ПОНОМАРЕНКО І. С.,
аспірант відділу аспірантури
і докторантури
*(Національна академія
Служби безпеки України)*

УДК 342.7
DOI https://doi.org/10.32842/2078-3736/2020.6.2.2.18

ПРАВОВЕ РЕГУЛЮВАННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У МЕДИЧНІЙ СФЕРІ: ВІТЧИЗНЯНИЙ ТА МІЖНАРОДНИЙ ДОСВІД

У статті проаналізовано вітчизняне та міжнародне нормативно-правове регулювання захисту «чутливих» даних із метою вдосконалення системи національного законодавства у сфері охорони здоров'я. Констатовано, що як вітчизняне, так і міжнародне законодавство у виключних випадках дозволяє опрацьовувати персональні дані осіб без їх згоди, однак особливістю міжнародного законодавства є те, що держава гарантує їх інформаційний захист. З'ясовано, що обмін персональними даними про здоров'я між постачальниками медичних послуг, інформаційними мережами охорони здоров'я, медичними працівниками та пацієнтами ускладнюється проблемою як технічного, так і правового захисту так званих «чутливих» персональних даних, що мають підвищені вимоги щодо захисту згідно з відповідними законами. Проблемним питанням залишається рівень обізнаності громадян, адже досить часто вони просто ігнорують проблеми, пов'язані із захистом власних персональних даних, у тому числі через неповне розуміння законодавчих стандартів та вимог у цій сфері. Окреслено неоднозначність трактування Закону України № 555-IX «Про внесення змін до Закону України «Про захист населення від інфекційних хвороб» щодо запобігання поширенню коронавірусної хвороби (COVID-19)», надано пропозиції щодо конкретизації мети та кола суб'єктів, чиї персональні дані будуть оброблятися. Проаналізовано епохальний документ у напрямі захисту персональних даних – Загальний регламент із захисту персональних даних (General Data Protection Regulation). Акцентовано увагу на тому, що захист персональних даних є не просто обов'язком держави та предметом державно-правового регулювання, його необхідно розглядати у поєднанні із захистом прав людини. Надано пропозиції щодо внесення змін у вітчизняне законодавство про захист персональних даних з метою приведення його у відповідність до Регламенту (ЄС) 2018/1725.

Ключові слова: *персональні дані, захист інформації, медична сфера, норми вітчизняного та міжнародного законодавства, цифровізація, відповідальність.*

Ponomarenko I. S. Legal regulation of personal data protection in the medical field: domestic and international experience

It is stated that both domestic and international legislation in exceptional cases allows the processing of personal data of persons without their consent, but the peculiarity of international legislation is that the state guarantees their information protection. It was found that the exchange of personal health data between health care providers, health information networks, medical professionals and patients is complicated by the problem of both technical and legal protection of so-called "sensitive" personal data, which has increased protection requirements under the relevant laws. The level

of awareness of citizens remains a problematic issue, because quite often they simply ignore the problems associated with the protection of their own personal data, including due to an incomplete understanding of legislative standards and requirements in this area. The ambiguity of the interpretation of the law of Ukraine No. 555-IX "on amendments to the law of Ukraine "on protection of the population from infectious diseases" on preventing the spread of coronavirus disease (COVID-19)" is outlined, proposals are made to specify the purpose and range of subjects whose personal data will be processed. The article analyzes an epochal document in the field of personal data protection – the General Data Protection Regulation. Attention is drawn to the fact that the protection of personal data is not just an obligation of the state and the subject of State Legal Regulation, it should be considered in conjunction with the protection of human rights. Proposals are made to amend the domestic legislation on personal data protection in order to bring it into compliance with regulation (EU) 2018/1725.

Key words: *personal data, Information Protection, medical sphere, norms of domestic and international legislation, digitalization, responsibility.*

Є речі, для яких лікар має вуха, але рота не має.
О. Герцен

Вступ. Розвиток інформаційного суспільства нерозривно пов'язаний як із розвитком інформаційних технологій, так і з розширенням прав людини. Одним із проявів цього є розроблення відповідної системи захисту персональних даних під час їх автоматизованої обробки. Захист персональних даних є не просто обов'язком держави і предметом державно-правового регулювання, його необхідно розглядати в поєднанні із захистом прав людини, тим більше що створення належної системи захисту персональних даних передбачено міжнародними зобов'язаннями України.

Сфера охорони здоров'я не є винятком, адже зараз все більше закладів охорони здоров'я для поліпшення ефективності діяльності застосовують інформаційно-комунікаційні технології. Цифрові технології охоплюють цілу низку електронних або цифрових процесів діагностики, моніторингу та лікування. Лікувально-профілактичні установи створили різні платформи в Інтернеті для забезпечення процесів, пов'язаних з охороною здоров'я. На базі цих платформ, як правило, можна створювати і зберігати індивідуальні електронні медичні записи. Крім того, сформовані особисті дані про здоров'я можуть бути використані для медичних досліджень і прогнозування стану здоров'я людей. Однак, на жаль, обмін персональними даними про здоров'я між надавачами медичних послуг, інформаційними мережами охорони здоров'я, медичними працівниками та пацієнтами ускладнюється проблемою як технічного, так і правового захисту так званих «чутливих персональних даних, що мають підвищені вимоги щодо захисту згідно з відповідними законами. Залишається також проблемним питанням рівень обізнаності громадян, адже досить часто вони просто ігнорують проблеми, пов'язані із захистом власних персональних даних, у тому числі через неповне розуміння законодавчих стандартів і вимог у цій сфері.

Питання щодо захисту персональних даних, порядку обробки персональних даних у сфері охорони здоров’я, відповідальності за порушення законодавства у вказаній сфері у своїх наукових працях досліджували як вітчизняні, так і зарубіжні вчені, такі як: А.А. Баранов, З.С. Гладун, М.Г. Гончаров, О.С. Каретник, Н.В. Коробцова, Д.В. Ланде, І.Ф. Літвінова, Р.А. Майданик, В.П. Радкевич, І.Я. Сенюта, О.Д. Сидєльников, Р.О. Стефанчук, С.Г. Стеценко,Т.М. Ямненко та інші. Проте їхні висновки у зв’язку із останніми законодавчими змінами частково втратили актуальність, що і зумовило вибір теми дослідження.

Постановка завдання. Метою статті є аналіз вітчизняного та міжнародного нормативно-правового регулювання захисту «чутливих» даних з метою вдосконалення системи національного законодавства у сфері охорони здоров’я.

Результати дослідження. Право на здоров'я має комплексний характер і включає: право на інформацію та конфіденційність інформації про стан здоров'я; право на медико-соціальну допомогу; право на згоду на лікування та медичне втручання; право на сприятливе екологічне середовище, яке впливає на стан здоров'я, тощо. Статтею 32 Конституції України передбачено: «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» [1]. Відповідно до 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, встановлених законом» [2]. Особливі вимоги до обробки чутливих даних передбачає ст. 7 Закону України «Про захист персональних даних», зокрема ч. 1 «забороняється обробка персональних даних про расове або етнічне походження, а також даних, що стосуються здоров'я, статевого життя, біометричних або генетичних даних». Положення частини першої цієї статті не застосовується, якщо обробка персональних даних: здійснюється за умови надання суб'єктом персональних даних однозначної згоди на обробку таких даних (п. 1 ч. 2); необхідна в цілях охорони здоров'я (п. 6 ч. 2) [3]. Відповідно до ч. 3, 4 ст. 6 Закону України «Про психіатричну допомогу» допускається передача відомостей про стан психічного здоров'я особи і про надання їй психіатричної допомоги без згоди особи або без згоди її законного представника для організації надання особі, яка страждає на тяжкий психічний розлад, психіатричної допомоги або провадження досудового розслідування, складання досудової доповіді щодо обвинувачених або судового розгляду за письмовим запитом слідчого, прокурора, суду та представника уповноваженого органу з питань пробації [4]. Частиною 2 ст. 26 Закону України «Про захист населення від інфекційних хвороб» передбачено, що відомості про зараження особи інфекційною хворобою, що передається статевим шляхом, проведені медичні огляди та обстеження з цього приводу, дані інтимного характеру, отримані у зв'язку з виконанням професійних обов'язків посадовими особами та медичними працівниками закладів охорони здоров'я, становлять лікарську таємницю. Надання таких відомостей дозволяється у випадках, передбачених законами України [5]. «Медичні працівники та інші особи, яким у зв'язку із виконанням професійних або службових обов'язків стало відомо про хворобу, медичне обстеження, огляд та їх результати, інтимну і сімейну сторони життя громадянина, не мають права розголошувати ці відомості, крім передбачених законодавчими актами випадків» (ч. 1 ст. 40 Основ законодавства про охорону здоров'я) [6].

Окремої уваги заслуговує прийнятий 13 квітня 2020 року Закон України № 555-IX «Про внесення змін до Закону України «Про захист населення від інфекційних хвороб» щодо запобігання поширенню коронавірусної хвороби (COVID-19)», пп.1 п.2 розділу II якого на період встановлення карантину або обмежувальних заходів, пов'язаних із поширенням коронавірусної хвороби (COVID-19), та протягом 30 днів з дня його відміни «дозволяється обробка персональних даних без згоди особи, зокрема даних, що стосуються стану здоров'я, місця госпіталізації або самоізоляції, прізвища, імені, по батькові, дати народження, місця проживання, роботи (навчання), з метою протидії поширенню коронавірусної хвороби (COVID-19), у порядку, визначеному в рішенні про встановлення карантину, за умови використання таких даних виключно з метою здійснення протиепідемічних заходів» [7]. Після закінчення періоду встановлення карантину така інформація упродовж 30 днів підлягає знеособленню, а у разі неможливості – знищенню. Як бачимо, формулювання закону досить неоднозначне, оскільки визначення мети обробки персональних даних як протидії поширенню коронавірусної хвороби (COVID-19) та можливість їх використання виключно з метою здійснення протиепідемічних заходів – дуже широке за своїм змістом поняття. Воно може довільно трактуватись органами державної влади, підприємствами, установами, організаціями, які надають медичну допомогу. Закон мав би містити більш конкретизоване визначення мети та кола суб'єктів, чиї персональні дані будуть оброблятися.

Таким чином, незважаючи на те, що обробка персональних даних без надання згоди межує з порушенням фундаментальних прав та свобод людини, вітчизняне законодавство дозволяє обробку персональних даних у виняткових випадках.

Проте, на жаль, зважаючи на рівень як законодавчого, так і технічного захисту інформації, ніхто не може гарантувати її належний захист. Так, наприклад, 08.12.2020 видання «Readovka» повідомило, що у відкритому доступі в Інтернеті виявилися персональні дані москвичів, інфікованих коронавірусом у квітні-травні 2020 року. За результатами перевірки в архіві виявлено понад 105 тисяч записів (повні імена хворих, номери телефонів, супутні діагнози і результати перевірок дотримання карантину). На думку керівника компанії «Інтернет-розшук» І. Бедерова, «найбільш вірогідною є версія, що списки хворих формувались у Excel у медичних закладах, а потім пересилались у мерію чи Міністерство охорони здоров'я. Таблиці могли «гуляти» по міністерствах, відомствах у вигляді посилань на Google Drive, де їх і виявили. Версія підтверджується також тим, що «хмарних» таблиць, які містять відомості про хворих, було декілька» [8].

Перейдемо до аналізу основних норм міжнародного законодавства. Так, Концепцією про захист прав людини й основоположних свобод 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, у тому числі для захисту прав і свобод інших осіб [9]. Відповідно до Конвенції про захист осіб у зв'язку із автоматизованою обробкою персональних даних «персональні дані, які свідчать про расову приналежність, політичні, релігійні чи інші переконання, а також дані, що стосуються здоров'я та статевого життя, не можуть піддаватися автоматизованій обробці, якщо внутрішнє законодавство не забезпечує відповідних гарантій» [10]. Директивою Європейського Парламенту і Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» (ст. 8) передбачено: «Держави-члени забороняють обробку персональних даних, що вказують на расове чи етнічне походження, обробку даних, що стосуються здоров'я чи статевого життя людини», окрім випадків, коли «обробка необхідна для захисту життєво важливих інтересів суб'єкта даних чи іншої особи, якщо суб'єкт даних не може дати свою згоду через свою недієздатність чи неправоздатність; якщо обробка даних необхідна з метою профілактичної медицини, медичної діагностики, надання медичних послуг чи лікування або для керування служб охорони здоров'я, і якщо ці дані обробляються медичним працівником, що зв'язаний зобов'язанням збереження професійної таємниці» [11]. Загальним регламентом 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» передбачено, що персональні дані, які за своєю специфікою є особливо чутливими щодо фундаментальних прав і свобод, потребують особливого захисту, оскільки контекст їхнього опрацювання може створити істотні ризики для фундаментальних прав і свобод. Цим документом також передбачено, що опрацювання спеціальних категорій персональних даних може бути необхідним у цілях суспільних інтересів у галузях охорони здоров'я без згоди об'єкта даних [12].

Таким чином, міжнародне законодавство, як і вітчизняне, у виключних випадках дозволяє опрацьовувати персональні дані осіб без їх згоди, однак особливістю міжнародного законодавства є те, що держава гарантує їх інформаційний захист. Незважаючи на значущість зазначених вище міжнародних положень про захист персональних даних пацієнтів, які досить важливі для забезпечення особі її права, на жаль, на практиці вони не завжди належним чином реалізуються. Так, наприклад, знаковою для науковців стала справа «Gillberg v. Sweden» [13]. Вчений Крістофер Гілберг досліджував дитячу психіатрію в Гетеборзькому університеті. Два інших науковці звернулися до нього із проханням надати їм окремі документи цього дослідження. Гетеборзький університет як розпорядник зазначеної інформації відмовив у її наданні, проте запитувачі звернулися до суду й отримали рішення, яким їм було дозволено отримати потрібні документи на певних умовах секретності. Гілберг та університет знову відмовили запитувачам і знищили документи, пов'язані із дослідже-

ням. За це вченого, його колег і віце-президента університету було піддано кримінальному покаранню. Крістофер Гілберг звернувся до Європейського суду із заявою про порушення його прав за статтями 8 (право на повагу до приватного життя) та 10 Конвенції. Він стверджував, що стаття 10 передбачає разом із позитивними правами передавати та одержувати інформацію також і негативне право не надавати відомості, які він не хоче поширювати. Справу у 2010 році розглянула палата суддів, а у 2012 її переглянула Велика палата Європейського суду з прав людини (ЄСПЛ). У фінальному рішенні Європейського суду припущення заявника щодо такого негативного права було спростоване. За законодавством Швеції університет є публічною установою, його працівники – посадовими особами університету, а інформація, якою розпоряджається такий навчальний заклад, має статус публічної. У розглянутій ситуації посадова особа університету відмовилася надати інформацію третім особам, К. та Е., всупереч рішенням національних судів. ЄСПЛ зауважив, що такі дії професора перешкоджали вільному обміну думками та ідеями щодо проведеного дослідження. І навпаки, Європейський суд вказав, що визнання позиції професора Гілберга «становило б зазіхання на права К. та Е. за статтею 10 отримувати інформацію шляхом доступу до запитаних публічних документів» [14]. Таким чином, відбулася зміна в розумінні позиції Європейського суду, що повинно визначати також і підходи у національних судових установах.

Проривом у напрямі захисту персональних даних став прийнятий у травні 2018 року Загальний регламент із захисту персональних даних (General Data Protection Regulation – GDPR). 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 секторів; однак для інформації, що стосується здоров'я, визначені деякі винятки, спрямовані на захист прав суб'єктів даних та конфіденційності їх персональних даних. GDPR трактує дані про здоров'я як «особливу категорію» персональних даних, які за своєю природою вважаються «чутливими», і встановлює вищий рівень захисту їхньої обробки: «особисті дані, які за своєю природою є особливо «чутливими», оскільки контекст їх обробки може створювати значні ризики для основних прав і свобод, заслуговують на особливий захист». GDPR передбачає фундаментальні зміни щодо контролю та володіння даними про здоров'я – вони переходять від лікарів, науковців, лікарень та закладів охорони здоров'я до пацієнтів. Тепер пацієнти повинні надати згоду на використання своїх даних про стан здоров'я та можуть відкликати її, коли це необхідно. Таким чином, порівняно з попередніми нормативними актами щодо захисту даних про здоров'я GDPR приділяє набагато більше уваги задоволенню нових вимог, що виникли з підвищенням рівня цифровізації у сфері охорони здоров'я, і, отже, може сприяти посиленню захисту даних про здоров'я в ЄС.

GDPR вперше дає більш детальне визначення поняття «дані, що стосуються здоров'я», посилаючись на особисті дані, пов'язані з фізичним або психічним здоров'ям фізичної особи, включаючи всі дані про стан її здоров'я в минулому, теперішньому або майбутньому, зібрані під час реєстрації або надання медичних послуг. Він встановлює нові стандарти захисту даних, що стосуються здоров'я, і посилює обов'язки контролерів та процесорів, що обробляють дані в галузі охорони здоров'я. У цьому контексті слід пояснити, що контролером даних є організація, відповідальна за збір та управління ними. Наприклад, лікарня, яка збирає інформацію, – це контролер. Процесор (обробник) даних – це організація, яка допомагає у наданні послуги з обробки даних. Власник програмного продукту, в якому зберігаються та обробляються дані, – процесор (обробник) даних. GDPR встановлює вищі стандарти стосовно інформованої згоди та обов'язків щодо повідомлення (ст. 7), посилює захист права на доступ до персональних даних про здоров'я. Заслуговує на увагу і те, що у разі витоку персональних даних (ст. 33, 34) контролери даних інформують контролюючий орган протягом 72 год., а у разі порушення безпеки даних вони повинні інформувати пацієнтів.

GDPR розширює і права пацієнтів – вони можуть вимагати від контролерів та процесорів даних видалення інформації про стан їхнього здоров'я. Крім того, найвищий рівень конфіденційності, за замовчуванням, має тепер автоматично застосовуватися до нового сервісного продукту для здоров'я. У разі недотримання GDPR організаціям охорони здоров'я

загрожуватимуть санкції. Суттєво збільшено адміністративні штрафи – до 2% від загального річного доходу закладу або 10 млн євро у разі незначних порушень, а також до 4% від загального річного доходу або 20 млн євро у разі серйозних порушень (ст. 83) [15]. 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 і того, як вони захищені. Крім того, Директивою Європейського Парламенту і Ради ЄС «Про заходи для високого рівня безпеки мережевих та інформаційних систем на території Союзу» також передбачено повноваження контролюючим органам здійснювати аудит операторів життєво важливих послуг. Операторами у медичній сфері визначено постачальників медичних послуг – медичні заклади [16].

Українська влада вирішила впровадити Загальний регламент із захисту персональних даних (GDPR) і визначила відповідне завдання у Плані заходів з виконання Угоди про асоціацію, а саме удосконалення законодавства про захист персональних даних з метою приведення його у відповідність із Регламентом (ЄС) 2018/1725. У листопаді 2019 року при Секретаріаті Уповноваженого Верховної Ради України з прав людини було 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.

Крім того, у 2020 році міжвідомчою робочою групою при Уповноваженому Верховної Ради України з прав людини з метою деталізації форм надання згоди на обробку персональних даних та надання можливості органам державної влади і місцевого самоврядування обробляти персональні дані на підставі їх повноважень, а також імплементації міжнародних стандартів у сфері захисту персональних даних, передбачених у Загальному Регламенті Європейського Парламенту і Ради (ЄС) 2016/679, розроблено та подано на розгляд Парламенту 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 № 2671-1. Проте 04.03.2020 зазначений вище проєкт повернуто на доопрацювання.

Висновки. Підсумовуючи, ми дійшли висновку, що, незважаючи на певні позитивні зміни у напрямі захисту персональних даних у сфері охорони здоров'я, необхідно внести зміни у вітчизняне законодавство про захист персональних даних із метою приведення його у відповідність до Загального Регламенту Європейського Парламенту і Ради (ЄС) 2016/679 та Регламенту (ЄС) 2018/1725, зокрема необхідно: створити спеціальний незалежний наглядовий орган за дотриманням законодавства у сфері захисту персональних даних (нині функції наглядового органу у сфері захисту персональних даних здійснює Уповноважений Верховної Ради України з прав людини, проте такий контроль не притаманний його конституційно-правовому статусу), повноваження якого повинні відповідати вимогам, передбаченим Загальним Регламентом Європейського Парламенту і Ради (ЄС) 2016/679; зобов'язати медичні заклади отримувати чітку згоду користувачів на обробку даних; передбачити у медичних закладах відповідальних за захист персональних даних, а також забезпечити безпеку персональних даних (кодування); надати користувачу право «стирання» даних, якщо у них немає необхідності; надати регулятору повноваження штрафувати компанії за порушення.

Перспективи подальших наукових розвідок, на наш погляд, полягають у подальшому науковому дослідженні питань, що стосуються аналізу міжнародного досвіду у контексті удосконалення адміністративного законодавства та адміністративної відповідальності у сфері захисту інформації персонального характеру в Україні.

Список використаних джерел:

1. Конституція України від 28 червня 1996 року. *Відомості Верховної Ради України.* 1996. № 30. Ст. 141.

2. Про інформацію: Закон України від 02.10.1992 № 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.

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

4. Про психіатричну допомогу: Закон України від 22.02.2000 № 1489-III (у редакції від 20.12.2018). *Відомості Верховної Ради України* (ВВР). 2000. № 19. Ст. 143. URL: https://zakon.rada.gov.ua/laws/show/1489-14#Text.

5. Про захист населення від інфекційних хвороб: Закон України від 06.04.2000 № 1645-III (у редакції від 23.05.2020). *Відомості Верховної Ради України* (ВВР). 2000. № 29. Ст. 228. URL: https://zakon.rada.gov.ua/laws/show/1645-14#Text.

6. Основи законодавства про охорону здоров'я: Закон України від 19.11.1992 № 2801-XII. URL: http://zakon.rada.gov.ua/laws/show/2801-12.

7. 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 № 555-IX. *Відомості Верховної Ради України* (ВВР). 2020. № 19. Ст. 127. URL: https://zakon.rada.gov.ua/laws/show/555-20#Text.

8. «Человеческий фактор» и стыд. В сети появились личные данные москвичей, инфицированных коронавирусом. URL: https://www.currenttime.tv/a/koronavirus-utechka-moskva/30992104.html.

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

10. Конвенція про захист осіб у зв'язку із автоматизованою обробкою персональних даних від 28.01.1981. URL: https://zakon.rada.gov.ua/laws/show/994_326#Text.

11. Директива Європейського Парламенту і Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» від 24.10.1995 № 95/46/ЄС. URL: https://zakon.rada.gov.ua/laws/show/994_242#Text.

12. Загальний регламент 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» від 27.04.2016 № 2016/679. URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text.

13. Рішення Великої палати ЄСПЛ у справі «Gillberg v. Sweden» від 03.04.2012 § 82-97. URL: https://cedem.org.ua/articles/pravo-na-dostup-do-informatsiyi-evolyutsiya-pidhodiv-yevropejskogo-sudu-z-prav-lyudyny.

14. Рішення ЄСПЛ у справі «Gillberg v. Sweden» від 02.11.2010 §120-127. URL: https://zakonbase.ru/content/base/186728/?print=1.

15. Загальний регламент із захисту персональних даних № 2018/1725. URL: http://aphd.ua/gdpr-ofitsiinyi-ukranskyi-pereklad.

16. Директива Європейського Парламенту і Ради ЄС «Про заходи для високого рівня безпеки мережевих та інформаційних систем на території Союзу» від 06.07.2016 № 2016/1148. URL: https://zakon.rada.gov.ua/laws/show/984_013-16#Text.