УДК 316.324.8

БРИЖКО В.М., *доктор філософії (Ph.D.) з юридичних наук.*
ORCID: https://orcid.org/0000-0002-3941-1013.

МОДАЛЬНІСТЬ ПРАВОВОЇ ВИЗНАЧЕНОСТІ У СФЕРІ ЗАХИСТУ ТА БЕЗПЕКИ ПРИВАТНОСТІ ПЕРСОНАЛЬНИХ ДАНИХ

Анотація. *З урахуванням результатів раніше проведених досліджень, розглянуто понятійні, термінологічні і семантичні питання приватності, захисту та безпеки персональних даних щодо визначення, тлумачення та кореляції ключових понять у зв'язку з забезпеченням прав людини на особисте життя та життєдіяльність у інформаційній сфері. Подано пропозиції з вдосконалення систематизації законодавства сфери персональних даних в Україні.*

Ключові слова: *приватність, інформаційна приватність, приватність у комунікаціях, конфіденційність приватності, захист та безпека приватності персональних даних.*

Summary. *Taking into account the results of previous research, the conceptual, terminological, and semantic issues of privacy, protection and security of personal data are considered with regard to human rights to privacy and life activities in the information sphere. Proposals are given to improve the systematization of legislation on personal data in Ukraine.*

Keywords: *privacy, information privacy, privacy in communications, protection and security of privacy of personal data.*

Аннотация. *С учетом результатов прежде проведенных исследований, рассмотрены понятийные, терминологические и семантические вопросы приватности, защиты и безопасности персональных данных в контексте определения, толкования и корреляции ключевих понятий в связи с обеспечением прав человека на личную жизнь и жизнедеятельность в информационной сфере. Представлены предложения по совершенствованию систематизации законодательства сферы персональных данных в Украине.*

Ключевые слова: *приватность, информационная приватность, приватность в комуникациях, конфиденциальность приватности, защита и безопасность приватности персональных данных.*

Постановка проблеми. У 2016 році Європейський Парламент і Рада затвердили Пакет захисту персональних даних (англ. – GDPR) [1], який передбачає нові Правила та порядок захисту персональних даних для країн європейського континенту (набули чинності 25.05.18 р.). Головним документом є Регламент (ЄС) 2016/679 "Про захист фізичних осіб у зв'язку з обробкою персональних даних та про вільне переміщення таких даних…" (далі – Регламент GDPR) [2, с. 2-103]. Важливою новацією у Регламенті GDPR є те, що вперше у міжнародному документі щодо захисту персональних даних у п. 1 Преамбули офіційно констатовано: *"**Захист фізичних осіб у зв'язку з обробкою персональних даних є основоположним правом**"* (курсив – *Авт.*).

Застосування слова ***"основоположні"*** до слова ***"право"*** знаменно тим, що вказує на придання пріоритетності вихідним принципам, приписам та нормам у зв'язку з обробкою персональних даних людини, яка має здійснюватися на підставі законності та справедливості. "Справедливість" (з грец. означало лише "звичай", "уклад життя" [3]), завжди була та є важливою категорією соціально-філософської думки, моральної та правової свідомості, наявність якої передбачає встановлення та виконання у соціумі вимог, зокрема щодо рівних прав та обов'язків, а також юридичної відповідальності та захисту від правопорушень. При цьому, як пам'ятаємо, у Конвенції Ради Європи "Про захист прав людини і основоположних свобод" від 1950 р. мова йде про "основоположні свободи", а стаття 8 сформульована як "Право на повагу до приватного …життя" [4]. Зараз, згідно

рішення інституцій Європейського Союзу, права людини саме у зв'язку з захистом персональних даних віднесено до "основоположних прав". Це може бути свідченням того, що права людини у зазначеної сфері удосконалюються, розвиваються та посилюються.

Також, можна виходити з того, що права людини у сфері персональних даних, як царина морально-етичних поглядів та загальних принципів щодо "справедливості", стають однією з пріоритетних сфер правової думки, яка потребує нових юридичних конструкцій щодо удосконалення правової (юридичної) визначеності та відповідних нормативних змін, зокрема у зв'язку з розвитком новітніх технологій та цифрової трансформації.

Результати аналізу наукових публікацій. Як вважаємо, на увагу заслуговують результати робіт таких вчених, як: Пилипчук В.Г., Баранов О.А., Богуцький П.П, Брайчевський С.М., Дзьобань О.П., Корж І.Ф., Леонов Б.Д., Радутний О.Е., Серьогін В.О.

Поряд з пошуками перспектив розвитку інформаційно-комунікаційної сфери, продовжує існувати неоднозначність у термінологічному визначенні та тлумаченні різних понять та термінів, що складають основу такої, зокрема, домінантної категорії в сфері прав людини як "приватність". Вона, як "стрижень" у багатогранних процесах захисту та безпеки персональних даних, потребує не лише чіткого уявлення, але й оцінки суттєвих ознак, предметного змісту, кореляції (взаємозв'язку) та юридичного визначення таких супутніх їй словосполучень, як: інформаційна приватність, приватність у комунікаціях, конфіденційність приватності, захист та безпека приватності персональних даних.

Метою статті є узагальнення семантично-понятійного тлумачення та кореляції основних понять у сфері захисту та безпеки приватності персональних даних, а також надання пропозицій вдосконалення систематизації законодавства в Україні.

Виклад основного матеріалу.

Приватність. Поняття "приватність" (англ. – *privacy)* у англомовних країнах розглядається як можливості та право людини *"на самоту", "бути залишеною у спокої", "бути наданою самої собі".* За узагальненням – *"кожна людина має право на свій "куточок" у просторі, захищений від довільних зазіхань із боку інших"* [5]. Вищевказані словосполучення можливо й прийнятні для прецедентного загального права (*common law*) разом з статутним правом, як у США та Британії [6], але не дуже сприймаються стосовно розуміння відмінностей у ознаках різних за змістом понять, як прийнято в континентальній правовій системі, що може позначатися на суб'єктивному трактуванні предмета захисту приватності. Важливість означеного полягає у тому, що коли предмет (об'єкт, явище тощо) визначається, він повинен мати *"чіткість, зрозумілість та однозначність"* змісту сенсу ознак, для встановлення його ідентичності (тотожності). В Україні про це йдеться у Рішеннях Конституційного Суду України, див. [7; 8].

Сьогодні, в аспекті уявлень про "приватність", недоторканність приватного життя, згадується у ст. 3, 12 Загальної декларації прав людини 1948 р., ст. 5, 8 Європейської Конвенції з прав людини та основоположних свобод 1950 р., ст. 6-8, 11 Хартії основних прав Європейського Союзу 2000 р., рішеннях Європейського Суду з прав людини, що уточнюють сенс окремих формулювань та продовжують прецедентну практику. Загалом, документи ЄС не мають юридичного визначення поняття "приватність", а у Регламенті GDPR "приватність" лише згадано у п. 4- 6, 19, 45 Преамбули. В Україні – це слово наведене у ст. 41 Конституції щодо майнових відносин, але у законодавстві визначення не має.

У загально-соціальному контексті поняття "приватність" може розумітися як право людини жити своїм життям при мінімальному сторонньому втручанні та як захищеність від втручання в її особисте життя та стосунки безпосередньо фізичним шляхом або через публікацію інформації про неї. Це надає можливість інтерпретації поняття "приватність" в термінах захисту персональних даних.

Якщо виходити з сенсу такого словосполучення як “особиста таємниця людини”, з юридичної точки зору можна запропонувати більш-менш точний зміст дефініції поняття “приватність” а саме: *приватність – це право людини на таємницю особистого життя та її захист від сторонніх на неї зазіхань*.

За предметно-складовими частинами “приватність” поділяють на такі види: інформаційна приватність (щодо збирання, використання, зберігання, поширення персональних даних та у зв’язку з їх обробкою, зокрема таких, як банківська, податкова, медична, маркетингова та ін. будь-яка інформація про людину), приватність у комунікаціях (недоторканність телефонних переговорів, електронної пошти та інших засобів зв’язку), фізична приватність (захист людського тіла від стороннього втручання, несанкціонованих медичних випробувань і використання внутрішніх органів) та територіальна приватність (обмеження на вторгнення в житло, робоче місце, громадські місця). Саме вони є визначальними складовими загального стану та рівня безпеки приватності в сфері захисту персональних даних людини в державі.

Інформаційна приватність. Поняття “інформаційна приватність” визначається можливостями людини щодо нерозголошення її особистого життя у інформаційній сфері, що передбачає нормативне забезпечення захисту людини щодо нецільового та несанкціонованого опрацювання відомостей (або обробки персональних даних) про неї. Під цим розуміється встановлення правил збирання, зберігання, використання та поширення відомостей про особисте життя людини, які відповідно до принципів обробки персональних даних, визначених Регламентом GDPR, передбачають такі основоположні права на інформаційну приватність [9]:

право на самітність, тобто право людини на захист від втручання в її особисте життя і родинні стосунки через поширення (публікацію) інформації (персональних даних);

право доступу, на припинення обробки, виправлення та видалення персональних даних (“право бути забутим”);

право на заперечення обробки та автоматизоване індивідуальне прийняття рішень;

право контролювати інформацію про себе, тобто знати, ким, коли, яким чином і в яких межах інформація про неї може бути або буде використовуватися іншими особами.

Застосування поняття “приватність” в термінах права контролю людини щодо використання інформації про себе вважається однією з основних тенденцій за кордоном в політичних і юридичних дискусіях про захист приватності персональних даних [10].

Зазначені вище правові позиції-приписи є визначальними у висновку того, що в юридичній галузі людина може мати особливе та специфічне для інформаційної сфери право – “право приватної власності на відомості про себе”, які у електронно-інформаційному середовищі вже мають так звану фактуру, що визначається словосполученням “персональні дані”. Про наявність матеріальної специфічності в інформаційній сфері детально йдеться, зокрема у [11], де інформація (персональні дані) розглядаються як фіктивно-юридичний об’єкт майнового права, що повністю узгоджується з юридично прийнятою у світі “фікцією власності” в сфері інтелектуальної власності; у зазначеній сфері, говорячи по сутності, немає власності, є лише право використання та ін.

До вищевказаного вважаємо важливим звернути увагу на наступне. Ще у 1689 році видатний англійський філософ, правознавець Джон Локк, якій заклав у державне управління ідеї про поділ державної влади та громадянське суспільство, в роботі “Два трактати про правління” писав, що *“держава повинна функціонувати для досягнення тієї єдиної мети, заради якої вона споконвічно й була створена, а саме для захисту життя, свободи та власності”*. При цьому, він висловив дуже важливу концептуальну думку: *“Кожна людина має деяку особливу власність, що полягає в її власній особистості, на*

яку ніхто, крім неї самої, не має ніяких прав" [12]. Іншими словами, як стверджували у своїх роботах С. Олсаретті "Свобода, вознаграждение и рынок"(2004) [13] та М. Доньева-Коєна "Опасные мысли: произведения о законе, себе и морали" (2002) [14], Д. Локк виходив з того, що *"кожна людина має право власності на свою особистість"*.

У соціальному плані інформаційну приватність можна поділити на приватність у побуті та приватність у публічності, яка пов'язана із сферою засобів масової інформації, а також з відповідною діяльністю з боку держави. Але, якщо остання має значну скритність, то першість головного порушника приватності належить саме масмедіа.

Звичайно, у будь-якій державі (навіть у автократичній чи тоталітарній) державна безпека корелюється тією або іншою мірою з загальною безпекою людей, що може визначатися владою потребами суспільства взагалі. Одночасно, у правовій державі будь-яка особа не може мати абсолютного імунітету на недоторканність приватності. У такій державі приватність має поступатися місцем публічності щодо інформації про осіб, які представляють усе (або частково) суспільство формально і неформально – керівники політичних сил та органів державної влади тощо, які здійснюють вплив на формування влади та стан справ у державі, регіонах тощо, або мають можливість визначати осіб, які в силу тих чи інших соціальних обставин або ж суб'єктивних уявлень становлять загрозу національній безпеці. Проте, тут існує межа – приватні відомості публічних осіб повинні мати захист, який надає їм можливість забезпечити особисту безпеку та членів її родини [15, 16], але лише за законом.

У той же час можна виходити з того, що якщо будь-хто добровільно виявився в сфері суспільної уваги та надав про себе відомості, то він повинен прийняти факт обмеженням своїх прав на приватність.

З юридичної точки зору можна запропонувати такий зміст дефініції, а саме: *інформаційна приватність – це право людини на недоторканність та захист відомостей (даних), які стосуються або пов'язані з особистим її життям.*

Приватність у комунікаціях. Комунікації – це засоби та шляхи забезпечення інформаційної діяльності щодо взаємодії (повідомлень, спілкування) відповідних суб'єктів, які є носіями певних правомочностей та правозобов'язань.

Приватність у комунікаціях, як процес передавання (поширення) та обміну інформації, – це стан та рівень диспозитивності законодавства щодо інформаційної приватності та умов нерозголошення відомостей про людину, які здійснюються нормативно-правовими засобами захисту її персональних даних, завдяки чому забезпечується інформаційна безпека людини, суспільства та держави.

Умови запобігання порушень приватності у комунікаціях мають передбачати, насамперед, наявність правових можливостей реальної інформаційної захищеності та безпеки людини. Приватність визначає загально-соціальну потребу у порядної діяльності в інформаційному середовищі, оскільки відображає індивідуалізацію людини, утворює підставу її унікальної суб'єктності і саме у такій якості здійснює трансформацію усіх приватно-правових характеристик статусу людини у публічні інформаційно-правові відносини. В інформаційно-правовому статусі людини приватність є внутрішньою його характеристикою, яка розкриває сутність права людини на інформаційну безпеку [15].

Приватність у комунікаціях і приватність персональних даних тісним чином пов'язані з Інтернетом. Інтернет-приватність розглядається, як джерело персональної інформації не призначеної до поширення. До цього може бути застосовано словосполучення "приватність у електронних комунікаціях" (тобто, приватність у електронно-інформаційному середовищі). Ця приватність безпосередньо пов'язана з поняттям "дані", як формалізованими знаково-кодовими комбінаціями для їх автоматичної обробки, до яких "інформація" прикріплена,

пристосована, або цифровими даними – закодованими електричними сигналами та електронними структурами, які при декодуванні надають інформацію.

У електронно-інформаційному середовищі приватність також може визначатися як "інформаційна приватність" – це все, що пов'язане з будь-якими засобами комунікацій та техніко-технологічними діями, які стосуються, зокрема, таємниці телефонних розмов, поштових, електронних повідомлень, сайтів, інстаграм, блогів, постів та багато ін.

Сьогодні в Європі, поряд з Регламентом GDPR, діє Директива 2002/58/ЄС "Про обробку персональних даних та захист таємниці ("приватності") в секторі електронних комунікацій" від 12 липня 2002 року [17]. Вона передбачає можливість держав-членів ЄС здійснювати перехоплення інформації, переданої за допомогою електронного зв'язку, або ухвалювати інші необхідні заходи для кожної із цих цілей, відповідно до Конвенції РЄ про захист прав людини і основоположних свобод, і роз'ясненнями, що визначаються в постановах Європейського суду з прав людини. Такі заходи повинні бути строго пропорційними до визначеної мети та необхідними в межах демократичного суспільства, а також бути адекватними у заходах безпеки згідно загальних приписів зазначеної Конвенції.

Стосовно Регламенту GDPR, то він не застосовується до обробки персональних даних по відношенню до питань національної безпеки, які підпадають під дію Розділу V Договору про Європейський Союз, і діяльності правоохоронних органів (для цілей попередження, розслідування), а також до обробки персональних даних державами-членами ЄС по відношенню до загальної зовнішньої політики і політики безпеки ЄС. Персональні дані, які обробляються державними органами в цілях запобігання, розслідування, виявлення або судового переслідування злочинів або виконання покарань, зокрема по запобіганню загрозам суспільній безпеці і вільного переміщення таких даних, регулюються Директивою (ЄС) 2016/680, див. [2, с. 104-156].

В США існують два рівня правової регламентації будь-яких значимих відносин: на рівні федерації й на рівні штатів, чиї повноваження в області законотворчості по Конституції США дуже широкі. Законодавство штатів США автономне у своїй правовій творчості [18]. Щодо сфери приватності чинними для федеральних органів є закони: *Privacy Act of 1974, 5 U.S.C. § 552a* ("Закон про приватність") та *The Electronic Communications Privacy Act (ECPA) of 1986, 18 U.S.C. § 2510* ("Закон про приватність електронних комунікацій") [19]. При цьому, недоторканність приватного життя забезпечується також галузевим законодавством [20].

В державі одночасно існують дві моделі щодо сфери приватності. Перша передбачає необхідність забезпечення захисту шляхом використання різних форм саморегулювання, при якій провайдер може переглядати особисте електронне листування, зокрема, у випадку підозри про наявність збитку або з добровільної згоди відповідної людини. Інша – обмеження прав на приватність шляхом розширення повноважень поліції й спецслужб з прослуховування персональних розмов. Ця модель має дві складові. Перша передбачає – усі цифрові засоби, телефонні, стільникові і супутникові системи, а також комунікаційні технології, які удосконалюються, у тому числі Інтернет, повинні мати можливості контролю ззовні. Друга – спрямована на обмеження поширення криптографічних програм, які дозволяють громадянам самостійно шифрувати свої повідомлення.

Про "право бути наданим самому собі", зокрема й у контексті комунікацій, в США вперше заговорили в 1890 році, коли американський юрист Луїс Брэндейс і журналіст Сэмюэль Уоррен опублікували в журналі "Harvard Law Review" статтю "The Right to Privacy" (буквально – "право на приватність") [21]. Вони стверджували, що право на особисте життя не можна ставити в залежність від способу, яким здійснюється одержання інформації. Ця ідея була прийнята американською юстицією лише у 1934 р. (Л. Брэндейс

був тоді вже членом Верховного Суду), коли Конгрес США проголосував за Федеральний закон, який визнав за громадянами право на таємницю у комунікаціях у повному обсязі[1]. Поштовхом цьому слугував розвиток технічних та соціальних умов 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 та ПІБ, відомостей з медичних книжок, переписки з поштових карток, розмов по телефону та ін.) в особисте життя й несанкціонований та комерційний продаж інформації про людину.

Комерціалізація інформації про людину отримала початок у США у 1886 році, коли шовкоторговець Л'юіс Тепен із Нью-Йорка створив агентство збору та аналізу інформації про кредитоспроможність підприємців, які зверталися до нього за позикою. Накопичивши декількох томів кредитних звітів, він став продавати інформацію. Клієнти платили від 100 до 200 дол. у рік [22].

За деякими результатами досліджень цього "феномена", світовий ринок персональних даних на початку 2000 рр. досягав більш як $3 млрд.: відомості про людину, її матеріальний стан, особисте життя "відбираються" з різноманітних баз даних та реалізуються завдяки Інтернет. У ті часи коштувала така БД від $10 (дрібний продаж) – до $1500 (продаж через Інтернет). Інформація мобільного зв'язку також потрапляла та потрапляє на чорний ринок (номер коштує $50, прослуховування – $150 за рік.) [23].

Вся ця, звичайно, несанкціонована діяльність значно поширилась у всьому світі та здійснюється не лише завдяки активності окремих фігурантів, а й комерційних структур, зокрема, за допомогою програм типу "cookies", збирання анкет для маркетингу, електронних та IP-адрес, примусу надавати ПІБ, особисті телефонні номери (існує можливість крадіжки коштів завдяки е-банкінгу), надавати про себе всю інформацію для отримання входу на сайт, анонімним пропозиціям з матеріальними обіцянками та багато ін. Ті, хто займається маркетингом постійно вишукують нові шляхи для збору різноманітних відомостей про потенційних покупців та своїх конкурентів: їх інтереси, характер діяльності, погляди, оточення, стосунки та багато ін. Для бізнесу персональні дані – зручне, а тепер і необхідне доповнення із усього того, що надає Інтернет або інші мережі. Уже цілком чітко усвідомлено, що з допомогою засобів електронно-інформаційного середовища набагато легше збирати величезні обсяги різної інформації (ніж займатися звичайним промисловим шпигунством), а аналіз і взаємне ув'язування відомостей ("профілювання") забезпечує істотні прибутки в бізнесі [24]. При цьому активно працюють колекторські агентства, яким відомості про клієнтів несанкціоноване та масово передають (або отримують) не тільки банки, а й будь-які зацікавлені особи.

Таким чином, хоча інформація про людину (у електронних комунікаціях – персональні дані) й є предметом ототожнення та права конкретної людини на саму себе, а в реальних умовах життєдіяльності давно є товаром, який має грошово-мінову вартість та використовується з метою задоволення матеріального або ін. інтересу, вона (інформація) не розглядається як об'єкт власності відповідної людини.

Підсумовуючи, у будь-якому разі людина має розраховувати на приватність у комунікаціях та на реальні умови захисту та безпеки відомостей про її особисте життя.

---

[1] На сьогодні право на недоторканність приватного життя розглядається як одне з конституційних прав особи, хоча воно спеціально й не згадується в американській Конституції. На підставі цієї аргументації Верховний суд США у 1985 р. визнав його існування в обмеженому обсязі. На думку прибічників прайвесі, це право логічно випливає зі змісту 1-ої, 3-ої, 4-ої та 5-ої поправок до Конституції США, якщо тлумачити їх системно [20]. У загальному плані, в США немає єдності щодо тлумачення правової природи "права на приватність".

З юридичної точки зору можна запропонувати такий зміст дефініції, а саме: *приватність у комунікаціях – це право людини на таємницю особистого життя та захист недоторканності від сторонніх на неї зазіхань у сфері інформаційної взаємодії, незалежно від засобів якими здійснюється одержання відомостей (даних) про людину*.

Конфіденційність приватності. У загальному розумінні, конфіденційність (*confidentia* – від лат. "довіра", "прихованість", "секрет" або "таємниця") передбачає наявність властивості об'єкта (предмета) на обмежений доступ, зокрема інформації, що обумовлює умови правоспроможності фізичних або юридичних осіб у ознайомленні та можливостями використання.

Конфіденційність інформації стосується усіх відомостей з обмеженим доступом, які є складовою відповідного виду таємниці: особиста (приватна), професійна, комерційна.

Чіткої класифікації видів конфіденційної інформації немає. Налічується більше 30 її різновидності, одну з яких засновано на суб'єктності права власності на інформацію.

У сфері приватності "конфіденційність" – це форма захисту відомостей про особисте життя людини, тобто захисту та безпеки приватності персональних даних.

Поняття "конфіденційність" згадується у Регламенті GDPR у пп. 39, 49, 75, 83, 85, 163 Преамбули та у ст. 14, 28, 32, 38, 54, 76 Регламенту, але юридичного його визначення та суттєвих ознак не наведене.

В Україні, згідно ст. 21 Закону України "Про інформацію", "конфіденційна інформація" віднесена до інформації з обмеженим доступом (одночасно з "таємною" та "службовою"). У Законі зазначено – "*конфіденційною є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень*".

Згідно ст. 7 Закону України "Про доступ до публічної інформації", також маємо визначення: "*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*".

Незважаючи на деяку відмінність у визначеннях, загальним їх недоліком є те, що вони не надають ознак сутності самого предмета поняття "конфіденційність", тобто не зрозуміло про що йде мова (крім діяльності з нею), та сприяють різним особисто-суб'єктивним уявленням. Це відноситься до всього законодавства, див. [25, с. 38-40].

Іншою інформацією з обмеженим доступом, яка може бути пов'язана з конфіденційністю, є "службова інформація". Її визначення у законодавстві немаємо. Ст. 9 Закону України "Про доступ до публічної інформації" обмежується посиланням на переліки відомостей, що становлять службову інформацію, які складаються органами державної влади, органами місцевого самоврядування, ін. суб'єктами владних повноважень[2].

Хоча "службова інформація" за Законом України "Про інформацію" є окремою категорією обмеженого доступу, вона, як і "конфіденційна інформація", не має чітких предметно-суттєвих ознак, за якими може визначатися. Й це, до прикладу, при тому, що персональні дані людини можуть становити службову таємницю для судді, якій є державною посадовою особою, і професійну таємницю для працівника кадрової служби комерційної фірми.

Вважаємо, якщо службова інформація стосується сфери приватності та у зв'язку з потребою захисту відомостей про особисте життя людини, вона може визначатися як

[2] *Прим.* До прикладу, стосується відомостей щодо спеціального режиму збирання, зберігання, обробки, поширення та їх використання згідно Переліку відомостей, що становлять службову інформацію в системі Міністерства внутрішніх справ: наказ МВС України від 27.05.16 р. № 432.

“конфіденційна”. Однак навряд це реально практикується та приймається до уваги в умовах відсутності на сьогоднішній день чіткого, безперечного правового поділу між різними видами таємниць. Проте головне у іншому – законодавство України має значну кількість актів, які надають лише переліки інформації про особу з посиланням на її “конфіденційність”, у відсутності предметно-суттєвих ознак, за якими її можна визначати.

У той же час існує Державний стандарт України “Технічний захист інформації. Терміни та визначення” (ДСТУ 3396.2-97) [26], якій віднесено до угруповання 01.040.35 “Інформаційні технології” згідно п. 42. Переліку державних стандартів України. Він юридично та предметно визначає поняття “конфіденційність”, надає суттєві її ознаки крізь тріаду повноважень права власності: користування, володіння та розпорядження. Але практично цей чинний стандарт не згадують та не застосовують. Хоча добре відомо, що лише інститут права власності, як жоден інший є найбільш потужним з юридичних засобів забезпечення прав людини, у стані вирішувати проблеми в сфері приватності та захисту персональних даних на якісному рівні. Тим більше, з одного боку, придання у ЄС вихідним принципам щодо обробки персональних даних людини категорії “основоположне право”, а з іншого, наявність проблем цифрової трансформації, можуть визначати потребу у нових, нетрадиційних поглядах на упорядкування та регулювання суспільних відносин.

Виходячи з юридичних поглядів та загальноприйнятих підходів по відношенню до трактування поняття “конфіденційність”, можна запропонувати такий зміст дефініції, а саме: *конфіденційність приватності у інформаційній сфері – це форма захисту відомостей (даних) про особисте життя людини, яка визначається домовленістю та зобов’язанням будь-яких суб’єктів не розголошувати їх третій стороні*.

Захист приватності персональних даних. У загальному розумінні поняття “персональні дані” охоплює об’єктивні та суб’єктивні відомості про особисте, сімейне чи публічне життя фізичної особи, що виражені у формі літер, чисел, графіки, фото, звуку чи відео символів, якщо вони дозволяють ідентифікувати таку особу. Для визнання відомостей персональними даними обов’язковою є наявність зв’язку між такими відомостями та конкретною особою.

Початок досліджень у вирішенні проблеми створення в Україні системи захисту персональних даних було покладено у 1995 р. у Національному агентстві з питань інформатизації при Президенті України. На той час, у більшості європейських країн вже було запроваджені відповідні закони, а ще у 1981 році вступила в дію перша угода світового рівня – Конвенції Ради Європи “Про захист осіб у зв’язку з автоматизованою обробкою персональних даних”. В Україні питання прийняття закону для регулювання відносин у сфері захисту персональних даних дискутувалось впродовж 15 років, див. у [27].

Потрібен час, щоб прийти до думки про те, що поняття “захист персональні дані” – це не просто “захист даних або відомостей” про людину, яке визначає лише “форму-оболонку” цільової спрямованості їх внутрішнього змісту, завдяки прийнятій умовності розуміння букв, знаків, інших символів, сигналів тощо для відображення значеннєвого наповнення. У “формі” міститься основа реального змісту їх “сенсу”, а саме – бажання людини жити своїм життям при мінімальному сторонньому втручанні та у захисті особистого життя у відносинах з іншими людьми та державою, що й визначає соціально-правову потребу у практичному вирішенні проблем “приватності” та створення умов реального захисту прав людини.

Забезпечення приватності у сфері персональних даних є вкрай складною проблемою у зв’язку з тим, що вона стосується багатогранних та багатоаспектних питань життя та життєдіяльності людини, які слабко піддаються регламентації, та,

одночасно, необхідності створення збалансованості забезпечення прав людини та інтересів безпеки держави. Це вимагає однозначного трактування понять та їх юридичного визначення у чітких термінах, інше – неприпустимо для нормативного акта.

Виходячи з приписів багатьох міжнародно-правових актів, головний сенс яких полягає у тому, що *право на життя, свободу і власність є найважливішими природними правами людини*, а також – Конституції України – *людина, її життя і здоров'я, честь і гідність, недоторканність і безпека визнаються в Україні найвищою соціальною цінністю,* ще у 1998 році, у першій моделі законопроекту про захист персональних даних, було запропоновано запровадити у сферу захисту персональних даних України спеціальний інститут права власності людини на свої персональні дані [28][3]. Головна ідея виходила з того, що численність різноманітних актів щодо сфери персональних даних, нерідка невизначеність і важкість у сприйнятті норм та нормативна складність взагалі, будь-які адміністративні і організаційні заходи[4], обмеження, умовності та багато ін. не дуже надають захист людині так, як це може єдино потужний інститут власності.

Надалі дослідження з питань сфери персональних даних були продовжені, а їх результати представлено в ряді наукових праць в контексті стану, тенденцій і подальших перспектив у захисті та безпеці персональних даних [1; 7; 25; 27], зокрема в умовах цифрової трансформації та пов'язаних з нею проблем правового регулювання нових суспільних відносин у цій сфері, а також досліджено новий погляд на власність людини в сфері персональних даних у контексті словосполучення *"право приватної власності людини на свої персональні дані"* [29].

До вказаного можна додати, що за неофіційним повідомленням, питання власності на персональні дані було предметом розгляду інституцій ЄС, але єдності щодо правової природи "власності на персональні дані" так і не отримало.

Сьогодні чи навряд хто не згодний з тим, що світ рухається шляхом активного, малопередбачуваного розвитку процесів в електронно-інформаційному середовищі. Уже предметно обговорюється питання щодо "*цифрової людини, яка має бути визнана спеціальним суб'єктом правовідносин, спеціальною правовою персоною*" [30], штучним інтелектом, який вже почав здобувати здатність, що вважалася винятково людською прерогативою, – здатністю до навчання [31], у тому числі й у правотворчої діяльності [32]. Видання MIT Technology Review повідомляло [33] про успіхи по створенню штучного інтелекту для проектування інших систем штучного інтелекту, тобто про факти його самовдосконалення, у Массачусетському технологічному інституті, Каліфорнійському університеті в Берклі та у компанії Google.

У квітні 2021 р. Єврокомісія представила проект рекомендацій з регулювання штучного інтелекту [34], а у червні 2021 р. на саміті США-ЄС ухвалене рішення про

[3] Проект закону був внесений у 2003 р. народними депутатами України Родіоновим М., Ніколаєнко С., Юхновським І., Толочко П., Ситником К., прийнятий 13.03.2006 р. у 2-му читанні в цілому як Закон, але далі був скасований. На підставі проекту, у червні 2010 р., Верховна Рада України ухвалила інший проект закону України "Про захист персональних даних". У Законі було визначено – суб'єкт персональних даних має *особисті немайнові права* (тобто, не має економічного змісту) на персональні дані. Поняття "особисті немайнові права" було залучено з Цивільного кодексу України і застосовується лише у нашій державі. У міжнародному праві, праві ЄС, а також у законодавствах інших країн його не існує.

[4] Європейські правові стандарти визначають обов'язковість у виконанні приписів законодавства ЄС щодо створення незалежного, контролюючого органу з захисту персональних даних. На жаль, в Україні не створено відповідної та ефективної системи організації захисту прав людини у вказаній сфері (це сталося після внесення змін до законодавства у 2011 – 2013 рр.). Функції контролю стану справ було покладено на Уповноваженого Верховної Ради України з прав людини, що не відповідає нормам Конституції України.

розробку загальних підходів у використанні штучного інтелекту, керуванню даними та політиці щодо технологічних платформ [35]. За думками експертів – етичні проблеми штучного інтелекту в найближчі роки будуть ставати серйознішими й складнішими. Одна з них стосується приватності при застосуванні технологій штучного інтелекту [36].

Алгоритми штучного інтелекту, в основі яких лежать нейромережі зі зворотним зв'язком, вже здатні збирати багато персональних даних завдяки технологій "Хмарних обчислень" та "Великих Даних". Вони стали створювати умови фундаменту загальної конвергентно-аналітичної інтеграції в інформаційній сфері, завдяки можливостей швидко, більш предметно і повніше проводити автоматизований збір, фільтрацію, сортування, структуризацію і аналіз величезних обсягів даних та отримувати надсумарно-якісний ефект [37]. Терміном "Великі Дані" (*Big Data*) прийнято описувати обробку великих масивів різноманітної інформації з складною, неоднорідною або невизначеною структурою, що спрямована на параметри, які скорочено позначають як "3V"(по перших буквах англ. слів): *volume* – "обсяг", *velocity* – "швидкість" і *variety* – "різноманіття" [38]. Збираючи дедалі більше відомостей про конкретну людину, володілець алгоритму штучного інтелекту – державна або правоохоронна структура, компанія або будь-яка окрема особа, може одержати інформацію про різноманітні аспекти приватності людини, зокрема до прикладу щодо виборчих компаній, – які заходи буде відвідувати й коли, що прагне почути, за кого схильна (або ні) голосувати й багато ін. При цьому, будь-які відомості про приватність можуть дозволити не лише маніпулювати людиною, а й використовувати її у групових, корпоративних тощо інтересах.

Людство вже не повернеться назад і не відмовиться від технологій штучного інтелекту. Це отримало, навіть, назву – "технологічна сингулярність", зі смутною перспективою для людини, на що вказував, зокрема, М. Хайдеггер [39]. Про поглиблення проблем у співіснуванні людини й техніки ще у часи індустріалізації говорив, у своєму стилі, навіть В. Маяковський – *Насувається навала техніки. І якщо на неї не надягти естетичний намордник, вона всіх покусає* [28, с. 55]. Висновок з вказаного може полягати у тому, що сучасній світ стоїть на грані грандіозних змін. Головна причина – бурхливе вдосконалення й розвиток техніки та технологій приводить до того, що вони стають усе більш витонченими та розумними, а техніко-технологічний прогрес у майбутньому буде тільки більше, ширше й активніше використовуватися в самих різних сферах життєдіяльності.

Як вважаємо, може й не дуже ефективний засіб вирішення зазначених проблем, але є потреба задати хоча б рамки етичного кодексу "поведінки" штучного інтелекту з умовами захисту та безпеки приватності персональних даних (не відомо, як буде "переробляти" вказане штучний інтелект). Взагалі ж відомо, що у GDPR, проекті ЄС про "e-Privacy Regulation" [40] та "NIS Directive" [41] проблема "штучний інтелект – захист та безпека персональних даних" не розглядається або поки не має чіткого предметного вирішення.

Сучасна юриспруденція продовжує дуже повільно сприймати потребу у змінах підходів та засобів в упорядкуванні відносин у інформаційній сфері. Як деякий підсумок – законодавство про приватність та захист персональних даних в жодній країні світу не отримало своєї зрілості, насамперед на понятійно-термінологічному рівні. Повної адекватності національних законодавств не досягнуто. Основною дилемою нормативно-правового упорядкування відносин у сфері персональних даних є суперечність між прагненням максимального їх використання у корпоративних, державних та ін. інтересах, й, одночасно, бажання та спроби кожної окремої людини захистити свої особисті права від несанкціонованих дій з її персональними даними.

Щодо визначення, з юридичної точки зору можна запропонувати такий зміст дефініції, а саме: з*ахист приватності персональних даних – це нормативно-правові та*

соціальні умови, процес та результат забезпечення інформаційної недоторканності особистого життя та життєдіяльності людини, яка ідентифікована або може бути ідентифікованою.

Безпека приватності персональних даних. Безпека приватності персональних даних є складовою частиною інформаційної безпеки людини, суспільства та держави, яка безпосередньо пов'язана з негативними інформаційно-психологічними впливами через, зокрема, несанкціонований виток персональних даних, інформаційне насильство, інформаційний тероризм, маніпуляції свідомістю громадян та багато ін., про що йдеться у [42]. Це дає підстави запровадження у науковий та юридичний обіг визначення поняття "безпека приватності персональних даних".

В законодавстві України немає словосполучення "безпека приватності персональних даних" (або "безпека персональних даних"). У Законі України "Про Основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки" від 09.01.07 р. № 537-V [43] закріплено лише термін "інформаційна безпека". Згідно п. 13 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".

У вищезазначеному про "процес захищеності" прямо не ідеться.

Щодо розуміння сенсу слів (тобто, внутрішнього змісту предмета) "цілісність", "конфіденційність" та "доступність", то у законодавстві це залишається без предметно-ознакового визначення. Так, до прикладу, у досить компактній роботі [44], зазначається: *"До суттєвих ознак* (курсів – *Авт.*) поняття *інформаційної безпеки* відносять *конфіденційність* (стан інформації, при якому доступ до неї отримують тільки суб'єкти, які мають на це право), *цілісність* (запобігання несанкціонованій або незаконній модифікації інформації) та *доступність* (запобігання тимчасового або постійного приховування інформації від користувачів, які отримала право на доступ)".

Вважаємо, по-перше, мова у вищенаведеному йде не про "суттєві ознаки" (показники, за якими визначається предмет) інформаційної безпеки, а про "складові дій" (частини, які входять до єдиного утворення, цілого). По-друге, "конфіденційність" це не "стан інформації", а "форма її представлення", на певний час.

Враховуючи запроваджене у законодавство поняття "інформаційна безпека", можна запропонувати такий зміст дефініції: *безпека приватності персональних даних – це стан та процес забезпечення захищеності у недоторканності відомостей (даних) про особу від нецільового та несанкціонованого збирання, зберігання, використання та поширення у зв'язку з їх опрацюванням (обробкою)*.

Схематично, перелік та кореляція ключових понять у зв'язку з захистом та безпекою приватності персональних даних, див. на Рис.

Висновки.

Не претендуючи на семантично-понятійну завершеність та однозначність сприйняття, приведемо тлумачення поняття "приватність" та супутніх йому словосполучень.

1. ***Приватність*** (англ. – privacy), у англо-сакському розумінні, – це можливості та право "людини на самоту", "бути залишеною у спокої", "бути наданою самої собі". З юридичної точки зору, *приватність – право людини на таємницю особистого життя і захист від сторонніх на неї зазіхань*.

“Приватність”, як семантично-домінантне поняття, у інформаційній сфері пов’язано з такими основними словосполученнями-термінами: інформаційна приватність, приватність у комунікаціях, конфіденційність приватності, захист та безпека приватності персональних даних людини.

Інформаційна приватність передбачає наявність нормативно-правового захисту прав людини в інформаційній сфері, згідно її особистих уявлень, інтересів та намагань у житті. З юридичної точки зору, *інформаційна приватність – право людини на недоторканність та захист відомостей (даних), які стосуються або пов’язані з особистим її життям.* Інформаційна приватність безпосередньо пов’язана с такими поняттями, як: “приватність у комунікаціях”, зокрема з Інтернет-приватністю; в контексті забезпечення таємниці відомостей про особисте життя – з “конфіденційністю приватності”; в контексті запобігання несанкціонованим зазіханням на відомості про особисте життя – захистом та безпекою приватності персональних даних.

Рис.

Приватність у комунікаціях *– право людини на таємницю особистого життя та захист недоторканності від сторонніх на неї зазіхань у сфері інформаційної взаємодії, незалежно від засобів якими здійснюється одержання відомостей (даних) про людину.*

Конфіденційність приватності *– форма захисту відомостей (даних) про особисте життя людини, яка визначається домовленістю та зобов'язанням будь-яких суб'єктів не розголошувати їх третій стороні.*

Захист приватності персональних даних *– нормативно-правові та соціальні умови, процес та результат забезпечення інформаційної недоторканності особистого життя та життєдіяльності людини, яка ідентифікована або може бути ідентифікованою.*

Якщо розглядати захист приватності в контексті власності людини на свої персональні дані, то оцінка ознак предмета захисту може виходити з такої формули: *право приватної власності людини (фізичної особи) на персональні дані* – це сукупність приписів та норм, які регулюють право володіння, користування та розпорядження персональними даними людини про свою особу, за умов збалансованості та узгодженості цього права з правами інших громадян та потребами суспільства і держави у безпеці.

До зазначеного, *володіння персональними даними* – це наявність можливості людини та нормативно-правових умов забезпечення приватності персональних даних в незмінному вигляді; *користування персональними даними* – це наявність можливості людини та нормативно-правових умов забезпечення використання відомостей про себе на власний розсуд; *розпорядження персональними даними* – це наявність можливості людини та нормативно-правових умов забезпечення права на управління доступу до відомостей про себе, крім випадків визначених законом. Більш детально йдеться у [27, зокрема, с. 105-108].

Вважаємо важливим звернути увагу на наступне. У зв'язку з різноманітністю, різнобічністю життєдіяльності та потребами безпеки суспільства, "абсолютного" права приватної власності на самого себе в інформаційній сфері не існує. Проте це право стосується кожної людини в контексті історично визначених у суспільстві та пошуків напрямів подальшого удосконалення "принципів моралі, етики та правосвідомості", які спрямовуються природною потребою людини – визначати її тією, що для неї найкраще.

Безпека приватності персональних даних *– стан та процес забезпечення захищеності у недоторканності відомостей (даних) про особу від нецільового та несанкціонованого збирання, зберігання, використання та поширення у зв'язку з їх опрацюванням (обробкою).*

2. Визнання та обов'язковість у виконанні приписів європейських правових стандартів щодо основоположних прав захисту фізичних осіб у зв'язку з обробкою персональних даних, передбачає підвищення точності ключових юридичних дефініцій та однозначності у тлумаченні понять шляхом застосування семантичної оцінки ознак предмета захисту та безпеки приватності персональних даних. А це вимагає, зокрема, не лише внесення юридичних змін у зв'язку з появою нових міжнародно-правових документів, а, головне, концептуального оновлення відповідного законодавства.

3. Технологічно-цифрова та соціальна трансформації у суспільстві, перспективи поглиблення протистояння прав людини і прав "цифрової людини, як суб'єкта правовідносин", та спрямованість на збереження людини як виду, все більше потребують нової юридичної конструкції захисту приватності в контексті власності людини на свої персональні дані, тобто – надання людині специфічно-матеріального правового статусу "права власності на себе". Як вважаємо, ідейна підстава вищезазначеного узгоджується з поглядами англійського правознавця Д. Локка та тотожно-адекватна поглядам "батька приватності", члена Верховного Суду США Луїса Брэндейса, який ще на початку епохи індустріалізації відстоював право людини "бути наданою самій собі", хоча про "власність на приватність" у той час не могло бути й мови.

4. Зміни у соціальних процесах, зокрема завдяки застосуванню засобів електронно-інформаційного середовища, незворотне удосконалення та самовдосконалення штучного інтелекту (коли останній зможе приймати самостійні рішення, навіть на шкоду людині), захист прав людини в інформаційному середовищі в плані створення умов ефективного правового забезпечення захисту та безпеки приватності персональних даних, потребує більш значної, порівняно з сьогоденням, уваги органів державної влади не лише в правовому, але й адміністративно-організаційному та методологічному забезпеченні.

Вказане можна охарактеризувати тим, що у політичних, економічних, соціальних процесах життєдіяльності, нескінченності війн, революцій, переворотів, конфліктів, існує та завжди буде існувати (нерідко таємно, не усвідомлено) проблема пошуку людиною гарантій справедливих умов "особистої автономії". У державі воно може визначатися як "правовий суверенітет особистості", складовою якої є інформаційна приватність. Й важливим при цьому є те, що навряд чи технологічні досягнення та перспективи їх майбутнього зможуть ("забажають") надати гарантії справедливості людині, крім того, що може надати природне право власності людини на саму себе, яке є складовою дійсно правової держави.

5. В Україні законопроект про захист персональних даних розроблявся з 1997 року, мав 8 версій у 23 редакціях, та у декілька циклів неодноразово проходив узгодження з міністерствами, відомствами та експертним управлінням ВР України до 2010 року, у якому був прийнятий як закон.

З 2010 р. по наш час було прийнято не менше як 7 редакцій Закону України "Про захист персональних даних" [27, с. 74-85], які мали рамочно-базовий характер. На жаль, їх зміст, незважаючи на різні офіційні пояснення, мало що пояснював й не лише "пересічній людині" – як практично захистити свої права в умовах не повної визначеності понятійних, термінологічних та нормативних формулювань, що ускладнює розуміння та реальні можливості практичного захисту.

Сьогодні здійснюється робота з удосконалення законодавства України у плані запровадження приписів Регламенту (ЄС) 2016/679 (законопроект № 5628 від 07.06.21 р.). Преамбула проекту містить таке формулювання: *"Цей Закон визначає правові відносини, пов'язані із захистом і обробкою персональних даних, з метою забезпечення прав людини на захист персональних даних та повагу до особистого і сімейного життя"*.

Наше занепокоєння полягає в наступному.

По-перше. Як вважаємо, предметом законопроекту повинен бути не "захист даних", а ***захист основоположного права фізичних осіб*** *у зв'язку з обробкою персональних даних* (про що йдеться у п. 1 Преамбули Регламенту (ЄС) 2016/679), основу чого й складає головний принцип права – тобто, право на справедливість щодо сенсу та змісту того, що потребує захисту – тобто ***право на приватність*** *особистого і сімейного життя.*

По-друге. Також вважаємо, продовжує існувати недосконаліть термінологічного апарату. Законопроект має враховувати у повному обсязі викладене у ст. 4 Регламенту (ЄС) 2016/679 від 27.04.16 р., а також, можливо, напрацювання цієї статті.

По-третє. Деякі положення законопроекту не відповідають ***принципу правової визначеності***, який потребує *"чіткості, зрозумілості й однозначності правових норм, зокрема, їх передбачуваності (прогнозованості) та стабільності"* (абз. 6 п. 2.1 Рішення Великої палати Конституційного Суду України від 20.12.2017 р. № 2-р/2017) [7]. *"Юридична визначеність – це передовсім недвозначність"* (п. 10 Рішення Великої палати Конституційного Суду України від 14.07.2021 р. № 1-р/2021) [8]. Не врахування вказаного може ускладнювати подальше правозастосування.

По-четверте. У принципі, законопроект передбачає оцінювання *"контролюючим органом"* стану дотримання прав людини та основоположних свобод під час встановлення відповідності рівня захисту персональних даних. Проте, згідно європейських правових стандартів, відповідного *"контролюючого органу"* в Україні немає, а належна регламентація порядку проведення такої процедури у законопроекті відсутня. При цьому Уповноважений Верховної Ради України з прав людини вважає, що даний проект потрібно розглядати разом з законопроектом про створення *"спеціального органу з питань захисту персональних даних"*. Тобто мова йде про створення ще додаткового закону.

До вказаного, незрозумілі повноваження Уповноваженого Верховної Ради України з прав людини у сфері захисту персональних даних у зв'язку з тим, що у проекті не передбачено виконання ним зазначених повноважень.

По-п'яте. Реалізація положень нового європейського порядку захисту персональних даних (Пакет GDPR-2016), Директиви 2002/58/ЄС, Директиви ЄС "NIS Directive", а в майбутньому Регламенти ЄС про "e-Privacy Regulation" та про "довіру до штучного інтелекту", в умовах розвитку та конвергенції цифрових технологій, зокрема, "Великі Дані", "Хмарні обчислення", "Інтернет речей" тощо, а також перманентність у змінах інтерфейсів і протоколів, безлічі стандартів та ін., дедалі більше ускладнюють реальні можливості практичного захисту права людини на приватність. Головне у тому, що кожного разу поява нових технологій та європейських актів буде вимагати переробки національного закону.

Виходячи з завдання впровадження у національне законодавство правил передбачених Регламентом (ЄС) 2016/679, з урахуванням можливості держав-членів мати простір для маневру у визначенні власних правил (п. 10 Преамбули Регламенту), та не виходячи за межі повноважень, визначених, зокрема у Article 16 (ex Article 286 TEC) зведених актів Договору про Європейський Союз та Договору про функціонування Європейського Союзу [45], можна запропонувати розробку *консолідованого законодавчого акту* України – *Про захист та безпеку приватності персональних даних*, складовими якого можуть бути:

– *основна частина*: визначення термінів; загальні положення; права суб'єкта приватності персональних даних; види діяльності з обробки персональних даних; основні принципи, підстави та спеціальні вимоги з обробки персональних даних; порядок доступу до персональних даних третіх осіб; обробка персональних даних правоохоронними органами; заходи безпеки приватності персональних даних тощо, які визначають основи регулювання відносин в сфері забезпечення приватності персональних даних на території України;

– *особлива частина*: захист приватності у зв'язку з обробкою персональних даних у сфері електронних комунікацій за суб'єктною ознакою щодо галузей (областей) інформаційної діяльності та з екстраполяцією положень основної частини; обов'язки контролера і оператора щодо захисту та безпеки приватності персональних даних; Уповноважений державний орган з питань захисту персональних даних та контроль за додержанням законодавства у сфері захисту та безпеки приватності персональних даних; відповідальність за порушення законодавства про захист та безпеку приватності персональних даних тощо на території України;

– *спеціальна частина*: приписи європейських правових стандартів у сфері захисту персональних даних – основні положення регулювання відносин суб'єктів України з міжнародними організаціями тощо; критерії транскордонної передачі персональних даних.

Враховуючи напрацювання, які надано у цій статті, результати роботи щодо закону можуть дозволити мати документ із перспективою довгострокового його функціонування, остання частина якого буде лише наповнюватися згідно з поточними змінами законодавства ЄС і РЄ, зокрема, у зв'язку з розвитком цифровізації, а також, при необхідності, внесення лише окремих змін в основну або особливу частини.

Використана література

1. Пилипчук В.Г., Брижко В.М. Трансформація системи захисту персональних даних та приватності в контексті євроінтеграції України. *Вісник Національної академії правових наук України*: зб. наук. праць. № 3(90)/2017. С. 36-50.
2. Сучасні правові стандарти Євросоюзу у сфері захисту персональних даних / І. Майстренко – перек. з англ.; В. Брижко – ред. тексту. Київ: ТОВ "Видавничий дім "АртЕк", 2018. 177 с.
3. Философская энциклопедия. Справедливость. URL: https://dic.academic.ru/dic.nsf/encphilosophy/1150/%D0%A1%D0%9F%D0%A0%D0%90%D0%92%D0%95%D0%94%D9B%D%98%D0%92%D0%9E%D0%A1%D0%A2%D0%AC
4. Про захист прав людини і основоположних свобод: Конвенції Ради Європи від 4.XI.1950 р. URL: https://zakon.rada.gov.ua/laws/show/995_004#Text
5. Privacy & Human Rights. Privacy International and Electronic Privacy Information Center, 1999. URL: //www.epic.org; Смирнов С. Приватность. – (Межрег. группа "Правозащитная сеть)". Москва: Изд. "Права человека". 2002. 95 с. С. 1.
6. Бельсон Я., Ливанов К. История государства и права США. Ленинград: Изд. Ленинградского университета, 1982. 167 с. С. 69.
7. Рішення Великої палати Конституційного суду України від 20 грудня 2017 року № 2-р/2017 у справі за конституційним поданням 49 народних депутатів України щодо відповідності Конституції України (конституційності) пункту 7 частини другої статті 42 Закону України "Про вищу освіту". URL: https://zakon.rada.gov.ua/laws/show/v002p710-17#Text
8. Рішення Великої палати Конституційного суду України від 14 липня 2021 року № 1-р/2021 у справі за конституційним поданням 51 народного депутата України щодо відповідності Конституції України (конституційності) Закону України "Про забезпечення функціонування української мови як державної". URL: https://zakon.rada.gov.ua/laws/show/v001p710-21#Text
9. Пилипчук В.Г., Брижко В.М. Інформаційна безпека та приватність у сфері захисту персональних даних. *Інформація і право.* № 4(19)/2016. С. 60-70.
10. 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
11. Брижко В.М. Персональні дані та право власності. *Українське право.* 2002. № 1. С. 152-157; Брижко В.М. Інформаційний продукт як об'єкт права власності. *Інформація і право.* № 4(23)/2017. С. 5-15; Брижко В.М., Фурашев В.М. Інформаційне право та інформаційне законодавство: наукове видання. Київ: ТОВ "Видавничий дім "АртЕк", 2020. 288 с. С. 93-101.
12. Джон Локк. Два трактата о государственном управлении. Кн. 2. Пункт 27. Глава V. "О собственности". URL: http://www.civis_book.ru/files/File/Lokk.Traktaty_2.pdf
13. Цит.: Olsaretti, Serena. 2004. Liberty, Desert and the Market. Cambridge University Press. P. 9.
14. Цит.: Dan-Cohen, Meir. 2002. Harmful Thoughts: Essays on Law, Self, and Morality. Princeton University Press. P. 296.
15. Богуцький П.П. Інформаційна приватність і публічність як сутнісні ознаки інформаційно- правових комунікацій: матеріали другої наук.-практ. конф. *Захист прав, свобод і безпеки людини в інформаційній сфері в сучасних умовах,* м. Київ, 21.05.2021. Київ, 2020. 258 с.
16. Корж І.Ф. Право на відкриті дані – як право приватного характеру. *Інформація і право.* № 1(28)/2019. С. 19-28.

17. Європейські нормативно-правові акти та підходи до упорядкування суспільних інформаційних відносин у зв'язку з автоматизованою обробкою даних: посібник. Кн. 2 / В. Брижко, М. Швець та ін. Київ: ТОВ "Пан Тот", 2006 р. 509 с. С. 379-392.

18. Защита персональных данных в США. URL: https://searchinform.ru/resheniya/biznes-zadachi/zaschita-personalnykh-dannykh/realizaciya-zashchity-personalnyh-dannyh/mezhdunarodnaya-sistema-zashchity-personalnyh-dannyh/v-ssha

19. Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. §§ 2510-2523. URL: https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285

20. Серьогін В.О. Прайвесі у США: політико-правова теорія і практика. *Форум права*. 2011. № 1. С. 891-897. URL: http://www.nbuv.gov.ua/e-journals/FP/2011-1/11cvotip.pdf

21. S.D. Warren., L.D. Brandeis. The right to privacy. Originally published in the *Harvard Law Review*, No. 5. December 1890. Vol. IV. P. 193-220. URL: https://faculty.uml.edu/sgallagher/Brandeis privacyhtm

22. Ходорович. Расколотая база. URL: //www.aferizm.ru/bb_bd.htm

23. Михеев В. Проблема правовой защиты персональных данных. URL: www.kiev-security.org.ua/box/4/136.shtml; Цена персональных данных – рыночная цена конфиденциальности, или буря в стакане воды. URL: www.i2r.ru/article.shtml?id=1384A; Брижко В., Швець М. Про економічний аспект захисту персональних даних у контексті права власності на інформацію. *Правова інформатика.*" № 1(9)/2006. С. 47-56.

24. Берд Киви. Анонимность в Сети как залог свободы. URL: //www.sdteam.com/articles/hack058.shtml

25. Брижко В.М., Пилипчук В.Г. Приватність, конфіденційність та безпека персональних даних. *Інформація і право.* № 1(32)/2020. С. 33-46.

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

27. Становлення і розвиток правових основ та системи захисту персональних даних в Україні: монографія / за ред. В.М. Брижка, В.Г. Пилипчука. Київ: ТОВ "Видавничий дім "АртЕк", 2017. 226 с.

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

29. Брижко В.М., Пилипчук В.Г. Безпека персональних даних: правові стандарти європейського союзу та сучасні прикладні проблеми. *Інформація і право*. № 1(36)/2021. С. 17-28;

30. Радутний О.Е. Мораль і право для штучного інтелекту та цифрової людини: закони робототехніки та "проблема вагонетки". *Інформація і право*. № 3(30)/2019. С. 78-95; Брайчевський С.М. Проблема персональних даних в системах Інтернету речей з елементами штучного інтелекту. *Інформація і право.* № 4(31)/2019. С. 61-67; Дзьобань О.П. Цифрова людина як філософська проблема. *Інформація і право*. № 2(37)/2021. С. 2-37; Радутний О.Е. Правовий статус та характеристика цифрової людини. *Інформація і право*. № 4(39)/2021. С. 22-39.

31. Нечеловеческие способности. URL: https://www.gazprom-neft.ru/press-center/sibneft-online/archive/2018-september-projects/1863686

32. Лиев Э.Р. Внедрение механизмов искуственного интеллекта в правотворческую среду: материалы 1-й Международной научно-практической конференции *Шаг в будущее: искусственный интеллект и цифровая экономика.* Вып. 3. Москва: Издат. дом ГУУ, 2017. 369 с. С. 153-159.

33. AI Software Learns to Make AI Software. URL: https://www.technologyreview.com/2017/01/18/154516/ai-software-learns-to-make-ai-software

34. Europe fit for the Digital Age: Commission proposes new rules and actions for excellence and trust in Artificial Intelligence. URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_1682

35. ЕС и США разработают общие принципы искусственного интеллекта. URL: https://internetua.com/es-i-ssha-razrabotauat-obsxie-principy-iskusstvennogo-intellekta; https://forklog.com/es-i-ssha-razrabotayut-obshhie-printsipy-iskusstvennogo-intellekta

36. Кривошапко Ю. Взяться за разум. URL: https://rg.ru/2020/01/14/eksperty-neobhodimo-sozdat-kodeks-povedeniia-iskusstvennogo-intellekta.htm

37. Брижко В.М., Фурашев В.М. Конвергенція новітніх технологій: стан і перспективи змін у інформаційних відносинах. *Інформація і право".* № 1(20)/2017. С. 51-67.

38. Больше, чем данные. URL: https://www.gazprom-neft.ru/press-center/sibneft-online/archive/2018-september-projects/1863684

39. Аблязов Н. Технологическая сингулярность. Исследование предпосылок возникновения и последствий для человечества. URL: https://mipt.ru/education/chair/philosophy/publications/aspers/a_1xes5v.php

40. ePrivacy Regulation. Proposal for a Regulation on Privacy and Electronic Communications (2017). URL: https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications; Confidentiality of electronic communicatio ns: Council agrees its position on ePrivacy rules. URL: https://www.consilium.europa.eu/en/press/press-releases/2021/02/10/confidentiality-of-electronic-communications-council-agrees-its-position-on-eprivacy-rules

41. The Directive on Security of Network and Information Systems (NIS Directive). URL: https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_3651

42. Брижко В.М. е-боротьба в інформаційних війнах та інформаційне право: монографія; за ред. члена-кореспондента АПрН України, д.е.н., професора М. Швеця. Київ: НДЦПІ АПрН України, 2007 р. 236 с. С. 41-117; Пилипчук В.Г., Дзьобань О.П. Теоретичні та державно-правові аспекти протидії інформаційному тероризму в умовах глобалізації. *Стратегічні пріоритети*. 2011. № 4. С. 12-17; Гуцалюк М.В. Новітні тенденції кіберзлочинності. *Інформація і право.* № 1(36)/2021. С. 79-89; Леонов Б.Д. Тероризм: інформаційно-правовий вимір. *Інформація і право.* № 2(37)/2021. С. 60-66.

43. Про Основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки: Закон України від 09.01.07 р. № 537-V. URL: //www.rada.gov.ua

44. Безуглий Д.С. Інформаційна безпека України: огляд останніх тенденцій. *Фізико-математична освіта*. 2018. Вип. 2(16). С. 2. URL: http://fmo-journal.fizmatsspu.sumy.ua

45. Consolidated version of the Treaty on the Functioning of the European Union. *Official Journal*. C. 326. 26/10/2012. P. 0001-0390. URL: http://data.europa.eu/eli/treaty/tfeu_2012/oj

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