УДК 340
DOI https://doi.org/10.32836/2521-6473.2021-2.15

О. В. Легка, доктор юридичних наук, професор,
професор кафедри міжнародного права
Університету митної справи та фінансів

АКТУАЛЬНІ ПИТАННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ: ВІТЧИЗНЯНИЙ ТА МІЖНАРОДНИЙ ДОСВІД

Статтю присвячено розгляду позитивного міжнародного досвіду щодо законотворчої діяльності з питань захисту персональних даних. Визначено, що серед негативних наслідків упровадження інформаційно-телекомунікаційних технологій у різних сферах суспільного життя є порушення життєво важливих прав людини, що проявляється в незаконному зборі, використанні й поширенні персональних даних, у тому числі в мережі Інтернет. Констатовано, що наразі система правового забезпечення інформаційної сфери в Україні не повною мірою відповідає змінам у змісті суспільних відносин, що сталися або відбуваються. Аналіз інформаційного законодавства, сформованого за останні два десятиліття, свідчить про його фрагментарність і неповноту, наявність дублювань і протиріч в окремих нормативно-правових актах, невідповідність сучасним вимогам розвитку інформаційної сфери.

Проаналізовано основні норми міжнародних та вітчизняних нормативно-правових документів, які регулюють питання захисту персональних даних. Досліджено основні нововведення Загального регламенту про захист фізичних осіб стосовно обробки персональних даних та про вільне переміщення таких даних (GDPR), положення про екстратериторіальність дії GDPR у контексті можливості його застосування щодо фізичних та юридичних осіб України, місце «права бути забутим» (основні правові акти, які регламентують даний напрям, рішення ЄСПЛ у справі Маріо Костехи Гонсалеса). Розкрито особливості відповідальності за порушення законодавства у сфері захисту персональних даних, наведено приклади порушень у даному напрямі. Окреслено причини невідповідності інформаційного законодавства України вимогам сучасності. Теоретично обґрунтовано, що наразі Україна перебуває на етапі становлення національної свідомості, що надає особливого значення відповідному існуючим умовам правовому регулюванню сфери інформаційних відносин. Одним із головних завдань держави на такому етапі розвитку є визначення напрямів правового регулювання та створення правових гарантій, необхідних для самореалізації суб'єктів в інформаційній сфері. Надано пропозиції щодо основних шляхів адаптації вітчизняного законодавства про захист персональних даних до міжнародних стандартів.

Ключові слова: *захист інформації, цифровізація, міжнародний досвід, інформаційні технології, законодавство, цілісність та конфіденційність, інформаційні загрози.*

O. V. Lehka. Current issues of personal data protection: domestic and international experience

It is devoted to the consideration of positive international experience in legislative activity on personal data protection. It is determined that among the negative consequences of the introduction of information and telecommunication technologies in various spheres of public life is the violation of vital human rights, which manifests itself in the illegal collection, use and dissemination of personal data, including on the Internet. It is stated that currently the system of legal support of the information sphere in Ukraine does not fully correspond to the changes in the content of public relations that have occurred or are taking place. The analysis of the information legislation formed for the last two decades testifies to its fragmentation and incompleteness, existence of duplications and contradictions in separate regulatory legal acts, inconsistency with modern requirements of development of information sphere.

The basic norms of international and domestic normative-legal documents, which regulate the issues of personal data protection, are analyzed. The main innovations of the General Regulation on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data (GDPR), the provisions on the extraterritoriality of the GDPR in the context of its application to individuals and legal entities of Ukraine, the place of regulating this area, the decision of the European Court of Human Rights in the case of Mario Costeha Gonzalez). The peculiarities of liability for violations of the legislation in the field of personal data protection are revealed, examples of violations in this direction are given. The reasons for the inconsistency of the information legislation of Ukraine with modern requirements are outlined. It is theoretically substantiated that Ukraine is currently at the stage of formation of national consciousness, which attaches special importance to the legal regulation of the sphere of information relations corresponding to the existing conditions. One of the main tasks of the state at this stage of development is to determine the areas of legal regulation and the creation of legal guarantees necessary for self-realization of subjects in the information sphere. Suggestions are given on the main ways to adapt domestic legislation on personal data protection to international standards: to systematize and codify national legislation in accordance with European law and international law; develop a single legal act that would regulate at the legislative level the collection, processing, protection and transfer of information, following the example of the GDPR

Key words: *information protection, digitalization, international experience, information technologies, legislation, integrity and confidentiality, information threats.*

> Інформація – це не тільки сила, що створює. На жаль, вона володіє дестабілізуючим потенціалом для суспільства, якщо її практично необмежені можливості впливу на людину і суспільство використовуються в інтересах коаліційних співтовариств, окремих держав, політичних угруповань чи окремих осіб. Досвід новітньої історії світу визначив очевидність: інформація може стати джерелом політичної та соціальної загроз.
>
> А. Ю. Нашинець-Наумова

Постановка проблеми. Однією з найважливіших характеристик держави, яка істотно впливає на всі процеси соціально-економічного розвитку суспільства, є рівень інформаційного забезпечення системи державної влади. Свобода доступу до інформації та свобода її поширення, підвищення конкурентоспроможності економіки й розширення можливостей її інтеграції у світову систему господарства, підвищення ефективності державного керування – усі ці переваги надає нам користування інформаційно-комунікативними технологіями. Світ стає більш залежним від сучасних технологій. Під впливом загальних тенденцій цифровізації змінюються умови функціонування, розширюється коло електронних ресурсів, збільшуються обсяги інформації, що використовуються органами влади в різних напрямах діяльності, запроваджуються нові засоби та методи їх комунікації, змінюються їхні інформаційні потреби та інтереси, а відповідно, модернізуються правові засади щодо захисту інформації. Зважаючи на те, що в геополітичному просторі світу інформаційні технології та інформація в цілому отримали визначальне значення, правовий аспект дослідження питань щодо захисту інформації, на думку А.Ю. Нашинець-Наумової, набуває все більшої актуальності, адже процеси збору, накопичення, перероблення і розповсюдження інформації стають необхідною умовою існуючих структур політичного та іншого управління, здійснення ефективних політичних впливів, вирішення масштабних економічних задач [1]. Ця проблематика, як слушно зазначає Х.Я. Терешко, сенситивна, людиноцентристська, адже є особливо вразливою, про що неодноразово у своїх рішеннях наголошував Європейський суд з прав людини: «Охорона відомостей особистого характеру має основоположне значення для здійснення права на повагу до приватного і сімейного життя. Дотримання конфіденційності відомостей – основний принцип правової системи всіх держав – учасниць Конвенції» (справа «М. С. проти Швеції», 1997) [2]. Згідно з даними аналітичного центру Info Watch, за минулі 13 років у всьому світі з комерційних компаній і державного сектора витекло приблизно 44 млрд записів персональних даних, з них близько 14 млрд записів – тільки за останній рік. Тобто тема захисту персональних даних громадян в умовах цифровізації набуває не просто актуальності, але й виняткової важливості.

Аналіз останніх досліджень і публікацій. Аналіз наукової літератури дозволяє нам стверджувати, що проблемам захисту персональних даних приділяли увагу в наукових дослідженнях як вітчизняні, так і зарубіжні вчені, зокрема, питання міжнародної та національної інформаційної безпеки розглядали: О.А. Баранов, Г.О. Блінова, В.М. Брижко, Д.П. Василенко, І.М Забара, О.О. Золотар, Б.А. Кормич, Д.А. Коваль, Є.А. Макаренко, А.Ю. Нашинець-Наумова, С.А. Серьогін, В.І. Теремецький, Є.Б. Тихомирова, Т.Ю. Ткачук, К.С. Шахбазян та ін.; проблематиці визначення права на забуття приділяли увагу Г.О. Андрощук, Ю.С. Размєтаєва, П.М. Сухорольський, М.І. Тарнавський, І.С. Федоришина; питання щодо захисту інформації в медичній сфері досліджували В.І. Акопов, А.С. Андрійчук, М.М. Малеїна, А.І. Марущак, І.Я. Сенюта, С.Г. Стеценко та ін. Проте їхні висновки, як свідчить аналіз міжнародного та вітчизняного законодавства, наукових досліджень у даному напрямі, а також судової практики, у т.ч. Європейського суду з прав людини, у зв'язку з останніми законодавчими змінами частково втратили актуальність, що й зумовило вибір теми дослідження.

Метою статті є аналіз міжнародно-правового та вітчизняного досвіду регулювання захисту персональних даних в інтересах удосконалення системи національного законодавства.

Виклад основного матеріалу. Питання захисту інформації, зокрема персональних даних, наразі перебуває на етапі становлення як у національному, так і в міжнародному політичному, правовому та науковому дискурсі. Адже захист персональних даних є не просто обов'язком держави і предметом державно-правового регулювання, його необхідно розглядати в поєднанні із захистом прав людини. «Джерелом» системи захисту персональних даних вважається Конвенція про захист прав людини і основоположних свобод, ст. 8 якої передбачено, що «органи державної влади не можуть втручатись у здійснення цього права, за винятком випадків, коли втручання здійснюється згідно із законом і є необхідним у демократичному суспільстві в інтересах національної та громадської безпеки чи економічного добробуту країни, <…> в тому числі для захисту прав і свобод інших осіб» [3]. Європейський суд з прав людини, заснований Конвенцією, у своєму рішенні у справі «Леандер проти Швеції» вперше зазначив, що зберігання державними органами інформації про особу є втручанням в її право на повагу до приватного життя, а тому таке втручання повинне відповідати вимогам, викладеним у ч. 2 ст. 8 Конвенції [4]. «Кожен має право на повагу до свого приватного та сімейного життя, до свого житла і кореспонденції», – закріплено у ст. 8 Конвенції.

У науці права сьогодні розглядаються дві діаметрально різні позиції стосовно поняття приватності: відповідно до першої приватність, зважаючи на обсяги персональних даних, з часом зникне, інша ж наголошує на абсолютній цінності права на повагу до приватного життя, потреба в якій зростає в еру технологій, коли є можливість заробити на витоку персональних даних, а отже, політика держави щодо підвищення безпеки даних набуває першочергового значення [5].

Нормативне регламентування захисту персональних даних передбачено в нормах міжнародних договорів з прав людини як складова частина права на приватність: ст. 17 Міжнародного Пакту про громадянські та політичні права («Ніхто не повинен зазнавати <…> свавільних чи незаконних посягань на недоторканність його житла або таємницю його кореспонденції…» (дану норму включено і до ст. 16 Конвенції про права дитини) [6]; ст. 11 Американської конвенції з прав людини; ст. 7 Хартії основних прав Європейського Союзу; Керівних принципах із захисту недоторканності приватного життя і транскордонних потоків персональних даних; Керівних принципах регулювання комп'ютерних файлів, які містять персональні дані; Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних; ст. 8 Директиви Європейського Парламенту і Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних»; Загального регламенту Європейського Парламенту і Ради (ЄС) «Про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС». До речі, Закон України «Про захист персональних даних» базується саме на положеннях Директиви 95/46/ЄС.

На національному рівні питання захисту персональних даних регламентовано: ст. 32 Конституції України: «Не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини» [7]; ч. 2 ст. 21 Закону України «Про інформацію»: «конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, установлених законом» [8]; ч. 1 ст. 7 Закону України «Про захист персональних даних», причому норми ч. 1 цієї статті не застосовуються в разі, якщо обробка персональних даних здійснюється за умови надання суб'єктом персональних даних однозначної згоди на обробку таких даних (п. 1 ч. 2) чи необхідна в цілях охорони здоров'я (п. 6 ч. 2) [9]; та підзаконними нормативно-правовими актами (Типовий порядок обробки персональних даних; Порядок здійснення Уповноваженим ВРУ контролю за додержанням законодавства про захист персональних даних; Порядок повідомлення Уповноваженого ВРУ з прав людини про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних, про структурний підрозділ або відповідальну особу, що організовує роботу, пов'язану із захистом персональних даних під час їх обробки, а також оприлюднення вказаної інформації).

Епохальним документом у напрямі захисту персональних даних став прийнятий 26.04.2016 (набув чинності 25.05.2018) Загальний регламент із захисту персональних даних (General Data Protection Regulation – GDPR), який замінює попередні закони про захист даних ЄС, встановлює правила обробки та вільного руху персональних даних і застосовується до всіх доменів публічного та приватного секторів. Незважаючи на те, що Україна не є державою-учасницею Європейського Союзу (ЄС), правила, закріплені в GDPR, можуть стосуватися безпосередньо суб'єктів, що належать до її юрисдикції. Оскільки відповідно до ст. 3 Загального регламенту «територіальна сфера дії GDPR має екстратериторіальну дію, то його норми поширюються не лише на держави-члени ЄС, а й на фізичних та юридичних осіб інших країн у конкретних випадках, передбачених GDPR» [10].

Загальним регламентом передбачено, що персональні дані повинні оброблятися відповідно до таких принципів захисту даних: оброблено законно, справедливо та прозоро; збираються із законною метою; адекватні, актуальні й обмежені необхідністю; точні; зберігаються стільки, скільки потрібно; забезпечено безпеку, цілісність та конфіденційність [11]. Крім того, GDPR встановлює вищі стандарти стосовно інформованої згоди та обов'язків щодо повідомлення, посилює захист: права на доступ до персональних даних про здоров'я та права громадян на видалення інформації.

Роблячи екскурс в історію, зазначимо, що ще у 2012 році Європейською комісією було запропоновано законодавчий пакет щодо модернізації правил захисту даних (у ньому, зокрема, і було передбачено право на видалення інформації, тобто «право на забуття», яке гарантує особам право вимагати від контролера видалення незаконно оброблених чи застарілих, недоречних, неповних, неточних або надлишкових даних чи інформації, законні підстави для зберігання якої зникли з плином часу), який включав два законодавчі інструменти – загальні правила захисту даних (призначені для заміни Директиви 95/46/ЄС 1995 року) та Директиви захисту даних у галузі правоохоронної діяльності (призначеної замінити Рішення Ради в межах захисту персональних даних, що обробляються в рамках поліцейської та судової співпраці у кримінальних справах 2008/977/JHA 2008 року [12]). Європейський суд з прав людини (ЄСПЛ) у 2014 році виніс рішення, яким право бути забутим було затверджено. Це викликало неабиякі зміни в юридичній практиці та дискусії щодо відповідного права по всьому світу. Справа розглядалася на підставі звернення іспанського громадянина Маріо Костехи Гонсалеса, який поскаржився на оголошення в газеті (електронна версія видання містилася

на сайті), що були опубліковані в 1998 році, але все ще були доступні в Інтернеті. Вони стосувалися банкрутства та аукціону нерухомості щодо продажу його будинку за борги. Пошуки Google за його іменем приводили до посилань на ці сторінки. Маріо Костехи хотів, щоб їх було видалено, оскільки його борги давно були погашені, і ця інформація була неактуальною і не відображала той стан справ, яким він є сьогодні, що шкодило його репутації [13]. ЄСПЛ постановив, що з метою забезпечення прав, передбачених у згаданих положеннях Директиви, «оператор пошукової системи, посилання на веб-сторінки, розміщені третіми особами, що містять інформацію про цю особу, також і у випадку, коли ім'я або інформація не видалена перед тим або у той самий час із самих веб-сторінок системи, зобов'язаний видалити зі списку результати, видані у відповідь на пошуковий запит на основі імені особи, і навіть коли публікація на цих сторінках розміщена на законних підставах» [13; 14, с. 94]. Зазначимо, що за останні 5 років Google отримав понад 800 тис. таких звернень, у 45% він їх прийняв, хоча це не завжди обходилося без втручання суду.

Загальним регламентом із захисту персональних даних «право бути забутим» передбачено ст. 17 «Right to erasure (right to be forgotten)» («Право на стирання (право бути забутим)», яку доповнює ст. 21 «Right to object» («Право подавати заперечення») [11]. Згідно з нормами цих статей суб'єкт даних має право вимагати стирання персональних даних, які його стосуються, і відповідний обов'язок стирати ці дані з боку контролера даних у випадку, якщо суб'єкт даних заперечує проти обробки даних і відсутні легітимні підстави для такої обробки, які переважають інтереси, права та свободи суб'єкта даних. Разом із цим п. 3 ст. 17 GDPR обмежує можливості вимагати стирання даних, коли йдеться про реалізацію права на свободу вираження та інформації, виконання завдань, пов'язаних з публічними інтересами, науковими, історичними, статистичними дослідженнями тощо [14, с. 95]. Що стосується національного законодавства, то відповідно до Закону України «Про захист персональних даних» суб'єкт персональних даних має право «пред'являти вмотивовану вимогу щодо зміни або знищення своїх персональних даних будь-яким власником та розпорядником персональних даних, якщо ці дані обробляються незаконно чи є недостовірними» [9]. Крім того, Законом України «Про внесення змін до Закону України «Про захист населення від інфекційних хвороб» від 13.04.2020 р. № 555-IX щодо запобігання поширенню коронавірусної хвороби (COVID-19)» передбачено, що після закінчення періоду встановлення карантину, інформація, яка відноситься до персональних даних, упродовж 30-ти днів підлягає знеособленню, а в разі неможливості – знищенню [15].

Заслуговує на увагу й те, що в разі витоку персональних даних відповідно до ст. ст. 33, 34 Загального регламенту із захисту персональних даних контролери даних інформують контролюючий орган протягом 72 год., а у разі порушення безпеки даних вони повинні інформувати пацієнтів [11]. Таким чином, GDPR дає зрозуміти, що організації повинні нести відповідальність за зібрані ними персональні дані, це забезпечується шляхом проведення юридичного аудиту для оцінки не лише того, які особисті дані були набуті, але й того, як вони захищені. Найменша сума штрафу відповідно до GDPR – 20 млн євро (для порівняння: ч. 5 ст. 188-39 Кодексу України про адміністративні правопорушення – 34 тис. грн).

Слід звернути увагу, що вже на наступний день після набрання чинності GDPR надійшли перші скарги щодо його порушення, які стосувалися порушень Facebook, Instagram, WhatsApp, Google, Android вільного надання згоди на обробку даних користувачами. Восени 2018 року португальський наглядовий орган (CNPD) оштрафував місцеву клініку на загальну суму 400 тис. євро за доступ працівників клініки до персональних даних пацієнтів через фальшиві облікові записи. У березні 2019 року в Польщі накладено штраф на загальну суму 220 тис. євро. на компанію, яка займалася збором даних із відкритих реєстрів та фактично здійснювала обробку даних понад 7 млн фізичних осіб без належного повідомлення всіх осіб про обробку їхніх персональних даних. У 2020 році через помилку співробітника лікарні, який випадково завантажив на Git Hub електронну таблицю з іменами користувачів, паролями і ключами доступу до конфіденційних державних систем, у відкритий доступ потрапили особисті та медичні дані 16 млн бразильців, які лікувалися від коронавірусу. У результаті інформацію було видалено з Git Hub, а урядовці змінили паролі й відкликали ключі доступу, щоб убезпечити свої системи [16].

Не стала винятком і Україна. Так, у кінці 2020 року Національний координаційний центр кібербезпеки (НКЦК) при Раді безпеки і оборони України в ході моніторингу виявив витік персональних медичних даних з однієї з найбільших клінік Дніпра. «Серед інформації, яка опинилася у відкритому доступі, – персональні дані працівників і клієнтів цієї клініки, зокрема ПІБ, дати народження, адреси проживання, телефони, e-mail, діагнози, дані медичної карти (що становить медичну інформацію), включаючи результати аналізів, діагнози, інформацію про захворювання, результати проведення ПЛР-тестів, списки хворих на COVID-19». Витік стався в результаті помилок конфігурації в інформаційних системах і базах даних клініки, які мали доступ в мережу Інтернет. Варто звернути увагу на те, що вільний доступ до баз даних надавав можливість не лише викрадення персональної інформації, але й несанкціонованого внесення змін, включаючи модифікацію призначень ліків, результатів аналізів і обстежень, редагування записів у протоколах [17].

Відповідно до п. 11 Плану заходів щодо імплементації Угоди про асоціацію між Україною та ЄС, затвердженого 25.10.2017 р., Україна має вдосконалити законодавство про захист персональних даних з метою приведення його у відповідність до GDPR. Однією з основних причин невідповідності інформаційного законодавства України вимогам сучасності, на думку В.П. Горбуліна, є несформованість у суспільній і науко-

вій думці цілісного уявлення про інформаційну безпеку з позиції права та юридичної науки [18]. Сьогодні в Україні захистом персональних даних опікується лише Уповноважений Верховної Ради з прав людини та кіберполіція. Уповноважений може скласти адміністративний протокол на державний орган чи установу, якщо вони порушують право людини на захист персональних даних, а кіберполіція розслідує кримінальні правопорушення, зокрема пов'язані з «витоком» даних із держреєстрів. Відповідно до інформації з Єдиного порталу судових рішень у 2020 р. налічується лише 15 реальних вироків за такими справами. За минулі роки таких справ ще менше [19]. «Невелика кількість складених протоколів про адміністративні правопорушення щодо захисту персональних даних, зазначає І. Берназюк, представник Уповноваженого Верховної Ради України з прав людини, викликана передусім обмеженням строків притягнення до відповідальності (3 місяці із дня вчинення), а звернення здебільшого надходять до секретаріату Уповноваженого вже після пропущення строків» [19]. Викладене вище свідчить, що національне законодавство потребує суттєвих і негайних змін.

Слід зазначити, що в листопаді 2019 року при Секретаріаті Уповноваженого Верховної Ради України з прав людини створено міжвідомчу робочу групу щодо розроблення законодавчих пропозицій у сфері захисту персональних даних, крім того, створено координаційну робочу групу з розроблення законопроєкту щодо внесення змін до Закону України «Про захист персональних даних» відповідно до положень GDPR. Проте наразі суттєвих змін у вітчизняному законодавстві не відбулося. Поданий міжвідомчою робочою групою при Уповноваженому Верховної Ради України з прав людини проєкт Закону України «Про внесення змін до Закону України «Про захист персональних даних» (щодо форм та умов надання згоди на обробку персональних даних)» від 10.02.2020 р. № 2671-1, 04.03.2020 повернуто на доопрацювання.

Висновки з дослідження та перспективи подальших розвідок у цьому напрямі. Підсумовуючи, зазначимо, що наразі Україна перебуває на етапі становлення національної свідомості, що надає особливого значення відповідному існуючим умовам правовому регулюванню сфери інформаційних відносин. Одним із головних завдань держави на такому етапі розвитку є визначення напрямів правового регулювання та створення правових гарантій, необхідних для самореалізації суб'єктів в інформаційній сфері. Із цією метою необхідно: систематизувати та кодифікувати національне законодавство відповідно до норм європейського законодавства та міжнародного права; розробити єдиний нормативно-правовий акт, який на законодавчому рівні врегулював би збір, обробку, захист та передачу інформації за прикладом GDPR; привести понятійний апарат у відповідність до міжнародного законодавства; передбачити обов'язкову сертифікацію на захист інформації; розробити технології криптографії/кодування; посилити відповідальність за порушення захисту інформації про персональні дані.

Перспективи подальших наукових розвідок, на наш погляд, полягають у подальшому науковому дослідженні питань, що стосуються аналізу міжнародного досвіду в контексті вдосконалення вітчизняного у сфері захисту інформації персонального характеру в Україні.

Список використаних джерел:

1. Нашинець-Наумова А.Ю. Інформаційна безпека: питання правового регулювання : монографія. Київ : Гельветика, 2017. 168 с. С. 5.

2. Терешко Х.Я. Види інформації як об'єкта цивільних правовідносин у сфері медичного обслуговування. *Медичне право*. 2019. № 1 (23). С. 65–73.

3. Концепція про захист прав людини і основоположних свобод від 04.11.1950 р. (ратифікована 17.07.1997 р. № 475/97-ВР). URL: https://zakon.rada.gov.ua/laws/show/995_004#Text

4. Бем М.В., Городиський І.М. Захист персональних даних: правове регулювання та практичні аспекти : науково-практичний посібник. Київ : К.І.С., 2015. 220 с.

5. Вчимося на помилках: найбільші штрафи за порушення норм GDPR. *Юридична газета онлайн.* 2020. № 10 (716). URL: https://yur-gazeta.com/publications/practice/informaciyne-pravo

6. Міжнародний Пакт про громадянські та політичні права від 16.12.1966 р. № 995_043. URL: https://zakon.rada.gov.ua/laws/show/995_043#Text

7. Конституція України від 28 червня 1996 року. *Відомості Верховної Ради України (ВВР).* 1996. № 30. Ст. 141.

8. Про інформацію: Закон України від 02.10.1992 р. № 2657-XII (у редакції від 16.07.2020). *Відомості Верховної Ради України (ВВР).* 1992. № 48. Ст. 650. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text

9. Про захист персональних даних : Закон України від 01.06.2010 р. № 2297-VI. URL: http://zakon.rada.gov.ua/laws/show/2297-17

10. Овчаренко Я.О. Регламент захисту персональних даних Європейського Союзу. *Юридичний науковий електронний журнал*. 2018. № 3. С. 237.

11. Загальний регламент із захисту персональних даних Європейського Союзу (GDPR) № 2018/1725. URL: http://aphd.ua/gdpr-ofitsiinyi-ukranskyi-pereklad

12. Council framework decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters of 27 November 2008. URL: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32008F0977&from=EN

13. Google Spain SL Google Inc. V Agencia Española de Protección de Datos (AEPD) Mario Costeja González Judgment of the Court (Grand Chamber) in Case C-131/12, 13 May 2014. URL: http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=794833

14. Сухорольський П. Право бути забутим у правовій системі Європейського союзу: реалії, проблеми та перспективи. Наука міжнародного права на рубежі століть. Тенденції розвитку та трансформації: спеціальне видання наукових статей. Львів : ЛНУ імені Івана Франка, 2016. С. 90–101.

15. Про внесення змін до Закону України «Про захист населення від інфекційних хвороб» щодо запобігання поширенню коронавірусної хвороби (COVID-19)» : Закон України від 13.04.2020 р. № 555-IX. *Відомості Верховної Ради України* (ВВР). 2020. № 19. Ст. 127. URL: https://zakon.rada.gov.ua/laws/show/555-20#Text

16. У Бразилії у відкритий доступ потрапили дані 16000000 пацієнтів з COVID-19. URL: https://xakep.ru/2020/11/27/covid-leak

17. Выявлена утечка персональных данных пациентов в одной из крупнейших частных клиник Днепра. URL: https://interfax.com.ua/news/general/692349.html

18. Горбулін В.П., Додонов О.Г., Ланде Д.В. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання : монографія. Київ : Інтертехнологія, 2009. 164 с.

19. Хто і як контролює сферу захисту персональних даних. *Юридична газета*. URL: https://yur-gazeta.com/publications/practice/informaciyne-pravo-telekomunikaciyi/skandal-cifra-diya.html