

**ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ ЯК ГАРАНТІЯ ЗАБЕЗПЕЧЕННЯ
ПРАВА НА ПОВАГУ ДО ОСОБИСТОГО ТА СІМЕЙНОГО ЖИТТЯ**

ЗМІСТ

Вступ.....	3
Розділ 1. Теоретичні аспекти захисту персональних даних	7
1.1 Поняття та ознаки персональних даних у правовій доктрині	7
1.2 Нормативно-правове регулювання сфери захисту персональних даних в Україні.....	9
1.3 Основоволожні засади захисту персональних даних за чинними міжнародними актами та договорами.....	12
Розділ 2. Зарубіжний досвід захисту персональних даних.....	15
2.1 Забезпечення захисту персональних даних у деяких країнах Європи	15
2.2 Законодавче врегулювання захисту персональних даних у Сполучених Штатах Америки	16
Розділ 3. Проблемні питання та шляхи їх вирішення у сфері захисту персональних даних під час діяльності правоохоронних органів	19
3.1 Проблематика законодавчого забезпечення та практики у регулюванні діяльності правоохоронних органів	19
3.2 Перспективи удосконалення сфери захисту персональних даних.....	21
Висновки	25
Список використаних джерел	28
Анотація	31
Додатки.....	33

ВСТУП

Із розвитком технологій сфера захисту інформації, що містить персональні дані стає більш уразливою, оскільки ми іноді можемо надати згоду на обробку персональних даних, навіть не здогадуючись про це. Найчастіше це може статись серед активних користувачів соціальних мереж або під час завантаження додатків на гаджети, а також під час незаконних дій шахраїв.

Актуальність теми. Актуальність обраної теми зумовлена низьким рівнем правової освіченості громадян у сфері захисту персональних даних. З кожним роком обіг інформації збільшується, полегшується доступ до інтернет-ресурсів, а отже є ймовірність того, що будь-хто може неправомірно заволодіти інформацією про ту, чи іншу особу, якщо не вживати засобів захисту.

Наразі права людини і громадянина знаходяться у центрі уваги як вітчизняних, так і зарубіжних науковців і практиків, зокрема, проблематику захисту персональних даних як однієї із гарантій забезпечення права на особисте та сімейне життя досліджують В. Брижко, А. Головченко, П. Діхтієвський, С. Єсімов, П. Макушев, В. Марченко, Т. Обуховська, А. Пазюк та інші, однак захист персональних даних в окремих сферах, зокрема при проведенні оперативно-розшукової та контррозвідувальної діяльності правоохоронними органами залишається неврегульованим у повній мірі.

Об'єктом даного дослідження є суспільні відносини у сфері захисту персональних даних.

Предметом даного дослідження є захист персональних даних як гарантія забезпечення права на повагу до особистого та сімейного життя і їх таємницю.

Метою даної роботи є вивчення та узагальнення знань про сферу захисту персональних даних, зокрема під час діяльності правоохоронних органів; виявлення недоліків законодавчого забезпечення із захисту персональних даних та встановлення шляхів їх усунення; аналіз законодавчого забезпечення сфери захисту персональних даних у зарубіжних країнах.

Для успішного досягнення поставленої мети має бути виконано такі завдання: 1) дослідити поняття та ознаки персональних даних; 2) нормативно-правове регулювання сфери захисту персональних даних; 3) визначити принципи обробки персональних даних у міжнародній практиці та за законодавством України; 4) розглянути законодавчі гарантії заходів захисту персональних даних у зарубіжних країнах; 5) виявити проблеми законодавчого забезпечення та практичної спрямованості сфери захисту персональних даних; 6) визначити перспективи вдосконалення сфери захисту персональних даних під час діяльності правоохоронних органів.

Методологічну основу даного дослідження становить система загальнонаукових та спеціально-наукових методів:

1) метод структурного аналізу і синтезу використовувався для поділу отриманої інформації на окремі структурні одиниці та системне поєднання різних сторін інформації в єдину структуровану систему на прикладі принципів обробки персональних даних;

2) порівняльно-правовий метод лежить в основі встановленні відмінних та подібних рис комплексних заходів щодо захисту персональних даних у різних країнах;

3) моделювання та прогнозування полягає у приблизному створенні та уявленні моделі заходів щодо захисту сфери персональних даних;

4) системний підхід – полягає у визначенні окремих заходів забезпечення захисту персональних даних як нерозривної системи, зокрема, на прикладі заходів із захисту персональних даних.

Наукова новизна полягає у:

1) класифікації категорій осіб, персональні дані яких можуть використовуватись під час роботи із розслідування кримінального правопорушення;

2) напрацюванні типових інструкцій для правоохоронних органів під час роботи із персональними даними.

Теоретичне значення роботи полягає комплексному дослідженні сфери захисту персональних даних, визначенні основних способів захисту прав суб'єктів персональних даних. У дослідженні увагу також зосереджено на забезпеченні прав суб'єктів персональних даних під час діяльності правоохоронних органів, оскільки на сьогодні дана сфера не є достатньо врегульованою. Більшість дослідників сфери захисту персональних даних приділяють увагу забезпеченню прав суб'єктів персональних даних під час ведення господарської діяльності або у цивільно-правових відносинах, проте не є достатньо дослідженими способи захисту під час діяльності правоохоронних органів.

Практичне значення полягає у тому, що матеріали дослідження та його висновки можуть бути використані у:

- 1) науково-дослідній роботі – як основа для поглибленого вивчення та удосконалення даної роботи з окремим дослідженням особливостей сфери захисту персональних даних як забезпечення права на повагу до особистого та сімейного життя;
- 2) навчальному процесі – під час створення спеціальних курсів або факультативів у середніх навчальних закладах та закладах вищої освіти;
- 3) правотворчій діяльності – як основа для створення удосконаленої нормативної бази у сфері захисту персональних даних, зокрема і під час роботи із кримінальними провадженнями;
- 4) правозастосовній діяльності – для удосконалення публічно-владних відносин органів державної влади та народу;
- 5) правовиховній роботі – для підвищення рівня правової культури населення України у частині, що стосується захисту своїх прав під час обробки персональних даних.

Апробація результатів дослідження. Теоретичний матеріал та висновки, що містяться у роботі, були опубліковані на всеукраїнських та міжнародних науково-практичних конференціях: «Сучасний вимір прав людини:

конституційний контекст» (27 жовтня 2018, м. Харків) та «Верховенство права очима правників-початківців» (2 листопада 2018, м. Одеса).

РОЗДІЛ 1. ТЕОРЕТИЧНІ АСПЕКТИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

1.1 Поняття та ознаки персональних даних у правовій доктрині

Кожен має право на доступ до інформації, що гарантується ст. 34 Конституції України, та його «...слід розуміти як закріплену у законодавстві можливість отримувати будь-які відомості та/або дані на матеріальних носіях або в електронному вигляді...» [17; с. 260]. Право на доступ до інформації тісно межує із правом на повагу до особистого та сімейного життя, підставою порушення якого може виступати несанкціоноване заволодіння персональними даними.

Сфера персональних даних не є новою або недосліджуваною правовою категорією, але зазвичай дослідниками виступають представники цивільного, інформаційного та адміністративного права. З погляду конституціоналістики, захист персональних даних виступає гарантією забезпечення реалізації права на повагу до особистого та сімейного життя. Доволі часто науковцями використовуються близькі за значенням категорії, серед яких: «конфіденційна інформація», «персональні дані», «персоніфікована інформація», «особисті дані», «особиста інформація», що ускладнює розуміння не тільки для недосвідчених громадян, а й для фахівців у сфері правового забезпечення.

С. Єсімов зазначає, що захист персональних даних має конституційну природу, є елементом права громадян на повагу до особистого життя, а також правові норми, які регламентують питання захисту персональних даних, охоплюють більшість галузей права [20] .

У правовій доктрині досі не існує єдиного підходу щодо визначення терміну «персональні дані», проте, проаналізувавши здобутки вчених, можна дійти висновку, що науковці мають схожі думки щодо його розуміння. Так, і законодавець обрав лаконічне та чітке визначення, що найбільш повно характеризує зміст даної категорії.

На думку В. Речицького, персональні дані – це юридичний термін спеціального призначення. Він означає не просто конфіденційну інформацію, а її конкретний тип, різновид [21].

Відповідно до Закону України «Про захист персональних даних» персональні дані – це відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована [9].

Інститут недоторканності особистого та сімейного життя почав розглядатись як обов'язкова умова розвитку демократичного суспільства після проголошення суддею Верховного Суду Сполучених Штатів Америки Луї Брандейсом, що у Конституції США наявне «право бути залишеним у спокої» [21].

Розглядаючи сутність права на повагу до особистого та сімейного життя, можна дійти висновку, що «інформація, яка містить персональні дані» та «інформація про приватне життя» подібні за змістовою наповненістю та співвідносяться як «ціле та частина». Згідно з цією концепцією існує два основних підходи до її розуміння:

- 1) персональні дані входять до інформації про приватне життя, пояснюючи це тим, що міжнародна практика відносить до сфери приватного життя будь-яку інформацію, яку можна зв'язати з конкретною особою;

- 2) інформація про приватне життя входить до персональних даних, оскільки не будь-які відомості можуть містити інформацію про особисте життя (наприклад, стандартні анкетні дані про дату народження або місце проживання) [18].

На нашу думку, доцільним є застосування підходу, за якого інформація про приватне життя та персональні дані співвідносяться як «ціле та частина» відповідно. Це можна обґрунтувати тим, що:

- 1) за допомогою анкетних даних можна отримати будь-яку іншу інформацію, наприклад, за місцем проживання є можливість визначити у яких відносинах перебувають особи, якщо відомі відомості про декількох людей, як і відбувається з відомими людьми (намагання встановити родинні зв'язки);

2) за ПІБ та датою народження завдяки інтернет-ресурсам та телефонним довідникам також можна встановити родинні зв'язки між особами або встановити їх місце проживання.

Завдяки напрацюванням правової доктрини та законодавчому забезпеченню можна дійти висновку, що поняття та значення персональних даних необхідно досліджувати та удосконалювати із урахуванням розвитку новітніх технологій, оскільки тільки у тому разі можна забезпечити їх ефективний захист.

Враховавши здобутки вчених та нормативне визначення персональних даних, можна дійти висновку, що персональні дані – це будь-яка інформація, що містить відомості про особу, яка ідентифікована або може бути конкретно ідентифікована у будь-який спосіб та потребує особливого правового захисту.

1.2 Нормативно-правове регулювання сфери захисту персональних даних в Україні

На сьогодні вітчизняна нормативно-правова база у сфері захисту персональних даних частково відповідає міжнародним стандартам, оскільки у травні 2018 року відбулась зміна законодавства країн ЄС у сфері захисту персональних даних, звідси і зміна використовуваної термінології, та з удосконаленням та впровадженням новітніх технологій, вона має поступово оновлюватись, оскільки суб'єкти персональних даних потребують постійного додаткового захисту.

На нашу думку, необхідним є визначити, що законодавство України є основою національної моделі сфери захисту персональних даних – системи методів, прийомів та способів, завданням якої є регулювання відносин у сфері захисту персональних даних, з метою дотримання права на повагу до особистого та сімейного життя.

Згідно з Конституцією України ніхто не може зазнавати втручання в його особисте та сімейне життя, крім випадків, передбачених цією ж Конституцією [1]. Наразі однією з найбільш частих підстав для втручання в особисте та

сімейне життя є вчинення кримінального правопорушення, особливо, якщо це стосується сфери національної безпеки та злочинів проти життя та здоров'я людини.

На думку Л. Ємчук, статті 31 та 32 Конституції України є саме тими нормами, які безпосередньо стосуються захисту персональних даних. Автор також визначає, що право на повагу до особистого життя регулює такі правові відносини, які пов'язані із захистом і обробкою персональних даних [19].

Так, Конституційний Суд України у своєму Рішенні, яке було прийнято 20.01.2012 р. вказав, що інформацією про особисте та сімейне життя особи є відомості та/або дані щодо відносини майнового та немайнового характеру, обставини, події, стосунки тощо, пов'язані з конкретною особою, її сім'єю, винятком є передбачена законами інформація, що стосується здійснення службовою особою. Також було зауважено, що така інформація є конфіденційною, а будь-які дії з конфіденційною інформацією про особу без її згоди державою, органами місцевого самоврядування, юридичними або фізичними особами є втручанням в її особисте та сімейне життя. Таке втручання є допустимим лише у випадках, визначених законом в інтересах національної безпеки, економічного добробуту та прав людини [15].

Відома практика Європейського суду з прав людини щодо порушення права на повагу до приватного і сімейного життя. Одним з яскравих прикладів якої є справа «Заїченко проти України» від 26.02.2015. У справі вирішувалось питання щодо законності дій органів внутрішніх справ під час збирання відомостей про стан здоров'я заявника, що не було необхідними по суті справи.

Не дивлячись на те, що Конституцією не передбачено спеціально визначеного права на захист персональних даних, це не є перешкодою для визнання цього права предметом конституційного захисту, оскільки такий захист передбачений наукою положень 2 розділу Основного Закону [18].

Законом України «Про захист персональних даних» від 01.06.2010 визначаються також суб'єкти відносин, пов'язаних із персональними даними:

суб'єкт, володілець, розпорядник персональних даних; третя особа; Уповноважений Верховної Ради з прав людини.

Суб'єкт персональних даних – особа, яка надає персональні дані, які у подальшому підлягають обробці. Його права та особисті інтереси найбільше охороняються законом, оскільки він надає відомості, що входять до права на повагу до особистого та сімейного життя.

Володілець персональних даних – особа, яка встановлює мету обробки персональних даних, склад цих даних, а також процедури їх обробки, якщо інше не визначено законом.

Розпорядник персональних даних – особа, якій володілець персональних даних надав право обробляти отримані персональні дані [9].

На нашу думку, останні дві категорії несуть підвищену юридичну відповідальність, оскільки мають дотримуватись міжнародних засад та правил обробки персональних даних. Неправильно визначена мета обробки персональних даних, надмірна їх кількість або розповсюдження відомостей про особу є підставами притягнення до відповідальності.

Третя особа – будь-яка інша особа, яка не є суб'єктом, володільцем, розпорядником персональних даних або Уповноваженим Верховної Ради України з прав людини. Розповсюдження відомостей, які надав суб'єкт персональних даних третім особам не допускається.

Законодавче забезпечення сфери захисту персональних даних складають понад 20 нормативних актів, серед яких є як закони, так і підзаконні акти, зокрема Закон України «Про захист персональних даних», Наказ Міністерства юстиції України «Про затвердження форм заяв про реєстрацію бази персональних даних та про внесення змін до відомостей Державного реєстру баз персональних даних і порядку їх подання», Наказ Уповноваженого Верховної Ради України з прав людини «Про затвердження документів у сфері захисту персональних даних» та інші.

Якщо звернути увагу на термінологію, що застосовується у Законі України «Про захист персональних даних» та Загальному регламенті про захист

даних (Регламенті Європейського Парламенту і Ради (ЄС), який був прийнятий 27.04.2016, можна дійти висновку, що її необхідно скорегувати відповідно до вищевказаного Регламенту для уникнення колізій.

Загалом, національна модель захисту сфери персональних даних потребує удосконалення для відповідності міжнародним вимогам та стандартам. Законодавством із захисту персональних даних мають бути забезпечені найважливіші сфери суспільного життя, зокрема, трудові та цивільні правовідносини; правовідносини, що виникають у зв'язку з притягненням особи до юридичної відповідальності та інші.

1.3 Основоволожні засади захисту персональних даних за чинними міжнародними актами та договорами

Основою для захисту конфіденційної інформації, що входить до категорії персональні дані, у європейській спільноті стало прийняття Конвенції про захист прав людини і основоположних свобод у 1950 році. Стаття 8 вищезазначеного Акту визначає, що кожна людина має право на повагу до житла і кореспонденції, свого приватного і сімейного життя. Також Конвенція надає можливість втручатися у здійснення цього права органам державної влади відповідно до закону лише у випадках, коли це є необхідністю у демократичному суспільстві в інтересах національної та громадської безпеки, економічного добробуту держави, а також для запобігання протиправним діям чи злочинам, для захисту здоров'я та моралі або для захисту прав і свобод інших осіб [4].

Продовженням підтримки ідеї, що була закладена у Конвенції, для міжнародного захисту персональних даних стало прийняття Міжнародного пакту про громадянські та політичні права 1966 року. Відтоді захист персональних даних увійшов до складу права на приватність і стало прийнятим, що ніхто не може зазнавати свавільного втручання у його особисте та сімейне життя, заборону свавільного або незаконного втручання до його житла або

посягань на таємницю кореспонденції, а також гарантується захист від такого втручання або посягань [3].

Пізніше подібна норма була відтворена вже у Конвенції про права дитини 1989 року, де об'єктом захисту стає право на приватність життя дитини [2].

Після отримання персональних даних органами державної влади, зокрема і правоохоронними органами, наступним етапом є їх обробка, саме цей процес найбільше охороняється міжнародними нормами та національним законодавством.

Міжнародною спільнотою сформовано декілька основоположних засад, відповідно до яких повинна здійснюватись обробка персональних даних, а саме: законності та справедливості; точності (достовірності), актуальності персональних даних; склад та зміст персональних даних мають бути відповідними, адекватними та ненадмірними стосовно встановленої мети їх обробки [13].

Законності та справедливості. Згідно з цією засадою, обробка персональних даних повинна відбуватись лише на законних підставах та у тій мірі, яка потрібна для встановлення необхідної інформації. Будь-яке незаконне та безпідставне отримання конфіденційної інформації про особу є недопустимим та має наслідком юридичну відповідальність.

Точності (достовірності), актуальності персональних даних. Інформація, що становить персональні дані, має надаватися своєчасно та достовірно. На практиці, наприклад, під час проходження конкурсу на посади державного службовця у нашій державі, громадяни беруть на себе обов'язок своєчасно надавати інформацію у разі зміни персональних даних, що є необхідними.

Склад та зміст персональних даних мають бути відповідними, адекватними та ненадмірними стосовно встановленої мети їх обробки [13].

На сьогодні цей принцип не є достатньо розвиненим навіть у практиці

Європейського суду з прав людини, часом, навіть вимоги, що містяться у нормативних актах не завжди можуть гарантувати ненадмірність затребуваної інформації. Так, у справі «Гардель проти Франції» заявник звернувся зі скаргою після вчинення ним зґвалтування, оскільки на той час було прийнято закон про створення Реєстру осіб, які вчинили статеві злочини. Він вважав, що внесення відомостей про нього до Реєстру не є необхідним та пропорційним, проте ЄСПЛ не визнав, що відбулось порушення прав заявника.

Розглядаючи останній принцип, що включає такі слова як «адекватність», «відповідність» та «ненадмірність», можуть виникнути питання щодо їх значення та співвідношення саме у сфері захисту персональних даних. Дані категорії співвідносяться як «зміст», «актуальність» та «кількість» відповідно. Вони доволі близькі за значенням, тому є доцільним їх комплексне використання.

Під «адекватністю» розуміється змістовне наповнення отриманої інформації, що становить персональні дані. Тобто, на конкретний запит про отримання персональних даних має надаватись повна відповідь.

Відповідність стосується актуальності персональних даних у конкретному проміжку часу, тобто на запитувану інформацію мають надаватись відповідні до питання актуальні дані.

Ненадмірність включає в себе затребування лише тієї кількості інформації, яка необхідна для вчинення конкретного правочину або вирішення справи.

Наразі принципи, які закріплені у міжнародних актах, імплементовано у національне законодавство, це підтверджується їх наявністю у статті 6 Закону України «Про захист персональних даних» [9]. Проте їх нормативного закріплення недостатньо, вбачаємо за необхідне звернути увагу на їх практичне виконання та дотримання, особливо при проведенні оперативно-розшукової роботи правоохоронними органами.

РОЗДІЛ 2. ЗАРУБІЖНИЙ ДОСВІД ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

2.1 Забезпечення захисту персональних даних у деяких країнах Європи

Велике значення у сфері захисту персональних даних для держав-учасників Європейського Союзу мала Директива Ради Європи 95/46/ЄС, яка була прийнята у 1995 році [8]. Не зважаючи на те, що вона була прийнята майже 15 років тому, до травня 2018 року залишалась провідним актом для захисту прав і особистих інтересів фізичних осіб у сфері використання їх персональних даних. На сьогодні цей документ не є частиною українського законодавства, проте враховуючи європейський вектор розвитку нашої держави та проаналізувавши зміст Акту, можна дійти висновку, що норми Директиви було враховано при прийнятті Закону України «Про захист персональних даних».

Європейська спільнота завжди намагалась удосконалити свою нормативну базу для того, щоб вона відповідала розвитку сучасних технологій, її реформування тривало з 2012 року, наслідком якого стало прийняття General Data Protection Regulation (Загального регламенту про захист даних) (далі – Регламент), який почав застосовуватись з 28 травня 2018 року [14]. Дія цього документу поширюється на всіх держав-учасниць Європейського Союзу та може розповсюджуватись також і на інших осіб, які вступають із ними у правовідносини. Основною метою прийняття Регламенту було:

- 1) уніфікація та систематизація законодавства ЄС у сфері захисту персональних даних;
- 2) створення додаткового захисту для персональних даних, що надаються фізичними особами;
- 3) посилення вимог для притягнення до відповідальності відповідальних осіб.

З прийняттям Регламенту згода осіб на обробку персональних даних має бути чітко визначеною та прямою. Однією з новел є також можливість «відкликати свою згоду на обробку даних» за суб'єкта персональних даних у

будь-який час. Вважаємо, що це доволі дискусійна норма, оскільки використовуючи «право на забуття» враховуються лише інтереси суб'єкта персональних даних.

Законодавство деяких європейських держав здійснює поділ персональних даних за критерієм їх «чутливості» (див. Додаток 1):

1) дані загального характеру, до яких входять: ПІБ, дата і місце народження, громадянство, місце проживання;

2) «чутливі» або вразливі, до них можна віднести: інформація про стан здоров'я, відбитки пальців, дані про наявність судимості, відомості про етнічну належність, ставлення до релігії тощо [18].

Поділ за цим критерієм дозволяє встановлювати для «чутливої» категорії додаткові засоби захисту, що є доцільним для уникнення дискримінації за будь-якою із підстав для її виникнення.

2.2 Законодавче врегулювання захисту персональних даних у Сполучених Штатах Америки

Захист персональних даних у Сполучених Штатах Америки регламентується великою кількістю нормативно-правових актів задля забезпечення кожної сфери суспільного життя. Використання такого цілісного підходу дає змогу більш упевнено гарантувати захист сфери персональних даних.

Політика США у сфері захисту персональних даних базується на тому, що заволодіння персональними даними іноземними державами або будь-якими організаціями загрожує державній безпеці та громадянам. Завдяки цьому держава зосереджує якомога більше зусиль для забезпечення конфіденційності своїх громадян.

Банківська та фінансова сфери має додаткові гарантії конфіденційності фінансових запитів за допомогою The Right to Financial Privacy Act (Закону «Про право на фінансову приватність»), який був прийнятий 1978 року. Також

вказаний Закон встановлює заборону надання конфіденційної інформації, окрім як на вимогу суду або іншого адміністративного органу.

Центральним керівним органом, який забезпечує безпеку у сфері обробки персональних даних є Агентство національної безпеки. Воно входить до структури Міністерства оборони США та виконує одночасно такі найбільш важливі функції, як забезпечення і контроль збору та аналізу іноземної розвідувальної інформації, а також захист інформаційних систем і комп'ютерних мереж Уряду США.

На відміну від української національної моделі захисту персональних даних, в США доволі багато приділяється уваги захисту конституційних прав і свобод людини в мережі Інтернет. Важливим чинником у сфері забезпечення захисту персональних даних громадян стало прийняття Закону «Про захист приватної інформації про особу». Згодом ідею було продовжено прийняттям Закону «Про захист онлайнових персональних даних дітей», завдяки цьому було заборонено збирати персональні дані дітей віком до 13 років без згоди на це їх батьків. Це надає змогу убезпечити дітей від несанкціонованого втручання в особисте життя сторонніх осіб. Будь-який ресурс, доступ до якого має дитина, в обов'язковому порядку має подавати державним органам інформацію з відомостями про те, з якою метою збираються персональні дані [22].

Враховуючи досвід США, для захисту права на повагу до особистого та сімейного життя у просторах мережі Інтернет у нашій державі є необхідним:

- 1) оновлення законодавчої бази у сфері захисту персональних даних для користувачів мережі Інтернет;
- 2) обмеження доступу дітей до інтернет-ресурсів, метою яких є збір персональних даних у зв'язку з тим, що дитина може не володіти достатньою кількістю необхідних знань для того, щоб захистити себе від неправомірного заволодіння інформацією про неї ;
- 3) запровадити обмежувальні заходи для соціальних мереж щодо обробки персональних даних;

4) створення контролюючих органів за дотриманням законодавства у сфері захисту персональних даних.

Таким чином, можна зменшити кількість інтернет-шахрайств та підвищити рівень безпеки користувачів мережі Інтернет. Проте, дані заходи не можуть гарантувати захист від вірусних посилань, що мають змогу зчитувати інформацію, яка може становити персональні дані.

РОЗДІЛ 3. ПРОБЛЕМНІ ПИТАННЯ ТА ШЛЯХИ ЇХ ВИРІШЕННЯ У СФЕРІ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ПІД ЧАС ДІЯЛЬНОСТІ ПРАВООХОРОННИХ ОРГАНІВ

3.1 Проблематика законодавчого забезпечення та практики у регулюванні діяльності правоохоронних органів

Законодавче забезпечення сфери захисту персональних даних у загальному розумінні відповідає встановленим принципам і нормам міжнародного права, але не повною мірою. Однією із таких сфер, яка потребує законодавчого вдосконалення, є захист персональних даних під час діяльності правоохоронних органів, оскільки для успішного виконання своєї роботи їм доводиться працювати із інформацією, що становить персональні дані.

Типовими для правоохоронних органів є проведення слідчих (розшукових) та негласних слідчих (розшукових) дій. Під час проведення останніх, звичною справою є таємне збирання конфіденційної інформації. Враховуючи той факт, що відомості про стан здоров'я, зразки відбитків пальців відносяться до «чутливої» категорії персональних даних, звертаємо увагу, що детально регламентованих рекомендацій та вказівок не вбачається щодо збирання та зберігання, наприклад, дактилокарток, біологічних матеріалів чи зразків ДНК [7].

Будь-яке втручання в особисте та сімейне життя, проведення різних операцій з персональними даними особи проводяться із конкретних підстав, а також з мотивів захисту національної безпеки й забезпечення прав людини і громадянина за наявності вмотивованого рішення суду. Якщо виникає необхідність, кожен громадянин може вільно звертатися до органів державної влади, місцевого самоврядування, установ і організацій з запитом щодо ознайомлення з відомостями про себе, що не становлять державну або захищену законом таємницю [1]. Таким чином держава забезпечує реалізацію права на повагу до особистого та сімейного життя, а також права на

інформацію. Подібні заходи також допомагають своєчасно оновлювати бази даних та попереджують потрапляння до них недостовірної інформації.

Процедури доступу до персональних даних, їх збирання, обробка та розповсюдження мають бути суворо передбачені чинним законодавством, а особливо у випадках, коли вони містять інформацію, що має значення для визначення причетності особи до скоєння злочину. Зазвичай, це особиста інформація, яка охороняється Конституцією України.

Закон не регламентує чіткий порядок проведення заходів щодо формування відповідних баз, проте вказує на можливість їх проведення, що може стати причиною порушення права на повагу до особистого та сімейного життя. Ситуація з відсутністю поетапної регламентації проведення операцій із персональними даними стала підґрунтям для звернення Уповноваженого Верховної Ради України з прав людини Валерії Лутковської до Конституційного суду України з поданням щодо відповідності Конституції України (конституційності) положень частини другої статті 26 Закону України «Про національну поліцію» [12].

Враховуючи європейський вектор розвитку України, омбудсмен у якості переконливих аргументів щодо необхідності деталізації порядку обробки персональних даних наводить практику Європейського суду з прав людини та законодавство країн ЄС.

Серед причин порушення законодавства у сфері захисту персональних даних правоохоронними органами та їх посадовими особами слід зазначити:

- 1) недостатнє нормативно-правове регулювання діяльності правоохоронних органів щодо збирання, зберігання та використання персональних даних;
- 2) відсутній порядок підстав для притягнення до відповідальності за розголошення відомостей, що входять до персональних даних;
- 3) недостатня досвідченість правоохоронних органів у сфері захисту персональних даних;
- 4) відсутність електронного обліку доступу до персональних даних;

- 5) умисне розголошення відомостей, що становлять персональні дані;
- 6) відсутність посад, основною метою створення яких був би облік та контроль доступу до персональних даних.

Враховуючи виявлені недоліки та подання Уповноваженого Верховної Ради України з прав людини до Конституційного Суду України, наявність прогалин у законодавстві, варто зауважити, що чинна нормативно-правова база держави потребує вдосконалення та доповнення у сфері захисту персональних даних під час діяльності правоохоронних органів, оскільки за сучасних умов вона є однією з найбільш уразливих. Новостворені норми мають детально регламентувати кожную дію, пов'язану із обробкою персональних даних та передбачати процедуру притягнення до відповідальності службових осіб у разі бездіяльності у сфері захисту таких. Перспективи вирішення проблем законодавчого забезпечення під час діяльності правоохоронних органів розглянуто у підрозділі 3.2.

3.2 Перспективи удосконалення сфери захисту персональних даних

Правоохоронна діяльність не може здійснюватись без збирання, зберігання, обробки та використання персональних даних, адже це є невід'ємною складовою їх діяльності, особливо під час проведення слідчих (розшукових) дій.

Враховуючи недосконалість нормативної бази для правоохоронних органів у сфері захисту персональних даних, є необхідним введення єдиних стандартів щодо процесу обробки персональних даних. Для того, щоб уніфікувати процес збору інформації та подальші дії із отриманими матеріалами, є необхідним запровадження Типових інструкцій для окремого правоохоронного органу відповідно.

Обов'язково у типових інструкціях мають бути передбачені наступні пункти:

- 1) підстави та порядок збору інформації про суб'єкта персональних даних, якщо це біологічні матеріали – порядок забору таких із детальною регламентацією дій;
- 2) перелік уповноважених органів (осіб), що можуть здійснювати такий збір та забір та перелік документів, що можуть посвідчувати такий дозвіл;
- 3) підстави та порядок доступу до персональних даних третіми особами;
- 4) порядок призначення відповідальних осіб за процес обробки та збереження персональних даних;
- 5) порядок обліку інформації, що містить персональні дані та місце, де така інформація повинна зберігатися (картотеки, архів тощо);
- 6) порядок знищення інформації, що містить персональні дані;
- 7) порядок притягнення до відповідальності осіб, якими було порушено законодавство у сфері захисту персональних даних.

При створенні проектів типових інструкцій для правоохоронних органів необхідно враховувати специфіку окремого правоохоронного органу.

Порядок збирання та надання доступу третім особам до персональних даних, що містяться у базах даних правоохоронних органів, має бути однаковим за будь-яких умов для кожної з категорій, окрім інформації з обмеженим доступом.

Типові інструкції мають відповідати вимогам, зазначеним у ст. 5 Конвенції Про захист осіб у зв'язку з автоматизованою обробкою персональних даних. Враховуючи той факт, що бази даних мають лімітований обсяг для зберігання інформації, то вважаємо за необхідне встановити обмежений час зберігання відомостей, що становлять персональні дані. Також, дотримуючись міжнародних принципів та стандартів у сфері захисту персональних даних, такі заходи нададуть додаткових гарантій для дотримання права на повагу до особистого та сімейного життя [3].

Керуючись Законом України «Про оперативно-розшукову діяльність», для зручності варто виділити наступні категорії населення для визначення порядку та терміну *зберігання* персональних даних:

1) свідки, очевидці злочину та близькі родичі особи, що скоїла злочин, а також особи щодо яких було закрито кримінальне провадження. Такі особи мають обов'язково надати згоду для збирання, зберігання та використання їх персональних даних. Термін зберігання такої інформації – до кінця стадії судового розгляду (у т.ч. апеляційного та касаційного перегляду) кримінального провадження. Якщо судом буде виключено можливість виникнення підстав для відкриття провадження за нововиявленими обставинами. У подальшому зберіганні таких даних немає необхідності, тому інформація має бути знищена та виключена із баз даних.

2) особи, яких було засуджено вперше за злочини невеликої або середньої тяжкості, щодо яких судимість була знята або погашена відповідно до чинного законодавства. Враховуючи доволі невелику суспільну небезпечність таких осіб, доцільним було б зберігати інформацію щодо них протягом 1 року з дня зняття або погашення судимості. Варто вважати, що це є найбільш оптимальний термін для зберігання інформації, оскільки, зазвичай, такі злочини вчиняються з необережності та цього часу буде достатньо для того, щоб установити чи виправилась особа.

3) особи, яких було засуджено вперше за тяжкі або особливо тяжкі злочини, щодо яких судимість була знята або погашена відповідно до чинного законодавства. Така категорія населення є потенційно небезпечною та є ризик виникнення рецидиву, тому зберігання даних протягом деякого часу є необхідним у рамках превенції наступних злочинів, а у разі скоєння таких – для полегшення роботи правоохоронних органів. Оптимальним терміном зберігання інформації в базах даних про таких осіб є 3 роки, оскільки, на відміну від попередньої групи, зазначена з імовірно більшим ризиком, що особи після відбування/виконання покарання не зможуть ресоціалізуватися та повернутися до попереднього способу життя.

4) особи, щодо яких було винесено два або більше обвинувальних вироків протягом життя за будь-які види злочинів. Дана категорія населення є небезпечною, що підтверджено наявністю рецидивів. Є висока ймовірність того, такі випадки будуть повторюватись, тому є необхідність у постійному або довготривалому (понад 15 років) зберіганні відомостей про таких осіб у базах даних.

5) категорії справ, які залишаються нерозкритими, варто розмежувати, керуючись ст. 49 Кримінального кодексу України, у якій встановлені терміни звільнення особи від кримінальної відповідальності у зв'язку із закінченням строків давності. Варто виокремити такі строки зберігання персональних даних: а) 2 роки - у разі вчинення злочину невеликої тяжкості, за який передбачено покарання менш суворе, ніж обмеження волі ; б) 3 роки - у разі вчинення злочину невеликої тяжкості , за який передбачено покарання у вигляді обмеження або позбавлення волі; в) 5 років - у разі вчинення злочину середньої тяжкості (ч. 1.ч. 2 ст. 191 КК України); г) 10 років - у разі вчинення тяжкого злочину (ч. 3 , ч. 4. ст. 191 КК України); д) 15 років - у разі вчинення особливо тяжкого злочину (ч. 5 ст. 191 КК України) [6].

Обов'язковим також є оновлення баз персональних даних, що потребує додаткового фінансування з боку держави. З використанням досвіду США є необхідним запровадження нової системи захисту баз персональних даних для того, що забезпечити їх збереження та унеможливити несанкціонований доступ до них, це сприятиме підвищенню рівня безпеки держави та захисту гарантованих Конституцією прав і свобод.

ВИСНОВКИ

Останні декілька десятиліть відбувається активна інформатизація суспільства, впровадження передових технологій, збільшення кількості соціальних мереж, звідси і виникає потреба у додатковому забезпеченні захисту персональних даних. З конституційного погляду, захист персональних даних виступає гарантією забезпечення реалізації права на повагу до особистого та сімейного життя.

Персональні дані – це будь-яка інформація, що містить відомості про особу, яка ідентифікована або може бути конкретно ідентифікована у будь-який спосіб та потребує особливого правового захисту.

Забезпечення захисту персональних даних є однією з гарантів реалізації права на повагу до особистого та сімейного життя, оскільки це право може бути порушеним за умови, що відомий суб'єкт володіння цим правом. Зарубіжний досвід свідчить про те, що для забезпечення вищезгаданого права необхідно використовувати комплексний підхід, який допоможе захистити інтереси людини та держави.

Систему національного законодавства у сфері захисту персональних даних становить понад 20 законодавчих актів, які потребують часткового оновлення, зокрема у частині термінології, що використовується у Загальному регламенті про захист даних, хоча це не є обов'язковим, проте значно полегшить його застосування суб'єктами господарювання при співпраці із членами ЄС. Особливу увагу варто звернути на законодавче забезпечення, що регламентує діяльність правоохоронних органів під час обробки персональних даних.

Запровадження досвіду США у сфері захисту персональних даних користувачів соціальних мереж та інтернет-ресурсів є необхідним в Україні. Правова неосвіченість громадян, а в особливості дітей, може загрожувати захисту конституційних прав і свобод, оскільки доволі часто користувачам доводиться заповнювати електронні анкети, вказувати відомості при реєстрації,

що може мати наслідком неправомірне заволодіння відомостями про особу та загрожує реалізації права на повагу до особистого та сімейного життя.

Для ефективної діяльності правоохоронних органів та одночасного забезпечення захисту персональних даних є необхідним запровадження Типових інструкцій, які б приймалися єдиним законом. Такі інструкції мають встановлювати: підстави та порядок збору інформації про суб'єкта персональних даних, якщо це біологічні матеріали – порядок забору таких із детальною регламентацією дій; перелік уповноважених органів (осіб), що можуть здійснювати такий збір та забір та перелік документів, що можуть посвідчувати такий дозвіл; підстави та порядок доступу до персональних даних третіми особами; порядок призначення відповідальних осіб за процес обробки та збереження персональних даних; порядок обліку інформації, що містить персональні дані та місце, де така інформація повинна зберігатися (картотеки, архів тощо); порядок знищення інформації, що містить персональні дані; порядок притягнення до відповідальності осіб, якими було порушено законодавство у сфері захисту персональних даних.

Підсумовуючи вищевикладене, можна дійти висновку, що сфера захисту персональних даних має бути якісно захищеною не лише від неправомірного використання інформації державними органами, а і від протиправних посягань осіб, які можуть отримати доступ до баз даних.

Захищеність персональних даних залежить не тільки від стану законодавства, а і від його практичної реалізації. Для того, щоб сфера захисту персональних даних була достатньо стійкою, необхідним є:

- 1) належне фінансування суб'єктів, які відповідають за обробку персональних даних;
- 2) оновлення систем електронного захисту баз даних;
- 3) підготовка висококваліфікованих спеціалістів, які зможуть надавати правову допомогу та консультації у сфері захисту персональних даних;
- 4) співпраця із провідними державами для отримання позитивного досвіду.

Для успішної реалізації реформування сфери захисту персональних даних варто реалізувати комплексний підхід, який поєднав би у собі усучаснене законодавче забезпечення та ефективну політику з його активної реалізації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Конституція України : Закон України від 28.06.1996 р. № 254к/96-ВР. URL: <http://zakon5.rada.gov.ua/laws/show/254к/96-вр> (дата звернення: 18.09.2018).
2. Convention on the Rights of the Child of 20.11.1989. URL: <https://www.ohchr.org/en/professionalinterest/pages/crc.aspx> (last accessed: 21.10.2018).
3. European Convention on Human Rights of 04.11.1950. URL: https://www.echr.coe.int/Documents/Convention_ENG.pdf (last accessed: 20.10.2018).
4. International Covenant on Civil and Political Rights of 16.12.1966. URL: <https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx> (last accessed: 20.10.2018).
5. The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108) URL: <https://rm.coe.int/1680078b37> (last accessed: 19.09.2018).
6. Кримінальний кодекс України : Закон України від 05.04.2001р. № 2341-III. URL: <http://zakon.rada.gov.ua/laws/show/2341-14> (дата звернення: 20.09.2018).
7. Кримінальний процесуальний кодекс України : Закон України від 13.04.2012 р. № 4651-VI. URL: <http://zakon.rada.gov.ua/laws/show/4651-17> (дата звернення: 18.09.2018).
8. Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних : Директива 95/46/ЄС Парламенту і Ради від 24.10.1995 р. № 994_242. URL: https://zakon.rada.gov.ua/laws/show/994_242 (дата звернення: 24.10.2018).
9. Про захист персональних даних : Закон України від 01.06.2010 р. № 2297-VI. URL: <http://zakon.rada.gov.ua/laws/show/2297-17> (дата звернення: 18.09.2018).

10. Про Національну поліцію : Закон України від 02.07.2015 р. № 580-VIII. URL: <http://zakon.rada.gov.ua/laws/show/580-19> (дата звернення 18.09.2018).

11. Про оперативно-розшукову діяльність : Закон України від 05.04.2001 р. № 2341-III. URL: <http://zakon.rada.gov.ua/laws/show/2135-12> (дата звернення 01.10.2018).

12. Щодо відповідності Конституції України (конституційності) положень частини другої статті 26 Закону України «Про національну поліцію» : Подання Уповноваженого Верховної Ради України з прав людини від 13.02.2017 р. URL: http://www.ccu.gov.ua/sites/default/files/ccu/5_422.pdf (дата звернення 01.09.2018).

13. Постановление ЕСПЧ по делу «Гардель против Франции». *Европейская конвенция о защите прав человека: право и практика*. URL: <http://www.echr.ru/documents/doc/12077726/12077726.htm> (дата обращения: 22.09.2018)

14. 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) : Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27.04.2016 р. №984_008-16. URL: https://zakon.rada.gov.ua/laws/show/984_008-16 (дата звернення: 01.11.2018).

15. Щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України : Рішення Конституційного Суду України від 20.01.2012 р. № 2-рп/2012. URL: <https://zakon.rada.gov.ua/laws/show/v002p710-12> (дата звернення: 21.11.2018)

16. Адвокат розповів, як має регламентуватися збір зразків ДНК : *Закон і Бізнес*, 2017. URL: http://zib.com.ua/ua/print/128054advokat_rozpoviv_yak_mae_reglamentuvatisya_zbir_zrazkiv_dnk.html (дата звернення 24.09.2018).

17. Віткова В. С. Право на доступ до інформації у рішеннях Європейського суду з прав людини. *Правові та інституційні механізми забезпечення розвитку України в умовах європейської інтеграції* : матеріали

Міжнародної науково-практичної конференції (м. Одеса, 18 травня 2018 р.) У 2-х т. Т. 1. Одеса, 2018. С. 260-262.

18. Головченко В. Правові основи захисту персональних даних. URL: <http://jur-gazeta.com/publications/practice/inshe/pravovi-osnovi-zahistu-personalnih-danih.html> (дата звернення: 22.10.2018).

19. Ємчук Л. В. Конституційно-правове регулювання особистого та сімейного життя людини і громадянина. URL: <https://www.uzhnu.edu.ua/uk/infocentre/get/7948> (дата звернення: 24.09.2018).

20. Єсімов С. С. Захист персональних даних у контексті розвитку динамічних інформаційних систем. URL: http://www2.lvduvs.edu.ua/documents_pdf/visnyky/nvsvy/03_2013/13yessdis.pdf (дата звернення: 24.09.2018).

21. Обуховська Т. І. Захист персональних даних в умовах розвитку інформаційного суспільства: передумови, принципи та міжнародне законодавство. URL: <http://visnyk.academy.gov.ua/wp-content/uploads/2014/05/2014-1-17.pdf> (дата звернення: 30.10.2018).

22. Речицький В. В. Проект Конституції України – 2009. Перспектива прав людини. URL: <http://library.khpg.org/files/docs/1243605312.pdf> (дата звернення: 02.12.2018)

23. Теремецький В. І., Цвірюк Д. В. Застосування зарубіжного досвіду правового захисту персональних даних в Україні. *Часопис академії адвокатури України*. Т.7, 2014. С. 73-82.

АНОТАЦІЯ

Актуальність теми. Актуальність обраної теми зумовлена низьким рівнем правової освіченості громадян у сфері захисту персональних даних. З кожним роком обіг інформації збільшується, полегшується доступ до інтернет-ресурсів, а отже є ймовірність того, що будь-хто може неправомірно заволодіти інформацією про ту, чи іншу особу, якщо не вживати засобів захисту.

Метою даної роботи є вивчення та узагальнення знань про сферу захисту персональних даних, зокрема під час діяльності правоохоронних органів; виявлення недоліків законодавчого забезпечення із захисту персональних даних та встановлення шляхів їх усунення; аналіз законодавчого забезпечення сфери захисту персональних даних у зарубіжних країнах.

Для успішного досягнення поставленої мети має бути виконано такі **завдання**: 1) дослідити поняття та ознаки персональних даних; 2) нормативно-правове регулювання сфери захисту персональних даних; 3) визначити принципи обробки персональних даних у міжнародній практиці та за законодавством України; 4) розглянути законодавчі гарантії заходів захисту персональних даних у зарубіжних країнах; 5) виявити проблеми законодавчого забезпечення та практичної спрямованості сфери захисту персональних даних; 6) визначити перспективи вдосконалення сфери захисту персональних даних під час діяльності правоохоронних органів.

Методологічну основу даного дослідження становить система загальнонаукових та спеціально-наукових методів: 1) метод структурного аналізу і синтезу використовувався для поділу отриманої інформації на окремі структурні одиниці та системне поєднання різних сторін інформації в єдину структуровану систему на прикладі принципів обробки персональних даних; 2) порівняльно-правовий метод лежить в основі встановленні відмінних та подібних рис комплексних заходів щодо захисту персональних даних у різних країнах; 3) моделювання та прогнозування полягає у приблизному створенні та уявленні моделі заходів щодо захисту сфери персональних даних; 4) системний підхід — полягає у визначенні окремих заходів забезпечення захисту

персональних даних як нерозривної системи, зокрема, на прикладі заходів із захисту персональних даних.

Структура роботи. Загальний обсяг становить 34 сторінки. Роботу складають вступ, три розділи, сім підрозділів, висновки, список використаних джерел (23 найменування) та один додаток.

ДОДАТКИ

Додаток 1.

