УДК 347.2/3

ЄВРОПЕЙСЬКИЙ ПРИНЦИП ПОВАГИ ДО ПРИВАТНОГО ЖИТТЯ В КОНТЕКСТІ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ОСОБИ

Гуйван П. Д.

Робота присвячена дослідженню міжнародно-правового регулювання охорони та захисту персональних даних. Зокрема, детально вивчена правова база, присвячена безпеці інформації про громадян у країнах Європейського Союзу. Це розглядається як один із висхідних елементів захисту прав людини, зокрема права на приватність. Проаналізовано зміст основних Директив Європейського Союзу із цього питання, їх позитивні й негативні чинники. На цій основі надано конкретні рекомендації для подальшого розвитку українського законодавства в цій царині, яке нині перебуває в занедбаному стані.

Ключові слова: *персональні дані, захист інформації про особу в Європейському Союзі.*

Работа посвящена исследованию международно-правового регулирования охраны и защиты персональных данных. В частности, подробно изучена правовая база, посвященная безопасности информации о гражданах в странах Европейского Союза. Это рассматривается как один из главных элементов защиты прав человека, в частности права на приватность. Проанализированы содержание основных директив Европейского Союза по данному вопросу, их положительные и отрицательные элементы. На этой основе предоставлены конкретные рекомендации для дальнейшего развития украинского законодательства в этой области, которое сейчас находится в запущенном состоянии.

Ключевые слова: *персональные данные, защита информации о лице в Европейском Союзе.*

The work is devoted to the study of international legal regulation of protection and protection of personal data. In particular, the legal framework devoted to the security of information about citizens in the countries of the European Union has been thoroughly studied. This is seen as one of the upward elements of the protection of human rights, in particular, the right to privacy.

It has been established that the general principle of the adoption by the European Union of regulatory and administrative acts in the field of personal data protection as an element of the human right to publicity is person-centrism, that is, the focus of any organizational or technical actions on serving human needs. A person must be the highest value for all state activities. His rights and freedoms should not be questioned, much less endangered. Following these principles, the relevant acts were adopted, binding on the members of the European Union.

The work analyzes in detail the general European legal approaches to the principle of processing personal data. According to the basic regulations of the relevant acts, personal data can be processed only on condition that the data subject explicitly gave his consent to this. In other cases, processing is possible only to fulfill a contract to which the data subject is party, or to take action at the request of the data subject before signing the contract, when processing is necessary to comply with the legal obligation that the controller is connected to, processing is necessary to protect the vital interests of the data subject. processing is necessary to complete an assignment carried out in the public interest, or in the exercise of official authority with which the controller or third party is vested Data is provided, processing is necessary for purposes of legitimate interests pursued by the controller or a third party or parties for whom data are provided, unless the interests of the basic rights and freedoms of the data subject that require protection prevail over such interests.

The content of the main EU directives on this issue, their positive and negative elements is analyzed. On this basis, specific recommendations have been provided for the further development of Ukrainian legislation in this field, which is now in a state of neglect.

Key words: *personal data, protection of information about a person in the EU.*

Постановка проблеми та її актуальність. Потреба в нормативному закріпленні правових механізмів, які опосередковують порядок збирання, використання даних про особу, є досить нагальною. У світі цьому питанню приділяється неабияка увага, адже інформаційна безпека особи визнається однією з головних цінностей прав людини [1]. Охороні персональних даних присвячено низку міжнародно-правових актів. Достатньо згадати Конвенцію про захист фізичних осіб при автоматизованій обробці персональних даних [2]. Ця Конвенція заклала основу для формування уніфікованої роботи щодо обробки та захисту особистої інформації. Вона, зокрема, постулює персональні дані як інформацію, що стосується конкретного суб'єкта, котрий ідентифікований або може бути ідентифікованим (суб'єкта даних). У Конвенції також сформульовано ключові принципи обробки персональних даних, права особи у зв'язку з їх обробкою, базові норми щодо транскордонної передачі даних. Передбачені також основні засади міждержавної співпраці в цій сфері, які повинні базуватися на принципі субсидіарності, що передбачає обробку індивідуальної інформації про фізичну особу на базі національного законодавства, яке регулює рівень можливих ризиків утрати або витоку інформації. Водночас указується на необхідність зближення законодавств у сфері захисту персональних даних. Однак то не має бути причиною зниження рівня безпеки, а, навпаки, слугувати підвищенню якості послуг захисту персональної інформації.

Не оминуло це питання й внутрішнє законодавство більшості цивілізованих країн. Стали з'являтися внутрішньодержавні галузеві закони з визначення правового становища персональних даних, а також порядку й умов їх обробки. Скажімо, захист та охорона персональних даних особи регулюються національними законами Великої Британії, Німеччини, Канади, Фінляндії, Нідерландів, Франції, Угорщини. До цього процесу принаймні на нормотворчому рівні долучилася й Україна, прийнявши спеціальний Закон «Про захист персональних даних» [3].

Особлива увага інформаційній безпеці громадян приділяється в країнах Європейського Союзу (далі – ЄС).

Це розглядається як один із висхідних елементів захисту прав людини. Скажімо, у ст. 8 Хартії основних прав Європейського Союзу вказується, що кожна людина має право на охорону відомостей особистого характеру. Ці відомості повинні використовуватися відповідно до встановлених правил у певних цілях і на підставі дозволу заінтересованої особи або на інших правомірних підставах, передбачених законом. Кожна людина має право на доступ до зібраних про неї відомостей і домагання внесення в них виправлення [4]. Отже, право на приватність інформаційного обміну оцінюється як одне з основних у сенсі стрімкого розвитку інформаційних технологій та інформаційного суспільства в Європі. Варто зазначити, що ця спільнота виробила стабільні й усталені механізми регулювання обороту даних про особу на рівні спільних умов поведінки всіх країн-учасників, тому національне законодавство лише конкретизує загальні правила. Варто, наприклад, згадати, що понад 20 років діяльність з обігу та захисту персональних даних регулювалася спеціальним документом у цій сфері – Директивою 95/46/ЄС («Загальні положення про захист даних») [5]. Наприклад, ст. 1 Директиви вимагає від держав-учасників захищати фундаментальні права і свободи фізичних осіб, особливо їхнє право на таємність щодо автоматизовано оброблюваних персональних даних. При цьому вказаний документ поширюється як на випадки, коли обробка персональних даних є автоматизованою, так і на ті, коли оброблені дані розміщуються чи призначені для розміщення в картотеках, структурованих за визначеними критеріями, що стосуються фізичних осіб, отже, щоб забезпечити легкий доступ до відповідних персональних даних (ст. 15).

Дуже важливим є загальний підхід Директиви до принципу обробки персональних даних. Згідно з приписом ст. 7 цього акта, персональні дані можуть оброблятися тільки за умови, що суб'єкт даних недвозначно дав свою згоду на це. В інших випадках обробка можлива лише на виконання контракту, стороною якого є суб'єкт даних, чи для вживання заходів на прохання суб'єкта даних до підписання контракту, коли обробка необхідна для дотримання правового зобов'язання, яким зв'язаний контролер, обробка необхідна для захисту життєво важливих інтересів суб'єкта даних, обробка необхідна для виконання завдання, здійснюваного в суспільних інтересах, чи під час виконання офіційних повноважень, якими наділений контролер або третя сторона, якій надаються дані, обробка необхідна в цілях законних інтересів, переслідуваних контролером чи третьою стороною або сторонами, для яких надаються дані, крім випадків, коли над такими інтересами переважають інтереси основних прав і свобод суб'єкта даних, що вимагають захисту.

Навіть попри те що вказана Директива формально скасована з 25 травня 2018 року, Рада Європейського Союзу, Європейський Парламент указують, що всі її положення залишаються чинними до їх заміни чи зміни. Як бачимо, в Європі кардинально займаються регулюванням охорони приватності особи, зокрема в царині обігу її персональних даних, чого, як не прикро, не можна сказати про нашу державу. Тому дуже важливим і нагально необхідним є цей досвід, аби адаптувати його до українських нормативних і правозастосовних кондицій.

Аналіз останніх досліджень і публікацій. У літературі питанням охорони та захисту права особи на приватність у сенсі належної обробки персональних даних присвятили праці такі вчені, як М. Гуцалюк, А. Пазюк, В. Головченко, М. де Сальвіа, Б. Кормич, Л. Чернявський, В. Цимбалюк, М. Швець, Р. Чанишев, А. Чернобай, П. Макушев, О. Оніщенко, І. Сенюта, М. Швець та інші. Однак указані публікації переважно висвітлюють проблематику практичної реалізації права на приватність у світлі конкретних рішень Європейського суду з прав людини. Разом із тим питання потребує теоретичного осмислення та концептуального вирішення, позаяк європейські нормативні напрацювання є значною мірою взірцем для подальшого розвитку національної законодавчої доктрини.

Отже, **метою статті** є аналіз європейських підходів до запровадження регулятивних механізмів захисту даних і напрацювання певних рекомендацій щодо їх адаптації на українському правовому полі.

Виклад основного матеріалу. Окрім базової Директиви 1995 року, про яку вже вказувалося, євроспільнота виробила й ефективно застосовує низку спеціальних актів, що опосередковують конкретні відносини в досліджуваній царині. При цьому загальним принципом їх прийняття є персоноцентризм, тобто спрямованість будь-яких організаційних чи технічних вчинків на обслуговування потреб людини. Людина має бути найвищою цінністю для будь-якої діяльності держави. Її права та свободи не повинні ставитися під сумнів, тим більше, під загрозу. З дотриманням указаних засад прийнято відповідні акти, обов'язкові для членів ЄС. Скажімо, 15 грудня 1997 року Європейський Парламент ухвалив Директиву № 97/66/ЕС про порядок обробки персональних даних і захисту приватності в телекомунікаційному секторі [6]. Ця Директива зобов'язує країни ЄС належним чином урегулювати приватність інформаційних потоків у сфері публічних телекомунікаційних мереж і публічно доступних телекомунікаційних послуг. Має бути забезпечена приватність операційних даних (transactional data), тобто інформації, яка збирається операторами під час надання телекомунікаційних послуг. У статті 6 цього документа, зокрема, вказується, що дані щодо потоку обміну, які стосуються абонентів і користувачів і які обробляються для встановлення дзвінка і зберігаються оператором телекомунікаційної мережі загального користування чи постачальником загальнодоступної телекомунікаційної послуги, повинні стиратися чи перетворюватися на анонімні після завершення дзвінка. Обробка даних щодо потоку обміну й рахунків має обмежуватися особами, які діють у рамках повноважень операторів телекомунікаційних мереж загального користування чи постачальників загальнодоступних телекомунікаційних послуг, що займаються виставлянням рахунків чи управлінням потоками обміну, запитами клієнтів, виявленням обману та збутом власних телекомунікаційних послуг постачальника, і ця обробка не повинна виходити за межі того, що необхідно для цілей такої діяльності.

У подальшому цей акт замінений Директивою № 2002/58/ЄС Європейського Парламенту і Ради ЄС стосовно обробки персональних даних і захисту права на недоторканність особистого життя у сфері електронних засобів зв'язку [7]. Вона забезпечила уніфікований рівень захисту персональних даних та інформації про приватне життя користувачів загальнодоступних послуг електронного зв'язку незалежно від технологій,

що використовуються. Так, у ст. 4 цього документа вказується, що провайдер загальнодоступних послуг електронного зв'язку повинен зробити необхідні технічні й організаційні заходи для забезпечення безпеки послуг, які надаються, за необхідності спільно з провайдером мережі зв'язку загального доступу, якщо це стосується питання безпеки мережі. З огляду на рівень розвитку технологій і вартість їх упровадження, така політика має гарантувати рівень безпеки, відповідний наявним загрозам. При цьому належні заходи мають щонайменше гарантувати, що доступ до персональних даних може бути надано тільки уповноваженому персоналу в дозволених законом цілях, захищати персональні дані, збережені або передані, від випадкового чи незаконного знищення, випадкової втрати або зміни, несанкціонованого чи незаконного зберігання, обробки, доступу або розкриття й гарантувати введення політики безпеки щодо обробки персональних даних.

Держави-члени ЄС повинні гарантувати, що зберігання інформації або отримання доступу до інформації, вже збереженої на термінальному обладнанні абонента або користувача, допускається тільки за умови, що зацікавлений абонент або користувач дали свою згоду, будучи забезпеченими точною й повною інформацією, відповідно до Директиви 95/46/ЄС, крім іншого, про цілі обробки інформації. Цей пункт не має перешкоджати будь-якому технічному зберіганню або доступу до інформації з єдиною метою здійснення передачі повідомлення по мережі електронного зв'язку або в разі необхідності надання провайдером послуги інформаційного суспільства відповідних послуг за явно вираженим запитом абонента або користувача (ст. 5 Директиви).

Черговим європейським регулювальним актом у цій сфері є Директива про юридичний захист баз даних від 11 березня 1996 року № 96/9 [8]. Річ у тім, що бази даних як носії інформації в тому числі й про особу недостатньо охоронялися національними законодавствами, а принципи чинної охорони значно різнилися, що мало прямий негативний вплив як на функціонування внутрішнього ринку щодо баз даних, так і, зокрема, на свободу фізичних і юридичних осіб щодо використання онлайнових баз даних для товарів і послуг на основі гармонізованих правових положень. Це спонукало ЄС розробити уніфіковані правила поведінки в цій сфері. Указаний документ поширив правовий режим захисту персональної інформації, що автоматично обробляється, на дані, які збираються й обробляються вручну (ст. 1).

7 березня 2002 року прийняті Рамкова Директива 2002/20/ЄС Європейського Парламенту й Ради про дозвіл для мереж і послуг електронних засобів зв'язку [9] і Директива 2002/22/ЄС про універсальну послугу і права користувачів стосовно мереж і послуг електронного зв'язку [10]. У пунктах 7 і 8 Додатку до першого із цих актів і в ст. 7 другого наголошено, що захист особистих даних і приватності, що стосується електронно-комунікаційного сектора, здійснюється відповідно до Директиви 2002/58/ЄС, а також указано на особливості захисту прав споживачів, які стосуються електронно-комунікаційного сектора, та умови доступності для користувачів з фізичними вадами. У порядку перегляду й коригування правових рамок ЄС для електронних комунікаційних мереж і послуг 25 листопада 2009 року прийнята Директива 2009/136/ЄК Європейського Парламенту й Ради [11], якою конкретизовано необхідні заходи країн-учасників для гарантування інформаційної безпеки людини під час здійснення комунікацій в електронних засобах зв'язку. Зокрема, в п. 26 цього акта зазначається, що в інтересах громадськості є отримання інформації щодо порушень авторського права, іншого незаконного використання та розповсюдження шкідливого контенту, а також надано рекомендації й засоби захисту від ризику персональній безпеці, що може, наприклад, виникнути в результаті розкриття персональних даних за певних обставин, так само як і ризик приватності й персональних даних, доступність простого у використанні та конфігуруванні програмного забезпечення або опцій програмного забезпечення, які дають змогу захистити дітей та уразливих осіб.

Споживачів потрібно повідомити про їхні права щодо використання їхньої персональної інформації в довідниках користувачів і, зокрема, про цілі таких довідників, так само як і про право безкоштовно не бути включеним до загальнодоступного довідника користувачів. Користувачі повинні бути проінформовані про системи, які дають можливість включати інформацію в базу даних довідника без надання такої інформації користувачам довідкової служби (п. 33 Директиви). Наголошено на необхідності обробки даних трафіку провайдерами технологій і служб безпеки, які діють як контролер даних, в обсязі, суворо необхідному з метою забезпечення мережевої та інформаційної безпеки, тобто мережа має бути здатною протистояти на належному рівні випадковим подіям, незаконним чи злочинним діям, які становлять загрозу доступності, істинності, цілісності й конфіденційності накопичених чи переданих даних, безпеці пов'язаних послуг, що надаються чи доступні за допомогою цих мереж і систем. Має бути гарантовано, щоб споживачі та користувачі могли дозволити необхідний рівень захисту секретності й персональних даних, незалежно від технології, яка використовувалась для надання окремої послуги (п. п. 53, 54 Директиви).

Провайдер загальнодоступних електронних комунікаційних послуг має вжити відповідні технічні та організаційні заходи, щоб гарантувати безпеку своїх послуг. Вони повинні гарантувати, що до персональних даних отримати доступ може лише авторизований персонал для законних цілей і що накопичені чи передані персональні дані, так як і мережа чи послуги, захищені. Крім того, повинна бути встановлена політика безпеки щодо обробки персональних даних, щоб визначати слабкі місця в системі, регулярно мають проводитись контрольні та профілактичні, корегувальні й пом'якшувальні дії. Компетентні національні органи мають відстоювати інтереси громадян, між іншим, сприяючи забезпеченню високого рівня захисту персональних даних і секретності. Із цією метою компетентні національні органи повинні мати необхідні засоби для виконання своїх обов'язків, включаючи повні та надійні дані про інциденти порушення безпеки щодо персональних даних фізичних осіб. Вони мають контролювати вжиті заходи й розповсюджувати найкращу практику серед провайдерів загальнодоступних електронних комунікаційних послуг. Провайдери повинні підтримувати список порушень персональних даних для подальшого аналізу та оцінювання компетентними національними органами. Контролери даних мусять приймати відпо-

відні технічні й організаційні дії щодо захисту проти, наприклад, утрати даних. Вони повинні невідкладно повідомляти компетентним органам і зацікавленим фізичним особам, якщо до персональних даних здійснено несанкціонований доступ. Повідомлення про порушення правил безпеки відображає загальний інтерес громадян стосовно того, щоб бути проінформованими про порушення безпеки, що може призвести до втрати їхніх персональних даних чи навіть поставити їх під загрозу, а також про доступні чи рекомендовані застережні заходи, які вони можуть ужити, щоб мінімізувати можливі економічні втрати чи соціальну шкоду внаслідок таких порушень (п. п. 57–59, 61 Директиви).

Однак варто зазначити, що нормотворча практика ЄС не завжди є плідною, трапляються випадки прийняття недієвих правових актів у досліджуваній царині. Наприклад, 15 березня 2006 року прийнята Директива 2006/24/ЕС68, яка повністю присвячена зберіганню персональних даних особи [12]. За правилами цього документа, мало забезпечуватися зберігання провайдерами загальнодоступних послуг електронного зв'язку або мереж громадських зв'язків даних, які збиралися для ідентифікації користувачів послуг, визначення дати, часу і тривалості повідомлень, визначення місця розташування обладнання мобільного зв'язку, ідентифікації комунікаційного обладнання. Указані дані повинні зберігатися не менше ніж 6 місяців, але не більше ніж 2 роки. Власне, метою цього документа було забезпечення збереження даних про осіб, які можуть бути так чи інакше залучені до серйозних злочинів, або суб'єктів, котрі могли б сприяти запобіганню серйозним злочинам чи виявленню серйозних злочинів. На виконання цього акта окремі його положення імплементовані до національних законодавств багатьох країн. Проте таке законодавство викликало несприйняття, і в деяких державах воно офіційно визнано неконституційним. Зрештою, рішенням Європейського суду від 8 квітня 2014 року вказана Директива визнана недійсною на території ЄС [13]. Як указано в рішенні Суду (п. 60), зазначений акт не встановлює якихось об'єктивних критеріїв, що дають змогу визначити межі доступу компетентних національних органів до збережених даних з їх подальшим використанням з метою запобігання злочинам, виявлення або кримінального переслідування злочинів, які в силу ступеня своєї суспільної небезпеки можуть уважатися досить серйозними, щоб виправдати таке втручання в право на повагу до приватного й сімейного життя й у право на захист персональних даних.

Крім того, як відзначив Суд, Директива 2006/24 не містить основних і процесуальних умов, що стосуються доступу компетентних національних органів до даних і подальшого їх використання. Стаття 4 Директиви, яка регулює доступ цих органів до збережених даних, прямо не передбачає, що доступ і подальше використання даних має суворо обмежуватися метою запобігання точно визначеним тяжким злочинам і виявлення точно визначених тяжких злочинів або проведення кримінального переслідування, пов'язаного із цим. Вона лише передбачає, що кожна держава-член має визначити процедури, яких потрібно дотримуватися, й умови, що мають бути виконані для отримання доступу до збережених даних відповідно до вимог необхідності й пропорційності (п. 61 рішення). Отже, Суд констатував особливо серйозне втручання в основні права людини на повагу до приватного й сімейного життя та в право на захист персональних даних без того, щоб таке втручання не було суворо обмежене положеннями, які гарантують, що воно можливе тільки тоді, коли це дійсно необхідно (п. 65 рішення).

Але, за великим рахунком, у євроспільноті набагато більше позитивних напрацювань у галузі охорони персональних даних, бо цьому питанню приділяється значна увага. Можемо навести такий офіційний документ, як регламент Європейського Парламенту й Ради від 18 грудня 2000 року № 45/2001 стосовно захисту осіб з погляду обробки персональних даних установами й органами Спільноти й вільного руху таких даних [14]. У цьому акті запроваджується новий незалежний контрольний орган – Європейський інспектор із захисту персональних даних Ця особа відповідає за забезпечення того, що фундаментальні права та свободи фізичних осіб, поміж іншого їхнє право на приватність, поважаються установами й органами Спільноти. Європейський інспектор із захисту даних відповідає за моніторинг і забезпечення реалізації положень цього Регламенту та інших актів Спільноти, які стосуються захисту фундаментальних прав і свобод фізичних осіб стосовно обробки персональних даних установами або органами, й надає рекомендації установам та органам Спільноти й суб'єктам даних із питань, які стосуються обробки персональних даних (ст. 41). Із цією метою інспектор наділений повноваженнями попереджувати або застерігати контролера; розпоряджатися про виправлення, блокування, знищення або стирання всіх даних, коли вони були оброблені з порушенням положень, що регулюють обробку персональних даних, і повідомляти про такі дії третім сторонам, яким ці дані були відкриті; накладати тимчасову або постійну заборону на обробку даних (ст. 47).

У частині 1 ст. 22 Закону України «Про захист персональних даних» у первинній редакції також було передбачено адміністративний і парламентський контроль за додержанням законодавства про захист персональних даних. Для цього, зокрема, мав бути створений спеціальний уповноважений державний орган з питань захисту персональних даних. До його повноважень належало здійснення державної політики у сфері захисту персональних даних, він мав досить широку компетенцію у сфері запобігання порушенням правил обробки персональних даних та усунення негативних наслідків. У статті 23 Закону вказувалося, що уповноважений державний орган з питань захисту персональних даних є незалежним у реалізації повноважень, передбачених цим Законом. Але в подальшому шляхом унесення змін до цього Закону від 3 липня 2013 року згадка про подібну інституцію вилучена, в Законі вказано лише про парламентський і судовий контроль питань захисту персональних даних.

Висновки. З викладеного можемо резюмувати таке. Найбільш ефективним і дієвим щодо захисту й охорони персональних даних особи є законодавство ЄС. Воно розглядає ці питання в контексті захисту права суб'єкта на приватне життя, є досить структурованим і змістовним, у тому числі за галузевою спрямованістю збирання, обробки, зберігання та поширення інформації про особу. Попри те що вказані норми формально не поширюються на Україну, все ж, якщо наша держава прагне до вступу в ЄС, вона мусить поступово адаптувати своє національне законодавство до вимог Європейської

спільноти. І тут як узірець має використовуватися усталене нормативне врегулювання обороту персональних даних у ЄС. На жаль, мусимо констатувати, що національна нормативна база залишається абсолютно не розробленою. Спеціальний Закон України «Про захист персональних даних» визначає лише загальні засади, тоді як персональні дані потребують конкретного і предметного захисту в усіх сферах їх обігу.

Варто також відмітити невиправдане звуження кола осіб, які здійснюють контроль за дотриманням законодавства з питань захисту даних про особу. Абсолютно невиправданою є відмова від напрацьованої та ефективної практики ЄС щодо створення й функціонування спеціального уповноваженого державного органу з питань захисту персональних даних. Неправильним у цьому контексті є перекладання його повноважень, передбачених раніше законом, на Уповноваженого Верховної Ради з питань захисту прав людини. По-перше, заміняється адміністративний контроль на парламентський, що, погодьтеся, не одне й те саме, бо способи управління в цих органах не однакові. По-друге, компетенція Уповноваженого щодо захисту персональних даних не є виключною. Сьогодні в Україні існують численні порушення основоположних прав людини не лише в цій сфері. Тому Уповноважений мусить приділяти основну увагу їх охороні, особливо в умовах війни. При цьому питанням захисту персональних даних приділяється відверто недостатньо уваги, про що переконливо свідчить рівень нинішнього українського законодавства та судової практики, як результат, величезний набір порушень права особи на приватність шляхом незаконної обробки її персональних даних. За такого стану порушники переважно залишаються безкарними.

Література

1. Міжнародний пакт про громадянські і політичні права, прийнятий 16 грудня 1966 року Генеральною Асамблеєю ООН. URL: http://zakon.rada.gov.ua/cgibin/laws/main.cgi?nreg=995_043.

2. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних від 28 січня 1981 року. Ратифікована Україною 6 липня 2010 року. URL: http://zakon2.rada.gov.ua/laws/show/994_326.

3. Про захист персональних даних: Закон України від 1 червня 2010 року № 2297-VI. URL: http://zakon3.rada.gov.ua/laws/show/2297-17/.

4. Хартія основних прав Європейського Союзу від 7 грудня 2000 року. URL: http://zakon5.rada.gov.ua/laws/show/994_524.

5. Директива Європейського Парламенту і Ради № 95/46/ЄС про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних. URL: http://zakon.rada.gov.ua/ laws/show/994_242.

6. Про обробку персональних даних і захист прав осіб у телекомунікаційному секторі: Директива 97/66/ЄС Європейського парламенту та Ради від 15 грудня 1997 року. URL: http://zakon5.rada.gov.ua/laws/show/994_243.

7. Директива Європейського Парламенту і Ради ЄС стосовно обробки персональних даних і захисту права на недоторканність особистого життя у сфері електронних засобів зв'язку від 12 липня 2002 року № 2002/58/ЄС. URL: http://zakon5.rada.gov.ua/laws/show/994_b34.

8. Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases. URL: http://lexdigital.ru/2012/052/.

9. Рамкова Директива 2002/20/ЄС Європейського Парламенту і Ради Про дозвіл для мереж і послуг електронних засобів зв'язку від 7 березня 2002 року. URL: http://www.nkrzi.gov.ua/images/upload/58/19/612c7f47edc6f0524aaeee7546d3668b.pdf.

10. Директива 2002/22/ЄС про універсальну послугу і права користувачів стосовно мереж і послуг електронного зв'язку від 7 березня 2002 року. URL: http://nkrzi.gov.ua/images/upload/58/19/6ad521f49a3af8c4642834474a790eac.pdf.

11. Директива 2009/136/ЄК Європейського Парламенту та Ради від 25 листопада 2009 року. URL: http://www.nkrzi.gov.ua/index.php?r=site/index&pg=104&language=uk.

12. Директива Европейского парламента и Совета ЕС № 2006/24/EC. URL: http://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=celex:32006L0024.

13. Judgment of the Court (Grand Chamber), 8 April 2014. Joined Cases C-293/12 and C-594/12. Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others; Kärntner Landesregierung (C-594/12), Michael Seitlinger, Christof Tschohl and others. URL: http://curia.europa.eu/juris/document/document.jsf?docid=150642&doclang=EN.

14. Регламент Європейського Парламенту і Ради стосовно захисту осіб з точки зору обробки персональних даних установами та органами Спільноти і вільного руху таких даних від 18 грудня 2000 року № 45/2001. URL: https://www.dst.dk/ext/454209204/0/.../UKR_Regulation-(EC)-No-45_2001--docx.

Гуйван П. Д.,
кандидат юридичних наук,
заслужений юрист України, докторант
Національного юридичного університету
імені Ярослава Мудрого