УДК 316.324.8

БРИЖКО В.М., *доктор філософії (Ph.D.) з юридичних наук, с.н.с.*
ORCID: https://orcid.org/0000-0002-3941-1013.
ПИЛИПЧУК В.Г., *доктор юридичних наук, професор,*
член-кореспондент НАПрН України.

ПРИВАТНІСТЬ, КОНФІДЕНЦІЙНІСТЬ ТА БЕЗПЕКА ПЕРСОНАЛЬНИХ ДАНИХ

Анотація. *У статті розглядаються окремі проблеми стану та формування правових основ системи захисту персональних даних в умовах євроінтеграції України у контексті застосування поняття "приватність людини" як фактору, який визначає основу інформаційної безпеки демократичного суспільства. Формулюються окремі пропозиції в плані можливого вдосконалювання сучасного законодавства.*

Ключові слова: *приватність, захист та безпека персональних даних, кіберзлочинність.*

Summary. *The article deals with certain problems of the state and formation of the legal foundations of the personal data protection system in the conditions of European integration of Ukraine in the context of the application of the concept of "human privacy" as a factor that determines the basis of information security of a democratic society. Proposals are formulated in terms of possible improvement of current legislation.*

Keywords: *privacy, protection and security of personal data, cybercrime.*

Аннотация. *В статье рассматриваются отдельные проблемы состояния и формирования правовых основ системы защиты персональных данных в условиях евроинтеграции Украины и в контексте применения понятия "приватность человека" как фактора, который определяет основу информационной безопасности демократического общества. Формулируются отдельные предложения в плане возможного совершенствования современного законодательства.*

Ключевые слова*: приватность, защита и безопасность персональных данных, киберпреступность.*

Постановка проблеми. Необхідність створення умов захисту людини в контексті використання її персональних даних іншими людьми та суб'єктами влади з правового погляду досліджувалася та визначалася протягом значного історичного часу. Це пов'язано з поступовим і доволі тривалим становленням конституційних прав людини та спрямованості на формування правових засад недоторканності приватного життя.

Важливим при цьому є те, що особиста свобода невід'ємна від небезпеки. І справа по обмеженню свободи, з одного боку, є справою зміцнення безпеки людини, а з іншого – визначається потребами національної безпеки держави. Захист, хочемо ми цього чи ні, це обмеження, встановлені законом. Обмеження з боку правової держави мають сенс лише тоді, коли цими обмеженнями переслідується мета поставити перешкоди на шляху довільного поводження з правами людини.

Метою статті є узагальнення проблемних питань приватності, конфіденційності та безпеки персональних даних, а також визначення логічності зв'язків між ними.

Виклад основного матеріалу.

Приватність та інформаційна приватність. Життя, бажання, мрії та діяльність людини завжди пов'язані зі словосполученням "недоторканність особистого життя", еквівалент у застосуванні якого використовують у законодавстві США, англомовних країнах, публічних виданнях Європи та визначають терміном ***"privacy"***. Цей термін є

запозиченням з латинської мови слова “privaus” – “приватний”, “особистий” та трактується як: особистість, інтимність, таємність, самітність, власність, між особисті відносини [1].

Узгодженого уявлення та юридичного визначення поняття “privacy” немає. Зустрічаються його різні розуміння та тлумачення, зокрема: “особисте життя, право на приватне життя, недоторканність приватного життя, право на самоту” [2].

В української “Юридичної енциклопедії” “privacy” (укр. “прайвесі”) визначено як “приватна справа, таємниця, усамітненість” – правова категорія в англо-саксонській правовій системі , пов’язана із захистом інтимного життя людини [3].

В “Великому юридичному словнику” термін “privacy” тлумачиться як: “таємниця, самота, приватне життя” – особлива правова категорія, яка означає таємницю й недоторканність приватного життя, інтимну сферу людини. Термін може означати в одних випадках приватне життя, в інших – право на приватне життя, по-третє – право на захист недоторканності приватного життя і т.д.” [4].

У 1990 році, у Звіті Комітету Британії по конфіденційності та суміжних питань, було зазначено, що за результатами проведених досліджень трактувань “privacy” в рамках різних епох, культур та політичних систем “ніде не знайдено абсолютно прийнятного правового визначення цього поняття” [5].

Як уважається, історія *приватності* та безпосередньо пов’язаною з нею *конфіденційністю інформації* має більш як 3000 років, а у тому розумінні у якому її намагаються зрозуміти сьогодні – усього лише понад 150 років. Вона свідчить, що приватність раніше завжди була другорядною. На практиці потреба у виживанні часто затьмарювала бажання усамітнення. Не було класично-середньовічного латинського слова, еквівалентного “приватності”; було “privatio”, що визначалось як “відняти” [6].

Одне із тлумачень “privacy”, що часто використовується сьогодні, таке: приватність – це “право бути наданим самому собі”. Кожна людина має право на свій “куточок” у просторі, захищений від довільних зазіхань із боку [7].

Про “право бути наданим самому собі” вперше заговорили з 15 грудня 1890 року, коли американські юристи Луїс Брэндейс і Сэмюэль Уоррен опублікували в юридичному журналі Гарварда “Harvard Law Review” статтю “Право на приватність”. Вони писали, зокрема, що: “Інтенсивність і складність життя, пов’язані з розвитком цивілізації, сформували необхідність у самоті, і люди, під впливом культури, стали більш чутливим до публічності, через що самота й конфіденційність стали більш важливими для індивідуума; але сучасні підприємства й винаходи, вторгаючись в особисте життя людини, піддають його щиросердечному болю й стражданням, набагато більшим, ніж могли б заподіяти йому тілесні ушкодження” [8]. У подальшому, у 1928 р., суддя Луїс Брэндейс, який був вже членом Верховного суду США, стверджував що право на недоторканність приватного життя не можна ставити у залежність від способу, яким здійснюється отримання інформації про людину. Важливо не те, як технологічно або технічно здійснюється знімання інформації (зокрема, прослуховування), а те, що людина має право розраховувати на таємницю спілкування. Вказані думки формулювались у часи, коли слів інформатизація, телекомунікації, Інтернет, штучний інтелект тощо взагалі не існувало, і мова йшла лише про “особисту недоторканість” у звичайній, не віртуальній, життєдіяльності. Й хоча батько права на приватність Луїс Брэндейс випередив свій час, тоді його стаття та погляди не одержали великого поширення, а те висвітлення, яке мало місце в пресі, не було харцизьким та не дуже притягало до себе уваги.

Проте, у 1934 р. “право бути наданим самому собі” було узаконено Рішенням Конгресу США та увійшло до складу основних джерел права, які існують у англо-саксонській системі прецедентного права. Поштовхом цьому слугував, як вважаємо, розвиток технологій індустріалізації й, що важливо для розуміння процесів щодо нашого часу стосовно інформатизації, на тій же підставі, на якій вона зараз актуалізується: вторгнення вже новітніх технологій (раніше це стосувалося комерції з комплектування картотек щодо збирання та продажу адрес, відомостей ПІБ, переписки з поштових карток, телефону, відомостей з медичних книжок та ін.) в особисте життя й несанкціонований та комерційний продаж інформації про людину.

З правової точки, можливо, більш-менш точний сенс “privacy” – це *право на недоторканність приватного життя,* тобто *“право на себе”*, що спрямовано на можливість людини *“бути залишеною у спокої”*. Хоча зрозуміло, що такі визначення прийнятно для англо-саксонській прецедентної правовій системи, але занадто широкі для застосування у романо-германської системі щодо предметно-нормативної практиці, так як не визначають сутність ознак предметного захисту та не відповідають на питання – що для людини становить його втрата. Останнє важливо тому, що втрата або погіршення недоторканності приватного життя створює умови іншим здійснювати надмірну владу над психологічним, соціальним, економічним благополуччям та здоров’ям людини.

Сьогодні, в контексте уявлень про “privacy”, недоторканність приватного життя захищається ст. 12 Загальної декларації прав людини 1948 р., ст. 8, 12 Європейської Конвенції з прав людини та основоположних свобод 1950 р. та ст. 6-8, 11 Хартії основних прав Європейського Союзу 2000 р. та ін. міжнародно-правовими актами. Рішення Європейського Суду з прав людини постійно уточнюють сенс окремих формулювань.

Складовими приватного життя, що розглядалися з 1992 р. згідно із прецедентним правом у різних справах Європейського Суду із прав людини, є [9]:

- персональна ідентифікація. Визначалося, що це стосується зміни прізвища, реєстрації імен, а також зміни статі й внесення виправлень в акти цивільного стану;
- визначення законних зв’язків. Вказувалося, що важливою складовою приватного життя є доступ людини до інформації про своє минуле й свої родинні зв’язки, можливість не тільки встановлення, але й заперечування батьківства;
- фізична й моральна недоторканність. Визначалося, що обов’язкові медичні обстеження, примус до медичного й психіатричного лікування, фізичне насильство й відсутність юридичної можливості притягати винних до відповідальності, а також заборона на добровільну смерть і на аборт за медичними показниками можуть бути визнані втручанням у приватне життя;
- особистий простір. Розглядалися справи щодо “екологічних” прав людини, а також про публікацію світлин як інформації особистого змісту;
- збір і використання інформації. Визначалося, що сучасне суспільство неможливо уявити без систем спостереження, дактилоскопії, баз ДНК, офіційного перепису населення – уся зібрана в такий спосіб інформація, безумовно, стосується приватного життя;
- доступ до персональних даних. Мало місце рішення – незважаючи на те, що певна інформація може підлягати зберіганню, це не обов’язково означає, що особа, про яку вона зібрана, буде мати автоматичний доступ до неї;
- сексуальні відносини. Було рішення, що сексуальне життя окремої особи є частиною й важливим аспектом її особистого життя. Також заявники в Європейському Суді відстоювали своє право на гомосексуальні відносини, садомазохістську практику й публічну демонстрацію сексуальної поведінки;

• соціальна активність. Стосувалося можливості ефективної взаємодії з іншими людьми;

• професійні взаємини. На думку Суду, немає принципових підстав вважати, що поняття "приватного життя" виключає діяльність професійного та ділового змісту, саме у своїй роботі більшість людей мають значну, якщо не найбільшу, кількість шансів будувати відносини із зовнішнім світом.

Європейський Суд з прав людини також здійснив роботу з визначення недоторканності особистої переписки згідно ст. 8 Європейської Конвенції з прав людини та свобод 1950 р. Важливим є те, що Суд уточнив обставини, за яких державі дозволено порушити цю недоторканність, а також виробив стандарти перехоплення телефонних повідомлень (розмов), які підлягали захисту згідно з Конвенцією як "кореспонденція". Щоб перехоплення не було порушенням, воно має здійснюватися [10]:

1. "*На підставі закону*". Будь-яке спостереження має проводитися згідно національного закону, що має задовольняти наступні вимоги:

• доступність – громадянин повинен мати можливість переконатися, що прослуховування відповідає нормам закону;

• передбачуваність – громадянин повинен бути здатний (при необхідності за допомогою адвоката) передбачити наслідки будь-якої можливої дії;

• якість – закон повинен мати ефективні заходи проти можливих зловживань.

Зокрема, це означає, що закон має визначати:

- список злочинів, здійснення яких може призвести до прослуховування;

- обмежуватися випадками, коли фактичні підстави підозрювати особу в здійсненні тяжкого злочину вже виявлені іншими засобами;

- санкціонувати прослуховування тільки на підставі мотивованої письмової заяви високої посадової особи;

- дозволяти прослуховування тільки після одержання санкції органа або посадової особи, що не належить до виконавчої влади (судді);

- установлювати обмеження на тривалість прослуховування, із вказівкою періоду часу;

- визначати правила складання звітів щодо змісту прослуховування;

- обмежувати обмін матеріалами прослуховування між державними органами;

- визначати обставини, за яких записи прослуховування слід знищити;

- ухвалити рішення, що робити з матеріалами прослуховування, якщо обвинувачувану особу (жертву) буде виправдано. Будь-яка особа в країні, де діють положення про таємне прослуховування, може вимагати визнання себе жертвою без будь-якого обов'язку надавати докази про те, що спостереження дійсно велося.

2. *"Як необхідність у демократичному суспільстві"*. Прослуховування має бути:

• тільки такою мерою, яка необхідна для безпеки демократичних інститутів;

• за виняткових умов та в інтересах національної безпеки й/або попередження безладу або злочинів.

На думку закордонних спеціалістів, юридичне забезпечення права на приватність означає встановлення й дотримання меж припустимого втручання в будь-яке приватне життя, що виходить із таких наступних посилок [11]:

- границі між публічною і приватною сферами інтересів, в останню з яких інші люди, організації й або уряди не можуть вторгатися (також стосується обліку біометричних даних як еквіваленту тіла людини);

- форми діяльності, поведінки й способу дій, які людина має право захищати (приховувати) від уваги сторонніх;

- захист від вторгнення в приватне життя й свобода вибору його форми;
- можливістю людини контролювати інформацію про себе – вирішувати, коли, як і в якому обсязі інформація про неї стає відомою або повідомляється іншим.

Сьогодні приватність розглядається як фундаментальне право людини й перебуває в одному ряді із правом на життя, свободою переконань, власністю на майно та особисті здобутки на результати інформаційної та інтелектуальної праці.

Фахівці громадських організацій, E1ectronic Privacy Information Center та Privacy International, у своєму спільному дослідженні запропонували (умовно) розділити приватність на чотири види [7]. Це:

- фізична приватність – це умови захисту від примусових для людини процедур, зокрема медичних та багато ін. Деякі міри обумовлені потребами врахування інтересів суспільства та держави. Так поліції надане право зняти в арештованого відбитки пальців або узяти в нього аналіз ДНК для включення в національну базу даних і т.п.;
- територіальна та майнова приватність – звичайно мається на увазі недоторканність фізичних речей та житла. Певний рівень приватності мають не тільки будинки й квартири, але й робочі місця, готельні номери, купе поїзда і т.д. Майнова приватність визначається правом власності на майно та правом використання об'єктів інтелектуальної власності. Право власності на інформаційний продукт законодавством не визначається, хоча інформацією завжди торгували і вона знаходиться у комерційному у обігу;
- інформаційна приватність – під цим розуміється наявність захисту прав людини та свобод в інформаційній сфері, її уявлень та намагань покращити своє життя;
- приватність комунікацій – це все, що пов'язане з технічними засобами та техніко-технологічними діями, які стосуються, зокрема, таємниці телефонних розмов, поштових, електронних повідомлень. Приватність комунікацій найтіснішим чином пов'язана з інформаційною приватністю, зокрема з Інтернетом, який, як ніколи раніше, надає можливості несанкціонованих контролю та впливу на особисте життя людини.

Інформаційна приватність завжди займала особливе місце у стосунках між людьми. Її основою є забезпечення захисту відомостей про людину щодо нецільового та несанкціонованого отримання та використання її персональних даних.

Виділяють наступні елементи права на інформаційну приватність:

- право на самітність;
- право на інтимність;
- право на анонімність;
- право контролювати інформацію про себе [9], а також
- право "бути забутим" [12, с. 40].

У законодавстві це передбачає наявність пріоритетних гарантій забезпечення умов приватности для будь-яких дій по відношенню до персональних даних, які повинні:

- бути отримані законним способом;
- збиратися з відома й згоди особи, у кількості мінімально необхідній для певної мети;
- бути точними й захищеними від несанкціонованого доступу;
- використовуватися тільки з метою, заради якої вони були отримані;
- надаватися третім особам тільки за згодою особи, про яку вони зібрані;
- бути доступними тій особі, якої вони стосуються, зокрема, в контексті права на одержання інформації про її використання з виправленням невірної інформації та права доступу до комп'ютерних даних;
- знищуватися після того, як мета, заради якої їх збирали, досягнута й у даних більше немає потреби.

Зазначені гарантії не є абсолютними, а значною мірою залежать від контексту, у рамках якого визначаються норми захисту приватного життя й вимоги того, що може й повинне бути розкрите для публічності або держави [11]. Тобто, вважається, що границі інформаційної приватности рухливі й засновані на бажанні або небажанні індивіда повідомляти ту або іншу інформацію про себе.

Слід також звернути увагу на те, що визначення приватности людини в термінах права на контроль використання інформації про себе – одна з основних тенденцій за кордоном в політичних і юридичних дискусіях про захист персональних даних [13].

Сьогодні забезпечення інформаційної приватності дедалі більше ускладнюється у зв'язку з поширенням телекомунікаційних технологій та мереж. Вже загально зрозуміло, що будь-які відомості про людину можуть бути отримані завдяки Інтернет-технологіям та використані не лише на її користь, а з метою маніпулювання свідомістю, вимагання грошей, шантажу, залякування, або, нерідко, щоб проштовхувати на ринок якийсь комерційний продукт та ін. Зазначені дії безпосередньо стосуються проблеми забезпечення безпеки інформаційної приватності персональних даних в Україні, яка є невід'ємною складовою забезпечення національної безпеки держави.

Разом з вказаним зазначимо, що в українському законодавстві немає та не використовується поняття "приватність" за виключенням її згадування у ст. 182 КПК України та у нормативному документі КМ України – "Про ратифікацію Угоди між Кабінетом Міністрів України та Урядом Держави Ізраїль про тимчасове працевлаштування українських працівників в окремих галузях на ринку праці Держави Ізраїль" від 31.08.16 р. № 0108. Стаття 8 "Захист персональних даних" Угоди визначає: "*Сторони зобов'язуються вживати необхідних заходів відповідно до національного законодавства у сфері* ***охорони приватних персональних даних з метою захисту персональних даних*** *українських громадян, відібраних для тимчасового працевлаштування відповідно до цієї Угоди, у тому числі від випадкової їх втрати, пошкодження, незаконної обробки та доступу*" [14].

Конфіденційність персональних даних в Україні. Згідно ст. 10 Закону України "Про інформацію" (2016 р.) одним з видів інформації за змістом є те що вкладається в поняття "відомості про фізичну особу" або "персональні дані людини". Вони є складовою та невід'ємною частиною будь-яких професійних таємниць.

Сьогодні існують багато видів професійних таємниць, у основі яких лежить так звана "конфіденційність" інформації (confidentia – від англ. "довіра"). Вона, згідно ст. 21 Закону України "Про інформацію" (2016 р.), у функціональному колі свого предмета призначення передбачає наявність забезпечення захисту персональних даних у конфіденційному порядку, зокрема в таких сферах діяльності, як комерційна, податкова, банківська, адвокатська, нотаріальна, журналістська тощо, навіть у таємниці сповіді. Однак, проблема у тому, що дефініції, тобто наявності визначення істотних ознак предмета поняття під назвою "конфіденційна інформація", у законі 2016 р. немає. Її було вилучено з однойменного Закону України 1992 р. Стосовно сфери інформаційно-комунікаційної приватності в українській юридичній енциклопедії також маємо твердження про те, що персональні дані є конфіденційною інформацією [20].

Сучасне законодавство України має значну кількість законів, які надають лише переліки інформації про особу з посиланням на її "конфіденційність", без нормативного визначення (дефініції) та легального (предметно-правового) застосування словосполучення "конфіденційна інформація", як це прийнято у романо-германської (континентальної) системі права, яка притаманна і Україні. Наведемо деякі з них:

Конституція України від 28.06.96 р. № 254к/96-ВР (ст. 32) – …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. *Примітка.* Слово "приватність" у Конституції не використовується.

Цивільний кодекс України від 28.02.19 р. № 2694-VIII (ст. 895) – визначає конфіденційними – відомості щодо предмета договору на виконання науково-дослідних або дослідно-конструкторських та технологічних робіт, хід їх виконання та результати. *Примітка.* Самого визначення поняття "конфіденціність" немає.

Кримінальний кодекс України від 06.06.19 р. № 2747-VIII (ст. 182) – має лише одне згадування про конфіденційність: порушенням недоторканності приватного життя є незаконне збирання, зберігання, використання, знищення, поширення конфіденційної інформації про особу або незаконна зміна такої інформації, крім випадків, передбачених іншими статтями Кодексу. *Примітка.* Визначення поняття "конфіденціність" відсутнє.

Податковий кодекс України від 07.12.17 р. № 2245-VIII (п. 70.15) – до конфіденційної відноситься інформація про реєстраційний, ідентифікаційний номер платника податків, номер облікової картки фізичної особи тощо. *Примітка.* Словосполучення "конфіденційна інформація" застосовано у ст. 17.1.9 – платник податків має право: на нерозголошення контролюючим органом (посадовими особами) відомостей про такого платника без його письмової згоди та відомостей, що становлять конфіденційну інформацію, державну, комерційну чи банківську таємницю та стали відомі під час виконання посадовими особами службових обов'язків, крім випадків, коли це прямо передбачено законами. Визначення поняття "конфіденціність" відсутнє.

Митний кодекс України від 19.12.19 р. № 395-IX (ст. 11) – про додержання вимог щодо конфіденційності інформації; (ст. 37) – використовує словосполучення "інформація конфіденційного характеру". *Примітка.* У суспільних відносинах, тобто у юриспруденції (а не у публіцистиці), ніяка інформація, відомості або дані не мають характеру; характер – це психічні, моральні та інтелектуальні складові здібності лише біологічної істоти. Визначення поняття "конфіденціність" відсутнє.

Закон України "Про інформацію" від 06.12.16 р. № 1774-VIII (ст. 11) – до конфіденційної інформації про фізичну особу (персональні дані) належать, зокрема, дані про її національність, освіту, сімейний стан, релігійні переконання, стан здоров'я, а також адреса, дата і місце народження. *Примітка.* У техніці складання нормативних формул звичайно уникають її незавершеності (стосується слова "зокрема"). Визначення поняття що таке "конфіденціність" не маємо, мова йде лише про окремі її види.

Закон України "Про доступ до публічної інформації" від 09.04.15 р. № 319-VIII (ст. 7) – конфіденційна інформація – 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. *Примітка.* Ця дефініція визначає процес надання доступу, але не надає визначення про сенс та предметно-правовий зміст поняття "конфіденційна інформація".

Закон України "Про друковані засоби масової інформації (пресу) в Україні" від 02.10.18 р. № 2581-VIII (ст. 2) – має лише згадування наявності "конфіденційность" в контексті свободи діяльності друкованих засобів масової інформації.

Закон України "Про телебачення і радіомовлення" від 02.10.18 р. № 2581-VIII (с. 56.) – має лише згадування в контексті вимог до розповсюдження конфіденційної інформації. Крім цього, без згадування конфіденційності (ч. 3 ст. 62) – у програмах та передачах телерадіоорганізації не мають права без письмової згоди батьків або осіб, що їх

замінюють, а також відповідних правоохоронних органів розголошувати будь-яку інформацію, яка може сприяти ідентифікації особи неповнолітнього правопорушника або яка стосується факту самогубства неповнолітнього.

Й далі, в контексті визначення конфіденційності приватних (особистих) відомостей (інформації, даних) в інформаційно-комунікаційній сфері, де предметно-понятійного визначення поняття "конфіденційність" не маємо.

Закон України "Про свободу пересування та вільний вибір проживання в Україні" (ст. 6 ч. 8.) – відомості про місце проживання.

Закон України "Про загальнообов'язкове державне соціальне страхування у зв'язку з тимчасовою втратою працездатності та витратами, зумовленими похованням" (ст. 33) – відомості про страховий стаж, результати медичних обстежень, отримані доходи застрахованої фізичної особи.

Закон України "Про звернення громадян" (ст. 10.) – відомості про особисте життя громадян, одержані із звернень громадян.

Закон України "Про загальнообов'язкове державне пенсійне страхування" (ч. 1. ст. 98) – інформація про стан пенсійних активів, облікованих на накопичувальному пенсійному рахунку застрахованої особи.

Закон України "Про недержавне пенсійне страхування" (ст. 53 ч. 3.) – інформація про пенсійні внески, пенсійні виплати та інвестиційний прибуток (збиток), що обліковується на індивідуальному пенсійному рахунку учасника пенсійного фонду, пенсійні депозитні рахунки фізичних осіб, договори страхування довічної пенсії;

Закон України "Про оплату праці" (ст. 31) – відомості про оплату праці працівника.

Закон України "Про лікарські засоби" (ст. 9 ч. 8.) – інформація, що міститься в заяві про державну реєстрацію лікарського засобу та додатка до них.

Закон України "Про біженців та осіб, які потребують додаткового або тимчасового захисту" (ст. 7 ч. 10) – відомості, що подаються заявником на визнання біженцем або особою, яка потребує додаткового захисту.

Закон України "Про забезпечення безпеки осіб, які беруть участь у кримінальному судочинстві" (ст. 15) – дані про особу взяту під захист у кримінальному судочинстві.

Закон України "Про державний захист працівників суду і правоохоронних органів" (ст. 10) – дані про працівника суду або правоохоронного органу, взятого під захист.

Закон України "Про доступ до судових рішень" (ст. 7) – відомості, що містяться в текстах судових рішень та дають можливість ідентифікувати фізичну особу, зокрема: імена (ім'я, по батькові, прізвище) фізичних осіб; місце проживання або перебування фізичних осіб із зазначенням адреси, номерів телефонів чи інших засобів зв'язку, адреси електронної пошти, ідентифікаційних номерів (коди); реєстраційні номери транспорту.

Закон України "Про Всеукраїнський перепис населення" (ст. 16) – первинні дані, отримані в процесі проведення Перепису населення.

Закон України "Про поховання та похоронну справу" (ст. 7) – інформація про померлого, та багато ін. нормативних актів.

За підсумками можна сказати, що українське законодавство загальносистемного визначення поняття "конфіденційність" не має та не застосовує. Існуючий підхід до захисту персональних даних в Україні йде по шляху, на якому відсутні загальні юридичні критерії поняття *"конфіденційна інформація" яка має особливі властивості, що обумовлюють потребу в конкретних умовах дотримання її приватності в використанні та у відповідних засобах захищеності,* і не вирішене питання місця персональних даних у обсязі відповідності логічному колу цього поняття.

До зазначеного вважаємо за необхідне звернути увагу на те, що згідно п. 4.1.1.2 існуючого в Україні з 1997 року нормативного акту – ДСТУ 3396.2-97 "Технічний захист інформації. Терміни та визначення" [21]: *"конфіденційна інформація – це інформація з обмеженим доступом, якою володіють, користуються чи розпоряджаються окремі фізичні чи юридичні особи або держава і порядок доступу до якої встановлюється ними"*. При цьому, у п. 2 Передмови до Стандарту визначене, що його вимоги забезпечують реалізацію норм Закону України "Про інформацію". Але, як зазначалося раніше, ця норма-дефініція (тобто, стаття 30) з Закону було вилучено у 2011 р. До слова, з Закону також було вилучено норми щодо "право власності на інформацію" (ст. 38) та "визначення інформації товаром" (ст. 39), і взагалі він був перетворений у засіб забезпечення діяльності ЗМІ.

Головне полягає у тому, що наведена вище дефініція визначає тріаду повноважень права власності людини, а саме: права володіння, користування і розпорядження своїми відомостями-даними, про що детально йдеться у [12, с. 90-97; 22, с. 163-175]. Саме ця дефініція є чіткою класифікацією критеріїв за якими визначається наявність предмету приватності та конфіденційності інформації для будь-якого виду персональних даних. І це важливо з погляду активного поширення процесів щодо електронно-інформаційного середовища, у якому традиційні нормативні підходи й організаційні механізми щодо захисту персональних даних свідчать про їхню малу ефективність.

Безпека приватності персональних даних. В українському законодавстві немає словосполучення "безпека приватності персональных данных" (або "безпека персональних даних"), закріплено лише термін "інформаційна безпека" у Законі України "Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки" від 09.01.07 р. № 537-V. Згідно п. 13 Розділу ІІІ Закону інформаційна безпека – це стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації. Про "процес" захищеності не йдеться.

Відповідно до Доктрини інформаційної безпеки України [15] до суттєвих ознак поняття "інформаційна безпека" віднесено:

- *конфіденційність* – стан поводження з інформацією, при якому доступ до неї отримують тільки суб'єкти, які мають на це право;
- *цілісність* – запобігання несанкціонованій або незаконній модифікації інформації;
- *доступність* – запобігання тимчасовому або постійному приховуванню інформації від користувачів, які мають право на доступ.

Виходячи, зокрема, з вищенаведеного, *безпеку приватності персональних даних вважаємо за необхідне розглядати не лише як стан захищеності відомостей про особу, а й процес забезпечення їх захисту.*

В наш час поширення інформаційно-віртуальної реальності, яка раніше лише проявлялася у житті, завдяки швидкому розвитку ІКТ, мереж поняття "приватності" та юридичного захисту персональних даних дедалі більше перетворюється на нормативно-фіктивну сферу намірів та бажань в упорядкуванні суспільних відносин, де усе більш складно уявити собі світ, у якому буде існувати приватність. Зростаючі збір, об'єднання та обробка персональних даних в різних базах, що документують деталі ідентифікаційних та фізичних атрибутів, поведінку, бажання, відносини, недоліки, досягнення та будь-що ін., створює таке уявлення про людину, коли можна вже вести розмову про наявність лише *віртуальної приватності* з *віртуальною конфіденційністю*.

Глобальні інформаційні мережі й безліч сервісів несанкціоноване та непомітно збирають про користувачів терабайти даних, та й самі користувачі постійно викладають своє життя на загальний огляд у соцмережах, з різних причин.

Так, до прикладу, коли користувачі Інтернету намагаються ввійти до якогось сайту або бази даних, вони натрапляють на обов'язкові для відповіді запитання. Потім їх електронні відповіді та е-сліди автоматизовано обробляються та поширюються з одного сервера на інший, фільтруються, сортуються, аналізуються, зберігаються у невідомих базах даних, хмарних сховищах (сервісів, які все ще мають високі ризики їхнього залучення) та використовуються з невідомою для суб'єкта даних ціллю. Звичайно відповіді "для чого" немає, проте мало хто хвилюється з цього приводу.

Тим часом нецільове використання персональних даних здатне завдати людині великої шкоди. Особливо якщо мова йде про "чутливі персональні дані" (sensitive personal data), які потребують особливо делікатного до них ставлення, тобто особливих заходів у законодавчому захисту, наприклад інформація про стан здоров'я. Відомі не тільки випадки, коли медичні діагнози проти бажання пацієнта розміщалися в мережі з баз даних лікувальних закладів, і наслідки виявлялися досить жалюгідними, а взагалі давно поширена практика, коли Інтернет використовують для пропозицій з продажу різноманітних баз персональних даних.

Сьогодні інформаційно-комп'ютерні технології є потужним інструментом для злочинців різних країн, який вони можуть використовувати для протиправної діяльності, у тому числі на транснаціональному рівні. Боротьба з кіберзлочинністю стає однією з головних тем сучасної міжнародної політики, де проглядаються намагання пошуку балансу між приватністю та безпекою. Найкраще це помітно на прикладі Європейської Конвенції про кіберзлочинність.

Робота над Конвенцією в Раді Європи почалася навесні 1997 року [16]. Це був закритий процес, у якому брали участь не тільки представники європейських держав, але і юристи Департаменту юстиції США. Через три роки, коли число версій дійшло до 22, публіка змогла познайомитися з текстом. На його творців посипалися гнівні листи. Уважалося, що Конвенція встановить європейські стандарти в боротьбі з атаками на комп'ютерні системи, шахрайством у мережі, поширенням вірусів, порнографії, пропагандою насильства й т.п., що зрозуміло. Інтернет не має границь, цим користуються злочинці. І виходить, як стверджували розробники Конвенції, настав час поставити "на безмежну основу" і роботу правоохоронних органів різних країн. Вони запевняли, що поки Конвенції немає, можливі будь-які порушення, а от якщо вона буде прийнята, процес боротьби зі злочинністю стане більш ефективним. Однак, розширивши повноваження спецслужб, було занадто мало приділено уваги гарантіям прав користувачів Інтернету.

18 жовтня 2000 року кілька десятків громадських організацій виступили із загальним відкритим листом проти Конвенції. Критикували, зокрема, ідею зобов'язати провайдерів Інтернету складати звіти про дії клієнтів. Автори відкритого листа вважали, що стаття 18 проекту несумісна зі статтею 8 Європейської Конвенції з прав людини й з рішеннями Європейського Суду. Схожі думки було від незалежних експертів, журналістів і деяких державних чиновників. Наприклад, Комісари з захисту персональних даних під час своєї зустрічі в Стокгольмі у квітні 2000 року висловили стурбованість проектом Конвенції. Проте 8 листопада 2001 року документ був схвалений Радою Європи.

Учасниками Конвенції є 35 європейських держав-членів Ради Європи та 5 держав, які не є членами Ради Європи (Австралія, Домініканська Республіка, Японія, Панама, США) [17]. Конвенція є необхідною для зупинення дій, спрямованих проти конфіденційності, цілісності і доступності комп'ютерних систем, мереж і комп'ютерних

даних, а також зловживання такими системами, мережами і даними, шляхом встановлення кримінальної відповідальності за таку поведінку, надання повноважень, для ефективної боротьби з такими кримінальними правопорушеннями шляхом сприяння їхньому виявленню, розслідуванню та переслідуванню, як на внутрішньодержавному, так і на міжнародному рівнях, і укладення домовленостей щодо швидкого і надійного міжнародного співробітництва.

Згідно з положеннями Конвенції, Сторони надають одна одній взаємну допомогу з метою розслідування або переслідування кримінальних правопорушень, пов'язаних із комп'ютерними системами і даними, або з метою збирання доказів у електронній формі.

Сторона може запитати іншу Сторону видати ордер чи іншим чином провести термінове збереження комп'ютерних даних, які зберігаються за допомогою комп'ютерної системи, яка знаходиться на території такої іншої Сторони, і відносно якої Сторона, яка запитує, має намір надіслати запит про взаємну допомогу щодо обшуку чи подібного доступу, арешту чи подібних дій або розголошення таких даних.

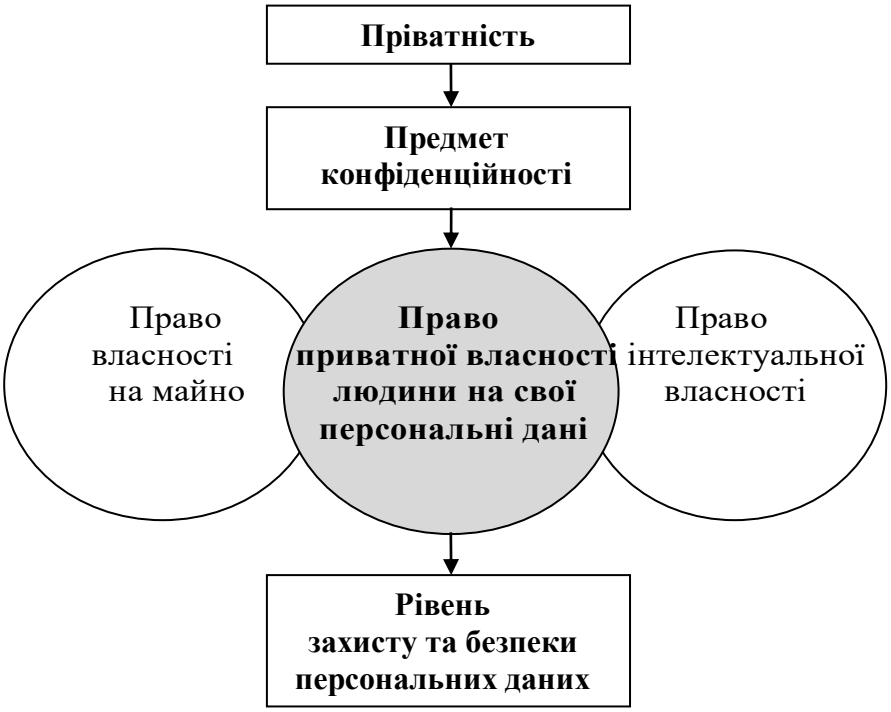
У 2011 році в ООН була створена Міждержавна група експертів з вивчення кіберзлочинності, зусиллями якої у 2013 році було проведено "Всебічне дослідження проблеми кіберзлочинності" [18]. У цьому документі проаналізовані такі аспекти як законодавство у даній сфері, діяльність правоохоронних органів, міжнародне співробітництво тощо. В ньому, зокрема, зазначається, що 80 відсотків кіберзлочинів вчиняється в організованій формі. Сьогодні Робота міждержавної групи експертів продовжується. Так у доповіді за наслідками засідання даної групи 27-29 березня 2019 року у Відні були розглянуті питання удосконалення законодавства, у тому числі міжнародного, проблеми діяльності правоохоронних органів, використання електронних доказів. Було зазначено, що, зважаючи на транснаціональний характер кіберзлочинності і той факт, що значна більшість глобальних кіберзлочинів вчиняються організованими групами, державам-членам слід більш широко застосовувати Конвенцію ООН проти транснаціональної організованої злочинності для сприяння обміну інформацією та доказами в ході кримінальних розслідувань, що стосуються кіберзлочинності.

В Україні Конвенція про кіберзлочинність 2001 року набула чинності 1 липня 2006 року [19]. Центральними органами України, які уповноважені розглядати відповідні запити компетентних органів іноземних держав, а також направляти запити до компетентних органів іноземних держав на підставі та на умовах, визначених Конвенцією, є Міністерство юстиції України (щодо виконання судових рішень) та Генеральна прокуратура України (щодо процесуальних дій під час розслідування кримінальних справ). Порядок і умови розгляду відповідних запитів компетентних органів іноземних держав, так само як і направлення запитів до компетентних органів іноземних держав, визначені Главою 42 Кримінального процесуального кодексу України. Відповідно до Закону України "Про внесення зміни до Закону України "Про ратифікацію Конвенції про кіберзлочинність" від 21.09.10 р. № 2532-VI в Україні органом, на який покладаються повноваження щодо створення та функціонування цілодобової контактної мережі для надання невідкладної допомоги при розслідуванні злочинів, пов'язаних з комп'ютерними системами та даними, переслідуванні осіб, що обвинувачуються у вчиненні таких злочинів, а також збирання доказів в електронній формі, є Міністерство внутрішніх справ України [18].

Висновки.

1. Приватність та безпека персональних даних забезпечується нормативно-правовими умовами конфіденційності відомостей. Рівень конфіденційності, як стан та процес захисту приватності, впливає на загальне становище інформаційної безпеки в Україні.

У контексті наявності логічності взаємозв'язків (кореляції) приватності, конфіденційності та безпеки персональних даних вважаємо за можливе виходити з того, що вони проявляються у властивостях виду персональних даних у будь-якій області приватності (прайвеси), визначаються предметом інформаційної конфіденційності в обсязі права приватної власності людини на дані про себе, яке забезпечує захист та відповідний рівень безпеки персональних даних. Використовуючи раніше здійснені наробітки щодо визначення обсягу та зв'язку суттєвих ознак різних понять ("право власності на майно", "право інтелектуальної власності" та "право приватної власності людини на свої персональні дані"), які, згідно логічних кругів Ейлера завжди частково збігаються (див. [12, с. 92-93]), взаємний зв'язок та співвідношення між приватністю, конфіденційністю, захистом та безпекою персональних даних наочно може бути подано таким чином:



2. Сучасне законодавство, зокрема в Україні, не має юридичного визначення таких понять, як "приватність" (privacy) та "безпека персональних даних". Враховуючи дедалі активніше їх застосування у наші часи, вони потребують юридичного визначення, яке відображає істотні ознаки їх предметного змісту.

Те ж саме стосується поняття "конфіденційна інформація", яка має особливі властивості, що обумовлюють потребу в конкретних умовах дотримання її приватності в використанні та у відповідних засобах захищеності. А це визначає необхідність запровадження чітких істотних ознак (критеріїв) щодо поняття "конфіденційність".

У загальному плані вважаємо, що законодавству України потрібні не стільки переліки видів персональних даних, кожен з яких за різних уявлень може бути суб'єктивно віднесений (або не віднесений) до категорії "конфіденційність", а практичне запровадження та застосування уніфікаційних критеріїв, які й визначають предмет конфіденційності, зокрема в сфері захисту персональних даних. Уніфікація надає системний підхід до конкретності у визначенні наявності інформаційно-комунікаційної приватності, особливо в умовах поширення застосування засобів електронно-інформаційного середовища, запобігає розпорошеності по законодавству

відомостей у численних наборах переліків, створює однаковість у підході до кваліфікації персональних даних конфіденційними, сприяє більш чіткій модальності суджень у побудові усієї системи захисту та безпеки персональних даних.

3. У сучасних умовах поширення ІКТ та мереж боротьба з кіберзлочинністю стає однією з головних тем сучасної міжнародної політики, де проглядаються намагання пошуку балансу між приватністю та безпекою. Баланс між приватністю та безпекою персональних даних – складне питання, яке в епоху інформатизації не може вирішуватися політиками, юристами, технічними фахівцями або спецслужбами на підставі поглядів минулого часу. Захист персональних даних взагалі не зводиться лише до вимог забезпечення якості технічної обробки даних і посилення заборонних заходів в інтересах створення умов загальної безпеки. Виходячи з приписів ст. 3 Конституції України, яка визначає наявність та пріоритетність природних прав людини, – *"Людина, її життя і здоров'я, честь і гідність, недоторканність і безпека визнаються в Україні найвищою соціальною цінністю. Права і свободи людини та їх гарантії визначають зміст і спрямованість діяльності держави…",* мірою оцінки суджень про допустимість втручання в особисте життя може стати "право приватної власності людини на свої персональні дані" та "контроль використання інформації про себе", за умов правового обмеження у правах фізичних осіб, якщо це офіційно та чітко визначено, що стосується державної чи громадської безпеки, фінансової стабільності, боротьби зі злочинністю, захисту прав та основоположних свобод інших осіб.

Використана література

1. Прохвачева О. (2000) Лингвокультурнний концепт "приватность". URL: http://www.dissercat.com/content/lingvokulturnyi-kontsept-privatnost-na-materiale-amerikanskogo-varianta-angliiskogo-yazyka#ixzz3AMsvTYM

2. Большой англо-русский словарь; под ред. проф. И.Р. Гальперина. Москва, 1988 г.

3. Юридична енциклопедія: в 6 т.; редкол. Ю.С. Шемшученко (голова редкол.) та ін. Київ: "Українська енциклопедія", 2003. Т. 5 : П–С. С. 53.

4. Большой юридический словарь; под ред. А.Я. Сухарева, В.Е. Крутских. Москва: Инфра-М, 2003.

5. Report of the Committee on Privacy and Related Matters. Responsibility: Chairmant David Calcutt. Cmnd. 1102. London: H.M.S.O., 1990; Особливості захисту персональних даних і сучасному кіберпросторі: правові та технологічні аспекти: анал. доповідь. Київ: Нац. інст. страт. досл., 2013. 51 с. С. 4.

6. Приватность: рождение и смерть. 3000 лет истории приватности. URL: https://www.habr.com/ru/company/parallels/blog/348922

7. Privacy & Human Rights. Privacy International and Electronic Privacy Information Center, 1999. URL: //www.epic.org; Смирнов С. Приватность. Москва: Изд. "Права человека". 2002. 95 с. С. 9.

8. Brandeis Louis D, Warren Samuel D. The Right to Privacy. *Harvard Law Review*. 1890. P. 193-220. URL: https://www.louisville.edu/library/kaw/brandeis/privacy/html

9. Соколова М. (2014). Защита персональных данных он-лайн: основные понятия. URL: https://www.researchgate.net/publication/281459597_Zasita_personalnyh_dannyh_onlajn_osnovnye_ponatia

10. Прослушивание телефонов в международном праве и законодательстве одиннадцати европейских стран: сост. Е. Захаров. – (Харьковская правозащитная группа). Харьков: Фолио. 1999. 152 с. С. 14-15.

11. Westin A. (2003) Social and Political Dimensions of Privacy. URL: http://www.asc. upenn.edu/usr/ogandy/Gandy%20Comm664/westin%20-%20social%20and%20political%20dimensions%20of%20privacy.pdf

12. Становлення і розвиток правових основ та системи захисту персональних даних в Україні: монографія; за ред. В.М. Брижка, В.Г. Пилипчука. – (НДІІП НАПрН України). Київ: ТОВ "Видавничий дім "АртЕк", 2017. 226 с.

13. Bygrave L. (2010) Privacy and data protection in an international perspective. URL: http://www.uio.no/studier/emner/jus/jus/JUS5630/v13/undervisningsmateriale/privacy-and-data-protection-in-international-perspective.pdf

14. "Про ратифікацію Угоди між Кабінетом Міністрів України та Урядом Держави Ізраїль про тимчасове працевлаштування українських працівників в окремих галузях на ринку праці Держави Ізраїль" від 31.08.16 р. № 0108. URL: http://www.w1.c1.rada.gov.ua/pls/zweb2/webpro c4_1?pf3511=59911

15. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року "Про Доктрину інформаційної безпеки України": Указ Президента України від 25.02.17 р. № 47/2017. URL: https://www.president.gov.ua/documents/472017-21374

16. Дембичь Д.А. Обзор проекта Европейской конвенции о преступности в киберпространстве. URL: http//www.conf3.parkmedia.ru/any_r.asp?; Волеводз А.Г. Проект Европейской Конвенции о киберпреступности: особенности и новации правового регулирования международного сотрудничества в противодействии компьютернмм преступлениям. *Защита информации. Конфидент.* 2001. № 5. С. 18-25, № 6. С. 23-27.

17. Сайт Мінюсту України. URL: https://www.minjust.gov.ua/news/ministry/1-lipnya---vosma- richnitsya-nabuttya-chin nosti-dlya-ukraini-konventsii-pro-kiberzlochinnist-20026

18. Гуцалюк М.В. Загрозливі тенденції організованої кіберзлочинності. *Інформація і право*. № 1(32)/2020. С. 88-98.

19. Конвенція про кіберзлочинність: Закон України від 07.09.05 р. № 2824-IV. URL: https://zakon.rada.gov.ua/laws/show/994_575

20. Юридична енциклопедія: в 6 т.; редкол. Ю.С. Шемшученко (голова редкол.) та ін. Київ: "Українська енциклопедія", 2001. Т. 3: К–М. С. 332.

21. Державний стандарт України (ДСТУ) 3396.2-97. "Технічний захист інформації. Терміни та визначення". URL: http://www.online.budstandart.com/ua/catalog/doc-page.html?id_doc=69175

22. Брижко В.М., Фурашев В.М. Інформаційне право та інформаційне законодавство: наукове видання. – (НДІІП НАПрН України). Київ: ТОВ "Видавничий дім "АртЕк", 2019. 288 с.

~~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~~
~~~~~~~~~~~~~~