелюється з похідними поняттями, як-то: «науково-технічна інформація», «інформація про фізичну особу», «екологічна інформація», «інформація про товар», «податкова інформація», «правова інформація», «конфіденційна інформація» тощо. Більшість таких понять визначено законодавцем просто як відомості або дані, безвідносно до форми фіксації. Єдиний виняток становить поняття науково-технічної інформації (ст. 15 закону), побудоване за моделлю базової категорії.

За загальним визнанням, нова редакція Закону України «Про інформацію» невиправдано звузила коло суб'єктів права на інформацію. Принаймні саме такий висновок можна зробити на підставі аналізу ст. 5, відповідно до якої «кожен

має право на інформацію, що передбачає можливість вільного одержання, використання, поширення, зберігання та захисту інформації, необхідної для реалізації своїх прав, свобод і законних інтересів. Реалізація права на інформацію не повинна порушувати громадські, політичні, економічні, соціальні, духовні, екологічні та інші права, свободи і законні інтереси *інших громадян*, права та інтереси юридичних осіб» *(курсив мій. – А.П.)*.

Формально ця норма може слугувати підставою для відмови у наданні інформації за запитом/на вимогу суб'єктів публічної влади, а також лазівкою, яка дає змогу уникнути відповідальності за неподання, несвоєчасне подання або за подання недостовірної інформації державним органам, установам, організаціям.

Аналогічне зауваження стосується законодавчо окресленого кола суб'єктів інформаційних відносин. До нього увійшли суб'єкти владних повноважень, однак не потрапили Україна та інші держави, хоч, відповідно до міжнародного й вітчизняного законодавства, інформаційні відносини можуть виникати між державами як самостійними суб'єктами у приватно-правовій та публічно-правовій площинах.

Права та обов'язки суб'єктів інформаційних відносин у законі теж не конкретизовано. Сьогодні, як і десятиліття тому, їх правовий статус визначається широким колом розрізнених нормативних актів, зі змісту яких дуже складно сформувати цілісне уявлення про компетенції в інформаційній сфері, засади міжвідомчої та міжінституційної взаємодії, сутність інформаційних прав та обов'язків, межі й механізми їх реалізації.

Недостатньо обґрунтованим видається закріплений у ст. 10 перелік видів інформації. Брак єдиного критерію класифікації не дає змоги провести чітку межу між статистичною та соціологічною інформацією, між правовою та податковою тощо. У підсумку така невизначеність вкрай негативно позначається на галузевому нормотворенні, правозастосуванні та й загалом на функціонуванні інформаційних відносин.

Стаття 11 Закону «Про інформацію» визначає інформацію про фізичну особу (персональні дані) як «відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована». Водночас ст. 21 зараховує таку інформацію до конфіденційної. По суті, це означає, що поширення будь-яких персональних відомостей про особу, в тому числі навіть прізвища, ім'я та по-батькові, може здійснюватися виключно за її попередньою згодою.

Надмірна жорстокість цієї вимоги очевидна. Так само очевидна практична неможливість і недоцільність її всезагального дотримання.

Як цілком слушно зауважують Є. Скулиш та А. Марущак, фізична особа може, але не зобов'язана встановлювати режим обмеженого доступу до пов'язаної з нею особистої інформації. Зважаючи на це, автоматичне присвоєння їй статусу конфіденційної видається некоректним, оскільки це питання повністю покладене на розсуд суб'єкта персональних даних [139, с. 9].

Варто наголосити, що, за законодавством більшості країн ЄС, персональні дані класифікуються за критерієм чутливості: а) дані загального характеру (П.І.Б., дата і місце народження, громадянство, стать, місце роботи, робочий телефон/факс/e-mail, місце проживання тощо); б) чутливі *(англ. – vulnerable personally identifiable information),* тобто дані, які за природою можуть порушити основні свободи і таємницю приватного життя (до таких належать відомості про стан здоров'я, етнічну належність, релігійні погляди, політичні переконання, власність, заробітну плату та інші джерела доходу, ідентифікаційні коди, біометричні записи, реквізити документів та платіжних карток, номерні знаки транспортних засобів, дактилоскопічні відбитки, зразки почерку, записи голосу, фото- та відеоматеріали, кредитна історія, інформація про судимість і ін.). Саме для чутливих персональних даних передбачено високий рівень захисту. Саме вони вважаються конфіденційними. І їх збирання, зберігання, використання та поширення без згоди суб'єкта забороняється законом й має наслідком юридичну відповідальність [140, с. 83].

Віднедавна аналогічну класифікацію (читай – диференційований підхід до конфіденціалізації персональних даних) запроваджено і в Україні: наказом уповноваженого Верховної Ради з прав людини від 8 січня 2014 року № 1/02-14 затверджено перелік даних, обробка яких становить особливий ризик для прав і свобод суб'єктів персональних даних. Зокрема, до переліку увійшли персональні дані про: расове, етнічне та національне походження; політичні, релігійні або світоглядні переконання; членство в політичних партіях та/або організаціях, професійних спілках, релігійних чи громадських організаціях світоглядної спрямованості; стан здоров'я; статеве життя; біометричні дані; генетичні дані; притягнення до адміністративної чи кримінальної відповідальності; застосування щодо особи заходів у межах досудового розслідування; вжиття щодо особи оперативно-розшукових заходів; вчинення щодо особи тих чи інших видів насильства; місцеперебування та/або шляхи пересування особи.

Однак, на жаль, ні ці види інформації, ні сам термін «дані, обробка яких становить особливий ризик для прав і свобод суб'єктів персональних даних» у Законі України «Про інформацію» відображення досі не знайшли.

Концептуальною новелою Закону «Про інформацію» стало визначення предмета суспільного інтересу, тобто інформації, яка є суспільно необхідною. Так, у ст. 1 ст. 29 закону зазначено: «інформація з обмеженим доступом може бути поширена, якщо вона є суспільно необхідною, тобто є предметом суспільного інтересу, і право громадськості знати цю інформацію переважає потенційну шкоду від її поширення».

Навіть поверхневий аналіз цієї норми свідчить, що вона сформульована в спосіб, який не дає змоги розраховувати на її ефективне застосування. Фактично правозастосовцю (в даному разі – суду) пропонується зіставляти (читай – порівнювати) дві абсолютно різні абстрактні категорії, одна з яких виражає міру суб'єктивної можливості, інша – має суто гіпотетичний характер. До того ж не зрозуміло, в якій саме площині (моральній, ідеологічній, матеріальній абощо) їх

потрібно зіставляти. Адже перевага публічного інтересу в одному аспекті може нівелюватися колосальними втратами в іншому. Цілком очевидно, що провести таке зіставлення, а тим більше сформувати на його основі єдино правильний висновок – справа надзвичайно складна, а в багатьох випадках майже не вирішувана.

Не менш дискусійне положення, згідно з яким суб'єкти інформаційних відносин звільняються від відповідальності за розголошення інформації з обмеженим доступом, якщо суд встановить, що ця інформація характеризується суспільною необхідністю (ч. 3 ст. 31 Закону «Про інформацію»). Фактично запровадивши це положення, законодавець встановив додаткові підстави для звільнення від юридичної відповідальності та розширив рамки однойменного інституту.

Практична доцільність та наукова обґрунтованість цього кроку викликають серйозні сумніви. Адже відповідно до вітчизняної парадигми регулювання деліктних відносин, підстави для звільнення від юридичної відповідальності визначаються галузевими кодифікованими актами: Кодексом України про адміністративні правопорушення, Кримінальним кодексом, Господарським кодексом та ін. Переліки визначених ними підстав є вичерпними і не підлягають розширеному тлумаченню.

На сьогодні жоден з цих актів не визнає суспільної значущості інформації з обмеженим доступом підставою для звільнення від відповідальності за її розголошення. Як наслідок, кореспондуючі положення Закону «Про інформацію» не можна застосовувати на практиці, під час вирішення конкретних юридичних справ (адміністративних, кримінальних, господарських тощо).

Ситуації можуть зарадити тільки комплексні зміни до галузевих кодексів, зокрема закріплення в їхньому змісті додаткових підстав для звільнення від відповідальності за інформаційні правопорушення. Що стосується ч. 3 ст. 30 Закону «Про інформацію», то його положення радше декларативні, ніж такі, що мають практичний сенс.

Висвітлені недоліки Закону «Про інформацію» диктують необхідність його системного оновлення з урахуванням об'єктивних тенденцій інформатизації суспільства, положень міжнародного законодавства, вимог юридичної техніки.

Ще одним стрижневим актом інформаційного законодавства є Закон України «Про захист персональних даних», яким урегульовано суспільні відносини, пов'язані із захистом та обробкою персональних даних, захистом основоположних прав і свобод людини та громадянина: права на невтручання в особисте життя, права вимагати вилучення будь-якої інформації про себе та членів своєї сім'ї, права на ознайомлення в органах державної влади, органах місцевого самоврядування, установах і організаціях з відомостями про себе, які не становлять державної або іншої захищеної законом таємниці [90].

За висновками міжнародних експертів, ухвалення цього закону в 2010 році істотно сприяло соціальному, економічному та науково-технічному прогресу, забезпеченню балансу прав людини, суспільства й держави у сфері інформації, поліпшенню нормативно-правового забезпечення захисту персональних даних відповідно до норм міжнародного права та законодавства ЄС, зокрема Страсбурзької конвенції про захист осіб стосовно автоматизованої обробки даних особистого характеру від 28 січня 1981 року [84] та директиви 95/46/ЄС Європейського парламенту і Ради від 24 жовтня 1995 р. про захист фізичних осіб під час обробки персональних даних і про вільне переміщення таких даних [141].

Закон має загальносистемний характер і визначає фундаментальні засади обробки та захисту персональних даних в Україні. Його чинність поширюється на діяльність щодо обробки персональних даних із застосуванням автоматизованих засобів, а також на обробку персональних даних, які містяться в картотеках чи призначені для внесення до картотек із застосуванням неавтоматизованих засобів.

Охопивши найважливіші аспекти захисту персональних даних, він акумулював загальні та особливі вимоги щодо їх збирання, обробки, накопичення, зберігання, використання, поширення, видалення та знищення.

Чимало уваги в законі приділено питанням доступу до персональних даних. Зокрема, ст. 16 регламентує відповідну процедуру, визначає форму запиту на доступ до персональних даних, закріплює строки його подання та розгляду. Ст. 17 визначає підстави для відстрочення або відмови у доступі до персональних даних, ст. 18 гарантує право на оскарження рішень про відстрочення/відмову в доступі, а ст. 19 поряд із правом безкоштовного доступу до інформації про себе врегульовує питання плати за доступ до персональних даних інших осіб.

Серед позитивних рис закону варто згадати внутрішню узгодженість, логічну структуру, врахування вимог міжнародного інформаційного законодавства. Навіть саме його ухвалення стало вагомим здобутком в контексті виконання Україною міжнародних зобов'язань.

Проте аналіз ключових положень Закону України «Про захист персональних даних» та практики його застосування не дає особливих підстав для оптимізму. За одностайним визнанням вітчизняних і зарубіжних експертів, чинна редакція закону характеризується великою кількістю недоліків, котрі помітно знижують ефективність регулювання відповідної сфери правовідносин.

Як зауважує І. Усенко, навіть сама назва закону не зовсім добре узгоджена з його сьогоднішнім змістом, який здебільшого стосується не всіх питань захисту персональних даних, а лише тих, які пов'язані з їх обробкою в електронних базах і картотеках [142]. І хоч наприкінці 2012 року до закону було внесено зміни, спрямовані на розширення меж його чинності (зокрема, остання редакція ст. 5 визнала об'єктом правового захисту будь-які персональні дані безвідносно до форми систематизації), це питання досі відкрите. Адже, попри оновлення деяких положень, загальна структура закону залишилась незмінною: нині, як і раніше, він акцентує на регламентації відносин з приводу функціонування відповідних інформаційних баз.

Так, зі змісту ч. 2 ст. 1 та абз. 1 ст. 2 Закону «Про захист персональних даних» однозначно випливає, що будь-який неструктурований масив персональних даних (наприклад, матеріали особових справ) не являє собою базу даних, отже не підпадає під чинність закону. Тобто закон, який відповідно до назви й задекларованої мети мав би забезпечувати захист всіх видів персональних даних, фактично захищає лише систематизовану інформацію. Питання збирання, обробки та використання персональних даних, не структурованих за визначеним критерієм, здебільшого залишилися поза межами правового регулювання та захисту.

З іншого боку, сферу функціонування баз систематизованих персональних даних закон охоплює надто щільно. Передбачені ним вимоги поширюються на всі види обробки персональних даних, крім двох винятків: 1) якщо обробку персональних даних здійснює фізична особа виключно для особистих чи побутових потреб; 2) якщо обробка персональних даних здійснюється виключно для журналістських та творчих цілей, за умови забезпечення балансу між правом на повагу до особистого життя та правом на свободу вираження поглядів (ст. 25).

Фактично це означає, що під чинність закону та його обов'язкових вимог підпадають випадки: обробки архівних документів, що містять персональні дані; обробки персональних даних у рамках єдиного державного реєстру юридичних осіб та фізичних осіб-підприємців; обробки персональних даних, віднесених до відомостей, що становлять державну таємницю.

Доцільність застосування загальних положень закону до зазначених випадків викликає серйозні сумніви. Наслідком цього можуть стати ліквідація важливих архівних даних, послаблення публічного контролю у сфері підприємницької діяльності, порушення законодавства про державну таємницю та завдання шкоди національним інтересам.

Слабким місцем закону є термінологічний апарат (ст. 2), який характеризується багатьма невизначеностями та недостатнім опрацюванням.

Зокрема, важко збагнути, чому під базою даних слід розуміти саме іменовану сукупність упорядкованих персональних даних. Невже структуровані інформаційні масиви без власної назви не вважаються картотеками та не підпадають під чинність закону? Гадаємо, це питання риторичне.

До «володільців персональних даних» закон зараховує фізичних або юридичних осіб, які визначають мету обробки персональних даних, встановлюють склад цих даних та процедури їх обробки, якщо інше не визначено законом.

Закономірно постає запитання: чи вважати володільцем персональних даних особу, котра здійснює їх безпосередню обробку, без формалізації цілей, складу та процедури такої обробки? Якщо виходити з буквального тлумачення закону, виявляється, що ні. Але в такому разі ситуація буде вельми заплутаною, оскільки з кола чинності закону випадає достатньо численна категорія суб'єктів обробки персональних даних, з чим категорично не можна погодитись.

Крім того, наведене визначення містить очевидну внутрішню суперечність. Володільцями персональних даних у ньому визначає не особи, які мають в своєму розпорядженні/володінні персональні дані, а ті, хто визначає цілі, склад і процедуру такої обробки. Отож з формальної точки зору, володільцем персональних даних може виступати особа, котра ними фактично не володіє (наприклад, суб'єкт, який ще не розпочинав збирання інформації, але вже визначив його процедуру). Такий підхід суперечить загальноприйнятому уявленню про володіння як фактичне володіння чимось [143].

Визначаючи згоду суб'єкта персональних даних як «добровільне волевиявлення фізичної особи (за умови її поінформованості) щодо надання дозволу на обробку її персональних даних відповідно до сформульованої мети їх обробки, висловлене у письмовій формі або у формі, що дає змогу зробити висновок про її надання» *(підкреслення моє. – А.П.)*, законодавець не конкретизував змісту такого інформування. Не відомо, яку саме інформацію, в якій формі та в який спосіб слід надати суб'єкту персональних даних для отримання дозволу на їх обробку.

З огляду на те що інформування суб'єкта персональних даних покликане забезпечити їх справедливу обробку згідно з європейськими стандартами (а саме ст. 10 директиви Європейського парламенту і Ради ЄС від 24.10.1995 № 95/46/ЄС «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» та пропозиціями Європейської комісії стосовно захисту прав людини у зв'язку з обробкою та поширенням персональних даних від 25 січня 2012 р. С7-0025/2012 [85; 115]) видається доцільним закріпити в Законі України «Про захист персональних даних» такі вимоги:

а) щодо обов'язкового направлення фізичній особі запиту про надання дозволу на обробку її персональних даних у письмовій, електронній або іншій формі;

б) щодо обов'язкового зазначення у відповідному запиті відомостей про володільця та розпорядника (розпорядників) персональних даних, мету збирання інформації, склад та зміст питомих персональних даних; строк їх обробки; осіб, яким їх передаватимуть; про права суб'єкта персональних даних у сфері їх захисту;

в) про те, що ненадання відповіді на запит слід розглядати як відсутність дозволу (читай – заборону) на обробку персональних даних.

Небездоганними є й інші визначення, наведені у ст. 2 закону.

Наприклад, поняття «обробка персональних даних» містить вичерпний, проте недостатньо повний перелік технічних операцій, здійснюваних у рамках обробки. Зокрема, ним не охоплено такі операції з даними, як: пошук, аналіз, упорядкування, комбінування, блокування, стирання тощо. Видається, що перелік технічних дій у визначенні має бути відкритим. Він має містити лише типові приклади операцій з обробки, оскільки неможливо навести всі види технічних операцій, які можна здійснювати з даними, особливо у світлі невпинного розвитку інформаційних технологій.

Визначення поняття «суб'єкт персональних даних» (фізична особа, персональні дані якої обробляють) погано

корелюється з іншими положеннями закону, зокрема з тими, які регулюють питання «отримання згоди суб'єкта персональних даних» на їх обробку. Фактично ці положення визнають суб'єктами персональних даних осіб, які ще тільки-но мають дати відповідну згоду (отже, інформацію про них ще навіть не почали обробляти). Та й чи коректно іменувати суб'єктом персональних даних лише ту особу, інформація про яку перебуває в стані обробки? Невже всіх інших людей, котрі *a priori* є носіями персональних даних, не можна вважати їх суб'єктами? Гадаємо, це питання риторичні.

Перелік дискусійних моментів Закону «Про захист персональних даних» не вичерпується вадами термінології. Достатньо підстав для критичних зауважень дають й інші його положення.

Впадає у вічі невідповідність абз. 3 ст. 2 та ч. 2 ст. 4 закону. Якщо перша норма визнає володільцем персональних даних усіх фізичних осіб, яким законом чи договором дано право їх обробки (до речі, аналогічний підхід застосовано в директиві Європейського парламенту і Ради ЄС від 24.10.1995 № 95/46/ЄС), то згідно з другою, володільцем персональних даних можуть бути лише фізичні особи-підприємці.

Вище вже згадувалося про недоцільність віднесення всіх типів персональних даних до інформації з обмеженим доступом. На жаль, кореспондуючі настанови Ради ЄС під час творення та внесення подальших змін до закону враховано не було. Як наслідок, будь-які типи персональних даних, навіть найбільш загальні та широковідомі, можна вважати конфіденційними. Слід підкреслити, що це системний недолік вітчизняного інформаційного законодавства, який знайшов відображення і в новій редакції Закону «Про інформацію». Тож його виправлення можливе тільки в рамках комплексного підходу.

Недостатньо чіткою та обґрунтованою видається вимога ч. 1 ст. 6 закону: «У разі зміни визначеної мети обробки персональних даних суб'єктом персональних даних має бути надана згода на обробку його даних відповідно до зміненої

мети, якщо нова мета обробки несумісна з попередньою». Критерій сумісності/несумісності є суто відносним, що створює передумови для його вільного тлумачення як володільцями персональних даних, так і суб'єктами юрисдикційних повноважень. Ця обставина зумовлює ризик маніпуляцій, в ході яких первинна (узгоджена із суб'єктом персональних даних) мета обробки інформації без його згоди може бути змінена на іншу, зовні подібну, але відмінну по суті.

З нашої точки зору, будь-які зміни в цільовому призначенні обробки персональних даних слід узгоджувати з їх суб'єктом. Лише такий підхід здатен гарантувати право особи на захист персональних даних та приватність особистого життя.

Взаємовиключний характер мають окремі положення ст. 7 закону, яка визначає особливі вимоги до обробки персональних даних. Зокрема, ч. 1 цієї статті містить заборону обробки персональних даних про засудження до кримінального покарання. Натомість ч. 2, що встановлює виняток із загального правила, наголошує, що положення частини першої цієї статті не застосовується, якщо обробка персональних даних стосується вироків суду.

У зв'язку з цим слід наголосити, що ст. 8 директиви Європейського парламенту і Ради ЄС від 24.10.1995 № 95/46/ЄС (саме вона лягла в основу відповідних положень закону) не містить рекомендацій щодо заборони на обробку даних, пов'язаних із правопорушеннями, юридичною відповідальністю та судовою практикою.

Вона передбачає спеціальний режим обробки такої інформації: «Обробка даних, що стосуються правопорушень, обвинувачення у кримінальних справах чи засобів безпеки, може проводитися тільки під контролем офіційного органу або якщо національне законодавство передбачає відповідні спеціальні гарантії, відповідно до національних положень, що передбачають такі гарантії. Однак повний реєстр обвинувачень у кримінальних справах може вестися лише під контролем офіційного органу. Держави-члени можуть

передбачити, що дані про адміністративні санкції чи про судові рішення в цивільних справах теж повинні обробляти під контролем офіційного органу» [85].

На наш погляд, саме цю нормативну модель потрібно взяти на озброєння вітчизняному законодавцю. Адже обробка персональних даних деліктологічного характеру є важливим аспектом функціонування правоохоронної системи, запорукою ефективності планування профілактичних, оперативно-розшукових та інших заходів, спрямованих на боротьбу з деліктністю, охорону громадського порядку, гарантування особистої безпеки громадян, захист їхніх прав, свобод і законних інтересів. Тобто обробка таких даних має являти собою правило, а не виняток (звичайно ж, за умови суворого дотримання гарантій конфіденційності та пов'язаних з ними обмежень).

Що ж до інших винятків з правила про заборону обробки деяких видів персональних даних, то частина з них потребує уточнення й конкретизації. Зокрема, доцільно розкрити поняття медичний працівник, яке використовується в п. 6 ч. 2 ст. 7 закону. А у п. 7 ч. 2 цієї статті разом з контррозвідувальною і оперативно-розшуковою діяльністю варто зазначити ще й розвідувальну. Аналогічні зауваження стосуються також ч. 4 ст. 15 та п. 1 ч. 2 ст. 21 закону [90].

Перелік закріплених у законі (ст. 8) прав суб'єкта персональних даних відповідає букві і духу рекомендацій Ради ЄС, але містить принципові відмінності. Головна з них полягає в тому, що закон «Про захист персональних даних» гарантував право особи знати про місцезнаходження бази персональних даних, яка містить його персональні дані, місцезнаходження та/або місце проживання (перебування) володільця чи розпорядника персональних даних або дати відповідне доручення щодо отримання цієї інформації уповноваженим ним особам, крім випадків, встановлених законом.

У зв'язку з цим варто дослухатись до експертів Ради Європи Марі Жорж та Грема Саттона, які застерігають: «право знати місце, де зберігаються дані, може поставити під

загрозу безпеку бази даних» [144, с. 19]. І це застереження немарне. Адже ніщо не зобов'язує суб'єкта персональних даних зберігати конфіденційність отриманої інформації. Як наслідок, вона може потрапити, образно кажучи, не в ті руки та бути використана для несанкціонованого доступу до бази персональних даних.

Крім того, відповідне положення закону створює конфлікт суб'єктивних прав: права суб'єкта персональних даних на отримання пов'язаної з ним (його даними) інформації та права фізичної особи – володільця персональних даних на конфіденційність інформації про себе.

Викладене ставить під сумнів необхідність законодавчого закріплення (та й загалом існування) права суб'єкта персональних даних отримувати відомості про місце знаходження відповідної бази даних, а також про місце проживання володільця чи розпорядника персональних даних.

Неможливо обійти увагою і те, що в тексті закону деякі права суб'єктів персональних даних сформульовані у спосіб, який утруднює їх реалізацію та захист на практиці.

Наприклад, гарантуючи право доступу до інформації про себе (зокрема право особи знати про джерела збирання персональних даних, місцезнаходження своїх персональних даних; місце проживання (перебування) володільця чи розпорядника персональних даних; право отримувати інформацію про умови надання доступу до персональних даних, зокрема інформацію про третіх осіб, яким передають її персональні дані; право отримувати не пізніш як за 30 календарних днів з дня надходження запиту відповідь про те, чи зберігаються його персональні дані у відповідній базі, а також отримувати її зміст). Закон не визначає, хто саме повинен надавати суб'єкту персональних даних відповідну інформацію: володілець, розпорядник, уповноважений орган з питань захисту персональних даних абощо?

Іншим прикладом є право суб'єкта персональних даних «знати механізм автоматичної обробки персональних даних», закріплене у ч. 12 ст. 8 закону. Стосовно цієї норми постають

одразу два запитання. Чи насправді суб'єкту персональних даних потрібна інформація саме про механізм (читай сукупність засобів) автоматичної обробки інформації? Чому суб'єкт персональних даних наділяється правом знати механізм автоматичної обробки всіх персональних даних, а не лише тих, які стосуються його особисто?

У пошуку відповідей звернімося до директиви Європарламенту та Ради ЄС від 24.10.1995 № 95/46/ЄС: «Держави-члени гарантують кожному суб'єкту даних право отримати від контролера: інформацію про логіку, використовувану під час автоматизованої обробки даних, що його стосуються» *(підкреслення моє – А.П.)*. Зі змісту цього положення стає очевидним, що обидва дискусійні моменти ч. 12 ст. 8 Закону України «Про захист персональних даних» зумовлені не стільки практичною доцільністю, скільки невдалим калькуванням рекомендацій ЄС.

Вельми неоднозначний характер має ч. 1 ст. 10 «Використання персональних даних», у якій зазначено: «Використання персональних даних передбачає будь-які дії володільця щодо обробки цих даних, дії щодо їх захисту, а також дії щодо надання часткового або повного права обробки персональних даних іншим суб'єктам відносин, пов'язаних із персональними даними…». Як неважко помітити, ця норма пов'язує процес використання персональних даних виключно з діями володільця, що суперечить іншим законодавчим положенням (зокрема, у ст.ст. 2, 4 та 8 закону передбачено використання персональних даних не лише володільцем, а й розпорядником).

Крім того, згадана норма вступає в суперечність із логікою понятійно-категоріального апарату закону. Зокрема, в поняття «використання персональних даних» вона вкладає невиправдано широкий зміст (ним охоплено і захист персональних даних, і їх обробку, і надання права такої обробки іншим суб'єктам). Хоча, наприклад, у ст. 2 використання персональних даних розглянуто лише як окремий різновид обробки.

Суттєвого уточнення потребує й законодавча вимога щодо обов'язкового повідомлення в момент збирання персональних даних (або протягом 30 робочих днів з дня збирання персональних даних – в інших випадках) суб'єкта персональних даних про володільця персональних даних, склад та зміст зібраних персональних даних, його законні права, мету збирання та осіб, яким їх передають (ст. 12).

Слушність існування цієї вимоги безсумнівна. Однак цього не можна сказати про абсолютний характер її дії. Як відомо, збирання персональних даних здійснюється не лише для задоволення приватних, корпоративних, наукових чи творчих потреб, а й з метою національної безпеки, оборони, запобігання, виявлення та розслідування злочинів тощо. Відповідно постає необхідність закритого збирання персональних даних, що зумовлено специфікою розвідувальної, контррозвідувальної та оперативно-розшукової діяльності. У таких випадках повідомлення суб'єкта про збирання пов'язаної з ним інформації може призвести до провалу важливих оперативних заходів, поставити під удар інтереси держави, створити загрозу для життю і здоров'ю громадян.

З огляду на викладене вважаємо за доцільне закріпити в ст. 12 Закону України «Про захист персональних даних» застереження про те, що передбачені цією статтею вимоги можуть бути обмежені на підставі закону, якщо таке обмеження необхідне в інтересах національної безпеки, оборони, боротьби зі злочинністю, захисту важливих економічних та фінансових інтересів держави, гарантування особистої безпеки громадян.

Одразу кілька зауважень викликає чинна редакція ст. 14 «Поширення персональних даних». У ч. 1 цієї статті розкрито суть поширення персональних даних: «дії щодо передачі відомостей про фізичну особу за згодою суб'єкта персональних даних». Натомість ч. 2 передбачає можливість поширення персональних даних без згоди суб'єкта чи уповноваженої ним особи у випадках, визначених законом, і лише (якщо це необхідно) в інтересах національної безпеки, економічного добробуту та прав людини.

Стосовно наведених положень слід вказати таке:

вони охоплюють лише окремий аспект поширення персональних даних в розумінні ст. 2 закону (абз. 8), згідно з якою цей процес не обмежується передачею даних, а й передбачає їх розповсюдження та реалізацію;

жоден акт інформаційного законодавства не дозволяє обробки персональних даних суб'єкта за згодою уповноваженої ним особи. Єдиний випадок опосередкованого надання згоди на обробку персональних даних передбачений у ч. 3 ст. 8, де зазначено: «розпорядження персональними даними фізичної особи, обмеженої в цивільній дієздатності або визнаної недієздатною, здійснює її законний представник». Однак у цьому разі представницькі повноваження (піклування та опікунство) покладено на особу судом, а не суб'єктом персональних даних;

ч. 2 ст. 14 не просто встановила виняток з правила, встановленого ч. 1, а й певною мірою спростувала її зміст. Адже остання сформульована у вигляді категоричного судження-дефініції, яке не допускає винятків, зокрема, щодо обов'язкової згоди на поширення персональних даних. З точки зору формальної логіки, можливість поширення персональних даних без згоди суб'єкта (ч. 2) означає, що це твердження (ч. 1) не є істинним.

Для усунення окреслених недоліків доцільно: по-перше, конкретизувати в ч. 1 ст. 14 основні способи поширення персональних даних; по-друге, вилучити з ч. 1 ст. 14 вказівку щодо обов'язкової згоди суб'єкта на поширення його персональних даних (дія цієї вказівки все одно поглинається загальною забороною обробки персональних даних без дозволу); по-третє, замінити в ч. 2 ст. 14 слова «уповноваженої ним особи» словами «його законним представником».

Поряд із вимогами щодо поширення персональних даних підлягають уточненню законодавчі підстави для їхнього видалення або знищення. На сьогодні ст. 15 зазначеного згодою суб'єкта на їх обробку або законом; 2) припинення правовідносин між суб'єктом персональних даних та

володільцем чи розпорядником; 3) набрання законної сили рішенням суду щодо видалення або знищення персональних даних; 4) видання відповідного припису уповноваженого Верховної Ради України з прав людини або визначених ним посадових осіб секретаріату уповноваженого.

Проте вона не враховує права суб'єкта відкликати згоду на обробку персональних даних та/або пред'являти вмотивовану вимогу володільцю персональних даних із запереченням проти обробки інформації, котра його стосується. В обох випадках умотивована вимога суб'єкта персональних даних заперечує можливість їх подальшої обробки, отже і зберігання володільцем і розпорядником. З огляду на це єдино можливим правовим наслідком такої вимоги є знищення інформації, що, за логікою, мало б знайти відображення в ст. 15.

Ще один приклад недосконалого регулювання інформаційних відносин являє собою ст. 19, яка регламентує питання оплати доступу до персональних даних. Згідно з ч. 4 цієї статті, органи державної влади та органи місцевого самоврядування *(на відміну від усіх інших третіх осіб)* мають право на безперешкодний і безоплатний доступ до персональних даних відповідно до їхніх повноважень.

У цьому аспекті варто погодитися з думкою про те, що наведене положення підлягає доопрацюванню на предмет відповідності загальній ідеї про рівність усіх суб'єктів інформаційних відносин [142]. І справді, питання про те, чи не означає воно дискримінацію третіх осіб та чи не порушує економічні права володільця/розпорядника бази персональних даних, образно кажучи, лежить на поверхні. Воно потребує обов'язкового розгляду та вирішення.

Проте куди більшу суперечливість ідеології інформаційних відносин та захисту персональних даних містить концепція безперешкодного доступу органів влади до персональних даних фізичних осіб. По суті, вона вступає в суперечність із конституційною забороною використовувати конфіденційну інформацію про особу без її згоди, крім

випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини (ст. 32 Конституції України); принципом захищеності особи від втручання в її особисте та сімейне життя (ст. 2 Закону «Про інформацію»); правом суб'єкта персональних даних визначати порядок доступу до пов'язаної з ним інформації (ст. 16 Закону «Про захист персональних даних»).

Існування такої суперечності неприпустиме. Реалізацію права безперешкодного доступу органів влади до персональних даних не можна здійснювати всупереч праву людини на захист приватної інформації. Виняток може бути зроблено тільки на підставі закону, за наявності спеціальних гарантій, з метою захисту життєво важливих інтересів громадянина, суспільства, держави.

З огляду на викладене вважаємо за доцільне викласти ч. 4 ст. 19 закону в такій редакції: «На підставі закону, на виконання своїх законних повноважень, а також за наявності згоди суб'єкта персональних даних (крім випадків, коли за законом така згода не є обов'язковою), органи державної влади та органи місцевого самоврядування (їхні посадові особи) мають право на безперешкодний і безоплатний доступ до персональних даних».

Суттєвого оновлення потребують також ст. 20 «Зміни і доповнення до персональних даних» та ст. 21 «Повідомлення про дії з персональними даними».

Цілком очевидно, що назва ст. 20 недостатньо чітко корелюється з її змістом, де йдеться тільки про випадки зміни персональних даних і жодним словом не згадано про їхнє доповнення. Крім того, покладаючи на володільців і розпорядників баз персональних даних зобов'язання вносити зміни до персональних даних на підставі вмотивованої письмової вимоги суб'єкта персональних даних (див. ч. 1 ст. 20), вона не встановлює строків внесення кореспондуючих змін. Тим самим створюється підґрунтя для тривалого ігнорування вимог суб'єкта володільцями та розпорядниками персональних даних.

Ситуація ускладнена тим, що під час визначення обов'язків володільця та розпорядника персональних даних законодавець використовує протиставний сполучник чи (отже, маємо: володільці чи розпорядники). Результатом стала невизначеність у ключовому питанні про те, хто ж саме повинен нести відповідальність за своєчасне внесення змін/доповнень до персональних даних.

Аналогічні зауваження стосуються ст. 21 закону, яка покладає обов'язок повідомляти суб'єкта персональних даних про передачу пов'язаної з ним інформації виключно на володільця персональних даних. Однак виходячи з практичних міркувань, цей обов'язок доцільно покласти не тільки на нього, а й на розпорядника, який у багатьох випадках безпосередньо здійснює передачу персональних даних.

Виходячи з викладеного вище, обидві статті (20 і 21) потребують комплексу змін, спрямованих на усунення внутрішніх суперечностей і невизначеностей і прогалин.

До вразливих місць Закону України «Про захист персональних даних» слід зарахувати і недостатньо продуману структуру. Нині багато законодавчих положень містяться у статтях, які не відповідають їх змісту, характеру та предметній спрямованості.

Наприклад, за усталеною традицією нормотворення, норма про пріоритет міжнародних договорів України перед актами внутрішнього законодавства повинна міститись у ст. 3 «Законодавство про захист персональних даних» (а не в ч. 2 ст. 29 закону, як це має місце нині). До цієї статті варто ввести таку норму: «Положення щодо захисту персональних даних, викладені в цьому законі, можуть доповнюватися чи уточнюватися іншими законами, за умови, що вони встановлюють вимоги щодо захисту персональних даних, які не суперечать вимогам цього закону» (нині це ч. 1 ст. 27).

А положення, яке обмежує чинність закону та його окремих статей (ст. 25) за логікою мало б міститися або у ст. 1 «Сфера дії Закону» (як окрема частина), або одразу після неї (як самостійна стаття).

Отже, як свідчить аналіз, чинна редакція Закону України «Про захист персональних даних» характеризується багатьма недоліками, які дестабілізують сферу інформаційних відносин, знижують ефективність правозастосовної діяльності, призводять до виникнення конфліктних ситуацій між суб'єктами інформаційного права. Зважаючи на це, вітчизняний законодавець неодноразово вдавався до перегляду ключових положень закону з метою їх удосконалення та пристосування до вимог практики.

Попри відносно нетривалий строк існування, Закон України «Про захист персональних даних» неодноразово зазнавав істотних змін, внаслідок чого його нинішня редакція вельми далека від первинної (на сьогодні тільки шість статей закону – 3, 13, 17, 19, 26 та 28 – залишились у первинному вигляді). Однак всі ці зміни так і не спричинилися до кардинальних позитивних зрушень. Не маючи системного характеру та не будучи ув'язаними в єдину концепцію, вони давали змогу розраховувати на локальні поліпшення, але не могли забезпечити якісно новий рівень правового захисту персональних даних. Більш того, іноді законодавчі новели вносили додаткову невизначеність і сум'яття в регламентацію відповідної сфери суспільних відносин.

Наочним прикладом може слугувати останній пакет нововведень, передбачений Законом України від 3 липня 2013 року «Про внесення змін до деяких законодавчих актів України щодо удосконалення системи захисту персональних даних» (набув чинності 1 січня 2014 року) [145]. Цей документ запровадив новий механізм адміністрування сферою захисту персональних даних, чільне місце в якому посідає не державний орган, а незалежний суб'єкт парламентського контролю – уповноважений Верховної Ради України з прав людини.

Не вдаючись в деталі функціонування цього механізму, маємо вказати на дискусійний характер пов'язаних з ним законодавчих положень.

Так, однією з новел закону став кардинальний перегляд кола органів, уповноважених провадити контроль за додержанням законодавства про захист персональних даних. Якщо попередня редакція закону (ст. 22) зараховувала до нього Державну службу України з питань захисту персональних даних та інші органи державної влади, то нова – уповноваженого Верховної Ради України з прав людини та суди.

З цього приводу слід наголосити, що, за чинним законодавством, суд – орган правосуддя, а не адміністративного контролю. Контрольні повноваження суду поширюються виключно на захист прав, свобод та інтересів осіб у кримінальному провадженні [146]. Суд не може і не повинен забезпечувати контроль за додержанням законодавства в певних галузях або сферах суспільного життя. Це функція інших спеціалізованих органів/інститутів, орієнтованих на здійснення контролю та нагляду. Відповідно зарахування суду до числа органів контролю за додержанням законодавства про захист персональних даних не має достатніх правових підстав.

Крім того, слід ураховувати, що, відповідно до чинного законодавства, уповноважений Верховної Ради України з прав людини має статус посадової особи, а не органу, як це випливає зі змісту ст. 22 Закону України «Про захист персональних даних».

Нова редакція ст. 24 містить щонайменше дві контрадикторні тези: згідно з ч. 2, в органах державної влади, місцевого самоврядування, а також у володільців чи розпорядників персональних даних (як відомо, до них належать і фізичні особи-підприємці), що здійснюють обробку персональних даних, створюється (визначається) структурний підрозділ або відповідальна особа, що організовує роботу, пов’язану із захистом персональних даних при їх обробці; натомість ч. 4 визначає, що фізичні особи-підприємці, у тому числі лікарі, які мають відповідну ліцензію, адвокати, нотаріуси особисто забезпечують захист персональних даних, якими вони володіють, згідно з вимогами закону.

У зв'язку з цим постають запитання: чи повинні фізичні особи підприємці створювати/визначати особу, відповідальну за захист персональних даних (адже ч. 2 ст. 24 не допускає винятків із правила); чи поширюється на них обов'язок повідомляти інформацію про відповідальну особу уповноваженому Верховної Ради з прав людини; чи коректно сформульована ч. 4 ст. 24 закону, адже насправді ні адвокати, ні нотаріуси не мають статусу фізичних осіб-підприємців? Як видається, обґрунтовані відповіді на них може дати тільки сам законодавець шляхом внесення коректив до ст. 24.

На підставі викладеного вище можна констатувати, що оновлення законодавства про захист персональних даних характеризується спорадичністю, неузгодженістю та слабкою опрацюванням нормативного матеріалу. Наслідок – загальна недосконалість закону.

Закон України «Про захист персональних даних» помітно розширив сферу правового регулювання інформаційних відносин, увів до законодавства доволі багато нових понять і підходів, суттєво розширив коло юридичних обов'язків учасників інформаційних відносин, – пише І. Усенко, – водночас така «юридизація» була здійснена без належної системності, з істотними суперечностями і прогалинами» [142]. За перші два роки чинності закону його візитівкою стали нечіткі й розмиті визначення багатьох ключових понять, покладення невиправдано важких обов'язків на володільців баз персональних даних, відсутність адекватного регулювання передачі персональних даних за кордон», – констатують В. Шестаков і Л. Чернявський [147]. «Закон створює суттєві труднощі кожному бізнесу, що веде картотеку клієнтів (а це фактично всі підприємства України). Його основними проблемами є невиправдана всеохопність, відсутність розмежування персональних даних на ідентифікуючі та вразливі, надто широкі повноваження контролюючого органу», – додає В. Пекар [148]. «Попри численні переваги закону, він містить багато суттєвих недоліків та недосконалостей, які потребують якнайшвидшого усунення», – резюмує О. Одинець [149, с. 6].

Важливе місце у правовому забезпеченні захисту персональних даних посідають акти Президента України. З огляду на особливий статус Президента як провідного суб'єкта формування інформаційної політики, більшість його актів з питань захисту персональних даних мають концептуальний, плановий і програмний характер.

Такими є: укази Президента від 6 грудня 2001 року № 1193/2001 «Про рішення Ради національної безпеки і оборони України від 31 жовтня 2001 року «Про заходи щодо вдосконалення державної інформаційної політики та забезпечення інформаційної безпеки України» [150], від 8 липня 2009 року № 514/2009 «Про доктрину інформаційної безпеки України» [151], від 13 квітня 2011 року № 468/2011 «Про затвердження Річної національної програми співробітництва Україна – НАТО на 2011 рік» [152], від 22 квітня 2011 року № 1121/2007 «Про Національний план з виконання Плану дій щодо лібералізації Європейським Союзом візового режиму для України» [153], від 12 березня 2013 року № 128/2013 «Про Національний план дій на 2013 рік щодо впровадження Програми економічних реформ на 2010–2014 роки «Заможне суспільство, конкурентоспроможна економіка, ефективна держава» [154].

Аналіз зазначених планів, програм і концепцій дає змогу констатувати дуже обнадійливий стан їх практичної реалізації в частині заходів, спрямованих на захист персональних даних. На тлі багатьох інших галузей, де показник реалізації програмних/планових документів становить 40–45% [155, с. 163], стратегічне планування у сфері захисту персональних даних вирізняється високим рівнем ефективності.

Наочним прикладом може слугувати Національний план дій на 2013 рік щодо впровадження Програми економічних реформ на 2010–2014 роки (указ Президента України від 12 березня 2013 року № 128/2013). За підсумками 2013 року було виконано майже всі заходи цього плану, у тому числі:

п. 170.2. Розроблення та внесення на розгляд Верховної Ради України законопроекту щодо внесення змін до Закону України «Про захист персональних даних» в частині приведення у відповідність із регулюванням ринку поштового зв'язку держав – членів Європейського Союзу;

п. 205.1. Створення та впровадження в усіх територіальних органах Держземагентства України комплексної системи захисту інформації з обмеженим доступом, у тому числі персональних даних, під час ведення Державного земельного кадастру;

п. 226.1. Розроблення та внесення на розгляд Верховної Ради проекту закону щодо передачі уповноваженому Верховної Ради України з прав людини функцій контролю за дотриманням вимог законодавства у сфері захисту персональних даних;

п. 249.4. Розроблення та внесення на розгляд Верховної Ради проекту закону «Про державну інформаційну систему електронної взаємодії державних електронних інформаційних ресурсів», передбачивши, зокрема аспекти захисту персональних даних при обробці інформації [154].

Максимальний відсоток реалізації планових/програмних заходів, з одного боку, є результатом продуманого галузевого планування, з іншого – свідчить про актуальність та значущість ініціатив Президента у сфері захисту персональних даних. Ця обставина має дуже велику вагу, адже, насамперед, від політичної волі глави держави залежить динаміка правових та організаційних процесів, покликаних забезпечити гармонійну інтеграцію України у світовий інформаційний простір.

Питома вага актів Кабінету Міністрів України в загальному масиві нормативно-правового регулювання захисту персональних даних відносно незначна. Умовно їх можна поділити на дві групи:

1) акти, які регламентують питання створення та функціонування електронних баз даних, обробки інформації, ведення реєстрів тощо. Це зокрема постанови від 25 грудня 2013 р. № 958 «Про затвердження Положення про Державну

інформаційну систему електронних звернень громадян [156], від 20 березня 2013 р. № 198 «Про затвердження Порядку реєстрації, перереєстрації безробітних та ведення обліку осіб, які шукають роботу» [157], від 3 січня 2013 р. № 13 «Про затвердження Порядку ведення Єдиного державного порталу адміністративних послуг» [158], від 6 червня 2012 р. № 546 «Про затвердження Положення про електронний реєстр пацієнтів [159], від 18 квітня 2012 р. № 303 «Про затвердження Положення про створення та функціонування Єдиного державного реєстру злочинів торгівлі людьми» [160], від 13 липня 2011 р. № 752 «Про створення Єдиної державної електронної бази з питань освіти» [161], від 25 травня 2011 р. № 616 «Про затвердження Положення про Державний реєстр баз персональних даних та порядок його ведення» [162].

2) акти, які визначають організаційні засади діяльності державних суб'єктів у сфері обробки та захисту персональних даних: постанови від 2 липня 2014 року № 228 «Про затвердження Положення про Міністерство юстиції України» [163], від 20 лютого 2013 року № 118 «Про затвердження Примірного положення про центр надання адміністративних послуг» [164], від 1 серпня 2013 року № 573 «Про затвердження Загального положення про центр соціальних служб для сім'ї, дітей та молоді» [165], від 26 вересня 2012 року № 887 «Про затвердження Типового положення про структурний підрозділ місцевої державної адміністрації» [166] та інші.

Аналіз нормативно-правових актів Кабінету Міністрів України з питань захисту персональних даних свідчить, що значна їх частина недостатньо чітко корелюється з положеннями інформаційного законодавства, а деякі діють попри втрату об'єктивних підстав для існування. Наочним прикладом слугує Положення про Державний реєстр баз персональних даних та порядок його ведення, затверджене постановою Кабінету Міністрів України від 25 травня 2011 р. № 616.

Як відомо, з набранням чинності Закону України від 3 липня 2013 року «Про внесення змін до деяких законодавчих актів України щодо удосконалення системи захисту персональних даних» (тобто з 1 січня 2014 року) в Україні було: а) скасовано процедуру реєстрації баз персональних даних; б) припинено видачу свідоцтв про державну реєстрацію баз персональних даних; в) припинено ведення Державного реєстру баз персональних даних [167]. Тож фактично відповідна реєстраційна процедура перестала існувати.

Однак нормативного реагування на це з боку Кабінету Міністрів України так і не було. Урядове Положення про Державний реєстр баз персональних даних та порядок його ведення досі не скасоване та формально чинне, воно покладає відповідні зобов'язання на суб'єктів суспільних відносин у сфері захисту персональних даних, у тому числі на ДСУЗПД (як володільця реєстру), хоч ця служба вже не має ні реєстраційних, ні контрольних повноважень.

Крім того, неузгодженість законодавчих та урядових актів з питань захисту персональних даних проявляється на рівні термінології. Наприклад, у постанові Кабінету Міністрів України від 13 липня 2011 р. № 752 «Про створення Єдиної державної електронної бази з питань освіти» замість законодавчих термінів використано поняттєві аналоги, яких не знає закон («адміністратор бази даних», «держатель бази даних»). Водночас термін «оброблення персональних даних» вживається не як збірний (тобто в розумінні закону), а як такий, що позначає лише окрему операцію з персональними даними поряд із їх збиранням, верифікацією, обробленням, захистом тощо [161].

Отже, як випливає зі сказаного, урядовий блок нормативно-правової регламентації захисту персональних даних характеризується недоліками, які гальмують процеси його розвитку та знижують ефективність правозастосовної діяльності. З огляду на це відповідні акти Кабінету Міністрів потребують системного перегляду, вдосконалення та гармонізації з іншими актами інформаційного законодавства.

Починаючи з 2014 року, важлива роль у регулюванні відносин сфери захисту персональних даних відводиться нормативно-правовим актам (наказам) уповноваженого Верховної Ради України з прав людини.

Розроблення більшості нормативно-правових актів з питань захисту персональних даних уповноважений здійснював в умовах жорсткого цейтноту. З набуттям відповідних адміністративно-контрольних функцій (1 січня 2014 року) уповноважений мусив якнайшвидше унормувати організаційні аспекти обробки та захисту персональних даних. Адже на той момент в Україні функціонували понад 100 тис. баз персональних даних, тисячі звернень (заяв, скарг, запитів) з питань захисту персональних даних потребували невідкладного розгляду. Однак нормативна база, створена до 2014 року, де-факто втратила актуальність і не підлягала практичному застосуванню.

Адекватною (і що не менш важливо, своєчасною) відповіддю на посталу необхідність стало прийняття уповноваженим наказу від 8 січня 2014 року № 1/02-14 «Про затвердження документів у сфері захисту персональних даних» – комплексного акта, який визначає: типовий порядок обробки персональних даних; процедуру здійснення контролю за додержанням законодавства про захист персональних даних; порядок повідомлення про обробку вразливих персональних даних; засади діяльності структурних підрозділів та/або посадових осіб, відповідальних за безпеку обробки персональних даних, а також інші організаційні питання захисту персональних даних в автоматизованих системах і картотеках.

Значення цього документа важко переоцінити. Він не тільки впорядкував процедуру обробки персональних даних, а й створив підґрунтя для регламентації суспільних відносин в сфері їх захисту на галузевому та регіональному рівнях. Його положення лягли в основу широкого кола відомчих і місцевих нормативних актів. Саме на них ґрунтуються механізми інституційного контролю та публічного адміністрування захисту персональних даних у сучасній Україні.

Однак як свідчить практика вітчизняного нормотворення, форсована розробка нормативно-правового акта не завжди позитивно впливає на його якість. Не став винятком і наказ «Про затвердження документів у сфері захисту персональних даних». За загальним визнанням фахівців, певна частина його положень характеризується істотними недоліками та потребує вдосконалення.

У цьому аспекті чи не найбільшу проблему становить недостатня узгодженість змісту наказу та Закону України «Про захист персональних даних». Розглянемо кілька прикладів.

Відповідно до ч. 6 ст. 6 закону, не допускається обробка даних про фізичну особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини *(підкреслення моє – А.П.)*. Натомість п. 2.7. Типового порядку обробки персональних даних, затвердженого наказом, допускає обробку персональних даних без згоди суб'єкта у всіх випадках, коли такої згоди не вимагає законом.

П. 2 ст. 12 закону зобов'язує володільця персональних даних в односторонньому порядку (без додаткових умов) інформувати суб'єкта цих даних про себе, склад та зміст зібраної інформації, його законні права, мету збирання, а також осіб, яким їх передають. А із контексту п. 2.9. Типового порядку обробки персональних даних (абз. 4) випливає, що зазначена інформація надається тільки за заявою суб'єкта персональних даних.

20 закону наділяє правом вимагати внесення змін до персональних даних, що обробляються, не лише суб'єктів персональних даних, а й інших суб'єктів відносин, пов'язаних із персональними даними, якщо на це є згода суб'єкта персональних даних чи відповідна зміна здійснюється згідно з приписом уповноваженого або визначених ним посадових осіб секретаріату уповноваженого чи за рішенням суду, що набрало законної сили. Наказ же визнає це право тільки за суб'єктами персональних даних.

На підставі п. 5 ст. 23 закону за підсумками контрольних перевірок або розгляду звернень уповноважений може видавати обов'язкові для виконання приписи щодо запобігання або усунення порушень законодавства про захист персональних даних *(підкреслення моє – А.П.)*. Наказ (точніше, затверджений ним Порядок здійснення контролю за додержанням законодавства про захист персональних даних) передбачає можливість складання уповноваженим тільки одного різновиду приписів – припису про усунення порушень законодавства.

Поряд із цими вадами наказу уповноваженого від 8 січня 2014 року № 1/02-14 «Про затвердження документів у сфері захисту персональних даних» властиві й інші недоліки:

неповнота правового регулювання (в наказі розкриті далеко не всі процедурні аспекти обробки та захисту персональних даних);

використання некоректної термінології («протокол про притягнення до адміністративної відповідальності» замість «протокол про адміністративне правопорушення», «особа, присутня при виявленні правопорушення» замість «свідок» тощо);

посилання на неіснуючі нормативно-правові акти (зокрема, в п.п. 5.15 та 5.16 Порядку здійснення контролю за додержанням законодавства про захист персональних даних ідеться про не відомий юридичній практиці документ – Порядок оформлення матеріалів про адміністративні правопорушення);

непослідовність у визначенні деяких процесуальних строків (одні з них обчислюються робочими днями, інші – календарними) і т.ін.

Аналогічні похибки криються також і в численних роз'ясненнях уповноваженого з питань обробки та захисту персональних даних.

Викладене дає підстави для висновку про недостатній якісний рівень нормативно-правового забезпечення захисту персональних даних уповноваженим Верховної Ради України з прав людини. У зв'язку з цим постає необхідність

комплексного аналізу відповідних актів уповноваженого, виявлення та усунення їх недоліків, узгодження їх змісту з чинним інформаційним законодавством та вимогами юридичної техніки.

Значний масив правових норм, які врегульовують ключові аспекти захисту персональних даних, зосереджений у нормативних актах центральних органів виконавчої влади та державних органів зі спеціальним статусом: Міністерства юстиції, Державної служби України з питань захисту персональних даних та інших. Дослідження цього масиву засвідчило наявність широкого спектра проблем, притаманних системі нормативно-правового забезпечення захисту персональних даних загалом. До них належить:

1) невідповідність законодавчим актам з питань обробки та захисту персональних даних. Прикладом може слугувати наказ МВС України від 21 серпня 2013 року № 805 «Про затвердження Порядку обробки персональних даних у базі персональних даних «Електронний журнал обліку запитів на публічну інформацію» [168].

Зокрема, п. 1.7. цього наказу передбачає обов'язкову реєстрацію бази даних «Електронний журнал обліку запитів на публічну інформацію» в Державному реєстрі баз персональних даних, хоч і процедуру обов'язкової реєстрації, і відповідний Державний реєстр було ліквідовано ще за місяць до його видання – на підставі Закону України від 3 липня 2013 року «Про внесення змін до деяких законодавчих актів України щодо удосконалення системи захисту персональних даних» [169].

Згідно з п. 7.4. наказу, суб'єкт персональних даних повідомляється про володільця персональних даних, склад та зміст зібраних персональних даних, свої права, мету збирання та осіб, яким передають його персональні дані: а) в момент збирання персональних даних, якщо персональні дані збирають у суб'єкта персональних даних; б) в інших випадках протягом 10 робочих днів з дня збирання персональних даних. А Закон України «Про захист персональних даних» (ч. 2 ст. 12) відводить на процедуру повідомлення в інших випадках 30 робочих днів.

До того ж, попри безпосередній зв'язок з питаннями доступу до публічної інформації, наказ не враховує деяких положень Закону України «Про доступ до публічної інформації»;

2) внутрішня неузгодженість. Нормативно-правові акти центральних органів виконавчої влади (державних органів зі спеціальним статусом) з питань захисту персональних даних погано корелюються не тільки з актами вищої юридичної сили, а й поміж собою. У їх змісті нерідко мають місце помітні розбіжності. Дуже поширеним явищем є посилання в чинних актах на скасовані.

Так, наказ МВС України від 21 серпня 2013 року № 805 «Про затвердження Порядку обробки персональних даних у базі персональних даних «Електронний журнал обліку запитів на публічну інформацію» [168], постанова Національної комісії державного регулювання у сфері комунальних послуг від 9 серпня 2013 року № 109 «Про затвердження Порядку обробки персональних даних у базі персональних даних «Працівники»« [170], а також постанова Національної комісії державного регулювання у сфері енергетики від 17 січня 2013 року № 20 «Про затвердження Порядку обробки персональних даних у базі персональних даних НКРЕ» [171] (всі документи чинні) ґрунтуються на положеннях наказу Міністерства юстиції України від 30 грудня 2011 року № 3659/5 «Про затвердження Типового порядку обробки персональних даних у базах персональних даних», який втратив чинність 28 листопада 2013 року [172];

3) неповнота правового регулювання. Більшість відомчих нормативно-правових актів упорядковує лише окремі аспекти захисту персональних даних. Як правило, це загальні відомості про бази даних, що перебувають у віданні конкретного органу державної влади (місцезнаходження, форми обробки інформації тощо), цілі та підстави обробки персональних даних, їх структура, коло суб'єктів правовідносин з приводу їх обробки (суб'єкти персональних даних, володільці, розпорядники, треті особи, посадові особи/підрозділи,

відповідальні за обробку та захист персональних даних), права, обов'язки й повноваження цих суб'єктів, а також загальні моменти процедури обробки персональних даних.

При цьому за межами регламентації або недостатньо врегульованими залишаються питання, пов'язані з визначенням джерел збору персональних даних, повідомленням уповноваженого про обробку персональних даних, що становить особливий ризик для прав і свобод громадян, відстроченням доступу до персональних даних, тривалості їх зберігання у відповідній базі та багато інших;

4) недосконале формулювання змісту. Як показало дослідження, окремі положення нормативно-правових актів центральних органів виконавчої влади (державних органів зі спеціальним статусом) з питань захисту персональних даних сформульовані в спосіб, який утруднює їх правильне розуміння та ефективне застосування.

Наприклад, п. 1.7 постанови Національної комісії державного регулювання у сфері комунальних послуг від 9 серпня 2013 року № 109 «Про затвердження Порядку обробки персональних даних у базі персональних даних «Працівники» визначає, що третіми особами, яким здійснюється передача персональних даних відповідно до закону, є будь-які «юридичні та фізичні особи, що звертаються із запитом щодо доступу до персональних даних працівників» [170].

Цілком очевидно, що таке формулювання, по-перше, не має під собою належного законодавчого підґрунтя (жоден закон не передбачає вільного поширення відомостей з названої бази даних); по-друге, суперечить ч. 2 п. 4.15 цієї постанови, яка допускає поширення персональних даних без згоди суб'єкта тільки на підставі закону і лише в інтересах національної безпеки, економічного добробуту та прав людини; по-третє, позбавляє сенсу ч. 1 п. 4.15 постанови, згідно з якою передача персональних даних третім особам визначається або умовами згоди працівника на їх обробку, або відповідно до вимог закону (адже в розумінні п. 1.7 постанови будь-які випадки передачі персональних даних здійснюються на підставі закону, отже не потребують обов'язкової згоди суб'єкта).

Або інший приклад. Відповідно до п. 5.1 наказу МВС України від 21 серпня 2013 року № 805, фізична особа, персональні дані якої обробляються, має право: отримувати інформацію про умови надання доступу до персональних даних, зокрема, інформацію про третіх осіб, що міститься в базі персональних даних «Електронний журнал обліку запитів на публічну інформацію» *(підкреслення моє. – А.П.)* [168]. Суть цього положення нелегко збагнути, оскільки відповідна база даних стосується виключно тих громадян, які подали до МВС України запит на публічну інформацію, і не містить жодних відомостей про третіх осіб (читай – осіб, яким може здійснюватись передача персональних даних).

Подібних прикладів багато. Проте гадаємо, викладеного цілком достатньо для усвідомлення того, що й відомчий рівень нормативно-правового забезпечення захисту персональних даних не вирізняється досконалістю. Відповідні акти центральних органів виконавчої влади та державних органів зі спеціальним статусом мають чимало недоліків, ліквідація яких має стати одним з пріоритетних завдань інституціонального нормотворення.

І нарешті місцевий рівень нормативно-правового забезпечення захисту персональних даних репрезентують акти територіальних підрозділів центральних органів виконавчої влади, місцевих державних адміністрацій та місцевих рад.

Конкретні форми цих актів визначаються законодавством і характеризуються різноманітністю [195, с. 127–128]. Так, відповідно до ст. 59 Закону України «Про місцеве самоврядування», сільські, селищні, міські, районні та обласні ради, а також виконкоми місцевих рад ухвалюють акти у вигляді рішень. Нормативно-правові акти сільських, селищних та міських голів мають форму розпоряджень [173]. Ст. 6 Закону України «Про місцеві державні адміністрації» уповноважує голів місцевих державних адміністрацій видавати розпорядження, а керівників їхніх структурних підрозділів (управлінь, відділів тощо) – накази [174]. Так само у формі

наказів видають акти територіальні підрозділи (органи) центральних органів виконавчої влади (див. п. 9 постанови Кабінету Міністрів України від 25 травня 2011 р. № 563 «Про затвердження Типового положення про територіальні органи міністерства та іншого центрального органу виконавчої влади» [175]).

За своєю цільовою спрямованістю нормативно-правові акти суб'єктів місцевої влади з питань захисту персональних даних вельми однотипні. Майже всі вони мають внутрішньо-організаційний характер і скеровуються на регулювання процедур обробки та захисту персональних даних у відповідному органі, його підрозділах або у ж конкретній базі даних, яка перебуває в їх володінні. Ця риса зумовлює невелику кількість нормативно-правових актів, виданих одним і тим самим органом (підрозділом, посадовою особою). Як правило, більшість суб'єктів місцевої влади обмежуються виданням одного нормативно-правового акта (порядку, регламенту, положення) в сфері обробки та захисту персональних даних.

Однак через велику кількість суб'єктів видання (у наш час загальна їх загальна кількість обчислюється десятками тисяч) продукований ними масив нормативно-правових актів є надзвичайно великий. І саме в ньому найбільш виразно проявляються системні вади нормативно-правового забезпечення захисту персональних даних.

Нині навіть на рівні аналогічних організаційних структур (обласних рад, обласних державних адміністрації, обласних управлінь центральних органів виконавчої влади і т.ін.) досить виразно проявляються розбіжності в деталізації правового регулювання, трактуванні законодавчих положень, використанні термінології, послідовності викладу нормативного матеріалу. Уніфікована хіба що структура нормативно-правових актів з питань захисту персональних даних, та й то лише завдяки тому, що в основу більшості з них покладено єдиний базовий документ – Типовий порядок обробки персональних

даних у базах персональних даних, затверджений наказом Міністерства юстиції України від 30 грудня 2011 року № 3659/5 [172]. Але оскільки цей документ втратив чинність ще восени 2013 року, таку одноманітність навряд чи можна вважати істотним здобутком.

Взагалі посилання на акти, які вже втратили чинності або зазнали принципових змін, є типовою рисою нормативно-правового регулювання захисту персональних даних на місцях. Як показав аналіз 24 регламентів обробки та захисту персональних даних, затверджених на рівні обласних рад, жоден з них після ухвалення не піддавався оновленню у зв'язку зі змінами інформаційного законодавства. Проте останніми роками ці зміни мали всеосяжний, кардинальний характер. Із 2012 року лише Закон «Про захист персональних даних» щонайменше шість разів зазнавав комплексних змін. Протягом цього періоду змінювались і інші закони. Було суттєво змінено більшу частину урядових і відомчих актів з питань захисту персональних даних. Багато з них втратили юридичну силу внаслідок скасування або ж через зміну обставин, на які вони були розраховані.

Однак на системі актів місцевої влади з питань захисту персональних даних ці нормативно-правові перетворення жодним чином не позначились. Як наслідок, останні відсилають правозастосовця до вже не актуальних документів та неіснуючих вимог, слідування яким за сучасних умов є не тільки алогічним, а й контрпродуктивним. Нині всі регламенти обласних рад (ідеться про регламенти щодо обробки та захисту персональних даних), а також більшість регламентів інших місцевих рад і місцевих державних адміністрацій посилаються на раніше скасовані акти вищої юридичної сили. При цьому деякі з них містять по два і більше таких посилань. Здебільшого це посилання на постанову Кабінету Міністрів України від 25 травня 2011 р. № 616 «Про затвердження Положення про Державний реєстр баз персональних даних та порядок його ведення» [162], наказ Міністерства

юстиції України від 30 грудня 2011 року № 3659/5 «Про затвердження Типового порядку обробки персональних даних у базах персональних даних» [172], наказ Міністерства юстиції України від 8 липня 2011 року № 1824/5 «Про затвердження форм заяв про реєстрацію бази персональних даних та про внесення змін до відомостей Державного реєстру баз персональних даних і порядку їх подання» [176] та ін.

Такий стан справ вкрай негативно відображається на якості нормативно-правового регулювання захисту персональних даних. Поступова втрата зв'язків із чинним законодавством (законами, постановами уряду, наказами міністерств тощо) зумовила деактуалізацію великого масиву нормативно-правових актів суб'єктів місцевої влади з питань обробки та захисту персональних даних. У ході оновлення актів загальнодержавної дії їх положення дедалі більше дисонували з актами місцевого рівня, розвиток яких перебігав дуже мляво. Зрештою це призвело до появи великої кількості неробочих норм, різноманітних неузгодженостей і колізій, а також до різнобою в правозастосуванні.

І це далеко не вичерпний перелік проблем правового забезпечення сфери захисту персональних даних на місцевому рівні. Поширені недоліки нормативно-правового регулювання такі: недостатня чіткість та неоднозначність окремих нормативних положень; фрагментарність і недостатня повнота правової регламентації; внутрішня неузгодженість нормативних актів та суперечність їх окремих положень.

Підсумовуючи аналіз нормативно-правового забезпечення захисту персональних даних, мусимо констатувати, що фактично всім рівням інституціонального законодавства властиві системні недоліки. Це зокрема і вади понятійного апарату, і фрагментарне регулювання суспільних відносин, і неузгодженість правових вимог, і наявність колізій, і дисгармонійність структури, і змістові огріхи, і багато іншого. Здебільшого ці недоліки мають комплексний характер. Їх не усунути шляхом розрізнених заходів і точкових змін. На часі масштабне оновлення вітчизняного інформаційного

законодавства з урахуванням актуальних проблем, нагальних потреб практики, вимог техніки нормотворення, міжнародних зобов'язань України та рекомендацій ЄС.

У межах цієї мети доцільно:

1) здійснити ґрунтовний перегляд вітчизняного інформаційного законодавства на предмет відповідності міжнародним договорам України, наявності прогалин, колізій і дублювань, повноти регуляторного охоплення, змістової та структурної узгодженості, відповідності правилам юридичної техніки. Усунути наявні недоліки шляхом внесення комплексних змін до законодавчих і підзаконних нормативно-правових актів з питань захисту інформації;

2) внести до Закону України «Про інформацію» зміни, спрямовані на: уточнення дефініції поняття «інформація»; розширення кола суб'єктів права на інформацію та суб'єктів інформаційних відносин; побудову науково обґрунтованої класифікації видів інформації; запровадження диференційованого підходу до конфіденціалізації персональних даних (законодавчий поділ персональних даних на загальні та чутливі); конкретизацію переліку чутливих персональних даних; чітке визначення підстав для поширення інформації з обмеженим доступом; кореляцію положень закону з актами деліктного законодавства (Кримінальний кодекс України, Кодекс про адміністративні правопорушення та ін.) у частині визначення підстав для звільнення від відповідальності за інформаційні правопорушення;

3) розробити та ухвалити проект закону «Про внесення змін до Закону України «Про захист персональних даних», який передбачатиме:

- вдосконалення законодавчої термінології, зокрема, уточнення понять «база персональних даних», «обробка персональних даних», «використання персональних даних», «одержувач» та ін.;
- законодавче закріплення вимог: а) щодо обов'язкового направлення фізичній особі запиту про надання дозволу на обробку її персональних даних у письмовій, електронній або

іншій формі; б) щодо обов'язкового зазначення у відповідному запиті відомостей про володільця та розпорядника (розпорядників) персональних даних, мету збирання інформації, склад та зміст питомих персональних даних; строк їх обробки; осіб, яким їх передаватимуть; права суб'єкта персональних даних у сфері їх захисту; в) те, що ненадання відповіді на запит слід розглядати як відсутність дозволу (читай заборону) на обробку персональних даних;

- введення держави та суб'єктів міжнародного права до кола суб'єктів правовідносин, пов'язаних з персональними даними;
- узгодження положень закону (абз. 3 ст. 2 та ч. 2 ст. 4), якими визначається суб'єктний склад володільців персональних даних;
- вилучення зі змісту закону та практичного обігу терміна «знеособлені персональні дані» як такого, що містить внутрішню суперечність та не узгоджується із правилами формальної логіки;
- запровадження вимоги, згідно з якою будь-які зміни в цільовому призначенні обробки персональних даних (а не лише не сумісні з раніше узгодженою метою) вимагають обов'язкової згоди їх суб'єкта;
- узгодження права суб'єкта персональних даних на отримання пов'язаної з ним (його даними) інформації та права фізичної особи – володільця персональних даних на конфіденційність інформації про себе;
- конкретизацію основних способів поширення персональних даних;
- розширення переліку підстав для видалення або знищення персональних даних (до таких потрібно зарахувати випадки відкликання суб'єктом персональних даних раніше даної згоди на їх обробку, а також пред'явлення ним умотивованої вимоги володільцеві персональних даних із запереченням проти обробки інформації, яка його стосується);
- обмеження права безперешкодного доступу органів влади до персональних даних випадками, коли такий доступ

здійснюється на підставі закону, за наявності спеціальних гарантій, з метою захисту життєво важливих інтересів громадянина, суспільства, держави;

- удосконалення механізмів обробки персональних даних (зокрема збирання, внесення змін і доповнень до персональних даних, повідомлення про дії з ними);
- гармонізацію структури закону, викладення його положень у чіткій логічній послідовності, з урахуванням їхнього характеру, змісту та предметного спрямування;

4) скасувати постанову Кабінету Міністрів України від 25 травня 2011 р. № 616 «Про затвердження Положення про Державний реєстр баз персональних даних та порядок його ведення»;

5) розробити та впровадити дієвий механізм моніторингу інформаційного законодавства (як вітчизняного, так і міжнародного), який би забезпечив ретельне відстеження поточних змін, синхронне оновлення всіх його рівнів і складових, кореляцію галузевої нормотворчості;

6) створити умови для залучення наукових кіл і широкої громадськості до нормопроектувальної роботи у сфері інформаційної безпеки. Організувати регулярне проведення тематичних заходів: форумів, конференцій, семінарів, круглих столів, громадських слухань тощо;

7) посилити контроль за якістю інституціонального нормотворення, додержанням законності у сфері розроблення та ухвалення нормативно-правових актів з питань захисту персональних даних, а також за ефективністю практичної реалізації їх положень.

2.2. Публічна адміністрація у сфері захисту персональних даних

На загальнодержавному рівні захист персональних даних являє собою складний багатоаспектний процес, перебіг якого визначається широким колом суб'єктів: органами

державної влади, громадськими інститутами, приватними структурами, юридичними та фізичними особами. Усі вони (і ті, хто формує інформаційну політику, і ті, хто її реалізовує, і ті, хто здійснює обробку персональних даних, і ті, хто гарантує безпеку конфіденційної інформації) чинять істотний вплив на функціонування та розвиток сфери захисту персональних даних.

Однак, поза всяким сумнівом, ключову роль у цьому процесі відіграє публічна адміністрація. Правове регулювання кореспондуючих суспільних відносин, забезпечення їх комплексної організації, охорони та захисту здійснює система державних і представницьких органів, наділених владними повноваженнями (зокрема правом застосування примусу), широкий організаційний інструментарій, відповідні матеріальні, технічні й кадрові ресурси.

У сучасних умовах публічна адміністрація несе основний тягар відповідальності за формування та реалізацію державної політики у всіх сферах суспільного життя. Суб'єкти публічного адміністрування як провідна організаційна сила демократичного суспільства визначають стратегічні та пріоритетні напрями соціально-економічного розвитку. Вони здійснюють організаційний вплив на провідні сектори суспільних відносин, формують зміст конкретних соціальних зв'язків, сполучають їх правову форму, забезпечують підтримку, охорону та захист, гарантують стабільність і безпеку. Вони вибудовують організаційний механізм такого впливу і самі ж виступають його стрижневим елементом [177, с. 37]. Публічна адміністрація є головним виконавцем суспільного замовлення на ефективний, відповідальний і професійний менеджмент в масштабах держави, регіону, галузі [178, с. 37].

Аналіз чинного законодавства дає підстави для висновку, що публічна адміністрація у сфері захисту персональних даних охоплює розгалужену систему владних суб'єктів (органів та посадових осіб), котрі, поряд із вирішенням загально-управлінських питань, реалізують специфічні

напрями адміністрування в царині обробки та захисту персональних даних. На сьогодні до цієї системи входять: Верховна Рада, Президент, Кабінет Міністрів, уповноважений Верховної Ради України з прав людини, центральні органи виконавчої влади, місцеві державні адміністрації та органи місцевого самоврядування.

1. Верховна Рада України відіграє важливу роль у формуванні засад публічного адміністрування захисту персональних даних. Як єдиний орган законодавчої влади (ст. 75 Конституції) Верховна Рада на вищому нормативно-правовому рівні встановлює вимоги щодо обробки та захисту персональних даних, окреслює коло суб'єктів відповідних правовідносин, визначає порядок інституціонального контролю, спеціальні повноваження органів влади, кореспондуючі права та обов'язки фізичних і юридичних осіб.

У рамках реалізації правовстановлюючої функції Верховна Рада дає згоду на обов'язковість міжнародних договорів з питань захисту персональних даних, що автоматично робить їх елементом вітчизняного законодавства. Наочним прикладом можуть слугувати Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних та Додатковий протокол до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних стосовно органів нагляду та транскордонних потоків даних, ратифіковані Верховною Радою України 6 липня 2010 року [89].

Верховна Рада впливає на адміністрування захисту персональних даних шляхом регулювання правового статусу уповноважених суб'єктів. Саме акти парламенту (закони України) визначають організаційні засади діяльності уповноваженого за прав людини, центральних і місцевих органів виконавчої влади, суб'єктів місцевого самоврядування [90; 118; 138].

Не менш важливим напрямом впливу Верховної Ради на сферу захисту персональних даних є вирішення кадрових

питань у системі публічної адміністрації. Зокрема, саме Верховна Рада призначає на посаду ключового суб'єкта публічного контролю в сфері захисту персональних даних – уповноваженого Верховна Рада України з прав людини [179].

Поряд з ухваленням законодавчих актів, вирішенням організаційних питань та узгодженням кадрових призначень Верховна Рада регламентує сферу захисту персональних даних за допомогою різних форм парламентського контролю. Так, на підставі п. 13 ст. 85 Конституції України у випадках, передбачених законом, Верховна Рада України здійснює контроль за діяльністю уряду, а саме: приймає рішення щодо схвалення програми діяльності Кабінету Міністрів; щорічно заслуховує та розглядає звіт Кабінету Міністрів про перебіг і підсумки виконання Програми діяльності уряду, а також доповіді про хід і результати виконання загальнодержавних програм (у томі числі програм інформаційної безпеки та захисту персональних даних); розглядає питання про відповідальність Кабінету Міністрів [116].

2. Президент як глава держави та гарант державного суверенітету, територіальної цілісності, додержання Конституції України, прав і свобод людини та громадянина здійснює загальне керівництво всіма напрямами державно-політичної діяльності, в тому числі діяльністю щодо гарантування інформаційної безпеки та захисту персональних даних. Глава держави репрезентує державу загалом. Це зумовлює неможливість його входження до інших владних структур, які втілюють лише окремі напрями реалізації державної влади (законотворення, правосуддя, виконавчо-розпорядчу діяльність). Визнання Президента главою держави зумовлює його організаційну самостійність та здатність чинити комплексний вплив на функціонування всіх гілок державної влади.

Однак як показує практика, попри особливий правовий статус, потужний арсенал владних повноважень, реальна участь Президента в адмініструванні сфери вельми обмежена. Після конституційної реформи початку 2014 року значна

частина повноважень (зокрема щодо створення центральних органів виконавчої влади та призначення їх керівництва) перейшли від глави держави до парламенту та Кабінету Міністрів, що автоматично спричинило звуження форм адміністративної діяльності. Однак у розпорядженні Президента залишаються вельми потужні важелі адміністративного впливу: право зупинення чинності актів Кабінету Міністрів України з мотивів невідповідності Конституції, призначення голів місцевих державних адміністрацій, керівництво Радою національної безпеки і оборони як суб'єктом контролю за діяльністю органів виконавчої влади у сфері національної безпеки та інші.

Викладене дає підстави для висновку, що і сьогодні, і в осяжному майбутньому Президент України відіграватиме важливу роль у системі управління сферою захисту персональних даних, визначаючи загальні тенденції її розвитку та скеровуючи процеси, які в ній відбуваються.

3. Чільне місце у вітчизняній системі публічного адміністрування займає Кабінет Міністрів, як вищий виконавчої влади. Кабінет Міністрів здійснює адміністрування сферою захисту персональних даних як безпосередньо, так і через окремі міністерства, інші центральні органи виконавчої влади, Раду міністрів Автономної Республіки Крим та місцеві державні адміністрації, спрямовуючи, координуючи й контролюючи їхню діяльність.

У чинному законодавстві спеціальні повноваження Кабінету Міністрів щодо адміністрування сфери захисту персональних даних не конкретизовано. Тому належне уявлення про зміст і характер цих повноважень можна сформувати лише на підставі вивчення загальних положень Закону «Про Кабінет Міністрів України» та практичних аспектів урядової діяльності [180].

Аналіз правового статусу Кабінету Міністрів, а також його нормотворчої та правозастосовної практики свідчить, що основними формами його участі в адмініструванні сфери

захисту персональних даних є: розроблення законопроектів з питань захисту персональних даних;* забезпечення розроблення та організація виконання загальнодержавних програм з питань захисту інформації, фінансування цих програм, контроль за їх виконанням; спрямування й координація роботи міністерств та інших органів виконавчої влади у сфері захисту персональних даних; створення, реорганізація та ліквідація центральних органів виконавчої влади, відповідальних за проведення державної інформаційної політики; здійснення кадрових призначень (зокрема призначення на посади та звільнення з посад керівників центральних органів виконавчої влади, які не входять до складу уряду); контроль за додержанням законодавства органами виконавчої влади, їх посадовими особами, а також органами місцевого самоврядування в частині делегованих їм виконавчих повноважень; визначення правових засад функціонування та порядку ведення Державного реєстру баз персональних даних; планування та реалізація заходів щодо захисту інформаційних прав і свобод, в тому числі права на конфіденційність приватного життя; забезпечення виконання органами виконавчої влади та їх керівниками судових рішень у справах про захист персональних даних.

Наведений перелік не є вичерпним. Чинне законодавство наділяє Кабінет Міністрів значним обсягом повноважень та широкими можливостями щодо адміністрування захисту персональних даних. Однак далеко не всі з них сповна реалізуються на практиці.

Частково це можна пояснити об'єктивними чинниками. Наприклад, повноваження щодо створення центральних органів виконавчої влади, визначення їх правового статусу та

* Зокрема, на розгляд VII сесії Верховної Ради України уряд вніс проекти законів «Про вдосконалення інституційної системи захисту персональних даних» (від 12.02.2013 р., реєстр. № 2282) та «Про внесення змін до законів України, пов'язаних з діяльністю Уповноваженого Верховної Ради України з прав людини у сфері захисту персональних даних» (від 25.03.2014 р., реєстр. № 4551).

самостійного формування їх кадрового складу уряд отримав лише з проведенням конституційної реформи 2014 року. Тому до останнього часу їх реалізація на рівні Кабінету Міністрів була неможливою.

Проте в більшості випадків інертність уряду зумовлена браком уваги до проблематики захисту персональних даних.

За роки незалежності в Україні не було ухвалено жодної державної програми з питань інформаційної безпеки та захисту персональних даних (не було розроблено навіть концепції таких програм). Недостатньо добре налагоджена взаємодія між різними суб'єктами адміністрування захисту персональних даних, наявні дублювання їх повноважень не усуваються. Зміни законодавства про захист персональних даних знаходять відображення в нормативно-правових актах уряду з великим запізненням. Вельми низький рівень контролю за станом додержання інформаційного законодавства в системі виконавчої влади. Непослідовно і мляво провадиться соціально-інформаційна робота.

Такий стан справ не відповідає запитам сьогодення. В умовах, коли проблеми інформаційної безпеки стоять на шляху євроінтеграційних устремлінь та гальмують втілення амбітних міжнародних проектів, їх вирішенню слід приділити значно більше уваги. І насамперед уряд повинен відігравати головну роль у цьому процесі, консолідуючи та скеровуючи зусилля виконавчої влади на найбільш відповідальних ділянках адміністрування захисту персональних даних.

Важливими кроками в цьому напрямку мають стати:

розроблення та затвердження державної цільової програми захисту персональних даних, яка мала б міжгалузевий характер та ґрунтувалася на принципах доцільності, комплексності, цілеспрямованості, соціальної та економічної обґрунтованості;

комплексний аналіз правового статусу суб'єктів, задіяних в адмініструванні сфери захисту персональних даних, чітке розмежування їх компетенції, спеціальних повноважень та сфер відповідальності;

посилення контролю за станом додержання законодавства про захист персональних даних органами виконавчої влади, в тому числі – за виконанням відповідних судових рішень;

створення дієвого механізму координації роботи органів виконавчої влади в сфері захисту персональних даних.

Крім того, на наш погляд, основні напрями діяльності уряду щодо захисту персональних даних повинні знайти обов'язкове закріплення в чинному інформаційному законодавстві, зокрема, в Законі України «Про захист персональних даних». З цією метою вказаний закон пропонуємо доповнити спеціальним положенням (статтею чи низкою статей), котре б окреслювало коло суб'єктів публічного адміністрування сфери захисту персональних даних та визначало коло їх повноважень у цій сфері.

4. Переходячи до висвітлення ролі уповноваженого Верховної Ради України з прав людини в адмініструванні захисту персональних даних, слід обмовитись, що історія його участі в адмініструванні захисту персональних даних є відносно нетривалою. Її початок датується 1 січня 2014 року – моментом набуття чинності змін до Закону України «Про захист персональних даних», згідно з якими омбудсмана було визнано суб'єктом відносин у сфері обробки персональних даних, та, одночасно, наділено комплексом спеціальних нормотворчих, організаційних, розпорядчих, контрольних і юрисдикційних повноважень, зокрема: отримувати пропозиції, скарги та інші звернення з питань захисту персональних даних та приймати рішення за результатами їх розгляду; проводити на підставі звернень або із власної ініціативи перевірки володільців та розпорядників персональних даних; затверджувати нормативно-правові акти в сфері захисту персональних; видавати обов'язкові для виконання вимоги (приписи) про запобігання або усунення порушень законодавства про захист персональних даних, у тому числі щодо зміни, видалення або знищення персональних даних, забезпечення доступу до них, надання чи заборони їх надання третій особі, зупинення або припинення обробки персональних даних; надавати

рекомендації щодо практичного застосування законодавства про захист персональних даних; складати протоколи про притягнення до адміністративної відповідальності та направляти їх до суду у випадках, передбачених законом; інформувати про законодавство з питань захисту персональних даних, проблеми його практичного застосування, права і обов'язки суб'єктів відносин, пов'язаних із персональними даними; здійснювати моніторинг нових практик, тенденцій та технологій захисту персональних даних; організовувати та забезпечувати міжнародну взаємодію у сфері захисту персональних даних тощо [90].

На перший погляд, наведений перелік повноважень видається достатньо змістовним і повним. Він втілює у собі потужний адміністративний інструментарій, покликаний забезпечувати багатоаспектний вплив на кореспондуючу сферу суспільних відносин. Разом з тим нинішній стан його практичної реалізації неможливо визнати задовільним. Наразі більшість повноважень омбудсмана щодо захисту персональних даних є радше декларативними, аніж такими, що послідовно втілюються у життя. Головна причина того – гострий дефіцит кадрових ресурсів.

З метою належного виконання функцій уповноваженого на місцях діють регіональні представництва уповноваженого [181] та представники уповноваженого [182], які представляють його інтереси з усіма правами, що надані чинним законодавством. Та, вочевидь, їх організаційний потенціал недостатній для повноцінного виконання омбудсмана у сфері захисту персональних даних.

Станом на 2018 рік в Україні функціонувало 12 регіональних представництв та 8 представників омбудсмана. Через розмаїття виконуваних функцій (лише один представник уповноваженого спеціалізується на вирішенні питань захисту персональних даних) їм надзвичайно складно забезпечити всебічний і повний контроль за додержанням законодавства про захист персональних даних.

Якщо до 2014 року більшість контрольних функцій у сфері захисту персональних даних виконувала Державна служба України з питань захисту персональних даних – центральний орган виконавчої влади з досить потужним кадровим складом (51 особа), то сьогодні ці функції реалізує управління секретаріату омбудсмана з питань захисту персональних даних, в структурі якого працюють близько 20 осіб.

У світлі цього здатність управління (в його нинішньому складі) ефективно впоратися з усіма напрямами діяльності у сфері захисту персональних даних виглядає досить сумнівною. На наш погляд, неабияка складність, різноплановість та об'ємність завдань, поставлених перед управлінням, зумовлюють постановку питання про розширення його посадового складу до меж, які б відповідали реальним обсягам робочого навантаження на підрозділ та його працівників.

Ще одним чинником негативного впливу на діяльність секретаріату уповноваженого щодо захисту персональних даних є недоліки правового забезпечення. Аналіз нормативно-правові актів, якими визначається правовий статус уповноваженого та його секретаріату, свідчить про принципові суперечності.

Наприклад, п. 10 ст. 23 Закону України «Про захист персональних даних» покладає функцію щодо складання протоколів про адміністративні проступки у сфері захисту персональних даних безпосередньо на уповноваженого; ст. 255 КУпАП – на посадових осіб секретаріату уповноваженого; п. 6.7. Положення про представників уповноваженого Верховної Ради України з прав людини – на представників омбудсмана, а п. 7.5. Положення про регіональні представництва уповноваженого – на працівників відповідних регіональних представництв [90; 138; 181; 182].

Водночас ціла низка визначених Законом України «Про захист персональних даних» повноважень секретаріату

омбудсмана (як-то видання обов'язкових для виконання приписів, взаємодія з підрозділами/особами, відповідальними за обробку персональних даних, тощо) не знайшли відображення в Положенні про секретаріат, затвердженому наказом уповноваженого від 20 червня 2012 року № 4/8-12 [183].

Цілком очевидно, що наявні колізії аж ніяк не сприяють ефективному адмініструванню сфери захисту персональних даних. Їх існування спричиняє юрисдикційну невизначеність та створення конфліктних ситуацій. Тож існує нагальна необхідність комплексного перегляду та узгодження змісту нормативно-правових актів, якими визначається правовий статус уповноваженого, його секретаріату, регіональних представництв і представників.

5. Характеризуючи роль центральних органів виконавчої влади в публічному адмініструванні захисту персональних даних, слід зауважити, що більшість їх реалізують відповідні адміністративні функції тільки в окремій галузі. Вони не визначають категорії персональних даних, обробка яких становить особливий ризик для прав і свобод громадян, не встановлюють загальних вимог щодо їх захисту, не провадять надвідомчих перевірок, не беруть участі у виявленні, припиненні та розкритті інформаційних правопорушень. Фактично даний напрям діяльності реалізується ними лише тією мірою, яка продиктована внутрішньоорганізаційними потребами та специфікою галузевого управління.

Однак перед кожним центральним органом виконавчої влади, незалежно від напряму його діяльності, постає завдання щодо всебічного забезпечення прав людини у сфері оброблення персональних даних. З цією метою у структурі всіх міністерств, служб, агенцій та інших відомств створюються спеціалізовані підрозділи (визначаються відповідальні особи) з питань захисту персональних даних, до компетенції яких входить: визначення реальних і потенційних загроз для безпеки персональних даних, що обробляються; аналіз стану додержання інформаційного

законодавства, виявлення правопорушень, інформування про них керівництва з метою вжиття необхідних заходів; взаємодія з уповноваженим Верховної Ради України з прав людини та визначеними ним посадовими особами його секретаріату щодо запобігання й усунення порушень законодавства про захист персональних даних; забезпечення реалізації прав і свобод суб'єктів персональних даних. Вимоги такого підрозділу/особи щодо гарантування безпеки обробки персональних даних обов'язкові для всіх працівників, які здійснюють обробку персональних даних [184].

Крім того, в системі центральних органів виконавчої влади існує орган, уповноважений здійснювати адміністрування захисту персональних даних на міжгалузевому (загальнодержавному) рівні. Це Міністерство юстиції України.

Міністерство юстиції України є головним органом системи центральних органів виконавчої влади з формування та забезпечення реалізації державної політики захисту персональних даних. До найбільш типових форм діяльності міністерства в сфері захисту персональних даних належать інституціональне нормотворення, контроль за додержанням законодавства, видання обов'язкових наказів і доручень, а також спрямування й координація діяльності суб'єктів публічної адміністрації у сфері захисту персональних даних [163].

На жаль, як показує досвід останніх років, реальна участь Міністерства юстиції в адмініструванні захисту персональних даних обмежується вирішенням представницьких і внутрівідомчих питань. Натомість питання стратегічного планування та міжвідомчої координації в цій сфері здебільшого перебувають без уваги.

А саме Міністерство юстиції, відповідно до покладених на нього завдань і функцій, мало б торувати шляхи для реалізації державної політики захисту персональних даних. Саме воно має повинно давати загальну оцінку її ефек-

тивності, знаходити витоки наявних проблем, вибудовувати стратегію їх вирішення та, у разі потреби, виступати провідником інституційних перетворень в системі адміністрування захисту персональних даних.

Вважаємо, що вказані напрями діяльності мають знайти конкретизацію як у провідних актах інформаційного законодавства (Законі «Про інформацію», Законі «Про захист персональних даних» та ін.), так і в Положенні про Міністерство юстиції України, затвердженому постановою Кабінету Міністрів від 2 липня 2014 року № 228 [163].

6. Місцеві державні адміністрації та органи місцевого самоврядування здійснюють адміністрування захисту персональних даних на рівні окремих адміністративно-територіальних одиниць. Зокрема, відповідно до чинного законодавства, обласні, районні, Київська та Севастопольська міські державні адміністрації: організовують реалізацію державних програм захисту персональних даних; у межах своїх повноважень здійснюють контроль за додержанням інформаційного законодавства; затверджують правила обробки персональних даних в підпорядкованих органах, підрозділах, підприємствах, установах, організаціях; здійснюють заходи щодо організації правового інформування населення з питань захисту персональних даних; реалізують інші функції, передбачені Конституцією та законами України, актами Президента, Кабінету Міністрів, органів виконавчої влади вищого рівня.

Суб'єкти місцевого самоврядування: забезпечують виконання вимог законодавства та рішень центральних органів виконавчої влади з питань інформаційної безпеки та захисту персональних даних; затверджують положення про порядок обробки та захист персональних даних, які перебувають у їхньому володінні; контролюють діяльність комунальних підприємств щодо обробки та захисту персональних даних; здійснюють заходи профілактики порушень інформаційного законодавства.

Отже, як свідчить наведений перелік повноважень, основний вектор діяльності суб'єктів місцевої влади спрямовується на захист персональних даних всередині їх системи. Вони впорядковують обробку персональних даних виключно в рамках своєї організаційної структури. Здійснюваний ними контроль за додержанням законодавства має суто внутрішній характер. Зовнішню (скеровану на організаційно не пов'язаних з ними суб'єктів) нормотворчу, контрольну, наглядову та юрисдикційну діяльність вони не провадять.

Однак внесок суб'єктів місцевої влади в реалізацію державної політики захисту персональних даних не слід недооцінювати. З огляду на величезну кількість підпорядкованих структур, колосальний масив оброблюваної інформації та велику інтенсивність такої обробки їхній вплив на сферу захисту персональних даних має неабиякі масштаби. Не варто скидати з рахунків функції, спрямовані на реалізацію інформаційної політики регіону, як-то: участь у державному плануванні (програмуванні) заходів інформаційної безпеки, нормопроектувальній діяльності, проведення інформаційно-роз'яснювальної роботи (зокрема соціальна реклама) тощо.

Таким чином, місцеві державні адміністрації та органи місцевого самоврядування є важливою складовою системи адміністрування захисту персональних даних, від якої залежить не тільки безпека обробки інформації на окремих об'єктах, а й ефективність інформаційної політики загалом.

У зв'язку з цим неможливо оминути увагою нагальні проблеми місцевого адміністрування захисту персональних даних, як-то:

– анахронізм нормативно-правового регулювання (здебільшого місцеві органи влади реагують на новели вітчизняного інформаційного законодавства з великим запізненням, не поспішаючи корелювати з ними раніше видані акти);

– нечіткий розподіл повноважень (а в окремих випадках навпаки – дублювання функцій) місцевих державних адміністрацій та органів місцевого самоврядування, які функціонують на одній і тій самій території;

– недостатня увага до питань захисту персональних даних, відведення їм другорядної (порівняно з питаннями економічного характеру) ролі та низька активність у їх вирішенні.

За загальним визнанням науковців і практиків, окреслені проблеми потребують якнайшвидшого розв'язання в рамках як загальнодержавної, так і регіональних інформаційних політик.

Отже, підсумовуючи аналіз організаційних засад механізму адміністрування захисту персональних даних, мусимо констатувати недостатню реалізацію його багатого потенціалу. Попри наявність безперечних здобутків, цей механізм функціонує розбалансовано, а результати його діяльності не відповідають об'єктивним потребам суспільства. Такий стан справ зумовлений широким колом організаційно-правових проблем, котрі проявляються на всіх рівнях публічного адміністрування (державному, галузевому, регіональному, місцевому тощо). Наявні проблеми тісно пов'язані між собою і можуть бути вирішені тільки в рамках комплексного підходу.

2.3. Форми та методи публічного адміністрування захисту персональних даних

У контексті аналізу ключових аспектів організаційно-правового механізму захисту персональних даних особливої ваги набувають питання про форми та методи його функціонування. На відміну від організаційних і правових ланок цього механізму, які утворюють його статичний каркас, форми та методи адміністрування втілюють динаміку його роботи, репрезентуючи фактичний бік адміністративного впливу на сферу захисту персональних даних. Цілком очевидно, що без з'ясування характеру такого впливу всебічне уявлення про механізм публічного адміністрування захисту персональних даних (як феномен, що існує, а не суто теоретичну конструкцію) побудувати неможливо. Видатний російський правник С. Алексєєв наголошує: «Будь-яке дослідження організаційно-правових

систем, незалежно від глибини аналітичного опрацювання, буде неповним без ретельного вивчення форм і методів їх практичної взаємодії із суспільним середовищем. Розглядати їх (системи) у відриві від процесу функціонування – все одно, що вивчати право поза фактичними відносинами, які складаються між людьми: і некоректно, і безперспективно» [192, с. 79].

Та перш ніж перейти до безпосереднього розгляду форм і методів публічного адміністрування сфери захисту персональних даних, необхідно визначитися зі змістом названих понять. Хоч як парадоксально, але попри широке висвітлення форм і методів публічного адміністрування на сторінках юридичних видань (нині без нього не обходиться жоден підручник з адміністративного права), сучасна правова наука досі на виробила єдиного погляду на їх природу, типологію та зміст.

Наприклад, І. Пастух розуміє під формами публічного адміністрування «зовнішньо виражену дію суб'єктів публічної адміністрації, що здійснюється в рамках їх компетенції для виконання поставлених перед ними завдань та має певні наслідки» [193, с. 181]. Класифікуючи їх «за ступенем правової регламентації», цей вчений виокремлює такі форми публічного адміністрування: встановлення норм права (видання нормативних актів), застосування норм права, укладання адміністративних договорів, здійснення реєстраційних та інших юридично значущих дій, провадження матеріально-технічних дій та виконання матеріально-технічних операцій» [193, с. 181].

На думку В. Дзюндзюка, Н. Мельтюхової та Н. Фоміцької, форма публічного адміністрування – це уніфікований за зовнішніми ознаками, формалізований вид результатів конкретних дій органу управління, його структурних підрозділів та службових осіб, спрямованих на досягнення поставленої мети. Як основні форми публічного названі автори розглядають: нормативно-правові (становлення норм права); застосування норм права; організаційне регламентування внутрішньої роботи апарату органів влади; позаапаратну організаційну діяльність; матеріально-технічне забезпечення [187, с. 98].

Т. Гуржій визначає форми публічного адміністрування як регламентовані правом види і способи реалізації органами (посадовими особами) публічної адміністрації наданих їм повноважень. При цьому основними формами публічного адміністрування пропонує вважати такі: 1) видання адміністративно-правових актів; 2) укладання адміністративних договорів; 3) надання адміністративних послуг та здійснення інших юридично значущих дій [188, с. 115, 116].

Аналогічна розбіжність думок спостерігається і стосовно методів публічного адміністрування. Зокрема, одні вчені розуміють під ними «сукупність універсальних та спеціальних способів і прийомів, які застосовують органи влади під час здійснення тих чи інших функцій державного управління або в процесі розроблення, прийняття та реалізації рішень щодо впливу на керовані об'єкти» [194, с. 102]. Другі розглядають їх як «засоби та способи здійснення функцій суб'єкта публічної адміністрації, впливу суб'єктів публічної адміністрації на об'єкти публічної діяльності» [189, с. 178]. Треті вбачають у них «певні способи практичного виконання суб'єктами публічної адміністрації їхніх адміністративних зобов'язань, що відповідають характеру та обсягу наданої їм компетенції» [76, с. 227]. З точки зору четвертих, ними є «прийоми безпосереднього й цілеспрямованого впливу виконавчих органів (посадових осіб) на підставі закріпленої за ними компетенції, у встановлених межах і відповідній формі на підпорядковані їм органи та громадян» [190, с. 155].

Не вдаючись до глибокого аналізу наведених уявлень про форми і методи публічного адміністрування (з нашої точки зору, вони мають стати предметом окремого капітального дослідження), можемо констатувати, що багато з них небездоганні як з точки зору логіки побудови, так і відповідності реаліям сучасного адміністрування. Зважаючи на це, пропонуємо виходити з таких концептуальних положень:

1) згідно з європейською доктриною права, публічна адміністрація являє собою сукупність усіх фізичних і юридичних осіб (включаючи державу, місцеве самоврядування, незалежні публічні інститути тощо), на яких покладено здійснення офіційних владних повноважень. Це означає, що форми та методи публічного адміністрування не можна розглядати як властивість виключно державних органів, органів управління, чи то пак виконавчих органів влади. Ними оперує все розмаїття суб'єктів публічної адміністрації незалежно від статусу та форм існування;

2) у сучасній Україні відбулося глибоке переосмислення сутності адміністративно-правових відносин. Нині це не тільки відносини між керуючим та підпорядкованим суб'єктами. Значною мірою це відносини між рівноправними партнерами, які на основі поєднання загальних та індивідуальних інтересів добровільно беруть на себе роль розпорядника і виконавця [195, с. 10, 144]. Отож говорячи про форми або методи публічного адміністрування, було б неправильно вбачати в них вплив публічної адміністрації на *керовані* об'єкти, *підпорядковані* органи, а тим більше на громадян. Публічна адміністрація, суспільні та громадські інститути, юридичні особи приватного права, фізичні особи є рівними та не перебувають у відносинах субординації. На наш погляд, ця обставина має знайти відображення у відповідних визначеннях та класифікаціях;

3) виходячи із загальнофілософського розуміння форми (з точки зору матеріалістичної філософії, це «внутрішня структура і зовнішній вираз чогось» [191, с. 161]), форму публічного адміністрування слід розглядати як спосіб організації (втілення, вираження) цього процесу, а не як його кінцевий результат. Аналогічно до того, як нормотворчість не можна ототожнювати з нормативно-правовими актами, публічне адміністрування (як діяльність і процес) не можна іменувати «формалізованим видом результатів», «наслідками впливу» абощо;

4) будь-яка свідома діяльність, а тим більше діяльність суб'єктів владних повноважень завжди цілеспрямована. Кожен суб'єкт публічної адміністрації покликаний реалізовувати певний спектр завдань, визначених законодавством та зумовлених загальними цілями публічного адміністрування. Немає і не може бути суб'єкта, який би як носій адміністративних повноважень провадив відповідний напрям діяльності без конкретної мети, без прагнення суспільно бажаного результату. З огляду на це будь-які вказівки, що форми і методи публічного адміністрування спрямовані на досягнення поставленої мети, видаються зайвими. Куди важливіше підкреслити, що і перші, й другі повинна реалізовувати публічна адміністрація в межах закону та наданих повноважень. Адже вітчизняна історія публічного адміністрування знає чимало прикладів, коли суб'єкти владних повноважень виходили за ці межі, порушуючи право та ігноруючи закон. Поза будь-яким сумнівом, такі випадки слід суворо відмежовувати від правових форм і методів діяльності публічної адміністрації;

5) отже, публічне адміністрування як системний і послідовний процес завжди спрямоване на певну мету. Однак далеко не кожен елемент цього процесу (стадія, етап, дія, акт) має конкретні осяжні наслідки. Ідеться не лише про наслідки юридичного характеру – загальновідомо, що окремі форми публічного адміністрування (як-то здійснення матеріально-технічних дій, виконання матеріально-технічних операцій) таких наслідків не можуть мати в принципі. Ідеться про будь-які матеріальні наслідки взагалом: соціальні, економічні, технічні тощо. Так, не завжди нормотворчий процес завершується ухваленням нормативно-правового акта, не завжди порушення адміністративної справи має наслідком притягнення особи до відповідальності тощо. Проте у всіх подібних випадках можемо констатувати реалізацію певних форм і методів публічного адміністрування. І оскільки не всі форми та методи публічного адміністрування характеризуються обов'язковими наслідками, цю ознаку не можна вводити до змісту відповідних понять;

6) з наведеного вище висновку випливає, що перелік форм публічного адміністрування не вичерпується формами, здатними мати конкретні юридичні наслідки. Такі форми, як вчинення матеріально-технічних дій, виконання матеріально-технічних операцій та здійснення інших внутрішньоорганізаційних заходів часто не спричиняють наслідків правового характеру, однак не перестають бути зовнішнім вираженням публічного адміністрування. Діяльність публічної адміністрації багатовекторна. Вона скеровується не тільки на зовнішні об'єкти, а й усередину адміністративної системи, маючи на меті забезпечення ефективної роботи всіх її ланок і складових. Ігнорувати цей напрям діяльності, виносити його поза межі публічного адміністрування, не вважати його формою адміністрування – означає однобоке сприйняття публічної адміністрації як системи, не здатної до саморегулювання та саморозвитку. У зв'язку з цим видається спірною думка вчених, які не вводять внутрішньоорганізаційні дії до переліку форм публічного адміністрування.

На підставі викладених міркувань під *формами публічного адміністрування сфери захисту персональних даних* пропонуємо розуміти зовнішній (формалізований) вираз діяльності публічної адміністрації, здійснюваної на підставі закону та в межах наданої компетенції, щодо захисту прав людини (зокрема права на невтручання в особисте життя) у зв'язку з обробкою персональних даних.

Методи публічного адміністрування сфери захисту персональних даних доцільно визначити як прийоми та способи реалізації завдань, функцій і повноважень публічної адміністрації у сфері обробки та захисту персональних даних.

Аналіз практичних аспектів діяльності публічної адміністрації у сфері захисту персональних дає змогу констатувати широке використання всіх форм і методів публічного адміністрування. Однак зупинимося на розгляді лише тих з них, котрі превалюють в інституціональному адмініструванні та характеризують провідні напрями його здійснення.

Із 2010 року в Україні невпинно розширюється нормативно-правова база регулювання захисту персональних даних. За цей час на рівні центральних органів виконавчої влади ухвалено понад 50 нормативно-правових актів з питань обробки персональних даних. Фактично в усіх місцевих державних адміністраціях та виконкомах місцевих рад затверджено нормативні регламенти обробки персональних даних, чинність яких поширюється також на підпорядковані їм структури (заклади, установи, підприємства тощо).

З позитивного боку слід відзначити нормотворчу діяльність ДСУЗПД, яка протягом І півріччя 2014 року опрацювала три проекти законів України, чотири проекти указів Президента, шість проектів постанов Кабінету Міністрів, сім проектів наказів міністерств та інших центральних органів виконавчої влади. Зазначені проекти стосувалися питань захисту персональних даних щодо регіонального розвитку, будівництва та житлово-комунального господарства, аграрної політики та продовольства, адміністративних послуг та фіскальної політики, міграційної політики, освіти і науки, соціальної політики, електронної комерції та інших.

На виконання рішення РНБО України «Про заходи щодо удосконалення, формування та реалізації державної політики в сфері інформаційної безпеки України», введеного в дію Указом Президента від 1 травня 2014 року № 449, ДСУЗПД взяла участь у підготовці проектів Стратегії забезпечення кібернетичної безпеки України, Стратегії розвитку інформаційного простору України, а також у розробленні комплексу змін до Доктрини інформаційної безпеки України. Крім того, в 2014 році фахівці ДСУЗПД завершили розроблення національного стандарту «Інформаційні технології. Методи захисту. Основні положення щодо забезпечення невтручання в особисте життя (ISO/IEC 29100:2011, MOD)», який створює базу для забезпечення відповідності управлінських процесів в організаціях та на підприємствах вимогам захисту персональних даних [192].

Попри загальні позитивні тенденції, нормотворча діяльність у сфері захисту персональних даних супроводжується рядом проблемами, котрі істотно знижують її якість та ефективність. Це зокрема такі:

недосконала техніка нормотворення (як наслідок, чимало нормативних положень характеризуються неоднозначністю, неповнотою та суперечностями змісту);

безсистемне оновлення нормативно-правової бази (нормативно-правові зміни вносять асинхронно, адаптація підзаконних нормативно-правових актів до новел законодавства відбувається з великими затримками в часі);

повільні темпи розроблення низки важливих нормативно-правових актів з питань захисту персональних даних (наприклад, Порядок здійснення ДСУЗПД державного контролю за додержанням законодавства про захист персональних даних побачив світ 26 червня 2012-го, тобто через півтора року після фактичного заснування ДСУПЗД) [193].

Ці та інші проблеми інституціональної нормотворчості детально висвітлені в інших підрозділах монографії (підрозділи 2.1, 3.1, 3.3), тож наразі обмежимося констатацією необхідності їх якнайшвидшого розв'язання в межах комплексного підходу, який би охоплював усі рівні нормативно-правової регламентації – від локального (місцевого) до загальнодержавного.

Ще одна форма публічного адміністрування – застосування правових норм – у сфері захисту персональних даних реалізується переважно через методи нагляду (зокрема систематизації відомостей про бази персональних даних), контролю (виїзні та безвиїзні перевірки), запобігання та припинення правопорушень (складання відповідних письмових приписів), юридичної відповідальності (адміністративної, дисциплінарної тощо).

Протягом 2012–2013 років уповноважені суб'єкти публічної адміністрації здійснили 219 перевірок стану додержання вимог законодавства про захист персональних даних, з них 77 планових та 142 позапланових.

У 2013 році об'єктами таких перевірок були: органи державної влади, органи місцевого самоврядування, підприємства, установи та організації державної форми власності – 44; підприємства, установи та організації житлово-комунального господарства – 41; суб'єкти приватного права – 45; компанії, які здійснюють обробку персональних даних з використанням веб-ресурсів, – 24; банківські та фінансові установи – 29; страхові компанії – 4.

Проведені контрольні заходи засвідчили, що найпоширеніші порушення законодавства про захист персональних даних такі:

неналежне оформлення договірних відносин між володільцем та розпорядником персональних даних (часто письмових договорів між ними немає);

перевищення розпорядником обсягів обробки персональних даних, визначених у договорі з їх володільцем, обробка персональних даних з іншою метою;

мета обробки персональних даних, задекларована у внутрішніх документах їх володільця або розпорядника, не відповідає меті, вказаній у документах, які подають на розгляд уповноважених суб'єктів контролю;

невідповідність складу персональних даних, що обробляються, встановленим цілям їх обробки;

обробка персональних даних без належних підстав;

незаконне поширення персональних даних;

неповідомлення особи про зміни в обробці пов'язаних з нею персональних даних (про зміну володільця персональних даних, складу та змісту зібраних персональних даних, мети їх збирання та осіб, яким їх передають);

надання доступу до персональних даних третім особам з порушенням вимог чинного законодавства;

невиконання вимоги щодо створення структурного підрозділу (визначення відповідальної особи), що організовує роботу, пов'язану із захистом персональних даних під час їх обробки;

невизначеність внутрішнього порядку обробки та захисту персональних даних;

неналежний захист приміщень, де зберігаються бази персональних даних.

За результатами проведених перевірок складено 219 актів, 140 приписів щодо усунення виявлених порушень, 10 протоколів про адміністративні правопорушення, накладено штрафних санкцій на суму 6,8 тис. гривень [194; 195].

Загалом аналіз правозастосовної діяльності у сфері захисту персональних даних дає підстави для таких висновків.

По-перше, ця форма інституціонального адміністрування знаходить реалізацію переважно в примусових методах (наглядових, контрольних, юрисдикційних тощо), орієнтованих на боротьбу з порушеннями законодавства про захист персональних даних. Натомість так званим позитивним методам адміністративного впливу (інформування, переконання, заохочення тощо) відведено другорядну роль. З нашої точки зору, такий недогляд не тільки не сприяє гармонізації відповідної сфери суспільних відносин, а й істотно гальмує процеси її розвитку. Адже попри всю важливість примусових методів, ефективність їх застосування вельми обмежена. Вони реакція на негативні процеси, які вже тривають. Протидіяти таким процесам надзвичайно важливо, але ще важливіше запобігти їм, виробивши в суспільній свідомості чітку установку на додержання законності, підвищення правової культури, розвиток соціальної відповідальності. Зважаючи на це примус має поєднуватися з позитивними методами адміністрування, виступати їх логічним продовженням, коли вони не дали позитивного результату. Заходи непримусового характеру (пропагандистські, роз'яснювальні, виховні, навчальні та інші) мають посісти належне місце серед методів адміністрування захисту персональних даних.

По-друге, загальна ефективність правозастосування у сфері захисту персональних даних невисока. Навіть примусові методи, які становлять ядро правозастосовного

інструментарію, реалізуються недостатньо широко та не дають масштабних результатів. Наочне свідчення цього – слабка щільність адміністративного контролю (упродовж 2013 року в Україні було зареєстровано майже 4 тис. баз персональних даних і проведено лише 187 перевірок стану їх функціонування, більшість із яких мали безвиїзний характер), зростання деліктності у сфері захисту персональних даних та водночас висока латентність відповідних правопорушень (за загальним визнанням володільців персональних даних та суб'єктів адміністративного контролю, реальна кількість правопорушень у цій сфері значно перевищує офіційні показники), непоодинокі випадки повторного вчинення правопорушень суб'єктами, яких уже притягували до юридичної відповідальності.

Серед основних причин такого невтішного стану справ: низький рівень кадрового та матеріально-правового забезпечення суб'єктів інституціонального контролю, зокрема секретаріату уповноваженого Верховної Ради України з прав людини; нестача дієвої координації в системі публічного адміністрування захисту персональних даних; дублювання повноважень окремих представників цієї системи; брак методик виявлення, кваліфікації та процесуального оформлення правопорушень. Усунення цих чинників має стати першочерговим завданням державної політики захисту персональних даних. Із цією метою доцільно закріпити комплекс відповідних заходів (правових, організаційних, інформаційних, матеріально-технічних тощо) на рівні державної цільової програми захисту персональних даних.

Торкаючись такої форми публічного адміністрування, як укладення адміністративних договорів, варто зазначити, що у сфері захисту персональних даних вона застосовується вельми обмежено. Більшість угод у цій сфері (зокрема, між володільцями і розпорядниками персональних даних) мають приватно-правовий характер: їх укладають з ініціативи сторін, а не на вимогу законодавства; не вимагають обов'язкової участі суб'єкта публічної адміністрації; не передбачають обмеження волі сторін

(в тому числі свободи вибору контрагента); не мають публічних інтересів тощо. Можливо, саме тому сучасні науковці майже ніколи не розглядають питання адміністративно-договірних відносин у контексті захисту персональних даних. У вітчизняній юридичній літературі навряд чи знайдеться бодай одне капітальне дослідження, яке хоч побіжно стосувалося відповідної проблематики.

Однак цей дефіцит уваги важко визнати закономірним. На сьогодні є всі підстави констатувати практику укладення адміністративних договорів у сфері захисту персональних даних.

Так, на підставі Закону України «Про Державний реєстр виборців» (ст. 24), політичні партії, що мають фракцію у поточному скликанні Верховної Ради, або входять до складу виборчого блоку, який має таку фракцію, має право брати участь у здійсненні публічного контролю за веденням Державного реєстру виборців.

З цією метою раз на рік, а також не пізніше як за 60 днів до дня голосування на виборах Президента, виборах народних депутатів України, всеукраїнському референдумі, чергових місцевих виборах за письмовим зверненням політичної партії розпорядник реєстру (Центральна виборча комісія) подає представникові цієї партії засвідчену цифровим підписом електронну копію бази даних реєстру [126].

Електронну копію бази даних реєстру передають разом з програмою для її перегляду, інструкцією з користування нею, запечатаним конвертом з персональним ідентифікаційним номером і персональним кодом розблокування, а також носієм ключової інформації (матеріальний носій інформації, призначений для запису та збереження ключів доступу). При цьому передача носія ключової інформації здійснюється *за договором* встановленої форми відповідно до Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації, затвердженого наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 20 липня 2007 року № 141 [196].

За всіма ключовими ознаками цей тип договорів належить до числа адміністративних. Його обов'язковими (і єдино можливими) суб'єктами виступають орган державної влади (ЦВК) та політична партія, представлена у Верховній Раді. Його предмет та основні умови заздалегідь визначені законодавством. Його укладають в рамках публічного контролю, він не має на меті отримання комерційного прибутку чи задоволення іншого приватного інтересу.

Таким чином, наявність адміністративно-договірної практики у сфері захисту персональних даних не викликає жодних сумнівів. Цілком очевидно, що попри свої відносно скромні масштаби, вона стосується надзвичайно важливої царини публічної діяльності – виборчого процесу і відіграє значущу роль в механізмі формування представницьких органів влади.

Це зумовлює доцільність визнання адміністративних договорів однією з форм публічного адміністрування сфери захисту персональних даних, а також необхідність їх предметного розгляду як у рамках спеціальних наукових досліджень, так і в ході викладання інформаційно-правових дисциплін.

Підсумовуючи цю частину дослідження, маємо визнати, що реалізація провідних форм і методів адміністрування сфери захисту персональних відбувається з численними збоями. Вади нормативно-правового регулювання, невисокий рівень організації, брак кваліфікованих кадрів, дефіцит матеріальних ресурсів – всі ці чинники мають деструктивний вплив не тільки на систему захисту персональних даних, а й на стан інформаційної безпеки загалом.

Зважаючи на це, постає гостра потреба у вдосконаленні адміністративно-правових форм і методів захисту персональних даних. Вони мають отримати вичерпну, детальну та узгоджену правову регламентацію. Найшвидше потрібно гармонізувати нормативно-правову базу, оптимізувати інституціональне нормотворення, здійснити перегляд інформаційного законодавства на предмет актуальності, узгодженості, повноти регулювання та відповідності запитам практики.

Межі компетенції, повноваження та сфери відповідальності всіх суб'єктів інституціонального адміністрування повинні бути чітко розмежовані. Їх діяльність має ґрунтуватися на засадах плановості, послідовності, міжгалузевої й міжрегіональної координації. Водночас кожному з них потрібно створити умови для максимально ефективного здійснення адміністративних функцій. У деяких випадках це передбачає оптимізацію їх структури, зміни в штатному розписі, а також в обсягах бюджетного фінансування та характері матеріально-технічного забезпечення.

В арсеналі методів публічного адміністрування сфери захисту персональних даних належне місце мають посісти методи позитивного (непримусового) характеру: інформаційні, роз'яснювальні, виховні тощо. Ця вимога підлягає обов'язковому врахуванню під час розроблення державних цільових програм з інформаційної безпеки.

Вважаємо, що тільки за цих умов можна розраховувати на збільшення ефективності адміністрування захисту персональних даних. Тільки так його форми та методи розвиватимуться у прогресивному руслі, отримають надійний механізм реалізації і забезпечать нові можливості для успішної реалізації завдань державної інформаційної політики.

***

Як засвідчив проведений аналіз, вітчизняна система правового та організаційного забезпечення захисту персональних даних нині перебуває у фазі активного розвитку. Протягом останніх років відбувається кардинальне оновлення тематичного законодавства, реформується система інституціонального контролю, оптимізуються механізми обробки персональних даних, посилюються вимоги щодо її захисту, впроваджуються нові форми та методи адміністрування, здійснюється пошук оптимального співвідношення між гарантіями права на доступ до інформації та права суб'єктів на конфіденційність приватного життя.

Водночас на тлі загальних позитивних тенденцій мусимо констатувати широкий комплекс проблем, які проявляються на всіх рівнях нормативно-правового регулювання та правозастовної діяльності. Це зокрема і неузгодженість нормативно-правових актів, і недоліки їх структури та змісту, і недостатній рівень їх регуляторного охоплення, і розбалансованість системи публічного адміністрування, і дефіцит кадрових ресурсів, і відсутність цільових програм розвитку, і обмежена сфера використання позитивних (непримусових) адміністративних методів, і багато інших.

Окреслені проблеми помітно знижують ефективність державної політики захисту персональних даних, роблять її непослідовною та вразливою до негативних впливів. Їх розв'язання потребує комплексного підходу, який охоплював би ключові аспекти публічного адміністрування обробки та захисту персональних даних. У рамках цього підходу доцільно:

1) здійснити докорінний перегляд інформаційного законодавства в частині регламентації питань захисту персональних даних з метою виявлення та усунення наявних прогалин, колізій, дублювань і неточностей; внести до нормативно-правових актів з питань захисту персональних даних комплекс змін, спрямованих на гармонізацію їх системи, вдосконалення їх структури та змісту, імплементацію міжнародних правових стандартів; розглянути питання про скасування/оновлення нормативно-правових актів (їх окремих положень), деактуалізованих внаслідок законодавчих, організаційних та інших перетворень у сфері захисту персональних даних; запровадити постійний моніторинг законодавства про захист персональних даних, забезпечити узгоджене оновлення всіх його складових; посилити контроль за якістю нормотворення та ефективністю правозастосування у сфері захисту персональних даних;

2) ухвалити державну цільову програму, покликану забезпечити комплексну реалізацію політики захисту персональних даних на загальнодержавному, міжгалузевому/ галузевому та місцевому рівнях; забезпечити чітке розмежування

функцій і повноважень суб'єктів публічного адміністрування сфери захисту персональних даних; завершити юридичне оформлення ліквідації ДСУПЗПД, зокрема скасувати Положення про ДСУПЗПД, затверджене указом Президента України від 06.04.2011 року № 390; вилучити зі змісту Положення про Міністерство юстиції України, затвердженого постановою Кабінету Міністрів від 2 липня 2014 року № 228, норми про покладення на міністра юстиції України функцій спрямування та координації діяльності ДСУПЗПД;

3) постійно вдосконалювати форми і методи публічного адміністрування захисту персональних даних, забезпечити їх вичерпну нормативно-правову регламентацію, створити належні умови (правові, організаційні, економічні, технічні та ін.) для підвищення їх ефективності; розширювати сферу застосування позитивних методів адміністративного впливу, покласти в основу інституціонального адміністрування правовиховні, роз'яснювальні та інші методи непримусового характеру.

РОЗДІЛ 3. ДЕРЖАВНИЙ ПРИМУС ЯК ІНСТРУМЕНТ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

3.1. Профілактика правопорушень у сфері захисту персональних даних

Демократичний розвиток суспільства та супутні тенденції щодо зміцнення законності й зростання правосвідомості громадян обумовлюють пріоритизацію так званих позитивних методів правового впливу на інформаційні відносини. Такі методи (заохочення, переконання тощо) передбачають невимушене гармонійне узгодження індивідуальних і публічних інтересів в інформаційній сфері. Вони не обмежують волю учасників правовідносин, забезпечуючи захист інформаційних прав і свобод шляхом формування в людській свідомості твердих установок на дотримання вимог законодавства, неприпустимість правопорушень, повагу до права на конфіденційність приватного життя.

Та, на жаль, досягти гармонійного поєднання особистих і суспільних інтересів тільки за рахунок позитивних методів вдається не завжди. Часто ці методи не спрацьовують належно і не у всіх випадках детермінують людську поведінку, скеровуючи її в русло суспільного блага. На практиці трапляється багато ситуацій, коли позитивні методи не дають очікуваного результату, а конфлікт між суспільними і власними інтересами людина врегульовує на користь останніх.

У таких ситуаціях захист інформаційних відносин потребує діаметрально протилежного підходу, за якого поведінка людини гармонізується із суспільними стандартами примусовим шляхом. Примусові методи мають виражений авторитарний характер. Вони ґрунтуються на приматі державної волі та не передбачають свободи вибору, зобов'язуючи (а деколи змушуючи) суб'єкта діяти у спосіб, визначений державою.

Однак попри всю авторитарність примусових методів, жодна галузь суспільних відносин не впорядковується без їх

застосування. І це закономірно. Адже немає і не може бути такої життєвої сфери, де б прагнення окремого суб'єкта завжди збігалися з інтересами суспільства, де б не виникали конфлікти інтересів, і кожен неухильно слідував праву.

Сфера обробки та захисту персональних даних – не виняток. Щороку в ній фіксують десятки правопорушень: адміністративних проступків, цивільних деліктів та кримінальних злочинів. І це лише видима частина айсберга. Нині для їх виявлення задіяно настільки малий технічний і кадровий ресурс, що основна маса інформаційних порушень непоміченими проходить крізь сито державного обліку.

«Незважаючи на усвідомлення проблеми захисту персональних даних як з боку держави, так і з боку недержавних організацій, – пише О. Ігнатов, – у цій сфері вчиняються дедалі більше порушень, котрі заподіюють величезну соціальну та економічну шкоду. Відсутність гучних справ є наслідком високої латентності протиправних діянь, а не свідченням їх малої кількості. Порушення законодавства про захист персональних даних – це масштабне явище, яке не здолати без всебічної державної підтримки» [197, с. 58]. «Порушення вимог щодо обробки та захисту персональних даних належить до деліктів з найвищим рівнем латентності. Забезпечення їх своєчасного виявлення та припинення є важливим напрямом реалізації державної інформаційної політики», – резюмує Р. Амєлін [198, с. 34, 35].

Висхідна динаміка деліктності, високий рівень латентності інформаційних деліктів, складність відновлення порушених ними прав та інтересів – усі ці чинники зумовлюють необхідність широкого застосування примусових заходів забезпечення законності у сфері захисту персональних даних. І безумовно, провідна роль у цьому процесі відводиться заходам запобігання (профілактики) правопорушенням, які мають дуже важливі цілі, а саме: недопущення протиправної поведінки конкретних осіб; запобігання різним видам правопорушень; виявлення правопорушень; ліквідація умов та причин, що сприяють їх вчиненню; відвернення різноманітних загроз для суспільних відносин, а також прав, свобод та інтересів їх учасників.

Як відомо, запобігти суспільно шкідливим явищам набагато легше, ніж потім ліквідовувати їх негативні наслідки. З огляду на це застосуванню заходів запобігання слід приділяти особливу увагу [188, с. 93]. Передусім саме вони дозволяють передбачити, виявити та не допустити потенційно небезпечну ситуацію із застосування мінімального обсягу примусу. Вони дають змогу ліквідувати таку ситуацію в зародку або й взагалі унеможливити її виникнення. Варто погодитися з С. Стефанишиною, на думку якої, з-поміж усіх примусових заходів, спрямованих на захист персональних даних, найбільш дієвими, ефективними та раціональними виявляються заходи запобігання, що, з одного боку, не передбачають жорсткого репресивного впливу, а з іншого – здатні приносити максимальне позитивний результат, гарантуючи безпеку права приватності та стабільне функціонування інформаційних відносин [199, с. 27].

Сфера захисту персональних даних передбачає нерозривний зв'язок людини і техніки, безперервну взаємодію соціального й технічного елементів. У зв'язку з цим її доцільно розглядати як сукупність кількох підсистем, відмінних за природою, але об'єднаних спільною метою: 1) техніко-технологічної підсистеми обробки персональних даних; 2) підсистеми організації обробки та захисту персональних даних; 3) підсистеми публічного адміністрування обробки та захисту персональних даних.

У площині саме цих підсистем формуються об'єктивні умови та чинники, які сприяють порушенням законодавства про захист персональних даних: недосконаліть програмно-технічного забезпечення з точки зору захищеності від несанкціонованого доступу до електронних баз даних; численні вади правового регулювання; низький рівень правосвідомості суб'єктів обробки персональних даних; недосконаліть механізмів контролю у сфері обробки та захисту персональних даних, дублювання функцій і повноважень контролюючих структур; недостатність кадрового, матеріального й технічного забезпечення системи адміністрування захисту персональних даних; неефективність цільових програм розвитку тощо.

Детермінанти деліктності у сфері захисту персональних даних можуть бути пов'язані з діяльністю уповноважених суб'єктів публічного контролю. Їх продукують поведінка володільців та розпорядників персональних даних, а також третіх осіб, яким передають дані. Багато в чому їх обумовлюють дії (бездіяльність) операторів електронних баз даних та осіб, відповідальних за їх технічний стан і безпеку. Вони безпосередньо залежать від якості програмного забезпечення, організації режиму конфіденційності та багатьох інших організаційних, правових і технічних чинників.

Цілком очевидно, що для ефективної протидії настільки широкому розмаїттю негативних чинників потрібно застосовувати не менш різноманітний комплекс профілактичних заходів, спрямованих на вдосконалення засобів обробки персональних даних, підвищення правосвідомості суб'єктів інформаційних відносин, розвиток системи інституційного адміністрування (зокрема планування та програмування профілактичних заходів), оптимізацію нормативно-правового регулювання тощо.

Останнім часом за цим напрямом докладають чимало зусиль.

Профілактика порушень законодавства про захист персональних даних становить основу державних цільових програм і концепцій.

Наприклад, Концепція створення єдиної інформаційно-аналітичної системи управління міграційними процесами (затверджена розпорядженням Кабінету Міністрів України від 7 листопада 2012 р. № 870-р) передбачає запровадження організаційних і технічних заходів, спрямованих на забезпечення захисту персональних даних про громадян України, іноземців та осіб без громадянства, які на законних підставах перебувають на території України, а також запровадження інформаційної (автоматизованої) системи обліку та аналізу міграційних процесів із забезпеченням конституційних гарантій щодо недопущення поширення конфіденційної інформації про особу без її згоди [200]. Концепція створення

та функціонування інформаційної системи електронної взаємодії державних електронних інформаційних ресурсів (розпорядження Кабінету Міністрів України від 5 вересня 2012 р. № 634-р) ґрунтується на засадах забезпечення захисту персональних даних та державних електронних інформаційних ресурсів; підвищення відповідальності державних органів за формування і збереження державних електронних інформаційних ресурсів; забезпечення прозорості та відкритості діяльності державних органів у сфері обробки персональних даних [201].

Хоч і повільно, але змінюється інституційна система контролю за дотриманням законодавства про захист персональних даних. Етапною віхою її розбудови стало покладення контролюючих функцій на не залежну від державних органів структуру – секретаріат уповноваженого Верховної Ради України з прав людини. Цей крок дав змогу не тільки наблизитися до європейських зразків адміністрування захисту персональних даних, а й істотно поліпшити стан дотримання законності в інформаційній сфері. В умовах появи незалежного (не інтегрованого в систему державної влади) суб'єкта контролю державні органи, які здійснюють обробку персональних даних, фактично втратили можливість впливати на юрисдикційні рішення, приховувати факти порушень, зволікати з їх припиненням та усуненням їх шкідливих наслідків.

Паралельно триває розвиток інституціонального законодавства. Із 2010 року в Україні ухвалено законодавчі акти, якими з-поміж інших питань визначаються засади профілактики деліктності у сфері захисту персональних даних. У цьому контексті на особливу увагу заслуговують закони України «Про захист персональних даних» (2010) [90], «Про ратифікацію Страсбурзької Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних» [89], «Про внесення змін до деяких законодавчих актів України щодо посилення відповідальності за порушення законодавства про захист персональних даних» (2011) [202], «Про внесення змін до деяких законодавчих актів України

щодо удосконалення системи захисту персональних даних» (2013) [145], «Про внесення змін до деяких законів України щодо діяльності уповноваженого Верховної Ради України з прав людини у сфері захисту персональних даних» (2014) [203].

Дуже динамічно розвивається підзаконний рівень нормативно-правової регламентації. З одного боку, це пояснюється завершенням початкового етапу формування законодавчої бази, що створило плідне підґрунтя для підзаконної нормотворчості. З іншого – зумовлюється кардинальними змінами в системі адміністрування захисту персональних даних та супутніми процесами перерозподілу адміністративних (зокрема контрольних) функцій і повноважень.

Показовим прикладом може слугувати наказ уповноваженого Верховної Ради України з прав людини від 8 січня 2014 року № 1/02-14 «Про затвердження документів у сфері захисту персональних даних», яким затверджено типовий порядок обробки персональних даних, порядок здійснення контролю за додержанням законодавства про захист персональних даних, порядок повідомлення про обробку персональних даних, яка становить особливий ризик для прав і свобод, а також положення про підрозділ чи відповідальну особу, яка організовує роботу, пов’язану із захистом персональних даних під час їх обробки [184]. Ухвалення цього документа пов’язане з передачею контрольних функцій у сфері захисту персональних даних від ДСУЗПД до секретаріату уповноваженого Верховної Ради України з прав людини.

Суттєво активізувалась інформаційно-роз’яснювальна робота стосовно надання рекомендацій зі практичного застосування законодавства про захист персональних даних. Лише упродовж 2013 року в Україні з цією метою було проведено близько 50 тематичних семінарів, конференцій, круглих столів, консультацій за участю органів влади, представників приватного сектору, інститутів громадянського суспільства тощо.

За цей період на провідних вітчизняних телеканалах (ТРК «Київ», «Тоніс», «1+1» та ін.), а також у друкованих засобах масової інформації оприлюднено понад 40 інтерв’ю

з посадовими особами ДСУЗПД і секретаріату уповноваженого. Проведено два виїзних розширених засідання колегії ДСУЗПД у прес-центрах Укрінформу та ЛІГАБізнесІнформу, на яких розглянуто питання особливостей обробки персональних даних з використанням веб-ресурсів [195].

Для забезпечення оперативного розгляду питань, пов'язаних із захистом персональних даних, у секретаріаті уповноваженого функціонує загальна «гаряча» телефонна лінія, а також спеціалізована довідкова телефонна лінія з питань захисту персональних даних. Протягом 2013 р. було проведено 192 тематичні «гарячі» лінії. Під час їх проведення фахівці дали відповіді більш як на 20 тис. запитань, які стосувалися практичних аспектів застосування законодавства про захист персональних даних. З метою надання практичних консультацій дедалі активніше використовуються ресурси електронних соціальних мереж [195].

Формування тематики практичних рекомендацій ґрунтується на аналізі запитань, поставлених фізичними та юридичними особами шляхом надсилання звернень, запитів, під час особистого прийому громадян посадовими особами секретаріату уповноваженого.

Крім того, на офіційному сайті ДСУЗПД *(http://zpd.gov.ua)*, з 2014 року – і на сайті уповноваженого (*ombudsman.gov.ua*) регулярно розміщується інформація про основні вимоги щодо обробки та захисту персональних даних, характер і кількість контрольних перевірок, здійснюваних у цій сфері, виявлені правопорушення, заходи їх припинення, усунення їх шкідливих наслідків.

Профілактичний вплив інформаційних заходів не можна недооцінювати. У сучасних умовах вони справляють істотний вплив на правосвідомість суб'єктів інформаційних відносин, дисциплінуючи їхні, збагачуючи їх правові знання, демонструючи на конкретних прикладах як суспільну небезпеку протиправних діянь, так і невідворотність відповідальності за їх вчинення.

Окремий напрям профілактичної діяльності становить розроблення професійно-етичних норм, які визначають принципи професійної діяльності у сфері обробки персональних даних. Тільки в 2013 р. було погоджено та рекомендовано для впровадження три корпоративних кодекси поведінки, підготовлені професійними об'єднаннями та громадськими організаціями для забезпечення ефективного захисту прав суб'єктів персональних даних, сприяння додержанню законодавства, враховуючи специфіку обробки персональних даних у різних галузях.

Викладене свідчить, що вітчизняна система профілактики правопорушень у сфері захисту персональних даних перебуває на етапі сталого розвитку. Вдосконалюється її правове регулювання, розвивається її інституційний механізм, збагачується функціональний інструментарій. Попри наявність загальних позитивних тенденцій, деякі аспекти функціонування цієї системи дають чимало підстав для критики.

За загальним визнанням, динаміка її розвитку надто повільна, а організаційно-правове, кадрове та інформаційне забезпечення все ще далеке від оптимуму. Численні порушення мають місце фактично у всіх формах та на всіх етапах обробки персональних даних. Як показує статистика, їх кількість збільшується з року в рік, що свідчить про недостатню ефективність заходів протидії деліктності загалом та заходів профілактики зокрема.

Значною мірою недостатня ефективність профілактики порушень законодавства про захист персональних даних зумовлена проблемами правового та організаційного забезпечення.

Незважаючи на постійне розширення нормативно-правової бази, яке слугує важливим чинником запобігання деліктності в інформаційній сфері, практичні аспекти профілактики правопорушень залишаються майже неврегульованими. Жоден законодавчий акт не визначає цілей такої профілактики, не окреслює її напрямів, не визначає кола її суб'єктів, не конкретизує форм та методів її здійснення. Чи

не єдиний виняток становить п. 5 ч. 1 ст. 28 Закону України «Про захист персональних даних», згідно з яким уповноважений Верховної Ради України з прав людини за підсумками перевірки або розгляду звернень може видавати обов'язкові для виконання вимоги (приписи) щодо запобігання та припинення порушень законодавства про захист персональних даних [90]. Однак існування цієї норми – радше виняток, ніж правило. Нею впорядковано лише дещицю колосального масиву питань, пов'язаних з реалізацією профілактичних заходів у сфері обробки та захисту персональних даних. Решта перебуває за межами правової регламентації.

Аналогічна картина спостерігається на рівні підзаконного регулювання. Підзаконні нормативно-правові акти щодо захисту персональних даних (зокрема акти Кабінету Міністрів, Міністерства юстиції, уповноваженого Верховної Ради України з прав людини та ін.) жодним чином не конкретизують питання профілактики інформаційних правопорушень. Більш того, вони «забувають» про ці питання навіть усупереч актам вищої юридичної сили.

Наприклад, чинний Порядок контролю за додержанням законодавства про захист персональних даних, затверджений наказом уповноваженого від 8 січня 2014 року № 1/02-14, передбачає можливість складання уповноваженим тільки одного типу приписів – припису щодо *припинення* порушень законодавства (п. 5.10 порядку) [184]. Як неважко помітити, в даному разі відбувається невиправдане звуження змісту ч. 1 ст. 28 Закону України «Про захист персональних даних», якою передбачена можливість винесення приписів як щодо *припинення*, так і щодо *запобігання* порушенням законодавства про захист персональних даних [90].

Доводиться констатувати, що найважливіші з точки зору профілактики правопорушень у сфері захисту персональних даних пласти суспільних відносин (стратегічне планування, міжінституційна взаємодія, механізми реалізації тощо) врегульовані недостатньо. Багато нагальних організаційних питань узагалі не визначено. Нечіткість і суперечливість змісту відповідних законодавчих положень ускладнює їх правильне розуміння та застосування на практиці.

На рівні державних цільових програм і концепцій заходи профілактики правопорушень у сфері безпеки персональних даних планують неузгоджено та, як правило, у контексті реалізації інших заходів державної інформаційної політики. Здебільшого вони розраховані не на всю сферу обробки персональних даних, а лише на її окремі сектори: обробку персональних даних стосовно міграції, з використанням державних інформаційних ресурсів, фінансовими установами, під час надання комунальних послуг і т.ін. Здебільшого ці заходи не ідентифікуються як профілактичні. Не пов'язані між собою за формою, змістом і строками реалізації, вони не становлять системної єдності, тож заздалегідь позбавлені синергетичного ефекту.

Поряд з недоліками правової регламентації даються взнаки організаційні проблеми в системі публічного адміністрування захисту персональних даних. Із моменту створення ця система зазнала кардинальних змін, внаслідок чого її нинішній абрис дуже далекий від первинного. Якщо в 2011–2013 роках провідним суб'єктом адміністрування захисту персональних даних виступала ДСУЗПД, то з кінця 2013-го майже всі адміністративні (переважно контрольні) функції та повноваження в цій сфері виконує секретаріат уповноваженого Верховної Ради України з прав людини.

З необхідністю такого кроку важко не погодитися. Покладення адміністративних функцій на структуру, не залежну від інших державних органів, – це об'єктивна вимога часу, продиктована міркуваннями всебічного публічного контролю за дотриманням прав людини у сфері захисту персональних даних. Однак як це нерідко трапляється у вітчизняній практиці інституційного реформування, механізм реалізації цих нововведень недосконалий.

Незважаючи на передачу всіх адміністративно-контрольних повноважень від ДСУЗПД до секретаріату уповноваженого, вона існує в незмінному вигляді. Залишається чинним Положення про ДСУЗПД (указ Президента від 6 квітня 2011 року № 390/2011), яке зберігає за службою весь перелік

колишніх повноважень, тобто суперечить Закону України «Про захист персональних даних». При цьому, як уже зазначалося, профілактичні функції обох вказаних структур (і ДСУЗПД, і секретаріату повноваженого) перебувають у стані майже повної невизначеності. Вони не конкретизовані ні на законодавчому, ні на підзаконному рівнях нормативно-правового регулювання.

Дублювання адміністративних функцій, колізійність нормативно-правових актів, якими вони визначені, а також недостатнє кадрове забезпечення їх реалізації – всі ці чинники аж ніяк не сприяють здійсненню послідовної, системної та ефективної протидії деліктності. Саме в організаційно-правовій площині слід шукати витоків більшості проблем, пов'язаних із профілактикою правопорушень у сфері захисту персональних даних.

«Передумови поширення інформаційної деліктності криються не тільки (і не стільки) в технічних вадах чи недоліках роз'яснювальної роботи, – підкреслює А. Возінцев, – врешті-решт технічні й соціальні проблеми можна вирішити шляхом грамотного професійного адміністрування. Однак якщо немає надійного правового підґрунтя, якщо з перебоями функціонують відповідальні структури, кардинально покращити ситуацію неможливо. Організаційно-правові негаразди трансформуються в численні загрози для суб'єктів персональних даних. І якщо їх не усунути, ступінь загроз постійно зростатиме» [204, с. 18].

Слушність цього висновку не підлягає сумніву. Без удосконалення організаційно-правових засад профілактики інформаційної деліктності годі й сподіватися на істотний прогрес у боротьбі з порушеннями законодавства про захист персональних даних. Як свідчить зарубіжний досвід, удосконалення правової регламентації та інституційної системи адміністрування є визначальним чинником і головною передумовою ефективності профілактичних заходів у сфері захисту персональних даних.

На наш погляд, першочерговими кроками за цим напрямом мають стати:

- оптимізація законодавства про захист персональних даних, усунення наявних дублювань, суперечностей і невизначеностей;
- внесення до Закону «Про захист персональних даних» доповнень, спрямованих на забезпечення правової регламентації питань профілактики деліктності у сфері захисту персональних даних. В окремому розділі цього закону мають бути конкретизовані завдання й цілі профілактичної діяльності, основні напрями, форми та методи її здійснення, коло уповноважених суб'єктів та механізми їх системної взаємодії;
- ухвалення державної цільової програми захисту персональних даних (розрахованої на 3–5 років), яка б поряд із конкретними профілактичними заходами містила критерії оцінки їх ефективності та передбачала регулярний контроль за їх виконанням;
- конкретизація повноважень секретаріату уповноваженого Верховної Ради України з прав людини щодо здійснення заходів профілактики правопорушень у сфері захисту персональних даних. Зокрема, в чинному Порядку контролю за додержанням законодавства про захист персональних даних (затверджений наказом уповноваженого від 8 січня 2014 року № 1/02-14) слід передбачити можливість винесення Уповноваженим приписів, спрямованих на запобігання порушенням інформаційного законодавства;
- чіткий розподіл повноважень суб'єктів захисту персональних даних, розмежування ділянок їхньої відповідальності та усунення перетинів компетенції, налагодження міжінституційної взаємодії у сфері профілактики порушень законодавства про захист персональних даних.

3.2. Заходи припинення у сфері захисту персональних даних

Термін «припиняти» багатозначний. Згідно з Академічним словником української мови, має такі значення: «зупиняти рух або розвиток чого-небудь»; «змушувати кого-небудь перестати робити щось»; «скасовувати що-небудь, переривати яку-небудь дію або діяльність» [205, с. 704]. Як неважко помітити, попри деякі змістові відмінності, у всіх випадках припинення розглядається як акт, спрямований на зупинення певного процесу (руху, діяльності, розвитку), що триває в об'єктивній дійсності.

Саме такий характер мають і заходи державного припинення. Як наголошує Т. Гуржій, головне їх призначення полягає в тому, щоб вчасно відреагувати на суспільно небезпечні діяння, зупинити розгортання протиправної поведінки, запобігти настанню її шкідливих наслідків або принаймні мінімізувати їх негативний вплив на суспільні відносини [195, с. 98].

Таким чином, головна функція державного припинення у сфері захисту персональних даних полягає в якнайшвидшому (оперативному) зупиненні правопорушень, які посягають на конфіденційність приватного життя та інформаційну безпеку людини. Реалізацію цієї функції покладено на систему контролю за додержанням законодавства про захист персональних даних, до якої належать суди та уповноважений Верховної Ради України з прав людини.

Аналіз процесуальних повноважень судів загальної юрисдикції свідчить про те, що залежно від спеціалізації у сфері захисту персональних даних вони можуть застосовувати такі заходи припинення:

у порядку адміністративного судочинства – заборона вчиняти певні дії або вжиття інших припиняючих заходів, якщо існує очевидна небезпека заподіяння шкоди правам, свободам та інтересам позивача до ухвалення рішення в адміністративній справі, або захист цих прав, свобод та інтересів

стане неможливим без вжиття таких заходів, або для їх відновлення необхідно буде докласти значних зусиль та витрат, а також якщо очевидними є ознаки протиправності рішення, дії чи бездіяльності суб'єкта владних повноважень (ст. 117 КАС України) [206];

у рамках адміністративно-деліктного провадження – вилучення речей і документів (ст. 265 КУпАП України) [138];

у рамках цивільного провадження – накладення арешту на майно, що належить відповідачеві і знаходиться у нього або в інших осіб; заборона вчиняти певні дії; встановлення обов'язку вчинити певні дії; інші заходи забезпечення (ст. 152 ЦПК України) [207];

у рамках кримінального провадження – тимчасове вилучення майна *(зокрема пристроїв, які використовують для обробки та зберігання електронних баз даних. – А.П.)* (ст. 167 КК України) [208].

Попри очевидні змістові відмінності, перераховані заходи мають спільні ознаки. По-перше, вони реалізуються в ході деліктних проваджень та підпорядковані їх загальній меті. По-друге, мають подвійну мету – недопущення продовження протиправної поведінки та забезпечення об'єктивного розгляду справи про відповідальність за правопорушення у сфері захисту персональних даних. По-третє, виступають заходами процесуального забезпечення, тобто не мають самостійного характеру. По-четверте, на відміну від багатьох інших припиняючих заходів, не спрямовані на виявлення правопорушень (майже у всіх випадках їх застосування відбувається за фактом виявлених протиправних діянь). По-п'яте, їх можна застосовувати за ініціативи не лише суду, а й інших суб'єктів юридичного процесу (потерпілого, позивача тощо).

Заходи судового припинення у сфері захисту персональних даних дуже різноманітні. При цьому основну частку в їхньому масиві становлять організаційні заходи, пов'язані із забороною вчинення певних дій або ж із зобов'язанням

вчинити певні дії. Саме їх найчастіше застосовують суди на практиці, і вони слугують головним інструментом припинення правопорушень у сфері прайвесі.

На відміну від судів, уповноважених застосовувати широкий спектр заходів припинення, уповноважений Верховної Ради України з прав людини має в своєму розпорядженні тільки один такий захід: видання припису про усунення порушень законодавства про захист персональних даних (ст. 23 Закону України «Про захист персональних даних») [90]. Такий припис видає уповноважений на підставі акта перевірки додержання вимог законодавства про захист персональних даних у разі, якщо під час перевірки було виявлено порушення вимог щодо обробки персональних даних в автоматизованих системах або картотеках.

Відповідно до наказу уповноваженого Верховної Ради України з прав людини від 8 січня 2014 року № 1/02-14 «Про затвердження документів у сфері захисту персональних даних», у приписі зазначають: номер, дату і місце складання припису; для суб'єкта перевірки – органу державної влади та місцевого самоврядування: найменування, місцезнаходження; для суб'єкта перевірки – юридичної особи: найменування, місцезнаходження, прізвище, ім'я та по батькові керівника юридичної особи; для суб'єкта перевірки – фізичної особи та/або фізичної особи підприємця: прізвище, ім'я та по батькові, місце її проживання; підстава для видачі припису; заходи, необхідні для усунення порушень, виявлених під час перевірки; строк виконання припису; строк інформування суб'єктом перевірки уповноваженого про усунення виявленого порушення; підпис уповноваженої посадової особи (осіб), яка проводила перевірку [184].

Що ж стосується самих заходів з усунення порушень законодавства про захист персональних даних, то їх орієнтовний перелік наведено у п. 5 ч. 1 ст. 23 Закону України «Про захист персональних даних». До цього переліку входять

такі заходи, як зміна, видалення, знищення, забезпечення доступу до персональних даних, надання чи заборона надання персональних даних третій особі, зупинення обробки персональних даних та припинення їх обробки.

Цей перелік не є вичерпним. Зміст п. 5 ч. 1 ст. 23 Закону України «Про захист персональних даних» сформульовано в спосіб, який допускає можливість застосування й інших, крім вказаних у законі, заходів щодо усунення порушень законодавства про захист персональних даних. Як такі заходи можна застосовувати знеособлення, реєстрацію, перегляд персональних даних, отримання згоди суб'єкта персональних даних на їх обробку зі зміною мети обробки, вимога гармонізувати внутрішньоорганізаційні процедури або акти з вимогами законодавства про захист персональних даних та інші.

Припис стосовно усунення порушень законодавства про захист персональних даних хоч і має обов'язковий характер, але не обмежує адресата у виборі форм його реалізації.

Наочним прикладом може слугувати припис від 13.09.2013 № 125 «Про усунення порушень вимог законодавства у сфері захисту персональних даних», виявлених під час перевірки Державної адміністрації залізничного транспорту України (Укрзалізниця).

Зокрема, п. 1 припису містить вимогу: «забезпечити внесення до проїзних документів прізвища та імені пасажира зі слів особи, яка здійснює оплату проїзного документа, при оформленні у квитковій касі повних та дитячих проїзних документів, без зберігання персональних даних таких пасажирів у базах даних Єдиної автоматизованої системи керування пасажирськими перевезеннями, яка експлуатується ДП «ГІОЦ Укрзалізниця», та в будь-яких інших базах даних» *(підкреслення моє. – А.П.*).

Укрзалізниця у рамках поставленої вимоги здійснила оновлення програмного забезпечення Єдиної автоматизованої системи керування пасажирськими перевезеннями (АСК ПП УЗ), внаслідок чого під час друкування прізвища та імені пасажира у бланку проїзних документів відповідні дані

перестали заносити та зберігати у базі даних АСК ПП УЗ. Програмне забезпечення із внесеними змінами було введено в експлуатацію з 28 листопада 2013 року [209].

Подібно до багатьох інших заходів державного примусу, припинення порушень законодавства про захист персональних даних реалізується за чітко визначеною процедурою, покликаною забезпечити послідовність і впорядкованість юрисдикційної діяльності, об'єктивність і своєчасність розгляду справи, одноманітність правозастосування, всебічне забезпечення прав учасників правовідносин.

Деталі цієї процедури, а також юридичні наслідки її порушення конкретизовані в наказі уповноваженого Верховної Ради України з прав людини від 8 січня 2014 року № 1/02-14 «Про затвердження документів у сфері захисту персональних даних» [184]. Згідно з п.п. 5.12 – 5.17 цього наказу, у разі виявлення порушень інформаційного законодавства під час перевірки суб'єкта обробки персональних даних уповноважена посадова особа складає припис про їх усунення у двох примірниках. Перший примірник не пізніше п'яти робочих днів з дня складання акта перевірки надсилаю суб'єкту перевірки чи уповноваженій ним особі рекомендованим листом з повідомленням про вручення. Другий – зберігається в секретаріаті уповноваженого.

Адресат припису (читай суб'єкт перевірки) повинен протягом зазначеного у приписі строку (не менш ніж 30 календарних днів) вжити заходів щодо усунення порушень, зазначених у приписі, й письмово поінформувати про них уповноваженого разом із наданням копій документів, що це підтверджують.

У разі невиконання припису адресатом щодо нього складає протокол про адміністративне правопорушення, передбачене ст. 188-40 КУпАП «Невиконання законних вимог уповноваженого Верховної Ради України з прав людини» [184].

Аналіз наведених положень змушує констатувати надмірну і, на наш погляд, невиправдану розтягнутість процедури реалізації заходів, спрямованих на припинення порушень законодавства про захист персональних даних.

Як відомо, необхідною умовою ефективності припиняючих заходів є невідкладність їх здійснення. Чим швидше припиняється порушення, тим більше шансів на цілковите відновлення дестабілізованих ним правовідносини, тим вища ймовірність відвернення (мінімізації) його шкідливих наслідків, тим дієвіша система захисту прав та інтересів людини. Саме тому заходи припинення передбачають спрощений (порівняно із заходами юридичної відповідальності) порядок реалізації. І саме тому в основу їх застосування покладено принцип оперативності.

Нині цього не можна сказати про державне припинення у сфері захисту персональних даних. Згідно з процедурою, яка існує, мінімальний строк реалізації відповідних заходів становить 30 (!) календарних днів, та й то за умови невідкладного винесення припису про усунення виявлених порушень. На практиці ж цей строк фактично завжди більший.

У світлі викладеного вище строки винесення та виконання припису уповноваженого про усунення порушень інформаційного законодавства видаються необґрунтованими. Насамперед це стосується строку, відведеного на реалізацію припису адресатом. Парадоксально, але факт: на відміну від більшості правозастосовних процедур, процедура реалізації припиняючих заходів у сфері захисту персональних даних не тільки не спонукає до якнайшвидшого припинення порушень, а навпаки, всіляко його відтерміновує. Саме такий висновок випливає зі змісту п. 5.13 наказу уповноваженого від 8 січня 2014 року № 1/02-14, яким передбачено, що зазначений у приписі строк усунення порушень має бути меншим, ніж 30 календарних днів [184].

Як наслідок, маємо ситуацію, коли виявлене порушення правил обробки та захисту персональних даних замість негайного припинення, триває й надалі, продовжуючи чинити деструктивний вплив на суспільні відносини та створюючи загрозу інформаційним правам людини.

Про причини настільки значного терміну між часом складання припису та часом реалізації передбачених ним заходів можна тільки здогадуватись. Як засвідчили результати опитування посадових осіб секретаріату уповноваженого та ДСУПЗПД (до 2014 року ця служба здійснювала контроль у сфері захисту персональних даних за аналогічною процедурою), 21% респондентів пояснюють тим, що усунення виявлених порушень може потребувати великих часових затрат, пов'язаних зі змінами програмного забезпечення, вдосконаленням технічних систем захисту інформації, розробленням регламентних документів тощо.

На думку 37% опитаних, 30-денний строк виконання припису уповноваженого зумовлений аналогічною тривалістю строків, відведених на здійснення оператором персональних даних обов'язкових організаційних дій, зокрема: повідомлення уповноваженого про обробку персональних даних, яка становить особливий ризик для прав і свобод їх суб'єктів; повідомлення суб'єкта про збирання та обробку пов'язаних з ним персональних даних; задоволення запиту на доступ до персональних даних і т.ін. На підставі цього робиться припущення, що, оскільки впродовж 30 днів необхідну дію можна виконати в цілком законному порядку, констатувати порушення раніше – означає порушувати права володільця/розпорядника персональних даних.

Варто додати, що більшість практиків не можуть дати логічного пояснення 30-денної тривалості припису про усунення порушень у сфері персональних даних. Це і не дивно, адже за детального розгляду вищенаведені пояснення видаються недостатньо переконливими. По-перше, далеко не завжди усунення інформаційних порушень пов'язане з удосконаленням (модернізацією) програмно-технічного забезпечення обробки персональних даних. Зазвичай такі порушення мають суто організаційний характер і полягають у недотриманні вимог способів збирання й накопичення персо-

нальних даних, строків та умов їх зберігання, зміни, видалення або знищення, порядку доступу до персональних даних, отримання згоди на обробку персональних даних, задоволення законних вимог суб'єкта персональних даних, своєчасного повідомлення про обробку персональних даних тощо. Відповідно припиняти ці порушення слід у якнайкоротший строк.

По-друге, теза про доцільність 30-денного терміну для усунення виявлених порушень на тій підставі, що аналогічний строк відводиться на вчинення обов'язкових дій з організації обробки персональних даних, не витримує перевірки практикою. На практиці припис про усунення порушень правил обробки персональних даних видає уповноважений під час планових або позапланових перевірок стану дотримання інформаційного законодавства. Планові перевірки проходять не частіше разу на рік, а плани їх проведення заздалегідь оприлюднюють на сайті уповноваженого (п.п. 3.2 та 3.3 наказу уповноваженого від 8 січня 2014 року № 1/02-14). Це дає змогу презюмувати обізнаність суб'єкта обробки персональних даних із часом проведення перевірки. Останній завжди має змогу прискорити здійснення необхідних організаційних операцій і вчинити їх до початку перевірки, або ж, якщо це об'єктивно неможливо, зазначити точний час їх здійснення безпосередньо в акті перевірки. У будь-якому разі організаційні заходи, не здійснені на момент перевірки, однак заплановані у визначений законом строк, не вважаються порушенням, отже не можуть слугувати підставою для вжиття припиняючих заходів.

Що ж до позапланових перевірок, то, як правило, їх проводять за фактом виявлених порушень (у разі безпосереднього виявлення порушень вимог законодавства про захист персональних даних уповноваженим, за наявності інформації про порушення вимог інформаційного законодавства у ЗМІ, звернення фізичних та юридичних осіб з повідомленням про порушення), тобто тоді, коли строки вчинення необхідних організаційних дій, пов'язаних з обробкою персональних даних, вже спливли (п. 4.1 наказу уповноваженого від 8 січня

2014 року № 1/02-14). За таких умов жодної потреби в 30-денному очікуванні немає. Навпаки, потрібне негайне припинення наявних порушень та якнайшвидше усунення їхніх наслідків.

З урахуванням викладеного встановлення для реалізації заходів щодо усунення порушень у сфері захисту персональних даних мінімального строку 30 календарних днів видається необґрунтованим. На наш погляд, у наказі уповноваженого від 8 січня 2014 року № 1/02-14 має йтися не про встановлення відповідного терміну, а про обов'язок суб'єкта обробки персональних даних усунути допущені порушення в розумний строк – тобто в найкоротший строк, достатній для своєчасного (без невиправданих зволікань) припинення порушення та відновлення порушених прав, свобод та інтересів.

Ще одним чинником, який гальмує припинення порушень законодавства про захист персональних даних, є надмірна тривалість процедури складання та надіслання відповідного припису. Чинний порядок контролю за додержанням законодавства про захист персональних даних (п. 5.12 наказу уповноваженого від 8 січня 2014 року № 1/02-14) відводить на цю процедуру п'ять робочих днів. В умовах, коли порушені права людини потребують невідкладного захисту та відновлення, такий строк навряд чи можна визнати оптимальним. Більш того, є всі підстави для висновку про доцільність його скорочення.

Як уже зазначалося, припис щодо порушень законодавства у сфері захисту персональних даних складають на підставі раніше складеного акта перевірки. При цьому останній обов'язково містить інформацію «про виявлені в діяльності суб'єкта перевірки порушення вимог законодавства про захист персональних даних, їх детальний опис із посиланням на норми чинного законодавства, які порушено» *(п. 5.3 наказу уповноваженого від 8 січня 2014 року № 1/02-14)* [184].

Фактично це означає, що виявлення, кваліфікація та аналіз усіх юридично значущих обставин порушення відбуваються на етапі складання акта перевірки. Натомість процес

складання припису щодо усунення виявлених порушень не потребує проведення складних логіко-юридичних і технічних операцій – дані про вчинене правопорушення механічно переносяться до нього з акта перевірки.

Не потребує особливих часових затрат і розроблення заходів припинення. Зазвичай суб'єкт перевірки (уповноважений) такі заходи у приписі не конкретизує, обмежуючись вимогою усунення порушень законодавства та покладаючи вибір необхідних для цього засобів на розсуд самого порушника.

Таким чином, складання та надіслання припису про усунення порушень у сфері захисту персональних даних – це відносно негроміздка в бюрократичному і технічному плані процесуальна дія. Її можна і потрібно здійснювати у максимально стислий строк, що дасть змогу якнайшвидше припинити наявне порушення, усунути пов'язані з ним ризики, відновити порушені ним права, нейтралізувати його шкідливі наслідки. Що ж стосується тривалості цього строку, то, вочевидь, він не повинен перевищувати трьох робочих днів з дня складення акта перевірки уповноваженого.

Отже, з урахуванням викладеного можемо констатувати, що на сьогодні у сфері захисту персональних даних застосовують розмаїту систему заходів припинення. Вона охоплює широкий комплекс майнових та організаційних заходів, котрі реалізуються як у судовому, так і в позасудовому порядку. Аналіз практики застосування цих заходів свідчить про достатньо високий рівень їх ефективності. Здебільшого вони характеризуються своєчасністю, обґрунтованістю, доцільністю й результативністю, що забезпечує чітке припинення правопорушень та мінімізацію їх шкідливих наслідків.

Проте варто звернути увагу на надмірну тривалість процедури застосування припиняючих заходів у позасудовому порядку. Нинішні нормативні обмеження фактично унеможливлюють миттєве реагування на делікт. Мінімальна тривалість процедури усунення порушень, які виявляють у ході

перевірок суб'єктів обробки персональних даних, становить 30 календарних днів з дня винесення припису про усунення таких порушень. Враховуючи, що це лише мінімальний строк, а також те, що на складання й надіслання відповідного припису відведено п'ять робочих днів, процес застосування припиняючих заходів, як правило, триває значно довше. В умовах необхідності якнайшвидшого припинення інформаційних правопорушень такий стан справ неможливо визнати прийнятним.

Оптимальним способом розв'язання цієї проблеми є оптимізація строків складання, надіслання та виконання припису уповноваженого щодо усунення порушень у сфері захисту персональних даних. З цією метою пропонуємо внести до наказу уповноваженого від 8 січня 2014 року № 1/02-14 такі зміни:

абз. 8 п. 5.11 наказу викласти в такій редакції: «строк виконання припису (найкоротший строк, достатній для своєчасного (без невиправданих зволікань) припинення порушення та відновлення порушених прав, свобод та інтересів)»;

п. 5.12 наказу викласти в такій редакції: «Припис складається у двох примірниках: перший примірник не пізніше трьох робочих днів з дня складення акта перевірки надсилається суб'єкту перевірки чи уповноваженій ним особі рекомендованим листом з повідомленням про вручення, а другий примірник залишається в секретаріаті уповноваженого»;

у п. 5.13 слова «(не менш ніж 30 календарних днів)» вилучити.

Пропоновані зміни забезпечать істотне прискорення процесу припинення порушень у сфері захисту персональних даних, гарантуючи якнайшвидше відновлення порушених прав, стабілізацію інформаційних правовідносин, усунення причин і умов, що сприяють деліктності.

3.3. Юридична відповідальність за порушення законодавства про захист персональних даних

На сучасному етапі розвитку інформаційних відносин основним засобом їх правового захисту виступає юридична відповідальність. Являючи собою «реагування держави на делікт, виражене в негативній оцінці протиправного вчинку та примушуванні порушника до виконання вимог права» [210, с. 297], «інструмент охорони правопорядку» [211, с. 470] та «важливу детермінанту правомірної поведінки» [212, с. 116], юридичну відповідальність вчені розглядають як визначальний чинник інформаційної безпеки та захисту персональних даних.

Її роль у механізмі захисту персональних даних неможливо переоцінити. Передусім саме юридична відповідальність забезпечує невідворотність кари за порушення вимог інформаційного законодавства, гарантує відновлення порушених інформаційних прав, сприяє вихованню громадян в дусі поваги до фундаментальних прав людини (зокрема права на конфіденційність приватного життя). Саме вона гарантує стабільне функціонування сфери інформаційних відносин і забезпечує її стійкість до протиправних посягань.

Зважаючи на актуальність, питання юридичної відповідальності за порушення законодавства про захист персональних даних виступають предметом високого наукового інтересу. Зокрема, їх дослідженню присвячені капітальні праці О. Горпинюк, А. Чернобай, С. Ясечко та інших представників вітчизняної правової науки [30; 33; 34; 51; 53]. Не лишаються вони й поза увагою законодавця. Починаючи з 2011 року, до КУпАП та КК було внесено положення, спрямовані на вдосконалення правових засад відповідальності за делікти проти безпеки персональних даних.

Аналіз матеріалів юрисдикційної практики змушує констатувати, що стрімкого прогресу в справі протидії пору-

шенням законодавства про захист персональних даних немає. Щороку уповноважені суб'єкти юрисдикції розглядають сотні скарг на порушення законодавства про захист персональних даних. Вони фіксують часті випадки несанкціонованого збирання конфіденційної інформації, надмірних персональних даних, безпідставної відмови в доступі до них, поширення персональних даних без згоди особи, невиконання законних вимог суб'єкта персональних даних та інших порушень законодавства. За інформацією ДСУЗПД, порушення правил обробки персональних даних нині мають місце на більшості (понад 60%) підприємств, установ та організацій усіх форм власності. Часто такі порушення мають непоодинокий, повторний або систематичний характер [213].

Як свідчить проведений аналіз, така ситуація зумовлена багатьма чинниками. Це і недосконале адміністрування, і малоефективність профілактичних заходів, і недостатня щільність галузевого контролю, і багато інших. Але безсумнівно, головна її причина полягає в недоліках законодавства про юридичну відповідальність.

За загальним визнанням науковців і практиків, кореспондуючі законодавчі положення охоплюють далеко не всі суспільні відносини, які об'єктивно потребують правового захисту. Зокрема, ними не передбачено конкретних заходів відповідальності за порушення прав суб'єктів персональних даних (на вимогу проти обробки своїх персональних даних, щодо зміни своїх персональних даних тощо), порушення правил обробки, а також за недодержання встановленого порядку захисту персональних даних (відповідно до ст. 188–39 КУпАП, такі дії мають наслідком відповідальність лише тоді, коли вони спричинили незаконний доступ до персональних даних або порушення прав суб'єкта персональних даних).

Суспільна небезпека цих порушень не підлягає сумніву. Цілком очевидно, що порушення прав суб'єктів персональних даних суперечать ідеології демократичного інформа-

ційного суспільства та ст. 32 Конституції України, згідно з якою кожний громадянин має право ознайомлюватися в органах державної влади, органах місцевого самоврядування, установах і організаціях з відомостями про себе, котрі не є державною або іншою захищеною законом таємницею.

Порушення порядку захисту персональних даних містять широкий спектр загроз для конфіденційності приватного життя людини. Часто такі порушення не спричиняють реальної шкоди лише через збіг обставин. Тож боротьба з ними (зокрема засобами юридичної відповідальності) має нітрохи не менше значення, ніж протидія деліктам з матеріальними шкідливими наслідками.

Що ж стосується порушень правил обробки персональних даних, то вони чинять деструктивний вплив на систему інформаційних відносин, роблячи її менш стабільною та більш вразливою до незаконних втручань. За великим рахунком, вони мають ті самі наслідки, що й порушення вимог щодо їх захисту. Однак попри це, законодавець не відносить їх до суспільно небезпечних діянь і не встановлює за них юридичної відповідальності.

Викладене зумовлює необхідність деліктизації порушень прав суб'єктів персональних даних, а також порушень встановленого законом порядку їх обробки та захисту. На наш погляд, здійснюючи цей крок, слід виходити з того, що:

здебільшого відповідні порушення вчинюють у сфері публічного й корпоративного адміністрування, являють собою порушення адміністративно-регламентних норм, характеризується помірним (порівняно з кримінально караними діяннями) ступенем суспільної небезпеки, отже мають бути віднесені до розряду адміністративних проступків;

оскільки вже сам факт таких порушень справляє негативний вплив на інформаційні відносини, відповідальність за їх вчинення має наставати безвідносно до наявності/відсутності матеріальних наслідків у вигляді матеріальної чи моральної шкоди. Юридичні склади цих порушень мають бути формальними, що уможливить кваліфікацію та притягнення винних до відповідальності за фактом протиправних дій (бездіяльності);

настання шкідливих матеріальних наслідків можна розглядати як кваліфікаційну ознаку складу та обставини, яка зумовлює підвищену відповідальність за порушення законодавства про захист персональних даних.

Істотною перепоною на шляху до підвищення ефективності механізмів відповідальності за делікти у сфері захисту персональних даних є некоректне формулювання змісту відповідних юридичних норм. Окремі положення КУпАП та КК України характеризуються суперечливими і невизначеними моментами, які утруднюють кваліфікацію правопорушень, вибір належного стягнення (покарання) та здійснення юрисдикційних процедур.

Наочним прикладом може слугувати ч. 4 ст. 188-39 КУпАП, якою передбачена відповідальність за «недодержання встановленого законодавством про захист персональних даних *порядку захисту персональних даних*, що призвело до незаконного доступу до них або порушення прав суб'єкта персональних даних» *(курсив мій. – А.П.)*. Очевидно, під час створення (2011 р.) та подальшого редагування (2013 р.) цієї норми з поля зору законодавця випало те, що порядок захисту персональних даних не визначається законом ні як правове поняття, ні як юридична процедура.

Нинішні законодавчі вимоги стосуються виключно *порядку обробки персональних даних*. Вони не підпадають під охорону ч. 4 ст. 188-39 КУпАП, оскільки законодавець чітко розмежовує процеси обробки та захисту персональних даних (наприклад, ст. 1, ст. 10 і ст. 24 Закону України «Про захист персональних даних»).

Таким чином, склалася дещо парадоксальна ситуація, коли норми адміністративно-деліктного законодавства охороняють порядок, не врегульований правом, тоді як детально впорядковані на законодавчому та підзаконному рівнях відносини з приводу обробки персональних даних перебувають поза межами їхнього впливу. Закономірним наслідком такої ситуації є неузгодженість рішень суб'єктів кваліфікації.

Багато нарікань серед правозастосовців викликає також формулювання змісту ст. 212-3 КУпАП «Порушення права на

інформацію», якою передбачено відповідальність за неправомірну відмову в наданні інформації, несвоєчасне або неповне надання інформації, надання інформації, що не відповідає дійсності, у випадках, коли така інформація підлягає наданню на запит громадянина чи юридичної особи відповідно до законів України «Про доступ до публічної інформації», «Про звернення громадян», «Про доступ до судових рішень», «Про засади запобігання і протидії корупції», «Про адвокатуру та адвокатську діяльність».

По-перше, в наведеному переліку законодавчих актів, які вимагають обов'язкового надання інформації на запит фізичних і юридичних осіб, нема Закону «Про захист персональних даних». Це дезорієнтує суб'єктів правозастосування та змушує їх сумніватися в обґрунтованості кваліфікації за ст. 212-3 КУпАП випадків порушення права особи на доступ до інформації про себе.

По-друге, конкретизацію у змісті адміністративно-деліктної норми всіх охоронюваних нею законів слід вважати явним порушенням нормотворчої техніки. Адже за такого підходу навіть найменші зміни в назвах законів потребуватимуть вимушеного оновлення КУпАП. На сучасному етапі розвитку вітчизняного законодавства, який вирізняється активністю і глибиною системних перетворень, імовірність таких змін дуже висока (принаймні два закони з переліку ст. 212-3 КУпАП мають вже не першу редакцію та назву, відмінну від первинної). Крім того, у разі ухвалення нового закону, який потребуватиме адміністративно-правового забезпечення, будь-яка затримка із включенням його назви до ст. 212-3 КУпАП зумовлюватиме вразливість і беззахисність регламентованих ним відносин.

По-третє, ст. 11 Закону України «Про інформацію» гарантує кожному право на доступ до інформації про себе. Це право забезпечується обов'язком володільців і розпорядників персональних даних повідомляти особі зміст пов'язаних з нею даних, які перебувають в обробці. Однак попри те, що за чинним законодавством носіями такого обов'язку виступають і фізичні, і посадові особи (ст.ст. 2, 8 та 16 Закону

України «Про захист персональних даних»), ст. 212-3 КУпАП передбачає відповідальність тільки останніх. Чинність цієї статті не поширюється на фізичних осіб. Як наслідок, вчинювані ними порушення не підпадають під вплив адміністративних санкцій, а відповідні суспільні відносини мають вельми низький рівень правового захисту.

По-четверте, останнє оновлення редакції ст. 212-3 КУпАП (Закон від 27 березня 2014 року «Про внесення змін до деяких законодавчих актів України у зв'язку з прийняттям Закону України «Про інформацію» та Закону України «Про доступ до публічної інформації») мало наслідком розмежування складів проступків, пов'язаних з порушенням права на інформацію [214]. Замість однієї норми, яка передбачала відповідальність за всіх види обмежень права на інформацію (ч. 1 ст. 212-3 КУпАП в редакції від 5 липня 2012 року) в ст. 212-3 КУпАП з'явилося кілька окремих частин, які встановлюють відповідальність за різні види інформаційних обмежень: права на доступ до публічної інформації (ч. 2), права на доступ до інформації, що надається на адвокатський запит (ч. 4), права на доступ до судового рішення або матеріалів справ (ч. 5).

Доцільність такої новели (читай законодавчого розмежування норм про відповідальність за порушення права на інформацію) доволі сумнівна, адже всі ці порушення характеризуються однотипністю, мають однаковий ступінь суспільної небезпеки, а за їх учинення передбачено абсолютно тотожні санкції – накладення штрафу від 25 до 50 неоподатковуваних мінімумів доходів громадян. Єдиним практичним наслідком нововведень стало утруднення кваліфікації, оскільки суб'єкти правозастосовної діяльності в ході юридичної оцінки посягань тепер змушені звертатись не до однієї, а одразу до кількох конкуруючих адміністративно-деліктних норм.

Крім того, якщо попередня редакція ст. 212-3 КУпАП в числі інших порушень передбачала відповідальність за неправомірну відмову в наданні інформації на підставі вимог Закону України «Про інформацію» (отже, охоплювала випадки ненадання інформації на вимогу суб'єкта персональ-

них даних), то в новій редакції згадки про цей закон немає. Фактично зі змісту ст. 212-3 КУпАП зникло положення, котре давало підстави кваліфікувати за нею випадки обмеження права людини на інформацію про себе. У результаті згадане право залишилося без правових гарантій, а кореспондуючі суспільні відносини – без адміністративно-правового захисту.

У світлі викладеного вище постає необхідність кардинального оновлення змісту ст. 212-3 КУпАП, яка, з одного боку, має охоплювати всі випадки порушення права на інформацію (а не лише порушення вимог окремих законів), а з іншого – передбачати відповідальність усіх осіб, які такі порушення вчиняють.

Проблема недосконалого формулювання змісту норм про відповідальність за делікти у сфері захисту персональних даних властива також і кримінальному праву. Зокрема, недостатньою вичерпністю опису протиправних діянь характеризується ст. 182 КК України «Порушення недоторканості приватного життя». У ч. 1 цієї статті наведено перелік операцій обробки конфіденційних даних, незаконне здійснення яких має наслідком кримінальну відповідальність (нині це збирання, зберігання, використання, поширення, зміна та знищення конфіденційної інформації). Однак з невідомих причин до переліку не було внесено такі операції: накопичення, що передбачає об'єднання, систематизацію та внесення персональних даних до відповідних інформаційних баз; адаптування, тобто переведення даних в іншу форму (зокрема цифрову) для забезпечення їх обробки на конкретних технічних засобах або під управлінням конкретних програмних продуктів; знеособлення – дії, в результаті яких унеможливлюється встановлення особи суб'єкта персональних даних без застосування додаткової інформації (додаткових засобів).

Як наслідок, незаконне проведення цих операцій з точки зору букви закону, не може вважатися злочином та слугувати підставою для кримінальної відповідальності. В умовах очевидності їх суспільної небезпеки таке становище неприйнятне. На наш погляд, у ст. 182 КК України мають бути конкретизовані всі види обробки конфіденційної інформації,

визначені Законом «Про захист персональних даних» (ст. 2). З одного боку, це сприятиме розширенню меж правової охорони конфіденційності приватного життя, а з іншого – дасть змогу уникнути невизначеностей і різночитань під час кваліфікації злочинів.

Поряд із вадами законодавчого опису правопорушень у сфері захисту персональних даних мусимо констатувати недоліки конструювання санкцій відповідних норм. Наочним прикладом може слугувати ст. 212-3 КУпАП. З часу введення до КУпАП (2003 р.) вона зазнавала неодноразових уточнень, аж до повної зміни редакції в 2014 році. Проте ці зміни стосувалися переважно опису протиправних діянь, зокрема їх об'єктивних ознак. Санкції ст. 212-3 КупАП якщо й змінювались, то несуттєво. Сьогодні розміри передбачених ними штрафів коливаються в діапазоні від 25 до 80 неоподаткованих мінімумів громадян, що не відповідає ні реальному ступеню небезпеки правопорушень (тим більше, що чинна редакція ст. 212-3 КУпАП встановлює відповідальність за службові/посадові делікти), ні сучасним економічним реаліям. В умовах, коли розміри шкоди, заподіюваної порушенням права на інформацію, значно перевищують розміри кореспондуючих адміністративних стягнень, ефективність останніх завжди перебуватиме під питанням.

Про недостатню увагу законодавця до конструювання санкцій ст. 212-3 КУпАП свідчить і те, що і ч. 3 цієї статті, яка передбачає відповідальність за неправомірне обмеження доступу до інформації (основний склад), і ч. 7, що встановлює відповідальність за повторне вчинення таких порушень (кваліфікований склад), містять тотожні грошові стягнення – від 60 до 80 неоподатковуваних мінімумів доходів громадян. Таку ситуацію, коли за вчинення двох однотипних діянь, одне з яких *a priori* характеризуються вищим рівнем суспільної небезпеки, на порушників накладаються однакові штрафи, неможливо визнати прийнятною.

Ще одну проблему становить чималий розрив між межами санкцій, передбачених за вчинення правопорушень з основними та кваліфікованими складами.

Як відомо, з метою диференціації юридичної відповідальності законодавець нерідко встановлює різні (як за характером, так і за розміром) санкції для правопорушень, які мають спільні конституюючі ознаки, але відрізняються за додатковими параметрами. Здебільшого наявність цих параметрів свідчить про підвищену небезпеку посягання, отже про необхідність застосування щодо порушника більш жорстких заходів примусу.

При цьому теорія права виходить з того, що основний та кваліфікований склади мають різний ступінь суспільної небезпеки за умов її єдиного характеру, що зумовлює неприпустимість розриву між максимумом покарання за делікт з основним складом та мінімумом покарання за делікт із кваліфікованим складом. «Принципово важливо дотримуватися правила, згідно з яким нижня межа санкції кваліфікованого складу має перекривати верхню межу санкції основного складу або принаймні дорівнювати їй», – пише Г. Радбрух [215, с. 200]. «У разі з основними та кваліфікованими складами ланцюг санкцій повинен іти або встик, або з перекриттям», – підтверджує цю тезу Т. Леснієвскі-Костарєва [216, с. 341].

На жаль, конструюючи санкції норм про відповідальність за делікти у сфері захисту персональних даних, це правило враховували не завжди. Наприклад, санкція ч. 1 ст. 188-39 КУпАП, якою встановлено відповідальність за порушення правил повідомлення уповноваженого Верховної Ради України з прав людини про обробку персональних даних, передбачає накладення штрафу від 100 до 200 неоподатковуваних мінімумів доходів громадян (далі н.м.д.г.), на посадових осіб, громадян – суб'єктів підприємницької діяльності – від 200 до 400 н.м.д.г. Водночас ч. 3 ст. 188-39 КУпАП за повторне вчинення таких порушень передбачає штрафи: для громадян – від 300 до 500 н.м.д.г., для посадових осіб, громадян – суб'єктів підприємницької діяльності – від 500 до 2 тис. н.м.д.г.

Значно більший розрив існує між санкціями норм про відповідальність за недодержання встановленого порядку захисту персональних даних, що призвело до незаконного доступу до них або порушення прав їх суб'єкта. За вчинення такого порушення вперше на громадян накладається штраф у розмірі від 100 до 500 н.м.д.г. (ч. 4 ст. 188-39 КУпАП), а за повторне вчинення протягом року після накладення стягнення – від 1 тис. до 2 тис. н.м.д.г. (ч. 5 ст. 188-39 КУпАП).

Аналогічна проблема спостерігається і в кримінальному законодавстві, зокрема, у ст. 362 КК України «Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах, автоматизованих системах, комп'ютерних мережах…». Якщо дії, передбачені ч. 1 цієї статті (основний склад злочину), караються штрафом або виправними роботами на строк до двох років, то скоєння злочину із кваліфікованим складом (ч. 3) має наслідком позбавлення волі на строк від трьох до шести років з позбавленням права обіймати певні посади або займатися певною діяльністю.

Наявні проблеми диктують необхідність перегляду санкцій, передбачених за делікти у сфері захисту персональних даних з основними та кваліфікованими складами, на предмет взаємної узгодженості та системного зв'язку.

Ще одним недоліком законодавчого конструювання відповідних санкцій є надмірна різниця між верхньою та нижньою межами визначених ними заходів примусу. З одного боку, це свідчить про невдалу диференціацію юридичної відповідальності та стирає грань між деліктами різного ступеня суспільної небезпеки. З іншого – створює певні корупційні ризики. Як цілком справедливо підкреслює В. Красніков, широкі межі санкцій слугують підґрунтям для різноманітних маніпуляцій, адже що вища різниця між мінімальним і максимальним стягненням, то більшу неправомірну вигоду можна отримати під час вибору меншого з них [217, с. 47].

Особливо широким діапазоном стягнень характеризуються санкції норм про адміністративну відповідальність за порушення законодавства про захист персональних даних. Наочний

приклад – ст. 188-32 КУпАП: різниця між мінімальним і максимальним розмірами штрафу, передбаченими ч. 1 цієї статті, становить 100%; ч. 2 – 330%; ч. 3 – 400%; ч. 4 – 500%. В умовах, коли звуження діапазону санкцій виступає одним із ключових моментів реформування інституту адміністративної відповідальності, такі приклади не можна вважати допустимими. У зв'язку з цим доцільно розглянути питання про усунення наявних диспропорцій шляхом підвищення мінімального обсягу стягнень, передбачених за правопорушення у сфері захисту персональних даних.

Аналіз адміністративно- та кримінально-правових підстав відповідальності за делікти у сфері захисту персональних даних свідчить про брак єдиного підходу до визначення міри стягнення/покарання стосовно службових (посадових) осіб.

Так, вітчизняне адміністративно-деліктне законодавство встановлює підвищену відповідальність посадових осіб, які вчинили порушення законодавства про захист персональних даних. Відповідно до ст. 188-39 КУпАП, за вчинення таких порушень до посадових осіб застосовуються значно суворіші санкції, ніж до пересічних громадян (в окремих випадках різниця між максимальними сумами штрафу, передбачених для різних категорій осіб, становить 400%). Де факто це означає визнання законодавцем підвищеної суспільної небезпечності адміністративних проступків, вчинюваних посадовими особами, і необхідності посиленої боротьби з ними шляхом застосування більш жорстких заходів примусу.

Однак в рамках інституту кримінальної відповідальності реалізується інший підхід. Норми про відповідальність за злочини у сфері захисту персональних даних (напр. ст.ст. 182, 330, 361-2, 362 та 363 КК України) не передбачають диференційованого покарання службових (посадових) і фізичних осіб. Наявність у винної особи службового (посадового) статусу жодним чином не впливає на вид і розмір застосовуваних щодо неї правових обтяжень. Не є вона і кваліфікуючою ознакою, яка зумовлювала б кваліфікацію злочинів за іншими положеннями кримінального законодавства, зокрема за тими, які встановлюють підвищену міру відповідальності.

Таким чином, на рівні кримінально-правового забезпечення захисту персональних даних ідею про підвищену небезпеку деліктів, учинених з використанням службового становища, не втілено.

З таким підходом важко погодитись. Адже обробка персональних даних – це сфера, де службове становище особи відкриває перед нею широкі можливості щодо збирання, систематизації та використання конфіденційної інформації. Службові особи нерідко користуються правом безперешкодного доступу до великих баз даних, мають у розпорядженні потужні інформаційні ресурси, володіють ексклюзивним правом на обробку найбільш вразливих видів конфіденційної інформації.

Відповідно порушення службовими особами законодавства про захист персональних даних становлять високу загрозу для сфери інформаційних відносин та права громадян на конфіденційність приватного життя. Значно вищим у цьому разі є також і ризик спричинення негативних наслідків: моральної шкоди, матеріальних втрат абощо. Усе це зумовлює постановку питання про посилення відповідальності за злочини у сфері захисту персональних даних, вчинювані з використанням службового становища.

Одним з можливих шляхів його вирішення може стати внесення службового становища особи до переліку кваліфікуючих ознак злочинів, передбачених ч. 2 ст. 182 КК України.

Важливою запорукою ефективного функціонування механізмів юридичної відповідальності є наявність досконалого процесуального забезпечення, здатного гарантувати невідворотність покарання порушника, об’єктивність і неупередженість розгляду справи, своєчасність і повноту відновлення порушених прав, законність і послідовність правозастосування. Водночас навіть незначні вади процесуального регулювання суттєво погіршують стан юрисдикційної практики. Нині більшість рішень у справах про делікти у сфері захисту персональних даних оскаржують саме через порушення процесуальних правил. Останні ж характеризуються

багатьма невизначеностями, що суттєво утруднює (а інколи взагалі унеможливлює) їх одноманітне розуміння та реалізацію.

Особливо гостро ця проблема постає у ході застосування заходів адміністративної відповідальності. Так, на сьогодні в чинному КУпАП не визначено моменту початку річного строку, необхідного для кваліфікації повторних правопорушень. У ч. 3 та ч. 5 ст. 188-39, а також у ч. 2 ст. 212-3 КУпАП законодавець використовує формулу: «повторне протягом року вчинення порушення…, за яке особу вже було піддано адміністративному стягненню», однак не роз'яснює, з якого саме моменту слід розпочинати відлік річного строку: чи з моменту вчинення правопорушення, чи з моменту накладення адміністративного стягнення, чи то пак з моменту його виконання. Не містить відповідних роз'яснень і Загальна частина КУпАП. Закономірним наслідком такої невизначеності став брак узгодженого підходу серед суб'єктів кваліфікації.

Не менш гостро постає проблема неузгодженості правових актів, якими визначаються адміністративно-процесуальні функції та загальний правовий статус уповноваженого Верховної Ради України з прав людини. Відповідно до п. 10 ст. 23 Закону України «Про захист персональних даних» уповноважений наділяється повноваженням складати протоколи про притягнення до адміністративної відповідальності й направляти їх до суду у випадках, передбачених законом. Водночас чинне законодавство таких випадків просто не знає.

Чинний КУпАП (ст. 255) наділяє правом складення адміністративних протоколів в справах про порушення тільки посадових осіб секретаріату уповноваженого. По суті, це означає, що саме їх (а не уповноваженого) наділено функціями щодо попереднього розслідування адміністративно-деліктних посягань, порушення справ про адміністративні проступки та відкриття адміністративно-деліктного провадження.

Неприйнятність такої ситуації очевидна. Адже неузгодженість окремих елементів правового статусу органу чи посадової особи (цілей, завдань, функцій, сфери відання, прав, обов'язків тощо) спричиняє внутрішні організаційні

суперечності, збої механізму адміністрування, виникнення юридичних конфліктів [218, с. 42, 44]. З огляду на це вважаємо, що адміністративно-процесуальні функції посадових осіб секретаріату уповноваженого мають знайти відображення в положеннях Закону України «Про захист персональних даних». Натомість право уповноваженого складати адміністративні протоколи слід конкретизувати у ст. 255 КУпАП.

Дискусійний характер мають і деякі положення кримінально-процесуального законодавства. Зокрема, відповідно до ст. 477 КПК України, провадження в справах про порушення недоторканості приватного життя (ст. 182 КК України) здійснюється лише у формі приватного обвинувачення, тобто виключно на підставі заяви потерпілого.

На перший погляд, такий підхід може здатись обґрунтованим, оскільки і з назви ст. 182 КК України, і з доктринального уявлення про безпосередній об’єкт передбачених цією статтею порушень випливає їх спрямованість проти приватних інтересів окремої особи [54, с. 111]. Отож, з точки зору законодавця, саме вона й повинна вирішувати питання про кримінально-правовий захист своїх прав та кримінальне переслідування порушника.

Однак при детальному розгляді ситуація не видається настільки однозначною. Адже незаконні операції з персональними даними, особливо на первинних етапах їх обробки (збирання, систематизація, зберігання), здебільшого мають закритий характер. Вони перебігають приховано, а ймовірність їх виявлення суб’єктом персональних даних (читай потерпілою особою) дуже мала. Часто потерпіла особа констатує порушення своїх прав не за фактом протиправного діяння, а за його наслідками, тобто вже після того, як воно справило реальний негативний вплив на її життя. У решті випадків незаконні операції з персональними даними залишаються непоміченими. Та це зовсім не означає, що вони не становлять суспільної небезпеки.

У цьому плані варто погодитися з російським правником О. Рязанцевим, який пише: «Будь-яка обробка конфіденційної

інформації, здійснювана всупереч закону, становить об'єктивну загрозу для приватних інтересів та конституційного права на таємницю приватного життя. Незаконна обробка інформації про особу завжди небезпечна, незалежно від того, знає про неї особа чи ні. Вона завжди становить ризики для людини, для її близького оточення та й загалом для суспільства, зацікавленого в безпечному стані інформаційних відносин. Останні ж потребують постійного та надійного кримінально-правового захисту» [219, с. 74].

Крім того, як показує практика, незаконні операції з персональними даними найчастіше здійснюють в рамках функціонування великих інформаційних баз (баз персональних даних). У ході їх реалізації відбувається системна обробка інформації про велику кількість громадян, що свідчить про масовий характер порушень недоторканності приватного життя. Таким чином, порушення, передбачені ст. 182 КК України, хоч і посягають на суто приватні інтереси, але в багатьох випадках це інтереси не окремого індивіда, а широкого кола осіб.

Зважаючи на викладене вище та враховуючи те, що основна маса правопорушень проти недоторканності приватного життя, зокрема у сфері обробки персональних даних, виявляються під час реалізації заходів публічного контролю, а також беручи до уваги необхідність системної протидії незаконній обробці персональних даних на всіх її стадіях та етапах, вважаємо за доцільне повернутися до практики розгляду відповідних кримінальних справ у загальному порядку, який передбачає можливість відкриття провадження не лише за заявою потерпілого, а й у разі отримання інформації про злочин з будь-яких інших джерел.

Окрему проблему становить правове забезпечення захисту персональних даних у трудових (службових) відносинах. Нині вітчизняне законодавство передбачає лише загальну можливість застосування дисциплінарної та матеріальної відповідальності за вчинення так званих інформаційних порушень (ст. 27 Закону України «Про інформацію»),

однак не визначає при цьому ні підстав такої відповідальності, ні конкретних її форм, ані механізмів її втілення. Зокрема, чинний КЗпП не містить жодної норми, яка встановлювала б відповідальність працівників за порушення правил обробки та захисту персональних даних, допущені в ході професійної діяльності. Вважаємо це значною прогалиною, оскільки за таких умов питання про відповідальність порушника та відшкодування ним заподіяної шкоди на рівні трудових відносин вирішити фактично неможливо [227].

У цьому плані вартий уваги досвід країн близького зарубіжжя. Наприклад, ст. 243 Трудового кодексу Російської Федерації встановлює повну матеріальну відповідальність працівника за розголошення ним відомостей, які становлять охоронювану законом службову, комерційну або іншу таємницю [220]. Статтею 190 Кодексу законів Болгарії про працю (ст. 190) передбачено можливість звільнення працівника в порядку дисциплінарного стягнення за «зловживання довірою роботодавця та розголошення конфіденційних даних про нього» [221]. Трудовий кодекс Польщі містить вимогу щодо збереження конфіденційної інформації (ст. 100) та відшкодування збитків, заподіяних недотриманням цієї вимоги (Розділ V Глави I) [222]. За ст. 235 Трудового кодексу Литовської Республіки, відмова в наданні інформації, якщо закони та інші правові акти чи правила трудового розпорядку зобов'язують її надавати, а також надання завідомо неправдивої інформації є грубим порушенням трудових обов'язків, яке має наслідком дисциплінарну відповідальність працівника [223].

Високий рівень правової регламентації питань відповідальності за порушення правил обробки та захисту конфіденційних даних у трудовому законодавстві інших країн видається цілком обґрунтованим. Такі порушення вельми специфічні як з точки зору спричинюваної шкоди, так і з точки зору ефективності правових заходів реагування. Як свідчить практика, боротьба з ними здійснюється винятково засобами адміністративного, кримінального та цивільного права й далеко не завжди здатна спричинити максимальний результат.

Наприклад, порушення (особливо неодноразове) працівником вимог законодавства про захист персональних даних зумовлює порушення питання не тільки про адміністративну відповідальність порушника за ст. 188-39 КУпАП, а й про доцільність його перебування на займаній посаді, відшкодування шкоди, заподіяної роботодавцеві, тощо. Та, на жаль, в Україні для вирішення цих питань не створено належного правового підґрунтя, внаслідок чого вони вже багато років залишаються без відповідей.

Нині існує нагальна потреба формування правових засад боротьби з інформаційними порушеннями у трудовій сфері. З цією метою доцільно внести до чинного КЗпП комплекс змін, спрямованих на визначення підстав, умов та заходів відповідальності за порушення учасниками трудових відносин вимог щодо захисту персональних даних і безпеки приватності.

Обов'язковому врахуванню підлягають два такі моменти:

по-перше, дисциплінарну (матеріальну) відповідальність за порушення законодавства про захист персональних даних слід розглядатись не як альтернатива іншим заходам примусу (зокрема заходам адміністративної, кримінальної й цивільної відповідальності), а як інтегральну складову їх системи. У цьому сенсі неможливо підтримати тезу про те, що «дисциплінарна відповідальність за порушення норм, котрі регулюють обробку і захист персональних даних працівника, може наставати тільки за умови, якщо в діях особи нема складу злочину чи адміністративного правопорушення» [34, с. 152]. На наш погляд, роль дисциплінарної відповідальності не зводиться до заповнення порожнин в репресивному механізмі. Вона покликана збагатити правовий інструментарій боротьби з порушеннями інформаційного законодавства. Її заходи потрібно реалізувати не на додачу, а разом з іншими заходами відповідальності, забезпечуючи комплексний вплив на суспільні відносини та всебічний захист конфіденційності приватного життя;

по-друге, правове регулювання суспільних відносин з приводу обробки та захисту персональних даних у трудовій

сфері має ґрунтуватися на засадах взаємної відповідальності працівника й роботодавця. Як засвідчив проведений аналіз, і у вітчизняній правничій літературі, і в трудовому законодавстві інших країн основну увагу приділено відповідальності працівників, натомість питання відповідальності роботодавців часто залишаються без належної уваги. Вважаємо це невиправданим, адже порушення інформаційного законодавства (зокрема про захист персональних даних) становлять небезпеку для всіх учасників трудових відносин. Внаслідок їх учинення матеріальна та інша шкода може бути завдана не тільки певному підприємству (органу, установі, організації), а й конкретним працівникам. Більш того, на практиці випадки порушення інформаційних прав працівника роботодавцем трапляються значно частіше, ніж навпаки. За цих умов надання роботодавцеві повнішого й надійнішного правового захисту від порушень, пов'язаних з обробкою персональних даних, дисонує з ідеями справедливості та рівності, задекларованими в чинному законодавстві.

На наш погляд, урахування зазначених моментів – важлива умова дієвості й ефективності кроків з удосконалення правового захисту персональних даних у трудовій сфері.

Істотного вдосконалення потребують також правові засади цивільної відповідальності у сфері захисту персональних даних. На сьогодні Цивільний кодекс України врегульовує питання відповідальності за порушення права на захист персональних даних вельми опосередковано, через визначення способів захисту інформаційних відносин (ч. 2 ст. 200), закріплення права на охорону особистих немайнових благ (ч. 1 ст. ст. 201), встановлення загальної заборони на збирання, зберігання, використання і поширення інформації про особисте життя фізичної особи без її згоди (ст. 302 ЦК). При цьому відповідні законодавчі положення характеризуються недостатньою чіткістю, повнотою та послідовністю викладу змісту.

Зокрема, ч. 2 ст. 200 передбачає всього два способи захисту порушених прав у сфері інформації: вимогу щодо усунення порушення таких прав, а також відшкодування майнової і моральної шкоди, завданої такими правопору-

шеннями. Натомість ст. 275 вказує, що захист особистого немайнового права фізичної особи (а саме до цієї категорії належить право на захист персональних даних) може здійснюватись будь-яким з десятка способів, встановлених главою 3 ЦК України, а також іншим способом відповідно до змісту цього права, способу його порушення та наслідків, що їх спричинило це порушення.

Заборона на обробку конфіденційної інформації про особу без її згоди ЦК України розглядає не в рамках забезпечення таємниці особистого життя (ст. 301), а в контексті реалізації права на інформацію (ст. 302). Таке розставлення акцентів видається необґрунтованим. З одного боку, воно суперечить загальному уявленню про захист персональних даних як ключову гарантію прайвесі (а не права на інформацію), а з іншого – нівелює роль захисту персональних даних у забезпеченні конституційних прав і свобод людини, зводячи її до встановлення окремих правових обмежень.

Ст. 301 ЦК України «Право на особисте життя та його таємницю», яка, за логікою, мала б розкривати сутність права на захист конфіденційності приватного життя та конкретизувати підстави цивільної відповідальності за його порушення, обмежується констатацією наявності прав: на особисте життя, на визначення особистого життя, на збереження в таємниці його обставин тощо.

Конкретніший характер (з точки зору визначення підстав відповідальності за порушення права на захист персональних даних) має ч. 4 цієї статті: «Обставини особистого життя фізичної особи можуть бути розголошені іншими особами лише за умови, що вони містять ознаки правопорушення, що підтверджено рішенням суду, а також за її згодою» [137]. Однак її аж ніяк не можна визнати досконалою. Майже дві третини (64%) уповноважених суб'єктів кваліфікації вважають, що ч. 4 ст. 301 ЦК України сформульована у спосіб, який суттєво утруднює її застосування на практиці.

Зокрема, на думку 75% респондентів, поширення конфіденційної інформації може здійснюватись або за згодою суб'єкта

такої інформації, або згоди, якщо інформація стосується вчинених ним правопорушень. Решта ж наполягають, що розголошення обставин особистого життя особи може відбуватися тільки за наявності обох зазначених умов (згоди суб'єкта та безпосереднього стосунку інформації до правопорушення).

Майже 90% опитаних вважають семантичну конструкцію «обставини особистого життя, що містять ознаки правопорушення, що підтверджено рішенням суду» юридично неграмотною й складною для сприйняття. Як основне зауваження наголошує, що обставини особистого життя за визначенням не можуть містити ознак правопорушення. Тим більше, це не може підтверджувати рішення суду.

Крім того, чинна редакція ч. 4 ст. 301 ЦК України погано корелюється з положеннями інших законодавчих актів, а саме:

з ч. 1 ст. 9 Закону «Про інформацію», відповідно до якої інформація з обмеженим доступом може бути поширена тільки, якщо вона суспільно необхідна, тобто є предметом суспільного інтересу, і право громадськості знати цю інформацію переважає потенційну шкоду від її поширення;

з ч. 1 ст. 7 Закону «Про захист персональних даних», яка забороняє обробку персональних даних про засудження до кримінального покарання;

з ч. 1 ст. 302 ЦК України та ч. 2 ст. 14 Закону «Про захист персональних даних», які передбачають, що поширення персональних даних без згоди суб'єкта персональних даних або уповноваженої ним особи дозволено у випадках, визначених законом, і лише (якщо це необхідно) в інтересах національної безпеки, економічного добробуту та прав людини *(підкреслення моє. – А.П.)*.

Такий стан справ зумовлює необхідність комплексного перегляду положень ЦК України, які регламентують питання захисту конфіденційності приватного життя, в тому числі відповідальності за порушення права особи на захист персональних даних.

Підбиваючи остаточний підсумок, мусимо констатувати, що сучасний стан правового забезпечення відповідальності за правопорушення у сфері захисту персональних даних вельми далекий від досконалості. Йому притаманні численні недоліки, котрі проявляються фактично у всіх сферах правової регламентації (адміністративно-правовій, кримінально-правовій, цивільно-правовій, трудовій, господарській) та істотно знижують ефективність протидії не тільки окремим порушенням, а й боротьби з інформаційною деліктністю загалом.

До найбільш дошкульних проблем суб'єкти юрисдикційної практики зараховують: неповноту й фрагментарність правового регулювання (81%), неузгодженість правових актів (75%), змістові вади юридичних норм (зокрема неповнота, нечіткість, неясність і суперечливість їх положень) (73%), розбалансованість системи санкцій, передбачених за делікти у сфері обробки персональних даних (25%), неврегульованість деяких процесуальних аспектів розгляду та вирішення відповідних юридичних справ (12%).

Окреслені проблеми тісно переплетені між собою, що потребує комплексного підходу до їх розв'язання. У рамках цього підходу доцільно:

1) здійснити деліктизацію порушень прав суб'єктів персональних даних, а також порушень правил обробки таких даних шляхом встановлення за них адміністративної відповідальності. Оптимальним способом реалізації цієї мети вбачається викладення ст. 188-39 КУпАП у такій редакції:

«Стаття 188-39. Порушення встановленого порядку обробки персональних даних

Порушення встановлених правил обробки (збирання, реєстрації, накопичення, зберігання, адаптування, зміни, поновлення, використання, поширення, знеособлення або знищення) персональних даних, а також невиконання законних вимог громадян щодо заборони, зміни або знищення пов'язаних з ними персональних даних,

– тягне за собою накладення штрафу на громадян від 100 до 300 неоподатковуваних мінімумів доходів громадян і на посадових осіб, громадян – суб'єктів підприємницької діяльності – від 300 до 500 неоподатковуваних мінімумів доходів громадян.

Ті самі дії, вчинені повторно протягом року після накладення адміністративного стягнення, або якщо вони заподіяли шкоду охоронюваним законом правам, свободам та інтересам особи,

– тягнуть за собою накладення штрафу на громадян від 500 до 1000 неоподатковуваних мінімумів доходів громадян і на посадових осіб, громадян – суб'єктів підприємницької діяльності – від 1000 до 2000 неоподатковуваних мінімумів доходів громадян.

Примітка. Під шкодою в цій статті, якщо вона полягає у заподіянні матеріальних збитків, слід розуміти шкоду на суму від 10 до 100 неоподатковуваних мінімумів доходів громадян»;

2) внести до КУпАП та КК України зміни, спрямовані на вдосконалення змісту положень, якими визначаються підстави відповідальності за делікти у сфері захисту персональних даних, а саме: викласти ст. 212-3 КУпАП у такій редакції:

«Стаття 212-3 Порушення права на інформацію та права на звернення

Неправомірна відмова в наданні інформації, ненаданні інформації, несвоєчасне або неповне надання інформації, надання недостовірної інформації у випадках, коли така інформація підлягає наданню відповідно до чинного законодавства – тягне за собою…

Неправомірне віднесення загальнодоступної інформації до інформації з обмеженим доступом, а також незаконне обмеження права на доступ до інформаційних ресурсів – тягне за собою…

Порушення права особи на доступ до судового рішення або матеріалів юридичної справи – тягне за собою…

Порушення встановленого порядку розгляду звернень громадян – тягне за собою…

Ті самі дії, вчинені повторно протягом року після накладення адміністративного стягнення, або якщо вони заподіяли шкоду охоронюваним законом правам, свободам та інтересам особи, – тягнуть за собою…

Примітка. Під шкодою у цій статті, якщо вона полягає у заподіянні матеріальних збитків, слід розуміти шкоду на суму від 10 до 100 неоподатковуваних мінімумів доходів громадян»;

викласти ч. 1 ст. 182 КК України в такій редакції:

«1. Незаконна обробка (збирання, реєстрація, накопичення, зберігання, адаптування, зміни, поновлення, використання, поширення, знеособлення або знищення) конфіденційної інформації про особу, крім випадків, передбачених іншими статтями цього Кодексу, – караються штрафом від 500 до 1000 неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або арештом на строк до шести місяців, або обмеженням волі на строк до трьох років»;

3) забезпечити комплексний перегляд санкцій, передбачених за делікти у сфері захисту персональних даних на предмет взаємної узгодженості, системного зв'язку, дотримання правил юридичної техніки, адекватності (співмірності) суспільній небезпеці правопорушень, відповідності соціально-економічним умовам сьогодення. Ключовими моментами такого перегляду мають стати:

гармонізація санкцій кримінально-правових та адміністративно-деліктних норм про відповідальність за делікти проти безпеки персональних даних;

усунення розривів між максимальними санкціями норм, що передбачають відповідальність за делікти з основними складами, і мінімальними санкціями норм, які встановлюють відповідальність за аналогічні делікти з кваліфікованими складами (напр. ст. 188-39 КУпАП та ст. 362 КК України);

мінімізація розриву між верхньою та нижньою межами стягнень/покарань, передбачених за одне й те саме правопорушення;

встановлення підвищеної відповідальності посадових (службових) за всі види правопорушень у сфері захисту персональних даних;

збільшення розмірів адміністративних стягнень за порушення права на інформацію (ст. 212-3 КУпАП) до меж, визначених реальним ступенем небезпеки таких порушень, а також критеріями ефективності й економічної доцільності заходів відповідальності;

4) здійснити заходи з удосконалення процесуальних засад відповідальності за правопорушення у сфері обробки та захисту персональних даних, зокрема:

визначити в Загальній частині КУпАП момент початку річного строку, необхідного для кваліфікації правопорушень, вчинюваних повторно протягом року (таким моментом пропонується визнати день накладення адміністративного стягнення за вчинення проступку вперше);

закріпити в КУпАП право уповноваженого Верховної Ради України з прав людини складати протоколи у справах про адміністративні правопорушення, передбачені ст.ст. 188-39 та 188-40 КУпАП. З цією метою доповнити ст. 255 КУпАП «Особи, які мають право складати протоколи про адміністративні правопорушення» пунктом 2-5 такого змісту: «Уповноважений Верховної Ради України з прав людини, посадові особи секретаріату уповноваженого Верховної Ради України з прав людини». Абзац 40 п. 1 ст. 255 КУпАП – вилучити;

відобразити в Законі України «Про захист персональних даних» адміністративно-процесуальні функції посадових осіб секретаріату уповноваженого Верховної Ради України з прав людини;

забезпечити розгляд кримінальних справ про порушення недоторканності приватного життя (ст. 182 КК України) в загальному порядку (а не в порядку приватного обвинувачення), вилучивши зі змісту ст. 477 КПК України слова «статтею 182 (порушення недоторканності приватного життя)»;

5) забезпечити формування правових засад відповідальності (дисциплінарної, матеріальної) за інформаційні правопорушення у трудовій сфері. Визначити в чинному КЗпП України підстави, умови та заходи відповідальності за порушення вимог щодо обробки персональних даних. Покласти в основу правового регулювання кореспондуючих суспільних відносин принцип взаємної відповідальності працівника і роботодавця;

6) розширити перелік способів захисту порушених прав у сфері інформації, визначений ст. 200 ЦК України; оптимізувати зміст ст. 301 ЦК України «Право на особисте життя та його таємницю», звільнивши її від декларативних поло-

жень, закріпивши в ній заборону на обробку конфіденційної інформації без згоди суб'єкта, переглянувши її на предмет відповідності вимогам юридичної техніки.

Врегулювати на рівні ЦК України відносини з приводу: поширення конфіденційної інформації сторонами цивільно-правових зобов'язань, обробки персональних даних, які оприлюднив їх суб'єкт (за його згодою) та перебувають в загальному доступі, використання персональних даних у наукових дослідженнях та під час створення об'єктів інтелектуальної власності, спадкування права на захист таємниці приватного життя, знищення матеріальних носіїв, які використовуються для незаконного зберігання персональних даних.

***

Незважаючи на постійне розширення впливу так званих позитивних методів публічного адміністрування, провідним інструментом захисту персональних даних виступають заходи примусу, спрямовані на профілактику та припинення правопорушень, притягнення порушників до відповідальності, а також відновлення порушених інформаційних прав.

Упродовж останніх років вітчизняна система захисту персональних даних накопичила чималий досвід у сфері боротьби з деліктністю. Поступово вдосконалюється законодавство, реформується інституційна система адміністрування, впроваджуються безпекові нормативи, активізується інформаційно-роз'яснювальна робота серед володільців та користувачів персональних даних.

Проте динаміка позитивних зрушень надто слабка, а результати боротьби з порушеннями законодавства про захист персональних даних неможливо визнати задовільними. Щороку в Україні фіксують десятки правопорушень (у тому числі злочинів), пов'язаних з недотриманням правил обробки та захисту персональних даних. І це лише офіційні дані. На переконання спеціалістів, вказаний вид правопорушень характеризується високим рівнем латентності, що дає змогу говорити про значні масштаби їх соціально-економічної небезпеки.

Як засвідчив аналіз, велика кількість правопорушень та брак стрімкого прогресу в боротьбі з деліктністю у сфері захисту персональних даних зумовлюються багатьма чинниками, як-то: постійні зміни правил автоматизованої обробки персональних даних, слабка резистентність програмно-технічного забезпечення до несанкціонованих втручань, низький рівень правосвідомості суб'єктів інформаційних відносин, недостатня щільність внутрішнього та зовнішнього контролю за додержанням законності тощо.

Однак головна причина невтішного стану справ полягає в недоліках організаційно-правового забезпечення. Фактично на всіх його ділянках мають місце системні збої, зумовлені вадами нормативно-правової регламентації, відсутністю системного підходу в адмініструванні, численними організаційними, методичними й кадровими проблемами, а також багатьма іншими чинниками, які вкрай негативно відображаються на загальному стані захисту персональних даних.

Згадані чинники та пов'язані з ними проблеми мають взаємозумовлений характер, що спричиняє необхідність комплексного підходу до їх вирішення. У рамках цього підходу основні зусилля мають бути скеровані на вдосконалення чинного законодавства (гармонізацію нормативного матеріалу, усунення колізій і дублювань, скасування деактуалізованих норм тощо), розвиток інституційної системи адміністрування, налагодження ефективної взаємодії всіх її ланок і складових, збагачення її ресурсної бази та кадрового потенціалу, вдосконалення механізмів публічного контролю за додержанням законодавства про захист персональних даних.

Та насамперед слід розробити довгострокову програму дій, яка визначить стратегічні цілі, окреслить напрями їх реалізації, об'єднає широкий спектр нормотворчих, організаційних, правозастосовних, інформаційних, технічних та інших заходів у єдиний комплекс із генеральною метою: забезпечити стале зниження деліктності та гарантувати надійний захист прав громадян у сфері захисту персональних даних.

ВИСНОВКИ

Підсумовуючи результати дослідження, можемо констатувати, що забезпечення надійного захисту персональних даних на загальнодержавному рівні потребує вжиття широкого комплексу правових, організаційних, інформаційних та інших заходів, покликаних гарантувати всебічну реалізацію права людини на конфіденційність приватної інформації. Розроблення та планомірне втілення цих заходів – надзвичайно складне завдання, успішне розв'язання якого можливе тільки на основі наукового підходу.

Аналіз стану науково-правових досліджень у сфері захисту персональних даних дає змогу констатувати доволі високий рівень їх актуальності, новизни та практичної значущості. Більшість тематичних досліджень здійснено на основі передового зарубіжного досвіду, з урахуванням міжнародних стандартів і світових тенденцій гарантування інформаційної безпеки. Їх висновки та пропозиції активно впроваджуються в практику вітчизняного нормотворення, правозастосування та правоохорони. Однак науково-правове забезпечення захисту персональних даних характеризується проблемами, зумовленими безсистемністю тематичних досліджень, недостатнім рівнем взаємодії їх виконавців та замовників, слабкою державною підтримкою науково-дослідної діяльності. З метою їх вирішення доцільно: ввести питання наукового забезпечення захисту персональних даних до змісту державних цільових програм і планів інформаційного розвитку; визначити коло нагальних проблем, які потребують першочергового наукового розв'язання; окреслити пріоритетні напрями досліджень у сфері захисту персональних даних, забезпечити їх цільове фінансування та ґрунтове розроблення охопленої ними тематики; постійно інформувати суб'єктів захисту персональних даних про наукові розробки та перспективи їх практичної реалізації; стимулювати розроблення малодосліджених аспектів інформаційної безпеки; налагодити тісну взаємодію між профільними навчальними закладами (науково-дослідними установами) та суб'єктами публічного адміністрування захисту персональних даних.

Цілком очевидно, що ефективне правове забезпечення захисту персональних даних неможливе без створення надійного теоретичного підґрунтя, зокрема, без вирішення питань про його природу, сутність і визначальні ознаки.

Аналіз провідних доктринальних концепцій, положень інформаційного законодавства та сучасної правозастосовної практики дає змогу розглядати захист персональних даних у трьох аспектах, а саме: а) фундаментальне право людини; б) напрям діяльності; в) інтегральну систему юридичних норм:

захист персональних даних як фундаментальне право – це гарантована суспільством можливість збереження конфіденційності й недоторканності приватного життя людини під час обробки даних, котрі її стосуються;

захист персональних даних як інститут права – це виокремлена в рамках галузі інформаційного права система норм, спрямованих на регулювання суспільних відносин з приводу забезпечення прав людини у сфері обробки інформації персонального характеру (тобто інформації, котра дає змогу ідентифікувати конкретну особу);

захист персональних даних як напрям діяльності – це комплекс правових, організаційних, технічних та інших заходів, спрямованих на забезпечення точності, цілісності та конфіденційності персональних даних у ході їх системної обробки (збирання, накопичення, зберігання, використання, поширення, знищення тощо) юридичними та фізичними особами.

Правові норми з питань захисту персональних даних характеризуються наявністю загального предмета регулювання, використовують імперативний метод регламентації, спрямовуються на досягнення єдиної мети, забезпечують комплексне регулювання правовідносин у сфері захисту персональних даних, формують спеціальний термінологічний апарат, перебувають у тісному взаємозв’язку та системній взаємодії з провідними галузями права, ґрунтуються на спільних принципах (законності, відкритості, доцільності,

адекватності, достовірності, обґрунтованості, конфіденційності, свободи волевиявлення, обов'язкового інформування, збереження персональних даних, заборони на обробку вразливих персональних даних, вільного доступу до власних персональних даних).

Викладене дає підстави стверджувати, що норми про захист персональних даних являють собою комплексний міжгалузевий інститут, який реалізує важливу соціальну функцію та посідає особливе місце у структурі вітчизняного права.

Як свідчить проведений аналіз, вітчизняне інформаційне законодавство нині перебуває у фазі активного розвитку. За останні роки воно неодноразово піддавалось оновленню та ґрунтовним змінам, спрямованим на вдосконалення правових засад захисту персональних даних. Результатом став помітний прогрес у регламентації відповідної сфери суспільних відносин, визначенні правового статусу їх учасників, розбудові механізму публічного адміністрування, вирішенні питань обробки персональних даних, функціонуванні відповідних інформаційних баз, правових гарантій та міжнародного співробітництва.

Водночас фактично всім рівням нормативно-правового забезпечення захисту персональних даних властиві серйозні недоліки. Це і вади понятійного апарату, і фрагментарне регулювання суспільних відносин, і неузгодженість правових вимог, і наявність колізій, і багато інших. Ці недоліки мають взаємопов'язаний характер, що потребує комплексного підходу до їх вирішення. У рамках цього підходу особливу увагу слід приділити гармонізації нормативно-правового матеріалу, усуненню нормативних колізій, прогалин, дублювань і неточностей. Необхідно внести до нормативно-правових актів з питань захисту персональних даних комплекс змін, спрямованих на узгодження їх системи, вдосконалення структури та змісту, імплементацію міжнародних правових стандартів. Обов'язковому скасуванню підлягають нормативно-правові акти, деактуалізовані внаслідок законодавчих, організаційних

та інших перетворень у сфері захисту персональних даних. Перспективним кроком є запровадження постійного моніторингу інформаційного законодавства, який би забезпечив ретельне відстеження його поточних змін, синхронне оновлення всіх його рівнів і складових, кореляцію нормотворчості у сфері захисту персональних даних.

На сучасному етапі розвитку вітчизняна система публічного адміністрування захисту персональних даних характеризується недостатньою ефективністю. У її роботі трапляються численні неузгодженості, паралелізми та внутрішні конфлікти. Її складові функціонують розрізнено, без належного рівня взаємодії й координації. Такий стан справ потребує вжиття комплексу заходів, спрямованих на оптимізацію системи інституційного адміністрування, а також на вдосконалення всіх її ланок і підсистем. У межах цієї мети доцільно:

– внести комплекс законодавчих змін, спрямованих на визначення кола суб'єктів формування та реалізації державної політики у сфері захисту персональних даних, конкретизацію їх правового статусу, чітке розмежування їх функцій, повноважень і меж компетенції;

– організувати розроблення та ухвалення державної цільової програми з питань реалізації політики захисту у сфері персональних даних на загальнодержавному, міжгалузевому/галузевому та місцевому рівнях;

– здійснити чітке розмежування функцій і повноважень суб'єктів публічного адміністрування захисту персональних даних;

– створити у структурі Міністерства юстиції спеціальний підрозділ з питань управління та координації у сфері захисту персональних даних;

– збільшити штатну чисельність ДПЗПД до показників, зумовлених об'єктивними потребами практики.

Імплементація міжнародних правових стандартів у національну інформаційну систему зумовила стрімкий розвиток

форм і методів публічного адміністрування захисту персональних даних. Поряд зі звичними для цієї сфери формами адміністрування (видання правових актів, контроль, нагляд, юрисдикційна діяльність) дедалі частіше застосовують адміністративні договори, що диктує необхідність їх предметного вивчення як у рамках спеціальних наукових досліджень, так і в ході викладання інформаційно-правових дисциплін студентам спеціальності «Правознавство».

Аналіз сучасної практики захисту персональних даних засвідчив тенденцію до поширення позитивних (непримусових) методів адміністрування (заохочення, переконання тощо), які передбачають гармонійне узгодження індивідуальних і публічних інтересів, не обмежують волі учасників правовідносин, ґрунтуються на засадах добровільності, правової свідомості, правової культури та соціальної відповідальності. Цю тенденцію слід враховувати під час розроблення державних цільових програм з інформаційної безпеки. Основу передбачених ними заходів мають становити методи позитивного (непримусового) характеру: інформаційні, роз'яснювальні, виховні та інші.

Попри стале зростання ролі позитивних (непримусових) методів публічного адміністрування, державний примус і надалі відіграє ключову роль у забезпеченні реалізації прав і свобод суб'єктів персональних даних. При цьому з огляду на широту застосування та вагомість результатів основними формами примусу у сфері захисту персональних даних виступають: профілактика правопорушень (як засіб ліквідації передумов і чинників, що сприяють деліктності); припинення (як інструмент виявлення правопорушень, зупинення процесу їх розгортання в часі та мінімізації їх шкідливих наслідків); юридична відповідальність (як репресивна форма реагування на делікт, яка полягає в покладенні спеціальних обтяжень на порушника).

Нині саме ці форми примусу становлять основу інституційного адміністрування і саме на них ґрунтується стабільність вітчизняної системи захисту персональних даних. Доводиться констатувати, що застосування державного примусу у сфері захисту персональних даних пов'язане з широким спектром проблем, зумовлених вадами правової регламентації, організаційними негараздами, браком належного методичного забезпечення та іншими негативними чинниками.

Першочерговими кроками за напрямом їх вирішення мають стати:

– внесення до Закону України «Про захист персональних даних» низки доповнень, спрямованих на забезпечення правової регламентації питань профілактики деліктності у сфері захисту персональних даних. В окремому розділі цього закону мають бути конкретизовані завдання й цілі профілактичної діяльності, основні напрями, форми та методи її здійснення, коло уповноважених суб'єктів та механізми їх системної взаємодії;

– конкретизація повноважень секретаріату уповноваженого Верховної Ради України з прав людини щодо здійснення заходів профілактики правопорушень у сфері захисту персональних даних. Зокрема, в чинному Порядку контролю за додержанням законодавства про захист персональних даних (затвердженого наказом уповноваженого від 8 січня 2014 р. №1/02-14) слід передбачити можливість винесення уповноваженим приписів, спрямованих на запобігання порушенням інформаційного законодавства;

– оптимізація строків складання, надсилання та виконання припису уповноваженого щодо усунення порушень у сфері захисту персональних даних. З цією метою пропонуємо внести до наказу уповноваженого від 8 січня 2014 р. № 1/02-14 такі зміни:

абз. 8 п. 5.11 викласти в такій редакції: *«строк виконання припису (найкоротший строк, достатній для своєчасного (без невиправданих зволікань) припинення порушення та відновлення порушених прав, свобод та інтересів)»;*

п. 5.12 викласти в такій редакції: *«Припис складається у двох примірниках: перший примірник не пізніше трьох робочих днів з дня складання акта перевірки надсилається суб'єкту перевірки чи уповноваженій ним особі рекомендованим листом з повідомленням про вручення, а другий залишається в секретаріаті уповноваженого»;*

у п. 5.13 слова *«(не менш ніж 30 календарних днів)» вилучити;*

– внесення до КУпАП змін, спрямованих на вдосконалення змісту положень, якими визначаються підстави відповідальності за делікти у сфері захисту персональних даних, а саме:

статтю 188-39 КУпАП викласти в такій редакції:

«Стаття 188-39. Порушення встановленого порядку обробки персональних даних

Порушення встановлених правил обробки (збирання, реєстрації, накопичення, зберігання, адаптування, зміни, поновлення, використання, поширення, знеособлення або знищення) персональних даних, а також невиконання законних вимог громадян щодо заборони, зміни або знищення пов'язаних з ними персональних даних, – тягне за собою…

Ті самі дії, вчинені повторно протягом року після накладення адміністративного стягнення, або якщо вони заподіяли шкоду охоронюваним законом правам, свободам та інтересам особи, – тягнуть за собою…

Примітка. Під шкодою у цій статті, якщо вона полягає у заподіянні матеріальних збитків, слід розуміти шкоду на суму від десяти до ста неоподатковуваних мінімумів доходів громадян».

Статтю 212-3 КУпАП викласти в наступній редакції:

«Стаття 212-3 Порушення права на інформацію та права на звернення

Неправомірна відмова в наданні інформації, ненадання інформації, несвоєчасне або неповне надання інформації, надання недостовірної інформації у випадках, коли така інформація підлягає наданню відповідно до чинного законодавства – тягне за собою…

Неправомірне віднесення загальнодоступної інформації до інформації з обмеженим доступом, а також незаконне обмеження права на доступ до інформаційних ресурсів – тягне за собою…

Порушення права особи на доступ до судового рішення або матеріалів юридичної справи – тягне за собою…

Порушення встановленого порядку розгляду звернень громадян – тягне за собою…

Ті самі дії, вчинені повторно протягом року після накладення адміністративного стягнення, або якщо вони заподіяли шкоду охоронюваним законом правам, свободам та інтересам особи, – тягнуть за собою…»;

–комплексний перегляд санкцій, передбачених за делікти у сфері захисту персональних даних на предмет взаємної узгодженості, системного зв'язку, дотримання правил юридичної техніки, адекватності (співмірності) суспільній небезпеці правопорушень, відповідності соціально-економічним умовам сьогодення;

–вдосконалення процесуальних засад відповідальності за правопорушення у сфері обробки та захисту персональних даних, зокрема, закріплення в КУпАП права уповноваженого Верховної Ради України з прав людини складати протоколи у справах про адміністративні правопорушення, передбачені ст.ст. 188-39 та 188-40 КУпАП. З цією метою доповнити ст. 255 КУпАП «Особи, які мають право складати протоколи про

адміністративні правопорушення» п. 2-5 такого змісту: «Уповноважений Верховної Ради України з прав людини, посадові особи секретаріату уповноваженого Верховної Ради України з прав людини». Абзац 40 п. 1 ст. 255 КУпАП – вилучити;

– формування правових засад відповідальності (дисциплінарної, матеріальної) за інформаційні правопорушення у трудовій сфері. Визначення в чинному КЗпП України підстав, умов та заходів відповідальності за порушення вимог щодо обробки персональних даних. Покладення в основу правового регулювання кореспондуючих суспільних відносин принцип взаємної відповідальності працівника і роботодавця;

– регламентація на рівні ЦК України відносин з приводу: поширення конфіденційної інформації сторонами цивільно-правових зобов'язань, обробки персональних даних, які були оприлюднені їх суб'єктом (за його згодою) та перебувають у загальному доступі, використання персональних даних під час здійснення наукових досліджень та створення об'єктів інтелектуальної власності, спадкування права на захист таємниці приватного життя, знищення матеріальних носіїв, які використовуються для незаконного зберігання персональних даних.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки: Закон України від 09.01.2007 № 537-V // Офіційний вісник України. – 2007. – № 8. – Ст. 273.
2. Брижко В.М. Національне агентство з питань інформатизації при Президентові України і проблеми захисту персональних даних в автоматизованих системах / В.М. Брижко, О.А. Баранов // Людина і духовність : зб. наук. пр. – Київ : НДІ «Проблеми людини» Інститут філософії НАН України, 1997. – С. 28–31.
3. Брыжко В.М. Защита персональных данных / А.А. Баранов, В.М. Брыжко, Ю.К. Базанов. – Київ : Национальное агентство по вопросам информатизации при Президенте Украины, 1998. – 128 с.
4. Брыжко В.М. Права человека и защита персональных даннях / В.М. Брыжко, А.А. Баранов, Ю.К. Базанов. – Київ : Національне агентство з питань інформатизації при Президентові України, 2000. – 128 с.
5. Брижко В.М. Персональні дані та право власності / В.М. Брижко // Українське право. – 2002. – № 1. – С. 152–157.
6. Брижко В.М. Правовий механізм захисту персональних даних: монографія / В.М. Брижко ; за заг. ред. М.Я. Швеця та Р.А. Калюжного. – Київ : Парламентське видавництво, 2003. – 120 с.
7. Брижко В.М. Про приєднання України до Конвенції № 108 Ради Європи / В.М. Брижко // Право України. – 2003. – № 1. – С. 34–37.
8. Інформаційне право та правова інформатика у сфері захисту персональних даних / В.М. Брижко, В.М. Гуцалюк, В.С. Цимбалюк та ін. ; за ред. М.Я. Швеця. – Київ : НДЦПІАПрН України, 2005. – 334 с.
9. Брижко В.М. Організаційно-правові питання захисту персональних даних : дис. ... канд. юрид. наук : 12.00.07 / В.М. Брижко. – Київ, 2004. – 252 с.

10. Калюжний Р. Проблеми державної інформаційної політики: гармонізація міжнародного і національного інформаційного права / Р. Калюжний, В. Гавловський, В. Цимбалюк // Правове, нормативне та методологічне забезпечення системи захисту інформації в Україні. – 2001. – №4. – С. 17–21.
11. Інформатизація, право, управління (організаційно-правові питання) / В.Д. Гавловський, Р.А. Калюжний, О.Д. Крупчан [та ін.] – Київ : Ін-Юре, 2002. – 191 с.
12. Інформаційне суспільство / В.М. Брижко, О.М. Гальченко, В.С. Цимбалюк [та ін.] ; за ред. Р.А. Калюжного та М.Я. Швеця. – Київ : Інтеграл, 2002. – 220 с.
13. Калюжний Р. Проблеми захисту прав людини в інформаційній сфері / Р. Калюжний, І. Андросюк // Правова інформатика. – 2004. – № 3. – С. 17–20.
14. Інформаційна безпека України / Л.С. Харченко, В.А. Ліпкан, О.В. Логінов [та ін.] ; за ред. Р.А. Калюжного. – Київ : Текст, 2004. – 136 с.
15. Арістова І.В. Реалізація державної інформаційної політики: інформаційне середовище управління в органах внутрішніх справ України / І.В. Арістова // Вісник Університету внутрішніх справ України. – 1999. – Вип. 9. – С. 405–410.
16. Арістова І.В. Інформаційне суспільство та державна інформаційна політика / І.В. Арістова // Вісник Запорізького юридичного інституту. – 2000. – № 2. – С. 13–20.
17. Арістова І.В. Державна інформаційна політика: організаційно-правові аспекти : монографія / І.В. Арістова; за ред. О.М. Бандурки. – Харків : Вид-во Ун-ту внутрішніх справ, 2000. – 368 с.
18. Арістова І.В. Правове регулювання суспільних інформаційних відносин: стратегія розвитку інформаційного законодавства / І.В. Арістова // Вісн. Університету внутрішніх справ. – 2001. – Вип. 14. – С. 122–128.

19. Арістова І.В. Державна інформаційна політика та її реалізація в діяльності органів внутрішніх справ України: організаційно-правові засади : автореф. дис. … докт. юрид. наук : спец. 12.00.07 / І.В. Арістова. − Харків, 2002. − 39 с.
20. Арістова І.В. Державне управління інформаційною сферою: організаційно-правові засади / І.В. Арістова, О.М. Бандурка // Актуальні проблеми державного управління. – 2002. – № 2. – С. 227–230.
21. Арістова І.В. Органи державного управління інформаційною сферою: концепція розвитку / І.В. Арістова // Вісн. національного університету внутрішніх справ. – 2004. – № 25. – С. 287–292.
22. Гелич Ю.О. Інформаційно-правова сутність таємниці особистого життя людини / Ю.О. Гелич // Актуальні питання кодифікації законодавства України: збірник наукових праць ; за заг. ред. В.О. Зайчука. – Вип. 1. – Київ : Ін-т законодавства Верховної Ради України, 2009. – С. 153–156.
23. Красіков Д.О. Особливості інформаційних правовідносин при побудові інформаційного суспільства / Д.О. Красіков // Право і суспільство. – 2010. – № 6. – С. 142–149.
24. Шевчук О.М. Особливості інформаційних правовідносин при побудові інформаційного суспільства / О.М. Шевчук // Національні інтереси та проблеми забезпечення безпеки України: матер. Всеукр. наук.-практ. конф. (19 березня 2008 року). – Кіровоград : Кіровоградський юридичний інститут, 2008. – С. 66–68.
25. Шевчук О.М. Адміністративно-правове регулювання у сфері забезпечення інформаційної безпеки : дис. ... канд. юрид. наук : 12.00.07 / О.М. Шевчук. – Запоріжжя, 2011. – 210 с.
26. Пазюк А.В. Міжнародно-правовий захист права людини на приватність персоніфікованої інформації : дис. ... канд. юрид. наук : 12.00.11 / А.В. Пазюк. – Київ, 2004. – 207 с.

27. Чернобай А.М. Поняття персональних даних працівника / А.М. Чернобай // Актуальні проблеми держави і права. – 2004. – Вип. 22. – С. 827–833.
28. Чернобай А.М. Становлення та розвиток законодавства України про захист персональних даних працівника / А.М. Чернобай // Підприємництво, господарство і право. – 2005. – №8. – С. 40–43.
29. Чернобай А.М. Цивільно-правова відповідальність за порушення норм, що регулюють обробку і захист персональних даних працівника / А.М. Чернобай // Прокуратура. Людина. Держава. – 2005. – № 7. – С. 95–101.
30. Чернобай А.М. Кримінальна та адміністративна відповідальність за порушення норм, що регулюють обробку і захист персональних даних працівника / А.М. Чернобай // Прокуратура. Людина. Держава. – 2005. – № 10. – С. 93–99.
31. Ясечко С.В. Правовий режим інформації з обмеженим доступом у цивільному праві / С.В. Ясечко // Підприємництво, господарство і право. – 2010. – Вип. 8. – С. 105–108.
32. Ясечко С. В. Інформація як об’єкт цивільного права / С.В. Ясечко // Господарсько-правове, цивільно-правове та фінансово-правове забезпечення розвитку сучасної економіки України : зб. доп. та тез повідомлень учасників цивільно-правової секції всеукр. наук.-практ. конф. (м. Донецьк, 14 листоп. 2008 р.). – Донецьк, 2008. – С. 193–195.
33. Ясечко С. В. Цивільно-правова відповідальність за порушення прав на інформацію з обмеженим доступом / С.В. Ясечко // Проблеми цивільного права та процесу: матеріали міжнар. наук.-практ. конф., присвяченої пам’яті проф. О.А. Пушкіна, 22 трав. 2010 р. – Харків : ХНУВС, 2010. – С. 164–166.
34. Чернобай А.М. Правові засоби захисту персональних даних працівника: дис. ... канд. юрид. наук : 12.00.05 / А.М. Чернобай. – Одеса, 2006. – 200 с.

35. Ясечко С.В. Цивільно-правова відповідальність за порушення права на інформацію : дис. ... канд. юрид. наук: 12.00.03 / С.В. Ясечко. – Харків : 2011. – 224 с.
36. Тунік А.В. Захист персональних даних: аналіз вітчизняного законодавства / А.В. Тунік // Підприємництво, господарство і право. – 2011. – № 8. – С. 97–100.
37. Тунік А.В. Міжнародно-правові стандарти захисту інформації про особу: стан та перспективи / А.В. Тунік // Підприємництво, господарство і право. – 2012. – № 1. – С. 131–134.
38. Тунік А.В. Захист інформації про особу (персональних даних) в окремих країнах ЄС / А.В. Тунік // Правова інформатика. – 2012. – № 1 (33). – С. 54–59.
39. Тунік А.В. Тенденції розвитку законодавства у сфері захисту персональних даних / А.В. Тунік, К.Г. Татарникова // Інформаційні стратегії в глобальному управлінні: матер. міжнар. наук.-практ. конф. (Київ, 29 жовтня 2011 р.). – Київ : ФОП Ліпкан О.С., 2011. – С. 65–67.
40. Тунік А.В. Правові основи захисту персональних даних : дис. ... канд. юрид. наук : 12.00.07 / А.В. Тунік. – Київ, 2012. – 229 с.
41. Гелич Ю.О. Таємниця особистого життя людини як інститут інформаційного права України / Ю.О. Гелич // Бюлетень Міністерства юстиції України. – 2009. – № 11 (97). – С. 91–98.
42. Гелич Ю.О. Принципи гарантування таємниці особистого життя людини в інформаційному праві України / Ю.О. Гелич // Правничий вісник Університету «Крок». – 2010. – № 5. – С. 111–118.
43. Сивухін В.С. Право на недоторканність особистого життя / В.С. Сивухін // Науковий вісник Національної академії державної податкової служби України. – 2002. – № 2 (16). – С. 274–279.
44. Сивухін В.С. Державний реєстр і недоторканність особистого життя платників податків / В.С. Сивухін // Науковий вісник Національної академії державної податкової служби України. – 2003. – № 4 (2). – С. 211–216.

45. Серьогін В.О. Право на недоторканність приватного життя (прайвесі) у конституційно-правовій теорії та практиці : монографія / В.О. Серьогін. – Харків : ФІНН. – 608 с.
46. Тихомиров О.О. Забезпечення інформаційної безпеки як функція держави : дис. ... канд. юрид. наук : 12.00.01 / О.О. Тихомиров. – Київ, 2011. – 234 с.
47. Сопілко І.М. Правові підстави для отримання органами державної влади України інформації / І.М. Сопілко // Часопис Київського університету права. – 2009. – № 1. – С. 135–142.
48. Сопілко І.М. Підходи до класифікації інформації, яку можуть отримувати органи державної влади України / І.М. Сопілко // Підприємництво, господарство і право. – 2009. – № 6. – С. 60–64.
49. Олійник О.В. Захист інформації в умовах інформаційного суспільства / О.В. Олійник // Право України. – 2005. – № 10. – С. 100–103.
50. Олійник О.В. Проблеми удосконалення захисту інформаційних ресурсів у процесі розширення міждержавного співробітництва / О.В. Олійник // Юридична Україна. – 2005. – № 11. – С. 50–56.
51. Горпинюк О.П. Кримінально-правова охорона приватності в іноземних державах / О.П. Горпинюк // Часопис Академії адвокатури України. – 2009. – № 4 (5) [Електронний ресурс]. – Режим доступу : http://www.nbuv.gov.ua/e-journals/Chaau/2009-4/09goppid.pdf
52. Горпинюк О. П. Інформація як предмет складів злочинів, що посягають на приватність / О.П. Горпинюк // Форум права. – 2010. – № 4. – С. 229–234 [Електронний ресурс]. – Режим доступу : http://www.nbuv.gov.ua/e-journals /FP/2010-4/10goppnp.pdf
53. Горпинюк О.П. Кримінальна відповідальність за розголошення конфіденційної інформації про особу, якщо інформація стала відома у зв'язку зі службовою чи професійною діяльністю за кримінальним законодавством України / О.П. Горпинюк // Порівняльне правознавство: загальнотеоретичні та галузеві аспекти: тези доповідей

учасників круглого столу 22 травня 2009 р. – Львів : ЛьвДУВС, 2009. – С. 48–50.
54. Дем'яненко Ю.І. Кримінальна відповідальність за порушення недоторканності приватного життя : дис. ... канд. юрид. наук : 12.00.08 / Ю.І. Дем'яненко. – Харків, 2008. – 242 с.
55. Баскаков В.Ю. Захист інформації з обмеженим доступом: розвиток вітчизняного законодавства / В.Ю. Баскаков // Підприємництво, господарство і право. – 2011. – № 4. – С. 126–128.
56. Баскаков В.Ю. Адміністративно-правовий режим інформації з обмеженим доступом : дис. ... канд. юрид. наук : 12.00.07 / В.Ю. Баскаков. – Київ, 2012. – 194 с.
57. Березовська І.Р. Адміністративно-правове регулювання інформаційної взаємодії органів виконавчої влади з громадянами: постановка проблеми / І.Р. Березовська // Наукові записки ЛУБП. – 2010. – Вип. 5. – С. 206–208.
59. Березовська І.Р. Адміністративно-правова відповідальність у сфері забезпечення інформаційної безпеки: постановка проблеми / І.Р. Березовська, М. Микитюк // Наукові записки ЛУБП. – 2011. – Вип. № 6. – С. 146–150.
59. Линник Г.М. Принципи адміністративно-правового регулювання інформаційної безпеки України / Г.М. Линник // Підприємництво, господарство і право. – 2010. – № 5. – С. 93–97.
60. Линник Г.М. Особливості адміністративних правопорушень інформаційного характеру / Г.М. Линник // Підприємництво, господарство і право. – 2010. – № 7. – С. 69–72.
61. Туранин В.Ю. Сущность и значение дефиниции в современном законодательном тексте / В.Ю. Туранин // Современное право. – 2006. – № 5. – С. 43–48.
62. Нашиц А. Правотворчество. Теория и законодательная техника / А. Нашиц ; под ред. Д.А. Керимова. – М. : Прогресс, 1974. – 256 с.

63. Возинцев А.С. Правовая защита персональных данных : монография / А.С. Возинцев. – М. : Изд-во МНАУ, 1995. – 244 с.
64. Козак В. Защита персональных данных в Украине: практика и проблемы / В. Козак // Персональные данные. – 2013. – № 7 (60).
65. Копылов В.А. Информационная безопасность и информационное законодательство / В.А. Копылов, А.В. Волокитин // Сборник НТИ. Серия 1. Организация и методика информационной работы. – 1996. – № 7. – С. 11–14.
66. Волошенюк С.Н. Собственность на информацию и защита информации / С.Н. Волошенюк // Сборник НТИ. Серия 1. Организация и методика информационной работы. – 1999. – № 5. – С. 9–12.
67. Соколова О.С. Административно-правовые режимы защиты конфиденциальной информации : дисс. ... канд. юрид. наук : 12.00.14 / О.С. Соколова. – СПб., 2005. – 212 с.
68. Вельдер И.А. Система правовой защиты персональных данных в Европейском Союзе: дисс. ... канд. юрид. наук : 12.00.10 / И.А. Вельдер. – Казань, 2006. – 165 с.
69. Федосин А.С. Защита конституционного права человека и гражданина на неприкосновенность частной жизни при автоматизированной обработке персональных данных в Российской Федерации : дисс. ... канд. юрид. наук : 12.00.14 / А.С. Федосин. – Саранск, 2009. – 191 с.
70. Баранов А.А. Права человека и защита персональных данных / А.А. Баранов, В.М. Брыжко, Ю.К. Базанов. – Київ, 2000. – 278 с.
71. Солодухин О.А. Логик : учебник / О.А. Солодухин ; под ред. В.А. Бочарова. – Ростов-на-Дону : Феникс, 2000. – 384 с.
72. Кириллов В.И. Логика : учебник / В.И. Кириллов, А.А. Старченко. – М. : Юристъ, 2001. – 256 с.
73. Кобзарь В.И. Логика : учебное пособие для студентов гуманитарных факультетов / В.И. Кобзарь. – СПб. : Изд-во СПГУ, 2001. – 175 с.

74. Тымцяс В.Г. Логика: курс лекций / В.Г. Тымцяс. – М. : ПРИОР, 1999. – 160 с.
75. Гуржій Т.О. Концептуальні засади розуміння джерел права / Т.О. Гуржій // Публічне право. – 2012. – № 2(6). – С. 247–252.
76. Курс адміністративного права України : підручник / В.К. Колпаков, О.В. Кузьменко, І.Д. Пастух [та ін.]. – Київ : Юрінком Інтер, 2013. – 872 с.
77. Тимошенко И.В. Административная ответственность : учеб. пособие / И.В. Тимошенко. – М. : 2004. – 288 с.
78. Цивільне право України : підручник / Д.В. Боброва, О.В. Дзера, А.С. Довгерт [та ін.]; за ред. О.В Дзери, Н.С. Кузнєцової. – Київ : Юрінком Інтер, 2005. – Ч. І. – 736 с.
79. Гражданское право : учебник / Е.Ю. Валявина, Н.П. Василевская, Н.Д. Егоров [и др.] ; под ред. А.П. Сергеева, Ю.К. Толстого. – М. : Проспект, 1998. – Ч. ІІ. – 784 с.
80. Магомедов М.А. Уголовная ответственность как институт публичного права : автореф. дисс. … канд. юрид. наук : спец. 12.00.07 / М.А. Магомедов. – М., 2004. – 28 с.
81. Миронов В.И. Трудовое право России : учебник / В.И. Миронов. – М. : Управление персоналом, 2005. – 1149 с.
82. Ерофеев Б.В. Земельное право России : учебник / Б.В. Ерофеев. – М. : Юрайт-Издат, 2004. – 656 с.
83. Кайль А.Н. Комментарий к Федеральному закону от 27 июля 2006 года № 152-ФЗ «О персональных данных» (постатейный) / А.Н. Кайль, Е.А. Новиков // Информационный портал «Консультант-плюс» [Електронний ресурс]. – Режим доступу : http://base.consultant.ru/cons/ cgi/online.cgi?req=doc; base=CMB;n=17445;dst=0
84. Конвенція Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних від 28 січня 1981 року // Офіційний вісник України. – 2011. – № 1. – С. 1994.
85. Directive 95/46/EC Of The European Parliament And Of The Council of 24 October 1995 «On the protection of individuals with regard to the processing of personal data and on the free movement of such data» // Official Journal. – L 281, 23/11/1995. – P. 31–50.

86. Data Protection Act 1998 (DPA) – London : Ministry of Justice, 2013. – 24 p.
87. Act of 29 August 1997 on the Protection of Personal Data // Journal of Laws. – 2002. – № 101. – it. 926.
88. Талапина Э.В. Правовая защита персональных данных во Франции / Э.В. Талапина // Журнал высшей школы экономики. Серия: Право. – 2012. – № 4. – С. 152–162.
89. Про ратифікацію Страсбурзької Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних : Закон України від 01.01.2014 // Відом. Верховної Ради України. – 2010. – № 46. – С. 542.
90. Про захист персональних даних : Закон України від 06.07.2010 № 2438-VI // Відом. Верховної Ради України. – 2010. – №34. – С. 481.
91. Алексеев С.С. Общая теория права / С.С. Алексеев. – М. : Юрид. лит., 1981. – Т. 1. – 523 с.
92. Малеин Н.С. Охрана прав личности советским законодательством / Н.С. Малеин. – М. : Наука, 1985. – 128 с.
93. Смирнов А.П. Соотношение понятий «охрана прав» и «защита прав» / А.П. Смирнов // Вестник Томского государственного университета. – 2010. – № 331. – С. 123–125.
94. Московченко Ю.С. Административно-правовая охрана политических прав граждан России : дисс. ... канд. юрид. наук : 12.00.14 / Ю.С. Московченко. – М., 2006. – 172 с.
95. Матузов Н.И. Правовая система и личность / Н.И. Матузов. – Саратов : Изд-во Сарат. ун-та, 1987. – 214 с.
96. Гаврилов Э.П. Комментарий Закона РФ «Об авторском праве и смежных правах» / Э.П. Гаврилов. – М. : Правовая культура, 1996. – 250 с.
97. Макарова З.В. Защита в российском уголовном процессе: понятие, виды, предмет и пределы / З.В. Макарова // Правоведение. – 2000. – № 3. – С. 217–231.
98. Общая теория права: курс лекций / В.К. Бабаев, В.М. Баранов, П.П. Баранов [и др.] ; под общ. ред. В.К. Бабаева. – Нижний Новгород : Изд. Нижегор. ВШ МВД РФ, 1993. – 544 с.

99. Про схвалення Стратегії розвитку інформаційного суспільства в Україні : Розпорядження Кабінету Міністрів України від 15 травня 2013 р. № 386-р // Офіційний вісник України. – 2013. – № 44. – С. 1581.
100. Марущак А.І. Інформаційне право: Доступ до інформації : навч. посіб. / А.І. Марущак. – Київ : КНТ, 2007. – 532 с.
101. Маркевич А.С. Организационно-правовая защита персональных данных в служебных и трудовых отношениях : дисс. ... канд. юрид. наук : 05.13.19 / А.С. Маркевич. – Воронеж, 2006. – 170 с.
102. Дворецький А.В. Защита персональных данных работника по законодательству Российской Федерации : дисс. ... канд. юрид. наук : 12.00.05 / А.В. Дворецкий. – Томск, 2006. – 223 с.
103. Матузов Н.И. Теория государства и права / Н.И. Матузов, А.В. Малько. – М. : Юристъ, 2005. – 541 с.
104. Киримова Е.А. Правовой институт: понятие и виды : учеб. пособие / Е.А. Керимова. – Саратов : Саратов. гос. акад. права. – 2000. – 55 с.
105. Якушев В.С. О понятии правового института / В.С. Якушев // Правоведение. – 1970. – №6. – С. 61–67.
106. Матузов Н.И. Теория государства и права / Н.И. Матузов, А.В. Малько. – М. : Юристъ, 2002. – 512 с.
107. Лаптев В.В. Цели правового регулирования и система права / В.В. Лаптев, В.П. Шахматов // Правоведение. – 1976. – № 4. – С. 26–35.
108. Черданцев А.Ф. Толкование советского права / А.Ф. Черданцев. – М. : Юрид. лит., 1979. – 168 с.
109. Алексеев С.С. Структура советского права : монография / С.С. Алексеев. – М. : Юрид. лит., 1975. – 264 с.
110. Серьогін В.О. Конституційне право особи на недоторканність приватного життя (прайвесі): проблеми теорії та практики : дис. ... докт. юрид. наук : 12.00.01, 12.00.02 / В.О. Серьогін. – Харків, 2011. – 432 с.
111. Інформаційне право та правова інформатика у сфері захисту персональних даних : монографія / [В. Брижко, М. Гуцалюк, В. Цимбалюк, М. Швець] ; за ред. М. Швеця. – Київ : НДЦПІ АПрН України, 2006. – 450 с.

112. Simitis S. Reconsidering the Premises of Labour Law: Prolegomena to an EU Regulation on the Protection of Employees' Personal Data / Spiros Simitis // European Law Journal, Oxford. – 1999. – Vol. 5. – №1. – P. 45–62.
113. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. – Paris : OECD, 1981. – 41 p.
114. Directive 2002/58/EC Of The European Parliament And Of The Council of of 12 July 2002 «On privacy and electronic communications» // Official Journal. – L 201, 31/7/2002. – P. 37.
115. EU Proposal for a Regulation 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 from 25.01.2012. COM(2012)0011 – 2012/0011(COD). – Strasburg : Committee on Industry, Research and Energy, 2012. – 118 p.
116. Конституція України // Відомості Верховної Ради України. – 1996. – № 30. – С. 141.
117. Рішення Конституційного Суду України від 20 січня 2012 року № 2-рп/2012 // Вісн. Конституційного Суду України. – 2012. – № 2. – С. 14.
118. Про інформацію : Закон України // Відом. Верховної Ради України. – 1992. – № 48. – С. 650.
119. Про міліцію : Закон України від 20.12.1990 № 565-XII // Відом. Верховної Ради УРСР. – 1991. – № 4. – С. 20.
120. Про захист прав споживачів : Закон України від 15.12.93 № 3682-XII // Відом. Верховної Ради УРСР. – 1991. – №30. – С. 379.
121. Про всеукраїнський перепис населення : Закон України від 19.10.2000 № 2058-III // Відом. Верховної Ради України. – 2000. – № 51. – С. 446.
122. Про платіжні системи та переказ коштів в Україні : Закон України від 05.04.2001 № 2346-III // Відом. Верховної Ради України. – 2001. – № 29. – С. 137.
123. Про електронний цифровий підпис : Закон України від 22.05.2003 № 852-IV // Офіційний вісник України. – 2003. – № 25. – С. 1175.

124. Про телекомунікації : Закон України від 18.11.2003 № 1280-IV // Офіційний вісник України. – 2003. – № 51. – Т. 1. – С. 2644.
125. Про свободу пересування та вільний вибір місця проживання в Україні : Закон України від 11.12.2003 № 1382-IV // Офіційний вісник України. – 2004. – № 1. – С. 4.
126. Про державний реєстр виборців : Закон України від 22.02.2007 № 698-V // Відомості Верховної Ради України. – 2007. – №20. – С. 282.
127. Про державний земельний кадастр : Закон України від 07.07.2011 № 3613-VI // Офіційний вісник України. – 2011. – № 60. – С. 2405.
128. Про державну службу : Закон України від 16.12.1993 № 3723-XII // Офіційний вісник України. – 2012. – № 4. – С. 115.
129. Про систему гарантування вкладів фізичних осіб : Закон України від 23.02.2012 № 4452-VI // Офіційний вісник України. – 2012. – № 22. – С. 824.
130. Про охоронну діяльність : Закон України від 22.03.2012 № 4616-VI // Офіційний вісник України. – 2012. – № 30. – С. 1099.
131. Про громадські об'єднання : Закон України від 22.03.2012 № 4572-VI // Офіційний вісник України. – 2012. – № 30. – С. 1097.
132. Про адвокатуру та адвокатську діяльність : Закон України від 05.07.2012 № 5076-VI // Офіційний вісник України. – 2012. – № 62. – С. 2509.
133. Про екстрену медичну допомогу : Закон України від 05.07.2012 № 5081-VI // Офіційний вісник України. – 2012. – № 63. – С. 2570.
134. Про зайнятість населення : Закон України від 05.07.2012 № 5067-VI // Офіційний вісник України. – 2012. – № 63. – С. 2565.
135. Про адміністративні послуги : Закон України від 06.09.2012 № 5 203-VI // Офіційний вісник України. – 2012. – № 76. – С. 3067.

136. Кримінальний кодекс України // Відом. Верховної Ради України. – 2001. – № 25–26. – С. 131.
137. Цивільний кодекс України // Відом. Верховної Ради України. – 2003. – № 40–44. – С. 356.
138. Кодекс України про адміністративні правопорушення // Відом. Верховної Ради Української РСР. – 1984. – Дод. до № 51. – С. 1122.
139. Скулиш Є.Д. Новели інформаційного законодавства України: проблеми теорії та практики / Є.Д. Скулиш, А.І. Марущак // Інформаційна безпека людини, суспільства, держави. – 2011. – № 1 (5). – С. 7–12.
140. Обуховська Т.І. Персональні дані: теорія та реальність / Т.І. Обуховська, В.П. Шуляк // Електронне урядування. – 2011. – № 2. – С. 76–88.
141. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. – Strasburg : European Council, 1981. – 10 p.
142. Усенко І. Коментар до Закону України «Про захист персональних даних» // «Права людини в Україні» Інформаційний портал Харківської правозахисної групи» [Електронний ресурс]. – Режим доступу : http://khpg.org/index.php?id=1330343937
143. Большой энциклопедический словарь / сост. И. Лапина, Е. Маталина, Р. Секачев и др. – М. : Астрель, 2002. – 1248 с.
144. Аналіз і коментарі до змін до Закону України «Про захист персональних даних» / М. Жорж, Г. Саттон. – Страсбург, 2012. – 71 с.
145. Про внесення змін до деяких законодавчих актів України щодо удосконалення системи захисту персональних даних : Закон України // Офіційний вісник України. – 2013. – № 57. – С. 2046.
146. Про судоустрій і статус суддів : Закон України від 07.07.2010 № 2453-VI // Офіційний вісник України. – 2010. – № 55/1. – С. 1900.

147. Шестаков В. Защита персональных данных в Украине: эволюция правового регулирования / В. Шестаков, Л. Чернявский // Руководство директора по персоналу. – 2013. – № 2. – С. 13–18.
148. Пекар В. Європейська інтеграція чи нова загроза підприємцям? / В. Пекар // Веб-сайт Українського союзу промисловців і підприємців [Електронний ресурс]. – Режим доступу : http://www.uspp.org.ua/interview/9.vropeyska-integraciya-chi-nova-zagroza-pidprimcyam.htm&print
149. Одинець О. Захист персональних даних: доведеться відповідати / О. Одинець // Правовий тиждень. – 2001. – № 20–21. – С. 6.
150. Указ Президента України від 6 грудня 2001 року № 1193/2001 «Про рішення Ради національної безпеки і оборони України» від 31 жовтня 2001 року «Про заходи щодо вдосконалення державної інформаційної політики та забезпечення інформаційної безпеки України» // Офіційний вісник України. – 2001. – № 50. – С. 2228.
151. Про доктрину інформаційної безпеки України : Указ Президента України від 8 липня 2009 року № 514/2009 // Офіційний вісник Президента України. – 2009. – № 20. – С. 677.
152. Про затвердження Річної національної програми співробітництва Україна – НАТО на 2011 рік : Указ Президента України від 13 квітня 2011 року № 468/2011 // Офіційний вісник України. – 2011. – № 12. – С. 634.
153. Про Національний план з виконання Плану дій щодо лібералізації Європейським Союзом візового режиму для України : Указ Президента України від 22 квітня 2011 року № 1121/2007 // Офіційний вісник Президента України. – 2011. – № 13. – С. 657.
154. Про Національний план дій на 2013 рік щодо впровадження Програми економічних реформ на 2010–2014 роки «Заможне суспільство, конкурентоспроможна економіка, ефективна держава» : Указ Президента України від 12 березня 2013 року № 128/2013 // Офіційний вісник Президента України. – 2013. – № 7 (спеціальний випуск). – С. 249.

155. Возиянов А.А. Неопарадигма нациобезопасности : монография / А.А. Возиянов. – СПб. : Акт, 2009. – 421 с.
156. Про затвердження Положення про Державну інформаційну систему електронних звернень громадян : Постанова Кабінету Міністрів України від 25 грудня 2013 р. № 958 // Офіційний вісник України. – 2014. – № 4. – С. 104.
157. Про затвердження Порядку реєстрації, перереєстрації безробітних та ведення обліку осіб, які шукають роботу : Постанова Кабінету Міністрів України від 20 березня 2013 р. № 198 // Офіційний вісник України. – 2013. – № 26. – С. 859.
158. Про затвердження Порядку ведення Єдиного державного порталу адміністративних послуг : Постанова Кабінету Міністрів України від 3 січня 2013 р. № 13 // Офіційний вісник України. – 2013. – № 4. – С. 109.
159. Про затвердження Положення про електронний реєстр пацієнтів : Постанова Кабінету Міністрів України від 6 червня 2012 р. № 546 // Офіційний вісник України. – 2012. – № 47. – С. 1232.
160. Про затвердження Положення про створення та функціонування Єдиного державного реєстру злочинів торгівлі людьми : Постанова Кабінету Міністрів України від 18 квітня 2012 р. № 303 // Офіційний вісник України. – 2012. – № 30. – С. 1112.
161. Про створення Єдиної державної електронної бази з питань освіти : Постанова Кабінету Міністрів України від 13 липня 2011 р. № 752 // Офіційний вісник України. – 2011. – № 55. – С. 2191.
162. Про затвердження Положення про Державний реєстр баз персональних даних та порядок його ведення : Постанова Кабінету Міністрів України від 25 травня 2011 р. № 616 // Офіційний вісник України. – 2011. – № 45. – С. 1833.
163. Про затвердження Положення про Міністерство юстиції України : Постанова Кабінету Міністрів України від 2 липня 2014 року № 228 // Офіційний вісник України. – 2014. – № 54. – С. 1455.

164. Про затвердження Примірного положення про центр надання адміністративних послуг : Постанова Кабінету Міністрів України від 20 лютого 2013 року № 118 // Офіційний вісник України. – 2013. – № 16. – С. 557.
165. Про затвердження Загального положення про центр соціальних служб для сім'ї, дітей та молоді : Постанова Кабінету Міністрів України від 1 серпня 2013 року № 573 // Офіційний вісник України. – 2013. – № 66. – С. 2381.
166. Про затвердження Типового положення про структурний підрозділ місцевої державної адміністрації : Постанова Кабінету Міністрів України від 26 вересня 2012 року № 887 // Офіційний вісник України. – 2012. – № 73. – С. 2941.
167. Про внесення змін до деяких законодавчих актів України щодо удосконалення системи захисту персональних даних: Закон України // Офіційний вісник України. – 2013. – №57. – С. 2046.
168. Про затвердження Порядку обробки персональних даних у базі персональних даних «Електронний журнал обліку запитів на публічну інформацію» : Наказ МВС України від 21 серпня 2013 року № 805 // Офіційний вісник України. – 2013. – № 75. – С. 2797.
169. Про внесення змін до деяких законодавчих актів України щодо удосконалення системи захисту персональних даних : Закон України // Офіційний вісник України. – 2013. – № 57. – С. 2046.
170. Про затвердження Порядку обробки персональних даних у базі персональних даних «Працівники» Національної комісії, що здійснює державне регулювання у сфері комунальних послуг : Постанова Національної комісії, що здійснює державне регулювання у сфері комунальних послуг від 9 серпня 2013 року № 109 // Офіційний вісник України. – 2013. – № 67. – С. 2459.
171. Про затвердження Порядку обробки персональних даних у базі персональних даних НКРЕ : Постанова Національної комісії, що здійснює державне регулювання у сфері енергетики від 17 січня 2013 року № 20 // Офіційний вісник України. – 2013. – № 15. – С. 540.

172. Про затвердження Типового порядку обробки персональних даних у базах персональних даних : Наказ Міністерства юстиції України від 30 грудня 2011 року № 3659/5 // Офіційний вісник України. – 2012. – № 3. – С. 104.
173. Про місцеве самоврядування : Закон України від 21.05.1997 № 280/97-ВР // Відом. Верховної Ради України. – 1997. – № 24. – С. 170.
174. Про місцеві державні адміністрації : Закон України від 09.04.1999 № 586-XIV // Відом. Верховної Ради України. – 1999. – № 190. – С. 20–21.
175. Про затвердження Типового положення про територіальні органи міністерства та іншого центрального органу виконавчої влади : Постанова Кабінету Міністрів України від 25 травня 2011 р. № 563 // Офіційний вісник України. – 2011. – № 41. – С. 1677.
176. Про затвердження форм заяв про реєстрацію бази персональних даних та про внесення змін до відомостей Державного реєстру баз персональних даних і порядку їх подання : Наказ Міністерства юстиції України від 8 липня 2011 року № 1824/5 // Офіційний вісник України. – 2013. – № 97. – С. 3600.
177. Мосянин С.А. Принципы публичного администрирования / С.А. Мосянин // Управление и право. – 2005. – № 3. – С. 31–39.
178. Алексеева Н.С. Зарубежный опыт публичного администрирования : монография / Н.С. Алексеева. – М. : МТУ, 2010. – 288 с.
179. Про Уповноваженого Верховної Ради України з прав людини : Закон України // Офіційний вісник України. – 1998. – № 1. – С. 5.
180. Про Кабінет Міністрів України: Закон України від 27.02.2014 №794-VII // Офіційний вісник України. – 2014. – №20. – С. 619.
181. Про затвердження Положення про регіональні представництва Уповноваженого Верховної Ради України з прав людини : Наказ Уповноваженого Верховної Ради України з прав людини від 19 лютого 2013 року № 14/02-13 //

Офіційний портал Верховної Ради України [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/v4_02715-13

182. Про затвердження Положення про представників Уповноваженого Верховної Ради України з прав людини : Наказ уповноваженого Верховної Ради України з прав людини від 6 липня 2012 року № 7/8-12 // Офіційний веб-портал Верховної Ради України [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/v07_8715-12
183. Про затвердження Положення про Секретаріат Уповноваженого Верховної Ради України з прав людини : Наказ Уповноваженого Верховної Ради України з прав людини від 20 червня 2012 року №4/8-12 // Офіційний веб-портал Верховної Ради України [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/v04_8715-12
184. Про затвердження документів у сфері захисту персональних даних : Наказ Уповноваженого Верховної Ради України з прав людини від 8 січня 2014 року № 1/02-14 // Бізнес-Бухгалтерія-Право. Податки. Консультації. – 2014. – № 9. – С. 14.
185. Алексеев С.С. Методологические основы научно-правовых исследований : научное пособие / С.С. Алексеев. – М. : Юрид. лит., 1981. – 212 с.
186. Курс адміністративного права України : підручник / В.К. Колпаков, О.В. Кузьменко, І.Д. Пастух [та ін.] ; за ред. В.В. Коваленка. – Київ : Юрінком Інтер, 2012. – 808 с.
187. Публічне адміністрування в Україні : навч. посіб. / В.Б. Дзюндзюк, Н.М. Мельтюхова, Н.В. Фоміцька [та ін.] ; за заг. ред. В.В. Корженка та Н.М. Мельтюхової. − Харків : Магістр, 2011. – 306 с.
188. Гуржій Т.О. Адміністративне право України : навч. посіб. / Т.О. Гуржій. – Київ : КНТ, 2011. – 680 с.
189. Адміністративне право України. Академічний курс / Т.О. Коломоєць, С.В. Ващенко, В.Г. Поліщук ; за ред. Т.О. Коломоєць. – Київ : Юрінком-Інтер, 2011. – 574 с.

190. Адміністративне право : підручник / Ю.П. Битяк, В.М. Гаращук, В.В. Богуцький [та ін.] ; за заг. ред. Ю.П. Битяка, В.М. Гаращука, В.В. Зуй. – Харків : Право, 2010. – 624 с.
191. Філософський словник / за ред. В.І. Шинкарука. – Київ : Головна редакція УРЕ, 1973. – 600 с.
192. Звіт про діяльність ДСЗПД України в І півріччі 2014 року // Офіційний сайт Державної служби України з питань захисту персональних даних [Електронний ресурс] – Режим доступу : http://zpd.gov.ua/dszpd/uk/publish/article/68655
193. Про затвердження Порядку здійснення Державною службою України з питань захисту персональних даних державного контролю за додержанням законодавства про захист персональних даних : Наказ Міністерства юстиції України від 26 червня 2012 року № 947/5 // Офіційний вісник України. – 2012. – № 51. – С. 2045.
194. Звіт про виконання Державною службою України з питань захисту персональних даних завдань у 2012 році // Офіційний сайт Державної служби України з питань захисту персональних даних [Електронний ресурс]. – Режим доступу : http://zpd.gov.ua/dszpd/uk/publish/article/50865
195. Звіт про виконання покладених на ДСЗПД України завдань у 2013 році // Офіційний сайт Державної служби України з питань захисту персональних даних [Електронний ресурс]. – Режим доступу : http://zpd.gov.ua/dszpd/uk/publish/article/65152
196. Про Порядок надання електронної копії бази даних Державного реєстру виборців представнику політичної партії для здійснення політичною партією публічного контролю за веденням Державного реєстру виборців : Постанова Центральної виборчої комісії від 15 листопада 2010 року № 516 [Електронний ресурс]. – Режим доступу : http://zakon1.rada.gov.ua/laws/show/v0516359-10
197. Игнатов А.С. Защита персональных данных: проблемы и пути их решения / А.С. Игнатов // Общество. Информация. Право. – 2010. – № 5. – С. 54–63.

198. Амелин Р.В. О правовых принципах разработки государственных АИС, обрабатывающих персональные данные / Р.В. Амелин // Информационное право. – 2009. – № 2. – С. 32–35.
199. Стефанишина С.Н. Актуальные проблемы борьбы з правонарушениями в сфере защиты персональных данных / С.Н. Стефанишина // Законность и порядок. – 2013. – № 2. – С. 25–34.
200. Про схвалення Концепції створення єдиної інформаційно-аналітичної системи управління міграційними процесами : Розпорядження Кабінету Міністрів України від 7 листопада 2012 року № 870-р // Офіційний вісник України. – 2012. – № 85. – С. 3469.
201. Про схвалення Концепції створення та функціонування інформаційної системи електронної взаємодії державних електронних інформаційних ресурсів : Розпорядження Кабінету Міністрів України від 5 вересня 2012 року № 634-р // Офіційний вісник України. – 2012. – № 67. – С. 2753.
202. Про внесення змін до деяких законодавчих актів України щодо посилення відповідальності за порушення законодавства про захист персональних даних : Закон України // Офіційний вісник України. – 2011. – №48. – С. 1954.
203. Про внесення змін до деяких законів України щодо діяльності Уповноваженого Верховної Ради України з прав людини у сфері захисту персональних даних : Закон України // Офіційний вісник України. – 2014. – № 44. – С. 1161.
204. Возинцев А.С. Правовые и организационные аспекты защиты персональных данных : монография / А.С. Возинцев. – СПб. : Фомальгаут, 2007. – 202 с.
205. Словник української мови: в 11 т. / О.Є. Марцинківська, Л.О. Родніна, В.М. Русанівський [та ін.] ; за ред. І.К. Білодіда. – Київ : Наук. думка, 1976. – Т. 7. – 723 с.
206. Кодекс адміністративного судочинства України // Офіційний вісник України. – 2005. – № 32. – С. 1918.

207. Цивільний процесуальний кодекс України // Офіційний вісник України. – 2004. – № 16. – С. 1087.
208. Кримінальний процесуальний кодекс України // Відом. Верховної Ради України. – 2013. – № 9–10, № 11–12, № 13. – С. 88.
209. Укрзалізницею виконано вимоги припису ДСЗПД України // Офіційний сайт Державної служби України з питань захисту персональних даних [Електронний ресурс]. – Режим доступу : http://zpd.gov.ua/dszpd/uk/publish/article/64463;jsessionid=42C6519EBAD7A8F3117218BB82786E50
210. Марчук В.М. Теорія держави і права : навч. посіб. / В.М. Марчук, О.В. Корольков. – Київ : Вид. КНТЕУ, 2012. – 416 с.
211. Скакун О.Ф. Теорія держави і права : підручник / О.Ф. Скакун. – Київ : Алерта, 2009. – 520 с.
212. Григорьева И.В. Теория государства и права : учеб. пособие / И.В. Григорьева. – Тамбов : Изд. ТГТУ, 2009. – 304 с.
213. Попередні підсумки здійснення ДСЗПД України функцій контролю за додержанням вимог законодавства про захист персональних даних [Електронний ресурс]. – Режим доступу : http://zpd.gov.ua/dszpd/uk/publish/article/52224;jsessionid=B9ACD8AC177D0E96A5AA4A4EC0BE7BBD
214. Про внесення змін до деяких законодавчих актів України у зв'язку з прийняттям Закону України «Про інформацію» та Закону України «Про доступ до публічної інформації» : Закон України від 27 березня 2014 року // Голос України від 18.04.2014. – № 77.
215. Radbruch G. Die gesetzliche Strafanderung / G. Radbruch. – Berlin : Verlag von Otto Liebmann, 1908. – 500 p.
216. Лесниевски-Костарева Т.А. Дифференциация уголовной ответственности. Теория и законодательная практика / Т.А. Лесниевски-Костарева. – М. : НОРМА, 2000 – 400 с.

217. Красников В.И. Коррупция: история, причины, стратегии борьбы / В.И. Красников // Научный вестник Уральской академии государственной службы: политология, экономика, социология, право. – 2008. – № 1 (2). – С. 44–51.
218. Шакун В.М. Коллизии в статусе (компетенции) органов государственной власти и должностных лиц / В.М. Шакун // Вестник Челябинского государственного университета. – 2006. – № 2 (75). – С. 42–48.
219. Рязанцев А. С. Нарушение неприкосновенности частной жизни: уголовно-правовой аспект : монография / А.С. Рязанцев. – Воронеж : Астел, 2013. – 267 с.
220. Трудовой Кодекс Российской Федерации // Собрание законодательства Российской Федерации. – 2002. – № 1. – Ч. 1. – Ст. 3.
221. Кодекс на труда Република България от 01.04.1986 г. // Държавен вестник. – № 26 & 27/1986.
222. Ustawa Rzeczpospolita Polska z dnia 26 czerwca 1974 r. Kodeks pracy // Dziennik ustaw. – 1974. – № 24. – Poz. 141.
223. Labour Code of the Republic of Lithuania of 4 June 2002 // Official Gazette (Valstybes Zinios). – 2002. – № 64/2569.

Наукове видання

ГУРЖІЙ Тарас Олександравич,
ПЕТРИЦЬКИЙ Андрій Леонідович

ПРАВОВИЙ ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ

Монографія

Редактор О. В. Шульга
Комп'ютерне верстання Л. І. Власової
Дизайн обкладинки Н. Ю. Слінкіної

Формат 60х84/16. Ум. друк. арк. 11,16. Тираж 300 пр. Зам. 343.

Видавець і виготовлювач
Київський національний торговельно-економічний університет
вул. Кіото, 19, м. Київ-156, Україна, 02156

Свідоцтво суб'єкта видавничої справи серія ДК № 4620 від 03.10.2013 р.