М. О. СЕМЕНИШИН, В. М. БЕСЧАСТНИЙ,
С. С. ВІТВІЦЬКИЙ, І. Б. МАЛАХОВСЬКА, Є. С. НАЗИМКО

АДМІНІСТРАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

НАУКОВО-ПРАКТИЧНИЙ ПОСІБНИК

ВД «ДАКОР»

МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ДОНЕЦЬКИЙ ЮРИДИЧНИЙ ІНСТИТУТ

М. О. Семенишин, В. М. Бесчастний,
С. С. Вітвіцький, І. Б. Малаховська, Є. С. Назимко

АДМІНІСТРАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

НАУКОВО-ПРАКТИЧНИЙ ПОСІБНИК

Київ
ВД «ДАКОР»
2020

УДК 351.745.083.8:004.6-027.552](477)(07)
А31

Рекомендовано до друку
Вченою радою Донецького юридичного інституту МВС України
(протокол № 11 від 24 червня 2020 року)

Рецензенти:
Ісаков М. Г. – голова Наглядової ради юридичної фірми «Глобус»доктор юридичних наук, доцент, Заслужений юрист України.
Сергєєв О. О. – начальник Департаменту організаційно-аналітичного забезпечення та оперативного реагування Національної поліції України.

Семенишин М. О., Бесчастний В. М., Вітвіцький С. С., Малаховська І. Б., Назимко Є. С.

А31 Адміністративно-правове забезпечення захисту персональних даних в діяльності Національної поліції України / М. О. Семенишин, В. М. Бесчастний, С. С. Вітвіцький, І. Б. Малаховська, Є. С. Назимко. – Київ : ВД «Дакор», 2020. – 176 с.

ISBN 978-617-7679-52-2

Науково-практичний посібник присвячений комплексному та системному вивченню теоретико-правових засад адміністративно-правового забезпечення захисту персональних даних, організаційно-правового механізму захисту персональних даних та визначенню напрямів удосконалення адміністративно-правового захисту персональних даних Національною поліцією України.

Видання може бути корисним для співробітників практичних підрозділів Національної поліції України, працівників, курсантів, студентів та слухачів закладів вищої освіти із специфічними умовами навчання, що здійснюють підготовку поліцейських.

УДК 351.745.083.8:004.6-027.552](477)(07)

ISBN 978-617-7679-52-2

ЗМІСТ

ВСТУП

Забезпечення прав і свобод людини в процесі формування інформаційного суспільства виступає в якості першочергового завдання державної політики України. Широке використання сучасних інформаційних технологій чинить не тільки позитивний вплив на комфорт та зручність повсякденного життя, але й утворює нові виклики та загрози, пов'язані із неконтрольованим накопиченням та обробкою інформації про особу, яка потенційно може бути використана в небажаний для індивіда спосіб. Подальше використання сучасних інформаційних технологій, таких як штучний інтелект, хмарні технології, Інтернет речей, технології великих даних тощо, може викликати загрозу самого факту існування приватного життя громадян.

Правове регулювання захисту персональних даних та питань, пов'язаних із доступом до них набувають особливого значення в діяльності Національної поліції України. Сучасні інформаційні технології та законодавство відкривають безпрецедентні можливості для Національної поліції стосовно оброблення величезних обсягів персональних даних. Прийнятий у 2015 році Закон України «Про Національну поліцію» надає широкі повноваження органам та підрозділам Національної поліції щодо формування та використання інформаційних ресурсів, які входять до єдиної інформаційної системи Міністерства внутрішніх справ України. Крім того, поліція наділена повноваженнями щодо утворення власних баз даних та має безпосередній оперативний доступ до інформації та інформаційних ресурсів інших органів державної влади. Проте, з огляду на численні переваги цих технологій, слід визнати, що несанкціоноване їх використання може призвести до серйозних негативних наслідків.

Ситуація ускладнюється й повною відсутністю прозорого управління у сфері захисту персональних даних в діяльності Національної

поліції. Аналіз численних нормативно-правових актів, які регулюють діяльність структурних підрозділів центрального органу управління Національної поліції, дозволив зробити висновок про відсутність правових норм, які б безпосередньо були пов'язані із функціями цих підрозділів щодо захисту персональних даних. Відтак, і результати перевірок підпорядкованих підрозділів поліції яскраво демонструють відсутність дієвого контролю у сфері захисту персоніфікованої інформації. Також не вирішеними залишаються питання забезпечення органами Національної поліції максимального інформування суб'єктів персональних даних про правові підстави, способи, мету обробки, строки зберігання та знищення персональних даних, що-привертає все більше уваги до проблем у даній сфері.

Отже, формування ефективного адміністративно-правового механізму захисту персональних даних в діяльності Національної поліції, забезпечення його законодавчої та організаційної основи виступає в якості важливої гарантії дотримання особистих прав громадян, що надає змогу контролювати обробку персоніфікованої інформації, а в першу чергу – визначати строки та умови доступу до неї. Таким чином, інститут персональних даних стає дедалі важливішим елементом правового статусу особи, спрямованим на забезпечення її інформаційної безпеки.

Разом з тим слід відмітити позитивну роль адміністративного права у сфері захисту персональних даних, адже провідні науковці в галузі адміністративно-правової науки та інших суміжних галузей права не залишаються осторонь актуальних проблем державного управління, зокрема, проблематики адміністративно-правового захисту персональних даних в діяльності правоохоронних органів. Тому проведення комплексного спеціального дослідження адміністративно-правового захисту персональних даних в діяльності Національної поліції представляється необхідним у практичному відношенні та актуальним в теоретичному плані.

Разом з цим, слід констатувати, що до теперішнього часу комплексні правові дослідження, присвячені висвітленню проблем адміністративно-правового регулювання обігу та захисту персональних даних в органах та підрозділах Національної поліції та виробленню

науково обґрунтованих пропозицій щодо вдосконалення нормативно-правового підґрунтя у сфері захисту персональних даних, вітчизняними науковцями не проводились. Поза увагою досі залишаються питання щодо місця й ролі Національної поліції у сфері захисту персональних даних; визначення форм та методів захисту персональних даних в адміністративній діяльності Національної поліції; вироблення дієвих адміністративно-правових механізмів захисту персональних даних та багатьох інших аспектів в окресленій сфері публічного управління.

Науково-практичний посібник присвячений комплексному та системному вивченню теоретико-правових засад адміністративно-правового забезпечення захисту персональних даних, організаційно-правового механізму захисту персональних даних та визначенню напрямів удосконалення адміністративно-правового захисту персональних даних Національною поліцією України.

1. ТЕОРЕТИКО-ПРАВОВІ ЗАСАДИ АДМІНІСТРАТИВНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

1.1 Персональні дані як об'єкт науки адміністративного права

Забезпечення в процесі формування інформаційного суспільства інтересів громадян, їх прав і свобод є першочерговим завданням сучасної української держави. Повсюдне використання сучасних інформаційних технологій, зокрема: хмарних, технологій великих даних, Інтернету речей, штучного інтелекту та інших, не тільки справляє позитивний вплив на якість повсякденного життя, але й генерує нові виклики та загрози, пов'язані із реальною небезпекою неконтрольованого накопичення та обробки даних про особу. Подальше повсюдне поширення сучасних інформаційних технологій може призвести до того, що сам факт існування приватного життя опиниться під загрозою. З урахуванням сказаного формування адекватного правового режиму персональних даних є важливою гарантією прав особистості, що дозволяє контролювати обробку інформації про себе і, в першу чергу, визначати порядок і умови доступу до неї.

Не зважаючи на необхідність та своєчасність для соціального та економічного розвитку країни впровадження сучасних технологій обробки інформації, вказані процеси супроводжуються зростанням

кількості інформаційних систем і обсягів даних, що містяться в них, в тому числі й персональних даних. Попри те, що розвиток цифрової економіки фактично визнаний одним з пріоритетних завдань державної політики не тільки в Україні, а й за кордоном, його динаміка та успішна реалізація багато в чому залежатиме від того, яким буде правовий режим персональних даних та його основні параметри, і в першу чергу – порядок доступу до них та умови їх обробки. Встановлення підвищених вимог до забезпечення конфіденційності персональних даних, як інформації обмеженого доступу, може призвести до вкрай негативних наслідків для економіки країни, особливо в тих сферах, де надання товарів і послуг безпосередньо пов'язане з необхідністю автоматизованої обробки персональних даних (державні послуги, послуги зв'язку , освіта, охорона здоров'я, транспорт та ін.).

Таким чином, інститут персональних даних стає важливим елементом правового статусу особи, спрямованим на забезпечення її інформаційної безпеки. Крім того, питання правового регулювання персональних даних і проблеми доступу до них мають важливе значення для правової науки.

У зв'язку з цим представляється вкрай важливим і значущим проаналізувати наукові здобутки вітчизняних та зарубіжних вчених, присвячені проблемам організаційного і правового забезпечення функціонування інституту захисту персональних даних, і сформулювати на цій основі науково обґрунтовані і практично значущі пропозиції до національного законодавства, спрямовані на вдосконалення механізму захисту персональних даних.

Крім того, окремим блоком у цьому параграфі будуть розглянуті наукові роботи, в яких вченими окреслювалася проблематика реалізації механізму захисту персональних даних в діяльності правоохоронних органів, зокрема Національної поліції. Визнаючи той факт, що зазначений напрямок наукових досліджень набув особливої актуальності у зв'язку з бурхливим розвитком інформаційних технологій не тільки в Україні, але й у загальносвітовому масштабі, вважаємо за необхідне продовжити наукову дискусію в зазначеному напрямку публічного управління.

Підкреслюючи важливість і значущість реалізації поставленої наукової задачі, а також аналізуючи сучасні публікації в сфері захисту персональних даних можемо зробити висновок, що з часу прийняття Закону України «Про Національну поліцію» зазначена проблематика в діяльності вказаного правоохоронного відомства комплексно не розглядалась, а всі наукові напрацювання у сфері захисту персональних даних в діяльності Національної поліції України як правило мали фрагментарний характер.

Одним із перших учених в сучасній Україні, хто розпочав наукову розвідку з питань захисту персональних даних небезпідставно вважається В. М. Брижко [1-8].

Підкреслюючи значення та важливість персональних даних, вчений цілком доречно визначає останні як «особливий вид приватної власності, яка юридично виступає у формі виключного права власності і монополія на яку обмежується законом в інтересах дотримання прав та основних свобод інших осіб, а також в інтересах дотримання балансу прав людини, суспільства і держави» [9, с. 15]. Важливість питання щодо визначення сутності персональних даних полягає також у тому, що дослідник у вказаній роботі визначає їх як «найбільш чуттєву, делікатну та важливу для людини інформацію». Згодом, у прийнятому в 2011 році Законі України «Про захист персональних даних», законодавець визначив персональні дані про особу у якості відомостей, що на нашу думку є не дуже коректним, оскільки обробці в інформаційних системах та базах даних підлягає саме інформація, а не відомості про особу. Але власну позицію з цього питання ми висловимо у наступному параграфі, при з'ясуванні юридичної природи персональних даних.

Попри те, що дослідження, проведене В. М. Брижком, є відносно застарілим та за відсутності вітчизняного, повноцінно сформованого інституту захисту персональних даних вчений спирається переважно на міжнародні нормативно-правові акти та європейську практику, слід зазначити, що в роботі висвітлюється низка проблемних питань, які не втрачають своєї актуальності й дотепер.

Наприклад, серед іншого вчений акцентує увагу на існуючих протиріччях у законодавстві та правозастосовній практиці стосовно

«прагнення максимального використання персональних даних у суспільних і державних інтересах, та, одночасно, бажання максимально захистити права на недоторканність приватного життя людини» [9, с. 11].

Дійсно, норми щодо заборони втручання в особисте та приватне життя громадян зафіксовані як у міжнародних нормативно-правових актах (ст. 12 Загальної декларації прав людини, ст. 8 Конвенції про захист прав людини і основоположних свобод), так й у національному законодавстві (ст.ст. 31, 32 Конституції України). У той же час, найважливішим завданням будь-якої держави у сфері забезпечення прав і свобод громадян є доступ до публічної інформації. Водночас, вказане завдання напряму пов'язане із забезпеченням інформаційної безпеки держави. Таким чином, виникає необхідність встановлення балансу між компетенцією органів державної влади (в тому числі правоохоронних) на доступ до інформації про громадян та правом особи на захист персональних даних.

Аналогічна правова проблема існує також і в зарубіжних країнах. Наприклад, окремі положення законодавчих та підзаконних нормативно-правових актів країн Європейського Союзу пов'язані із забезпеченням інформаційної безпеки та визначають останню в якості сукупності заходів організаційного та правового характеру, спрямованих на забезпечення бажаного стану, за якого досягається максимальне усунення реальних та потенційних загроз національній безпеці у інформаційній сфері [10]. Із наведеного визначення стає очевидним, що головна мета здійснення безпекових організаційно-правових заходів полягає у максимальному усуненні реальних та потенційних загроз в інформаційній сфері.

В процесі вирішення питання про дотримання балансу інтересів між дозволеним втручанням у приватне життя особи щодо захисту її персональних даних та правом особи на недоторканність особистого життя, вважаємо, що пріоритет у вказаному питанні повинен належати захисту права особи на приватність. До цього зобов'язують норми як міжнародного, так і національного законодавства.

Наприклад, положення статті 12 Загальної декларації з прав людини передбачають заборону безпідставного втручання у приватне

життя громадян, безпідставне посягання на недоторканність житла особи, таємницю її кореспонденції або на її честь і репутацію [11]. Норми, що зобов'язують поважати приватне та сімейне життя осіб, власне житло і кореспонденцію зафіксовані також у статті 8 Конвенції про захист прав людини і основоположних свобод [12]. В пункті 1 статті 17 Міжнародного пакту про громадянські і політичні права наголошується на забороні свавільного втручання до особистого чи сімейного життя, свавільних чи незаконних посягань на недоторканність житла або таємницю кореспонденції чи незаконних посягань на честь і репутацію особи [13]. Проголошені у якості основи демократичного суспільства права осіб на приватність та свободу вираження поглядів також зафіксовані у Резолюції № 1165 Парламентської Асамблеї Ради Європи та статті 8 Конвенції про захист прав людини і основоположних свобод [14].

Слід зазначити, що загальною рисою, яка властива приватності та відображена в усіх без винятку вище перелічених міжнародно-правових актах виступає її невичерпність певними рамками або межами. Тобто коло приватного життя особи не обмежується її помешканням або стосунками в родині, а являє собою набагато ширше поняття.

Приємно відзначити, що аналогічна правова норма згодом знайшла відображення і в національному законодавстві, в рішенні Конституційного суду України від 20 січня 2012 року № 2-рп/2012 «Щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України» [15].

Таким чином, враховуючи широкий діапазон розуміння приватності як у законодавстві, так і в правозастосовчій практиці, вважаємо, що надмірне втручання з боку правоохоронних органів у приватне життя осіб є неприпустимим.

Вказаний висновок також підтверджується й рішеннями ЄСПЛ. Зокрема, слід звернути увагу на рішення ЄСПЛ у справі Ромен і Шмідт проти Люксембургу (Roemen and Schmit v. Luxembourg 2003 року), в якому Суд визнав незаконним проведення обшуків та конфіскації особистої кореспонденції в службовому офісі заявниці, мотивуючи це фактом втручання правоохоронних органів у приватне життя заявниці.

Зауважте, Суд тлумачить межі приватності у розширеному контексті навіть з урахуванням того, що втручання правоохоронних органів у приватне життя особи мало законну мету та спиралось на положення національного кримінально-процесуального законодавства.

Показовим у вказаному контексті є й Рішення ЄСПЛ Мелоун проти Об'єднаного Королівства, в якому йдеться про порушення статті 8 Конвенції, оскільки «прослуховування телефонних розмов заявника (в рамках його кримінального переслідування) і реєстрація історії дзвінків (збереження номерів, набраних з певного телефону) не були передбачені законом» [16].

Таким чином, аналіз наукових публікацій Брижка В.М. дає підстави для висновку про їх прогресивний характер. Зазначений факт підтверджується тим, що автор одним із перших, використовуючи міжнародні нормативно-правові акти у сфері захисту персональних даних, розробив проект Закону України «Про захист персональних даних». Також заслуговує на увагу проведене Брижком В. М. ретельне опрацювання Конвенції № 108 Ради Європи від 28.01.1981 р. та Додаткового протоколу до неї від 08.11.2001 р., переклад яких з англійської здійснено автором власноруч.

Безперечну наукову цінність також представляють розроблені автором положення щодо теоретичного обґрунтування та вдосконалення понять «персональні дані», «право власності на персональні дані», «власник персональних даних», «володілець персональних даних» в доктринальному та нормативно-правовому аспектах [9, с. 8].

Разом з цим, слід відмітити, що численні пропозиції дослідника до законодавства у сфері захисту персональних даних наразі втратили свою актуальність у зв'язку із суттєвими прогресивними змінами у законодавстві України щодо досліджуваної проблематики.

Персональні дані в якості одного з елементів адміністративно-правового режиму інформації з обмеженим доступом розкрив В. Ю. Баскаков в дисертаційному дослідженні «Адміністративно-правовий режим інформації з обмеженим доступом». Ретельний аналіз Закону України «Про захист персональних даних» надав змогу констатувати «відсутність уніфікованого розуміння змісту

та складових персональних даних» [17, с. 13]. Однак, такий висновок автора, на нашу думку, цілком логічно випливає із специфічної природи приватності, яка полягає у широкому розумінні останньої. Вище ми вже вказували на таку особливість законодавчого закріплення приватності (особистого життя), при якій остання а ні в міжнародному, а ні в національному законодавстві фактично не має визначення та не обмежується власним помешканням або особистими стосунками із близькими особами.

А тому марними виглядають спроби автора конкретизувати персональні дані особи чітко визначеними відомостями про неї, як-от: «прізвище, ім'я та по батькові; національність; освіта; сімейний стан; релігійні переконання; стан здоров'я, історія хвороби; мета запропонованих досліджень і лікувальних заходів; прогноз можливого розвитку захворювання (в тому числі й про наявність ризику для життя і здоров'я); адреса народження; дата народження; місце народження; майновий стан; расове або етнічне походження; політичні, релігійні або світоглядні переконання; членство в політичних партіях та професійних спілках; дані, що стосуються здоров'я чи статевого життя тощо» [17, с. 14].

Доволі цікавою також є позиція вченого щодо необхідності звуження переліку персональних даних, з огляду на доцільність захисту деяких із них. У цьому контексті вчений посилається на міжнародну законодавчу практику, згідно з якою усі персональні дані поділяються на загальні, які не потребують режиму жорсткого захисту, та вразливі (або чутливі), вимоги до захисту яких набагато суворіші та жорсткіші. Аналогічної думки притримується й Т. І. Обуховська, яка також наголошує на необхідності приведення національного законодавства України у сфері захисту персональних даних до вимог норм європейського та міжнародного права [18, с. 97].

У той же час, аналізуючи обґрунтованість висловлених позицій, слід звернутися до норм міжнародного (передовсім європейського) законодавства, яке передбачає законність обробки персональних даних за умови: а) згоди суб'єкта персональних даних; б) забезпечення життєво важливих інтересів суб'єктів персональних даних; в) забезпечення основоположних прав суб'єктів персональних

даних; г) встановлення спеціальних, суворіших вимог, які дозволяють здійснювати обробку чутливих даних [19].

Відповідно до п. 39 Регламенту Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (скорочено – Регламент № 679), «будь-яке опрацювання персональних даних повинно бути законним та правомірним. Фізичні особи повинні бути обізнані про те, що їхні персональні дані збирають, використовують, обговорюють або іншим чином опрацьовують, а також про те, якою мірою опрацьовують чи опрацьовуватимуть персональні дані. Принцип прозорості вимагає, щоб будь-яка інформація та повідомлення щодо опрацювання таких персональних даних були доступними і зрозумілими, з використанням чітких і простих формулювань» [19].

Така позиція законодавця підтверджується також низкою рішень Європейського Суду з прав людини, а саме: СЄС, об'єднані справи С-465/00, С-138/01 та С-139/01, «Рахункова палата проти австрійської телерадіокомпанії «Österreichischer Rundfunk» та інших і Нойком та Лауерманн проти австрійської телерадіокомпанії «Österreichischer Rundfunk» (Rechnungshof v. Osterreichischer Rundfunkand Others and Neukomm and Lauermann v. Osterreichischer Rundfunk) від 20 травня 2003 р., п. 65; СЄС, С-524/06, «Губер проти Німеччини» (Huber v. Germany) від 16 грудня 2008 р., п. 48; СЄС, об'єднані справи С-468/10 та С-469/10, «Національна асоціація кредитних фінансових установ (ASNEF) і Федерація електронної комерції і прямого маркетингу (FECEMD) проти Державної адміністрації» (Asociacion Nacional de Establecimientos Financieros de Credito (ASNEF) and Federacion de Comercio Electronico y Marketing Directo (FECEMD) v. Administracion del Estado) від 24 листопада 2011 р., п. 26 [20, с. 88]. Це пояснює випадки, які узаконюють обробку нечутливих персональних даних.

Отже, аналізуючи вищевикладене, вважаємо, що слід відмежовувати правову позицію Ради Європи, відповідно до якої згода на обробку персональних даних взагалі не передбачена а ні статтею 8

ЄКПЛ, а ні Конвенцією 108. Хоча інші нормативно-правові акти Ради Європи, до яких віднесено низку рекомендацій РЄ та судову практику ЄСПЛ, все ж таки передбачають отримання згоди при обробці персональних даних

Наприклад, відповідно до п. 40 Регламенту № 679 [19], чітко встановлено необхідність отримання згоди власника інформації на обробку його персональних даних.

Таким чином, можемо зробити висновок, що позиція європейського законодавця з приводу встановлення дозволеної межі доступу до персональних даних не відрізняється однозначністю. Правові норми, спрямовані на врегулювання питання доступу до персональних даних варіюються в залежності від джерела походження нормативно-правового акту. Якщо позиція законодавчих органів Європейського союзу однозначно спрямована на необхідність отримання згоди від власника персональних даних, то законодавчі інституції Ради Європи займають двояку позицію, не використовуючи при цьому чітких зрозумілих критеріїв.

Відтак, вважаємо дискусійним питання щодо необхідності запровадження у національному законодавстві правових норм, спрямованих на звуження переліку персональних даних, згода на обробку яких в обов'язковому порядку повинна надаватися їх власником. На сьогоднішній день факти зловживання персональними даними мають розповсюджений характер та охоплюють суспільні відносини, починаючи від політики та закінчуючи сферою надання ритуальних послуг. Натомість вироблення чітких критеріїв, спрямованих на виокремлення загальних та спеціальних персональних даних, які, до речі, відсутні у чинному законодавстві, вважаємо цілком своєчасним та обґрунтованим.

Пропонуємо класифікувати персональні дані, в залежності від режиму їх захисту, на персональні дані, захист яких здійснюється у звичайному режимі (прізвище, ім'я та по батькові, дата і місце народження, громадянство, місце проживання) та інформація, захист якої здійснюється в особливому режимі інформація про шлюбні відносини (сексуальну орієнтацію; наявність в родині дітей, опікунів та піклувальників; умови проживання і т.д.); інформація про медичні

показники (стан здоров'я; перенесені хвороби; перебування на лікарняному; перенесені операції і т.д.); інформація про духовні відносини (віросповідання; ставлення до релігії і т.д.); інформація у сфері кредитно-фінансових відносин (вклади і рахунки в банках, наявність нерухомості, податковий статус; кредитна історія і т.д.); інформація у сфері трудових відносин (відомості про розмір зарплати або інші законні доходи, посаду, умови трудового договору, проходження професійного навчання та його результати і т.д.); інформація про деліктні відносини (дані про судимість та інші форми притягнення особи до кримінальної, адміністративної чи дисциплінарної відповідальності).

Сучасний етап адміністративно-правового забезпечення захисту персональних даних, на нашу думку, пов'язаний з науковими здобутками Петрицького А. Л., Різака М. В., Туніка А. В., Цвірюка Д. В., Шевчука О. М.

Аналіз наукових публікацій вищевказаних вчених у галузі адміністративного права дає підстави для висновку, що беззаперечними ознаками «осучаснення» інституту захисту персональних даних виступає: а) розширення сфери захисту персональних даних; б) урізноманітнення відносин, які входять до сфери захисту персональних даних, збільшення ступеня її правової регламентації, що відобразилось у великій кількості несистематизованих нормативно-правових актів; в) постійно зростаюча вага правової бази у сфері захисту персональних даних, а також необхідність визначення її ролі та місця у вітчизняній системі права [21, с. 9].

У продовження цього умовиводу М. В. Різак наголошує на актуальності деяких питань, у зв'язку із бурхливим розвитком законодавства про захист персональних, а саме: 1) визначення місця Закону України «Про захист персональних даних» у системі нормативних актів, що регулюють окремі види інформації обмеженого доступу; 2) упорядкування масиву підзаконних актів, що регламентують окремі питання обігу персональних даних; 3) зміщення акценту закону з порядку та умов обігу персональних даних на принципові питання захисту прав і свобод суб'єкта даних [22, с. 8].

У той же час, досліджувана робота не позбавлена слабких сторін, що проявляється, зокрема, у формулюванні окремих положень

новизни проведеного дослідження на основі вже досліджених у багатьох наукових працях проблемних питань. Зокрема, йдеться про змістовне наповнення правової категорії «персональні дані», яка вперше розкрита в широкому контексті як багатогранний об'єкт наукового пізнання. Мусимо констатувати, що окреслене розуміння персональних даних неодноразово висвітлювалось як у наукових працях вітчизняних та зарубіжних учених, так і в міжнародному, зокрема, європейському законодавстві.

Загалом, слід відзначити, що розвиток інституційної моделі захисту персональних даних позначився не тільки на якісному оновленні нормативно-правової бази, але й активному науковому супроводженні цього процесу. Причому для наукової розвідки у напрямку адміністративно-правового забезпечення захисту персональних даних властиві деякі специфічні риси, які підтверджують позитивну динаміку розвитку інституту захисту персональних даних, а саме: а) в роботах вітчизняних науковців в галузі адміністративного права питання захисту персональних даних все частіше пов'язуються із забезпеченням інформаційної безпеки держави. Наприклад, О.М. Шевчук під час дослідження адміністративно-правового механізму регулювання інформаційної безпеки органами державної влади пропонує запровадити самостійну посаду представника (або помічника) Уповноваженого Верховної Ради України з прав людини, яка передбачала б реалізацію повноважень щодо охорони та захисту прав громадян на доступ до інформації, в тому числі персональних даних [23, с. 4]; б) пропозиції науковців щодо вдосконалення адміністративно-правового забезпечення захисту персональних даних дедалі більше набувають практично орієнтованого змісту. Зокрема, вищезгаданим дослідником висловлена доволі цікава і в той же час практично значуща ідея щодо необхідності розроблення та прийняття Інформаційного кодексу України, який мав би узагальнити численні невирішені на теперішній час питання, пов'язані, наприклад, із правовою регламентацією електронної торгівлі, правовою охороною прав на зміст комп'ютерних програм, удосконалення захисту прав інтелектуальної власності, в тому числі авторського права при розміщенні та використанні творів у мережі

Інтернет, про охорону баз даних і т.д. [23, с. 4]. Слушною також є пропозиція А. Л. Петрицького щодо необхідності прийняття державної цільової програми, спрямованої на комплексну реалізацію політики захисту персональних даних на загальнодержавному, міжгалузевому/галузевому та місцевому рівнях [21, с. 5]; в) захист персональних даних дедалі частіше згадується в якості самостійного адміністративно-правового інституту. Так, М. В. Різак наполягає на існуванні національної системи регулювання персональних даних, в рамках якої успішно розвивається один з її ключових напрямків, пов'язаний із створенням спеціальної інституційної структури, що забезпечує нагляд за дотриманням прав суб'єктів персональних даних [22, с. 4].

Також доволі цікавими є пропозиції Д. В. Цвірюка, стосовно виокремлення в інституті персональних даних декількох підінститутів, зокрема: а) представництва Уповноваженого Верховної Ради України з прав людини в регіональних представництвах із захисту персональних даних; б) позбавлення володільця чи розпорядника права обробляти персональні дані у разі повторного порушення вимог відносно обробки й захисту персональних даних; в) інституту «адміністративної опіки» відносно володільців і розпорядників персональних даних, в якості яких виступають органи виконавчої влади та органи місцевого самоврядування [24, с. 3-4].

Слід зазначити, що проблематика захисту персональних даних також неодноразово виступала предметом наукових досліджень представників інших галузей правової науки та суміжних галузей наукових знань. У цьому контексті заслуговують на увагу наукові праці Горпинюк О. П., Кардаш А. В., Обуховської Т. І., Пазюк А. В., Серьогіна В. О., Чернобай А. М., Ясечко С. В.

Аналіз наукових публікацій вищевказаних дослідників дозволив зробити висновок, що не зважаючи на різні напрямки наукового пізнання, пріоритет у їх роботах надавався таким напрямкам дослідження як: а) з'ясування правової природи приватності та спроби її законодавчого врегулювання. Така тенденція найбільш яскраво простежується, наприклад, у дослідженні О.П. Горпинюк, яка пропонує розуміти приватність як інформацію про життєдіяльність особи, до якої самим її власником застосовано обмеження доступу.

Така правова конструкція виглядає найбільш вдалим варіантом розуміння приватності, оскільки ключовим її критерієм виступає не обсяг інформації про особу, а факт обмеження нею доступу до певних відомостей, навіть тих, які безпосередньо не стосуються особистого життя власника інформації. Разом з цим, при визначенні обсягу приватності, вчена пропонує відштовхуватися від охоронюваних кримінальним законом відносин, відтворених у складах кримінальних правопорушень статей Кримінального кодексу України, а саме: ст.ст. 182, 132, 145, 163, 168, 231, 232, 361-2, 381, 387 КК України [25, с. 6].

Приватність у якості конституційно-правового феномена висвітлена в монографічному дослідженні А. В. Кардаш на тему «Конституційно-правовий захист інформації про особу (порівняльно-правовий аспект)» [26, с. 6-7]. Попри те, що вчена вперше використала у вказаній науковій праці правову дефініцію «інформаційна приватність», розуміючи останню як процес реагування конституційно-правовими засобами на неправомірне втручання з боку держави і приватних осіб, все ж таки доволі дискусійними, на нашу думку, виглядають пропозиції автора щодо необхідності застосування дворівневого (змішаного) підходу при формуванні законодавства про захист персональних даних. У змісті публікації йдеться, зокрема, про доцільність формування правової бази у сфері захисту інформації про особу на законодавчому та галузевому рівнях з детальною регламентацією відповідних відносин на другому рівні. Слід зазначити, що на сьогоднішній день на галузевому рівні сформована доволі об'ємна нормативно-правова база щодо регулювання обігу персональних даних [27-29], тому надмірне перевантаження правової регламентації із вказаного питання може внести певну плутанину у правозастосовчу практику та негативно вплинути на якість виконання документів; б) захист персональних даних нерозривно пов'язується багатьма вченими із основоположними правами і свободами людини і громадянина. Наприклад, В. О. Серьогін розглядає захист персональних даних у міжнародно-правовому аспекті як один з напрямків реалізації прав громадян на недоторканність приватного життя [30, с. 5].

А. М. Чорнобай цілком справедливо виокремлює функцію захисту персональних даних, як один з основних напрямків в правотворчій та правозастосовчій діяльності міжнародних та європейських організацій із забезпечення прав людини. Право на недоторканість приватного життя, зазначає автор, суб'єктом якого є кожна людина, закріплене як одна з загальнолюдських цінностей в актах ООН, МОП, Ради Європи, Європейського Союзу, Організації економічного співробітництва і розвитку (ОБСР), а також договорах, укладених державами у рамках СНД та ратифікованих Україною [31, с. 5].

Право на інформацію, зазначає С. В. Ясечко, стало врівень із природними правами людини, хоча б тому, що поза здатністю сприймати, виробляти чи обробляти інформацію людина існувати в сучасному світі і бути успішною не може [32, с. 11]. Таким чином, на підставі наведених суджень вітчизняних науковців можна зробити висновок про дуалістичну правову природу інституту захисту персональних даних, який, з одного боку, виступає в якості органічного елементу системи інформаційного права, а з іншого – складовою частиною міжнародного та національного права щодо забезпечення основоположних прав і свобод людини і громадянина.

В контексті досліджуваної проблематики також окремо слід зупинитися на наукових працях прямо чи опосередковано пов'язаних із захистом персональних даних в діяльності Національної поліції.

Слід зауважити, що проблематиці захисту персональних даних в діяльності поліції (органів внутрішніх справ) приділено увагу в роботах І. В. Костенка [33], Д. О. Красікова [34], Є. О. Крапивіна [35, с. 16], Б. В. Семерея [36], В. С. Сивухіна [37], С. В. Чирика [38]. Однак, одним із перших комплексних монографічних досліджень проблем забезпечення інформаційної безпеки в діяльності вказаних правоохоронних органів по праву вважаємо дисертаційне дослідження І. В. Арістової на тему: «Державна інформаційна політика та її реалізація в діяльності органів внутрішніх справ України: організаційно-правові засади» [39]. Не зважаючи на те, що вказана наукова праця підготовлена ще в далекому 2002 році, деякі її положення й дотепер не втрачають актуальності. Наприклад, автор висловлює цілком прогресивне твердження щодо ключової ролі ОВС

у забезпеченні інформаційної безпеки країни, основна функція яких повинна полягати у охороні та захисті інформаційного порядку суспільства [39, с. 26]. Щоправда слід відмітити, що в даному випадку автор розуміє правовий статус ОВС щодо забезпечення інформаційної безпеки у широкому контексті, розглядаючи органи внутрішніх справ у якості суб'єкта державного управління національної інформаційної системи. Аналогічне розуміння функціональної приналежності Національної поліції щодо забезпечення інформаційної безпеки та захисту персональних даних відображено й у статті 25 Закону України «Про Національну поліцію». Будучи суб'єктом державного управління в інформаційній сфері Національна поліція: 1) формує бази (банки) даних, що входять до єдиної інформаційної системи Міністерства внутрішніх справ України; 2) користується базами (банками) даних Міністерства внутрішніх справ України та інших органів державної влади; 3) здійснює інформаційно-пошукову та інформаційно-аналітичну роботу; 4) здійснює інформаційну взаємодію з іншими органами державної влади України, органами правопорядку іноземних держав та міжнародними організаціями [40]. Поряд з цим, частина 4 коментованої статті визначає правову основу діяльності Національної поліції, в частині захисту та обробки персональних даних. Так, правовою основою вищевказаної діяльності поліції є Конституція України, Закон України «Про захист персональних даних» та інші закони України. Уявляється, що таке розуміння правової основи діяльності поліції у сфері захисту персональних даних занадто звужене законодавцем. Наприклад, компетенція поліції щодо здійснення інформаційно-пошукової та інформаційно-аналітичної роботи, а також оброблення персональних даних зафіксована у розділі 4 «Положення про Національну поліцію». Окремі положення щодо захисту Національною поліцією інформації від несанкціонованого доступу, а також впровадження механізмів технічного захисту інформації містяться також в положенні, затвердженому наказом Національної поліції від 03.08.2017 № 676 «Про інформаційно-телекомунікаційну систему «Інформаційний портал Національної поліції України» [41]. Таким чином, вважаємо, що необхідність внесення доповнень до частини 4 статті 25 Закону України «Про Національну

поліцію» цілком очевидна та полягає у застосуванні розширеного тлумачення правової основи діяльності Національної поліції у сфері захисту персональних даних.

Крім цього, заслуговують на увагу пропозиції І. В. Арістової щодо необхідності визначення довгострокової стратегічної мети державної інформаційної політики України в контексті «формування відкритого інформаційного суспільства на основі розвитку єдиного інформаційного простору цілісної держави та його інтеграція у світовій інформаційний простір з урахуванням національних особливостей і інтересів при забезпеченні інформаційної безпеки на внутрішньодержавному та міжнародному рівнях» [39, с. 15]. Слід зазначити, що реалізація зазначеної мети набула практичного втілення на національному рівні порівняно нещодавно.

З часів проголошення незалежності української держави національна інформаційна безпека розглядалась найвищими посадовими особами органів державної влади в якості недооціненого та, як наслідок, недостатньо розвиненого, напрямку забезпечення національної безпеки України. Відповідна тенденція спостерігалась і в правовому полі держави, коли інформаційна безпека фактично не згадувалась у нечисленних законодавчих актах серед основних загроз національній безпеці країни.

Ситуація поступово змінилась на початку XXI століття із активним розвитком інформаційних та телекомунікаційних технологій, розширенням та широкою доступністю мережі Інтернет, її використанням громадянами, бізнес-спільнотою та органами публічної адміністрації, а координальні зрушення в державному управлінні щодо вдосконалення інформаційної безпеки держави розпочались у 2014 році, з початком збройної агресії РФ на території України. Зазначені фактори змусили українське суспільство визнати інформаційну безпеку одним з ключових елементів системи національної безпеки держави. Зазначений факт, зокрема, підтверджується й висновком Р.О. Додонова, який наголошує на входженні України до найскладнішого періоду свого розвитку. Вчений зазначає, що поряд з низкою країн світової спільноти, Україна вперше у своїй історії зіткнулась із необхідністю організації оборони в умовах інформаційного

суспільства, коли інформаційно-психологічний вплив став головним чинником ведення сучасної війни, яка отримала назву «гібридної» [42, с. 135]. Як наслідок, значення інформаційної складової в системі національної безпеки наразі суттєво зростає.

На цьому фоні доволі сумнівним виглядає висновок колективу авторів науково-практичного посібника «Права людини в діяльності української поліції», щодо максимального обмеження доступу працівників поліції до баз даних із персональною інформацією про особу. Вчені пропонують «повністю заборонити доступ поліцейських до деяких із баз даних, за винятком випадків, коли конкретні поліцейські здійснюють досудове розслідування злочинів» [43, с. 16]. Зазначена точка зору ґрунтується на положеннях статті 27 Закону України «Про Національну поліцію», яка нібито надає працівникам поліції необмежений доступ до персональних даних інших осіб.

Не можемо погодитися із наведеною позицією з декількох причин. По-перше, у частині 1 статті 27 коментованого законодавчого акту йдеться про три підстави доступу поліцейських до баз даних, які містять персональну інформацію. Такий доступ повинен бути: а) безпосереднім; б) оперативним та в) з обов'язковим дотриманнямЗакону України «Про захист персональних даних».

Розуміння безпосереднього доступу поліцейських до оперативної інформації розкривається в частинах 2,3 коментованого Закону та передбачає максимально повну фіксацію в електронному архіві відомостей про користувача персональних даних, а саме: прізвище, ім'я, по батькові та номер спеціального жетона поліцейського, вид отриманої інформації, реєстр, з якого отримувалася інформація, час отримання інформації та інші дані, необхідні для ідентифікації поліцейського, який отримував інформацію з реєстрів [40].

Відомчими нормативно-правовими актами також передбачений механізм забезпечення порядку ідентифікації користувача інформації, шляхом надання останньому електронного цифрового підпису або інших програмно-технічних засобів авторизації користувачів та забезпечення цілісності даних [41]. Таким чином, можемо однозначно констатувати законне та повноцінне забезпечення на

законодавчому рівні порядку безпосереднього доступу працівників поліції до персональних даних власників інформації.

Зміст оперативного доступу до інформаційних ресурсів розкривається в Законі України «Про оперативно-розшукову діяльність», стаття 1 якого визначає одне з головних завдань оперативно-розшукової діяльності – отримання інформації в інтересах безпеки громадян, суспільства і держави [44].

Право працівників поліції, які провадять оперативну та оперативно-розшукову діяльність на отримання персональних даних осіб також зафіксовано у статті 8 коментованого законодавчого акту.

Зокрема, підрозділи, що здійснюють оперативно-розшукову діяльність мають право в установленому законом порядку:

- ознайомлюватись із документами й даними, що характеризують діяльність підприємств, установ та організацій, вивчати їх за рахунок коштів, що виділяються на утримання підрозділів, які здійснюють оперативно-розшукову діяльність, виготовляти копії з таких документів, на вимогу керівників підприємств, установ та організацій – винятково на території таких підприємств, установ та організацій, а з дозволу слідчого судді в порядку, передбаченому Кримінальним процесуальним кодексом України,
- витребовувати документи й дані, що характеризують діяльність підприємств, установ, організацій, а також спосіб життя окремих осіб, підозрюваних у підготовці чи вчиненні злочину, джерело й розміри їх доходів, із залишенням копій таких документів та опису вилучених документів особам, у яких вони витребувані, і забезпеченням їх збереження й повернення в установленому порядку;
- здійснювати аудіо-, відеоконтроль особи, зняття інформації з транспортних телекомунікаційних мереж, електронних інформаційних мереж згідно з положеннями ст. ст. 260, 263-265 Кримінального процесуального кодексу України;
- накладати арешт на кореспонденцію, здійснювати її огляд та виїмку згідно з положеннями ст. ст. 261, 262 Кримінального процесуального кодексу України;

- створювати й застосовувати автоматизовані інформаційні системи;
- звертатись у межах своїх повноважень із запитами до правоохоронних органів інших держав та міжнародних правоохоронних організацій відповідно до законодавства України, міжнародних договорів України, а також установчих актів і правил міжнародних правоохоронних організацій, членом яких є Україна [44].

Також частина 1 статті 27 Закону України «Про Національну поліцію» визначає ще одну підставу законного доступу працівників поліції до персональних даних осіб – обов'язкове дотримання Закону України «Про захист персональних даних».

Стаття 22 вказаного законодавчого акту визначає суб'єктів здійснення контролю за дотриманням законодавства про захист персональних даних, до яких віднесено Уповноваженого Верховної Ради з прав людини та суди. Таким чином, контролюючі суб'єкти у коментованому законі представлені законодавчою та судовою гілкою влади. Разом з цим, частина 3 статті 28 Закону України «Про Національну поліцію» визначає МВС України у якості контролюючого суб'єкта за дотриманням вимог законів та інших нормативно-правових актів під час формування та користування поліцейськими інформаційними базами (банками) даних. Тобто фактично йдеться про контрольну функцію вказаного Міністерства за дотриманням законодавства про захист персональних даних в процесі їх накопичення та обробки працівниками поліції під час роботи з базами даних.

Тому відсутність виконавчої гілки влади серед суб'єктів здійснення контролю за обробкою персональних даних вважаємо помилкою законодавця, на підставі чого пропонуємо доповнити перелік контролюючих суб'єктів, визначених у статті 22 Закону України «Про захист персональних даних» органами виконавчої влади.

1.2. Правова природа адміністративно-правового захисту персональних даних

Захист персональних даних справедливо розглядається багатьма вченими у якості провідної галузі інформаційного права як категорія, яка нерозривно пов'язана із забезпеченням права громадян на приватне життя. Контроль за обігом приватної інформації про особу сформувався як похідна ідея, в результаті реалізації прагнення держави забезпечити належний рівень захисту особи від інформаційних загроз [45-51].

Тому нелогічно, на наш погляд, розглядати правову природу захисту персональних даних відокремлено від більш об'ємної правової категорії, пов'язаної із охороною прав громадян на особисту недоторканність, гарантовану Конституцією України.

На теперішній час право на захист приватної інформації про особу, а рівно й необхідність поваги до приватної та особистої сфери життя громадян, забезпечення права на захист особистої інформації (персональних даних) вважаються невідчужуваними правами будь-якої людини та гарантовані Конституцією України.

У той же час, поглиблюючись у історичне минуле, слід констатувати, що в багатьох країнах світу захист персональних даних особи тільки наприкінці XIX століття став розглядатись у якості пріоритетного напрямку державної політики.

Уперше думку про необхідність поваги до приватного життя особи було висловлено у статті The Right to Privacy, опублікованої у 1890 році в журналі Harvard Law Review американськими юристами Семюелем Уореном та Луї Брендейсом [52, с. 67], в якій уперше висловлено необхідність судового захисту приватного життя від втручання. Фактично зазначений факт послужив поштовхом для поступового розвитку законодавства щодо захисту персональних даних, коли окремі американські штати розпочали законотворчу діяльність в окресленому напрямку.

Відтоді ідея захисту персональних даних достатньо швидко дістала правового забарвлення й в інших країнах світу, не зважаючи на те, що вказана проблематика безсумнівно виступала предметом

неофіційного обговорення серед представників влади та наукової спільноти.

Ідея протиставлення публічного і приватного життя особи, а рівно – ідея необхідності поваги до останнього, пов'язана з теорією природного права, де основною передумовою є невід'ємне право на володіння самим собою (своїм тілом), фізичної свободою і своїм майном.

Одним з перших законодавчих актів, який справив істотний вплив на появу подібних положень про захист приватного життя в законодавстві європейських країн, став Цивільний кодекс Німеччини 1900 року [53].

Однак, по праву світове визнання ідея щодо поваги до приватного життя громадян набула із прийняттям Загальної декларації з прав людини [11] та Міжнародного пакту про громадянські і політичні права [13].

Таким чином, можна стверджувати, що вищенаведені правові акти створили передумови для визначення недоторканності приватного життя людини одним з пріоритетних завдань державної політики багатьох країн світу та імплементації міжнародних норм права до національних правових систем.

У той же час, не зважаючи на всесвітнє визнання на законодавчому рівні права на приватне життя, вказаний правовий інститут не позбавлений численних правових та юридичних дискусійних аспектів, одним з головних серед яких залишається питання щодо юридичного змісту права на недоторканність приватного життя, а також, власне, розуміння приватного життя.

Слід зазначити, що деякі вчені [54, с. 81–88] в процесі вирішення зазначених дискусійних питань відштовхуються від положень ст.ст. 8, 12 Європейської конвенції про захист прав людини і основоположних свобод [12], яка визначає нерозривний зв'язок права на повагу та недоторканність приватного життя із свободою висловлення власної позиції, свободою думки, совісті та релігії, свободою асоціацій та зібрань, правом на справедливий розгляд справи, а також правом на створення сім'ї.

Інші автори під правом на повагу та недоторканність приватного життя розуміють право власного розпорядження, право на

таємницю приватного життя та таємницю кореспонденції, право на захист особистості та право на повагу до себе [55, с. 91].

Серед багатьох зарубіжних вчених укорінилася думка щодо права на приватне життя як невід'ємного елементу більш широкого поняття – права на особистість (droit/droits de la personalité. – фр.), до якого, серед іншого, відносяться: право на життя, особисту недоторканність, на повагу до свого ім'я, честі та гідності [53, с. 6].

За такого змістовного наповнення, стверджує В. М. Брижко, зацікавленість до проблеми недоторканності приватного життя почала істотно посилюватися, а право на приватне життя стало нероздільно пов'язуватись із правом на власне зображення та голос, а також іншими якостями людини, які дозволяють ідентифікувати її серед інших [56, с. 7].

Узагальнюючи усі вищенаведені судження, можемо констатувати безперечну складність правового інституту недоторканності приватного життя, що уособлює широкий спектр компетенцій окремо взятого індивіда. Разом з цим, перелік цих компетенцій, визначених у міжнародних та національних нормативно-правових актах, неможна за будь-яких умов вважати вичерпним у зв'язку із динамічним розвитком відносин у цій сфері. Передовсім, зазначений умовивід підтверджується положеннями статті 22 Конституції України, відповідно до якої права і свободи людини і громадянина, закріплені у основному законі держави, не є вичерпними [57]. Крім того, на розширеному тлумаченні правомочностей особи у сфері охорони приватного життя (приватності) акцентовано увагу багатьох учених.

Наприклад, В. О. Серьогін розуміє приватність як: прайвесі, або можливість бути залишеним у спокої, як обмежений доступ до себе, як секретність, як контроль над персональною інформацією, як захищену індивідуальність, як інтимність[58, с. 107–140]. Поряд з цим, учений наводить перелік додаткових правомочностей, які також, на думку автора, виступають об'єктом захисту від незаконного втручання, а саме: «право на свободу сімейних відносин; право на охорону таємниці міжособистісних відносин приватного характеру; право на блокування інформації (кореспонденції, телефонних переговорів, поштових і телеграфних повідомлень, Інтернету, ЗМІ); право

спілкування з іншими індивідами: право на захист від шкідливої інформації; право на свободу совісті і таємницю віросповідання» [58, с. 107–140]. Інші автори відносять до об'єкта права на недоторканність приватного життя більш особистісну інформацію, яка включає внутрішню інформаційну свободу особи, тобто право на охорону інформації про себе, а також право на особисту та сімейну таємницю [59, с. 62]. В англосаксонській правовій науці під час визначення права на приватне життя використовується дефініція «privacy», яка у довільному тлумаченні трактується як «право бути залишеним у спокої» [60]. Однак, розуміння наведеної дефініції не обмежується висловленим формулюванням. Наприклад, А. Уестін тлумачить термін «privacy», як право особи обирати, до якого ступеня вона може бути відкритою для оточуючого її суспільства [61]. Також заслуговує на увагу думка Е. Блоуштайна, який розуміє досліджувану категорію у її тісному зв'язку з недоторканністю особистості, індивідуальною свободою, незалежністю та гідністю людини [62]. У сучасній зарубіжній літературі право на недоторканність приватного життя дедалі частіше асоціюється із правом на спокій приватного життя, правом на побутове життя та правом на таємницю приватного життя [53, с. 174].

К. С. Сакович та І. Весью справедливо роблять акцент на актуальності захисту приватної інформації із появою всесвітньої мережі Інтернет. Велика кількість відкритої, особистої інформації в Інтернеті, за висловленням К. С. Саковича, «породжує розширення можливостей нагляду та контролю» [63, с. 41]. І. Весью продовжує висловлену думку та зазначає, що веб-сайти потребують значної кількості персональних даних для створення віртуального профілю або розширення його можливостей. Поява різноманітних пристроїв з мобільними версіями таких сайтів спричинила не тільки більш глибоке занурення у віртуальні світи, але й небезпеку в питанні збереження і захисту приватності [64].

Підсумовуючи наведені судження, а також на підставі аналізу міжнародного законодавства, можемо сформулювати основні види правомочностей, які так чи інакше можуть бути віднесені до права на недоторканність приватного життя: а) право на свободу

розпоряджатися собою та своїм життям; б) право на таємницю приватного життя; в) право на таємницю кореспонденції та листування; г) право на свободу думки; д) право на свободу совісті та віросповідання; є) право на свободу вираження своєї думки; е) право на користування рідною мовою; ж) право на захист особистості, честі, гідності та ділової репутації, національної приналежності; з) право на захист житла; і) право на таємницю голосування.

Зосереджуючись на правовій природі приватного життя, слід наголосити на складності виокремлення конкретних меж цього поняття. На нашу думку, сутність приватного життя як правової категорії найбільш вдало розкривається під час аналізу практики Європейського суду з прав людини (скорочено – ЄСПЛ), рішення якого мають обов'язків характер для національної правозастосовної практики.

Слід зазначити, що ЄСПЛ як правило застосовує широкий підхід до тлумачення приватного життя, офіційне визначення якого по суті відсутнє та взагалі не підлягає конкретизації [65]. У той же час, із змісту деяких рішень ЄСПЛ вбачається, що розуміння приватного життя включає будь-які сфери особистого життя людей, які передбачають вільний розвиток та наповнення його певним індивідуально визначеним змістом. Наприклад, у рішенні «Німітц проти Німеччини» від 16 грудня 1992 року Суд висловив позицію згідно з якою «було б недоречно обмежувати поняття особистого/приватного життя «внутрішнім колом», як критерієм, який визначає здатність людини жити особистим життям, із виключенням зовнішнього кола життєдіяльності особи. Повага до особистого/приватного життя повинна також включати певну сукупність правомочностей для встановлення та розвитку взаємовідносин у інших сферах суспільних відносин» [66]. Із наведеної позиції можна зробити висновок, що розуміння приватного життя не обмежується внутрішньо сімейними відносинами, а має набагато ширші рамки, які передбачають право на розвиток взаємовідносин з іншими особами та зовнішнім світом, виходячи за межі суто особистого життя. Більше того, в окремих випадках рішення ЄСПЛ фактично ототожнюють приватне життя особи із професійною діяльністю, яка передбачає виникнення трудових відносин [66].

Також, безсумнівним свідченням широкого підходу до тлумачення приватного життя виступає віднесення ЄСПЛ до таких відносин й екологічної безпеки громадян, про що недвозначно наголошено одразу у декількох рішеннях Суду, одне з яких привертає особливу увагу, з причини встановлення в ньому взаємозв'язку між погіршенням екологічної обстановки в регіоні та якістю життя громадян, в тому числі й приватного [67].

Національне законодавство також керується правилом, згідно з яким перелік відомостей про особу, які визнаються конфіденційною інформацією, не є вичерпним. Таке положення зафіксовано у рішенні Конституційного Суду України від 20 січня 2012 року № 2-рп/2012 «Щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України» [15].

Зокрема, Конституційний Суд України зазначив, що «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 займає посаду, пов'язану з виконанням функцій держави або органів місцевого самоврядування, посадових або службових повноважень. Така інформація про особу є конфіденційною» [15].

Виходячи з наведеного визначення, можемо сформулювати певні особливості правової природи приватного життя у національному законодавстві. Наприклад, замість правової конструкції «приватне життя», яка активно використовується у міжнародному законодавстві, в Конституції України застосовується категорія «особисте життя», що, в принципі, є ідентичним, а тому – не викликає суттєвих зауважень.

Поряд з цим, сутність інституційного підходу, який застосовується у національному законодавстві, проявляється у активному використанні на законодавчому рівні окремих сфер особистого життя людей, як-от: сімейного, інтимного, побутового і т.д., що не в повній мірі відображає багатогранність та багатоаспектність розуміння приватного життя.

Бернар Бен'є [53, с. 172] також визнає наявність тенденції щодо розширення змісту категорії приватне життя, яка перестає

обмежуватися рамками прихованої або невідомої іншим сфери діяльності індивіда, у зв'язку з чим існує доцільність розмежування понять «особисте життя» і, більш широкого - «приватне життя», що включає, на його думку, «приватне суспільне життя». Разом з цим, характеристика вищенаведених категорій не заважає переважній більшості авторів визнавати, що приватне й особисте життя за умов стрімкої динаміки інформаційних відносин дедалі більше піддаються негативному впливу.

Враховуючи те, що визначення усього розмаїття відносин приватного життя навряд чи можливе, доцільним є виокремлення його основних ознак, а саме: а) приватне життя являє собою особливу сферу життєдіяльності суспільства, ступінь відкритості якої визначається кожною особою в індивідуальному порядку; б) приватне життя має комплексний характер з невизначеним переліком його різновидів; в) межі приватного життя мають суб'єктивний характер та визначаються самим індивідом.

Таким чином, функціонування інституту охорони приватного життя створило передумови для формування нового правового режиму, пов'язаного із захистом персональних даних фізичних осіб, який фактично виступає галуззю інституту охорони приватного життя. Формування нової правової категорії «персональні дані» являє собою особливий різновид інформації про фізичну особу, з особливим правовим режимом, необхідність якого обумовлена потенційною небезпекою спричинення шкоди правам та свободам особи під час порушення правил її обробки.

У США та більшості європейських країн персональні дані набули правового забарвлення майже 90 років тому, як один з ключових елементів захисту прав на недоторканність та повагу приватного життя громадян [68, с. 67]. На сьогодні більше 40 країн світу імплементували міжнародні правові норми у сфері захисту персональних даних. Слід зазначити, що в усіх національних правових актах необхідність захисту персональних даних розглядається як обов'язковий елемент захисту прав і свобод громадян. У той же час, виникнення правової категорії «захист персональних даних» поряд із «охороною права на приватне життя» та

«інформацією про особу» започаткувало наукову дискусію щодо їх співвідношення.

Наприклад, А. В. Кардаш фактично ототожнює поняття персональних даних та інформацію про особу, мотивуючи це тим, що як за допомогою персональних даних, так і інформації про особу з'являється можливість ідентифікації індивіда. Вчена наводить класифікацію персональних даних, з їх поділом на звичайні та чутливі (вразливі), розуміючи останні як «дані про расове або етнічне походження; політичні, релігійні або світоглядні переконання; членство в політичних партіях та професійних спілках; засудження до кримінального покарання; дані, що стосуються здоров'я, статевого життя, а також біометричні або генетичні дані» [26, с. 11].

Інші автори безпосереднього зв'язку між захистом персональних даних та охороною приватного життя не проводять, хоча й не відкидають їх взаємозалежності та взаємообумовленості.

Міжнародне та зарубіжне законодавство також не надає чіткого уявлення щодо співвідношення досліджуваних правових категорій. Наприклад, у преамбулі Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних [69], в якості мети гармонізації національного законодавства наголошується на посиленні гарантій прав осіб і, передовсім, права на недоторканність приватного (особистого) життя в умовах автоматизованої обробки даних про неї. Аналогічне положення міститься й у Рекомендації Ради ОЕСР щодо основних положень про захист приватного життя та міжнародних обмінів персональними даними [70].

Свідченням взаємоузгодженості та взаємодоповненості міжнародних правових норм та норм національного законодавства є положення Регламенту № 679 [19], яким передбачено, що в разі необхідності уточнення його положень або обмеження його норм законодавством держав-членів, у такому разі останні можуть, мірою необхідності узгодження і забезпечення розуміння положень національного законодавства особами, на які вони поширюються, інкорпорувати елементи цього Регламенту у своє національне законодавство.

Крім цього, Європейський суд у своїй практиці, що стосується статті 8 Конвенції про захист прав людини і основоположних свобод,

також визнав, що захист персональних даних від розголошення є одним з найважливіших елементів здійснення права особи на повагу до особистого і сімейного життя, що в кінцевому випадку сприяє додержанню державами зобов'язань, взятих ними як Договірними Сторонами [71].

Також заслуговує на увагу й вищезгадане рішення Конституційного Суду України, в якому КСУ, даючи офіційне тлумачення частин першої та другої статті 32 Конституції України, фактично проводить паралель між особистим життям індивідів та персональними даними про них, визначаючи останні як сукупність відомостей про національність, освіту, сімейний стан, релігійні переконання, стан здоров'я, матеріальний стан, адресу, дату і місце народження, місце проживання та перебування тощо, дані про особисті майнові та немайнові відносини особи з іншими особами, зокрема членами сім'ї, а також відомості про події та явища, що відбувалися або відбуваються у побутовому, інтимному, товариському, професійному, діловому та інших сферах життя особи, за винятком даних стосовно виконання повноважень особою, яка займає посаду, пов'язану зі здійсненням функцій держави або органів місцевого самоврядування [15].

З наведеного визначення стає очевидним, що в національному законодавстві розуміння особистого (приватного) життя нерозривно пов'язано із персональними даними особи, і якщо у міжнародних правових актах останні виступають в якості структурного елементу приватного життя, то із змісту українських законів можна зробити висновок про рівнозначність досліджуваних категорій.

Відтак, можемо припустити наявність прямого зв'язку між захистом персональних даних та недоторканністю особистого життя, а також його складових елементів – сімейної, побутової, інтимної, товариської, професійної, ділової та інших сферах життя особи.

З іншого боку, не можемо оминути увагою позицію законодавця щодо застосування широкого підходу у визначенні сфер особистого життя особи. Зверніть увагу, у коментованому рішенні Конституційного Суду України [15] поряд із суто особистісними сферами приватного життя, такими як сімейна, інтимна, побутова,

згадуються й інші, які передбачають участь громадян у професійних, ділових, товариських та деяких інших стосунках, які також віднесені законодавцем до сфери особистого життя.

Разом з цим, Закон України «Про захист персональних даних» не конкретизує інформацію, яка складає зміст персональних даних, наголошуючи, однак, на тому, що останні являють собою «відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована» [72]. Таким чином, знову законодавець дає зрозуміти, що інформація, яка може бути представлена у вигляді персональних даних, не обмежується приватною, особистою чи сімейною сферою життя індивіда.

Зокрема, персональні дані можуть цілком включати відомості про суспільне життя індивіда, його службову або професійну діяльність, а також інші сфери життя особи, які не завжди можуть охоплюватися поняттям приватне життя або, принаймні, викликати сумнів такого віднесення до зазначеної категорії.

З аналізу існуючих положень законодавства випливає, що потенційно персональні дані включають, поряд з відомостями про приватне життя особи (таємницею приватного життя), низку відомостей, які охоплюються багатьма іншими правовими категоріями, виникнення яких у правовій матерії відбулось набагато раніше категорії «персональні дані».

Отже, не заперечуючи нерозривного прямого зв'язку між захистом персональних даних та недоторканністю приватного (особистого) життя, все ж таки слід зазначити, що вказані правові категорії не є тотожними.

В. М. Брижко пов'язує захист персональних даних із відомостями про ідентифіковану особу, які підлягають захисту [1, с. 51, 90]. У більш вузькому сенсі розуміє персональні дані В. Козак, пов'язуючи їх з обробкою інформації з конкретно визначеною метою. У цьому контексті вчений робить акцент безпосередньо на захисті персональних даних, що на нашу думку звужує розуміння вказаного правового інституту [73, с. 7]. Більш широкий зміст щодо розуміння персональних даних вкладає О. С. Соколова та пов'язує останні із «заходами спрямованими на попередження неправомірних

дій з персональними даними, а також на захист і відновлення порушених прав» [74, с. 79]. Також досить цікавою виглядає позиція А. М. Чернобай, яка розглядає персональні дані під кутом трудових відносин. Вчена розглядає досліджувану правову категорію як «сукупність організаційно-правових, інженерно-технічних, криптографічних та інших заходів, що вживаються власником цих даних або іншими особами за його замовленням, з метою запобігання заподіянню шкоди інтересам власника та особи, якої вона стосується, її неконтрольованому поширенню» [75, с. 125].

У цілому, аналізуючи судження науковців, слід зазначити, що деякі термінологічні та конструктивні розбіжності в процесі з'ясування правової природи захисту персональних даних ні в якому разі не суперечать головній ідеї – виокремленні правових норм, що регулюють захист персональних даних у самостійний правовий інститут.

Серед зарубіжних авторів можемо зустріти аналогічні судження щодо самостійності правового інституту захисту персональних даних у порівнянні з правом на недоторканність особистого життя [76; 77], що також підтверджує загальний вектор розвитку права в цьому напрямку, який орієнтує нас на самостійність правового інституту персональних даних.

Не менш важливе питання, яке виступає предметом обговорення вітчизняних та зарубіжних науковців та стосується з'ясування правової природи персональних даних, пов'язано із визначенням права на захист персональних даних у якості одного з фундаментальних прав особи.

Не викликає заперечень той факт, що динамічний розвиток самої ідеї забезпечення прав людини слугує напевно головною причиною її постійного прогресивного розвитку, у зв'язку з чим ми можемо спостерігати її наповнення новим змістом та значенням. Інакше кажучи, новими правами та свободами, які з розвитком суспільства поступово починають сприйматися у якості невід'ємних та фундаментальних.

Подібно тому, як право на захист приватного життя стало наслідком втілення ідеї особистої свободи індивіда, право на захист персональних даних виступило результатом бурхливого розвитку

інформаційно-телекомунікаційних технологій та сформованого на цій підставі інформаційного законодавства.

З іншого боку, право на захист персональних даних – це необхідний елемент інформаційної культури сучасного суспільства, за відсутності якого забезпечення високого рівня захисту особи в інформаційному просторі є неможливим.

У той же час, застосування деякими науковцями правової конструкції «право на конфіденційність персональних даних» [78, с. 61], на нашу думку є некоректним. Вважаємо, що правовий режим конфіденційності інформації скоріше за все може бути адресований операторам персональних даних та є, по суті, безумовною вимогою щодо нерозголошення інформації, а в деяких випадках взагалі не залежить від волі вказаних суб'єктів.

З іншого боку, конфіденційність можна розглядати як один із багатьох способів захисту персональних даних. Разом з цим, слід відмітити, що режим конфіденційності персональних даних позитивно впливає на встановлення режиму конфіденційності інформації, а рівно – на забезпечення гарантій недоторканності приватного життя, шляхом обмеження доступу до такої інформації третіх осіб.

Вказана обставина є вельми актуальною, з огляду на те, що а ні гарантії захисту персональних даних, а ні розуміння особистого життя громадян як комплексного правового явища, в Законі України «Про захист персональних даних» не визначені.

З'ясування правової природи захисту персональних даних передбачає відображення сутнісних ознак цього правового явища, та в кінцевому випадку сприяє розумінню їх місця та значення в правовій науці. На цій підставі вважаємо цілком доречним, з метою реалізації мети та завдань нашого дослідження розглянути зміст правової категорії «персональні дані» та її характерні ознаки, що в кінцевому випадку дозволить чітко сформулювати предмет цього дослідження та сформулювати сутність вітчизняного підходу до адміністративно-правового регулювання захисту персональних даних в діяльності Національної поліції.

Розуміння правової категорії «персональні дані» найбільш точно, на нашу думку, може бути розкрито через співвідношення із

дефініціями «конфіденційна інформація», «інформація про фізичну особу», «інформація», які також врегульовані чинним законодавством, але мають свої особливості.

Правова конструкція «інформація про фізичну особу» визначена у частині 1 статті 11 Закону «Про інформацію» та означає відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована [79]. Причому в даному випадку законодавець поряд із терміном «інформація про фізичну особу» використовує й словосполучення «персональні дані», таким чином підкреслюючи їх ідентичність. Аналогічне визначення міститься й у Законі України «Про захист персональних даних» [72]. У цьому контексті не можемо погодитися із Р. А. Майдаником, який використовуючи термін «інформація про особу» без вказівки на її фізичний статус, фактично ототожнює його із персональними даними [80, с. 45–48].

Слід зазначити, що Закон України «Про захист персональних даних» був прийнятий відповідно до положень Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних від 28.01.1981 [69], яка визначає персональні дані в якості будь-якої інформації, за допомогою якої особа ідентифікована або може бути конкретно ідентифікована

У цьому аспекті дискусійним або, навіть, нелогічним видається положення частини 1 статті 2 Закону України «Про захист персональних даних», в якій визначено поняття знеособлених персональних даних як процесу, пов'язаного із вилученням відомостей, які дають змогу прямо чи опосередковано ідентифікувати особу [72].

Тому видається дивним та нелогічним встановлене законодавцем положення про те, що знеособленість за певних обставин властива персональним даним. Мусимо припустити, що більш точним формулюванням у цьому контексті буде віднесення знеособлених відомостей не до персональних даних, а до інформації про персональні дані. За такого випадку зазначене нами коректоване формулювання буде цілком узгоджуватися із визначенням персональних даних, наведеним у статті 2 коментованого закону.

Також пропонуємо звернути увагу на рішення Конституційного Суду України [15], відповідно до якого такі правові категорії як конфіденційна інформація, інформація про фізичну особу, інформація про особисте та сімейне життя фактично ототожнюються. А в резолютивній частині рішення Конституційного Суду України у справі щодо офіційного тлумачення статей 3, 23, 31, 47, 48 Закону України «Про інформацію» та статті 12 Закону України «Про прокуратуру» (справа К.Г.Устименка), Суд фактично відніс до конфіденційної інформації про фізичну особу відомості про майновий стан особи та інші персональні дані [81].

У зв'язку з цим виникає запитання, чи доречно змішувати ці поняття та чи існують реальні підстави щодо їх розмежування. Відповідаючи на це запитання, слід звернутися до ч. 2 статті 11 Закону України «Про інформацію», яка, хоча й дещо звужено, але надає перелік конфіденційної інформації про фізичну особу, до якої, зокрема, належать дані про її національність, освіту, сімейний стан, релігійні переконання, стан здоров'я, а також адреса, дата і місце народження [79]. Вважаємо, що наведений перелік не може бути вичерпаний виключно зазначеними даними, про що безсумнівно має зазначатися у нормі вказаної статті.

Більш виважено законодавець підійшов до визначення конфіденційної інформації у статті 7 Закону України «Про доступ до публічної інформації», де остання визначається як інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень, та яка може поширюватися у визначеному ними порядку за їхнім бажанням відповідно до передбачених ними умов [82]. У даному випадку цілком справедливо законодавцем було зроблено акцент не на сферах приватного життя громадян, які підлягають охороні, а на режимі інформації, доступ до якої обмежено.

Вважаємо, що такий підхід може слугувати основним критерієм, який відмежовує конфіденційну інформацію від персональних даних. Якщо правова категорія «конфіденційна інформація» характеризується ступенем обмеження загального доступу до неї (фактично – режимом її функціонування), то дефініція «персональні

дані» скоріше відображає внутрішні властивості інформації, як такої, що належить певній особі.

І ще один принциповий момент. Не можемо погодитися із позицією законодавця, який визначає персональні дані у якості відомостей. По-перше, тлумачення цього терміну не відображено в жодному нормативно-правовому акті в інформаційній сфері.

Довідкова література говорить нам про те, що відомості тлумачаться як повідомлення, вісті, факти, дані про кого-небудь [83, с. 176]. Тобто жодним чином відомості не асоціюються з інформацією, тоді як, на наше переконання, персональні дані – це все ж таки у першу чергу інформація про фізичну особу.

Тому найбільш правильним підходом в такому випадку було б розкрити зміст правової категорії «персональні дані» через категорію «інформація», акцентуючи увагу на відмінних ознаках останньої, які полягають у її структурованості, а також в тому, що саме інформація, а не відомості підлягає збору та обробці, з метою її подальшого використання у інформаційних системах.

Таким чином, проведений аналіз дозволяє нам сформулювати визначення персональних даних як інформації, яка підлягає обробці в інформаційних системах за допомогою засобів автоматизації та включає перелік формалізованих даних про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована.

Зверніть увагу, що відмінною рисою наведеного визначення виступає нерозривний зв'язок особи – суб'єкта персональних даних та інформації про неї. Причому такий зв'язок може бути як безпосереднім, так і опосередкованим. Наприклад, безпосередній зв'язок проявляється шляхом посилання на суб'єкта персональних даних або властиві йому індивідуальні риси, які характеризують конкретно визначену особу, такі як зображення, голос та персональні ідентифікатори. З іншого боку, опосередкований зв'язок проявляється у відсутності прямої вказівки на конкретно визначену особу, хоча аналіз наявної сукупної інформації про суб'єкта безсумнівно ідентифікує його особу.

Важливість зазначеної інформації полягає в тому, що втрата або відсутність такого зв'язку не дозволяє віднести інформацію до

персональних даних. І в даному випадку доцільно згадати про положення частини 1 статті 2 Закону України «Про захист персональних даних», яка встановлює положення щодо знеособлення персональних даних, тобто нормативно закріплює хибне правило, згідно якого відсутність зв'язку між суб'єктом персональних даних та інформацією про нього визначається як персональні дані.

У той же час, питання щодо знеособлення даних породжує й інші, не менш важливі проблеми, оскільки використання сучасних технологій із знеособлення даних не гарантують у повній мірі відсутність можливості співвіднесення викладеної інформації із суб'єктом персональних даних.

А тому, правова категорія «знеособлення» потребує більш докладного вивчення та врегулювання на законодавчому рівні механізму його здійснення, з можливим розмежуванням за окремими рівнями або технологіями, які гарантуватимуть неможливість ідентифікації знеособленого суб'єкта.

Таким чином, на підставі проведеного дослідження можна зробити наступні висновки.

Вважаємо, що правова природа адміністративно-правового захисту персональних даних найбільш точно розкривається у сформульованому визначенні останніх, як інформації, яка підлягає обробці в інформаційних системах за допомогою засобів автоматизації та включає перелік формалізованих даних про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована.

З наведеного визначення стає очевидним, що в національному законодавстві розуміння персональних даних нерозривно пов'язано із особистим (приватним) життям особи, і якщо у міжнародних правових актах перші виступають в якості структурного елементу приватного життя, то із змісту українських законів можна зробити висновок про рівнозначність досліджуваних категорій.

Враховуючи те, що охоплення усього розмаїття відносин приватного життя навряд чи можливе, науковцем сформульовано характерні його ознаки, а саме: а) приватне життя являє собою особливу сферу життєдіяльності суспільства, ступінь відкритості якої визначається кожною особою в індивідуальному порядку; б) приватне

життя має комплексний характер з невизначеним переліком його різновидів; в) межі приватного життя мають суб'єктивний характер та визначаються самим індивідом.

1.3. Адміністративно-правовий режим захисту персональних даних

Перед тим, як приступити до аналізу правового режиму персональних даних як інформації обмеженого доступу слід зазначити, що сам термін «правовий режим» в теорії права має різне тлумачення, а тому вимагає певних уточнень. В цілому, правовий режим в якості правової категорії досить часто використовується як у науково-правовій літературі, так і в законодавстві.

Загалом слід констатувати єдність поглядів науковців щодо розуміння правової категорії правових режимів. Наприклад, Ю. П. Битяк тлумачить вказану правову категорію у вигляді комплексу організаційно-правових засобів, зміст яких наповнений сукупністю дозволів та заборон, а призначення полягає в уточненні напрямку правового регулювання [84, с. 185]. Таке твердження виглядає доволі точним та змістовним, оскільки віддзеркалює змістовну складову надзвичайних правових режимів з погляду на використання правових засобів в процесі їх реалізації. С. Г. Стеценко визначає сутність правового режиму через його критерії, до яких вчений відносить ступінь жорсткості юридичного регулювання, наявність відомих обмежень та пільг, допустимий рівень активності суб'єктів, межу їх правової самостійності тощо [85, с. 186]. Слід зазначити, що на нашу думку, критерії, використані автором, дуже яскраво демонструють обмежувальний характер надзвичайних правових режимів. Їх правова природа побудована на активному використанні заборон та обмежень. Д. М. Бахрах розкриває дуалістичну природу правового режиму: з одного боку зазначене правове явище вчений розглядає як певну сукупність суспільних відносин, а з іншого – наголошує на їх юридичному оформленні, тобто «закріпленні юридичними

нормами та забезпеченні сукупністю юридично-організаційних засобів» [86, с. 201]. Погоджуємося з думкою науковця, з тією лише поправкою, що суспільні відносини, про які йдеться у авторському твердженні, у сфері функціонування надзвичайних правових режимів, носять яскраво виражений державно-управлінський характер. У такому випадку варто говорити скоріше про відносини у сфері державного управління, але не про суспільні відносини. У підручнику з адміністративного права та адміністративної діяльності, за редакцією Л. Л. Попова, наводиться доволі розгорнута класифікація правових режимів, які, на думку вченого розподіляються на: загальні, універсальні та похідні [87, с. 162–163]. Теоретико-практична цінність зазначеної позиції проявляється у розкритті різноплановості та водночас універсальності правових режимів. Їх правова природа досить регламентована та передбачає застосування жорстких адміністративно-правових обмежень.

Також, адміністративно-правові властивості під час характеристики надзвичайних правових режимів підкреслюють і провідні українські вчені С. В. Ківалов та Л. Р. Біла, які виділяють ознаки, властиві адміністративно-правовим засобам регулювання, а саме: централізований порядок управління, імперативний метод правового впливу, юридична нерівність суб'єктів правовідносин [88, с. 38].

Слід зазначити, що правові режими виступають не тільки в якості предмета наукових досліджень, але й слугують регулятором суспільних відносин у багатьох законодавчих актах.

Наприклад, Лісовий кодекс України [89] містить декілька дефініцій так чи інакше пов'язаних із функціонуванням адміністративних правових режимів в процесі впорядкування лісових відносин, а саме: «режим використання земель», «режим обмеженого лісокористування», «режим використання лісового фонду України» тощо.

Водний кодекс України також оперує правовими категоріями різноманітних правових режимів під час регулювання адміністративно-правових відносин у сфері водного господарства. Наприклад, законодавець використовує поняття особливого санітарно-епідеміологічного режиму, гідрологічного режиму водного об'єкта, режиму обмеженої господарської діяльності, режимів роботи водосховищ тощо.

Поряд з цим, деякі законодавчі акти спеціально визначають правовий режим окремих територій. Наприклад, Законом України «Про правовий режим території, що зазнала радіоактивного забруднення внаслідок Чорнобильської катастрофи», який регулює питання поділу території на відповідні зони, режим їх використання та охорони, умови проживання та роботи населення, господарську, науково-дослідну та іншу діяльність в цих зонах [90].

Окрема група правових режимів закріплена на конституційному рівні, а також у спеціальних законах. Йдеться насамперед про правові режими власності (п. 7 ч. 1 статті 92); державного кордону (п. 18 ч. 1 статті 92); воєнного і надзвичайного стану (п. 19 ч. 1 статті 92); зон надзвичайної екологічної ситуації (п. 19 ч. 1 статті 92); економічний та міграційний (п. 8 ч. 2 статті 92) [57].

Виходячи із наведених прикладів можна зробити висновок, що використання правової категорії «правовий режим» має універсальний характер та застосовується для характеристики численних правових явищ, одна частина яких пов'язана із звичайною життєдіяльністю та нормальним станом правового об'єкта, а інша – із функціонуванням спеціальних або особливих режимів. Спеціальний (винятковий) характер правового режиму може позначатися або безпосередньо у законодавчому акті [91; 92], або ж випливати із змісту самого законодавчого акту [93].

У багатьох законодавчих актах зазначається один основний - загальний правовий режим, або режим звичайного стану, а в вигляді виключення визначаються особливі або спеціальні режими. У якості прикладу наведемо Сімейний кодекс, який встановлює законний режим майна подружжя в якості основного, тоді як інші режими, зокрема договірний, слід розглядати в якості спеціального.

У той же час, довільне використання дефініції «правовий режим» в законодавстві жодним чином не сприяє його уніфікованому розумінню, а відтак – єдиноманітному застосуванню в нормативно-правових актах, що опосередковано може доводити багатогранність та неоднозначність самої досліджуваної категорії.

В юридичній літературі також сформувалось неоднозначне розуміння термінів «режим», «правовий режим», «соціальний режим»,

які у переважній більшості виступають в якості предмету наукових досліджень із загальної теорії права.

Перш за все з'ясуємо розуміння вказаних дефініцій на енциклопедичному рівні. Етимологія терміну «режим», згідно Юридичної енциклопедії за редакцією Ю. С. Шемшученка, має латинське (французьке) походження та означає процес управління [94, с. 456]. З інших джерел з'ясовуємо, що будь-який режим функціонує в якості встановленого національним законодавством та нормами міжнародного права порядку в суспільних відносинах [95, с. 283].

Дослідження правової категорії «правовий режим» пройшло декілька етапів, найбільш ранній з яких датується серединою минулого століття, коли численні радянські науковці, такі як Н. Г. Александров, С. Г. Березовська, І. С. Самощенко, фактично ототожнювали вказану правову дефініцію із забезпеченням режиму законності в державному управлінні [96, с. 10].

Наступний етап наукового пошуку в окресленому напрямку розпочався з проголошенням незалежності української держави та тривав до початку 2000-х р.р. У цей період розуміння правового режиму у наукових працях провідних дослідників як правило асоціювалось із політичним устроєм в країні, механізмами державної влади, а також сукупністю форм та методів їх реалізації [97, с. 74; 98, с. 82; 99, с. 124]. Тобто правові режими фактично утворювали сукупність елементів правової політики держави [100, с. 19].

Новітній етап дослідження правових режимів характеризується кардинальною трансформацією філософії вказаної правової категорії, розуміння якої ототожнювалось та наразі асоціюється передовсім із правом, а не з державою чи державною владою.

Найбільш точно з цього приводу висловилась Т. П. Мінка, яка підкреслила провідне значення права, держави та політики у виникненні та функціонуванні правових режимів [101, с. 49]. Вказана позиція автора цілком справедливо підтверджує ключову роль права в процесі державотворення, формування правової політики держави та реалізації комплексу правових засобів, які утворюють цілісну систему правових режимів.

Вказана наукова позиція аналогічним чином відображена у підручнику «Загальна теорія держави і права» за редакцією О. В. Петришина та В. Д. Ткаченка, які розкривають зміст правових режимів через функціонування особливого порядку регулювання суспільних відносин «який забезпечується через особливе поєднання залучених для його здійснення способів, методів і типів правового регулювання» [102, с. 410]. Як бачимо, вчені також підкреслюють лідируючу роль права в процесі функціонування правових режимів як особливого різновиду суспільних відносин.

Висловлену думку цілком розділяють С. О. Кузніченко та А. С. Спаський, які характеризують правові режими у якості правової форми, в межах якої здійснюється регулювання певної групи суспільних відносин. При цьому суб'єктами забезпечення функціонування правових режимів використовується сукупність правових засобів, за допомогою яких відбувається реалізація механізмів правового регулювання у часі і просторі [103, с. 73].

Аналогічної думки притримується й І. О. Соколова, яка під правовим режимом розуміє порядок правового регулювання вираженого в комплексі правових засобів, які характеризують особливе поєднання взаємодіючих між собою в процесі регулювання суспільних відносин дозволів та заборон [104, с. 36].

Таким чином, розуміння сутності правових режимів часто залежить від особистого усвідомлення вченими самого поняття «право». На цьому аспекті також зосереджує увагу й Н. Д. Гетьманцева, яка зауважує, що «вчені під різним кутом зору сприймають саме поняття «право», залежно від того, прихильниками яких шкіл вони є (природної чи позитивістської), а тому і бачать різну сутність у даному понятті» [105, с. 327]. При цьому значення правових режимів в роботах вищевказаних науковців обумовлено низкою факторів, пов'язаних із: а) особливим соціальним та правовим значенням суспільних відносин, їх специфічними цілями та завданнями; б) використанням особливих принципів, форм та методів діяльності суб'єктів, які забезпечують функціонування правових режимів.

Під час дослідження правового режиму персональних даних особливу зацікавленість викликає з'ясування його чітких меж в рамках

загального правового режиму інформації з обмеженим доступом. Йдеться насамперед про те, що самі по собі персональні дані навряд чи можна віднести до інформації з обмеженим доступом, а їх конфіденційність, як правило, презюмується.

Як наслідок, правовий режим персональних даних в цілому має складну структуру, обумовлену специфікою самого об'єкта регулювання. З огляду на це можна виділити дві основні складові цього режиму: а) правовий режим «загальнодоступних персональних даних», який функціонує у сфері загального правового режиму інформації, тобто режиму загальнодоступної інформації; б) правовий режим персональних даних обмеженого доступу, який виступає в ролі складового елементу спеціальних правових режимів інформації, тобто сфери правового режиму інформації з обмеженим доступом.

При цьому останній також може бути розподілений на декілька складових, а саме: а) персональні дані, захист яких здійснюється в режимі державної таємниці; б) персональні дані обмеженого доступу, оброблення яких здійснюється в режимі архівної інформації; в) персональні дані, що захищаються в режимі особистої чи сімейної таємниці, а також таємниці приватного життя; г) конфіденційні персональні дані, захист яких здійснюється режимними заходами, передбаченими Законом України «Про захист інформації в інформаційних та телекомунікаційних системах».

Незважаючи на таку складну структуру, можна говорити, що певний інтерес для цього дослідження представляє виключно остання категорія, яка може бути охарактеризована як персональні дані, що захищаються в умовах правового режиму конфіденційності персональних даних як інформації обмеженого доступу в рамках профільного законодавчого акту. Попри те, що правові режими інших категорій персональних даних виступають в ролі різновидів інформації обмеженого доступу, вони не зорієнтовані безпосередньо на захист персональних даних як обмеженої в доступі інформації, а відтак, не виділяють їх у загальному масиві інформації, захист якої здійснюється за умовами цих режимів.

Винятком можна, мабуть, назвати персональні дані, що становлять особисту, сімейну таємницю і таємницю приватного життя, які

за своїми властивостями не можуть не відноситися до конкретного індивіда. Однак у цьому випадку законодавче регулювання будується виключно на визнанні у індивіда права на ці види таємниць і можливості їх самостійної охорони та, як наслідок, мінімального обсягу нормативних положень, що забезпечує велику особисту свободу і відповідає ідеї природних прав. Саме «довірча передача» інформації індивідом іншій особі, тобто розпоряднику або володільцю, обумовлює її захист в рамках спеціального правового режиму конфіденційних персональних даних.

В доповнення до висловленої позиції можна відзначити, що правовий режим конфіденційності персональних даних, відповідно до вимог міжнародних правових актів у сфері захисту персональних даних [19], включає два основні режими персональних даних, а саме: загальний правовий режим конфіденційності персональних даних та спеціальний правовий режим, до якого відносяться: а) особливо чутливі дані; б) генетичні дані; в) біометричні дані; та г) дані щодо стану здоров'я. Державам-членам, зазначається в Регламенті №679, необхідно дозволити мати або вводити подальші умови, в тому числі обмеження, у зв'язку з опрацюванням генетичних даних, біометричних даних або даних стосовно стану здоров'я, що свідчить про посилену увагу законодавця до захисту спеціального правового режиму персональних даних.

У той же час, в роботах деяких науковців мають місце спірні, а подекуди й помилкові, з точки зору адміністративно-правової науки, висновки. Наприклад, А. А. Антопольський використовує для характеристики правового режиму персональних даних та, в цілому, конфіденційної інформації узагальнюючу правову категорію «інформаційний об'єкт», визначаючи останній у якості сукупності правових норм, які стосуються певного об'єкту суспільних відносин. На думку автора, правовий режим інформаційного об'єкта має складатися з правових норм, які регулюють а) порядок його створення; б) механізм передачі та отримання інформації (визначення порядку доступу); в) питання щодо захисту прав суб'єктів інформаційних відносин [106, с. 8].

Вважаємо, що використання термінологічної конструкції «інформаційний об'єкт», який у даному випадку підміняє термін

«інформація» є некоректним. Помилковими, на нашу думку, виглядають й висловлені А. А. Антопольским припущення щодо основних складових елементів правового режиму інформації.

По-перше, не викликає заперечень той факт, що будь-який інформаційний правовий режим наділений власним об'єктом правового впливу. Такий режим може бути встановлений законом щодо конкретного виду інформації, як, наприклад, у випадку з персональними даними, тим самим припускаючи, що такий різновид інформації існує. Дія правового режиму може бути поширена на ту чи іншу інформацію, як, наприклад, у випадку з комерційною таємницею, коли її власник має право виконати запропоновані законом дії і поширити на неї режим комерційної таємниці.

По-друге, «порядок отримання і передачі інформації (включаючи встановлення режиму вільного або обмеженого доступу)» звучить досить дивно, враховуючи, що змістовне навантаження терміну «доступ» включає в себе обидві попередні дії, оскільки неможливий без двох взаємно кореспондуючих складових: права на отримання інформації та обов'язків щодо її надання.

По-третє, посилання виключно на захист «прав суб'єктів щодо об'єкта» можна розглядати як деяке звуження реального змісту правового режиму. Насправді, у якості об'єкту захисту, найімовірніше, слід розглядати сам правовий режим. Наприклад, в результаті порушення правового режиму порядку роботи з відомостями, що становлять державну таємницю не обов'язково може статися їх «витік», що потенційно в кінцевому випадку може призвести до заподіяння шкоди суверенітетові й безпеці держави. В той же час це буде розглядатися як порушення вимог відповідного режиму та передбачати відповідальність винної особи.

Метою правового режиму конфіденційності персональних даних в такому випадку слід вважати встановлення прав і обов'язків суб'єктів відносин, що виникають з приводу персональних даних, як різновиду інформації, їх захист і забезпечення інформаційної безпеки з урахуванням збереження балансу інтересів особи, суспільства і держави. Саме досягнення такого стану в кінцевому підсумку варто розглядати як кінцеву мету встановлення режиму персональних

даних. У зв'язку з цим було б не зовсім правильним розглядати захист персональних даних у якості процесу, спрямованого виключно на захист основоположних прав і свобод людини і громадянина, як це вказується в Законі України «Про захист персональних даних» [72].

З таким твердженням частково можна погодитися, однак говорити про те, що цим вичерпується цільове призначення правового режиму, представляється не зовсім точним. Встановлення певних обмежень на використання і обробку персональних даних в дійсності є результатом прагнення, з одного боку, до забезпечення захищеності прав і свобод особистості шляхом обмеження небажаних дій з інформацією персонального характеру, а з іншого – до забезпечення законних інтересів суспільства та держави, суверенітету і територіальної цілісності України, при обробці інформації про осіб, встановлюючи для останніх певне коло прав і обов'язків, а також гарантуючи їм можливість, за певних, визначених законом умов, мати доступ до персональних даних, обробляти їх, діючи за своїми власними інтересами.

Саме такі основоположні принципи державної інформаційної політики закріплені у Доктрині інформаційної безпеки України, яка підкреслює необхідність додержання прав і свобод людини і громадянина, поваги до гідності особи, захисту її законних інтересів, а також законних інтересів суспільства та держави, забезпечення суверенітету і територіальної цілісності України [107].

Безумовно, для особи право на інформацію і право на доступ до інформації є найважливішими з конституційних прав людини і громадянина, які пов'язані не тільки з вільним обміном інформацією, а й необхідністю забезпечення захисту інформації, що забезпечує особисту безпеку.

Конвенція Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних [69] у своїй преамбулі ясно вказує на необхідність збереження балансу інтересів особи в частині захисту її фундаментальних прав і свобод, зокрема права на повагу до приватного життя, в той же час визнаючи необхідність узгодження її з ідеєю свободи інформації та інформаційного обміну між народами. Ця ідея також простежується й у Регламенті № 679 [19], у п. 1

якого зазначається, що «принципи і норми щодо захисту фізичних осіб у зв'язку з опрацюванням їхніх персональних даних передбачають, незалежно від їхнього громадянства або місця проживання, дотримання їхніх фундаментальних прав і свобод, зокрема їхнього права на захист персональних даних».

Із змісту ст. 32 Конституції України також стає очевидним, що обмеження прав і свобод можливо тільки в тій мірі, яка необхідна для захисту прав і законних інтересів інших осіб, забезпечення оборони країни і безпеки держави, і тільки на підставі закону. Обмеження обробки персональних даних в зв'язку з цим може розглядатися наріжним каменем захисту прав і свобод особи в інформаційній сфері. Отже, існування правового режиму персональних даних пояснюється необхідністю забезпечення особистої інформаційної безпеки індивіда, тобто створення умов, що виключають посягання на права і законні інтереси особи з використанням персональної інформації, що варто розглядати в якості основної – кінцевої мети встановлення правового режиму персональних даних, за обов'язкової умови збереження балансу інтересів суспільства і держави, які можуть бути пов'язані з необхідністю використання відомостей про індивідів.

Об'єктом правового режиму конфіденційності персональних даних як інформації обмеженого доступу слід розглядати відносини, що виникають у зв'язку з обробкою персональних даних, тобто інформації, переданої індивідом іншим суб'єктам права за умови дотримання її конфіденційності, що й дозволяє розглядати їх як інформацію з обмеженим доступом або конфіденційну інформацію. Таким чином, об'єктом спеціального правового режиму персональних даних як інформації обмеженого доступу слід розглядати відносини, що виникають у зв'язку з обробкою «конфіденційних персональних даних» – тобто персональних даних, щодо яких на підставі положень закону встановлено вимогу щодо дотримання їх конфіденційності і, як наслідок, поширення правового режиму їх конфіденційності.

Коло суб'єктів спеціального правого режиму персональних даних вкрай широке, адже його суб'єктами можуть бути фізичні та юридичні особи, органи державної влади та органи місцевого

самоврядування. Виокремлено специфіку правового режиму персональних даних з врахуванням поділу всього кола потенційних суб'єктів, визначених Законом України «Про захист персональних даних», на кілька основних груп:

- суб'єкт персональних даних – завжди фізична особа, інформація про яку міститься в інформаційній системі персональних даних.
- розпорядник – орган державної виконавчої влади або орган місцевого самоврядування, юридична або фізична особа, що організують та (або) здійснюють обробку персональних даних, а також визначають цілі і зміст обробки персональних даних.
- уповноважений орган із захисту прав суб'єктів персональних даних. З огляду на характер цього дослідження і його цілі, тобто розгляд відносин, що складаються з приводу конфіденційних персональних даних, до вищенаведеного переліку можна внести деякі корективи.

Як і у випадках з іншими різновидами конфіденційної інформації основними учасниками таких відносин слід визнати: – володільця інформації (таємниці) і конфідента, якому вона довіряється, тобто якому надається доступ до інформації. Стосовно відносин з приводу персональних даних, очевидно, цими особами будуть суб'єкт персональних даних – володілець і розпорядник – конфідент. Саме цей факт зумовлює досить типову систему відносин між ними, яку можна описати схемою «володілець – конфідент». Основною відмінністю таких відносин є, як правило, можливість володільця визначати правила і порядок доступу до інформації, фактично визначати режим інформації – обмежити доступ до неї або зробити загальнодоступною; він також має право вимагати дотримання її конфіденційності в разі передачі її конфіденту – розпоряднику. В результаті відмінністю правового становища суб'єкта персональних даних, як учасника інформаційних відносин у сфері захисту персональних даних, слід вважати наявність в нього безумовного права на визначення режиму власних персональних даних, а саме:

- їх збереження у таємниці (особистій, сімейній, приватній тощо), якщо інше не передбачено законом;

- їх передачу розпоряднику за умови збереження їх конфіденційності, яка презюмується законом;
- зробити відомості про себе загальнодоступними, тобто застосувати режим загальнодоступної інформації про персональні дані.

Поряд з цим, правове положення розпорядника (конфідента) обумовлено обов'язком щодо збереження конфіденційності персональних даних, що виступає необхідною умовою їх обробки та не може бути скасовано на власний розсуд.

Наявність у системі відносин з обробки персональних даних органу із захисту прав суб'єктів персональних даних обумовлено специфікою самих відносин, враховуючи, що однією зі сторін відносин з обробки персональних даних є індивід, який часто не володіє істотними можливостями по контролю за обігом інформації про себе та дотримання в цілому режиму персональних даних розпорядниками, яких може налічуватися багато десятків, а то й сотні і навіть тисячі. В цьому відношенні орган із захисту прав суб'єктів персональних даних виступає органом адміністративного контролю (нагляду) за дотриманням законодавства про персональні дані розпорядниками і забезпечує захист прав суб'єктів персональних даних, що зумовлює специфіку його правого статуту.

В той же час, у відносинах з приводу обробки персональних даних та забезпечення їх конфіденційності приймають участь й інші суб'єкти інформаційних відносин, які побіжно згадуються в Законі України «Про захист персональних даних», а саме: а) працівник, тобто особа, яка знаходиться у трудових відносинах з розпорядником та має доступ до персональних даних в межах виконання своїх посадових обов'язків; б) особа, відповідальна за організацію обробки персональних даних в організаціях; в) особа, яка здійснює безпосередню обробку персональних даних за дорученням розпорядника.

Відзначимо, що оскільки персональні дані досить універсальна категорія і може бути об'єктом як публічно-правових відносин (формування державних автоматизованих систем і інші випадки), так і приватноправових відносин (відносини з просування товарів та послуг на ринку), то відповідно становище суб'єктів може бути

як рівним, так і нерівним. Насправді дуже часто надання персональних даних є необхідною умовою для отримання державних та інших послуг, вступу в договірні відносини, а також незліченної кількості інших випадків. У той же час, навіть в разі виникнення відносин приватного характеру, зберігається безумовна вимога, спрямована до розпорядника щодо дотримання конфіденційності даних, а також інші обов'язки перед суб'єктом персональних даних та уповноваженим органом, за винятком встановлених законом випадків.

Найбільш типовими способами правового регулювання режиму персональних даних прийнято вважати дозвіл, заборону та позитивне зобов'язання. Як правило, в рамках конкретного правового режиму використовується не один, а декілька способів в певному поєднанні або комплексі, при цьому частина з них може домінувати, що може свідчити про ступінь «жорсткості» правового режиму.

Цілком доречним можна вважати в цьому зв'язку класифікацію правових режимів, запропоновану Т. П. Мінкою, яка класифікує правові режими за такими основними критеріями: 1) за приналежністю норм права, які здійснюють державне регулювання суспільних відносин у відповідних сферах взаємодії публічної адміністрації з іншими суб'єктами права – на підгалузеві та інституціональні; 2) за сферами реалізації публічного інтересу весь масив адміністративно-правових режимів всередині галузі адміністративного права – на адміністративно-правові режими у сфері публічного управління (режими функціонування органів публічної адміністрації) та адміністративно-правові режими в адміністративно-політичній, економічній та соціально-культурній сферах; 3) за засобами правового регулювання – на прості, комплексні та міжгалузеві [108].

Очевидно, що з такої позиції слід характеризувати правовий режим того чи іншого виду інформації в цілому, враховуючи, що фактично в рамках правового режиму можуть бути використані всі способи правового регулювання різного ступеня. Найбільш істотне значення у визначенні способів і зрештою характеру правового режиму відіграє його кінцева мета, яка повинна бути досягнута шляхом встановлення такого режиму. Не є винятком в цьому випадку і правовий режим персональних даних, який спрямований на

забезпечення інформаційної безпеки особи через можливість обмеження свободи інформації в частині обігу відомостей персонального характеру. З огляду на загальний характер відносин з приводу персональних даних як інформації обмеженого доступу, можна говорити радше про регламентаційний характер режиму персональних даних в цілому, в тому числі конфіденційних. Такий висновок обумовлений в значній мірі характеристиками правового статусу суб'єкта персональних даних, який має право обирати у встановлених законом межах найбільш оптимальний, на власний розсуд, режим своїх персональних даних (конфіденційні і загальнодоступні персональні дані). З точки зору розпорядника персональних даних, вказаний правовий режим слід характеризувати як повідомлюючий, оскільки закон пов'язує діяльність по формуванню і обробці персональних даних із необхідністю повідомлення про такий уповноважений орган з захисту прав суб'єктів персональних даних, маючи на увазі (хоч це прямо і не зазначено в законі), що суб'єкт персональних даних особисто і добровільно передає йому дані, діючи у своєму власному інтересі, за умови збереження їх конфіденційності.

Слід відмітити, що за загальним правилом порядку обробки персональних даних, в тому числі й у Національній поліції, є наявність згоди суб'єкта персональних даних на їх обробку, яка може бути надана їм або його представником в будь-якій формі, яка дозволяє підтвердити факт її отримання, якщо інше не встановлено законом. Уявляється, що будь-яке виключення з цього правила повинно бути передбачено законами. У той же час, слід зазначити, що надана суб'єктом персональних даних згода на їх обробку не є незворотною, адже її може бути відкликано. При цьому не потрібно пояснювати причини такого рішення або виконувати будь-які умови, необхідно лише повідомити розпорядника персональних даних про прийняте рішення.

Однак, питання щодо відкликання згоди на обробку персональних даних лише частково врегульовано у профільному законі. Наприклад, стаття 8 Закону України «Про захист персональних даних» дійсно передбачає право суб'єкта персональних даних відкликати згоду на їх обробку. А із змісту статті 15 того ж законодавчого

акту стає зрозумілим, що однією з підстав знищення або видалення персональних даних може бути припинення правовідносин між суб'єктом персональних даних та володільцем чи розпорядником [72]. Разом з цим, механізм реалізації такої процесуальної дії в Законі не встановлений. Уявляється, що вказана правова процедура повинна передбачати зобов'язання розпорядника персональних даних припинити їх оброблення та знищити визначену інформацію у встановлений термін.

На підставі вищевикладеного пропонуємо доповнити Закон України «Про захист персональних даних» статтею 15-1 «Відкликання згоди на обробку персональних даних», наступного змісту: у разі відкликання суб'єктом персональних даних згоди на обробку його персональних даних розпорядник зобов'язаний припинити їх обробку або забезпечити припинення такої обробки (якщо обробка персональних даних здійснюється іншою особою, яка діє за дорученням розпорядника) і в разі, якщо збереження персональних даних більше не є необхідним для цілей обробки персональних даних, знищити персональні дані або забезпечити їх знищення (якщо обробка персональних даних здійснюється іншою особою, яка діє за дорученням розпорядника) в термін, що не перевищує тридцяти днів з дати надходження зазначеного відкликання, якщо інше не передбачено договором, стороною якого, вигодонабувачем або поручителем за яким є суб'єкт персональних даних, іншою угодою між розпорядником та суб'єктом персональних даних або якщо розпорядник не має права здійснювати обробку персональних даних без згоди суб'єкта персональних даних на підставах, передбачених цим законом або іншими законами».

У разі відсутності можливості знищення персональних даних протягом терміну, зазначеного в частині 1 цієї статті, розпорядник здійснює блокування таких персональних даних або забезпечує їх блокування (якщо обробка персональних даних здійснюється іншою особою, яка діє за дорученням розпорядника) і забезпечує знищення персональних даних у термін не більше ніж шість місяців, якщо інший термін не встановлено законами.

Крім того, вважаємо, що обробка персональних даних може бути продовжена після відкликання згоди суб'єкта персональних даних,

не зважаючи на положення статті 7 Закону України «Про захист персональних даних», яке фактично забороняє обробку персональних даних, якщо вони містять інформацію «про расове або етнічне походження, політичні, релігійні або світоглядні переконання, членство в політичних партіях та професійних спілках, засудження до кримінального покарання, а також дані, що стосуються здоров'я, статевого життя, біометричні або генетичні дані» [72].

Право відкликання згоди на обробку персональних даних не поширюється на випадки їх обробки, встановлені законами. Більш того, в ряді законів передбачаються випадки обов'язкового надання суб'єктом своїх персональних даних (наприклад, подача податкової декларації). Вимога про знищення персональних даних, у тому числі після досягнення заявлених цілей, як видається, потребує коригування і в зв'язку з дотриманням законодавства про архівну справу, яке встановлює вимоги та порядок поводження з документами, в тому числі що містять персональні дані. Уявляється, що в даний час законодавство про персональні дані та законодавство про архівну справу не узгоджені між собою.

Проблеми з отриманням персональних даних виникають досить часто, в тому числі і у державних органах виконавчої влади. Наприклад, відповідно до чинного законодавства, роботодавець зобов'язаний відмовити в наданні персональних даних, якщо особа, яка звернулася із запитом, не уповноважена законом на отримання такої інформації або ж відсутня письмова згода працівника на надання відомостей про нього особі, яка звернулася із запитом. Перелік осіб та органів, яким можуть передаватися персональні дані без згоди працівника, згадується у багатьох законодавчих актах, а відтак – не систематизований. Так, установи служби зайнятості населення не наділені правом отримання персональних даних працівника без його згоди. У ряді випадків виникають проблеми, пов'язані зі ступенем розкриття персональних даних. У даному випадку має значення для національної правозастосовної практики рішення ЄСПЛ від 6 жовтня 2009 року у справі «С. С. проти Іспанії» (скарга № 1425/06) [109].

Сутність вищевказаної справи полягала в тому, що позивач, який має ВІЛ-позитивний статус, був визнаний постійно і повністю

непрацездатним і вимагав відповідної компенсації, передбаченої договором страхування життя, укладеним в 2000 році. Коли страхова компанія відмовила у виплаті, заявник звернувся до суду із цивільним позовом. Повні медичні документи заявника були долучені до матеріалів справи. Вважаючи це порушенням свого права на повагу до приватного життя, заявник зажадав, щоб його персональні дані були видалені з документів справи, включаючи рішення разом з посиланнями на ВІЛ-захворювання, і щоб справа розглядалася в закритому засіданні. Суд відхилив вимоги заявника, наступні його скарги були залишені без задоволення. Європейський суд з прав людини зазначив, що оспорювана міра (долучення до матеріалів справи медичних документів) становила втручання державного органу у здійснення права заявника на повагу до його приватного життя. Разом з тим, це втручання було передбачено законом і його мета полягала в забезпеченні доступу іншої сторони до медичних документів, які були предметом розгляду. Суду також був необхідний доступ до інформації для розгляду справи та її вирішення по суті. Таким чином, мета оспорювання полягала в захисті прав і свобод інших осіб та забезпечення безперешкодного здійснення правосуддя. Своє завдання ЄСПЛ визначив як встановлення того, чи були достатні підстави, які виправдовують розкриття в рішенні національного суду повного імені заявника і факту його зараження ВІЛ-інфекцією. Суд обмежив розкриття особистості заявника відповідно до закону з підстав публічної політики та захисту прав і свобод. Була також правова можливість обмежити доступ до рішень і ухвал суду за наявності небезпеки втручання у реалізацію права на повагу до приватного життя або гарантії анонімності.

Відповідальна посадова особа могла в такому випадку прийняти рішення щодо обсягу обмеження доступу до справи, із врахуванням законного інтересу особи, яка запитувала інформацію.

Заявник просив видалити його ім'я з матеріалів справи в зв'язку із згадкою про стан його здоров'я. Достатньо було замінити його ім'я ініціалами в загальнодоступних документах і рішення, що дозволило б уникнути згодом проблеми доступу сторін, що мають інтерес до матеріалів справи і тексту рішення. З урахуванням конкретних

обставин цієї справи і необхідності особливого захисту конфіденційності інформації щодо зараження ВІЛ-інфекцією, розкриття якої здатне зробити негативний вплив на особисте і сімейне життя зацікавлених осіб і їх соціальну і професійну ситуацію, вказівка в рішенні повного імені заявника в зв'язку зі станом його здоров'я не було виправдано будь-якою нагальною необхідністю. Ще одна проблема, яка пов'язана із захистом персональних даних – можливість доступу самого суб'єкта персональних даних до інформації, що має для нього важливе значення. Судова практика в цьому відношенні суперечлива, в зв'язку з чим доцільно звернутися до практики ЄСПЛ на прикладі постанови від 15 жовтня 2009 року в справі «Цурлакіс проти Греції» (скарга № 50796/07) [110].

Заявник намагався отримати копію висновку товариства благополуччя дітей, наявного в матеріалах справи в Апеляційному суді, на підставі якого було винесено судове рішення, що зачіпає права заявника. Однак йому було відмовлено. ЄСПЛ зазначив, що неможливість ознайомлення заявника з висновком товариства благополуччя дітей після винесення рішення Апеляційним судом зачіпала реалізацію його права на доступ до інформації, що стосувалася права на повагу до особистого і сімейного життя. Інформація, яка містилася у висновку, мала відношення до заявника і його зв'язку з сином. Фактична відмова влади в дозволі на розкриття змісту висновку після закінчення розгляду в Апеляційному суді без вказівки причин була порушенням їх позитивного зобов'язання щодо забезпечення ефективного дотримання права заявника на повагу до його приватного і сімейного життя. ЄСПЛ визнав, що у справі було допущено порушення вимог ст. 8 Європейської конвенції про захист прав людини і основних свобод.

Таким чином, національна правова практика свідчить про те, що адміністративне законодавство про персональні дані по ряду питань не завжди має уніфіковане застосування, мають місце невизначеності, але головна необхідність в процесі функціонування режиму захисту персональних даних полягає у забезпеченні балансу інтересів суб'єкта персональних даних та інших зацікавлених осіб, суспільства в цілому з тим, щоб закон не став стримуючим фактором в реалізації прав інших осіб.

2. ОРГАНІЗАЦІЙНО-ПРАВОВИЙ МЕХАНІЗМ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ НАЦІОНАЛЬНОЮ ПОЛІЦІЄЮ

2.1. Національна поліція як суб'єкт адміністративно-правового захисту персональних даних

На теперішній час право фізичної особи на особисту таємницю закріплено конституціями всіх розвинених країн [58, с. 22–25]. Суть цього права полягає в тому, що тільки сама людина, що володіє будь-якою інформацією про себе, може вирішувати, підлягають вони розголошенню чи ні. У разі неправомірного розголошення таких відомостей їх власник має право на захист своїх порушених інтересів. У ряді країн, у тому числі в Україні, неправомірне розголошення персональних даних певного характеру є кримінальним злочином. Однак в судах все частіше розглядаються спори про розголошення персональних даних фізичних осіб. Вказана проблема, в тому числі, пов'язана з широким та, на жаль, неправомірним використанням інформаційних систем для обробки персональних даних. Відповідно до норм національного законодавства відомості про громадян після їх обробки в органах Національної поліції вносяться до баз (банків) даних.

Таким чином, Національна поліція є одним з найбільших, а можливо й найбільшим розпорядником інформації про стан соціального середовища, в тому числі інформації про приватне життя громадян. Таке соціальне завдання поліції обумовлене її функціональною спрямованістю на забезпечення особистої безпеки громадян та боротьбу

зі злочинністю. При цьому громадяни в одних випадках зобов'язані, в інших – вимушені, а іноді добровільно передають відомості про себе в розпорядження органів Національної поліції.

Прийняття Закону України «Про Національну поліцію» змусило багатьох науковців та практиків не тільки по-новому поглянути на змістовне наповнення поняття «персональні дані», але й в якійсь мірі переосмислити колишнє його сприйняття як чогось абстрактного, існуючого поза системою органів Національної поліції. Вперше у практиці національної правоохоронної системи згаданий законодавчий акт визначає повноваження поліції у сфері інформаційних відносин, надаючи їй право обробляти персональні дані про громадян і зобов'язуючи здійснювати цю обробку відповідно до вимог, встановлених законодавством у сфері захисту персональних даних.

Але повідомлення громадян в діяльності зі збору та обробки конфіденційної інформації хоча й найбільш значне за обсягом, але не єдине джерело, з якого Національна поліція отримує різну соціальну інформацію, яка є підставою для реалізації своїх державних функцій. До таких джерел можна також віднести і юридичних осіб, і органи публічної влади, які в ініціативному порядку або в силу нормативного зобов'язання передають до органів Національної поліції найрізноманітнішу інформацію, в тому числі таку, яка за своєю правовою природою має конфіденційний характер.

Описати всі джерела надходження відомостей до підрозділів поліції практично неможливо, тому слід зосередити увагу на основних, які окреслені законодавчими межами.

Одним із таких каналів є інформація, отримана із заяв та повідомлень громадян і організацій. Законодавчим фундаментом порядку прийняття звернень громадян органами державної влади, органами місцевого самоврядування та їх посадовими особами є Закон України «Про звернення громадян». Зробимо акцент на двох важливих для даного дослідження положеннях зазначеного правового акту. Зокрема, як випливає із змісту статті 5 коментованого законодавчого акту, звернення адресуються органам державної влади і органам місцевого самоврядування, підприємствам, установам,

організаціям незалежно від форми власності, об'єднанням громадян або посадовим особам, до повноважень яких належить вирішення порушених у зверненнях питань.

Також закон врегульовує процедуру повернення звернення, питання в якому не належать до компетенції відповідного органу. Так, стаття 7 Закону «Про звернення громадян» зобов'язує органи державної влади, органи місцевого самоврядування, їх посадових осіб, якщо порушені у зверненні питання не входять до їх повноважень, повернути звернення адресату у термін не більше 5 днів. У разі якщо звернення не містить даних, необхідних для прийняття обґрунтованого рішення органом чи посадовою особою, воно в той же термін повертається громадянину з відповідними роз'ясненнями [111].

Отже, будь-який орган Національної поліції, а також його посадові особи за будь-яких обставин зобов'язані прийняти та зареєструвати будь-яке звернення громадянина, спрямоване на їх адресу, незалежно від того, чи входить воно до компетенції цього органу. Вказане правове положення також підтримується й багатьма вітчизняними вченими [112-118].

Не менш важливе положення, яке стосується захисту персональних даних, зафіксовано у статті 10 коментованого законодавчого акту, відповідно до якого органам державної влади та органам місцевого самоврядування забороняється «розголошення одержаних із звернень відомостей про особисте життя громадян без їх згоди чи відомостей, що становлять державну або іншу таємницю, яка охороняється законом, та іншої інформації, якщо це ущемлює права і законні інтереси громадян» [111].

Із змісту вказаного положення стає зрозумілим, що зазначені органи та посадові особи Національної поліції зобов'язані забезпечити розгляд звернень таким чином, щоб виключити ознайомлення з їх змістом третіх осіб.

Деталізація положень Закону «Про звернення громадян», в частині захисту персональних даних в органах Національної поліції знайшла відображення у низці відомчих нормативно-правових актів, першорядне значення серед яких належить наказу МВС України від 15.11.2017 № 930, яким затверджено Порядок розгляду звернень

та організації проведення особистого прийому громадян в органах та підрозділах Національної поліції України (скорочено – Наказ № 930) [119] та наказу МВС України від 08.02.2019 № 100 «Про затвердження Порядку ведення єдиного обліку в органах (підрозділах) поліції заяв і повідомлень про кримінальні правопорушення та інші події» (скорочено – Наказ № 100) [120].

Під час характеристики вказаних нормативно-правових актів та проведення порівняльно-правового аналізу із Законом України «Про звернення громадян», звертають на себе увагу декілька аспектів. Наприклад, обидва коментовані накази МВС України доволі докладно врегульовують порядок реєстрації заяв та повідомлень громадян. Зазначені повноваження покладаються на підрозділи діловодства, працівники яких зобов'язані у визначені терміни прийняти, попередньо розглянути та централізовано зареєструвати звернення, із дотриманням Закону України «Про захист персональних даних» [119].

Крім цього, порядок реєстрації заяв та повідомлень громадян про кримінальні правопорушення та інші події визначений в розділі 3 Наказу №100, відповідно до якого вказані звернення реєструються уповноваженими службовими особами чергової служби центрального органу поліції, а також головних управлінь Національної поліції, в ІТС ІПНП (журналі ЄО) та невідкладно передають до органів (підрозділів) поліції нижчого рівня, на території обслуговування яких сталася подія, із зазначенням в ІТС ІПНП (журналі ЄО) номера реєстрації в ЄО відповідного органу (підрозділу) поліції [120].

Разом з цим, Закон України «Про звернення громадян» взагалі не містить вимог до реєстрації письмових звернень. Тільки усні звернення, відповідно до статті 5 коментованого законодавчого акту, що надійшли «на особистому прийомі або за допомогою засобів телефонного зв'язку через визначені контактні центри, телефонні «гарячі лінії», записується (реєструється) посадовою особою [111].

У той же час, ґрунтовний аналіз Наказу № 100 дозволив виокремити окремі проблемні питання, які виникають в процесі правозастосування, та сформулювати відповідні пропозиції

Наприклад, п. 4 розділу ІІ Наказу № 100 передбачає запровадження електронного талону-повідомлення про прийняття заяви про

кримінальне правопорушення чи іншу подію. На нашу думку, потребує уточнення питання про фізичне розміщення цього документу (у ІТС ІПНП або окремим документом у службовому комп'ютері службової особи). Також потребує роз'яснення те, у кого конкретно зберігаються корінці талонів повідомлень (у старшого кожної зміни, або у визначеної керівником підрозділу однієї особи).

У п. 6 розділу ІІ Наказу № 100, яким врегульована процедура негайного реагування поліцейського на виявлене правопорушення, потребує роз'яснення те, чи поширюються вимоги зазначеного пункту на працівників поліції, які перебувають поза службою (лікарняний, відпустка, відрядження тощо). У разі, якщо зазначені вимоги не поширюються на вказані категорії працівників поліції, пропонуємо сформулювати обов'язковість цього положення для поліцейських за будь-яких обставин.

Не в повному обсязі визначено й порядок реєстрації персоніфікованої інформації, яка стала відома працівнику поліції під час виявлення кримінального чи адміністративного правопорушення. Додаткова умова щодо наявності 24-годинного терміну для складання рапорту про виявлення правопорушення дає можливості для приховування, перекручення або неправомірного розповсюдження відповідної інформації. Тому пропонуємо викласти п. 7 розділу ІІ Наказу № 100 викласти у наступній редакції: «Поліцейський у разі самостійного виявлення з будь-якого джерела обставин, що можуть свідчити про кримінальні правопорушення, невідкладно доповідає рапортом, або іншим способом, керівникові органу (підрозділу) поліції або особі, яка виконує його обов'язки».

Разом з тим взагалі виникають сумніви щодо доцільності доведення до відома керівника інформації про кримінальне правопорушення або будь-яку іншу подію, оскільки відповідно до вимог п. 6 розділу ІІ Наказу №100 передбачено, що поліцейський у разі виявлення або отримання інформації про кримінальне правопорушення невідкладно повідомляє про це за скороченим номером екстреної допомоги поліції «102». Тобто, на момент доповіді керівникові про виявлення обставин, що можуть свідчити про кримінальні

правопорушення, відповідна персоніфікована інформація вже повинна бути зареєстрована до єдиного обліку.

Також потребує роз'яснення питання щодо заборони передачі з одного територіального (відокремленого) підрозділу поліції до іншого територіального (відокремленого) підрозділу матеріалів з відомостями, що вказують на кримінальні правопорушення без внесення цих відомостей до ЄРДР.

Так, п. 7 розділу ІІ Наказу № 100 передбачено, що за рішенням керівника органу (підрозділу) поліції, або особи, яка виконує його обов'язки, відомості про виявлене кримінальне правопорушення передаються до органів (підрозділів) поліції нижчого рівня та їх внесення до ЄРДР. Разом з тим, відповідно до вимог п. 9 розділу ІІ Наказу № 100 передавати з одного територіального (відокремленого) підрозділу (управління, відділу, відділення) поліції до іншого територіального (відокремленого) підрозділу (управління, відділу, відділення) поліції матеріали з відомостями, що вказують на кримінальне правопорушення, без їх реєстрації в ІТС ІПНП та внесення цих відомостей до ЄРДР заборонено.

Крім того, на нашу думку, потребує роз'яснення питання про те, чи реєструються в ІТС ІПНП матеріали ЄРДР, які надійшли до органу (підрозділу) поліції з іншого правоохоронного органу (прокуратура, СБУ та інші). Думається, що відповідні матеріали повинні реєструватись в обов'язковому порядку.

Невирішеним залишається й питання, викладене у п. 11 розділу ІІ Наказу №100 про те, чи буде виконання вимог зазначеного пункту рахуватись як порушення обліково-реєстраційної дисципліни, а саме: повторна реєстрація (перереєстрація) заяв та повідомлень з ознаками кримінальних правопорушень у термін понад 24 год. Нами пропонується зазначене як порушення не обліковувати.

Вимагає роз'яснення й положення, викладені у п. 5 розділу ІІІ Наказу №100 щодо строку інформування керівником органу досудового розслідування чергової служби про номер кримінального провадження, дату і час унесення відомостей до ЄРДР.

Так, згідно вимог зазначеного пункту керівник органу досудового розслідування невідкладно, але не пізніше 24 годин із часу

передання слідчому для внесення до ЄРДР відомостей про кримінальне правопорушення інформує чергову службу про номер кримінального провадження, дату і час унесення відомостей до ЄРДР [120].

Виникає питання, а якщо керівник органу досудового розслідування передасть слідчому для внесення до ЄРДР відомості про кримінальне правопорушення наприклад через 23 години, то у відповідного керівника органу досудового розслідування буде ще 24 години для інформування чергової служби про номер кримінального провадження, дату і час унесення відомостей до ЄРДР. Зазначене може призвести до порушень під час формування ІТС ІПНП, а саме: рішення за матеріалами з ознаками кримінальних правопорушень згідно ІТС ІПНП будуть залишатись не прийнятими понад 24 години.

На підставі викладеного пропонується керівнику органу досудового розслідування інформувати чергову службу про номер кримінального провадження, дату і час унесення відомостей до ЄРДР не пізніше 24 годин з моменту реєстрації повідомлення про кримінальне правопорушення до єдиного обліку.

Хоча це прямо не вказано в Наказі № 100, але при повідомленні про злочин, що надійшов від громадянина, в обов'язковому порядку зазначаються адреса його реєстрації, паспортні дані, що направлено на максимальну ідентифікацію особи заявника. З огляду на невизначеність кола осіб, які в реальній практиці мають доступ до змісту підсистеми «Єдиний облік», не можна однозначно стверджувати, що забезпечується конфіденційність відомостей про громадян, дані про яких внесені до вказаної підсистеми.

Слід також більш детально зупинитися на положеннях Наказу № 930, в частині правового регулювання захисту персональних даних. Зазначений докладний і ґрунтовний правовий акт детально розкриває окремі аспекти механізму прийняття та розгляду заяв та повідомлень громадян в органах Національної поліції. Слід зазначити, що Наказ № 930 доволі ретельно описує багато нюансів діяльності, пов'язаної з обігом документів, що містять звернення громадян, аж до того, в якому місці і в який спосіб нумеруються аркуші в матеріалах перевірки (справі).

Однак очікуваного від відомчого акту детального регулювання питань захисту відомостей, що містяться у зверненнях, якщо вони стосуються приватного життя громадян (а переважна більшість скарг саме цього і стосується), у вказаній інструкції не здійснено. У той же час, у вказаному нормативно-правовому акті визначено обов'язок працівника, уповноваженого на розгляд звернення (зауважимо, що не керівника органу або структурного підрозділу Національної поліції, а саме безпосереднього виконавця):

- внести до журналуреєстрації звернень громадян, які надійшли з використанням засобів поштового зв'язку, мережі Інтернет, електронного зв'язку (електронні звернення), через контактні центри державної установи «Урядовий контактний центр» та телефонну «гарячу лінію» Національної поліції України, до РКК резолюцію керівництва та встановлені терміни виконання доручень за зверненнями громадян;
- здійснити відправлення звернення за належністю відповідному державному органу чи посадовій особі з питань, що не належать до повноважень поліції, про що проінформувати їх авторів;
- забезпечити доведення звернень громадян до зазначених у резолюції виконавців;
- взяти на контроль звернення громадян у разі визначення такого контролю керівництвом органу (підрозділу) поліції [119].

Яким чином вказаний працівник підрозділу документального забезпечення здійснюватиме реалізацію цих обов'язків, наказом не визначено, а так само не встановлюється режим зберігання та пересилки такої документованої інформації в інші підрозділи або органи й інші аспекти адміністративного механізму захисту персональних даних, який має бути детально врегульований саме на цьому рівні правового регулювання.

З'ясування адміністративно-правового механізму захисту персональних даних Національною поліцією України в процесі їх накопичення та зберігання потребує розкриття не менш важливого питання, пов'язаного із дослідженням основних категорій відомостей

конфіденційного характеру, які накопичуються та використовуються органами Національної поліції в процесі службової діяльності. У цьому контексті звертають на себе увагу положення наказу МВС України від 27.05.2016 № 432 «Про затвердження Переліку відомостей, що становлять службову інформацію в системі Міністерства внутрішніх справ України» (скорочено – Перелік) [121].

Коментований нормативно-правовий акт складається з 13 розділів, найбільший інтерес з яких викликають положення, пов'язані з обігом службової інформації в процесі реалізації органами Національної поліції оперативно-службової діяльності.

Аналіз положень Переліку дозволяє зробити висновок про те, що в багатьох випадках нормотворець використовує персональні дані, які по суті є конфіденційною інформацією, у якості інформації службової. Викладення зазначеної інформації наводиться в залежності від сфери оперативно-службової діяльності органів Національної поліції. Наприклад, у сфері роботи з персоналом органів Національної поліції, до персональних даних, на які розповсюджується режим службової інформації, відносяться: «Персональні дані колишніх працівників органів внутрішніх справ та членів їх сімей, працівників навчальних закладів зі специфічними умовами навчання, а також закладів, установ і підприємств, що належать до сфери управління МВС, військовослужбовців, працівників і членів їх сімей Національної гвардії України (колишніх внутрішніх військ МВС України)» [121]; у сфері мобілізаційної роботи та мобілізації – це відомості про військовозобов'язаних; у сфері охорони інформації з обмеженим доступом – це відомості про особу, якій надано допуск до державної таємниці (прізвище, ім'я, по батькові, дата та місце народження, місце проживання, посада, найменування органу, підрозділу, номер і дата наказу про надання доступу; у сфері діяльності учасників антитерористичної операції МВС – це документи, що стали підставою для надання статусу учасника бойових дій; у сфері діяльності запобігання корупції та проведення люстрації МВС службова інформація включаєматеріали проведення перевірок осіб, відповідно до Закону Україн «Про запобігання корупції» [122] та щодо застосування заборон, передбачених Законом України «Про очищення влади» [123].

Дійсно, Закон України «Про захист персональних даних» дозволяє володільцю персональних даних здійснювати їх обіг, але покладає на останнього низку вимог щодо їх правомірного використання та збереження. Так, відповідно до частини 3 статті 10 коментованого Закону «використання персональних даних працівниками суб'єктів відносин, пов'язаних з персональними даними, повинно здійснюватися лише відповідно до їхніх професійних чи службових або трудових обов'язків» [72].

Але в той же час, до змісту Переліку з нашого боку є декілька зауважень. Це передовсім стосується механізму побудови вказаного документу, відомості в якому викладені за видами службової інформації, а не за її критеріями. Тому, оскільки критерії службової інформації в коментованому Переліку не визначені, спробуємо звернутися до інших юридичних та наукових джерел.

Наприклад, І. М. Мейдич наголошує на наявності суттєвих прогалин у законодавстві, в частині правового визначення службової інформації, критерії якої у нормативно-правових актах наразі відсутні [124, с. 164].

Слушні пропозиції з приводу об'єднання правових категорій «державна таємниця» та «службова інформація» в єдину категорію, доступ до якої обмежується виключно в інтересах, передбачених статтею 6 Закону України «Про доступ до публічної інформації», висловлює С. В. Болдир [125, с. 80].

Дійсно, Закон України «Про інформацію» згадує службову інформацію, поряд із конфіденційною та таємною, в контексті їх віднесення до інформації з обмеженим доступом.

Разом з цим, Закон України «Про доступ до публічної інформації» визначає тільки її окремі види, що надто звужує правове розуміння відомостей службового характеру. Зокрема, стаття 9 коментованого законодавчого акту відносить до службової інформації: а) документи суб'єктів владних повноважень, які становлять внутрівідомчу службову кореспонденцію; б) доповідні записки; в) рекомендації, якщо вони пов'язані з розробкою напряму діяльності установи або здійсненням контрольних, наглядових функцій органами державної влади, процесом прийняття рішень і передують публічному

обговоренню та/або прийняттю рішень; г) зібрана в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, яку не віднесено до державної таємниці [82].

Не вносить ясності в розуміння службової інформації і постанова Верховного Суду України від 07 лютого 2019 року № 9901/478/18 у справі за апеляційною скаргою Вищої ради правосуддя на рішення Верховного Суду, відповідно до якої позивач вимагає визнати протиправними дії відповідача щодо неповідомлення їй інформації про прізвища та ініціали членів Вищої ради правосуддя, які проводять перевірку її двох дисциплінарних скарг стосовно суддів [126].

У вказаному рішенні Верховний Суд України, не висловлюючи позиції щодо сутності службової інформації та її критеріїв, оцінює лише правомірність обмеження доступу до неї, посилаючись на положення пункту 1 частини першої статті 9 Закону України «Про доступ до публічної інформації».

Дискусійною також вважаємо позицію О. О. Караваєва щодо віднесення до критерію, покладеного в основу ідентифікації службової інформації, службової необхідності [127, с. 84]. У даному випадку критерієм віднесення інформації до категорії службової виступають не конкретні об'єктивні фактори, а суб'єктивна категорія – «службова необхідність», а тому виникає привід до можливості прийняття свавільних правозастосовних рішень.

Думається, що визначення службової необхідності в якості критерію віднесення інформації до числа службової має дуже широке тлумачення та може включати відомості, вказані у безлічі службових документів, як-от: доповідні записки, довідки, акти і т.д., що містять узагальнені відомості про фактичний стан справ з різних напрямків оперативно-службової діяльності. Визначення службової інформації з підстав наявності службової необхідності фактично дозволяє ввести обмеження на будь-який службовий документ, підготовлений в органі Національної поліції на будь-якому рівні, оскільки більше 90% службових документів так чи інакше містять інформацію про фактичний стан справ і мають певний рівень узагальненості відомостей. Використання аналогічної норми у правозастосуванні істотно перевантажить систему захисту інформації органів Національної

поліції, а її ігнорування створить підґрунтя для правового нігілізму при виконанні вимог відомчих нормативних правових актів.

Таким чином, інститут захисту службової інформації в Національній поліції практично не врегульовано законодавчо, крім того є великі проблеми у врегулюванні службової інформації в різних державних органах. Численні нормативні акти протирічать один одному. Питання здійснення управління в органах Національної поліції та врегулювання відносин з приводу використання службової інформації можна розглядати як з точки зору обмеження безконтрольного «засекречування» інформації, так і з точки зору уникнення ситуації маніпулювання інформацією або її «витоку». Крім того, безконтрольне обмеження доступу до службової інформації, що містить персональні дані, є вельми серйозним корупціогенним фактором. У зв'язку з цим вважаємо, що регулювання захисту службової інформації повинно підвищити прозорість діяльності органів Національної поліції та їх посадових осіб.

Таким чином, можна зробити наступні проміжні висновки.

1. Поняття «службова таємниця» є ключовим під час регулювання порядку поводження зі службовою інформацією обмеженого доступу. Необхідна уніфікація понятійно-категоріального апарату, що дозволить уникнути різночитань як в теорії, так і в практиці, крім того, дозволить уніфікувати механізм захисту та обігу такої інформації.

2. Суб'єктами відносин у сфері обігу персональних даних є органи Національної поліції та їх посадові особи, на які, в свою чергу, покладено обов'язок з охорони службової таємниці, також надані повноваження щодо віднесення тих чи інших відомостей до службової таємниці. Однак варто зауважити, що регламентацію відносин щодо порядку обігу та охорони службової таємниці необхідно закріпити на законодавчому рівні.

3. Об'єктами службової таємниці є відомості, які становлять так звану «чужу» таємницю - відомості конфіденційного характеру, які стали відомі органам Національної поліції та їх посадовим особам у зв'язку з виконанням ними покладених державних повноважень, а також відомості, що є внутрішньою інформацією державних

органів і органів місцевого самоврядування, до яких відносяться насамперед внутрішні інформаційно-аналітичні системи і службова кореспонденція, а також відомості про деякі стратегічно важливі підприємства.

4. У законодавстві вкрай не врегульовані основні питання, що стосуються відносин у сфері службової таємниці, а саме: немає конкретних критеріїв, на основі яких інформація може бути віднесена до категорії «службової таємниці». Також не врегульовано порядок обігу такої інформації та її зберігання. У той же час в законодавстві не визначені вимоги до терміну нерозголошення службової таємниці після припинення трудових відносин.

5. Також має місце малоефективна адміністративна відповідальність за розголошення службової таємниці. Дисциплінарна відповідальність, в свою чергу, також не в силах забезпечити безпеку відомостей, що становлять службову таємницю. На наш погляд, необхідно посилення адміністративної відповідальності в частині введення такої міри відповідальності за розголошення інформації, як дискваліфікація посадової особи. На наш погляд, назріла гостра необхідність в регулюванні службової таємниці на законодавчому рівні, що дозволило б вирішити численні протиріччя, що зустрічаються на практиці, а також упорядкувати діяльність органів Національної поліції щодо зловживання правом засекречування службової інформації. Крім того, це підвищить ефективність державного управління, підвищить інформаційну відкритість влади і, як наслідок, довіру населення до поліції.

У той же час, в системі правоохоронних органів, визначених частиною 1 статті 1 Закону України «Про державний захист працівників суду та правоохоронних органів», діяльність щодо збору, накопичення, обробки та використання персональних даних, окрім Національної поліції, здійснюють й інші державні правоохоронні інституції, такі як органи прокуратури, Служби безпеки України, Військової служби правопорядку у Збройних Силах України, Національне антикорупційне бюро України, органи охорони державного кордону, органи доходів і зборів, органи й установи виконання покарань, слідчі ізолятори, органи державного фінансового

контролю, рибоохорони, державної лісової охорони, інші органи, які здійснюють правозастосовні або правоохоронні функції [128].

Наприклад, відповідно до статті 25 Закону України «Про Службу безпеки України» [129] зазначено, що Службі безпеки України, її органам і співробітникам для виконання покладених на них обов'язків надається право:

- одержувати на письмовий запит керівника відповідного органу Служби безпеки України від міністерств, державних комітетів, інших відомств, підприємств, установ, організацій, військових частин, громадян і їхніх об'єднань дані й відомості, необхідні для забезпечення державної безпеки України, а також користуватись із цією метою службовою документацією і звітністю. Отримання від банків інформації, яка містить банківську таємницю, здійснюється в порядку та обсязі, встановлених Законом України «Про банки і банківську діяльність», тощо;
- входити в порядку, погодженому з адміністрацією підприємств, установ та організацій і командуванням військових частин, на їхню територію й у службові приміщення.

Відповідно до статей 23, 26 Закону України «Про прокуратуру» [130], під час здійснення повноважень прокурор має право:

- витребувати за письмовим запитом, ознайомлюватися та безоплатно отримувати копії документів і матеріалів органів державної влади, органів місцевого самоврядування, військових частин, державних і комунальних підприємств, установ і організацій, органів Пенсійного фонду України та фондів загальнообов'язкового державного соціального страхування, що знаходяться в цих суб'єктів, у порядку, визначеному законом;
- отримувати від посадових і службових осіб органів державної влади, органів місцевого самоврядування, військових частин, державних і комунальних підприємств, установ та організацій, органів Пенсійного фонду України та фондів загальнообов'язкового державного соціального страхування усні або письмові пояснення;

- знайомитися з матеріалами, отримувати їх копії, перевіряти законність наказів, розпоряджень, інших актів відповідних органів та установ і в разі невідповідності законодавству вимагати від посадових чи службових осіб їх скасування й усунення порушень закону, до яких вони призвели, а також скасовувати незаконні акти індивідуальної дії;
- вимагати від посадових чи службових осіб надання пояснень щодо допущених порушень, а також вимагати усунення порушень і причин та умов, що їм сприяли, притягнення винних до передбаченої законом відповідальності;
- знайомитися з матеріалами виконавчого провадження щодо виконання судових рішень у кримінальних справах, робити з них виписки, знімати копії й у встановленому законом порядку оскаржувати рішення, дії чи бездіяльність державного виконавця.

Стаття 12 Закону України «Про організаційно-правові основи боротьби з організованою злочинністю» [131] регламентує, що під час здійснення заходів боротьби з організованою злочинністю спеціальним підрозділам по боротьбі з організованою злочинністю Служби безпеки України надаються повноваження:

- заводити оперативно-розшукові справи. Постанова про заведення справи затверджується начальником спеціального підрозділу;
- на письмову вимогу керівників відповідних спеціальних підрозділів по боротьбі з організованою злочинністю одержувати від банків, а також кредитних, митних, фінансових та інших установ, підприємств, організацій (незалежно від форм власності) інформацію й документи про операції, рахунки, вклади, внутрішні та зовнішні економічні угоди фізичних і юридичних осіб. Отримання від банків інформації, яка містить банківську таємницю, здійснюється в порядку й обсязі, встановлених Законом України «Про банки і банківську діяльність» [132]. Документи та інформація повинні бути подані негайно, а якщо це неможливо – не пізніше як протягом 10 діб;

- одержувати інформацію з автоматизованих інформаційних і довідкових систем і банків даних, створюваних Верховним Судом України, Генеральною прокуратурою України, Антимонопольним комітетом України, Фондом державного майна України, міністерствами, відомствами, іншими державними органами України;
- в разі одержання фактичних даних про організовану злочинну діяльність для їх перевірки витребувати й одержувати від державних органів, об'єднань громадян, підприємств, установ, організацій (незалежно від форм власності) інформацію та документи. Витребувані документи та інформація повинні бути подані негайно або не пізніше як протягом 10 діб.

У статті 8 Закону України «Про оперативно-розшукову діяльність» [44] зазначено, що оперативним підрозділам для виконання завдань оперативно-розшукової діяльності за наявності передбачених статтею 6 цього Закону підстав надається право ознайомлюватися з документами й даними, що характеризують діяльність підприємств, установ та організацій, вивчати їх за рахунок коштів, що виділяються на утримання підрозділів, які здійснюють оперативно-розшукову діяльність, виготовляти копії з таких документів, на вимогу керівників підприємств, установ та організацій – виключно на території таких підприємств, установ та організацій, а з дозволу слідчого судді в порядку, передбаченому Кримінальним процесуальним кодексом України, а саме: витребувати документи й дані, що характеризують діяльність підприємств, установ, організацій, а також спосіб життя окремих осіб, підозрюваних у підготовці або вчиненні злочину, джерело та розміри їхніх доходів із залишенням копій таких документів та опису вилучених документів особам, у яких вони витребувані, і забезпеченням їх збереження й повернення в установленому порядку. Вилучення оригіналів первинних фінансово-господарських документів забороняється, крім випадків, передбачених Кримінальним процесуальним кодексом України.

Припущення щодо провідної ролі Національної поліції України в системі правоохоронних органів, які здійснюють захист персональних даних, обумовлено декількома факторами.

Так, відповідно до статті 25 Закону України «Про Національну поліцію», поліція здійснює інформаційно-аналітичну діяльність виключно для реалізації своїх повноважень, визначених цим Законом. Поліція в рамках інформаційно-аналітичної діяльності: 1) формує бази (банки) даних, що входять до єдиної інформаційної системи Міністерства внутрішніх справ України; 2) користується базами (банками) даних Міністерства внутрішніх справ України та інших органів державної влади; 3) здійснює інформаційно-пошукову й інформаційно-аналітичну роботу; 4) здійснює інформаційну взаємодію з іншими органами державної влади України, органами правопорядку іноземних держав і міжнародними організаціями. Поліція може створювати власні бази даних, необхідні для забезпечення щоденної діяльності органів (закладів, установ) поліції у сфері трудових, фінансових, управлінських відносин, відносин документообігу, а також міжвідомчі інформаційно-аналітичні системи, необхідні для виконання покладених на неї повноважень. Діяльність поліції, пов'язана із захистом та обробкою персональних даних, здійснюється на підставах, визначених Конституцією України, Законом України «Про захист персональних даних», іншими законами України [40].

Дослідницький інтерес в контексті організації захисту персональних даних в органах Національної поліції викликає затверджений на основі Закону України «Про захист персональних даних» наказ МВС України від 21.08.2013 № 805 «Про затвердження Порядку обробки персональних даних у базі персональних даних «Електронний журнал обліку запитів на публічну інформацію» (скорочено – Наказ № 805) [133], яким визначено комплекс організаційних та технічних заходів для забезпечення захисту персональних даних запитувачів від несанкціонованого доступу, витоку інформації, неправомірного використання або втрати під час обробки.

Зупинимося більш докладно на заходах, спрямованих на забезпечення безпеки персональних даних, накопичення та оброблення яких здійснюється в органах Національної поліції України. Аналіз вищевказаного нормативно-правового акту дає підстави для висновку, що заходи, здійснювані в органах Національної поліції України щодо створення системи технічного захисту персональних

даних можна розділити на дві групи: а) організаційно-управлінські та б) організаційно-технічні.

Перша група заходів спрямована на створення організаційно-правових передумов захисту персональних даних та безпосереднє управління цим процесом. Відповідно до Наказу № 805, безпосереднім володільцем бази персональних даних визначено Міністерство внутрішніх справ. Зазначеним документом також визначено обов'язок МВС України інформувати Державну службу України з питань захисту персональних даних про кожну зміну відомостей, необхідних для реєстрації бази персональних даних «Електронний журнал обліку запитів на публічну інформацію», не пізніше ніж протягом десяти робочих днів з дня настання такої зміни.

Друга група заходів безпосередньо спрямована на забезпечення безпеки персональних даних та атестацію інформаційних систем персональних даних на підставі вимог щодо захисту інформації.

Слід зауважити, що обидві групи заходів безпосередньо пов'язані між собою, адже обробка персональних даних в інформаційних системах Національної поліції повинна здійснюватися виключно після завершення робіт щодо створення системи технічного захисту персональних даних та вводу до експлуатації інформаційних систем, які містять персональні дані.

Службова діяльність Національної поліції щодо створення системи технічного захисту персональних даних врегульована нормативно [134] та передбачає виконання конкретних організаційно-практичних заходів, які включають в себе: а) отримання територіальним органом Національної поліції на регіональному рівні ліцензії на діяльність з технічного захисту конфіденційної інформації, наявність якої обумовлено необхідністю проведення атестації інформаційних систем, що обробляють персональні дані, за вимогами захисту інформації; б) створення комісії для визначення рівня захищеності інформаційної системи персональних даних. Комісія створюється наказом керівника (начальника) територіального органу Національної поліції, а до її складу входять представники структурних підрозділів, які експлуатують інформаційні системи персональних даних, а також представники підрозділів інформаційно-аналітичного

забезпечення і зв'язку та телекомунікацій; в) планування заходів, спрямованих на захист персональних даних, оброблюваних в інформаційних системах територіальних органів Національної поліції. Роботи щодо забезпечення безпеки персональних даних включаються до Плану основних організаційних заходів територіального органу Національної поліції окремим розділом; г) організація взаємодії підрозділів, що забезпечують створення і експлуатацію інформаційних систем персональних даних, з підрозділом по захисту персональних даних. Тобто взаємодія структурних підрозділів територіального органу Національної поліції, які експлуатують інформаційні системи персональних даних, з підрозділом режиму та технічного захисту інформації територіального органу Національної поліції на регіональному рівні. На теперішній час зазначений аспект є одним з найпроблемніших та найскладніших під час проведення заходів щодо забезпечення безпеки персональних даних в органах Національної поліції. Справа в тому, що в органах Національної поліції спостерігається серйозна нестача спеціально підготовлених співробітників для проведення робіт із захисту інформації, які можуть кваліфіковано організувати і провести необхідні підготовчі заходи. Крім того, з цієї ж причини після проведення атестаційних заходів в структурних підрозділах в ряді випадків не дотримуються організаційні та технічні заходи щодо захисту персональних даних; д) планування та організація проведення занять по вивченню вимог нормативних правових актів і методичних документів з питань забезпечення безпеки персональних даних, а також щорічної перевірки їх знань.

З метою підвищення рівня професійної підготовки працівників Національної поліції, уповноважених на обробку персональних даних, необхідно організовувати вивчення ними вимог законодавства з питань забезпечення безпеки персональних даних, а також щорічну перевірку їх знань; є) організація і здійснення контролю за виконанням встановлених вимог щодо забезпечення безпеки персональних даних. Метою такого контролю є дотримання структурними підрозділами територіального органу Національної поліції вимог щодо забезпечення безпеки персональних даних при їх обробці в інформаційних системах. Завданнями контролю є: встановлення

фактичного стану справ у структурному підрозділі по забезпеченню безпеки персональних даних при їх обробці в інформаційних системах; виявлення проблемних питань в організації забезпечення безпеки персональних даних; забезпечення дотримання законодавства в сфері захисту персональних даних; вироблення заходів з надання методичної та практичної допомоги структурним підрозділам територіального органу Національної поліції; підвищення відповідальності керівників за забезпечення безпеки персональних даних.

У якості висновків до вказаного параграфу ми хотіли би зазначити наступне:

1. Національна поліція є одним з найбільших розпорядників відомостей конфіденційного характеру в системі правоохоронних органів України, що має визначати детальне опрацювання питань правового врегулювання обігу й захисту даної інформації на всіх рівнях управління, а особливо під час створення та використання автоматизованих банків даних. Аналіз специфіки діяльності органів Національної поліції також показує, що в їх підрозділах утворюється значна кількість службових відомостей, які містять персональні дані та використовуються значним колом співробітників, але в той же час ці відомості повинні бути захищені від свавільного поширення.

2. Одним із основних джерел надходження інформації про стан соціального середовища до органів Національної поліції, що містить персональні дані фізичних осіб, є повідомлення про кримінальні правопорушення та інші події, для яких визначено окремий порядок реєстрації та розгляду. В інструкції, затвердженої наказом №100 МВС України, міститься цілий ряд норм, спрямованих на виключення зайвої фіксації відомостей про приватне життя громадян, проте вони носять декларативний характер, у зв'язку з чим вони складно піддаються практичній реалізації. Приблизно на такому ж декларативному рівні правового регулювання знаходиться забезпечення захисту відомостей про приватне життя громадян при реєстрації та розгляді їх звернень до органів Національної поліції.

3. Слід констатувати, що спеціалізоване відомче правове регулювання в сфері захисту персональних даних недостатньо врегульовано в правовому відношенні, відрізняється декларативністю,

внаслідок чого воно є малопридатним для практичного застосування при організації захисту інформації.

В силу того що вказаний посібник носить відкритий характер, автори не мають можливості ретельного аналізу положень всіх відомчих нормативних правових актів, де описується механізм захисту відомостей, що накопичуються в банках даних поліції. З огляду на зазначене,ми змушені акцентувати увагу на актах, що знаходяться у відкритому доступі. Одним із них є наказ МВС України від 21.08.2013 № 805 «Про затвердження Порядку обробки персональних даних у базі персональних даних «Електронний журнал обліку запитів на публічну інформацію».

Аналіз вищевказаного нормативно-правового акту дає підстави для висновку, що заходи, здійснювані в органах Національної поліції України щодо створення системи технічного захисту персональних даних можна розділити на дві групи: а) організаційно-управлінські та б) організаційно-технічні. Перша група заходів спрямована на створення організаційно-правових передумов захисту персональних даних та безпосереднє управління цим процесом. Друга група заходів безпосередньо спрямована на забезпечення безпеки персональних даних та атестацію інформаційних систем персональних даних на підставі вимог щодо захисту інформації. Слід зауважити, що обидві групи заходів безпосередньо пов'язані між собою, адже обробка персональних даних в інформаційних системах Національної поліції повинна здійснюватися виключно після завершення робіт щодо створення системи технічного захисту персональних даних та вводу до експлуатації інформаційних систем, які містять персональні дані.

2.2. Форми та методи захисту персональних даних в адміністративній діяльності Національної поліції

Форми та методи захисту персональних даних в діяльності Національної поліції набувають особливої актуальності у контексті дослідження ключових напрямків організаційно-правового

механізму їх захисту. Характерна особливість форм та методів захисту персональних даних в діяльності Національної поліції полягає в тому, що вони передовсім відображають динамічну складову механізму їх захисту, на відміну від організаційних та правових елементів цього механізму, які репрезентують його статичний фундамент.

Тому побудова цілісного реально існуючого механізму захисту персональних даних неможлива без розкриття форм та методів, які чинять безпосередній вплив на його формування в діяльності Національної поліції України. За справедливим висловленням С. С. Алексєєва «якісне вивчення форм і методів практичної реалізації будь-яких організаційно-правових систем, незалежно від глибини аналітичної проробки, буде неповним без ретельного дослідження їх 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...» [135, с. 79]. Однак, по-перше спробуємо з'ясувати сутність досліджуваних категорій, адже на цьому етапі формується загальне уявлення про предмет дослідження. Попри доволі повсюдне використання правових категорій «форма» та «метод» в науці адміністративного права, їх змістовне наповнення й дотепер викликає певні суперечки.

У класичному філософському розумінні «форма» визначається в якості зовнішнього вираження внутрішнього змісту будь-якого процесу та має декілька тлумачень, а саме: «зовнішній вид, зовнішній обрис; устрій, структура будь-чого, система організації» [136, с. 536], «зовнішнє вираження якого-небудь змісту» [137, с. 489] або «спосіб існування змісту: невіддільний від нього і є його вираженням» [138, с. 653].

Ю. М. Козлов трактує правову категорію «форма» у якості практичного вираження конкретних дій органів та інших суб'єктів управління [139, с. 26]. «Вони (форми управління) відзначаються помітною самостійністю й універсальністю щодо конкретних галузей і сфер владного впливу. Саме тому одні й ті самі форми успішно застосовуються в різних сферах суспільного життя» [140, с. 180]. У даному випадку автор дуже вдало, на нашу думку, підкреслює динамічний

характер форм державного управління, акцентуючи увагу на їх практичному вираженні, що виявляється у конкретних діях органів державної влади.

В процесі дослідження форм адміністративної діяльності ОВС В. Ю. Пантелеєв, І. П. Голосніченко доходять висновку про їх похідний характер від загального визначення форм адміністративної діяльності в адміністративно-правовій науці, та розуміють досліджувану категорію як сукупність однорідних за своїм характером та правовою природою груп адміністративних дій, що мають зовнішнє вираження, за допомогою яких забезпечуються охорона прав громадян, громадський порядок, безпека та здійснюється боротьба з правопорушеннями [141, с. 61–92; 142, с. 104]. Тут слід особливо підкреслити вдалі спроби авторів, поряд із загальними властивостями форм публічного управління, виокремити їх спеціальні елементи, розкриті завдяки визначенню мети їх використання, а саме: забезпечення охорони прав громадян, громадського порядку, безпеки та здійснення боротьби з правопорушеннями.

І. Д. Пастух також підкреслює важливість посилання на досягнення кінцевого результату в діяльності органів державної влади, під час використання форм публічного управління. Автор, зокрема, визначає останні у якості «зовнішньо виражених дій суб'єктів публічного управління, що здійснюються в рамках їх компетенції для виконання поставлених перед ними завдань та тягне за собою певні наслідки» [140, с. 181]. Класифікація форм публічного управління за ступенем правової регламентації дозволила вищевказаному автору виділити такі їх види, як: «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» [140, с. 181].

На думку В. Б. Дзюндзюка, Н. М. Мельтюхової та Н. В. 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 [143, с. 98]. Підсумовуючи

наведену дефініцію, автори виокремлюють в якості основних форм публічного управління наступні елементи: нормативно-правові (становлення норм права); застосування норм права; організаційне регламентування внутрішньої роботи апарату органів влади; позаапаратну організаційну діяльність; матеріально-технічне забезпечення.

Водночас, Т. О. Гуржій, навпаки, під час визначення форм публічного адміністрування, не намагається робити акцент на кінцевому результаті в діяльності органів публічної адміністрації, а підкреслює передовсім такі їх ознаки як регламентація форм публічного адміністрування адміністративно-правовими нормами; спрямованість форм публічного адміністрування на реалізацію повноважень відповідних суб'єктів адміністративно-правових відносин; змістовне наповнення форм публічного адміністрування, які включають види і способи реалізації таких повноважень. На підставі сформульованих ознак, вчений виокремлює наступні форми публічного адміністрування: 1) видання адміністративно-правових актів; 2) укладання адміністративних договорів; 3) надання адміністративних послуг та здійснення інших юридично значущих дій [144, с. 115, 116].

Таким чином, аналіз висловлених позицій з приводу розуміння форм державного управління дає підстави для висновку про наявність певних розбіжностей у поглядах науковців з приводу окресленої проблематики. Слід зазначити, що в численних дефініціях «каменем спотикання» виступає доцільність віднесення мети (а точніше – її кінцевої реалізації) діяльності органів державного управління до ключових ознак форм їх діяльності. Власну позицію з цього приводу висловимо трохи згодом.

А зараз зауважимо, що розбіжності щодо розуміння форм державно-управлінської діяльності спостерігаються й у процесі визначення методів державного управління. Узагальнюючи різноманітні наукові позиції щодо окресленої проблематики, спробуємо виокремити чотири ключові позиції щодо розуміння досліджуваного правового явища.

Перша група вчених трактує методи державного управління у якості «сукупності універсальних та спеціальних способів і прийомів,

які застосовуються органами влади при здійсненні тих чи інших функцій державного управління або в процесі розробки, прийняття та реалізації рішень щодо впливу на керовані об'єкти» [143, с. 102].

Друга група вчених визначає правову категорію «методи державного управління» у вигляді «засобів та способів здійснення функцій суб'єкта публічної адміністрації, впливу суб'єктів публічної адміністрації на об'єкти публічної діяльності» [145, с. 178].

На думку третьої групи дослідників це: «певні способи практичного виконання суб'єктами публічної адміністрації своїх адміністративних зобов'язань, що відповідають характеру й обсягу наданої їм компетенції» [140, с. 227].

Четверта група вчених переконана, що це: «... 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» [146, с. 155].

Навіть за результатами побіжного аналізу, не вдаючись до тонкощів досліджуваної проблематики, слід наголосити на небездоганності висловлених суджень, адже у поглядах науковців щодо сутності правових категорій «форм та методів державного управління» існують численні протиріччя, як з точки зору логіки побудови, так і з точки зору відповідності реаліям сучасного розуміння державного управління. З огляду на вищенаведене можемо сформулювати власну позицію щодо сутності досліджуваних явищ, ґрунтуючись на таких концептуальних позиціях:

1. Цілком погоджуємося з позицією деяких авторів, зокрема Т. О. Гуржія, який, ґрунтуючись на положеннях європейської доктрини права, використовує у своїх наукових працях правову категорію публічне адміністрування. Її більш широке тлумачення, на відміну від розуміння державного управління, дозволяє розглядати в контексті форм та методів управлінської діяльності увесь арсенал суб'єктів публічного адміністрування, не залежно від статусу та форм підпорядкування, та не обмежуватися виключно такими правовими категоріями, як «державні органи», «органи управління», «виконавчі органи влади».

2. Дещо сумнівною, на нашу думку, виглядає позиція численних авторів з приводу розуміння форм та методів державного управління як вплив органів публічної адміністрації на «керовані суб'єкти», «підпорядковані органи», «громадян». З часів проголошення незалежності України кардинально змінились адміністративно-правові відносини, а відтак – змінилась філософія публічного управління. Відбулась його трансформація, в контексті реалізації форм та методів державного управління, коли відносини, за схемою влади-підпорядкування поступово трансформувались та набули ознаки рівноправності, коли суб'єкти адміністративно-правових відносин «добровільно беруть на себе роль розпорядника і виконавця» [144, с. 10]. Зазначений висновок підтверджує й А. Л. Петрицький, який справедливо наголошує на рівноправності та відсутності відносин субординації між багатьма суб'єктами адміністративно-правових відносин в галузі публічного управління, як-от: публічна адміністрація, суспільні та громадські інститути, юридичні особи приватного права, фізичні особи тощо [147, с. 130].

Спираючись на розуміння форми будь-якого процесу, у її загально-філософському розумінні, як явища, «що виражає внутрішню побудову та зовнішній вираз чогось» [148, с. 161], можемо припустити, що форма публічного управління перш за все розглядається не в якості його кінцевого результату, а передовсім як спосіб організації та реалізації цього процесу. Як нормотворчий процес не може ототожнюватися із нормативно-правовими актами, так і форми публічного управління не можуть асоціюватися із наслідками їх впливу на будь-який управлінський процес або ж іменуватися «формалізованим видом результатів».

З приводу методів публічного управління хотілося б висловити наступну позицію. Не зважаючи на деякі розбіжності в теоретичних позиціях, у більшості адміністративно-правових досліджень сформульовано позицію щодо наявності у адміністративно-правових відносинах свого особливого методу правового регулювання, який виражається у підпорядкуванні з боку тих суб'єктів, відносно яких здійснюються управлінські функції виконавчо-розпорядчих органів. Для цього методу характерні такі риси, як перевага приписів,

виключення юридичної рівності учасників відносин, коли одному з них наданий певний обсяг юридично владних повноважень на адресу іншого. Як наслідок, під час дослідження методів публічного управління, багато наукових публікацій перевантажені висновками щодо однобічності волевиявлення одного з учасників відносин, наявності офіційної інстанції, уповноваженої вирішувати в односторонньому порядку різноманітні питання, незалежно від того, хто виступає в ролі ініціатора цих питань.

У той же час, функціонування керуючої та керованої системи неможливо розглядати виключно в якості суто суб'єктно-об'єктної дії. Державне управління та керівництво – це особливий різновид соціального управління, їх юридичні засоби та правові форми встановлюються та реалізуються через специфічні механізми мислення та поведінки.

Уявляється, що у викладених ознаках методу адміністративно-правового регулювання вірно вказано, що підпорядкування загалом характерно для державно-управлінських відносин, які також властиві й для адміністративної діяльності органів Національної поліції.

Узагальнюючи висловлені позиції науковців з приводу змістовного наповнення форм та методів публічного управління, можна зробити висновок, що у сфері захисту персональних даних вказані правові категорії наділені певною специфікою, яка, зокрема, проявляється у їх тлумаченні. Наприклад, форми державного управління в окресленій сфері публічно-управлінських відносин являють собою зовнішній прояв діяльності органів державного управління та їх посадових осіб, яка реалізується на підставі закону та в межах встановлених повноважень щодо захисту права на невтручання у приватне життя, у зв'язку з обробкою персональних даних.

У той же час, методи державного управління у сфері захисту персональних даних представляють сукупність прийомів та способів, спрямованих на реалізацію завдань, функцій та повноважень органів державного управління та їх посадових осіб, у сфері захисту та обробки персональних даних.

Адміністративна діяльність Національної поліції України у сфері охорони публічного порядку являє собою сукупність

організаційно-правових форм, «кожна з яких має свою специфіку, яка визначається її призначенням» [149, с. 186]. Відповідно до базового законодавчого акту, яким врегульовано діяльність Національної поліції, основними її формами є: адміністративна, оперативно-розшукова, кримінально-процесуальна [40].

Адміністративна діяльність поліції – це підзаконна, державно-владна, виконавчо-розпорядча діяльність, спрямована на організацію та практичне вирішення завдань і виконання функцій поліції з охорони публічного (громадського) порядку і безпеки, що здійснюється в адміністративно-правових формах із використанням адміністративно-правових методів. Відповідно до теорії управління адміністративна діяльність є зовнішньою щодо системи поліції. Зміст цієї діяльності спрямований на забезпечення прав і свобод людини та громадянина, створення умов для реалізації прав і законних інтересів [149, с. 186].

Одним із напрямів цієї діяльності, що покладено на Національну поліцію, є контроль і нагляд за дотриманням публічного порядку, правил дорожнього руху; профілактика і припинення адміністративних правопорушень, адміністративний нагляд; охорона власності. Закон України «Про Національну поліцію» відносить до адміністративної діяльності видачу дозволу (ліцензії) на провадження охоронної діяльності та контролю за нею, ліцензій на продаж і зберігання зброї. Характерними рисами адміністративної діяльності поліції є: підпорядкованість і підконтрольність представницьким і виконавчим органам державної влади та місцевого самоврядування, державно-владний характер, підзаконність, організуючий характер, гласність і урегульованість законодавством. Внутрішньоорганізаційні адміністративні функції забезпечують функціонування всіх служб і підрозділів, ефективне використання сил і засобів. До таких функцій належать: аналіз, прогнозування та планування, формування керуючої і керованої систем, підбір і розстановка кадрів, організація взаємодії, контроль і перевірка виконання, облік [149, с. 186].

Аналіз правозастосовної діяльності Національної поліції України дозволяє зробити висновок про широке використання її органами

та підрозділами усього спектру правових форм та методів адміністративної діяльності, в частині захисту персональних даних. У той же час, ми зупинимось лише на тих із них, які посідають першорядне значення у службовій діяльності поліції.

Перш за все слід наголосити на доволі активній правотворчій діяльності Міністерства внутрішніх справ у сфері захисту персональних даних. Зазначена активність обумовлена декількома факторами. По-перше, нагадаємо, що один з пунктів Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони [150] передбачає удосконалення законодавства про захист персональних даних з метою приведення його у відповідність з Регламентом (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних [19]. Так, 20 червня 2018 року представники МВС взяли участь у зустрічі координаційної групи щодо забезпечення проекту ЄС Twinning № UA/47b «Впровадження кращого європейського досвіду з метою посилення інституційного потенціалу Секретаріату Уповноваженого ВРУ з прав людини для захисту прав і свобод людини», яка відбулася в офісі Уповноваженого Верховної Ради України з прав людини. У ході зустрічі було розглянуто порівняльний аналіз Закону України «Про захист персональних даних» і Загального регламенту про захист персональних даних, який набирає чинності 25 травня 2018 року у державах Європейського Союзу, а також пропозиції до нового Закону України «Про захист персональних даних» [151].

Другий фактор, який, на нашу думку, чинить скоріше опосередкований вплив на підвищену правотворчу активність МВС України у сфері захисту персональних даних, полягає у створенні організаційно-правових підстав (або передумов) для такої діяльності. У цьому контексті слід зазначити, що на підставі Закону України від 03.07.2013 № 383-VII «Про внесення змін до деяких законодавчих актів України щодо удосконалення системи захисту персональних даних» [152], контрольні повноваження щодо дотримання законодавства у сфері захисту персональних даних передано від

Державної служби України з питань захисту персональних даних до Уповноваженого Верховної Ради з прав людини.

На цій підставі Уповноваженим Верховної Ради з прав людини видано наказ від 08.01.2014 № 1/02-14 «Про затвердження документів у сфері захисту персональних даних» [153]. Зазначеним нормативно-правовим актом затверджено три документи, а саме: а) Типовий порядок обробки персональних даних; б) Порядок здійснення Уповноваженим Верховної Ради України з прав людини контролю за додержанням законодавства про захист персональних даних; в) Порядок повідомлення Уповноваженого Верховної Ради України з прав людини про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних, про структурний підрозділ або відповідальну особу, що організовує роботу, пов'язану із захистом персональних даних при їх обробці, а також оприлюднення вказаної інформації.

Аналіз вищенаведених документів дозволяє зробити висновок про їх загальну спрямованість на визначення загальних вимог до обробки та захисту персональних даних суб'єктів персональних даних, що обробляються повністю чи частково із застосуванням автоматизованих засобів, а також персональних даних, що містяться у картотеці чи призначені до внесення до картотеки, із застосуванням неавтоматизованих засобів [153].

У той же час, аналіз правозастосовної практики свідчить про суттєві порушення норм законодавчих та підзаконних нормативно-правових актів, виявлені Уповноваженим Верховної Ради України з прав людини з боку суб'єктів відносин у сфері захисту персональних даних.

Наприклад, в процесі моніторингу дотримання вимог Закону України «Про захист персональних даних» виявлені наступні порушення:

- невиконання вимог статті 9 вказаного Закону щодо повідомлення про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних;
- недодержання вимог частини третьої статті 10 щодо отримання від працівників зобов'язань не допускати розголошення у будь-який спосіб персональних даних, які їм було

довірено або які стали відомі у зв'язку з виконанням професійних чи службових або трудових обов'язків, крім випадків, передбачених законом;

- неповідомлення суб'єкта персональних даних відповідно до вимог частини другої статті 12 про володільця персональних даних, склад і зміст зібраних персональних даних, свої права, визначені цим Законом, мету збору персональних даних та осіб, яким передаються його персональні дані;
- недотримання вимог частини другої статті 24 щодо визначення відповідальної особи, що організовує роботу, пов'язану із захистом персональних даних при їх обробці та обов'язку володільця персональних даних повідомити Уповноваженого про створення структурного підрозділу або призначення відповідальної особи, що організовує роботу, пов'язану із захистом персональних даних при їх обробці.

Під час перевірок володільців і розпорядників персональних даних фіксувалося недотримання вимог Типового порядку обробки персональних даних, затвердженого наказом Уповноваженого від 08.01.2014 № 1/02–14, а саме:

- пункту 1.2. щодо визначення порядку обробки персональних даних;
- пункту 3.4. щодо визначення порядку доступу до персональних даних працівників володільця / розпорядника;
- визначення порядку ведення обліку операцій, пов'язаних з обробкою персональних даних суб'єкта та доступом до них;
- розроблення плану дій на випадок несанкціонованого доступу до персональних даних, пошкодження технічного обладнання, виникнення надзвичайних ситуацій;
- пункту 3.5 щодо ведення обліку працівників, які мають доступ до персональних даних суб'єктів;
- пункту 3.11 щодо обов'язку володільця персональних даних вести облік операцій, пов'язаних з обробкою персональних даних суб'єкта та доступом до них [154].

Разом з цим, МВС України за даними статистики, станом на липень 2019 року, на виконання Закону України «Про захист персональних

даних» затвердило 65 нормативно-правових актів у сфері захисту персональних даних [155], які в подальшому послужили фундаментом для розробки органами та підрозділами Національної поліції локальних нормативно-правових актів у сфері захисту персональних даних.

У той же час, попри суттєву нормотворчу активність у сфері захисту персональних даних, вказана діяльність органів та підрозділів Національної поліції України пов'язана із численними проблемними питаннями, які істотно впливають на якість та ефективність прийняття управлінських рішень. До таких пропонуємо віднести:

- слабка юридична техніка в процесі розроблення нормативно-правових актів органами Національної поліції, як на загальнодержавному, так і на регіональному рівні. Зазначений фактор негативно впливає на єдиноманітність правової бази у сфері захисту персональних даних та відсутність суперечностей у змісті правових актів. І.О. Биля у цьому контексті цілком справедливо наголошує на необхідності уніфікації правил та засобів нормотворчої техніки, з метою її подальшого запровадження у нормотворчий процес. «При цьому важливе значення у вказаному напрямку, – продовжує автор, – набуває розвиток та удосконалення практики цілеспрямованої підготовки кадрів для роботи у сфері нормопроектування» [156, с. 14].
- повільне прийняття та оновлення змісту підзаконних нормативно-правових актів, відсутність системності нормотворчого процесу. У зв'язку із значним запізненням у часі, в процесі внесення змін до підзаконних нормативно-правових актів, спостерігається їх невідповідність вимогам базового законодавчого акту.

Окрім правотворчої форми державного управління також заслуговує на увагу дослідження правозастосовної діяльності органів Національної поліції у сфері захисту персональних даних. Зазначена форма управлінської діяльності реалізується переважно шляхом здійснення контролю та нагляду за діяльністю суб'єктів у сфері захисту персональних даних. На думку авторів дослідження нагляд

у найменшій мірі властивий для діяльності органів та підрозділів Національної поліції, та, як правило, передбачає спостереження за дотриманням законів та підзаконних нормативно-правових актів під час внесення відомостей персонального характеру уповноваженими суб'єктами до Інформаційного порталу Національної поліції.

Уявляється, що реалізація правозастосовної діяльності у сфері захисту персональних даних у найбільшій мірі проявляється через здійснення контролю за станом технічного захисту інформації.

Слід зазначити, що в органах та підрозділах Національної поліції контроль за дотриманням законодавства у сфері технічного захисту інформації, в тому числі й персональних даних, покладено на Управління режиму та технічного захисту інформації, відповідно до наказу МВС України від 29.02.2016 № 139 «Про затвердження Положення про контроль за станом технічного захисту інформації в органах і підрозділах Національної поліції України» [157]. Аналіз зазначеного нормативно-правового акту дозволяє зробити висновок, що форми захисту персональних даних в інформаційних системах, які використовуються в Національній поліції, загалом мають організаційний характер. Зокрема, форми з'ясування стану технічного захисту інформації у підрозділах Національної поліції передбачають здійснення планування службової діяльності, що має на меті складання основних організаційних і практичних заходів УРТЗІ НПУ, та проведення перевірок, які, відповідно до коментованого наказу, поділяються на комплексні, цільові (тематичні) та контрольні. Зазначені перевірки також можуть бути плановими та позаплановими.

Тоді як методи діяльності Національної поліції щодо дотримання технічного захисту інформації можна з упевненістю поділити на організаційні та технічні. Так, організаційні методи передбачають здійснення низки заходів, основними серед яких є: а) аналіз та узагальнення результатів контрольно-інспекторської роботи щодо стану технічного захисту інформації; б) доповіді Голові Національної поліції України щодо стану дотримання технічного захисту інформації у підпорядкованих підрозділах поліції; в) визначення відповідності комплексу технічного захисту інформації вимогам

нормативно-правових актів; г) здійснення доступу на об'єкти технічного захисту інформації для здійснення контролю їх відповідності вимогам правил, норм і стандартів в інформаційній сфері; д) ознайомлення та опрацювання документів, необхідних для перевірки (а також за її результатами). Крім цього, технічні методи щодо забезпечення технічного захисту інформації, в тому числі, й персональних даних, передбачають здійснення наступних заходів: а) встановлення паролей доступу до інформаційної системи; б) встановлення та підтримання в актуальному стані антивірусних програм; в) встановлення технічних засобів та систем, які передбачають обмеження і контроль доступу; г) знеособлення персональних даних.

Загалом, результати перевірок УРТЗІ НПУ щодо органів поліції нижчестоячого рівня свідчать про наявність численних недоліків в організації правозастосовної діяльності останніх у сфері дотримання законодавства із захисту персональних даних. Зокрема, найпоширенішими з них є наступні:

- відсутність оформлених належним чином договорів між суб'єктами персональних даних як правило свідчить про наявність прогалин у договірних відносинах;
- невідповідність цілей обробки персональних даних, а також порушення умов договору, укладеного між володільцем та розпорядником, в частині збільшення обсягів обробки відповідної інформації;
- відсутність підстав для належної обробки інформації;
- оброблення інформації під чужим логіном та/або паролем;
- неправомірне розповсюдження персональних даних;
- не інформування суб'єкта персональних даних про зміну суттєвих умов їхньої обробки (про зміну складу та змісту зібраних персональних даних, володільця персональних даних, мети збору персональних даних та осіб, яким вони адресовані);
- доступ третіх осіб до відомостей, оброблюємих в Інформаційному порталі Національної поліції;
- невиконання вимог щодо визначення особи, відповідальної за організацію захисту персональних даних;

- порушення в процесі організації внутрішньовідомчого порядку обробки та захисту персональних даних;
- порушення технічних умов, які висуваються до обладнання службових приміщень для здійснення обробки персональних даних.

Таким чином, на підставі проведеного аналізу спробуємо зробити наступні висновки:

1. Перш за все слід зазначити, що серед правових форм та методів державного управління, які превалюють у адміністративній діяльності Національної поліції у сфері захисту персональних даних превалюють примусові заходи, які полягають у здійсненні контрольно-наглядової діяльності та застосуванні юридичної відповідальності. Разом з цим, заходи переконання та позитивного адміністративного впливу в окресленому напрямку державно-управлінської діяльності, як правило, не застосовуються у службовій діяльності органів та підрозділів Національної поліції. Систематичне інформування щодо виявлених порушень у сфері захисту персональних даних, профілактична робота, спрямована на переконання працівників поліції у необхідності дотримання законодавства у сфері захисту інформації, заохочення правомірної поведінки та інші аналогічні заходи впливу повинні знайти відображення у адміністративній діяльності Національної поліції України.

Переваги позитивного адміністративного впливу на свідому поведінку працівників поліції цілком очевидні. Якщо методи примусу – це реакція держави в особі уповноважених органів на кінцеву поведінку суб'єктів адміністративно-правових відносин, то перелічені вище профілактичні заходи створюють передумови правомірної поведінки та чинять безпосередній вплив на недопущення правопорушень у подальшій службовій діяльності поліцейських.

2. У зв'язку з тим, що порушення технічного захисту інформації відрізняються високим ступенем латентності, ефективність правозастосовної діяльності у сфері захисту персональних даних є невисокою. Аналіз здійснення перевірок управлінням режиму та захисту інформації у сфері захисту інформації органами та підрозділами Національної поліції свідчить про недостатньо широке

використання примусових методів, які по суті виступають в ролі ключового елементу в системі заходів адміністративно-правового впливу.

Причинами такої невтішної ситуації виступають численні фактори, основними з яких є недостатній рівень матеріально-технічного та кадрового забезпечення органів та підрозділів Національної поліції; відсутність належної координації та обміну інформацією між підрозділами режиму та технічного захисту інформації у сфері захисту персональних даних; дублювання повноважень працівників різних служб у сфері захисту інформації, зокрема підрозділів інформаційно-аналітичної підтримки, зв'язку та телекомунікацій, режиму та технічного захисту інформації тощо; складності, обумовлені відсутністю фахових знань працівників поліції в процесі виявлення та фіксації правопорушень у сфері захисту інформації. Уявляється, що вироблення заходів щодо подолання зазначених негативних чинників повинно стати пріоритетним завданням керівництва Національної поліції України.

3. Форми та методи адміністративної діяльності поліції у сфері захисту персональних даних мають отримати відповідне правове забарвлення, основа якого передовсім полягає у виробленні гармонійного, дієвого та ефективного нормативно-правового підґрунтя, удосконаленні законодавства у сфері захисту інформації, в частині його актуальності та відповідності вимогам практики.

Функції завдання та повноваження органів Національної поліції у сфері захисту персональних даних повинні бути: а) чітко сформовані та б) відмежовані за сферами компетенції. Діяльність органів Національної поліції у вказаному напрямку повинна ґрунтуватися на принципах плановості, послідовності, міжрегіональної координації, взаємодії з органами державної влади та місцевого самоврядування у сфері захисту персональних даних.

Уявляється, що висловлені пропозиції стануть головною, але не єдиною умовою підвищення ефективності адміністративно-правового регулювання у сфері захисту персональних даних.

2.3. Реалізація адміністративно-правового механізму захисту персональних даних Національною поліцією

Змістовне наповнення права на захист персональних даних передбачає виключення можливості будь-яких дій з персоніфікованою інформацією без згоди суб'єкта персональних даних, а також забезпечення можливості останніх контролювати дії володільців персональних даних.

Причому в даному випадку презюмується, що отримання персональних даних здійснюється володільцями такої інформації за згодою їх носія або іншим законним способом. Механізм захисту права на недоторканність приватного життя при обробці персональних даних в автоматизованих інформаційних системах Національної поліції України розкривається в процесі аналізу трьох ключових напрямків його реалізації, а саме: а) адміністративно-правовому; б) нормативно-правовому; в) технічному. Спробуємо дослідити їх більш докладно.

1. Адміністративно-правові механізми захисту персональних даних. Основним законодавчим актом, в якому визначено адміністративно-правові механізми у сфері захисту персональних даних, є Закон України «Про захист персональних даних». Зокрема, частина 2 статті 24 коментованого законодавчого акту зобов'язує органи державної влади, органи місцевого самоврядування, володільців чи розпорядників персональних даних, які здійснюють їх обробку, утворювати структурні підрозділи із захисту персональних даних або визначати відповідальну за проведення вказаної роботи особу.

В цілому, органи державної влади, які є суб'єктами державного захисту права на недоторканність приватного життя в умовах автоматизованої обробки персональних даних, можна розділити на 3 групи: а) державні органи, головною метою діяльності яких є захист інформації та інформаційних ресурсів від несанкціонованого доступу; заходи, які застосовуються цими органами, використовуються для захисту широкого кола конституційних прав і мають універсальний характер. До вказаної групи належать: Національна поліція; спеціальний орган державної виконавчої влади, який здійснює функції

з контролю та нагляду у сфері інформаційних технологій і зв'язку (Державна служба спеціального зв'язку та захисту інформації); державний орган спеціального призначення з правоохоронними функціями, який забезпечує державну безпеку України (Служба безпеки України); б) державні органи, уповноважені Законом України «Про захист персональних даних» щодо здійснення контролю за дотриманням законодавства у сфері захисту персональних даних. До даної групи належать: Уповноважений Верховної Ради України з прав людини; суди.

В рамках теми нашого дослідження цілком логічним та обґрунтованим виглядає виділення третьої групи суб'єктів захисту персональних даних, специфіка діяльності яких обумовлена їх організаційним становищем, яке передбачає функціонування таких суб'єктів у структурі Національної поліції, а саме: а) Управління режиму та технічного захисту інформації (скорочено – УРТЗІ); б) Департамент внутрішньої безпеки (скорочено – ДВБ); в) Департамент протидії кіберзлочинності (скорочено – ДПК); г) інспекція з особового складу Департаменту кадрового забезпечення (скорочено – ІОС ДКЗ); д) управління моніторингу патрульної поліції; е) керівники органів та підрозділів Національної поліції.

Уявляється, що серед вищевказаних суб'єктів у сфері захисту персональних даних в органах та підрозділах Національної поліції, провідна роль належить Управлінню режиму та технічного захисту інформації, за яким закріплено функцію контролю за станом технічного захисту інформації в органах і підрозділах Національної поліції України.

Аналіз Положення про контроль за станом технічного захисту інформації в органах і підрозділах Національної поліції України, затвердженого наказом МВС України від 29.02.2016 № 139, дозволив охарактеризувати повноваження посадових осіб УРТЗІ НПУ, які під час здійснення перевірок стану технічного захисту інформації, мають право на:

1) доступ на об'єкти інформаційної діяльності органів, щодо яких здійснюється ТЗІ, для здійснення контролю за станом ТЗІ, а також до інших приміщень (на територію, у споруди, будівлі, кабінети) для вивчення питань, безпосередньо пов'язаних з перевіркою;

2) ознайомлення з будь-якими документами, необхідними для перевірки;

3) отримання копій необхідних документів, письмових пояснень посадових осіб (довідок, рапортів) з питань, що виникають під час перевірки;

4) надання за результатами перевірок обов'язкових для виконання рекомендацій щодо приведення стану ТЗІ у відповідність до вимог чинного законодавства України та здійснення контролю за їх виконанням;

5) порушення питання перед керівниками органів, щодо яких здійснюється ТЗІ, стосовно проведення службового розслідування (перевірки) при невиконанні вимог нормативно-правових актів і нормативно-технічних документів з питань технічного захисту інформації, вимога щодо захисту якої встановлена законом [157].

Авторський колектив науково-практичного видання «Моніторинг незаконного насильства в поліції України (2004–2017 рр.)» також розділяє висловлену думку, при цьому Д. Кобзін зазначає, що «усі старі структури, такі як інспекція з особового складу та управління внутрішньої безпеки, так і залишилися майже без змін у структурі та мандаті. Єдине, про що необхідно згадати при реформуванні поліції, це поява управління (відділу) моніторингу патрульної поліції, яке за змістом роботи є фактично копією інспекції з особового складу, але з новою назвою та повноваженнями, які стосуються виключно патрульних поліцейських» [158, с. 62].

Разом з цим, компетенційні повноваження щодо дотримання прав людини, в частині захисту їх персональних даних з 2016 до 2019 року належали Управлінню забезпечення прав людини. Відновлення системи контролю дотримання прав людини в діяльності поліції у вигляді функціонування УЗПЛ відбулось у 2016 році за ініціативи на той час Голови Національної поліції України Х. Деконаїдзе, яка називала новостворену структуру «поліцейськими омбудсманами» [158, с. 63].

Аналіз завдань, функцій та повноважень УЗПЛ дозволив зробити уявлення про існування цілісного та ефективного механізму забезпечення прав людини у сфері захисту персональних даних. Наприклад, головним завданням УЗПЛ в інформаційній

сфері діяльності Національної поліції є забезпечення контролю за дотриманням прав і свобод людини поліцейськими, державними службовцями та іншими працівниками поліції під час надання поліцейських послуг.

Функціональна спрямованість УЗПЛ також передбачає доволі розгалужену систему напрямків його діяльності, спрямованих на забезпечення прав людини у сфері захисту персональних даних. Зокрема, УЗПЛ наділено функціями щодо: а) забезпечення проведення перевірок дотримання прав і свобод людини в діяльності органів (підрозділів) поліції; б) ініціювання та участь у проведенні службових розслідувань у складі створених комісій за відомостями щодо порушення працівниками поліції прав і свобод людини.

Водночас, маємо констатувати недостатнє висвітлення результатів діяльності УЗПЛ щодо забезпечення прав людини у сфері захисту персональних даних. За результатами аналізу Звіту Голови Національної поліції України С. Князєва про результати роботи відомства за 2018 рік, де, на жаль, питання дотримання прав людини в діяльності Національної поліції не визначені в якості пріоритетних [159].

Крім того, аналіз огляду Національної поліції України, викладеному у доповідній записці від 01.08.2019 № 25027 «Про стан дотримання прав людини в діяльності органів Національної поліції України за 6 місяців 2019 року» дозволяє зробити висновок, що серед різних видів скарг на порушення прав людини в діяльності поліції, така їх підстава, як порушення законодавства щодо захисту персональних даних взагалі відсутня. До прикладу: за 6 місяців 2019 року зареєстровано 7862 скарги щодо порушення прав і свобод громадян працівниками органів Національної поліції, з яких 1771 (22,5%) – за катування, побиття, протиправне застосування фізичної сили (у тому числі 1 скарга дітей на жорстоке поводження), 3625 (46%) – за незаконне притягнення до адміністративної відповідальності, 266 (3,4%) – за незаконне затримання, доставляння до підрозділу поліції, 86 (1%) – за незаконний обшук, 79 (1%) – за незаконне притягнення до кримінальної відповідальності, 16 – за незаконне утримання в інших службових приміщеннях органів поліції,

9 – за незаконне утримання в кімнатах для затриманих/доставлених чергових служб, 8 – за позбавлення права на захист, 7 – за обмеження вільного пересування, 5 – за примушення до вчинення дій за ст.ст. 11, 18 КПК України, 4 – за расову, національну та релігійну нетерпимість, 3 – за незаконне утримання в ізоляторах тимчасового тримання [160].

Це передовсім свідчить про те, що попри сформовану організаційну структуру органів Національної поліції, діяльність яких спрямована на захист персональних даних, фактично контрольно-наглядова діяльність у цьому напрямку не здійснюється, а численні порушення законодавства про захист персональних даних в діяльності Національної поліції, не виявляються.

Подальший аналіз Закону України «Про захист персональних даних», надав змогу зробити висновок, що відповідно до частини 1 статті 24 цього Закону безпосередній обов'язок щодо забезпечення захисту цих даних від випадкових втрати або знищення, від незаконної обробки, у тому числі незаконного знищення чи доступу до персональних даних покладено на володільців, розпорядників персональних даних, а також третіх осіб.

Слід зазначити, що у п. 3 «Типового порядку обробки персональних даних у базах персональних даних», затвердженого наказом Уповноваженого Верховної Ради з прав людини від 08.01.2014 № 1/02-14 [153] перелік заходів із захисту персоніфікованої інформації докладно регламентований та передбачає покладення відповідних обов'язків на володільця та розпорядника персональних даних щодо забезпечення захисту персональних даних на всіх етапах їх обробки, у тому числі за допомогою організаційних та технічних заходів. Так, організаційні заходи щодо забезпечення захисту персональних даних охоплюють: а) визначення порядку доступу до персональних даних працівників володільця/розпорядника; б) визначення порядку ведення обліку операцій, пов'язаних з обробкою персональних даних суб'єкта та доступом до них; в) розробку плану дій на випадок несанкціонованого доступу до персональних даних, пошкодження технічного обладнання, виникнення надзвичайних ситуацій; г) регулярне навчання співробітників, які працюють з персональними даними.

Аналіз законодавства в сфері автоматизованої обробки персональних даних органами та підрозділами Національної поліції дозволяє виділити наступні заходи державного захисту права на недоторканність приватного життя в умовах автоматизованої обробки персональних даних:

- облік операторів обробки персональних даних в Інформаційному порталі Національної поліції;
- контроль виконання вимог безпеки при обробці персональних даних в автоматизованих інформаційних системах;
- ліцензування та контроль за додержанням ліцензіатами відповідних вимог і умов при здійсненні діяльності з технічного захисту персональних даних як виду інформації обмеженого доступу;
- застосування заходів дисциплінарного впливу до посадових осіб, уповноважених на обробку персональних даних за порушення їх конфіденційності, якщо умовою ліцензії є заборона на передачу персональних даних третім особам без згоди в письмовій формі суб'єкта персональних даних;
- припинення обробки персональних даних, яка здійснюється з порушенням вимог законодавства, шляхом обмеження доступу до Інформаційного порталу Національної поліції;
- опублікування звітів про стан захисту персональних даних в органах та підрозділах Національної поліції в засобах масової інформації.

Попри те, що на теперішній час на законодавчому рівні фактично відсутній механізм превентивного виявлення порушень обробки персональних даних, облік володільців та розпорядників персоніфікованої інформації має принципове значення в організації державного захисту права на недоторканність приватного життя, а тому має бути вдосконалений. Вважаємо, що основний акцент в удосконаленні адміністративно-правового механізму захисту персональних даних в Національній поліції слід зробити на посиленні контролю за обігом персоніфікованої інформації, збільшенні ефективності контрольних заходів, які повинні передбачати не тільки (і, навіть, не стільки) проведення безпосередніх перевірок стану дотримання

законодавства у сфері захисту персональних даних, але, перш за все, здійснення профілактичних заходів у вигляді постійного моніторингу обігу персональних даних в інформаційних системах Національної поліції. З іншого боку, набув актуальності процес професійного відбору працівників поліції, допущених до роботи з персональними даними, який також безпосередньо впливає на стан дотримання законодавства в окресленій сфері державного управління.

Одна з гарантій захисту прав суб'єктів персональних даних полягає в обов'язку володільця (розпорядника) персоніфікованої інформації до початку обробки персональних даних повідомити уповноважений орган із захисту прав суб'єктів персональних даних про свій намір здійснювати обробку персональних даних.

Слід зазначити, що основні права суб'єктів персональних даних визначені у статті 8 Закону України «Про захист персональних даних».

Докладний аналіз всієї сукупності прав суб'єктів персональних даних, визначених у статті 8 вищезгаданого законодавчого акту, дозволив нам класифікувати їх, в залежності від мети їх реалізації суб'єктами персональних даних, на основні та похідні. Наприклад, не викликає сумніву, що право на доступ до своїх персональних даних (п. 3 ч. 2 ст. 8 Закону) виступає в ролі основного права суб'єкта персональних даних, тоді як право на отримання інформації про умови надання доступу до персональних даних, зокрема інформації про третіх осіб, яким передаються персональні дані (п. 2 ч. 2 ст. 8 Закону), скоріше виступає в якості похідного права громадянина. Те ж саме стосується і права суб'єкта на захист своїх персональних даних (п. 7 ч. 2 ст. 8 Закону), яке має усі властивості основного права субєкта. У той же час, право громадянина звертатися із скаргами на обробку своїх персональних даних до Уповноваженого або до суду (п. 8 ч. 2 ст. 8 Закону), а також інші права, передбачені п.п. 5,6,9,10,11 ч. 2 ст. 8 Закону «Про захист персональних даних» виступають в ролі формального вираження основного права суб'єкта персональних даних – права на захист своїх персональних даних.

Також встановлені вимоги щодо захисту персональних даних й відносно працівників володільця персональних даних, які,

відповідно до Типового порядку обробки персональних даних у базах персональних даних [153], до безпосередньої обробки персональних даних, в обов'язковому порядку повинні пройти процедуру автентифікації; відповідно, й доступ до системи працівників, які не пройшли процедуру автентифікації, блокується оператором; коментований документ також визначає можливість здійснення реєстрації результатів ідентифікації або автентифікації працівників володільця персональних даних.

Слід зазначити, що вказані положення цілком узгоджуються із порядком надання доступу до роботи з персональними даними у Національній поліції та відбиваються у 4 розділі Положення про інформаційно-телекомунікаційну систему «Інформаційний портал Національної поліції України», затвердженому наказом МВС України від 03.08.2017 № 676. Зокрема, адміністратором системи ІПНП, в ролі якого виступає уповноважений структурний підрозділ апарату центрального органу управління Національної поліції України, забезпечується ведення обліку користувачів та надання їм доступу до інформації, що в ній обробляється. Також, на вказані структурні підрозділи поліції покладаються повноваження щодо захисту інформації від несанкціонованого доступу, знищення, модифікації та блокування доступу до неї шляхом здійснення організаційних і технічних заходів, впровадження засобів та методів технічного захисту інформації [29].

Звичайно, вимоги щодо захисту персональних даних в органах державної влади, органах місцевого самоврядування, на підприємствах, в установах, організаціях тощо, викладені в Типовому порядку обробки персональних даних у базах персональних даних в загальному вигляді. Кожна установа, в тому числі й органи Національної поліції, формують та реалізують заходи щодо забезпечення захисту персональних даних відповідно до відомчих нормативно-правових актів, що обумовлено специфікою діяльності поліції.

Таким чином, підбиваючи проміжні підсумки щодо функціонування та реалізації адміністративно-правових механізмів захисту персональних даних в органах та підрозділах Національної поліції, можемо сформулювати наступні висновки:

1. Загальні вимоги щодо адміністративно-правового забезпечення захисту персональних даних сконцентровані у низці законодавчих актів, чільне місце серед яких посідає Закон України «Про захист персональних даних». Разом з цим, організаційно-правові заходи у вказаній сфері державного управління докладно визначені на підзаконному рівні, зокрема, в Типовому порядку обробки персональних даних у базах персональних даних, затвердженому наказом Уповноваженого Верховної Ради з прав людини від 08.01.2014 № 1/02-14. Слід зазначити, що не зважаючи на доволі деталізований характер вказаного документу, процедура реалізації механізму захисту персональних даних сформульована в загальному вигляді та розповсюджується на діяльність усіх органів виконавчої влади, органів місцевого самоврядування, підприємств, установ, організацій та їх посадових осіб. В органах Національної поліції положення вказаного нормативно-правового акту деталізуються у низці відомчих правових приписів, які у свою чергу утворюють систему підзаконних нормативно-правових актів у сфері захисту персональних даних в органах та підрозділах Національної поліції.

2. Реалізація адміністративно-правового механізму у сфері захисту персональних даних покладено на низку державних органів, які класифіковані авторами, залежно від обсягу наданих їм повноважень у сфері захисту персональних даних. Зокрема, за вказаним критерієм органи державної влади, які є суб'єктами державного захисту права на недоторканність приватного життя в умовах автоматизованої обробки персональних даних, розподілено на 3 групи. В рамках теми цього дослідження особливу зацікавленість викликає третя група, сформована за принципом відомчої підпорядкованості органів поліції, наділених повноваженнями у сфері захисту персональних даних. До їх числа відносяться: а) управління режиму та технічного захисту інформації (скорочено – УРТЗІ); б) департамент внутрішньої безпеки (скорочено – ДВБ); в) департамент протидії кіберзлочинності (скорочено – ДПК); г) інспекція з особового складу Департаменту кадрового забезпечення (скорочено – ІОС ДКЗ); д) підрозділи моніторингу департаменту патрульної поліції; е) керівники органів та підрозділів Національної поліції.

Останній пункт запропонованої структури яскраво демонструє загальне завдання кожного керівника щодо забезпечення контролю за обігом персональних даних в органах Національної поліції. У той же час, провідна роль у цьому процесі безперечно належить управлінню режиму та технічного захисту інформації, адже вказаний орган Національної поліції наділений широкими повноваженнями у сфері технічного захисту інформації.

3. Реалізація адміністративно-правового механізму захисту персональних даних в органах та підрозділах Національної поліції полягає у здійсненні низки організаційно-практичних заходів, спрямованих на покращення правовідносин у вказаній сфері державного управління, а саме: а) облік операторів обробки персональних даних в Інформаційному порталі Національної поліції; б) контроль виконання вимог безпеки при обробці персональних даних в автоматизованих інформаційних системах; в) ліцензування та контроль за додержанням ліцензіатами відповідних вимог і умов при здійсненні діяльності з технічного захисту персональних даних як виду інформації обмеженого доступу; г) застосування заходів дисциплінарного впливу до посадових осіб, уповноважених на обробку персональних даних, за порушення їх конфіденційності; д) припинення обробки персональних даних, яка здійснюється з порушенням вимог законодавства, шляхом обмеження доступу до Інформаційного порталу Національної поліції; е) опублікування звітів про стан захисту персональних даних в органах та підрозділах Національної поліції в засобах масової інформації.

2. Нормативно-правовий механізм захисту персональних даних. Сучасний етап розвитку інформаційних відносин характеризується наявністю значних обсягів інформаційних ресурсів та інформації, яка відноситься до різних сфер суспільних відносин. Важливо й те, що стрімкий розвиток правових відносин в інформаційній сфері, з одного боку, та можливостей сучасних інформаційних та інформаційно-комунікаційних технологій – з іншого, у своїй сукупності об'єктивно формують необхідність удосконалення механізмів збору, зберігання, використання та розповсюдження інформації, оскільки остання являє собою відомості про навколишнє середовище та

процеси, які відбуваються в ньому. Характерним є й те, що з кожним роком перелік підстав та приводів для збору та обробки нових даних збільшується, а тому спостерігається постійно зростаюча потреба громадян у захисті особистої інформації.

У цьому контексті надзвичайної актуальності набувають питання нормативно-правової регламентації адміністративно-правових механізмів захисту персональних даних. Але особливого значення в цьому процесі належить реалізації завдань щодо захисту прав і свобод людини під час використання персональних даних органами Національної поліції.

У 2005 році Україна ратифікувала Конвенцію Ради Європи 1981 року №108 «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних» та взяла на себе відповідні зобов'язання у сфері захисту персональних даних, основні з яких полягають у прийнятті низки нормативно-правових актів, які сприятимуть покращенню механізму захисту персональних даних.

Аналіз нормативно-правового забезпечення механізму захисту персональних даних в органах Національної поліції України ми побудували в залежності від специфіки діяльності Національної поліції, яка наділена яскраво вираженою правоохоронною функцією, а тому акцент у цьому напрямку дослідження буде зроблено на матеріальних та процесуальних аспектах юридичної відповідальності за правопорушення у сфері захисту персональних даних.

1. Конституція України визначає вимогу щодо заборони втручання в особисте та сімейне життя громадян (частина 1 статті 32); також, відповідно до положень основного закону, 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 (частина 2 статті 32); особливо підкреслимо встановлення на конституційному рівні правових гарантій судового захисту права щодо спростування недостовірної інформації про себе та членів своєї сім'ї, а також права вимагати вилучення будь-якої інформації (частина 4 статті 32) [57].

2. Закон України «Про інформацію» встановлює легальне визначення персональних даних, ототожнюючи його з правовою категорією «інформація про фізичну особу», під якою розуміються відомості чи сукупність відомостей про фізичну особу, що ідентифікована або може бути конкретно ідентифікована (частина 1 статті 11). «Не допускаються 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 захисту прав людини» (частина 2 статті 11) [79].

3. Обов'язок щодо виконання вимог встановленого Законом України «Про захист персональних даних» режиму захисту персональних даних покладено на сторону, яка поширює ці дані (частина 3 статті 14). Коментований законодавчий акт також встановлює відповідальність за порушення законодавства про захист персональних даних (стаття 28) [72]. Одним із напрямків забезпечення режиму захисту персональних даних є реєстрація баз персональних даних, шляхом внесення відповідного запису уповноваженим державним органом з питань захисту персональних даних до Державного реєстру баз персональних даних.

4. Вимоги щодо застосування комплексної системи захисту з підтвердженою відповідністю під час використання інформації, яка є власністю держави або інформації з обмеженим доступом, встановлені частиною 2 статті 8 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» [161].

5. Кримінальна відповідальність за незаконне збирання, зберігання, використання, знищення, поширення конфіденційної інформації про особу або незаконна зміна такої інформації, крім випадків, передбачених іншими статтями Кримінального кодексу України передбачена статтею 182 КК України [162].

6. Стаття 29 Кодексу законів про працю передбачає обов'язок власника або уповноваженого ним органу проінструктувати працівника і визначити йому робоче місце. Зокрема, власник або уповноважений ним орган зобов'язаний «роз'яснити працівникові його права і обов'язки та проінформувати під розписку про умови

праці, ...ознайомити працівника з правилами внутрішнього трудового розпорядку та колективним договором, ...визначити працівникові робоче місце, забезпечити його необхідними для роботи засобами» [163].

7. З метою забезпечення виконання громадянами, органами державної влади, органами місцевого самоврядування, підприємствами, установами, організаціями незалежно від форм власності Закону України «Про захист персональних даних» Верховною Радою України 02 червня 2011 року прийнято Закон України «Про внесення змін до деяких законодавчих актів України щодо посилення відповідальності за порушення законодавства про захист персональних даних» [164], яким внесено зміни до Кодексу України про адміністративні правопорушення [165].

З 01 липня 2012 року за порушення у сфері захисту персональних даних на громадян, посадових осіб, громадян – суб'єктів підприємницької діяльності покладається адміністративна відповідальність. Зокрема, адміністративна відповідальність громадян, посадових осіб, громадян – суб'єктів підприємницької діяльності може наставати за наступні діяння: а) неповідомлення або несвоєчасне повідомлення суб'єкта персональних даних про його права у зв'язку із виключенням його персональних даних до бази персональних даних, мету збору цих даних та осіб, яким ці дані передаються; б) неповідомлення або несвоєчасне повідомлення спеціально уповноваженого центрального органу виконавчої влади з питань захисту персональних даних про зміну відомостей, що подаються для державної реєстрації бази персональних даних; в) ухилення від державної реєстрації бази персональних даних; г) недодержання встановленого законодавством про захист персональних даних порядку захисту персональних даних у базі персональних даних, що призвело до незаконного доступу до них (ст. 188-39 КУпАП).

8. У Цивільному кодексі України право на захист персональних даних зафіксовано у ст.ст. 301-308. Аналіз змісту вказаних статей ЦК України дозволив зробити наступні висновки: а) закон взагалі не використовує правову конструкцію «персональні дані», оперуючи переважно термінами «особисте життя» (ст. 301), «особисте немайнове

право» (ст. 280), «сімейне життя» (ч.4 ст. 281) і т.д.; б) проголошується право на таємницю особистого життя, за винятком випадків, коли обставини особистого життя містять ознаки правопорушення, що підтверджено рішенням суду або за згодою суб'єкта персоніфікованої інформації (ч.ч. 1–4 ст. 301); в) на виконання положень Конституції України, Цивільний кодекс України визначає право особи на вільне збирання, зберігання, використання та поширення інформації, за винятком випадків, передбачених законом (ст. 302); г) особисті папери фізичної особи визначені її власністю, у зв'язку з чим закон вимагає отримання згоди фізичної особи для їхнього використання (ст. 303); д) правила щодо захисту персональних даних розповсюджуються також і на таємницю кореспонденції, а також на проведення фото-, кіно-, теле- та відео зйомок (ст.ст. 306–308) [166].

Таким чином, нормативно-правовий механізм захисту персональних даних в діяльності Національної поліції являє собою взаємоузгоджену цілісну систему нормативно-правових актів, спрямованих на врегулювання правовідносин у сфері захисту та обробки персональних даних в службовій діяльності органів та підрозділів Національної поліції України.

3. Механізм технічного захисту персональних даних в органах та підрозділах Національної поліції.

Аналіз правових актів у сфері технічного захисту персональних даних дозволив зробити висновок про обов'язкове застосування комплексної системи захисту інформації до всіх автоматизованих систем, призначених для створення та обробки баз персональних даних, які підпадають під дію Закону України «Про захист персональних даних». Комплексна система захисту інформації включає такі елементи, як: а) проект технічного захисту інформації; б) система внутрівідомчих правових актів, які регламентують функціонування автоматичних систем, призначених для створення та обробки баз персональних даних; в) апаратно-програмне забезпечення; г) система підготовки фахівців у сфері захисту персональних даних. Механізм захисту персональних даних в інформаційних системах також зобов'язує власника автоматизованої системи

створення та обробки баз персональних даних присвоїти персоніфікованій інформації статус «обмежений доступ».

Дослідницький інтерес у цьому контексті викликає лист Державної служби України з питань захисту персональних даних від 02.04.2012 №10/1106-12, у якому надано роз'яснення стосовно змістовного наповнення та юридичного тлумачення правової категорії «персональні дані» [167].

Зокрема, у вказаному документі надані роз'яснення щодо необхідності розуміння правової категорії «персональні дані» із врахуванням всієї сукупності відомостей про фізичну особу, яка ідентифікована або може бути ідентифікована будь-яким можливим способом. Окремо в коментованому документі наголошується на тому, що для визначення факту ідентифікації особи необхідно враховувати всі можливі засоби, передбачені законом.

І тут же зазначається про необхідність доповнення переліку персональних даних «інформацією про особу, викладеною у візитниці, адресній книзі електронної пошти підприємства, а також списком контактів у мобільному телефоні». З одного боку, вважаємо такий підхід цілком справедливим, адже вказані документи відображають особисту інформацію про суб'єктів персональних даних. У той же час, уявляється, що вся сукупність персоніфікованої інформації не дозволяє вмістити її у будь-які чітко окреслені межі, в тому числі, шляхом визначення в нормативно-правових приписах конкретних їх прикладів.

Тому, на нашу думку, для вирішення цього питання, слід виходити із розуміння персональних даних як інформації особистого характеру, яка походить від самого суб'єкта персональних даних. Простіше кажучи, якщо особа визначає будь-яку інформацію про себе, або оточуюче її середовище персональними даними, її слід визнати саме в такому контексті.

З огляду на висловлену позицію, спробуємо сформулювати більш уточнююче визначення персональних даних, ніж наведене у Законі України «Про захист персональних даних», а саме: персональні дані – відомості чи сукупність відомостей, особистий характер яких визначено фізичною особою, яка ідентифікована або може бути конкретно ідентифікована.

Використання інженерно-технічних заходів виступає в якості важливого компоненту у побудові комплексної системи захисту інформації в органах та підрозділах Національної поліції. Вибір таких технічних засобів залежить від рівня захисту інформації, який необхідно забезпечити. До таких заходів належать, зокрема, застосування захищеного підключення до мережі, використання міжмережевих екранів, встановлення розмежування інформаційних потоків між частинами мережі.

За словами С.В. Сеника, нині важливим аспектом щодо використання інженерно-технічних заходів є застосування методів і засобів шифрування та захисту від несанкціонованого доступу. Не слід також забувати про можливість, а деколи і про необхідність установлення охоронної сигналізації, систем контролю та управління доступом, обладнання приміщень засобами захисту від витоку мовної (акустичної) інформації та від витоку інформації каналами побічних електромагнітних випромінювань [168, с. 182].

Значно жорсткіші умови передбачені для захисту інформації, яка становить державну таємницю. Технічними нормами в обов'язковому порядку передбачено створення комплексу технічного захисту інформації, захисту від її витоку через побічні електромагнітні випромінювання та наведення (1–3 категорій об'єктів, відповідно до ТПКО-95 [169]), або у разі, якщо потребу в цьому визначено власником інформації [170].

Встановлення комплексу засобів захисту також, на думку деяких науковців, здійснюється у випадку, якщо в інформаційно-телекомунікаційній системі опрацьовується інформація, що є власністю держави (може містити різні види інформації), необхідність захисту якої визначається законодавством, а також інформаційно-телекомунікаційні системи, де таку необхідність установив власник інформації. Цей комплекс має забезпечувати захист інформації з обмеженим доступом від витоку технічними каналами, насамперед каналами побічних електромагнітних випромінювань та наведень. Під час створення комплексу технічного захисту інформації має застосовуватися сукупність організаційно-правових, інженерно-технічних заходів та засобів, до яких вдаються з метою захисту від витоку

інформації з обмеженим доступом технічними каналами [168, с. 183].

Створення та випробовування комплексу технічного захисту інформації проводиться відповідно до положень НД ТЗІ 1.1-005-07 [171], НД ТЗІ 1.6-003-04 [172], НД ТЗІ 3.1-001-07 [173]. Задля з'ясування потреби запровадження заходів захисту інформації від витоку технічними каналами проводиться спеціальне дослідження персональних комп'ютерів, під час якого визначаються можливі канали витоку інформації. За результатами такого аналізу приймається рішення про необхідність встановлення активних та пасивних технічних засобів захисту інформації. З метою створення єдиного підходу до питань побудови комплексних систем захисту інформації в Україні розроблено та запроваджено низку нормативних документів [168, с. 184].

Приміром, створення комплексної системи захисту інформації в інформаційно-телекомунікаційних системах здійснюється відповідно до нормативного документа системи технічного захисту інформації НД ТЗІ 3.7-003-05 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі» [174] на підставі технічного завдання, розробленого згідно з вимогами нормативного документа системи технічного захисту інформації НД ТЗІ 3.7-001-99 «Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі» [175].

Підбиваючи загальні підсумки, слід зазначити, що адміністративно-правовий механізм захисту персональних даних Національною поліцією являє собою комплекс заходів щодо забезпечення конституційних прав громадян на захист персональних даних, створення умов, що обмежують її поширення і виключають незаконний доступ працівників поліції до цього виду конфіденційної інформації і її носіїв. Зазначені заходи спрямовані на запобігання витоку і втрати персональних даних, збереження їх повноти та достовірності.

Спробуємо сформулювати основні напрямки захисту персональних даних, які утворюють адміністративно-правовий механізм захисту персональних даних в Національній поліції України, а саме:

1. Дотримання порядку надання відомостей персонального характеру. Це один з основних напрямків захисту персональних даних,

який полягає в суворому дотриманні встановлених юридичних підстав на передачу інформації визначеному колу користувачів з урахуванням її обсягу і технології передачі. На наш погляд, при передачі персональних даних про особу уповноваженими працівниками поліції, за певних випадків необхідно в письмовій формі зафіксувати підставу і факт передачі інформації, а також попередити осіб, які отримують ці відомості, про те, що дані є конфіденційною інформацією персонального характеру.

2. Дотримання правил зберігання, обліку та обробки конфіденційних відомостей на паперових носіях. Оскільки переважна більшість персональної інформації зберігається на паперових носіях, для її захисту необхідно обмежити доступ сторонніх осіб до цих відомостей (наприклад, виключити зберігання персональних даних на робочих столах; організувати систему обліку відомостей та кодування персоніфікованих даних, інструктаж про порядок роботи з персональними даними).

3. Захист персональних даних, розташованих на електронних носіях. Актуальний у всіх випадках, коли для їх отримання, зберігання, обліку та обробки застосовуються засоби обчислювальної техніки. Заходи щодо захисту такої інформації тут різні: створення внутрішніх (локальних) мереж баз даних, розмежування прав доступу користувачів до автоматизованих робочих місць та баз даних; застосування системи кодування електронної інформації; використання знімних носіїв інформації і спеціальних технічних засобів її захисту. При цьому захист персональних даних повинен здійснюватися не тільки працівниками поліції, а й іншими суб'єктами (в першу чергу – технічними фахівцями).

4. Покладання відповідальності за втрату і розголошення персональної інформації. Встановлення юридичної відповідальності має профілактичне значення в системі заходів, що використовуються в органах та підрозділах Національної поліції щодо захисту персональних даних. Уповноважені посадові особи органів поліції, винні в порушенні норм, що регулюють отримання, обробку, зберігання і захист персональних даних про особу, що знаходяться в базах даних, повинні притягуватися до

дисциплінарної, адміністративної, цивільно-правової та кримінальної відповідальності.

5. Забезпечення режиму конфіденційності в роботі співробітників поліції. Даний напрямок пов'язано з особливостями професійної діяльності поліцейських, в ході якої вони інтенсивно використовують (отримують, передають) різні відомості персонального характеру. Таким чином, захист персональних даних виступає як один із важливих напрямків роботи органів та підрозділів Національної поліції та багато в чому обумовлює успішність реалізації інших видів заходів щодо забезпечення службової діяльності.

3. АКТУАЛЬНІ ПИТАННЯ УДОСКОНАЛЕННЯ АДМІНІСТРАТИВНО-ПРАВОВОГО ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ НАЦІОНАЛЬНОЮ ПОЛІЦІЄЮ

3.1. Міжнародно-правове забезпечення захисту персональних даних правоохоронними органами

Організація діяльності правоохоронних органів, пов'язана із захистом конфіденційної інформації, як на національному, так і міжнародному рівні, не може не враховувати загальносвітові тенденції, які так чи інакше впливають на стан та рівень захищеності персональних даних, а саме: рівень розвитку сучасного інформаційного суспільства, триваючі й дотепер процеси інтеграції та глобалізації, фактичний вихід взаємодії суб'єктів захисту конфіденційної інформації за межі адміністративних кордонів окремих країн.

Особливого значення вказані обставини набули в процесі здійснення правоохоронними органами багатьох провідних країн світу інформаційно-аналітичної діяльності, зокрема в частині збору та обробки персональних даних.

Загалом інформаційно-аналітична діяльність органів Національної поліції передбачає здійснення заходів, спрямованих на інформаційно-аналітичне та інформаційно-пошукове забезпечення правоохоронної діяльності та захист персональних даних при їх обробці в структурних підрозділах апарату Національної

поліції України, головних управліннях Національної поліції України в Автономній Республіці Крим та м. Севастополі, областях, м. Києві, міжрегіональних територіальних органах Національної поліції України, їх структурних (відокремлених) підрозділах [176].

Інформаційно-аналітичне забезпечення як один з ключових елементів організації роботи системи правоохоронних органів, у цілому передбачає реалізацію двох основних напрямків: а) здійснення інформаційно-пошукової роботи, спрямованої на підтримку оперативно-розшукової діяльності; б) аналітична робота щодо забезпечення прийняття стратегічних рішень у сфері правоохоронної діяльності та координація службової діяльності правоохоронних органів.

Особлива актуальність та значущість аналітичної роботи Національної поліції підкреслена керівниками апарату Національної поліції під час проведення за дорученням Голови Національної поліції України генерала поліції першого рангу Сергія Князєва на базі Головного управління Національної поліції в Закарпатській області з 14 по 16 червня 2018 року семінар-наради керівників підрозділів організаційно-аналітичного забезпечення та оперативного реагування і інформаційно-аналітичної підтримки [177].

Зауважимо, що необхідність активного використання інформації та інформаційних ресурсів працівниками поліції неухильно зростала протягом останніх декількох десятиліть. Поліцейські інформаційні системи, які в минулому існували у вигляді архівів з інформаційними картотеками, стрімко розвинулись поряд із розвитком інформаційних технологій, в рамках спеціального програмного забезпечення та навичок професійного аналізу злочинності. І в теперішній час використання інформації в службовій діяльності поліції не втрачає своєї актуальності, адже в стратегічному та тактичному аспектах інформація може бути використана для прийняття більш точних та виправданих рішень.

Але вказане питання викликає зацікавленість наукової спільноти та практичних працівників не тільки в рамках діяльності правоохоронних органів конкретно визначеної держави, а й на міжнародному рівні.

Аналіз численних наукових публікацій засвідчив, що на теперішній час на міжнародному рівні розроблено низку нормативно-правових актів, спрямованих на вироблення загальних принципів та підходів організації інформаційно-аналітичної діяльності в структурі правоохоронних органів, які дозволяють оптимальним чином збалансувати захист інтересів суспільства щодо протидії злочинності та підтриманню публічного порядку, з одного боку, а з іншого – забезпечення прав людини на приватність, зокрема, в частині захисту персональних даних [178–182].

До вказаних міжнародно-правових документів слід віднести Конвенцію про захист осіб у зв'язку з автоматизованою обробкою персональних даних [69], Рекомендацію Комітету міністрів Ради Європи № R(87)15 1987 року про використання персональних даних у секторі поліції [183], Додатковий протокол 2001 року до Конвенції Ради Європи 1981 року про захист осіб у зв'язку з автоматизованою обробкою персональних даних щодо органів нагляду та транскордонних потоків даних від 08.11.2001 [184].

В правовому полі Європейського Союзу зазначене питання врегульовано у низці нормативно-правових актів. Наприклад, в Регламенті №679 [19] уведені критерії для легітимізації обробки даних, розширені випадки обмеження права на захист персональних даних, передбачено утворення наглядових органів тощо. Низка важливих принципів у сфері захисту персональних даних визначені у Директиві 2002/58/ЄС про обробку персональних даних та захист таємниці сектора електронних комунікацій (Директива про секретність та електронні комунікації) [185]. У вказаному документі, зокрема, закріплений принцип конфіденційності (ст. 15), який забороняє прослуховування, перехоплення, зберігання та інші види втручання або спостереження з боку третіх осіб без згоди з боку зацікавленої особи. Водночас, вказане правило передбачає й виключення, яке розповсюджується на випадки захисту національної безпеки, публічного порядку і т.д.

Крім цього, Рішенням Ради Європейського Союзу 2008/633/JHA [186, с. 173] передбачений консультаційний доступ до Візової інформаційної системи уповноваженими посадовими особами

держав-членів Європолу, з метою запобігання, виявлення та розслідування терористичних дій та інших тяжких злочинів.

Не зважаючи на те, що наразі Україна фактично обмежила свою участь у роботі Співдружності Незалежних Держав «до критично необхідного мінімуму» [187], а постійне представництво нашої держави при координаційних інститутах Співдружності було закрито ще у серпні 2018 року, вважаємо за необхідне проаналізувати міжнародно-правові акти СНД щодо захисту конфіденційної інформації, з огляду на деякі особливості їх змістовного наповнення.

Так, для СНД правове регулювання питань, пов'язаних із захистом персональних даних сконцентровані у положеннях модельного закону країн СНД «Про персональні дані», прийнятому на чотирнадцятому пленарному засіданні Міжпарламентської асамблеї країн-учасниць СНД від 16 жовтня 1999 року [188].

На відміну від інших міжнародно-правових документів з окресленого питання, вказаний законодавчий акт доволі докладно розкриває правовий режим персональних даних (ст. 4), визначає основні форми державного регулювання дій отримувачів персональних даних, а саме: ліцензування діяльності щодо використання персональних даних, реєстрація баз персональних даних, реєстрація отримувачів персональних даних, сертифікація інформаційних систем, спрямованих на оброблення персональних даних (ст. 5), пропонує порядок утворення органів, діяльність яких доповнює існуючі можливості захисту прав суб'єктів персональних даних (ст. 16), визначає права суб'єктів персональних даних, права та обов'язки отримувачів персональних даних (ст. 12, 13), визначає ряд інших правил та процедур у сфері захисту персональних даних.

Цікаво й те, що тільки у п'ятьох країнах СНД на законодавчому рівні проведено роботу щодо розроблення та прийняття базових законодавчих актів у сфері правового регулювання персональних даних (РФ, Молдова, Вірменія, Україна, Азербайджан). Законодавчими органами вказаних країн розроблені та прийняті спеціальні закони, спрямовані на захист персональних даних.

Таким чином, аналіз вищеперерахованих міжнародних нормативно-правових актів у сфері захисту персональних даних дозволяє

визначити основні загальні тенденції та проблеми, які виникають в процесі організації інформаційно-аналітичної діяльності правоохоронних органів. При цьому, один з ключових аспектів цієї діяльності полягає у підвищеній увазі з боку фахівців до проблеми захисту персональних даних. Можемо погодитися із думкою тих фахівців, які стверджують, що персоніфікований характер окремих видів інформації, а також використання для їх отримання методів, пов'язаних із втручанням у приватне життя громадян, надають особливого значення використанню механізмів контролю та нагляду в службовій діяльності поліції та забезпеченню інформаційної безпеки під час їх реалізації [116; 189; 190; 191; 192].

Дійсно, бурхливий розвиток інформаційних технологій призвів до появи актуальної необхідності захисту персональних даних. Саме з цієї причини у наведених вище міжнародних нормативно-правових актах особливу увагу приділено правовому врегулюванню розуміння персональних даних та принципів поводження із персоніфікованою інформацією, в тому числі, в діяльності правоохоронних органів.

Так, відповідно до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних [69], персональні дані визначені як будь-яка інформація про особу, яка персоніфікована або може бути персоніфікована. Автоматизована обробка персональних даних, відповідно до вказаного документу, передбачає дотримання певних правил, а саме: а) персональні дані збираються та обробляються на справедливих та законних підставах; б) зберігаються для чітко визначених та законних цілей та не використовуються у будь-який інший спосіб, несумісний із визначеними цілями; в) персональні дані є адекватними, такими, що безпосередньо стосуються справи, співмірними з цілями їхнього зберігання, точними та оновлюваними; г) зберігаються у формі, яка дозволяє ідентифікувати суб'єктів персональних даних не довше, ніж це вимагають цілі зберігання таких даних.

Персональні дані, які стосуються расової приналежності , політичних поглядів або релігійних чи інших переконань, а також здоров'я чи статевого життя не можуть підлягати автоматизованій

обробці, якщо в законодавстві не встановлені спеціальні гарантії захисту такої інформації. Зазначені положення також розповсюджуються на випадки, пов'язані із судимістю особи. Використання особистих даних здійснюється тільки за наявності згоди з боку суб'єкта таких даних. При цьому, допускається відхилення від окреслених вище правил у випадку, коли подібне відхилення передбачене законодавством конкретної держави та виступає в ролі необхідного заходу, загальновизнаного у демократичному суспільстві й установленого в інтересах: а) забезпечення державної та публічної безпеки, кредитно-валютних інтересів держави або припинення кримінальних правопорушень; б) захисту суб'єктів персональних даних та/або прав і свобод інших осіб. Практика реалізації вказаного конвенційного положення у різних країнах яскраво демонструє усталену практику щодо можливості відхилення від прописаних у коментованій Конвенції гарантій, якщо це необхідно для припинення злочинів та протидії злочинності.

Класифікація обмежень щодо рівнів обігу інформації на міжнародному рівні можна об'єднати терміном «прихована інформація». На таких відомостях конфіденційного характеру як правило проставляється позначення рівня секретності. У зв'язку із наявними відмінностями позначень та грифів секретності, які використовуються у різних країнах, в поліцейських, урядових та військових організаціях, що діють на міжнародній основі (Інтерпол, НАТО), у практику правоохоронної діяльності запроваджені так звані «таблиці відповідності» із позначенням найменувань усіх рівнів секретності та розшифруванням кожного терміну, наприклад «restricted» (для службового користування), «confidential» (конфіденційно), «secret» (таємно) и «top secret» (цілком таємно) і т. д. [193]. Якщо інформація з обмеженим доступом позначена одним із визначених способів, використання даних визначається спеціальними обмеженнями, а доступ до них можуть отримати тільки особи із відповідним рівнем допуску.

Слід зазначити, що спеціальні обмеження відносно роботи з інформацією обмеженого доступу можуть розповсюджуватися не лише на осіб, які наділені правом отримання такої інформації, але

й умов її отримання, носіїв, способів передачі та порядку її знищення. Також існують варіанти, коли за внутрішнім законодавством щодо діяльності правоохоронних органів, інформація, що знаходиться в їх розпорядженні або зібрана ними, автоматично вважається закритою, не зважаючи на те, що її зміст по суті не є конфіденційним.

Аналіз прийнятих внутрішньодержавних законодавчих актів у сфері захисту персональних даних дозволяє зробити висновок, що всі вони, як правило, передбачають утворення офіційного незалежного наглядового органу, уповноваженого на розгляд звернень у визначеній сфері державного управління та уповноважений на проведення перевірок й надання обов'язкових до виконання вказівок щодо поводження з особистими даними.

Наприклад, в республіці Молдова в якості такого органу виступає Національний центр із захисту персональних даних Республіки Молдова. У ФРН вказаними повноваженнями наділена Федеральна комісія із захисту персональних даних, яка призначає комісарів із захисту персональних даних у всіх федеральних землях.

Комісар із захисту персональної інформації в Канаді є посадовою особою із спеціальними повноваженнями, яка призначається парламентом та відповідає перед ним. Комісаріат із захисту інформації у Великій Британії виступає в ролі незалежного агентства, призначення якого полягає у дотриманні законодавства у сфері захисту персональних даних. Аналогічні функції виконує й Національна комісія з інформатики та свобод у Франції [193].

Аналіз європейської судової практики дає підстави для висновку, що суб'єкти персональних даних наділені правом на судовий захист, за умови неналежного використання своїх особистих даних володільцями та розпорядниками цієї інформації. На міжнародному рівні вказане право реалізується шляхом звернення суб'єкта персональних даних до Європейського суду з прав людини (скорочено – ЄСПЛ).

Вивчення судової практики ЄСПЛ щодо захисту персональних даних суб'єктів від незаконного втручання з боку правоохоронних органів, опублікованої Секретаріатом цієї судової установи, свідчить про намагання ЄСПЛ знайти баланс між приватними інтересами

кожної особи та публічними інтересами, які виступають об'єктом право охорони. Позиція суду в даному випадку полягає в тому, що держави не можуть здійснювати будь-які заходи, мета яких полягає у протидії тероризму та шпіонажу. Саме з цієї причини, у тих випадках, коли використання персональних даних правоохоронними органами було незаконним, ЄСПЛ приймав рішення на користь заявників та відмовляв у визнанні порушеного права, якщо правоохоронні органи будь-якої країни діяли в рамках закону, маючи на меті забезпечення публічного порядку та державної безпеки.

Наступне, не менш важливе питання, пов'язане із здійсненням інформаційно-аналітичної діяльності у правоохоронних органах полягає у кадровому забезпеченні правоохоронних органів фахівцями відповідного напрямку роботи. Ефективна практика оцінювання значення інформації, надійності джерел її отримання, її сумісності з іншими відомостями здійснюється аналітиками.

Вивчення організації аналітичної роботи в Національній поліції свідчить про наявність двох її ключових напрямків, а саме: а) стратегічний аналіз, який розрахований на довгострокову перспективу та спрямований на забезпечення більш детального аналізу та б) тактичний аналіз, безпосередньо пов'язаний із вирішенням оперативних завдань. Стратегічна інформація спрямована на виявлення загроз та джерел їхнього походження. Разом з цим, тактична інформація відображає конкретну ситуацію або поточну операцію, часто в режимі реального часу.

Слід зазначити, що якісно проведений аналіз дозволяє аналітику зробити висновок у контексті всього обсягу інформації, передбачити подальший розвиток подій та сформулювати рекомендації щодо покращення оперативної обстановки.

У зв'язку із специфічним характером та важливістю інформації, яка підлягає обробці в інформаційно-аналітичних системах, вимоги до фахової підготовки працівників підрозділів інформаційно-аналітичної підтримки мають якісно відрізнятися від професійної підготовки працівників інших підрозділів Національної поліції.

Якості, необхідні для керівників підрозділів інформаційно-аналітичної підтримки доволі повно сформулював В. В. Сокуренко,

мотивуючи це тим, що саме від керівника аналітичного підрозділу залежать професійність та ефективність інформаційно-аналітичної діяльності. Таким чином, вчений виокремлює:

- загальну професійну майстерність, тобто набір якостей, які необхідні відповідно до кваліфікаційних вимог;
- ініціативність у прийнятті управлінського рішення;
- організованість;
- готовність нести відповідальність за свої вчинки;
- пунктуальність не лише під час інформаційно-аналітичної діяльності, а й у повсякденній діяльності;
- проінформованість;
- уміння зберігати службову таємницю;
- гарну пам'ять;
- уміння адаптуватися [194, с. 225].

Загалом погоджуємось із висловленою позицією автора та мусимо констатувати, що на теперішній час в системі професійної підготовки не сформовані ефективні програми навчання за напрямками службової діяльності органів та підрозділів Національної поліції. Крім того, з дореформених часів залишилась проблема ефективного розподілу випускників, відповідно до напрямків їхньої підготовки. Тому й дотепер мають місце випадки, коли випускники курсів початкової підготовки за напрямком підготовки дільничних офіцерів поліції, влаштовуються для подальшого проходження служби до підрозділів, діяльність яких лише опосередковано пов'язана із знаннями, здобутими випускником під час проходження курсів початкової підготовки.

Також не останнє місце серед актуальних проблем інформаційно-аналітичної діяльності підрозділів поліції іноземних країн у сфері захисту персональних даних посідають питання організації взаємодії між підрозділами поліції та обмін відповідною інформацією.

Обмін інформацію між правоохоронними відомствами різних країни – це, по суті, інший бік організації інформаційно-аналітичної діяльності, яка має взаємовигідний характер. Правові аспекти обміну інформацією між правоохоронними органами зарубіжних країн знайшли відображення у Рекомендації Комітету міністрів

Ради Європи № R(87)15 1987 року про використання персональних даних у секторі поліції [183].

Зокрема, стаття 5.1. вказаного міжнародно-правового акту визначає правило, відповідно до якого передача даних між поліцейськими органами для надання допомоги в процесі досягнення цілей поліції дозволяється виключно у випадках, якщо існує правомірний інтерес щодо передачі такої інформації, у межах повноважень вказаних органів. При цьому, передача даних іншим публічним закладам або приватним особам дозволяється тільки в особливих випадках, до яких відносяться: наявність відповідного дозволу на передачу інформації, необхідність отримання таких даних для цілей здійснення отримувачем своїх законних обов'язків, впевненість у тому, що передача інформації є необхідною умовою для припинення серйозної та неминучої небезпеки.

Відносно міжнародного обміну інформацією Рекомендація встановлює заборону для органів поліції на передачу даних зарубіжним органам (ст. 5.4). Такий обмін можливий лише за умови наявності національних або міжнародних норм з цього питання або у випадках, коли передача інформації є необхідною для запобігання серйозній та неминучій небезпеці або для запобігання серйозного кримінального правопорушення, відповідно до норм загального права, за умови не порушення національного законодавства із захисту людини.

Достатньо високий рівень організації взаємодії між поліцейськими відомствами, в частині передачі конфіденційної інформації, спостерігається на прикладі Італії. Зокрема, в МВС Італії функціонує Центр щодо оброблення оперативної інформації, головним завданням якого є обмін отриманою інформацією відносно діяльності мафіозних груп із службою Верховного комісара по боротьбі з мафією, Корпусом карабінерів, Фінансовою гвардією, місцями позбавлення волі, де утримуються представники мафіозних структур, а також із центрами координації та планування оперативної діяльності підрозділів МВС, розташованих у 12 найбільших містах Італії.

Крім цього, Центр з вивчення обстановки, який є найбільшим оперативно-технічним підрозділом МВС Італії, здійснює оперативно-службову діяльність, в тому числі із застосуванням

оперативно-технічних засобів, із збору оперативної інформації про стан організованої злочинності та її передачу до оперативних підрозділів міністерства. Вказаний підрозділ поліції підтримує постійні зв'язки щодо захисту персональних даних з розташованими в Італії представництвами ФБР, Управління по боротьбі з наркотиками та Митного управління США, а також з аналогічними підрозділами Європейського Союзу, з метою забезпечення чіткого та оперативного обміну конфіденційною інформацією.

Таким чином, можемо констатувати, що заборона передачі персональних даних, відповідно до норм міжнародно-правових актів, не має абсолютного характеру. Уявляється, що вказаний факт передовсім пов'язаний із необхідністю активної протидії правоохоронних органів кримінальним правопорушенням, терористичним актам, шпигунству тощо. Останнім необхідні більш широкі повноваження для проведення оперативно-технічних заходів як усередині країни, так і з метою контролю за міжнародним комунікаційним простором.

Слід зазначити, що спрощення процесів контролю за телекомунікаційними мережами також активно підтримується низкою міжнародних організації та приватних осіб. Загальновідомо, що Сполучені штати Америки, виступаючи в ролі монополіста з питань контролю за світовим телекомунікаційним простором, не тільки відмовляються передавати функції з контролю за мережею Інтернет до компетенції міжнародних організації, зокрема, ООН, але й активно сприяють створенню можливостей технічного доступу до всіх телекомунікаційних технологій. Більше того, Сполучені штати виступають активними ініціаторами в міжнародних організаціях, таких як ОЕСР, РЄ і т.д., щодо запровадження спрощеного контролю за інформаційними та телекомунікаційними системами.

Багато в чому таке спрямування розвитку законодавства про захист персональних даних в США обумовлено подіями 2001 року, коли ця країна стала об'єктом катастрофічних терористичних атак. Наслідком цих подій виявилося прийняття низки законодавчих актів, чільне місце серед яких посідає Акт «Про згуртування та зміцнення Америки, шляхом забезпечення належними засобами, необхідними для припинення та перешкоджання тероризму» [195].

Слід зазначити, що вказаний правовий акт найсерйознішим чином зачіпав право на недоторканність приватного життя. Термін «privacy», який уособлює усі аспекти особистого життя людини, уперше запроваджено у рішенні Верховного Суду США у справі «Griswoldv. Connecticut» у 1965 році. Зауважимо, що в США процедури оформлення дозволів на здійснення електронного спостереження, яке, в тому числі, передбачає й прослуховування телефонних переговорів, відрізняються в залежності від того, ким є суб'єкт контролю – громадянином США або іноземцем.

Контроль приватного життя іноземців здійснюється відповідно до Закону 1978 року «Про спостереження за діяльністю іноземних розвідувальних служб в США». Відмітимо, що правом видачі дозволу на здійснення електронного спостереження володіє Президент країни, а не судові органи, але вказане правило розповсюджується тільки на громадян інших країн [196]. Разом з цим, порядок електронного спостереження за громадянами США у деякій мірі юридично перевантажений та піддавався неодноразовому коректуванню після прийняття значимих рішень Верховного Суду США, таких як: «Bergerv. NewYork» (1967), «Katzv. UnitedStates» (1967), «Silvermanv. UnitedStates» (1967) та ін. Але й при цьому дозвіл нна проведення електронного спостереження, у разі настання загрози національній безпеці, видавався виключно спеціалізованим судом.

Відмітимо, що Акт про патріотизм запровадив кардинальні зміни до порядку отримання рішення на здійснення електронного спостереження, а саме: спрощено процедуру видачі ордеру на прослуховування так званих «кочуючих розмов», критерієм яких виступає прив'язка не до конкретного телефонного номеру, а відносно суб'єкта контролю, який потенційно може спілкуватися з різних номерів; розширено компетенцію спецслужб щодо спостереження за мережею Інтернет, в частині відстеження правоохоронними органами сайтів, в тому числі, з можливостями електронної переписки, без отримання судового ордеру; процедура контролю за абонентами телефонних переговорів без отримання судового ордеру поширена на здійснення контролю за обміном повідомлень, які надходять електронною поштою; розширено юрисдикцію суду, уповноваженого

видавати ордери на електронне спостереження. Крім того, Акт про патріотизм визначив додаткові обов'язки операторів зв'язку та Інтернет-провайдерів щодо надання інформації за запитами ФБР про власних абонентів.

Фактично Акт про патріотизм утворив правову основу для ефективної реалізації прийнятої раніше програми Федерального бюро розслідувань щодо тотального стеження за допомогою автоматичної системи шпіонажу «Carnivore», за допомогою якої здійснювалося виявлення та відстеження інформації з Інтернет-сторінок та серверів електронної пошти.

Підбиваючи проміжні підсумки, можемо констатувати, що: а) на теперішній час в США спостерігається запровадження безпрецедентних тотальних заходів контролю з боку правоохоронних органів за обігом персональних даних. Така тенденція стала наслідком значного розширення повноважень правоохоронних органів у сфері використання конфіденційної інформації; б) змінилась концепція обмежень права на недоторканність приватного життя. Рішення суду про можливість доступу до персональних даних поступово замінюється на автоматичну архівацію електронних даних, а видача ордеру – як формального вираження рішення судового органу, здійснюється за фактом доступу до вже отриманої інформації; в) спостерігається суттєве звуження контролю за володільцями та розпорядниками персональних даних, в особі яких виступають правоохоронні органи, тому відстежити факт ознайомлення з персоніфікованою інформацією без відповідного рішення практично неможливо; г) розширення повноважень щодо контролю за персональними даними розповсюджується не тільки на громадян США, але й на іноземців та осіб без громадянства, тобто має тотальний характер.

Аналіз європейського законодавства з питань захисту персональних даних говорить про те, що загальноприйняті міжнародні правові норми, які визначають право людини на недоторканність приватного життя, в цілому відображені у Регламенті №679 та дозволяють правоохоронним органам здійснювати заходи щодо контролю за телефонними переговорами та телекомунікаційними каналами зв'язку, але тільки в суворо обмежених випадках,

розширені підстави щодо застосування яких наведені у низці правових актів (головним чином, у разі підозри у вчиненні кримінальних правопорушень). У більшості європейських країн перехоплення інформації, яка надходить інформаційно-телекомунікаційними каналами, входить до повноважень правоохоронних органів, але тільки за рішенням суду або іншого уповноваженого органу. Також у переважній більшості випадків на законодавчому рівні встановлені вимоги щодо надання інформації з боку правоохоронного органу про попереднє використання всього комплексу слідчих заходів, які, однак, не дали бажаного результату.

Слід зазначити, що недоторканність переписки людини в міжнародному праві уперше була уперше знаходить відображення в Загальній декларації прав людини. Зокрема, стаття 12 вказаного документу визначає заборону «безпідставного втручання у особисте і сімейне життя осіб, безпідставного посягання на недоторканність житла, тайну кореспонденції або на честь і репутацію. Кожна людина має право на захист закону від такого втручання або таких посягань» [11].

У той же час, відповідно до норм переважної більшості міжнародних нормативно-правових актів, право на повагу до особистого та сімейного життя, а також право на таємницю кореспонденції не розглядаються в якості абсолютних прав людини. Так, вже згадана стаття 12 Загальної декларації прав людини застерігає від безпідставного втручання до особистих прав людини, імовірно протиставляючи його втручанню за законом.

У більш чіткому вигляді формулювання вказаного права визначено у Конвенції про захист прав людини і основоположних свобод. Зокрема, стаття 8(2) передбачає заборону втручання державних органів у здійснення особистих прав, за виключенням випадків «коли це передбачено законом та необхідно у демократичному суспільстві в інтересах державної безпеки, громадського порядку або економічного благоустрою держави, для підтримання порядку та запобігання злочинам, захисту здоров'я і моралі або захисту прав і свобод інших осіб» [12].

Не зважаючи на те, що норми початкової редакції Загальної декларації прав людини розповсюджувались суто на телефонні

переговори, телеграфні відправлення та поштову переписку, у 1988 році Верховний Комісар ООН з прав людини підтвердив розповсюдження захисту прав людини у сфері таємниці зв'язку на всі види комунікацій. «Вимога статті 17 Загальної декларації прав людини вимагає фактичного та юридичного дотримання цілісності та конфіденційності інформації. Будь-яка кореспонденція в не перехопленому вигляді повинна бути доставлена адресату. Заборона також розповсюджується на електронне та будь-яке інше стеження, перехоплення телефонних, телеграфних та інших видів зв'язку, прослуховування та запис на плівку розмов тощо» [197].

Питання доступу правоохоронних органів до інформації, що передається по відкритим телекомунікаційним системам також врегульовані не менш важливим міжнародно-правовим документом – Конвенцією про кіберзлочинність [198]. Вказаний документ рекомендує уніфікувати кримінальне законодавство, в частині вирішення питань, що стосуються комп'ютерних правопорушень та передбачити кримінальну відповідальність за правопорушення, пов'язані із незаконним доступом, а саме: а) доступ до інформації без відповідної санкції або з порушенням порядку її отримання; б) нелегальне перехоплення інформації технічними засобами або перехопленням комп'ютерного випромінювання.

Разом з цим, вказана Конвенція стала черговим міжнародним документом, положення якого прямо легалізують право втручання правоохоронних органів у приватне життя осіб, шляхом доступу до персональних даних. Зокрема, правові норми Конвенції про кіберзлочинність вказують на необхідність прийняття заходів «законодавчого та іншого характеру відносно ряду серйозних злочинів, визначених відповідно до національного законодавства, які дозволили б компетентним органам збирати та записувати в режимі реального часу змістовні дані визначених передач інформації, шляхом застосування технічних засобів на території цієї країни та змушувати постачальника послуг у межах наданих йому технічних можливостей сприяти реалізації зазначених заходів» [198]. Важливо й те, що в даному випадку йдеться про правомірність збору особистих даних у межах території держави, що в принципі виключає

можливість отримання конфіденційної інформації правоохоронними органами з відкритих телекомунікаційних систем за межами країни. При цьому, відповідно до п. 3 ст. 21 Конвенції передбачено вимогу збереження таємниці факту виконання будь-якого з вищевикладених повноважень, з боку постачальника послуг.

Таким чином, європейським міжнародним законодавством фактично окреслені межі легітимації контролю правоохоронних органів за телекомунікаційними мережами.

Загальне уявлення щодо меж правомірного втручання правоохоронних органів в особисте життя громадян, шляхом використання персональних даних, складається й під час аналізу інших, не менш важливих, міжнародних документів. Зокрема, в Європейському Союзі за різних часів було прийнято декілька нормативних актів, які врегульовують питання доступу правоохоронних органів до конфіденційної інформації, що передається по відкритим телекомунікаційним системам.

Так, Директива 97/66/ЄС Європейського Парламенту і Ради «Стосовно обробки персональних даних і захисту права на невтручання в особисте життя в телекомунікаційному секторі від 15.12.1997, містить положення, визначене у статті 5 цього документу, відповідно до якого «країни-члени зобов'язані на основі національних законів забезпечити конфіденційність комунікацій...Зокрема, вони повинні встановлювати заборону щодо прослуховування, підслуховування, записування та інші види перехоплень або контролю над комунікаціями будь-якими іншими особами, окрім користувачів, без згоди останніх, окрім тих випадків, коли це юридично дозволено, відповідно до статті 14(1)» [199].

Відповідно до останньої статті, питання щодо визначення механізму надання доступу до подібної інформації повинно вирішуватися згідно норм національного законодавства.

Також, найважливішим документом, який прямо врегульовує питання доступу правоохоронних органів до відкритих телекомунікаційних систем у державах-членах ЄС, є Резолюція Ради ЄС (96/С 329/01) про законне перехоплення телекомунікацій від 17 січня 1995 року [200]. На перший погляд викликає здивування

відсутність у даному документі чітко визначених підстав доступу правоохоронних органів до перехоплення конфіденційної інформації, але в той же час, стаття 1 коментованого документу фактично формулює мету цієї Резолюції, яка полягає у потребі компетентних органів у технічній реалізації, здійснюваного на законних підставах, перехоплення персональних даних у сучасних телекомунікаційних системах.

Уявляється, що вказаний документ, прийняття якого скоріше за все пов'язане із активним сприянням правоохоронних органів європейських країн, визначає вимоги до технічних аспектів перехоплення інформації та вимагає від операторів телекомунікаційних мереж надання правоохоронним органам доволі широких повноважень, врегульованих нормами національного законодавства, щодо контролю над телекомунікаційними мережами.

Таким чином, проведений аналіз міжнародного досвіду захисту персональних даних правоохоронними органами обумовлює існування ряду правових проблем, вирішення яких необхідно здійснювати як на рівні міжнародної взаємодії, шляхом вироблення узгодженої позиції щодо юридично значимих питань правового забезпечення глобальних інформаційних процесів, так й на національному рівні, шляхом розробки відповідного галузевого законодавства та імплементації норм міжнародного права у сфері захисту персональних даних. Йдеться передовсім про ефективне застосування в національному законодавстві норм Регламенту №679, яким відмінено Директиву №95/46, а остання, своєю чергою, виступила основою для прийняття Закону України «Про захист персональних даних».

3.2. Правові засади доступу уповноважених підрозділів Національної поліції до персональних даних в телекомунікаційних мережах

Сьогодні інформаційні технології охоплюють практично всі сфери суспільного життя, відтак, значні обсяги інформації

у телекомунікаційних мережах потребують забезпечення її надійного захисту.

Тому на ґрунті стрімкого розвитку глобального інформаційного суспільства, інформаційних та телекомунікаційних технологій наразі спостерігаються кардинальні трансформаційні процеси у сфері захисту інформації, що не може не позначатися на діяльності Національної поліції в процесі доступу до інформаційних ресурсів, які містять персональні дані. Нерідкими є випадки несанкціонованого розповсюдження персональних даних, що не тільки спричиняє збитки численним вітчизняним та міжнародним організаціям, але й порушує права громадян на недоторканність приватного життя, особисту та сімейну таємницю.

Забезпечення Національною поліцією захисту громадян від злочинних посягань, ефективне розкриття та розслідування вчинених правопорушень за сучасних умов неможливе без використання інформації, значна концентрація якої фокусується у мережах телекомунікаційного зв'язку. Разом з цим, діяльність органів та підрозділів Національної поліції в цьому напрямку обмежується положеннями статті 31 Конституції України, яка гарантує кожній особі таємницю листування, телефонних розмов, телеграфної та іншої кореспонденції. При цьому, винятки можуть бути встановлені лише судом у випадках, передбачених законом, з метою запобігти злочинові чи з'ясувати істину під час розслідування кримінальної справи, якщо іншими способами одержати інформацію неможливо [57].

У цьому контексті постає запитання щодо обсягу інформації, яка знаходиться у розпорядженні операторів зв'язку та має значення для попередження та розкриття правопорушень. Чи в повному обсязі потрапляє вона у сферу дії вищенаведеної конституційної норми або якусь її частку окреслені положення основного закону країни не зачіпають.

В міжнародному законодавстві відповідь на це запитання можна знайти у Регламенті №679, який визначає підстави для обмеження спеціальних принципів та прав на інформацію, а також доступу до персональних даних правоохоронних органів, в якості яких виступають: а) гарантування громадської безпеки, в тому числі захист

життя людини, особливо у відповідь на стихійні лиха і антропогенні катастрофи; б) запобігання, розслідування і переслідування осіб за скоєння кримінальних злочинів або виконання кримінальних покарань, у тому числі захист від загроз громадській безпеці та запобігання їм, в) порушення етичних норм для регульованих професій; г) важливий економічний або фінансовий інтерес Союзу або держави-члена; д) ведення публічних реєстрів на підставі загального суспільного інтересу; е) подальше опрацювання архівних персональних даних для надання конкретної інформації, що стосується політичної поведінки під колишніми тоталітарними державними режимами; є) захист суб'єктів даних або прав і свобод інших, у тому числі соціальний захист, охорона здоров'я населення або гуманітарні цілі [19].

У національному законодавстві однозначної відповіді на запитання щодо меж доступу правоохоронних органів й, зокрема, Національної поліції, до персональних даних, що містяться в мережах телекомунікаційного зв'язку, немає. Вчені та практики притримуються різних позицій щодо необхідності судового дозволу на отримання, наприклад, персональних даних абонентів мережевого зв'язку, відомостей про IMEI-номери мобільних телефонів, інформації про з'єднання невизначеного кола абонентів в межах конкретно визначеної території тощо.

У загальному вигляді ключовим аспектом триваючої й дотепер дискусії залишається дотримання розумного балансу між дотриманням прав громадян на невтручання у їх особисте життя, в частині доступу до їх персональних даних, а з іншого – законна діяльність правоохоронних органів щодо забезпечення публічного порядку та державної безпеки. Т. Обуховська з цього приводу зазначає про необхідність поєднання принципу недоторканності особи із принципом недоторканності власності. Тобто, на думку вченої, «особливої уваги потребує проблема врегулювання балансу інтересів сторін: особистості, суспільства і держави, на основі механізму взаємоврахування інтересів [201, с. 101].

Стосовно першого аспекту слід зазначити, що ефективна організація процесу надання телекомунікаційних послуг виступає

надійною гарантією реалізації громадянами права на приватність, в тому числі, й у сфері захисту персональних даних [202, с. 90]. Разом з цим, один із суттєвих проявів безпосереднього втручання у особисте та сімейне життя громадян дійсно пов'язаний із діяльністю органів та підрозділів Національної поліції, в процесі зняття інформації з телекомунікаційних мереж зв'язку.

У національному законодавстві право на таємницю особистого та сімейного життя врегульовано низкою законодавчих актів, першорядне місце серед яких посідає Конституція України, стаття 32 якої передбачає заборону втручання у особисте та сімейне життя осіб, за винятком випадків, передбачених Конституцією України. Частина 2 коментованої статті також містить заборону обігу конфіденційної інформації про особу без її згоди, однак, передбачає й певні виключення із цього правила, а саме: а) підстави, визначені законом; б) інтереси національної безпеки, економічного добробуту та прав людини [57].

Низку основоположних правил щодо забезпечення захисту особистого життя від свавільного втручання містить й Цивільний кодекс України, стаття 301 якого прямо передбачає право фізичної особи на особисте життя. Доволі чіткою та справедливою є позиція законодавця, висловлена у частині 2 цієї статті, яка пов'язана із власним визначенням фізичної особи кола та меж свого особистого життя та можливості ознайомлення з ним інших осіб [166]. Також із змісту статті 306 ЦК України можемо зробити висновок, що правовою категорією «кореспонденція» охоплюються не тільки листи та будь-які письмові документи, але й всі інші матеріальні та віртуальні носії інформації, а саме: телеграми, телефонні розмови, телеграфні повідомлення та інші види кореспонденції. Така позиція підтверджується й переважною більшістю науковців, які вкладають у термін «кореспонденція» такі її різновиди, як: телефонні розмови, телеграфні повідомлення, повідомлення електронною поштою, пейджером, SMS-повідомлення тощо [203, с. 472–473].

Охорона права громадян на втручання у їх особисте життя на законодавчому рівні визначена Кримінальним кодексом України, стаття 163 якого передбачає відповідальність за порушення таємниці

листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер [162].

Слід зазначити, що механізм забезпечення права громадян, передбаченого статтею 31 Конституції України розкривається у низці законодавчих актів, пріоритетне значення серед яких посідають Закон України «Про телекомунікації» [204] та Закон України «Про поштовий зв'язок» [205].

Так, стаття 9 Закону України «Про телекомунікації» містить положення, відповідно до якого держава гарантує забезпечення охорони таємниці та безпеку телекомунікаційних мереж під час передачі інформації технічними засобами телекомунікацій, а саме: а) в процесі телефонних розмов; б) під час відправлення телеграфної чи іншої кореспонденції [204]. Крім того, у частині 2 коментованої статті законодавець підкреслив заборону зняття інформації з телекомунікаційних мереж, крім випадків, передбачених законом.

Аналогічні вимоги до розповсюдження персоніфікованої інформації містяться у Законі України «Про поштовий зв'язок» передбачає конституційні гарантії таємниці поштових відправлень, у тому числі листування та іншої письмової кореспонденції, електронних повідомлень, що пересилаються (передаються) засобами зв'язку [205]. Виїмка та огляд письмової кореспонденції, вкладень в інших поштових відправленнях, одержання будь-яких довідок щодо них заборонено, крім випадків, визначених законом.

Таким чином, аналіз вищенаведених законодавчих актів надав змогу висловити з цього приводу певні міркування.

1. Слід констатувати доволі значний масив законодавчих актів, які визначають, на перший погляд, досконалий механізм забезпечення захисту особистої інформації громадян від втручання правоохоронних органів.

2. Складається доволі парадоксальна ситуація, коли законодавець на конституційному та законодавчому рівні намагається доволі ретельно захистити особисту таємницю, не визначаючи при цьому її зміст. Наприклад, за результатами аналізу конституційних норм доходимо висновку, що всі врегульовані національним законодавством таємниці можна розділити на: а) державні; б) особисті;

в) інші, під якими, вірогідно, розуміються таємниці за сферами соціально-економічних відносин, а саме: банківська, лікарська, адвокатська та ін.

3. У той же час, на відміну від особистої, розуміння державної таємниці доволі повно розкрито в Законі України «Про державну таємницю», стаття 1 якого визначає останню як «вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані у порядку, встановленому цим Законом, державною таємницею і підлягають охороні державою» [206]. Тобто державна таємниця представлена у вигляді сукупності відомостей у різних сферах державного управління, які функціонують в режимі таємної інформації.

4. Разом з цим, сукупність відомостей, які утворюють поняття особистої таємниці в жодному з проаналізованих законодавчих актів не визначено. Наприклад, якщо вважати, що зміст особистої таємниці складатиме таємниця листування, телефонних розмов, телеграфної та іншої кореспонденції, то як визначити правовий режим захисту персональних даних, які містяться в мережі Інтернет, а саме: в хмарних сервісах, соціальних мережах, Інтернет-магазинах тощо. Уявляється, що вказана персоніфікована інформація також буде складати зміст особистої таємниці.

Тому, вважаємо за доцільне сформулювати визначення особистої таємниці як виду таємної інформації про фізичну особу, яка включає персональні дані цієї особи та іншу персоніфіковану інформацію, яка підлягає охороні державою, а її розголошення може завдати шкоди інтересам фізичної особи. Із наведеного визначення стає зрозумілим, що особиста таємниця включає два різновиди інформації: а) персональні дані; б) інша персоніфікована інформація, яка, на нашу думку, включає персональні дані, функціонування яких врегульоване спеціальними законами України.

З іншого боку, аналіз законодавчих актів у сфері захисту персональних даних дає підстави для висновку про наявність виключень із загального конституційного правила про заборону втручання

у особисте життя громадян. Саме такі виключення й слугують підставою для правомірного втручання Національної поліції у приватне життя громадян, шляхом доступу до їх персональних даних в телекомунікаційних мережах.

Слід зазначити, що порядок доступу до персональних даних, які містяться у телекомунікаційних мережах врегульований низкою законодавчих та підзаконних актів [44; 128;204; 207; 208; 209; 210].

Зокрема, Кримінальний процесуальний кодекс України доволі докладно врегульовує порядок втручання у приватне спілкування громадян, різновидами якого, відповідно до статті 258 КПК, є: 1) аудіо-, відеоконтроль особи; 2) арешт, огляд і виїмка кореспонденції; 3) зняття інформації з транспортних телекомунікаційних мереж; 4) зняття інформації з електронних інформаційних систем [207].

Стаття 263 коментованого законодавчого акту врегульовує процедурні питання щодо зняття інформації з транспортних телекомунікаційних мереж. Так, частина 4 коментованої статті зобов'язує керівників та працівників операторів телекомунікаційного зв'язку сприяти органам Національної поліції та державної безпеки щодо виконання дій із зняття інформації з транспортних телекомунікаційних мереж, вживати необхідних заходів щодо нерозголошення факту проведення таких дій та отриманої інформації, зберігати її в незмінному вигляді.

Уявляється, що в наведеному правовому положенні дискусійним виглядає розуміння сприяння правоохоронним органам та його змістовного наповнення. Відповідь на це запитання також відсутня і в Законі України «Про телекомунікації». Наприклад, відповідно до статті 39 вказаного закону оператори телекомунікацій зобов'язані сприяти в межах своїх повноважень проведенню оперативно-розшукових заходів та недопущенню розголошення організаційних і тактичних прийомів їх проведення [204]. Однак, в чому виражається, власне, процес сприяння, не зрозуміло. Зокрема, чи повинні суб'єкти надання телекомунікаційних послуг надавати будь-яку додаткову персоніфіковану інформацію про своїх клієнтів, і якщо так, то яку саме, та чи повинна здійснюватися передача

такої інформації за рішенням слідчого судді – закон не дає відповіді на такі запитання.

Крім того, в ухвалі слідчого судді про дозвіл на втручання в приватне спілкування в цьому випадку додатково повинні бути зазначені ідентифікаційні ознаки, які дозволять унікально ідентифікувати абонента спостереження, ТТМ, кінцеве обладнання, на якому може здійснюватися втручання у приватне спілкування (ч. 2 ст. 263 КПК України). Такими ознаками можуть бути: номер абонента в телефонній мережі загального користування у форматі «код країни – код зони або оператора – номер абонента в мережі»; міжнародний ідентифікаційний номер мобільного терміналу (IMEI); міжнародний ідентифікаційний номер мобільного абонента (IMBI).

Однак ні Закон України «Про оперативно-розшукову діяльність», надаючи оперативним підрозділам право проводити зняття інформації з каналів зв'язку, ні КПК України, також не містяться норми, що розкривають сутність провадуваних дій [211, с. 37].

Вважаємо, що відповідь на запитання щодо обсягу персональних даних, які можуть надаватися суб'єктами надання телекомунікаційних послуг органам Національної поліції при проведенні оперативно-розшукових заходів, міститься у статті 34 Закону України «Про телекомунікації», відповідно до якої інформація про споживача та про телекомунікаційні послуги, що він отримав, може надаватись у випадках і в порядку, визначених законом. Також частина 2 коментованої статті містить перелік персональних даних, які можуть передаватися правоохоронним органам, а саме: прізвище, ім'я, по батькові абонента, найменування, адреса та номер його телефону.

Підстави та порядок зняття інформації з каналів зв'язку в телекомунікаційних мережах підрозділами Національної поліції, які здійснюють оперативно-розшукову діяльність, також визначено статтею 8 Закону України «Про оперативно-розшукову діяльність».

Відповідно до п. 9 частини 1 цієї статті підрозділи правоохоронних органів, які здійснюють оперативно-розшукову діяльність мають право здійснювати низку негласних заходів, в частині аудіо-, відеоконтролю осіб, зняття інформації з транспортних телекомунікаційних мереж, електронних інформаційних мереж тощо [44]. Вказана

норма має відсильний характер, адже передбачає реалізацію цієї діяльності відповідно до ст.ст. 260, 263–265 Кримінального процесуального кодексу України.

У той же час, частина 3 коментованої статті містить чітко визначений перелік оперативно-розшукових заходів, реалізація яких здійснюється лише на підставі ухвали слідчого судді, постановленої за клопотанням керівника відповідного оперативного підрозділу або його заступника, погодженого з прокурором. До таких заходів, зокрема, відносяться: а) негласне обстеження публічно недоступних місць, житла чи іншого володіння особи; б) аудіо-, відеоконтроль особи; в) аудіо-, відеоконтроль місця; г) спостереження за особою; д) зняття інформації з транспортних телекомунікаційних мереж, електронних інформаційних мереж; е) накладення арешту на кореспонденцію, здійснення її огляду та виїмки; є) установлення місцезнаходження радіоелектронного засобу [44].

Вказане правове положення яскраво демонструє намагання законодавця встановити суворо визначені правові межі діяльності правоохоронних органів у сфері доступу до персональних даних, які містяться у телекомунікаційних мережах. Такий висновок підтверджується й сформульованою метою застосування вищенаведених оперативно-розшукових заходів, які здійснюються, відповідно до тієї ж норми, виключно з метою запобігання вчиненню тяжкого або особливо тяжкого злочину, запобігання і припинення терористичних актів та інших посягань спеціальних служб іноземних держав та організацій, якщо іншим способом одержати інформацію неможливо [44].

Закон України «Про організаційно-правові основи боротьби з організованою злочинністю» також має безпосереднє відношення до організації порядку доступу правоохоронних органів до персональних даних, адже визначає головні напрями загальнодержавної політики та організаційно-правові основи боротьби з організованою злочинністю.

Уявляється, що положення статті 15 коментованого законодавчого акту, надаючи повноваження щодо можливості використання спеціальних технічних засобів виключно підрозділам Служби

безпеки України, мають бути доповнені посиланням також і на відповідні підрозділи Національної поліції. Дійсно, у вказаній статті законодавець наділив тільки підрозділи СБ України правом використовувати спеціальні технічні засоби, з метою втручання у приватне життя громадян, посилаючись на відповідні норми Кримінального процесуального кодексу та Закону України «Про оперативно-розшукову діяльність».

Разом з цим, частина 4 статті 263 КПК України надає право зняття інформації з транспортних телекомунікаційних мереж також й уповноваженим підрозділам Національної поліції. А стаття 8 Закону України «Про оперативно-розшукову діяльність» делегує вказане право усім підрозділам, які провадять оперативно-розшукову діяльність, до яких, безперечно, відноситься й Національна поліція. Тому зміст статті 15 Закону України «Про організаційно-правові основи боротьби з організованою злочинністю» однозначно повинен бути доповнений уповноваженими підрозділами Національної поліції.

Закон України «Про державний захист працівників суду і правоохоронних органів», серед видів спеціальних заходів забезпечення безпеки передбачає використання технічних засобів контролю і прослуховування телефонних та інших переговорів, а також візуальне спостереження, що також можна розцінювати в якості збору персоніфікованої інформації (стаття 5 Закону). Підстави та умови застосування наведених заходів деталізовані у статті 8 коментованого законодавчого акту, яка, зокрема, передбачає, що в разі загрози вчинення насильства або інших протиправних дій щодо осіб, взятих під захист, за письмовими заявами або згодою цих осіб може проводитися прослуховування телефонних та інших переговорів. У ході прослуховування переговорів осіб, взятих під захист, може застосовуватися звукозапис [128]. Аналогічні додаткові підстави доступу до персональних даних осіб, які беруть участь у кримінальному судочинстві викладені у ст.ст. 7, 10 Закону України «Про забезпечення безпеки осіб, які беруть участь у кримінальному судочинстві» [208].

Аналіз вказаних норм дозволяє класифікувати підстави доступу уповноважених підрозділів Національної

поліції до персональних даних на основні та додаткові. Основні підстави визначені Кримінальним процесуальним кодексом України, та передбачають обов'язкову наявність: а) клопотання керівника відповідного оперативного підрозділу Національної поліції або його заступника; б) погодження прокурора; в) ухвали слідчого судді. Разом з цим, існують і додаткові підстави доступу до персональних даних, які, наприклад, в Законах «Про державний захист працівників суду і правоохоронних органів» та «Про забезпечення безпеки осіб, які беруть участь у кримінальному судочинстві» виражені у наявності загрози вчинення насильства або інших протиправних дій щодо осіб, взятих під захист. Крім того, закон вимагає обов'язкової згоди охоронюваних осіб на фактичне втручання уповноважених підрозділів Національної поліції у їх особисте життя або написання ними письмової заяви. Уявляється, що головна особливість застосування основних та додаткових підстав доступу до персональних даних полягає у взаємозалежності цих підстав, жодна з них не застосовується самостійно, а застосування додаткових підстав є процесуальним продовженням щодо застосування основних.

На окрему увагу заслуговують підзаконні нормативно-правові акти щодо зняття персоніфікованої інформації з каналів зв'язку в інформаційно-телекомунікаційних мережах, призначення яких, головним чином, полягає у врегулюванні технічних питань щодо здійснення державної політики з розроблення, виготовлення, реалізації, придбання та застосування спеціальних технічних засобів для зняття інформації з каналів зв'язку. Наприклад, указом Президента України від 13 квітня 2001 року № 256/2001 «Про впорядкування, виготовлення, придбання та застосування технічних засобів для зняття інформації з каналів зв'язку» визначено орган (в особі Служби безпеки України), відповідальний за реалізацію вищевказаного напрямку державної політики [209]. Зазначені заходи державної політики набули практичного втілення у Положенні про порядок розроблення, виготовлення, реалізації та придбання спеціальних технічних засобів для зняття інформації з каналів зв'язку, інших засобів негласного отримання інформації, затвердженому постановою Кабінету Міністрів України від 27 жовтня 2001 року № 1450,

розробленому з метою впорядкування та координації діяльності органів виконавчої влади у цій сфері державного управління [210].

Відповідно до п.3 вказаного Положення, Національна поліція виступає одним з головних суб'єктів, уповноважених на здійснення державного замовлення щодо розроблення, виготовлення та придбання спеціальних технічних засобів, за допомогою яких здійснюється доступ до персоніфікованої інформації.

Про допустимість збору персональних даних без згоди особи у зв'язку із проведенням оперативно-розшукових заходів органами Національної поліції, відповідно до кримінально-процесуального законодавства, законів про національну безпеку, про оперативно-розшукову діяльність, неодноразово наголошувалось у науковій літературі. На думку авторів, вказана процесуальна діяльність повністю відповідає міжнародним нормам в області забезпечення прав людини, які визнають допустимість вимушеного втручання в недоторканність приватного життя в сфері боротьби зі злочинністю і розглядають такі обмеження необхідними в демократичному суспільстві.

Таким чином, ключове питання у сфері доступу правоохоронних органів до персональних даних полягає у необхідності дотримання балансу інтересів особи, суспільства та держави з причини їх дуже частого неспівпадіння. Порушення інтересів одних суб'єктів на користь інших нерідко призводить до серйозних негативних наслідків: збільшення соціальної напруги, нівелювання авторитету державних та правових інститутів, посиленні правового нігілізму.

Слід зазначити, що характерною властивістю права на недоторканність приватного життя і, як наслідок, права на захист персональних даних є його відносність. Зазначений факт підтверджується як міжнародними правовими актами, зокрема, Конвенцією про захист фізичних осіб при автоматизованій обробці персональних даних, так і нормами Конституції.

Також зазначимо, що відповідно до статті 8 Європейської конвенції про захист прав людини і основоположних свобод встановлює право на повагу до приватного і сімейного життя, включаючи заборону на втручання з боку органів державної влади у здійснення

цього права, за винятком випадків, коли втручання здійснюється згідно із законом і є необхідним у демократичному суспільстві в інтересах національної безпеки та громадського порядку, економічного добробуту країни, з метою запобігання заворушенням чи злочинам, для охорони здоров'я або моралі чи з метою захисту прав і свобод інших осіб [12].

Слід зазначити, що Конституція містить ідентичні за змістом норми, які безпосередньо пов'язані із захистом персональних даних. Наприклад, відповідно до статті 32 Основного Закону втручання у особисте та сімейне життя громадян заборонено, крім випадків, передбачених Конституцією. Тобто фактично, положення статті 32 Конституції складають розуміння недоторканності приватного життя.

Разом з цим, з наведених норм Конституції прямо не випливає висновок про необхідність знаходження балансу інтересів особи і суспільства, про що, наприклад, прямо вказано у Європейській конвенції про захист прав людини і основоположних свобод. Однак слід враховувати й те, що Конституція містить норму, згідно з якою права і свободи людини і громадянина можуть бути обмежені Основним Законом тільки в тій мірі, в якій це необхідно «для забезпечення інтересів національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя» (ст.ст. 34,35) [57].

У той же час, наразі спостерігається тенденція щодо усвідомлення захисту персональних даних як самостійного права громадянина, тобто окремо від більш широкого права на повагу до приватного і сімейного життя.

До персональних даних національне законодавство відносить будь-яку інформацію, зокрема, відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована [72], в тому числі його прізвище, ім'я, по батькові, рік, місяць, дату і місце народження, адреса, сімейний, соціальне,

майнове становище, освіту, професію, доходи. Уявляється, що з метою приведення національного законодавства про захист персональних даних у відповідність до норм міжнародного права, в Законі України «Про захист персональних даних» доцільно врахувати положення про неможливість обмеження переліку персональних даних суто визначеними в законі даними, адже вказані відомості можуть включати будь-яку іншу інформацію, що дозволяє ідентифікувати особу.

Відносно персональних даних встановлено режим конфіденційності, виключення з якого містяться як в Законі України «Про захист персональних даних», так й в інших законах України у сфері захисту персональних даних. Відтак, оброблення персональних даних, під яким розуміється будь-яка дія або сукупність дій, таких як збирання, реєстрація, накопичення, зберігання, адаптування, зміна, поновлення, використання і поширення (розповсюдження, реалізація, передача), знеособлення, знищення персональних даних, у тому числі з використанням інформаційних (автоматизованих) систем, здійснюється виключно за згодою суб'єкта персональних даних, що передбачено частиною 6 статті 6 Закону України «Про захист персональних даних».

Однак, зауважимо, що закон передбачає й виключення з цього правила, адже визначає випадки, коли згода суб'єкта персональних даних не потрібна. Однією з таких підстав закон визначає захист життєво важливих інтересів суб'єкта персональних даних (ч. 7 ст. 6). Крім того, законодавець встановив особливості обробки спеціальних категорій персональних даних, які фактично також виступають в якості виключення із загального режиму обробки персональних даних, але шляхом запровадження ще більших обмежень та заборон (ч. 1 ст. 7). Вважаємо такий підхід цілком виправданим, адже спеціальні категорії персональних даних як правило пов'язані із найбільш значимою для кожної особи інформацією, зокрема, її релігійними та політичними уподобаннями, расовою та національною належністю, станом здоров'я тощо.

Слід зазначити, що у всіх органах Національної поліції утворено відомчі інформаційні системи, які містять персональні дані, вимоги щодо забезпечення конфіденційності яких також розповсюджуються на всі органи Національної поліції.

Разом з цим, слід констатувати, що жодна з інформаційних систем Національної поліції, а відтак – і баз даних, які містяться в ній, не є досконалими та можуть бути об'єктом неправомірного збору конфіденційної інформації, як ззовні, так і в середині системи. Наприклад, на початку 2019 року у Національній поліції України почала функціонування електронна система збору та обробки персональних даних про осіб, поміщених до ізоляторів тимчасового тримання (скорочено – Custody Records), яка також включає систему відеонагляду за вказаними особами.

За словами Уляни Шадської, впровадження системи Custody Records створює додаткові гарантії фізичної безпеки людини, її права на життя та особисту недоторканість. Посилений контроль процедури затримання та перебування в місцях обмеження волі, убезпечує особі захист від неправомірних дій з боку держави, фізичного або психологічного насилля. Безперервний моніторинг дозволяє оперативно реагувати на екстрені ситуації, запобігати випадкам суїциду, самоушкодженню тощо [212].

Не зважаючи на те, що Custody Records має на меті виявлення та попередження порушень прав людини в місцях несвободи, вказана система також потенційно може виступати в якості об'єкту зловживань як ззовні, так і з боку персоналу цих закладів. З метою убезпечення подібних ситуацій представниками Експертного центру з прав людини розроблено Рекомендації [213], які розглядаються в процесі розробки проекту Інструкції про порядок використання систем відеоспостереження в ІТТ територіальних органів поліції.

Вважаємо, що обидва вищевказаних документи повинні бути враховані під час підготовки більш загального нормативно-правового акту у сфері захисту персональних даних в органах Національної поліції України. Уявляється, що мета вказаної інструкції має полягати у визначенні: а) порядку реалізації заходів щодо захисту персональних даних, які містяться у інформаційних системах органів Національної поліції; б) заходів із забезпечення безпеки персональних даних в процесі їх обробки в інформаційних системах; в) функціональних обов'язків уповноважених посадових осіб під час збору та обробки персональних даних.

Аналіз законодавчих актів у сфері захисту персональних даних дозволив зробити висновок, що їх переважна більшість орієнтована на забезпечення захисту виключно інформації та інформаційних ресурсів. Права громадян у цій сфері й дотепер залишаються незахищеними.

Водночас, офіційне отримання персональних даних про особу у законний спосіб стає майже неможливим, адже, на нашу думку, баланс інтересів особи, суспільства та держави в Законі України «Про захист персональних даних» не дотримується. Мусимо однозначно стверджувати, що питання про співвідношення інтересів особи, суспільства та держави вирішено на користь приватних інтересів особи.

Показовою у цьому контексті є справа ЄСПЛ «Костеха проти Іспанії» із скаргою до компанії Google, яка на думку позивача незаконно розмістила сторінку із газети «La Vanguardia» з його персональними даними. Позивач вимагав від газети видалити або змінити відповідні сторінки таким чином, щоб його персональні дані більше не відображалися.

Суд Європейського Союзу постановив, що збирання, індексація, зберігання та поширення персональних даних через пошукову систему Google Search є «обробкою даних». Усупереч позиції Генерального адвоката Суд встановив, що, незважаючи на те, що пошукові системи «не здійснюють контроль над персональними даними, опублікованими на веб-сторінках третіх сторін», вони визначають мету й засоби зазначеної вище обробки персональних даних. Відповідно, компанія Google повинна розглядатися як така, що здійснює контроль за даними. Фактично, вона відіграє ключову роль у забезпеченні доступу до онлайн інформації. Оскільки Google забезпечує доступ до онлайн інформації, її діяльність може «суттєво» впливати на такі основоположні права європейських Інтернет-користувачів як право на приватне життя і захист персональних даних [214].

За таких обставин вкрай необхідно дотримання балансу інтересів, адже відбувається зіткнення законних інтересів як мінімум двох сторін: власника персональних даних, який намагається розповсюдити на останні свій суверенітет, та іншого суб'єкта

правовідносин, наділеного законними підставами щодо отримання приватної інформації.

Фахівці в галузі правової науки небезпідставно звертають увагу на дисбаланс правового режиму персональних даних у національному законодавстві в бік абсолютного захисту інтересів суб'єкта персональних даних без врахування реальних можливостей володільців та розпорядників персоніфікованої інформації [215–217]. Це ключова відмінність між нормами Закону України «Про захист персональних даних» та Конвенції про захист фізичних осіб у зв'язку із автоматизованою обробкою персональних даних.

Слід зазначити, що в країнах, які імплементували у національне законодавство норми вказаної Конвенції, відсутні будь-які спеціальні заходи захисту, крім загальноприйнятих, які висуваються до володільців персональних даних, компетенція яких обмежується питаннями управління інформаційною безпекою та підготовкою кваліфікованого персоналу.

Поряд з цим, обрання конкретних заходів захисту, технічних рішень, керівних стандартів, архітектоніки інформаційних систем, оцінювання ризиків неправомірного доступу до конфіденційної інформації залишається у віданні розпорядників персональних даних. Останні самостійно визначають необхідні заходи захисту даних, із врахуванні їх правової природи та обсягу, вартості захисного обладнання, характеристик інформаційних систем тощо.

Крім цього, у більшості законодавчих актів країн ЄС міститься норма про необхідність врахування економічної доцільності заходів щодо захисту персональних даних, за умови відсутності вимог щодо встановлення будь-яких конкретних заходів захисту персональних даних. Тобто в законодавчих актах зарубіжних країн встановлюються вимоги стосовно змістовної характеристики захисту персональних даних, тоді як у національній правовій практиці підзаконними нормативно-правовими актами встановлені формальні вимоги, які фактично не мають відношення до змістовного забезпечення захисту персональних даних.

ВИСНОВКИ

У науково-практичному посібнику наведено теоретичне узагальнення й нове розв'язання наукового завдання щодо вдосконалення адміністративно-правового забезпечення захисту персональних даних в діяльності Національної поліції України.

Виокремлено специфічні риси наукової розвідки у напрямку адміністративно-правового забезпечення захисту персональних даних, які підтверджують позитивну динаміку розвитку інституту захисту персональних даних, а саме: а) в роботах вітчизняних науковців в галузі адміністративного права питання захисту персональних даних все частіше пов'язуються із забезпеченням інформаційної безпеки держави; б) пропозиції науковців щодо вдосконалення адміністративно-правового забезпечення захисту персональних даних дедалі більше набувають практично орієнтованого змісту; в) захист персональних даних дедалі частіше згадується в якості самостійного адміністративно-правового інституту.

Сформульовано поняття захисту персональних даних через співвідношення із правовими категоріями «захист конфіденційної інформації», «захист інформації про фізичну особу», «захист інформації», як комплекс заходів технічного, організаційного та правового характеру, спрямованих на захист інформації, яка відноситься до особи, що ідентифікована або може бути конкретно ідентифікована.

Розкрито правову природу захисту персональних даних у їх нерозривному зв'язку із недоторканністю приватного життя (приватністю), яка включає наступні правомочності: а) право на свободу розпоряджатися собою та своїм життям; б) право на таємницю приватного життя; в) право на таємницю кореспонденції та листування; г) право на свободу думки; д) право на свободу совісті та віросповідання; є) право на свободу вираження своєї думки; е) право на

користування рідною мовою; ж) право на захист особистості, честі, гідності та ділової репутації, національної приналежності; з) право на захист житла; і) право на таємницю голосування.

Доведено, що правовий режим захисту персональних даних включає: загальний правовий режим конфіденційності персональних даних та спеціальний правовий режим, до якого відносяться: а) особливо чутливі дані; б) генетичні дані; в) біометричні дані; та г) дані щодо стану здоров'я. Констатовано наявність безумовного права суб'єкта персональних даних на визначення режиму власних персональних даних, а саме: а) їх збереження у таємниці; б) їх передачу розпоряднику за умови збереження їх конфіденційності; в) зробити відомості про себе загальнодоступними.

Підкреслено особливий статус Національної поліції як одного з найбільших розпорядників відомостей конфіденційного характеру в системі правоохоронних органів України, що обумовлює необхідність забезпечення надійного захисту персональних даних під час створення та використання автоматизованих баз (банків) даних. Розкрито структуру органів Національної поліції у сфері захисту персональних даних, до числа яких віднесено: а) управління забезпечення прав людини; б) управління режиму та технічного захисту інформації; в) департамент внутрішньої безпеки; г) департамент протидії кіберзлочинності; д) інспекція з особового складу Департаменту кадрового забезпечення; е) управління моніторингу патрульної поліції; є) керівники органів та підрозділів Національної поліції.

Виокремлено властивості форм та методів адміністративної діяльності Національної поліції у сфері захисту персональних даних, які проявляються у їх тлумаченні. Форми захисту персональних даних являють собою зовнішній прояв діяльності органів Національної поліції та їх посадових осіб, яка реалізується на підставі закону та в межах встановлених повноважень щодо захисту права на невтручання у приватне життя, у зв'язку з обробкою персональних даних. Методи адміністративної діяльності Національної поліції у сфері захисту персональних даних представляють сукупність прийомів та способів, спрямованих на реалізацію завдань, функцій

та повноважень органів Національної поліції та їх посадових осіб, у сфері захисту та обробки персональних даних.

Адміністративно-правовий механізм захисту персональних даних Національною поліцією визначено як комплекс заходів щодо забезпечення конституційних прав громадян на захист персональних даних, створення умов, що обмежують її поширення і виключають незаконний доступ працівників поліції до персоніфікованої інформації. Сформульовано напрямки реалізації адміністративно-правового механізму захисту персональних даних: 1) дотримання порядку надання відомостей персонального характеру; 2) дотримання правил зберігання, обліку та обробки конфіденційних відомостей на паперових носіях; 3) захист персональних даних, розташованих на електронних носіях; 4) застосування юридичної відповідальності за втрату і розголошення персональної інформації; 5) забезпечення режиму конфіденційності в роботі співробітників поліції.

Проаналізовано загальні тенденції, які виникають в процесі організації інформаційно-аналітичної діяльності правоохоронних органів зарубіжних країн, головна з яких полягає у підвищенній уваз і правоохоронців до проблеми захисту персональних даних. Разом з цим, заборона передачі персональних даних, відповідно до норм міжнародно-правових актів, не має абсолютного характеру, що пов'язано із необхідністю активної протидії правоохоронних органів кримінальним правопорушенням, терористичним актам, шпигунству тощо.

Сформульовано пріоритетне завдання законотворчої діяльності у сфері доступу уповноважених підрозділів Національної поліції до персональних даних в телекомунікаційних мережах, яке полягає у необхідності дотримання балансу інтересів особи, суспільства та держави, порушення якого призводить до негативних наслідків у вигляду збільшення соціальної напруги, нівелювання авторитету державних та правових інститутів, посиленні правового нігілізму.

Підстави доступу уповноважених підрозділів Національної поліції класифіковано на основні та додаткові, головна особливість застосування яких полягає у взаємозалежності цих підстав, жодна з яких не застосовується самостійно, а застосування додаткових

підстав є процесуальним продовженням щодо застосування основних.

Надано пропозиції щодо вдосконалення адміністративного законодавства у сфері захисту персональних даних:

1) Розроблено проєкт Інструкції з організації захисту персональних даних в інформаційному порталі Національної поліції, яка визначає порядок виконання заходів щодо захисту персональних даних, що містяться в Інформаційному порталі Національної поліції, встановлює заходи щодо забезпечення безпеки персональних даних в процесі їх обробки, а також визначає обов'язки посадових осіб.

Проект Інструкції з організації захисту персональних даних в Інформаційному порталі Національної поліції, розроблений відповідно до Закону України від 01.06.2010 № 2297-VI «Про захист персональних даних», Закону України від 05.07.1994 №80/94-ВР «Про захист інформації в інформаційно-телекомунікаційних системах», Положення про інформаційно-телекомунікаційну систему «Інформаційний портал Національної поліції України», затвердженого наказом Національної поліції України від 03.08.2017 № 676, інших нормативно-правових актів, що регламентують порядок обробки та захисту персональних даних.

2) З метою приведення у відповідність до норм Регламенту Європейського парламенту і ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних), *запропоновано доповнити Закон України «Про захист персональних даних» наступними положеннями*:

- статтею 6-1. Режими обробки персональних даних

1. Обробка персональних даних здійснюється у загальному та спеціальному режимі.

2. У загальному режимі обробляються прізвище, ім'я та по батькові, дата і місце народження, громадянство, місце проживання.

3. У спеціальному режимі обробляються: особливо чутливі дані; генетичні дані; біометричні дані; дані щодо стану здоров'я.

- статтею 15-1. Відкликання згоди на обробку персональних даних

1. У разі відкликання суб'єктом персональних даних згоди на обробку його персональних даних розпорядник зобов'язаний припинити їх обробку або забезпечити припинення такої обробки (якщо обробка персональних даних здійснюється іншою особою, яка діє за дорученням розпорядника) і в разі, якщо збереження персональних даних більше не є необхідним для цілей обробки персональних даних, знищити персональні дані або забезпечити їх знищення (якщо обробка персональних даних здійснюється іншою особою, яка діє за дорученням розпорядника) в термін, що не перевищує тридцяти днів з дати надходження зазначеного відкликання, якщо інше не передбачено договором, стороною якого, вигодонабувачем або поручителем за яким є суб'єкт персональних даних, іншою угодою між розпорядником та суб'єктом персональних даних або якщо розпорядник не має права здійснювати обробку персональних даних без згоди суб'єкта персональних даних на підставах, передбачених цим законом або іншими законами».

- пунктом 3 частини 1 статті 22, виклавши її у наступній редакції:

Стаття 22. Контроль за додержанням законодавства про захист персональних даних

1. Контроль за додержанням законодавства про захист персональних даних у межах повноважень, передбачених законом, здійснюють такі органи:

1) Уповноважений;

2) суди;

3) органи виконавчої влади.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Брижко В. М. Організаційно-правові питання захисту персональних даних: дис. ... канд. юрид. наук [Текст]: 12.00.07 / В. М. Брижко. – К., 2004. – 252 с.

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: збірник наукових праць. – К.: НДІ «Проблеми людини» і Інститут філософії НАН України, 1997. – С. 28–31.

3. Брыжко В. М. Защита персональных данных / А. А. Баранов, В. М. Брыжко, Ю. К. Базанов. – К.: Национальное агентство по вопросам информатизации при Президенте Украины, 1998. – 128 с.

4. Брыжко В. М. Права человека и защита персональных даннях / А. А. Баранов, В. М. Брыжко, Ю. К. Базанов. – К.: Національне агентство з питань інформатизації при Президенті 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. – К.: 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. – К.: НДЦПІАПрН України, 2005. – 334 с.

9. Брижко В. М. Організаційно-правові питання захисту персональних даних: автореф. дис. ... канд. юрид. наук: 12.00.07 / В. М. Брижко. – К., 2004. – 23 с.

10. Законодавство та стратегії у сфері кібербезпеки країн Європейського Союзу, США, Канади та інших. – URL: http://parlament.org.ua/wp-content/uploads/2016/11/INFODOVIDKA-ZAKONODAVSTVO-TA-STRATEGIYI-KIBERBEZPEKA.pdf.

11. Загальна декларація прав людини: Декларація від 10.12.1948 // Офіційний вісник України. – 2008. – № 93. – Ст. 3103.

12. Конвенція про захист прав людини і основоположних свобод Конвенція від 04.11.1950 // Голос України. – 2001. – № 3.

13. Міжнародний пакт про громадянські і політичні права від 16.12.1966. – URL: https://zakon.rada.gov.ua/laws/show/995_043.

14. Резолюція № 1165 Парламентської Асамблеї Ради Європи та статті 8 Конвенції про захист прав людини і основоположних свобод. – URL: https://cedem.org.ua/library/rezolyutsiya-1165-1998-pravo-na-pryvatnist/.

15. Щодо офіційного тлумачення положень частини першої, другої статті 32, частин другої, третьої статті 34 Конституції України: рішення Конституційного суду України від 20.01.2012 № 2-рп/2012 // Офіційний вісник України. – 2012. - №9. – Ст. 332.

16. Порушення права на приватність в Україні. – URL: https://forbiddentoforbid.org.ua/uk/porushennya-prava-na-privatnist/.

17. Баскаков В. Ю. Адміністративно-правовий режим інформації з обмеженим доступом: дис. ... канд. юрид. наук: 12.00.07 / В. Ю. Баскаков. – К., 2012. – 23 с.

18. Обуховська Т. І. Класифікація персональних даних та режиму доступу до них / Т. І. Обуховська // Вісник Національної академії державного управління. – № 3. – 2011. – С. 97-104.

19. Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних) // Офіційний вісник Європейського Суду – 2016 / L 119/ стор. 1.

20. Посібник з європейського права у сфері захисту персональних даних. – К.: К.І.С., 2015. – 216 с.

21. Петрицький А. Л. Правові та організаційні засади захисту персональних даних: автореф. дис. ... канд. юрид. наук: 12.00.07 / А. Л. Петрицький. – К., 2015. – 24 с.

22. Різак М. В. Правове регулювання відносин обігу персональних даних: автореф. дис. ... канд. юрид. наук: 12.00.07 / М. В. Різак. – К., 2012. – 23 с.

23. Шевчук О. М. Адміністративно-правове регулювання у сфері забезпечення інформаційної безпеки: автореф. дис. ... канд. юрид. наук: 12.00.07 / О. М. Шевчук. – Запоріжжя, 2011. – 23 с.

24. Цвірюк Д. В. Адміністративно-правовий захист персональних даних в Україні: автореф. дис. ... канд. юрид. наук: 12.00.07 / Д. В. Цвірюк. – К., 2014. – 20 с.

25. Горпинюк О. П. Кримінально-правова охорона інформаційного аспекту приватності в Україні: автореф. дис. ... канд. юрид. наук: 12.00.08 / О. П. Горпинюк. – Львів, 2011. – 22 с.

26. Кардаш А. В. Конституційно-правовий захист інформації про особу (порівняльно-правовий аспект): автореф. дис. ... канд. юрид. наук: 12.00.02 / А. В. Кардаш. – Х., 2019. – 23 с.

27. Про затвердження Порядку обробки персональних даних у базі персональних даних «Працівники» Національної комісії, що здійснює державне регулювання у сфері комунальних послуг. – URL: https://zakon.rada.gov.ua/laws/show/z1244-13.

28. Про затвердження Порядку обробки і захисту персональних даних у Міністерстві оборони України. – URL: https://zakon.rada.gov.ua/laws/show/z0071-15.

29. Положення про інформаційно-телекомунікаційну систему «Інформаційний портал Національної поліції України»: наказ Національної поліції України від 03.08.2017 № 676. – URL: https://zakon.rada.gov.ua/laws/show/z1059-17.

30. Серьогін В. О. Конституційне право особи на недоторканність приватного життя (прайвесі): проблеми теорії та практики: автореф. дис. ... канд. юрид. наук: 12.00.01, 12.00.02 / В. О. Серьогін. – Х., 2011. – 42 с.

31. Чернобай А. М. Правові засоби захисту персональних даних працівника: автореф. дис. ... канд. юрид. наук: 12.00.05 / А. М. Чернобай. – Одеса., 2006. – 23 с.

32. Ясечко С. В. Цивільно-правова відповідальність за порушення права на інформацію: автореф. дис. ... канд. юрид. наук: 12.00.03 / С. В. Ясечко. – Х., 2011. – 19 с.

33. Костенко І. В. Проблеми правового захисту персональних даних у діяльності Національної поліції / І. В. Костенко // Юридичний часопис Національної академії внутрішніх справ. – 2018. – № 1(15). – С. 296–303.

34. Красіков Д. О. Правове забезпечення інформаційної безпеки в діяльності органів внутрішніх справ України: автореф. дис. ... канд. юрид. наук: 12.00.07 / Д.О. Красіков. – К., 2012. – 22 с.

35. Права людини в діяльності української поліції – 2015. Науково-практичне видання / Упоряд. Крапивін Є. О. – К. : Асоціація УМДПЛ, 2016 р. – 408 с.

36. Семерей Б. В. Адміністративно-правові засади реалізації принципу відкритості та прозорості у діяльності національної поліції України: автореф. дис. ... канд. юрид. наук: 12.00.07 / Б. В. Семерей. – К., 2017. – 22 с.

37. Сивухін В. С. Конституційне право людини і громадянина на невтручання в їх особисте і сімейне життя та його забезпечення органами внутрішніх справ України : дис... канд. юрид. наук: 12.00.02 / Київський національний ун-т внутрішніх справ. – К., 2007. – 238 с.

38. Чирик С. В. Принципи адміністративної діяльності патрульної поліції: автореф. дис. ... канд. юрид. наук: 12.00.07 / С. В. Чирик. – Запоріжжя., 2018. – 22 с.

39. Арістова І. В. Державна інформаційна політика та її реалізація в діяльності органів внутрішніх справ України: організаційно-правові засади : автореф. дис. ... докт. юрид. наук: 12.00.07 / І. В. Арістова. – Х., 2002. – 39 с.

40. Про Національну поліцію:Закон України від 02.07.2015 № 580-VIII // Відомості Верховної Ради України. – 2015. – № 40–41. – Ст. 379.

41. Положення про інформаційно-телекомунікаційну систему «Інформаційний портал Національної поліції України»: наказ Національної поліції України від 03.08.2017 № 676. – URL: https://zakon.rada.gov.ua/laws/show/z1059-17.

42. Гібридна війна: in verbo et in praxi: монографія / Донецький національний університет імені Василя Стуса / під заг. ред. проф. Р. О. Додонова. – Вінниця: ТОВ «Нілан-ЛТД», 2017. – 412 с.

43. Права людини в діяльності української поліції – 2015. Науково-практичне видання / Упоряд. Крапивін Є. О. – К. : Асоціація УМДПЛ, 2016 р. – 408 с.

44. Про оперативно-розшукову діяльність: Закон України від 18.02.1992 № 2135-XII // Відомості Верховної Ради України. – 1992. – № 22. – Ст. 303.

45. Калюжний Р. Проблеми державної інформаційної політики: гармонізація міжнародного і національного інформаційного права / В. Гавловський, Р. Калюжний, В. Цимбалюк // Правове, нормативне та методологічне забезпечення системи захисту інформації в Україні. – 2001. – № 4. – С. 17–21.

46. Інформатизація, право, управління: (організаційно-правові питання) / В. Д. Гавловський, Р. А. Калюжний, О. Д. Крупчан та ін. – К. : Вид. Дім «Ін-Юре», 2002. – 191 с.; Інформаційне суспільство / В.М. Брижко, О. М. Гальченко, В. С. Цимбалюк та ін.; за ред. Р. А. Калюжного та М. Я. Швеця. – К. : Інтеграл, 2002. – 220 с.

47. Калюжний Р. Проблеми захисту прав людини в інформаційній сфері / Р. Калюжний, І. Андросюк // Правова інформатика. – 2004. – № 3.– С. 17–20.

48. Інформаційна безпека України / Л. С. Харченко, В. А. Ліпкан, О. В. Логінов та ін.; за ред. Р. А. Калюжного. – К.: «Текст», 2004. – 136 с.

49. Арістова І. В. Інформаційне суспільство та державна інформаційна політика / І. В. Арістова // Вісник Запорізького юридичного інституту. – 2000. – № 2. – С. 13–20.

50. 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.

51. Арістова І. В. Правове регулювання суспільних інформаційних відносин: стратегія розвитку інформаційного законодавства / І. В. Арістова // Вісник Університету внутрішніх справ. – 2001. – Вип. 14. – С. 122–128.

52. Бачило И. Л. Информационное право: Основы практической информатики / И. Л. Бачило. – М. : Издание г-на Тихомирова М. Ю., 2001. – 352 с.

53. Beigner, B. La protection de la vie privee / B. Beigner // Libertes et Droits fondamentaux. – Paris: Dalloz, 2003. – PP. 6–9. – URL: https://fbls.eu/wp-content/uploads/2007/12/Convergence-des-syst%C3%A8mes-juridiques-et-protection-de-la-vie-priv%C3%A9e-Luc-Heuschling-Professeur-de-droit-public-Universit%C3%A9-de-Lille-2.pdf.

54. Короткий путівник Європейською конвенцією з прав людини [Текст] / Д. Гом'єн ; пер. С. Ткачук. – 3. вид. – К. : Фенікс, 2006. – 192 с.

55. Люшер, Ф. Конституционная защита прав и свобод личности / Ф. Люшер. – М.: ИГ Прогресс, 1993. – 384 с.

56. Брижко В. М. Захист персональних даних в умовах розвитку інформаційного суспільства // Винахідник України. – 2001. –№ 1. – С. 7–19.

57. Конституція України // Відомості Верховної Ради України. – 1996. – № 30. – Ст. 141.

58. Серьогін В. О. Право на недоторканість приватного життя у конституційно-правовій теорії та практиці : [монографія] / В. О. Серьогін. – Х. : Фінн, 2010. – 608 с.

59. Климчик, А. Свобода информации и право на частную жизнь в международном праве: дис. ... канд. юрид. наук: 12.00.10 / А. Климчик. – М., 2003. – 184 с.

60. Harvard Law Review, Vol. 4, No. 5. (Dec. 15, 1890), pp. 193-220. – URL: https://www.jstor.org/stable/1321160?seq=1#metadata_info_tab_contents.

61. Alan F. Westin, Privacy And Freedom, 25 Wash. & Lee L. Rev. 166-167 (1968). – URL: https://scholarlycommons.law.wlu.edu/wlulr/vol25/iss1/20.

62. Bloustein, E. Privacy as an Aspect of Human Dignity / E. Bloustein // New York University Law Review. – 1964. No 39. – PP. 962-1007., с. 971. – URL: http://courses.ischool.berkeley.edu/i205/s10/readings/week11/bloustein-privacy.pdf.

63. Сакович Е. С. Диалектика приватности и публичности в виртуальном пространстве / Е. С. Сакович // Международный журнал исследований культуры. – 2012. – № 3 (8). – С. 35–41.

64. Vasiu I. User generated content websites, a profitable medium for cybercriminals / I. Vasiu [Електронний ресурс]. – URL : https:// cybersecurity-romania.ro/cybersecurity-articles/user-generated-content-websites-a-profitable-mediumfor-cybercriminals/#.

65. Рішення ЄСПЛ у справі «Костелло-Робертс проти Сполученого Королівства» (Costello-Roberts v. UK) от 25 марта 1993 г., № 13134/87. – URL: http://hudoc.echr.coe. int/eng#%7B%22fulltext%22:%5B%22№13134/87%22%5D,%22itemid%22:%5B%22002-9660%22%5D%7D.

66. Рішення ЄСПЛ у справі «Німітц проти Німеччини» (Niemietz v. Germany) от 16 декабря 1992 г., № 13710/88. – URL: http:// hudoc.echr.coe.int/eng#%7B%22fulltext%22:%5B%22№13710/88%22%5D,%22itemid%22:%5B%22001-661%22%5D%7D.

67. Рішення ЄСПЛ у справі «Лопез Остра проти Іспанії» (Lopez Ostra v. Spain) от 9 декабря 1994 г., №16798/90. – URL: http://hudoc.echr.coe.int/eng#%7B%22fulltext%22:%5B%22№16798/90%22%5D,%22itemid%22:%5B%22002-10606%22%5D%7D.

68. Обуховська Т. І. Державні механізми забезпечення захисту персональних даних в Україні: автореф...канд.. наук з держ. Управління: 25.00.02 / Т. І. Обуховська; Національна академія державного управління при Президентові України. – К., 2016. – 229 с.

69. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних від 28.01.1981 // Офіційний вісник України. – 2011. – № 58. – Ст. 85.

70. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. – URL: http://www.oecd. org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

71. Посібник за статтею 8 Конвенції про захист прав людини та основоположних свобод. Право на повагу до приватного і сімейного життя. – URL: https://unba.org.ua/assets/uploads/1259d4263dac852ef056_file.pdf.

72. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI // Голос України. – 2010. - № 172.

73. Козак В. Защита персональных данных в Украине: практика и проблемы / В. Козак // Персональные данные. – 2013. – № 7 (60)., С. 7–8.

74. Соколова О. С. Административно-правовые режимы защиты конфиденциальной информации [Текст]: дисс. ... канд. юрид. наук: 12.00.14 / О. С. Соколова. – СПб., 2005. – 212 с.

75. Чернобай А. М. Правові засоби захисту персональних даних працівника: дис. ... канд. юрид. наук : 12.00.05 / А. М. Чернобай. – Одеса, 2006. – 200 с.

76. Beigner, B. Le droit de la personnalité / B. Beigner // Collection «Que sais-je?» – P.U.F., 1992. – n°2703;

77. Hustinx, P. J. Right to privacy and data protection: mission impossible? / P. J. Hustinx // European Data Protection Day. – 2010. – 28 January. – https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTM Content? documentId=09000016802fa384.

78. Вельдер И. А. Система правовой защиты персональных данных в Европейском союзе: дис. ... канд. юрид. наук: 12.00.10 / И. А. Вельдер. – Казань, 2006. – 165 с.

79. Про інформацію: Закон України від 02.10.1992 № 2657-XII // Відом. Верхов. Ради України. – 1992. – № 48. – Ст. 650.

80. Аномалії в цивільному праві України : навч.-практ. посіб. / відп. ред. Р. А. Майданик. – К. : Юстініан, 2007. – 912 с.

81. Рішення Конституційного Суду України у справі щодо офіційного тлумачення статей 3, 23, 31, 47, 48 Закону України «Про інформацію» та статті 12 Закону України «Про прокуратуру» (справа К. Г. Устименка) від 30.10.1997 № 5-зп. // Офіційний вісник України. – 1997. – № 46. – Ст. 126.

82. Про доступ до публічної інформації:Закон України від 13.01.2011 № 2939-VI // Голос України. – 2011. – № 24.

83. Великий тлумачний словник сучасної української мови : 250000 / уклад. та голов. ред. В. Т. Бусел. – Київ; Ірпінь: Перун, 2005. – VIII, 1728 с.

84. Учебник для студентов высш. учеб. заведений юрид. спец. / Ю. П. Битяк, В. В. Богуцкий, В. Н. Гаращук и др.]; Под ред. проф. Ю. П. Битяка. – Харьков: Право, 2003. – 576 с.

85. Адміністративне право України: [навчальний посібник / За заг. ред. С. Г. Стеценко. – К.: Атіка, 2008. – 624 с.

86. Бахрах Д. Н. Административное право России : учебн. для вузов / Д.Н. Бахрах. – М.: БЕК, 2002. – 443 с.

87. Административное право и административная деятельность органов внутренних дел: [учебник / Под ред. Л.Л. Попова.] – М.: Академия МВД СССР, 1990. – 223 с.

88. Ківалов С. В., Біла Л. Р. Адміністративне право України: навчально-метод. посібн. / С.В. Ківалов, Л.Р. Біла. – Вид. 2, перероб. і доп. – О. : Юрид. літ-ра, 2002. – 312 с.

89. Лісовий кодекс: Закон України від 21.01.1994 № 3852-XII // Відом. Верхов. Ради України. – 1994. – № 17. – Ст. 99.

90. Про правовий режим території, що зазнала радіоактивного забруднення внаслідок Чорнобильської катастрофи: Закон Україн и від 27.02.1991 № 791а-XII // Відомості Верховної Ради України. – 1991. – № 16. – Ст. 198.

91. Про правовий режим надзвичайного стану : Закон України від 16.03.2000 № 1550-III // Відомості Верховної Ради України. – 2000. – № 23. – Ст. 176.

92. Про правовий режим воєнного стану : Закон України від 12.05.2015 № 389-VIII // Відомості Верховної Ради України. – 2015. – № 28. – Ст. 250.

92. Про внесення змін до деяких законів України щодо обмеження доступу на український ринок іноземної друкованої продукції антиукраїнського змісту: Закон України від 08.12.2016 № 1780-VIII від 27.01.2017 // Відомості Верховної Ради України. – 2017. – № 4. – Ст. 41.

93. Юридична енциклопедія : в 6-и т. : юридические статьи / ред. кол. Ю. С. Шемшученко (гол. ред.) [та ін.] ; НАН України. – К.: Укр. енциклопедія, 2003. – Т. 5. – 736 с.

94. Юридична енциклопедія : в 6-и т. / редкол.: Ю. С. Шемшученко (голова редкол.) та ін. – К. : Укр. Енцикл., 1998. – Т. 2. – 736 с.

95. Беляєва Г. С. Правовой режим в общетеоретическом измерении : монографія / Г. С. Беляєва. – М.: Юрлитинформ, 2013. – 240 с.

96. Колодій А. М. Теорія держави і права / Колодій А. М., Копейчиков В. В., Лисенков С. Л., Пастухов В. П., Сумін В. О., Тихомиров О. Д. – К.: Юрінформ, 1995. – 190 с.

97. Загальна теорія держави і права / за ред. В. В. Копейчикова. – К.: ЮРінком, 1997. – 320 с.

98. Хропанюк В. М. Теория государства и права : учебное пособие для высших учебных заведений / под ред. В. Г. Стрекозова – М., 1999. – 378 с.

99. Матузов Н. И. Правовые режимы: Вопросы теории и практики / Н. И Матузов, А. В. Малько // Правоведение. – 1996. – № 1 – С. 16–29.

100. Мінка Т. П. Органи внутрішніх справ як суб'єкти забезпечення адміністративно-правових режимів : дис. ... доктора юрид. наук : спец. 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право» / Т. П Мінка. – Дніпропетровськ: Дніпроп. у-т внутр. справ, 2001. – 615 с.

101. Загальна теорія держави і права : підручник для студентів юридичних спеціальностей вищих навчальних закладів / [М. В. Цвік, В. Д. Ткаченко, Л. Л. Богачова та ін.]; за ред.. М. В. Цвіка, В. Д. Ткаченка, О. В. Петришина. – Харків : Право, 2002. – 432 с.

102. Кузніченко С. О. Категорія «адміністративно-правовий режим» у юридичній науці та законодавстві України / С. О. Кузніченко, А. С. Спаський // Актуальні проблеми держави і права. – 2007. – Вип. 35. – С. 70–75.

103. Соколова І. О. Правовий режим: поняття, особливості, різновиди. дис... канд. юрид. наук: спец. 12.00.14 «Теорія та історія держави і права; історія політичних і правових учень» / Соколова Ірина Олександрівна. – Харків., 2011 – 180 с.

104. Гетьманцева Н. Д. Особливості правового регулювання трудових відносин : монографія / Н. Д. Гетьманцева. – Чернівці : Технодрук, 2015. – 592 с.

105. Антопольский А. А. Правовое регулирование информации ограниченного доступа в сфере государственного управления: автореф. дис. ... канд. юрид. наук / А. А. Антопольский. – М., 2004. – С. 8–9.

106. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» // Офіційний вісник України. – 2017. – № 20. – 554.

107. Мінка Т. П. Особливості класифікації адміністративно-правових режимів. – URL: https://www.irbis-nbuv.gov.ua/.../cgiirbis_64.exe.

108. Постанова ЄСПЛ від 06.10.2009 у справі «С.С. проти Іспанії» (скарга № 1425/06). – URL: https://lawinstitut.wordpress.com/.

109. Постанова ЄСПЛ від 15.10.2009 у справі «Цуркаліс проти Греції» (скарга № 50796/07). – URL: https://lawinstitut.wordpress.com/.

110. Про звернення громадян: Закон України від 02.10.1996 № 393/96-ВР // Відомості Верховної Ради України. – 1996. – № 47. – Ст. 256.

111. 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.

112. Олійник О. В. Захист інформації в умовах інформаційного суспільства / О.В. Олійник // Право України. – 2005. – № 10. – С. 100–103.

113. Дем'яненко Ю. І. Кримінальна відповідальність за порушення недоторканності приватного життя [Текст]: дис. ... канд. юрид. наук: 12.00.08 / Ю.І. Дем'яненко. – Х., 2008. – 242 с.

114. Гуржій Т. О. Концептуальні засади розуміння джерел права / Т.О. Гуржій // Публічне право. – 2012. – № 2(6). – С. 247–252.

115. Усенко І. Коментар до Закону України «Про захист персональних даних» // «Права людини в Україні» Інформаційний портал Харківської правозахисної групи» [Електронний ресурс]. – URL: http://khpg.org/index.php?id=1330343937.

116. Білозерська Т. О. Реформування публічної адміністрації в Україні як крок до європейської інтеграції / Т. О. Білозерська // Форум права. – 2007. – № 2. – С. 11–19.

117. Гнидюк Н. Визначення поняття публічної адміністрації в ACQUIS COMMUNAUTAIRE / Н. Гнидюк // Законодавство України: науково-практичний коментар. – 2006. – № 10. – С. 74–77.

118. Про затвердження Порядку розгляду звернень та організації проведення особистого прийому громадян в органах та підрозділах Національної поліції України: наказ МВС України від 15.11.2017 № 930 // Офіційний вісник України. – 2018. – № 8. – Ст. 319.

119. Про затвердження Порядку ведення єдиного обліку в органах (підрозділах) поліції заяв і повідомлень про кримінальні правопорушення та інші події: наказ МВС України від 08.02.2019 № 100 // Офіційний вісник України. – 2019. – № 26. – Ст. 939.

120. Про затвердження Переліку відомостей, що становлять службову інформацію в системі Міністерства внутрішніх справ України: наказ МВС України від 27.05.2016 № 432. – URL: https://zakon.rada.gov.ua/rada/show/v0432320-16.

121. Про запобігання корупції:Закон України від 14.10.2014 № 1700-VII // Відомості Верховної Ради України. – 2014. – № 49. – Ст. 2056.

122. Про очищення влади: Закон України від 16.09.2014 № 1682-VII // Відомості Верховної Ради України. – 2014. – № 44. – Ст. 2041.

123. Мейдич І. М. Кримінально-правова охорона службової інформації : підходи до удосконалення : матеріали науково-практичної конференції, 08 червня 2016 р. ; упорядн. В. М. Фурашев, С. Ю. Петряєв., 2016. – 200 с.

124. Болдир С. В. Перспективи реформування системи охорони державної таємниці та службової інформації / С. В. Болдир // «Інформація і право» № 4(23)/2017. – С. 79–85.

125. Єдиний державний реєстр судових рішень. – URL: http://www.reyestr.court.gov.ua/Review/80364172.

126. Караваев А. А. Административно-правовое регулирование оборота и защиты конфиденциальной информации в органах внутренних дел 12.00.14 Воронеж, 2015. – 220 с.

127. Про державний захист працівників суду та правоохоронних органів:Закон України від 23.12.1993 № 3781-XII // Відомості Верховної Ради України. – 1994. – № 11. – Ст. 50.

128. Про Службу безпеки України: Закон України від 25.03.1992 № 2229-XII // Відомості Верховної Ради України. – 1992. – № 27. – Ст. 382.

129. Про прокуратуру: Закон України від 14.10.2014 № 1697-VII // Відомості Верховної Ради України. – 2015. – № 2–3. – Ст. 12.

130. Про організаційно-правові основи боротьби з організованою злочинністю: Закон України від 30.06.1993 № 3341-XII // Відомості Верховної Ради України. – 1993. – № 35. – Ст. 358.

131. Про банки і банківську діяльність: Закон України від 07.12.2000 № 2121-III // Відомості Верховної Ради України. – 2001. – № 5. – Ст. 30.

132. Про затвердження Порядку обробки персональних даних у базі персональних даних «Електронний журнал обліку запитів на публічну інформацію: Наказ МВС України від 21.08.2013 № 805 // Офіційний вісник України. – 2013. – № 75. – Ст. 2797.

133. ДСТУ №7531-2015 «Інформаційні технології. Методи захисту. Основні положення щодо забезпечення невтручання в особисте життя (ISO/IEC 29100:2011. – URL: https://zakon.rada.gov.ua/rada/show/v0061774-15/print.

134. Алексеев С. С. Методологические основы научно-правовых исследований: научное пособие / С. С. Алексеев. – М. : Юрид. лит., 1981. – 212 с.

135. Новий тлумачний словник української мови : у 4 т. : 42 000 сл. : [для студ. вищ. та серед. навч. закл.] / уклад. В. Яременко, О. Сліпушко. – К. : Аконіт, 1998. – 944 с.

136. Краткая философская энциклопедия / под ред. Е. Ф. Губского, Г. В. Кораблевой, В. А. Лутченко – М. : Прогресс, 1994. – 576 с.

137. Ожегов С. И. Словарь русского языка : ок. 57 000 слов / С. И. Ожегов ; под ред. Н. Ю. Шведовой. – 18-е изд., стереотип. – М. : Русский яз., 1987. – 798 с.

138. Козлов Ю. М. Понятие формы управленческой деятельности // Методы и формы государственного управления. – М. : Юрид. лит., 1977. – С. 12–15.

139. Курс адміністративного права України : підручник / В. К. Колпаков, О. В. Кузьменко, І. Д. Пастух, В. Д. Сущенко [та ін.] / за ред. В. В. Коваленка. – К. : Юрінком Інтер, 2012. – 808 с.

140. Пантелеев В. Ю. Административная деятельность органов внутренних дел: Учебное пособие для подготовки к экзаменам. – Екатеринбург: Изд-во Уральского юридического института МВД России, 2002. – С. 61–92.

141. Адміністративна діяльність ОВС. Загальна частина : [підручник / за заг. ред. І. П. Голосніченка, Я. Ю. Кондратьєва]. – К. : УАВС, 1995. – 177 с.

142. Публічне адміністрування в Україні: навчальний посібник / В. Б. Дзюндзюк, Н. М. Мельтюхова, Н. В. Фоміцька та ін.; за заг. ред. В. В. Корженка та Н. М. Мельтюхової. – Х. : Вид-во ХарРІ НАДУ «Магістр», 2011. – 306 с.

143. Гуржій Т. О. Адміністративне право України: навчальний посібник / Т. О. Гуржій. – К. : КНТ, 2011. – 680 с.

144. Адміністративне право України. Академічний курс / Т. О. Коломоєць, С. В. Ващенко, В. Г. Поліщук; за ред. Т. О. Коломоєць. – К.: Юрінком-Інтер, 2011. – 574 с.

145. 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. – Х.: Право, 2010. – 624 с.

146. Петрицький А. Л. Правові та організаційні засади захисту персональних даних: дис. ... канд. юрид. наук [Текст]: 12.00.07 / А. Л. Петрицький. – К., 2015. – 223 с.

147. Філософський словник / за ред. В. І. Шинкарука. – К.: Головна редакція УРЕ, 1973. – 600 с.

148. Єсімов С. С. Інформаційно-аналітична діяльність МВС України як об'єкт правового регулювання / С. С. Єсімов // Науковий вісник Дьвівського державного університету внутрішніх справ. – № 1. – 2017. – С. 184-195.

149. Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони від 27.06.2014 // Офіційний вісник України. – 2014. – № 75. – Ст. 2125.

150. Офіційний сайт Міністерства внутрішніх справ України. – URL: https://mvs.gov.ua/.

151. Про внесення змін до деяких законодавчих актів України щодо удосконалення системи захисту персональних даних: Закон України від 03.07.2013 №383-VII // Відомості Верховної Ради України. – 2014. – № 14. – Ст. 252.

152. Про затвердження документів у сфері захисту персональних даних: наказ Уповноваженого Верховної Ради з прав людини від 08.01.2014 № 1/02-14. – URL: https://zakon.rada.gov.ua/laws/card/v1_02715-14.

153. Щорічна доповідь Уповноваженого Верховної Ради України з прав людини про стан додержання та захисту прав і свобод людини і громадянина в Україні у 2018 році. – URL: http://www.ombudsman.gov.ua/ua/page/secretariat/gromadskist/zayavi-upovnovazhenogo-2018/.

154. Офіційний сайт Верховної Ради України. – URL: https://zakon.rada.gov.ua/laws/find/l325478?org=51.

155. Биля І. О. Теоретичні основи використання нормотворчої техніки: автореф. дис. ... канд. юрид. наук [Текст]: 12.00.01 / І. О. Биля. – Х., 2004. – 21 с.

156. Про затвердження Положення про контроль за станом технічного захисту інформації в органах і підрозділах Національної поліції України: наказ МВС України від 29.02.2016 № 139 // Офіційний вісник України. – 2016. – № 27. – Ст. 1081.

157. Д. Кобзін, А. Черноусов, К. Коренева, М. Колоколова Моніторінг незаконного насильства в поліції України (2004–2017 рр.), Харків, Харківський інститут соціальних досліджень (ХІСД). – 2017. – 97 с.

158. Звіт Голови Національної поліції України С. Князєва про результати роботи відомства за 2018 рік. – URL: https://www.naiau.kiev.ua/files/news/2018/Zvit_NPU_2018.pdf.

159. Про стан дотримання прав людини в діяльності органів Національної поліції України за 6 місяців 2019 року: доповідна записка Національної поліції України від 01.08.2019 № 25027.

160. Про захист інформації в інформаційно-телекомунікаційних системах Закон України від 05.07.1994 № 80/94-ВР // Відомості Верховної Ради України. – 1994. – № 31. – Ст. 286.

161. Кримінальний кодекс України: Закон України від 05.04.2001 № 2341-III // Відомості Верховної Ради України. – 2001. – № 25. – Ст. 131.

162. Кодекс законів про працю:Кодекс від 10.12.1971 № 322-VIII // Відомості Верховної Ради УРСР. – 1971. – № 50.

163. Про внесення змін до деяких законодавчих актів України щодо посилення відповідальності за порушення законодавства про захист персональних даних: Закон України від 02.06.2011 № 3454-VI // Відомості Верховної Ради України. – 2011. – № 50. – Ст. 549.

164. Кодекс України про адміністративні правопорушення. Відомості Верховної Ради Української РСР. 1984. Додаток до № 51. Ст.1122.

165. Цивільний кодекс України від 16 січня 2003 р. // Офіційний вісник України. – 2003. – № 11. – Ст. 461.

166. Відносно персональних даних: лист Державної служби України з питань захисту персональних даних від 02.04.2012 № 10/1106-12 // Бізнес-Бухгалтерія-Право. Податки. Консультації. – 2012. – № 25. – Стор. 58.

167. Сеник С. В. Дослідження організаційних основ побудови комплексних систем захисту інформації з обмеженим доступом у підрозділах Національної поліції України / С. В. Сеник // Науковий вісник Львівського державного університету внутрішніх справ. – № 4. – 2018. – С. 180–189.

168. Тимчасове положення про категоріювання об'єктів ТПКО-95: наказ Державної служби України з питань технічного захисту інформації від 10.07.1995 р. № 35. – URL: http://zakon.rada.gov.ua/rada/show/v0035267-95.

169. Положення про державну експертизу в сфері технічного захисту інформації: наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 16.05.2007 р. № 93. – URL: http://zakon.rada.gov. ua/laws/show/z0820-07.

170. НД ТЗІ 1.1-005-07. Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення: наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 12.12.2007. – № 232. – К., 2007.

171. НД ТЗІ 1.6-003-04. Створення комплексів технічного захисту інформації на об'єктах інформаційної діяльності. Правила розроблення, побудови, викладення та оформлення моделі загроз для інформації: наказ ДСТСЗІ СБ України від 10.03.2004. – № 04. – К., 2004.

172. НД ТЗІ 3.1-001-07. Захист інформації на об'єктах інформаційної діяльності. Створення комплексів технічного захисту інформації. Передпроєктні роботи: наказ Адміністрації Держспецзв'язку від 12.12.2007. – № 232. – К., 2007.

173. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. НД ТЗІ 3.7-003-05: наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від

08.11.2005 р. № 125. – URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=46074&cat_id=38835.

174. НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі: наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації СБ України від 28.04.1999 р. (зі зміною № 1, затвердженою наказом Департаменту СТСЗІ СБ України від 18.06.2002 р. № 37 та із змінами згідно з наказом Адміністрації Держспецзв'язку від 28.12.2012 р. № 806). – URL: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja &uact=8.

175. Департамент інформаційно-аналітичної підтримки Національної поліції України. – URL: https://www.npu.gov.ua/about/struktura/struktura/departament-informaczijno-analitichnoji-pidtrimki-naczionalnoji-policziji-ukrajini.html.

176. Офіційний сайт Донецького юридичного інституту. – URL: http://www.dli.donetsk.ua/news/2018-06-23-1.

177. Горпинюк О. П. Кримінально-правова охорона приватності в іноземних державах / О. П. Горпинюк // Часопис Академії адвокатури України. – 2009. – № 4 (5) [Електронний ресурс] – URL: http://www.nbuv.gov.ua/e-journals/Chaau/2009-4/09goppid.pdf.

178. Горпинюк О. П. Інформація як предмет складів злочинів, що посягають на приватність / О. П. Горпинюк // Форум права. – 2010. – № 4. – С. 229–234 [Електронний ресурс]. – URL: http://www.nbuv.gov.ua/e-journals /FP/2010-4/10goppnp.pdf.

179. Линник Г. М. Принципи адміністративно-правового регулювання інформаційної безпеки України / Г. М. Линник // Підприємництво, господарство і право. – 2010. – № 5. – С. 93–97.

180. Марущак А. І. Інформаційне право: Доступ до інформації: навчальний посібник / А. І. Марущак. – К.: КНТ, 2007. – 532 с.

181. 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.

182. Рекомендація Комітету міністрів Ради Європи № R(87)15 1987 року про використання персональних даних у секторі

поліції – URL: http://cyberpeace.org.ua/files/rekomendacia_km_radi_evropi_sodo_vikoristanna_personal_nih_danih_sektori_policii.pdf.

183. Додатковий протокол 2001 року до Конвенції Ради Європи 1981 року про захист осіб у зв'язку з автоматизованою обробкою персональних даних щодо органів нагляду та транскордонних потоків даних від 08.11.2001 // Офіційний вісник України. – 2011. – № 1/№ 58. – Ст. 86.

184. Про обробку персональних даних та захист таємниці сектора електронних комунікацій (Директива про секретність та електронні комунікації): Директива 2002/58/ЄС від 12 липня 2002 року. – URL: https://nkrzi.gov.ua/images/upload/58/19/6f96b8148ef15842f70cba3dd98f055b.pdf.

185. Рішення Ради (ЄС) № 2008/633/ JHA від 23 червня 2008 року про доступ до Візової інформаційної системи (VIS) компетентних органів держав-членів та Європолу в цілях запобігання, виявлення та розслідування терористичних та інших серйозних кримінальних правопорушень: Посібник з європейського права у сфері захисту персональних даних. – К.: К.І.С., 2015. – 216 с.

186. МЗС: Україна фактично завершила вихід з СНД https://www.unian.ua/politics/10443504-mzs-ukrajina-faktichno-zavershila-vihid-z-snd.html.

187. О персональных данных: модельный закон СНГ, принятый постановлением Межпарламентской ассамблеи государств-участников СНГ от 16.10.1999. – URL: http://docs.cntd.ru/document/901818602.

188. Аналіз і коментарі до змін до Закону України про захист персональних даних / М. Жорж, Г. Саттон. – Страсбург, 2012. – 71 с.

189. Пекар В. Європейська інтеграція чи нова загроза підприємцям? / В. Пекар // Веб-сайт Українського союзу промисловців і підприємців [Електронний ресурс]. – URL: http://www.uspp.org.ua/interview/9.vropeyska-integraciya-chi-nova-zagroza-pidprimcyam.htm&print.

190. Шестаков В. Защита персональных данных в Украине: эволюция правового регулирования / В. Шестаков, Л. Чернявський // Руководство директора по персоналу. – 2013. – № 2. – С. 13–18.

191. Колесникова К. О. Публічне адміністрування в Україні: огляд літературних джерел / К. О. Колесникова // Теорія та практика державного управління: зб. наук. пр. – Х. : Вид-во ХарРІ НАДУ «Магістр», 2013. – Вип. 3. – С. 107–115.

192. Коровяковский Д. Г. Российский и зарубежный опыт в области защиты персональных данных // Национальные интересы: приоритеты и безопасность. 2009. № 5. – URL: http://cyberleninka.ru/article/n/rossiyskiy-i-zarubezhnyy-opyt-v-oblasti-zaschity-personalnyh-dannyh.

193. Управління органами Національної поліції України : підручник / за заг. ред. д-ра юрид. наук, доц. В. В. Сокуренка ; [О. М. Бандурка, О. І. Безпалова, О. В. Джафарова та ін. ; передм. В. В. Сокуренка] ; МВС України, Харків. нац. ун-т внутр. справ. – Харків: Стильна типографія, 2017. – 580 с.

194. Act on the «Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism». Available at: https://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf.

195. Гриняев С. Интернет под колпаком /С. Гриняев // «Независимое военное обозрение», приложение к «Независимой газете». – URL: http://nvo.ng.ru/spforces/2001-05-18/7_Internet.html.

196. Official Journal of the European Communities, C 329, 4 November 1996. – URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=OJ%3AC%3A1996%3A329%3ATOC.

197. Конвенція про кіберзлочинність від 23.11.2001 // Офіційний вісник України. – 2007. – № 65. – Ст. 2535.

198. Директива 97/66/ЄС Європейського Парламенту і Ради «Стосовно обробки персональних даних і захисту права на невтручання в особисте життя в телекомунікаційному секторі: Директива від 15.12.1997. – URL: https://zakon.rada.gov.ua/laws/card/994_243.

199. Резолюція Ради ЄС (96/С 329/01) від 17 січня 1995 року про законне перехоплення телекомунікацій. – URL: https://zakon.rada.gov.ua/laws/card/994_235.

200. Обуховська Т. Захист персональних даних в умовах розвитку інформаційного суспільства: передумови, принципи та міжнародне законодавство. Вісник НАДУ. 2014. №1. С. 95-103.

201. Курочка М.Й. Законність в ОРД та прокурорський нагляд за її дотриманням: Монографія / За ред. члена-кореспондента АпрН України. Луган. ін-т внутр. справ. - Луганськ: РВВ ЛІВО, 2001. 210 с.

202. Гражданский кодекс Украины: Комментарий (с изменениями и дополнению по состоянию на 1 сентября 2003 года). - Т. 1. - Х.: ООО «Одисей», 2003. 240 с.

203. Про телекомунікації: закон України від 18.11.2003 № 1280-IV // Відомості Верховної Ради України. – 2004. – № 12. – Ст. 155.

204. Про поштовий зв'язок: закон України від 04.10.2001 № 2759-III // Відомості Верховної Ради України. – 2002. – № 6. – Ст. 39.

205. Про державну таємницю: закон України від 21.01.1994 № 3855-XII // Відомості Верховної Ради України. – 1994. – № 16. – Ст. 93.

206. Кримінальний процесуальний кодекс України: закон України від 13.04.2012 № 4651-VI // Відомості Верховної Ради України. – 2013. – № 9-10. – Ст. 88.

207. Про забезпечення безпеки осіб, які беруть участь у кримінальному судочинстві: закон України від 23.12.1993 № 3782-XII // Відомості Верховної Ради України. – 1994. – № 11. – Ст. 51.

208. Про впорядкування, виготовлення, придбання та застосування технічних засобів для зняття інформації з каналів зв'язку: указ Президента України від 13.04.2001 №256/2001 // Офіційний вісник України. – 2001. – №16. – Ст. 697.

209. Про затвердження Положення про порядок розроблення, виготовлення, реалізації та придбання спеціальних технічних засобів для зняття інформації з каналів зв'язку, інших засобів негласного отримання інформації: постанова Кабінету Міністрів України від 27.10.2001 № 1450 // Офіційний вісник України. – 2004. – №28. – Ст. 1870.

210. Мельник Д. Перспективи нормативно-правового врегулювання зняття інформації з телекомунікаційних мереж та електронних інформаційних систем у новому КПК України / Д. Мельник // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, 2(24) вип., 2012 р. – С. 34–40.

211. Захист даних в системі Custody Records. – URL: https://ecpl.com.ua/news/zakhyst-danykh-v-systemi-custody-records/.

212. Шадська У. 107 рекомендацій щодо забезпечення захисту персональних даних в інформаційних системах ізоляторів тимчасового тримання Національної поліції України. – URL: http://ecpl.com.ua/wp-content/uploads/2019/02/107-REKOMENDATSIY.pdf.

213. Приватне життя і захист персональних даних у практиці ЄСПЛ. – URL: http://www.ukrainepravo.com/international_law/european_court_of_human_rights/tuyvakhrye-zykhkhya-k-iashyfkh-tyeufsraoerysh-earysh-ts-tuankhyshchk-zhfto/.

214. Бем М. В., Городинський І. М., Саттон Г., Родіоненко О. М. Захист персональних даних: Правове регулювання та практичні аспекти: науково-практичний посібник. К.: К.І.С., 2015. 220 с.

215. Єсімов С С. Захист персональних даних у контексті розвитку динамічних систем. Науковий вісник державного університету внутрішніх справ. 2013. № 3. С. 198–207.

216. Волосецький В. О. Іноземний досвід правового регулювання захисту персональних даних / Міжнародний науковий журнал. – URL: https://www.inter-nauka.com/uploads/public/14815322304340.pdf.

Науково-практичний посібник присвячений комплексному та системному вивченню теоретико-правових засад адміністративно-правового забезпечення захисту персональних даних, організаційно-правового механізму захисту персональних даних та визначенню напрямів удосконалення адміністративно-правового захисту персональних даних Національною поліцією України.

Видання може бути корисним для співробітників практичних підрозділів Національної поліції України, працівників, курсантів, студентів та слухачів закладів вищої освіти із специфічними умовами навчання, що здійснюють підготовку поліцейських.

ISBN 978-617-7679-52-2