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,*
академік НАПрН України.
ORSID: https://orcid.org/0000-0002-3754-4592.

БЕЗПЕКА ПЕРСОНАЛЬНИХ ДАНИХ: ПРАВОВІ СТАНДАРТИ ЄВРОПЕЙСЬКОГО СОЮЗУ ТА СУЧАСНІ ПРИКЛАДНІ ПРОБЛЕМИ

Анотація. *Стаття є продовженням низки наукових праць щодо стану, тенденцій і подальшого забезпечення безпеки персональних даних в умовах цифрової трансформації та пов'язаних з нею проблем правового регулювання нових суспільних відносин у цій сфері. Розглядаються та оцінюються ключові аспекти документів ЄС, затверджених останніми роками, зокрема, Регламенту GDPR, Директиви NIS і проекту правового акту про e-Privacy. Висвітлено основні критерії й актуальні проблемні питання, що потребують врегулювання в контексті імплементації правових норм ЄС та розвитку національного законодавства з питань захисту персональних даних.*

Ключеві слова: *безпека, персональні дані, правові стандарти, ЄС.*

Summary. *The article is a continuation of a number of scientific works on the state, trends and further ensuring security of personal data in the context of digital transformation and related problems of legal regulation of new social relations in this area. The key aspects of the EU documents approved in recent years, in particular, the GDPR Regulation, the NIS Directive and the draft legal act on e-Privacy, are considered and evaluated. The main criteria and topical issues that need to be addressed in the context of the implementation of EU law and the development of national legislation on personal data protection are highlighted.*

Keywords: *protection, security, personal data, European legal standards.*

Аннотация. *Статья является продолжением ряда научных работ, касающихся состояния, тенденций и перспектив дальнейшего обеспечения безопасности персональных данных в условиях цифровой трансформации, а также связанной с ней проблемой правового регулирования новых общественных отношений в этой сфере. Рассматриваются и оцениваются ключевые аспекты документов ЄС, утвержденных в последние годы, в частности, Регламент GDPR, Директива NIS и проект о e-Privacy. Освещены основные критерии и актуальные проблемы, которые требуют урегулирования в контексте имплементации правовых норм ЄС и развития национального законодательства по вопросам защиты персональных данных.*

Ключевые слова: *безопасность, персональные данные, правовые стандарты ЄС.*

Постановка проблеми. Пошуки у вирішенні правових проблем щодо природи людських цінностей здійснюються з часів римського права й донині. Це пояснюється поступовими і доволі тривалими змінами у розумінні демократичних цінностей і прав людини, зокрема, у сфері захисту персональних даних. Формування теоретичних поглядів і правових приписів з питань недоторканності приватного життя має менш тривалий історичний шлях, який розпочався з кінця XVII століття [1].

В останні десятиліття прийнято значну кількість міжнародних актів (резолюцій, конвенцій, директив, протоколів, рекомендацій) Організації Об'єднаних Націй, Ради Європи, Європейського Парламенту і Ради Європейського Союзу, які безпосередньо або опосередковано стосуються правового регулювання захисту персональних даних

(наприклад, див. у [2]). Наявність великого переліку галузевих та інших документів, а також їх обсяги вражають і навіть можуть сприяти уявленню про послідовність та глибину наукових розробок у регулюванні суспільних відносин у цій сфері. Однак, як свідчить аналіз, практика сучасного життя ще залишається досить далекою від наявних теоретичних здобутків і нормативно-правової бази, а головне – від розуміння глибини суспільних трансформацій та потреби кардинального перегляду питань врегулювання суспільних відносин, які нині динамічно змінюються.

Сьогодні новітні інформаційні технології, які спочатку мали конкретне функціонально-цільове призначення, в умовах цифрової трансформації інтегруються з іншими технологіями і можуть надавати не лише нову якість результатів їх сумісного (сумарного) використання, але й створювати нові загрози та більші можливості для несанкціонованого отримання й використання персональних даних людини.

Проблеми розбудови та ефективності систем захисту персональних даних є предметом активних наукових розвідок та висвітлені у працях іноземних та українських вчених [3], але продовжують викликати багато правових та нормативних питань.

Метою статті є оцінка низки актуальних теоретичних та прикладних проблем у сфері захисту та безпеки персональних даних людини.

Виклад основних положень. У травні 2016 року Європейський Парламент і Рада затвердили постанову про нові правила і порядок захисту персональних даних – General Data Protection Regulation (далі – GDPR, з англ. "Пакет захисту даних"), який передбачає умови забезпечення узгодженої нормативно-правової бази на європейському рівні.

Головним документом, який визначає на території держав-членів ЄС застосування обов'язкових правил, є Регламент (ЄС) 2016/679 "Про захист фізичних осіб у зв'язку з обробкою персональних даних та про вільне переміщення таких даних, а також про скасування Директиви № 95/46/ЄС (Загальні Положення про захист даних)" від 27 квітня 2016 р. (див. [4, с. 2-103]).

Регламент GDPR має понад 100 стор. тексту, з яких Преамбула-роз'яснення наступних приписів складає 44 стор. (173 роз'яснення), де йдеться про підходи до правового регулювання захисту персональних даних у контексті раніше прийнятих документів ЄС та намаганнями врахування проблем щодо нових технологічних досягнень.

Важливою новацією Регламенту GDPR є те, що вперше у документах сфери захисту персональних даних офіційно констатовано (п. 1 Преамбули): *"**Захист** фізичних осіб у зв'язку з обробкою персональних даних **є основоположним правом**"* (курсів – *Авт.*). Далі, у п. 11 Преамбули, зазначено: "*Ефективний захист персональних даних на усій території ЄС вимагає зміцнення та детального визначення прав суб'єктів даних* та обов'язків осіб, які визначають та здійснюють обробку персональних даних". А згідно з п. 10 Преамбули щодо удосконалення законодавства встановлена така рекомендація – "*надати державам-членам можливість …введення національних положень з метою подальшого уточнення застосування правил, передбачених цим Регламентом,…більш точно визначаючи умови, за яких обробка персональних даних є законною*".

До GDPR включено Директиву (ЄС) 2016/680 "Про захист фізичних осіб у зв'язку з обробкою персональних даних компетентними органами в цілях запобігання, розслідування, виявлення чи судового переслідування кримінальних правопорушень або виконання кримінальних покарань, та про вільне переміщення таких даних, і скасування Рамкового рішення Ради 2008/977/ПВД" [4, с. 104-156], а також Директиву (ЄС) 2016/681 "Про використання даних записів реєстрації пасажирів (PNR) для профілактики, виявлення, розслідування і судового переслідування злочинів терористичного характеру і тяжкого злочину" [4, с. 157-176].

Питання скасування Директиви 1995 р. та Рамкового рішення 2008 р. пов'язано з проблемами наявності правової невизначеності у зв'язку з діяльністю у мережі Інтернет (п. 9 Преамбули).

Крім зазначеного, у 2016 р. Європейським Парламентом також була затверджена Директива ЄС "Про безпеку мережевих та інформаційних систем" (NIS Directive) [5], а з 2017 р. почалась робота над проектом ЄС ЄС про ePrivacy [6].

Вважаємо за доцільне розглянути деякі актуальні, на наш погляд, ключові аспекти згаданих документів.

1. Регламент GDPR.

Першим ключовим аспектом, зокрема у будь-якої науці, – це питання визначення та тлумачення термінів. У сфері захисту та безпеки персональних даних це, поперед усього, стосується термінів "персональні дані" та "ідентифікація" (для порівняння розбіжностей наведено Таблицю визначень), а також розуміння термінів "контролер" та "обробник".

Конвенції РЄ № 108 від 28.01.81 р.	**Директива 95/46/ЄС** від 24.10.95 р.	**Регламент GDPR** від 27.04.16 р.	**Закон України** від 01.06.10 р. № 2297-VI (ред. від 04.03.20 р.)
персональні дані – означають будь-яку інформацію, яка стосується конкретно визначеної особи або особи, що може бути конкретно визначеною ("суб'єкт даних") [2, с. 66].	**персональні дані** – означає будь-яку інформацію, що стосується встановленої фізичної особи чи фізичної особи, яку можна встановити ("суб'єкт даних"); особою, яку можна встановити, є така, яка може бути встановленою прямо чи опосередковано, зокрема, за допомогою ідентифікаційного коду або одного чи більше факторів, притаманних фізичним, ізіологічним, розумовим, економічним, культурним чи соціальним аспектам її особистості [2, с. 281].	**персональні дані** – означає будь-яку інформацію, що стосується фізичної особи, що ідентифікована або може бути ідентифікована ("суб'єкта даних"); фізична особа, що може бути ідентифікована – це особа, яка може бути ідентифікована, прямо чи опосередковано, зокрема за такими ідентифікаторами, як: ім'я, ідентифікаційний номер, дані про місце розташування, онлайн-ідентифікатор, один чи декілька специфічних факторів фізичної особи щодо: фізичної, фізіологічної, генетичної, ментальної, економічної, культурної і соціальної ідентичності [4, с. 45].	**персональні дані** – відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована.

У загально-теоретичному плані поняття *"персональні дані"* охоплює об'єктивні та суб'єктивні відомості про особисте, сімейне чи публічне життя фізичної особи-людини, що виражені у формі літер, чисел, графіки, фото, звуку чи відео, якщо вони дозволяють ідентифікувати таку особу, тобто обов'язково стосуються конкретної особи.

В інформаційних системах під *"ідентифікацією"* звичайно розуміють процес присвоєння як суб'єктам, так і об'єктам комунікації певних унікальних ідентифікаторів і їх порівняння з переліком привласнених ідентифікаторів. Для визначення особи-людини або об'єкту техніки, що застосовують інформаційні засоби, можна говорити не стільки про ідентифікацію, скільки про її автентифікацію. Саме автентифікація дозволяє

встановити відповідність названому нею ідентифікатору. Таким чином, при ідентифікації користувач Інтернету "визначає себе" інформаційній системі, підключеної до мережі, а завдяки автентіфікації встановлюється відповідність особи (або об'єкта) названому нею ідентифікатору, зокрема шляхом застосування пароля.

На практиці встановити наявність зв'язку між літерами і/або цифровими позначеннями та конкретною фізичною особою достатньо складно, оскільки за різних умов позначення можуть розглядатися як персональні дані, так і не бути ними, наприклад – набір цифр ідентифікатора окремо не є персональними даними. Якщо ж додати до нього, наприклад ПІБ, то виникають персональні дані.

За GDPR вирішення питання, чи є відомості про особу персональними даними залежить від поглядів та можливостей конкретного *контролера* (означає *фізичну чи юридичну особу, державний орган, агенцію або іншу установу, яка, самостійно чи спільно з іншими, визначає мету, засоби збирання та обробки персональних даних* (п. 7 ст. 4 Регламенту) ідентифікувати людину за наявних у нього відомостей, у тому числі за рахунок поєднання таких відомостей з інформацією, яку він може отримати від третіх осіб з урахуванням "доцільної ймовірності". Разом з умовністю (тобто наявності випадковості) вказане передбачає (згідно п. 26 Преамбули та ст. 25 Регламенту GDPR) оцінку фінансових витрат, існуючих технологій та часу, що необхідні для ідентифікації особи. При цьому, обробку даних за дорученням контролера може здійснювати *обробник* (означає *фізичну чи юридичну особу, державний орган, агенцію або іншу установу, яка здійснює обробку персональних даних від імені контролера* (п. 8 ст. 4 Регламенту)*, який також, як представляється, може слідувати "доцільної ймовірності".

Для збирання персональних даних сьогодні звичайно використовуються не лише аккаунти щодо онлайн ідентифікації, а й IP-адреса – набір чисел, що присвоюється приладу, забезпечує його ідентифікацію та зв'язок з іншими приладами через мережу Інтернет. Для провайдерів електронних комунікацій щодо Інтернет-послуг IP-адреси вважаються персональними даними, оскільки можна пов'язати IP-адресу з конкретною людиною. Стосовно контролерів, які не є провайдерами Інтернет-послуг, то вони використовуючи IP-адресу, можуть створювати профіль звичок людей та розрізняти їх один від одного (за аналогією з файлами cookie). Головне у тому, що коли людину можна ідентифікувати, поєднавши IP-адресу з додатковою інформацією, то IP-адреса може вважатися персональними даними. До того ж, інформація, отримана за допомогою файлів cookie, в більшості випадків буде вважатися персональними даними.

Таким чином, фізичні особи можуть асоціюватися з онлайн-ідентифікаторами, що надаються їх пристроями, застосуваннями, інструментами та протоколами, такими як адреси Інтернет-протоколів, ідентифікатори файлів cookie або інші ідентифікатори, наприклад, ідентифікаційні мітки радіочастоти. Це може спричинити появу електроних слідів, які, зокрема у комбінації з унікальними ідентифікаторами та іншими даними (відомостями), отриманими серверами, можуть бути використані для створення профілів фізичних осіб та їх ідентифікації, що визначається у Регламенті GDPR (п. 30 Преамбули).

---

* *Примітка.* Закон України "Про захист персональних даних" застосовує терміни *володілець персональних даних* – фізична або юридична особа, яка визначає мету обробки персональних даних, встановлює склад цих даних та процедури їх обробки, якщо інше не визначено законом та *розпорядник персональних даних* – фізична чи юридична особа, якій володільцем персональних даних або законом надано право обробляти ці дані від імені володільця.

Регламент GDPR зобов'язує – для того, *щоб визначити, чи є фізична особа такою, що може бути ідентифікована*, необхідно врахувати *усі засоби*, які можуть бути використані з достатнім ступенем ймовірності, наприклад, виокремлення контролером або іншою особою, прямо чи опосередковано. Для того, *щоб встановити, чи можуть засоби з достатнім ступенем ймовірності бути використані для ідентифікації фізичної особи*, необхідно врахувати *усі об'єктивні фактори*, такі як витрати та кількість часу, необхідного для ідентифікації, з урахуванням технологій, наявних на момент обробки, та технічних розробок (п. 26 Преамбулт). Ідентифікація повинна включати в себе цифрову ідентифікацію суб'єкта даних, наприклад, через механізм автентифікації, такий як реєстраційні дані, що використовуються суб'єктом даних для авторизації в системі онлайн-послуг, що пропонує контролер даних (п. 57 Преамбула).

Наступним ключовим аспектом у сфері захисту та безпеки персональних даних є визначення принципів та умов їх обробки.

Згідно положень Регламенту GDPR обробка має здійснюватися на основні таких принципів (ст. 5 Глави II Регламенту GDPR):

1) *законність, справедливість і прозорість* – персональні дані повинні оброблятися законно, справедливо і в доступній формі по відношенню до суб'єкта даних;

2) *цільове обмеження* – збиратися для певної, конкретної і законної мети і не піддаватися додатковій обробці, яка несумісна з цією метою; подальша обробка для цілей архівації, з метою наукових, дослідницьких, історичних і статистичних цілей не може бути несумісною з початковою метою;

3) *зведення до мінімуму даних* – бути адекватними і обмежуватися тими даними, які відповідають і необхідні для досягнення цілі, для яких вони обробляються;

4) *точність* – бути точними і, при необхідності, постійно підтримуватися в актуальному стані; неточні персональні дані, з урахуванням цілей, для яких вони обробляються, слід видаляти або виправляти без затримки;

5) *обмеження зберігання* – зберігається у формі, що дозволяє ідентифікувати суб'єкта даних не довше, ніж це необхідно для цілей, для яких вони обробляються; персональні дані можуть зберігатися протягом тривалішого періоду виключно з метою архівації, інтересів наукових, дослідницьких, історичних і статистичних цілей;

6) *цілісність і конфіденційність*[**] – оброблятися так, щоб забезпечити належний захист персональних даних, включаючи захист від несанкціонованої або незаконної обробки, випадкової втрати, знищення або пошкодження, з використанням відповідних технічних або організаційних заходів;

7) *підзвітність* – будь-яка установа (компанія тощо) несе відповідальність перед наглядовими органами і повинна бути здатна довести дотримання положень Регламенту.

У загальному плані правові новації Регламенту GDPR свідчать про спрямованість на подальше посилення захисту прав суб'єктів персональних даних. Це знайшло відображення у ст. 17 Регламенту GDPR яка встановлює за суб'єктом персональних

[**] *Примітка*. 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 ознак сутності не наведене*. У законодавстві України чинним є Державний стандарт "Технічний захист інформації. Терміни та визначення" (ДСТУ 3396.2-97), який *визначає це поняття та надає його суттєві ознаки застосування* крізь тріаду повноважень права власності (див. [7]), але практично їх не використовують. Сенс тлумачення "конфіденційності" може розумітися як "таємно-довірче" властивість об'єкта, зокрема, інформації, яка обумовлює умови її використання, тобто надані особам можливості по відношенню до об'єкта конфіденційності.

даних “право бути забутим” (англ. – *right to be forgotten*). Стаття уточнює “право на видалення даних” і визначає його умови, включаючи обов’язок володільця, який оприлюднив персональні дані, повідомляти треті сторони про вимогу суб’єкта даних щодо усунення будь-яких посилань на відповідні персональні дані, а також видалення будь-яких копій чи примірників таких персональних даних. Вона також передбачає право на обмеження обсягів обробки в певних випадках, уникаючи при цьому використання двозначності терміну “блокування даних”.

У Розділі 4 Регламенту GDPR передбачено право суб’єкта даних не бути предметом заходів, які ґрунтуються на “профілюванні”, що розвиває (з відповідними змінами та додатковими запобіжними заходами) положення ч. 1 ст. 15 Директиви № 95/46/ЄС щодо автоматизованих рішень та враховує численні рекомендації Ради Європи щодо запобігання профілювання.

Значна увага у Регламенті GDPR приділена правилам передачі персональних даних в межах ЄС та у треті країни або міжнародні організації, з урахуванням умов передачі з однієї системи електронної обробки до іншої (пп. 6, 48, 50, 68, 101, 107 та ін. Преамбули, а також у ст. 14, 15, 20 та ст. 44-49 Глави V Регламенту GDPR).

Нові правила-приписи мають застосовуватися до обробки даних фізичних осіб у компаніях, закладах, установах, організаціях та підприємствах, розташованих не тільки на території держав-членів ЄС, але і тих, що здійснюють свою діяльність за його межами і пов’язані з обробкою персональних даних в рамках ЄС. Правила не поширюються на обробку даних про юридичних осіб, а також на дані, які відносяться до анонімної інформації і померлих осіб (п. 26, 27 Преамбули).

Правила Регламенту GDPR не застосовуються до обробки персональних даних фізичною особою для особистої чи побутової діяльності та без зв’язку з професійною або комерційною діяльністю В то же час Регламент застосовується до контролерів чи осіб, що здійснюють обробку даних, які забезпечують засоби для обробки персональних даних у ході такої особистої чи побутової діяльності (п. 18 Преамбули, ст. 2 Регламенту). Особиста або побутова діяльність може включати, зокрема, листування, використання особистої адреси (е-пошта), здійснення онлайн діяльності в інформаційно-комунікаційних мережах тощо у зазначеному контексті діяльності. Суб’єкт даних повинен мати можливість передавати свої персональні дані з однієї системи електронної обробки до іншої без втручання інших осіб.

Згідно з положеннями Регламент GDPR не застосовується до обробки персональних даних в інтересах забезпечення національної безпеки та діяльності правоохоронних органів (для цілей попередження і розслідування протиправних дій), а також до обробки персональних даних державами-членами ЄС щодо загальної зовнішньої політики і політики безпеки ЄС (п. 16 Преамбули).

Персональні дані, які обробляються державними органами з метою запобігання, розслідування, виявлення чи судового переслідування злочинів або виконання покарань, зокрема, щодо запобігання загрозам суспільній безпеці та вільному переміщенню таких даних, регулюються іншим правовим актом ЄС, а саме – Директивою (ЄС) 2016/680 Європейського Парламенту і Ради.

У зв’язку з використанням нових технологій та з урахуванням характеру, обсягу, контексту та цілей обробки, що ймовірно, призведе до високого ризику для прав і свобод фізичних осіб, контролер повинен перед початком обробки провести *оцінку впливу* операцій з захисту та безпеці даних які передбачаються, тобто до початку проведення ризикованих операцій з обробки даних (п. 83, 84, 91, 94 Преамбули; ст. 35 Регламенту GDPR).

При цьому кожна держава-член ЄС може мати свої особливі погляди та відповідний зміст національного законодавства, але коли справа стосується та пов'язана зі співпрацею з будь-якими організаційними структурами держав-членів ЄС (зокрема, бізнес-діяльністю) слід керуватися приписами, що визначаються у Регламенті GDPR. У разі недодержання зазначеного можуть бути накладені такі *санкції*:

- *попередження у письмовій формі у разі першого й не навмисного недотримання приписів щодо захисту персональних даних;*
- *призначення регулярних або періодичних перевірок діяльності щодо захисту даних;*
- *призначення санкцій (в межах ЄС, на організацію, компанію та ін.) – штрафів у розмірі до 20 млн. EUR або до 4 % від загального річного обсягу фінансування (від показників поточного і попереднього фінансового року, виходячи з того, яка сума більше);*
- *призначення санкцій (при транскордонній передачі персональних даних) – штрафів у розмірі до 10 млн. EUR або до 2 % від загального річного обсягу фінансування (від показників поточного і попереднього фінансового року, виходячи з того, яка сума більше).*[***]

2. Директива ЄС "Про безпеку мережевих та інформаційних систем" (NIS Directive).

Основне завдання NIS Directive – забезпечення високого рівня інформаційної безпеки для операторів критичної інфраструктури і провайдерів цифрових послуг [5]. Тобто, йдеться не лише про захист персональних даних, але й про безпеку даних взагалі.

Для виконання цього завдання державам-членам ЄС запропоновано підвищити свою готовність і поліпшити співробітництво один з одним, а також зобов'язати операторів, які надають критично важливі послуги, пов'язані з певними об'єктами інфраструктури, і провайдерів окремих цифрових послуг вжити відповідних заходів з керування ризиками безпеки й повідомляти про серйозні інциденти компетентним національним органам.

Національні особливості існують при реалізації будь-яких міжнародно-правових актів. Проте, NIS Directive безпосередньо пов'язана з проблемами її практичного застосування, оскільки більшою мірою визначає дії, які необхідно виконати державам-членам ЄС, залишаючи деталі на розсуд таких країн.

Водночас, нагальною залишається проблема як саме держави-члени мають реалізовувати вимоги щодо організації співробітництва з метою забезпечення скоординованої відповіді на різні інциденти за наявності різних підходів до цих питань.

3. Проект ЄС про e-Privacy.

Сьогодні, поряд з GDPR, в Європейському Союзі діє Директива 2002/58/ЄС "Про обробку персональних даних та захист таємниці ("privacy") в секторі електронних комунікацій" від 12 липня 2002 року [2, с. 379-392]. Водночас, планується прийняття нового акту на рівні рекомендацій-директиви або правового стандарту (Регламенту ЄС) – "e-Privacy Regulation".

[***] *Примітка.* В Україні за *порушення законодавства у сфері захисту персональних даних* передбачається накладення штрафу: на громадян та посадових осіб від 100 до 500 неоподатковуваних мінімумів їх доходів; на громадян-суб'єктів підприємницької діяльності від 200 до 2000 неоподатковуваних мінімумів доходів (ст. 188^{39} Кодексу України про адміністративні правопорушення). *Порушення недоторканності приватного життя* караються штрафом від 500 до 1000 неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до 2 років, або арештом на строк до від 3 до 6 місяців, або обмеженням чи позбавленням волі на строк від 3 до 5 років (ст. 182 Кримінального кодексу України).

Процес розробки проекту розпочався ще в 2017 році [6], коли у ЄС затвердили GDPR та дійшли висновку, що Директива 2002/58/ЄС вже не відповідає вимогам цифрового суспільства, а її приписи, які були розроблені у розвиток Директиви 95/46/ЄС, в деяких питаннях не узгоджуються з приписами GDPR. Зазначимо, що на відміну від Директив ЄС, Регламент ЄС є правовим актом-стандартом Європейського Союзу, який негайно набирає чинності як закон в усіх державах-членах одночасно. Проте, "e-Privacy Regulation" може бути документом загального характеру, без необхідності імплементації його положень до національного законодавства кожної країни-учасниці ЄС.

Нині положення "e-Privacy Regulation" активно дискутуються, а погляди сильно різняться. До основних проблем, які розглядаються, можна віднести:

– конфіденційність комунікацій та посилення контролю за нею в умовах електронної згоди, застосування браузерів, файлів-cookie, не обмежуючись приватністю під час надсилання голосових та текстових повідомленнях в мережі Інтернет, крім обмеження щодо контролю "чутливих" персональних даних;

– необхідність позбавлення власників веб-ресурсів отримувати згоду щодо файлів-cookie, які використовуються для покращення роботи в Інтернеті, а також спрощення можливості для користувачів налаштовувати браузери в частині згоди або відмови від обробки файлів-cookie;

– надання фізичним особам можливості погоджувати отримання маркетингових листів, які надсилаються за допомогою SMS, електронної пошти або в будь-який інший спосіб (захист від спаму);

– доцільності збереження таких важливих прав споживачів, як "право на заперечення" та "оцінки впливу на захист даних", обробки даних про особу для різних цілей без згоди осіб тощо.

Водночас, розробники проекту e-Privacy висловлюють надію про те, що метою регулювання має бути посилення довіри та безпеки в умовах єдиного ринку цифрових технологій [8].

Загалом, можна зробити припущення, що "e-Privacy Regulation" може бути або окремим документом, який діятиме узгоджено з GDPR, або окремим спеціальним положенням, який в деяких частинах буде доповнювати та уточнювати приписи Регламенту GDPR щодо захисту та безпеки персональних даних [9].

4. Підготовка нової редакції Закону України "Про захист персональних даних".

В Україні, як свідчить аналіз, здійснюються певні заходи щодо удосконалення законодавства у сфері захисту персональних даних. Сьогодні це стосується проектів змін до Закону України "Про захист персональних даних" щодо форм та умов надання згоди на обробку персональних даних в органах влади (від КМ України - реєстр. № 2671 від 23.12.2019, та альтернативний законопроект - від народних депутатів - реєстр. № 2671-1, кер. Королевська Н.Ю.).

Не торкаючись деталей пропозицій щодо упорядкування відносин, висловимо свою загальну точку зору на сутність предмету пропозицій.

У контексті захисту та безпеки існують такі категорії персональних даних:

перша – це відомості, які необхідні органам державної влади та місцевого самоврядування для здійснення повноважень у вирішенні загальних суспільно-економічних питань. У такому разі "згода суб'єкта даних на обробку" не потрібна;

друга – це відомості про особисту приватність та приватність сімейного життя. Приватність – це право людини "на недоторканність її особистого життя", що передбачає наявність права на "самітність та самоту", "бути наданій самої собі", "бути забутою та

залишеною у спокої", "мати у житті особистий простір" тощо. Вона (приватність) не може бути предметом обробки органами державної влади та місцевого самоврядування. Водночас, право приватності повинно бути гнучким та здатним прилаштовуватись до потреб сьогодення, зокрема, воно не повинно забороняти публікацію матеріалів, що становлять суспільний або державний інтерес, зокрема щодо розслідувань, виявлення та судових переслідувань кримінальних правопорушень;

третя – це особливі відомості щодо персональних даних людини ("чутливі" дані**)**. Стосуються расового, етнічного і національного походження, політичних, релігійних, світоглядних вірувань, членства у політпартіях, профспілках, стану здоров'я, біометричні, генетичні дані, статева орієнтація. Чим більша " чутливість" цих даних, тим більший ризик порушення прав і свобод людини і тим більш надійними мають бути правові гарантії. Тому вони заслуговують на особливий захист. Однак, обробка зазначених даних може бути необхідною для забезпечення суспільних інтересів у сферах охорони здоров'я, правоохоронної діяльності тощо без згоди суб'єкта даних. Якщо в ході електоральної діяльності робота демократичної системи держави-члена потребує від політичних партій компіляції персональних даних щодо політичних переконань населення, обробка таких даних може бути дозволена з міркувань суспільних інтересів, за умови встановлення відповідних гарантій.

Зазначене, вважаємо, повинно отримати відображення у Законі України "Про захист персональних даних", наприклад у вигляді формулювання: *персональні дані приватного характеру не є предметом обробки у ході діяльності органів державної влади та місцевого самоврядування.* При цьому, вказане може бути додатком до п. 4 ст. 10 Закону та сформульовано таким чином – *відомості про приватне життя людини не можуть використовуватися як чинник, що підтверджує чи спростовує її ділові якості*.

Одночасно з вказаним, слід звернути увагу на те, що в державі триває робота щодо оцінки ефективності законодавства у сфері захисту персональних даних та визначення перспектив в його удосконаленні.

Так, у листопаді 2020 р. відбулися консультації з цих питань з представниками-експертами від ЄС та РЄ. При цьому зазначалося, що проект нової редакції Закону України "Про захист персональних даних" слугуватиме основою для захисту персональних даних у державному і приватному секторах, а також для ухвалення правових актів, що регулюють обробку і безпеку персональних даних [10].

У презентації до законопроекту представники-експерти від ЄС та РЄ відзначали, що: *"...для отримання якісного законодавства дуже важливо дотримуватися загальної мети внесення поправок та оцінити їхній вплив на права і свободи людини, а також на вільний рух персональних даних"*.

Рекомендації та пропозиції експертів від ЄС та РЄ стосувалися необхідності вирішення таких *проблемних питань*, а саме:

- *"уникнення положень законопроекту, які є занадто складними й навіть неможливими для реалізації на практиці, оскільки вони не матимуть жодної цінності для захисту прав і свобод людини;*
- *зобов'язання державних органів, залучених до законотворчого процесу, включати до правових актів, що регулюють обробку персональних даних, ціль обробки, про яку йдеться, та іншу необхідну інформацію залежно від обставин;*
- *передбачення процедури здійснення контролерами даних оцінки впливу на захист даних у процесі ухвалення законодавчих актів;*

- *встановлення основних принципів обробки персональних даних органами державного і недержавного секторів;*
- *визнання в законопроекті застосування механізмів ЄС з боку українських контролерів даних і операторів даних, передбачених у GDPR – кодексу поведінки (стаття 40) і зобов'язальних корпоративних правил (стаття 47);*
- *створення незалежного контролюючого органу з питань захисту персональних даних".*

В цілому, з огляду на викладене та стан сучасних процесів цифрової трансформації та євроінтеграції України, вкрай актуальною постає проблема кардинального перегляду поглядів та підходів щодо правового врегулювання новітніх суспільних відносин, які активно формуються і розвиваються в українському суспільстві.

З цього приводу, слушними видаються оцінки стану національного законодавства, надані першим заступником Голови Верховної Ради України, академіком НАПрН України Р. Стефанчуком: *"Кількість діючих нормативно-правових актів уже набагато перевищила один мільйон. 90 % законопроектів, які розглядаються українським парламентом, – це зміни й доповнення до чинного законодавства. Велика кількість законів обернено пропорційна їх якості. І якщо такі тенденції збережуться, то ми й надалі без єдиного системного підходу будемо робити величезну кількість нормативно-правових актів, які не забезпечують головного – якості українського законодавства. В Україні необхідно змінити підхід до правотворчої діяльності"* [11].

Висновки.

1. Реальні та потенційні ризики можливих порушень прав суб'єктів персональних даних (фізичної особи, людини і громадянина) залишаються вкрай актуальною прикладною проблемою в сучасних умовах розвитку інформаційних (цифрових) технологій, зокрема, впровадження "хмарних" технологій та технологій "великих даних" з їх конвергенцією, Інтернету речей, штучного інтелекту, розвитку ринку електронних комунікацій тощо. При цьому визначення та трактування терміну "персональні дані" є одним з головних аспектів, який безпосередньо пов'язаний з проблемами захисту прав та безпеки людини в умовах глобальних трансформаційних процесів та необхідності імплементації європейських правових стандартів в національне законодавство України.

2. До системних проблем у сфері захисту та безпеки персональних даних в сучасних умовах суспільних та цифрових трансформацій слід віднести такі:

– незважаючи на значну кількість прийнятих в установах Європейського Союзу і Ради Європи актів, законодавство про захист персональних даних у європейських країнах перебуває на етапі становлення. Повна відповідність національних законодавств держав-членів ЄС з питань захисту персональних даних європейським правовим стандартам також не досягнута. Вкрай актуальною ця проблема залишається й для України;

– реалізація положень нового європейського порядку захисту персональних даних, зокрема, GDPR, Директиви NIS, а у майбутньому – регламенту (або положення) про e-Privacy вимагає пошуку нових підходів та комплексних змін ділової практики у державах-членах ЄС та в країнах-партнерах ЄС. При цьому, потребує дуже значної уваги проблема суттєвого зростання розриву між стрімким розвитком інформаційних (цифрових) технологій та змінами законодавства у цій сфері;

– в сучасних умовах актуалізується проблема зміни концептуальних поглядів і правового регулювання з питань захисту прав в інформаційній сфері, тобто ***зміни існуючої правової модальності***. Передусім це стосується проблем забезпечення захисту та безпеки приватності персональних даних людини.

3. Виходячи з того, що людина, її життя і здоров'я, недоторканність та безпека віднесені до найвищих цінностей демократичного суспільства, у національному законодавстві мають бути відображені базові критерії з питань захисту та безпеки персональних даних за такою можливою формулою: *право приватної власності людини і громадянина (фізичної особи) на персональні дані – це право володіння, користування та виключного розпорядження своїми персональними даними, за умов збалансованості та узгодженості цього права з правами інших громадян та потребами суспільства і держави у безпеці.*

При цьому, володіння, користування та розпорядження персональними даними мають передбачати: *а) володіння персональними даними* – наявність можливості людини та нормативно-правових умов для забезпечення приватності персональних даних в незмінному вигляді; *б) користування персональними даними* – наявність можливості людини та нормативно-правових умов для забезпечення використання відомостей про себе на власний розсуд; *в) розпорядження персональними даними* – наявність можливості та нормативно-правових умов для забезпечення виключного права людини щодо порядку доступу до своїх персональних даних.

Запропоновані формули, як вважаємо, відповідають здобуткам історико-правової науки щодо загальної ідеї прав людини на життя, приватну власність і свободу, корелюється з приписами п. 1 Преамбули Регламенту GDPR, що ***захист персональних даних фізичних осіб є основоположним правом***, а також можуть визначати основу для законотворчості, правозастосування та оцінки ефективності діяльності у сфері захисту персональних даних.

4. Сьогодні продовжує існувати проблема імплементації приписів європейських правових стандартів щодо сфери захисту персональних даних у законодавство України. Це, поперед усього, стосується повної узгодженості законодавства з правовими приписами Регламенту GDPR, який є обов'язковим у виконанні для усіх держав-членів ЄС.

Роботу можна почати з запровадження у базовий Закон України (у ст. 2. Визначення термінів) дефініцій, сформульованих у ст. 4 Регламенту GDPR. Потім здійснити розміщення термінів у тексті Закону, з урахуванням потреби внесення в статті відповідних виправлень і змін.

Навіть з вищевказаного видно, що існує багато різнобічних проблем щоб привести законодавство України у відповідність до приписів Регламенту GDPR. Це можливо за наявності умов формування системності у організаційних та правових питаннях, вирішення яких потребує створення окремого у державі незалежного наглядового органу (згідно положень Глави VI Регламенту GDPR), який повинен сприяти послідовному впровадженню та застосуванню цього Регламенту.

Використана література

1. Защита персональных данных / А. Баранов, В. Брыжко, Ю. Базанов. Київ: Национальное агентство по вопросам информатизации при Президенте Украины, 1998 г. 128 с.; Права человека и защита персональных данных / А. Баранов, В. Брыжко, Ю. Базанов. – (Государственный комитет связи и информатизации Украины). Харьков: Фолио, 2000. 280 с. С. 11-36; Становлення і розвиток правових основ та системи захисту персональних данихв Україні: монографія ; за ред. В.М. Брижка, В.Г. Пилипчука. Київ: ТОВ "Видавничий дім "АртЕк", 2017 р. 226 с. С. 9-19.

2. Системна інформатизація правоохоронної діяльності: європейські нормативно-правові акти та підходи до упорядкування суспільних інформаційних відносин у зв'язку з автоматизованою обробкою даних у правоохоронній діяльності": посібник. Кн. 2 / В. Брижко, М. Швець та ін. Київ: ТОВ "Пан Тот", 2006 р. 509 с.

3. 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; Брижко В.М., Пилипчук В.Г. Приватність, конфіденційність та безпека персональних даних. *Інформація і право*. № 1(32)/2020. С. 33-46; Брайчевський С.М. Проблема персональних даних в системах Інтернету речей з елементами штучного інтелекту. *Інформація і право.* № 4(31)/2019. С. 61-67; Брайчевський С.М. Проблема персональних даних при використанні систем Інтернету речей в галузі охорони здоров'я. *Інформація і право.* № 2(33)/2020. С. 69-76; Брайчевський С.М. Персональні дані та мультимедіа. *Інформація і право.* № 4(35)/2020. С. 82-91; Сенюта І.Я. Обробка персональних даних за новими правилами: захист чи порушення прав людини. – (*Стосовно упорядкування відносин, пов'язаних з коронавірусною хворобою COVID-19*). URL: https://www.hsa.org.ua/blog/obrobka-personalnyh-danyh-v-umovah-covid-19-zahyst-chy-porushen nya-prav-lyudyny

4. Сучасні правові стандарти Євросоюзу у сфері захисту персональних даних / І. Майстренко – переклад з англ.; В. Брижко – редагування тексту. – (Науково-дослідний інститут інформатики і права Національної академії правових наук України). Київ: ТОВ "Видавничий дім "АртЕк", 2018. 177 с.

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

6. ePrivacy Regulation. URL: https://en.wikipedia.org/wiki/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

7. Пилипчук В.Г., Брижко В.М. Інформаційна безпека та приватність у сфері захисту персональних даних. *Інформація і право*. № 4(19)/2016. С. 67.

8. Підготувались до GDPR? Тепер готуйтесь до ePrivacy regulation. URL: https://legalit group.com/eprivacy-regulation

9. Council of the EU Released a (New) Draft of the ePrivacy Regulation (2021). URL: https://www.lexology.com/library/detail.aspx?g=21a1516a-4682-4403-a828-5cf761438d41; Opinion 5/ 2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the com petence, tasks and powers of data protection authorities. URL: https://edpb.europa.eu/our-work-tools/our-documents/topic/e-privacy-regulation_en; 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; The EU ePR (ePrivacy Regulation). A proposed regulation concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications). URL: https://www.itgovernan ce.co.uk/eprivacy-regulation-epr

10. Новий законопроект про захист персональних даних – експертні консультації за підтримки спільного проекту ЄС та Ради Європи. – (Україна). URL: https://www.coe.int/uk/web/ kyiv/-/new-draft-law-of-ukraine-on-personal-data-protection-expert-consultations-with-support-of-join -eu-and-coe-project

11. Стефанчук Р. Про необхідність змін у підходах до правотворчої діяльності. URL: https://www.rbc.ua/rus/news/otmenyayut-svyshe-tysyachi-aktov-sssr-rade-1614027171.html

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