

МІЖНАРОДНЕ ПРАВО. ПОРІВНЯЛЬНЕ ПРАВОНАВСТВО

УДК 340

DOI <https://doi.org/10.32782/2521-6473.2023-2.8>

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

ІМПЛЕМЕНТАЦІЯ МІЖНАРОДНИХ СТАНДАРТІВ ЩОДО ЗАХИСТУ ПРАВА НА ДОСТУП ДО ІНФОРМАЦІЇ В УКРАЇНІ

Присвячено дослідженню вітчизняного правового регулювання захисту права на доступ до інформації, ключових міжнародних стандартів, а також визначенню доцільності його імплементації у вітчизняне законодавство. Констатовано, що інформатизація – невід’ємна складова економічного розвитку країни, разом з тим сучасне інформаційне суспільство є контекстом формування нової загрози щодо права людини на безпеку. Проаналізовано Закон України «Про захист персональних даних» та Конвенцію Ради Європи про захист осіб у зв’язку з автоматизованою обробкою персональних даних. Виокремлено основні проблемні питання. Розглянуто статистику порушень вітчизняного законодавства у даному напрямі, факти витоку персональних даних через офіційні веб-сайти. Звернено увагу на певні обмеження конституційних права і свобод людини і громадянина, передбачені статтею 34 Конституції України у період правового режиму воєнного стану в Україні. Обґрунтовано, що основним міжнародним стандартом щодо захисту інформації є Загальний регламент ЄС про захист даних 2016/679. Він має не лише пряму регулятивну дію в рамках національного права держав-членів ЄС, але й пріоритет у разі «конфлікту» між національним правом та регламентом. Проаналізовано основні принципи та механізми Регламенту. Здійснено порівняльний аналіз Регламенту та Директиви Європейського парламенту та Ради ЄС «Про захист фізичних осіб щодо обробки персональних даних ...» № 2016/680. Розглянуто проекти законів України «Про захист персональних даних» № 8153 та «Про Національну комісію з питань захисту персональних даних та доступу до публічної інформації» № 6177, які розроблено відповідно до вимог Регламенту. Обґрунтовано, що реалізація ефективного контролю Уповноваженим Верховної Ради України з прав людини, відповідно до норм міжнародних стандартів, неможлива. Адже поєднання функцій контролю з правами, передбаченими мандатом Омбудсмана, впливає на зниження ефективності їх реалізації. Констатовано, на підставі аналізу Регламенту та Закону України «Про захист персональних даних», що вітчизняний механізм права на захист інформації «право бути забутим» не відповідає нормам міжнародних стандартів. Надано пропозиції щодо удосконалення правового регулювання у досліджуваному контексті.

Ключові слова: захист інформації, правовий захист, доступ до інформації, міжнародні стандарти, правове регулювання, контроль, відповідальність.

O. V. Lehka. Implementation of international standards regarding the protection of the right to access to information in Ukraine

Dedicated to the study of the domestic legal regulation of the protection of the right to access to information, key international standards, as well as determining the expediency of its implementation into the domestic legislation. It was established that informatization is an integral component of the economic development of the country, at the same time, the modern information society is the context of the formation of a new threat to the human right to security. The Law of Ukraine “On the Protection of Personal Data” and the Convention of the Council of Europe on the Protection of Individuals in Connection with Automated Processing of Personal Data are analyzed. The main problematic issues are singled out: illegal distribution and use of personal data; lack of mechanisms ensuring the integrity and confidentiality of information; collection by electronic services and mobile applications of excessive data regarding the primary purposes of processing. The statistics of violations of domestic legislation in this area, the facts of leakage of personal data through official websites were considered. Attention is drawn to certain limitations of the constitutional rights and freedoms of a person and a citizen, provided for by Article 34 of the Constitution of Ukraine during the period of the legal regime of martial law in Ukraine. It is substantiated that the main international standard for information protection is the EU General Data Protection Regulation 2016/679. It has not only a direct regulatory effect within the framework of the national law of the EU member states, but also a priority in case of “conflict” between the national law and the regulation. The main principles and mechanisms of the Regulation are analyzed. A comparative analysis of the Regulation and Directive of the European Parliament and the Council of the EU “On the protection of natural persons regarding the processing of personal data...” No. 2016/680 was carried out. Draft laws of Ukraine “On Personal Data Protection” No. 8153 and “On

the National Commission for Personal Data Protection and Access to Public Information” No. 6177, which were developed in accordance with the requirements of the Regulation, were considered. It is substantiated that the implementation of effective control by the Commissioner of the Verkhovna Rada of Ukraine on human rights, in accordance with the norms of international standards, is impossible. After all, the combination of control functions with the rights provided for by the mandate of the Ombudsman reduces the effectiveness of their implementation. Based on the analysis of the Regulation and the Law of Ukraine “On the Protection of Personal Data”, it was established that the domestic mechanism of the right to information protection “the right to be forgotten” does not meet the norms of international standards. Suggestions for improving legal regulation in the studied context are provided.

Key words: information protection, legal protection, access to information, international standards, legal regulation, control, responsibility.

Постановка проблеми. Активна інформатизація – невід’ємна складова економічного розвитку країни. З кожним роком зростає кількість адміністративних послуг, які надаються онлайн, упроваджуються електронні сервіси, мобільні додатки, функціоналом яких передбачено збір та обробку персональних даних у різних сферах, «перетворюючи їх на цифровий продукт, який може використовуватися з різною метою, в тому числі незаконною і шкідливою» [1]. Слушною у даному контексті є наукова думка О. Золотаря: «... сучасне інформаційне суспільство є контекстом формування нової загрози права людини на безпеку» [2]. Так, у 2020 році до Уповноваженого Верховної Ради України з прав людини надійшло 3800 скарг громадян щодо порушення їх права на захист доступу до публічної інформації [1], у 2021 – 1375 [3], у 2022 – 1370 [4]. Зазначимо, що ч. 1 ст. 24 Закону України «Про захист персональних даних» від 01.06.2010 № 2297-VI передбачено, що «володільці, розпорядники персональних даних та треті особи зобов’язані забезпечити захист цих даних від випадкових втрати або знищення, від незаконної обробки, у тому числі незаконного знищення чи доступу до персональних даних» [5]. Відповідно до ст. 6 Конвенції Ради Європи про захист осіб у зв’язку з автоматизованою обробкою персональних даних, персональні дані не можуть піддаватися автоматизованій обробці, якщо внутрішнє законодавство не забезпечує відповідних гарантій. Разом з тим, Уповноваженим Верховної Ради України з прав людини за результатами моніторингу засобів масової інформації виявлено непоодинокі випадки порушення посадовими особами володільців та розпорядників персональних даних цього обов’язку, що, як наслідок, призвело до незаконного до них доступу. Серед основних проблемних питань: неправомірне поширення та використання персональних даних; відсутність механізмів, що забезпечують цілісність та конфіденційність інформації; збір електронними сервісами та мобільними додатками надмірних даних щодо первинних цілей обробки; оприлюднення в мережі Інтернет персональних даних українських військових та іноземних громадян, які надають військову допомогу Україні на період дії воєнного стану; надмірний збір персональних даних надавачами гуманітарної, волонтерської та іншої благодійної допомоги населенню. Так, наприклад: у березні 2021 року в мережі Інтернет виявлено факт витоку персональних даних невизначеного кола осіб через офіційний веб-сайт Мінветеранів шляхом поширення гіперпосилання на відкриті Google-форми з особистими даними громадян, які хочуть вакцинуватися від COVID-19 (ПІБ, дата народження, адреса проживання, номер телефону, професійна діяльність тощо); у квітні 2021 року відкрито кримінальне провадження за статтю 182 Кримінального кодексу України (далі – ККУ) за фактом оприлюднення на веб-сайті та на Telegram-каналі файлів з персональними даними військовослужбовців ЗСУ, НГУ (ПІБ, дата народження, номер військової частини, звання, місце проживання та реєстрації, номер телефону); у вересні 2021 року відкрито кримінальне провадження за ст. 182 ККУ за фактом виявлення на одному з веб-сайтів у мережі Інтернет бази даних жителів України (понад 53 мільйони записів про персональні дані – ПІБ, номери телефонів, місця реєстрації, інформація про надані адмінпослуги, пов’язані з використанням транспортних засобів) [3].

Перебування України в умовах воєнного стану ще більше посилює питання щодо забезпечення ефективного захисту права на інформацію. Адже в таких умовах витік інформації може спричинити загрозу інформаційної безпеки не лише особи, але й обороноздатності держави. Згідно з інформацією Державної служби спеціального зв’язку та захисту інформації України у період з 24.02.2022 по 20.04.2023 Урядовою командою реагування на комп’ютерні надзвичайні події CERT-UA зареєстровано понад 1500 кібератак, більша частина яких з боку Російської Федерації [4].

Саме тому на сьогодні досить актуальним є розгляд питання щодо імплементації у вітчизняне законодавство позитивного міжнародного досвіду. Адже захист права на доступ до інформації є не просто обов’язком держави і предметом державно-правового регулювання, його необхідно розглядати у поєднанні із захистом прав людини.

Аналіз останніх досліджень та публікацій. Питанню щодо захисту прав на доступ до інформації приділяли увагу у своїх наукових дослідженнях М.В. Бем, В.М. Вовк, І.М. Городинський, О.М. Калітенко, У.М. Олійник, О.М. Радіоненко, Г. Саттон, В.І. Теремецький та інші. Звісно, зазначені наукові надбання заслуговують на увагу, разом з тим, зважаючи на набуття чинності у 2018 році Загального регламенту ЄС про захист даних від 2016/679, не вичерпують глибини всієї проблематики, оскільки ряд питань потребує додаткового вивчення та обґрунтування.

Метою є дослідження вітчизняного правового регулювання захисту прав на доступ до інформації, ключових міжнародних стандартів, а також визначення доцільності його імплементації у вітчизняне законодавство.

Результати дослідження. В Україні право на захист та доступ до інформації є фундаментальними правами людини і гарантуються Конституцією України (ст. 34), Конвенцією про захист прав людини і основоположних свобод (статті 8, 10), Загальною декларацією прав людини (статті 12, 19), Міжнародним пактом про громадянські і політичні права (статті 17, 19), Конвенцією Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних (Конвенція 108) та Конвенцією Ради Європи про доступ до офіційних документів. Крім того, законами України «Про інформацію» (визначено основні принципи, суб'єкти, об'єкти інформаційних відносин), «Про захист персональних даних» (урегульовано відносини, пов'язані із захистом персональних даних під час їх обробки), «Про доступ до публічної інформації» (передбачено порядок здійснення та забезпечення права кожного на доступ до інформації).

На період дії в Україні воєнного стану, право на свободу думки і слова, на вільне вираження своїх поглядів і переконань, передбачене статтею 34 Конституції України, може обмежуватися (п. 3 Указу Президента України «Про введення воєнного стану в Україні» від 24.02.2022 № 64/2022).

Глобальні реформи та «модернізація» стандартів захисту права на доступ до персональних даних у праві Ради Європи (Конвенція Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних, із змінами, внесеними Протоколом СЕТS № 223), та праві ЄС (прийняття Загального регламенту захисту персональних даних № 2016/679 (GDPR) та Директиви 2016/680/EU) розпочалися з 2018 року.

Загальний регламент ЄС про захист даних від 27.04.2016 № 679 (далі – GDPR) на сьогодні є основним міжнародним стандартом щодо захисту інформації. Він має не лише пряму регулятивну дію в рамках національного права держав-членів ЄС, але й пріоритет у разі «конфлікту» між національним правом та регламентом. GDPR замінює попередні закони про захист даних у ЄС, встановлює правила обробки та вільного руху персональних даних і застосовується до всіх доменів публічного та приватного сектору.

Серед основних прав суб'єктів персональних даних, передбачених GDPR, право на: доступ (ст. 15), уточнення (ст. 16), видалення даних (ст. 17), обмеження обробки (ст. 18), перенесення даних (ст. 20), заперечення (ст. 21), не бути об'єктом автоматизованого ухвалення рішень (ст.22), подати скаргу до наглядового органу (ст. 77), компенсацію.

GDPR має більш прозорий підхід до виконання зобов'язань, покладених на контролерів, зобов'язуючи їх надавати повне розкриття всієї діяльності щодо обробки даних, їх призначення, правових підстав (згода із зазначенням можливих ризиків щодо передачі даних; договірне та переддоговірне виконання; суспільний інтерес або життєво важливий інтерес фізичної особи, включаючи юридичні питання (судовий захист); згідно із законодавством ЄС та/або членів ЄС джерело даних є загальнодоступним [6]) та механізмів щодо трансграничної передачі персональних даних (запровадження сертифікаційних механізмів – гарантія для трансграничної передачі персональних даних за межі ЄС (ст. 46).

Зазначеним документом встановлено вищі стандарти щодо: інформованої згоди на збір та обробку інформації; права на видалення інформації, а також обов'язків контролера упродовж 72 год. повідомляти осіб у разі витоку їх персональних даних

Суттєвим нововведенням GDPR є підвищення рівня спільної відповідальності контролера та процесора як за невідповідність стандартам GDPR, так і за витік інформації. Так, наприклад, адміністративний штраф за «просте» недотримання норм GDPR сягає до 2% від загального річного доходу закладу або 10 млн євро і до 4% від загального річного доходу або 20 млн євро у разі серйозних порушень (ст. 83) [7].

До, речі, два з п'яти найбільших штрафів в історії GDPR було накладено саме за невідповідність нормам GDPR. Зокрема, у справі “Google LLC” французький DPA (CNIL) за скаргами приватних позивачів (суб'єктів даних) наклав штраф у розмірі 50 млн євро за невиконання зобов'язання щодо прозорості та поінформованості і нездатність отримати дійсну правову основу для обробки даних [8]. У справі “Deutsche Wohnen SE51” німецький DPA наклав штраф у розмірі 14,5 млн євро за неможливість встановити систему зберігання даних, яка б могла стерти дані, які вже не потрібні для цілей обробки [6].

Наступним важливим документом у досліджуваному напрямі є Директива Європейського парламенту та Ради ЄС «Про захист фізичних осіб щодо обробки персональних даних компетентними органами з метою запобігання, розслідування кримінальних злочинів, ведення розшукових чи судових дій або виконання кримінальних покарань, а також за вільне переміщення таких даних...» № 2016/680, яка дещо відрізняється від Регламенту (вона є актом не прямого застосування та «передбачає її інкорпорацію у правопорядок держав-членів, що реалізується за допомогою прийняття відповідного імплементуючого національного акта») [9].

Як бачимо, подальше удосконалення європейських стандартів та процес наближення України до ЄС потребують оновлення вітчизняного законодавства щодо захисту права на інформацію. У жовтні 2022 року на розгляд Верховної Ради України подано проект Закону України «Про захист персональних даних» № 8153. «Завданням законопроекту є приведення нормативного регулювання України в сфері захисту персональних даних у відповідність до нових міжнародних стандартів в цій сфері, які передбачені Конвенцією про захист фізичних осіб у зв'язку з автоматизованою обробкою персональних даних та Загальним регламентом про

захист персональних даних, а також врегулювати правові відносини, пов'язані з обробкою персональних даних, які не врегульовані чинним законом» [10]. Адже наразі правове регулювання в сфері захисту персональних даних не охоплює цілий ряд питань та правовідносин, які виникають на практиці, що зумовлено значним технологічним розвитком, який суттєво випереджає законодавство.

Крім того, Стратегією інтеграції України до Єдиного цифрового ринку Європейського Союзу («Дорожня карта»), узгодженою з ЄС, визначено, що «законодавче закріплення права на захист персональних даних серед основних прав і свобод фізичних осіб, а також положення про вільний рух персональних даних, приведення у відповідність до права ЄС принципів обробки персональних даних, та термінології має відбутись до грудня 2023 року» [10].

Наступним механізмом у напрямі покращення ефективності захисту інформації в Україні є дієвий контроль з боку незалежного наглядового органу з питань захисту персональних даних, діяльність якого ґрунтуватиметься на дотриманні законодавчих норм з урахуванням кращих міжнародних практик та стандартів, відображених в GDPR. Про це, зокрема, наголошено і у звіті експерта Ради Європи «Повноваження Уповноваженого Верховної Ради України з прав людини та законодавство у сфері доступу до публічної інформації», в якому, зокрема, вказується, що «... найважливішою рекомендацією для України є створення незалежного (спеціального) інституту Інформаційного комісара або комісії, який має бути єдиним органом другої інстанції з розгляду звернень/скарг щодо порушення права на доступ до інформації. З урахуванням того, що стандарти ЄС вимагають від кожної держави-члена створити незалежну установу із захисту даних, наполегливо рекомендується створити єдину незалежну установу, яка матиме подвійні повноваження: забезпечувати реалізацію права на доступ до публічної інформації та захист персональних даних. Як свідчить досвід багатьох сучасних демократичних держав, така модель є найбільш ефективною» [11].

На сьогодні зазначені функції в Україні відносяться до повноважень Уповноваженого Верховної Ради України з прав людини (далі – Уповноважений). Пунктом 7 ст. 3 Закону України «Про Уповноваженого Верховної Ради України з прав людини» передбачено, що метою парламентського контролю, який здійснює Уповноважений, є «сприяння правовій інформованості населення та захист конфіденційної інформації про особу» [12]. Порядок проведення Уповноваженим, його представником та іншими визначеними Уповноваженим службовими особами перевірок додержання законодавства про захист персональних даних визначено Порядком здійснення Уповноваженим Верховної Ради України з прав людини контролю за додержанням законодавства про захист персональних даних [13].

Разом з тим, реалізація ефективного контролю Уповноваженим Верховної Ради України з прав людини, відповідно до норм міжнародних стандартів, неможлива. Адже поєднання функцій контролю з правами, передбаченими мандатом Омбудсмана, впливає на зниження ефективності їх реалізації. Зазначене є також порушенням норм Конвенції Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних та Загального регламенту захисту персональних даних.

Слід зазначити, що у жовтні 2021 року у Верховній Раді України зареєстровано проєкт Закону України «Про Національну комісію з питань захисту персональних даних та доступу до публічної інформації» (№ 6177), яким запропоновано створити Національну комісію з питань захисту персональних даних та доступу до публічної інформації (орган утворюється Кабінетом Міністрів України, якому підзвітний, підконтрольний Верховній Раді України), «... як центрального органу виконавчої влади зі спеціальним статусом, який не лише забезпечить реалізацію державної політики у сфері захисту персональних даних та доступу до публічної інформації, але й державний контроль щодо дотримання законодавства про захист персональних даних та/або доступ до публічної інформації» [14].

Відповідно до норм GDPR, потребує також удосконалення і вітчизняний механізм права на захист інформації «право бути забутим». Право на забуття (англ. right to be forgotten) – право, яке дозволяє особі вимагати, за певних умов, видалення своїх особових даних із загального доступу через пошукові системи, тобто посиляти на ті дані, які, на її думку, можуть завдати їй шкоди [15]. На думку О. Совгіри та Ю. Ремінської, право на забуття – це право, надане фізичним та юридичним особам, яке дозволяє їм впливати на рівень відкритості наявної в Інтернеті інформації щодо себе/своєї діяльності, зокрема, включаючи можливість впливу на рівень індексації такої інформації та видачі пошукових запитів у різних пошукових системах (за ключовими словами) [16]. Разом з тим, як зазначає В. Майер-Шенбергер, однією з основних проблем електронної обробки та зберігання даних є те, що подібним процесам не властиво «забувати», адже така характеристика притаманна виключно людині ... [17].

Першою серед європейських держав концепцію права на забуття було упроваджено у Франції. Серед основних завдань – пояснити користувачам, на які ризики вони наражаються, даючи доступ до своєї персональної інформації в мережі; сприяти захисту даних і запровадженню «права бути забутим» як на національному рівні, так і на рівні ЄС» [18].

На сьогодні право бути забутим або право на видалення інформації закріплене у ст. 17 Загального регламенту ЄС про захист даних від № 679 “Right to erasure (right to be forgotten)” – «право на видалення (право бути забутим)» та доповнене ст. 21 “Right to object” – «право подавати заперечення». Вимоги законодавства про захист персональних даних передбачають видалення посилань на веб-сайти із суперечливою/

недостовірною/неповною інформацією, створеною у результаті пошуку за ключовим словом. Разом з тим, законодавчі положення не стосуються особливостей внутрішнього пошуку в соціальних мережах, виступають в основному своєрідною «боротьбою» з гіперпосиланнями, а не зі змістом самих веб-сайтів.

Слід зазначити, що наразі, «право бути забутим» застосовується лише у межах кордонів держав-членів ЄС. У вересні 2019 року Google виграв судовий процес із Францією перед Судом ЄС (TSUE) в Люксембурзі щодо права бути забутим (позов про видалення інформації зі світової мережі, а не тільки з пошукових систем країн ЄС). Суд ухвалив рішення про те, що «право бути забутим» поширюється лише на версію пошукової системи в державах-членах ЄС, але не за межами ЄС. Зазначена справа не є універсальною, а право на забуття – абсолютним [15].

Варто звернути увагу, що п. 6 ч. 2 ст. 8 Закону України «Про захист персональних даних» передбачено, що суб'єкт персональних даних має право звернутися з мотивованою вимогою на зміну або знищення його персональних даних будь-яким володільцем і контролером персональних даних, якщо ці дані обробляються незаконним шляхом чи є недостовірними [5]. Як бачимо, зміст формулювань Закону та GDPR дещо відрізняються. Проте у жовтні 2022 року на розгляд Верховної Ради України подано проєкт Закону України «Про захист персональних даних» № 8153, який розроблено з урахуванням основних вимог Загального регламенту ЄС про захист даних 2016/679. Даним законопроектом суттєво розширено права суб'єктів персональних даних, а також посилено вимоги до обробки персональних даних володільцями та розпорядниками персональних даних та відповідальність за порушення вимог законодавства у даному напрямі. У контексті досліджуваної тематики п. 2 ч. 4 ст. 17 «Використання технологій відстеження дій суб'єктів персональних даних у електронних комунікаціях та сервісах» законопроекту № 8153 передбачено: «контролери та оператори, які здійснюють обробку персональних даних, передбачених частиною першою цієї статті, повинні забезпечити безумовну автоматизовану можливість внесення суб'єктом персональних даних будь-яких змін до його персональних даних, що обробляються, включаючи їх видалення» [19]. Зважаючи на зазначене, ми дійшли висновку, що «право бути забутим» існує там, де право на приватність обмежує право на свободу вираження поглядів.

Висновки та перспективи. Таким чином, захист прав на доступ до інформації повинен відповідати нормам міжнародних стандартів, а «... обізнаність громадян щодо конфіденційності даних повинна бути піднята на більш високий рівень шляхом введення суворіших покарань у вигляді штрафів, примусового виконання» [6, с. 2–3], а також покращення рівня обізнаності щодо правових засад обробки та захисту персональних даних. Зазначимо, що у кінці 2021 року Уповноваженими з прав людини, спільно з Офісом Ради Європи в Україні та студією онлайн-освіти EdEra, проведено інформаційну кампанію щодо захисту інформаційної безпеки у частині, що стосується права на захист доступу до інформації, за результатами якої створено онлайн-курс «Захист персональних даних», який налічує дві версії: базова та підвищеної складності для державних службовців.

Крім того, Міністерством освіти і науки України (далі – МОН) та Державною науковою установою «Інститут модернізації змісту освіти» (відповідно до вимог спільного наказу МОН та Мінцифри України від 01.12.2021 № 12921/158), з метою упровадження позитивного досвіду у рамках запуску проєкту «EU4DigitalUA» підписано Меморандум про взаєморозуміння з Міжнародним та ібероамериканським фондом адміністративної та державної політики. Це надасть можливість прискорити процес імплементації міжнародних принципів та стандартів щодо захисту права на доступ до інформації в Україні.

Перспективним напрямом подальших наукових розробок є аналіз міжнародного позитивного досвіду та практики ЄСПЛ у контексті вдосконалення правового регулювання права на захисту персональних даних.

Список використаних джерел:

1. Рекомендації Уповноваженого Верховної Ради України з прав людини з питань додержання конституційного права людини і громадянина на доступ до інформації. URL: <https://rm.coe.int/recomendations-final-10-02-21/1680a165f7>.
2. Золотар О. Права людини – від епохи просвітництва до інформаційного суспільства. 2017. № 38/3. С. 7–20.
3. Щорічна доповідь Уповноваженого Верховної Ради України з прав людини. 2021. URL: <https://ombudsman.gov.ua/storage/app/media/uploaded-files/schoricha-dopovid-2021.pdf>.
4. Щорічна доповідь Уповноваженого Верховної Ради України з прав людини. 2022. URL: <https://ombudsman.gov.ua/report-2022/images/documents/annual-report-2022.pdf>.
5. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI. *Відомості Верховної Ради України (ВВР)*. 2010. № 34. Ст. 481. URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text>.
6. Аналіз законодавства про захист персональних даних в Україні: звіт Міністерства трансформації України. 2020. 55 с. С. 10.
7. Загальний регламент із захисту персональних даних № 2018/1725. URL: <http://aphd.ua/gdpr-ofitsiinyi-ukranskyi-pereklad>.
8. Посібник з європейського права у сфері захисту персональних даних. К. : К.І.С., 2020. 432 с.

9. Концептуальні питання директиви ЄС 2016/680. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4014545.

10. Висновок комітету з питань інтеграції України до Європейського Союзу щодо проекту Закону України «Про захист персональних даних». URL: <file:///C:/Users/Admin/Downloads/1562145.pdf>.

11. Повноваження Уповноваженого Верховної Ради з прав людини та законодавство у сфері доступу до публічної інформації. Аналіз законодавства та рекомендації: звіт. URL: <chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://rm.coe.int/report-access-to-public-information-ukr/1680992d5b>.

12. Про Уповноваженого Верховної Ради України з прав людини» : Закон України від 23.12.1997 № 776/97-ВР (у редакції від 31.01.2023) URL: <https://zakon.rada.gov.ua/laws/show/776/97-%D0%B2%D1%80>.

13. Порядок здійснення Уповноваженим Верховної Ради України з прав людини контролю за додержанням законодавства про захист персональних даних: наказ Уповноваженого ВРУ з прав людини «Про затвердження документів у сфері захисту персональних даних» від 08.01.2014 № 1/2-14. URL: https://zakon.rada.gov.ua/laws/show/v1_02715-14#Text.

14. Про Національну комісію з питань захисту персональних даних та доступу до публічної інформації: пояснювальна записка до проекту Закону України № 6177. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=72992.

15. Андрощук Г. Суд ЄС: Google виграв спір щодо права на забуття. URL: <https://yur-gazeta.com/publications/practice/zahist-intelektualnoyi-vlasnosti-avtorske-pravo/sud-es-google-vigrav-spir-shchodo-prava-na-zabuttya.html>.

16. Совгіря О., Ремінська Ю. Право на забуття: міркування з точки зору конституційно-правової «матерії». *Український часопис конституційного права*. 2021. № 3. С. 27.

17. Sofone I.N. The right to be forgotten a Canadian and comparative perspective. Routledge, Taylor & Francis Group, 2020. 130 p.

18. Гордієнко Т. «Право на забуття» – що це таке й чому про нього варто знати? URL: <https://ms.detector.media/trends/1411978127>.

19. Про захист персональних даних: проект Закону України № 8153 від 25.10.2022. URL: <https://itd.rada.gov.ua/billInfo/Bills/pubFile/1517426>.