УДК: 342.7:004.056.5/.6
DOI https://doi.org/10.24144/2307-3322.2023.80.1.63

ПРАВА СУБ'ЄКТІВ ПЕРСОНАЛЬНИХ ДАНИХ ЯК СКЛАДОВА ІНФОРМАЦІЙНИХ ПРАВ ЛЮДИНИ

Бочкова І.І.,
кандидат юридичних наук,
старший викладач кафедри патентознавства та основ правозастосовної діяльності
Харківського національного університету міського господарства
імені О.М. Бекетова
ORCID: 0000-0003-0522-2908
e-mail: inga.bochkova@gmail.com

Врублевська-Місюна К.М.,
кандидат юридичних наук,
доцент кафедри патентознавства та основ правозастосовної діяльності
Харківського національного університету міського господарства
імені О.М. Бекетова
ORCID: 0000-0002-6973-3945
e-mail: vkatrin21@gmail.com

Бочкова І.І., **Врублевська-Місюна К.М. Права суб'єктів персональних даних як складова інформаційних прав людини.**

Україна в преамбулі Конституції проголосила курс на євроінтеграцію, яка, зокрема, передбачає і співробітництва в галузі захисту інформаційних прав людини – захисту персональних даних на умовах наближення національного законодавства до найсуворіших регламентів ЄС. Стаття аналізує поняття інформаційних прав людини у контексті правової держави, особливо в період цифрової трансформації. Основна увага зосереджена на реальному забезпеченні прав і свобод громадян, зокрема інформаційних прав. Стаття містить аналіз стану дослідження в науці проблематики інформаційного права, зокрема понять «інформаційні права», «права на інформацію», «інформаційні свободи», а також підходів до розуміння інформаційних прав з позицій різних галузей права. Автори дійшли висновку про наявність розробок змісту відповідних категорій, але відсутність дослідження самих прав суб'єктів даних. У статті розглядається зміст інформаційних прав людини як складової правового статусу особи в державі на прикладі правового регулювання захисту прав суб'єктів персональних даних в українському законодавстві і в правових приписах Європейського Союзу. При порівнянні змісту правових підходів у регулюванні спільних ідей за наявності схожих лексичних конструкцій виявляються відмінності саме у «дусі» правового регулювання: європейський підхід характеризується антропоцентричністю, інтереси людини є пріорітетом регулювання, підставами для реалізації багатьох прав суб'єктів даних є їх воля, на відміну від національного законодавства, депідставою для виникнення і реалізації одних прав суб'єктів персональних даних є факти порушення інших прав цих суб'єктів.

Стаття містить аналіз існуючих категорій в сфері інформаційних прав, детально розглядається зміст елементів поняття «персональні дані», зокрема понять: «ідентифікація людини», «ідентифікатори в реальному житті» та «ідентифікатори в цифровому просторі». Проведене дослідження дозволяє припустити, що трансформація українського законодавства в сфері захисту персональних даних ще триває, що відкриває шлях для подальших досліджень в цій області.

Ключові слова: інформація, персональні дані, ідентифікація. ідентифікатори, володілець даних, розпорядник даних, суб'єкт даних.

Bochkova I.I., **Vrublevska-Misyuna K.M. Rights of personal data subjects as a component of information human rights.**

In the preamble to the Constitution, Ukraine proclaimed its course towards European integration, which, in particular, includes cooperation in the field of information human rights protection - protection of personal

data on the basis of approximation of national legislation to the strictest EU regulations.The article analyzes the concept of information human rights in the context of the rule of law, especially in the period of digital transformation. The main focus is on the actual enforcement of citizens' rights and freedoms, including information rights. The article analyzes the state of research in the field of information law, in particular, the concepts of "information rights", "rights to information", "information freedoms", as well as approaches to understanding information rights from the standpoint of various branches of law. The authors come to the conclusion that there are studies of the content of the relevant categories, but there is no study of the rights of data subjects themselves. The article examines the content of human information rights as a component of the legal status of a person in the State on the example of legal regulation of protection of the rights of personal data subjects in Ukrainian legislation and in the legal provisions of the European Union. When comparing the content of legal approaches to the regulation of common ideas in the presence of similar lexical constructions, the differences are revealed in the "spirit" of legal regulation: the European approach is characterized by anthropocentricity, human interests are the priority of regulation, and the grounds for exercising many of the rights of data subjects are their will, unlike national legislation, where the grounds for the emergence and exercise of some rights of personal data subjects are the facts of violation of other rights of these subjects.

The article contains an analysis of the existing categories in the field of information rights, and provides a detailed analysis of the content of the elements of the concept of "personal data", in particular, the concepts of: "human identification", "identifiers in real life" and "identifiers in digital space". The study suggests that the transformation of Ukrainian legislation in the field of personal data protection is still ongoing, which opens the way for further research in this area.

Key words: information, personal data, identification, identifiers, data controller, data processor, subject of personal data.

Постановка проблеми. Основною підставою для розмежування правової держави і неправової є реальне забезпечення прав і свобод людини і громадянина. У вік цифрової трансформації особливого значення з точки зору забезпечення стану дотримання свобод людини набувають саме інформаційні права. Право на інформацію, інформаційна безпека, кібербезпека, захист від безпідставної та незаконної обробки даних – це ті поняття і категорії, що вимагають їх розроблення, визначення механізмів забезпечення та встановлення способів захисту. Задля того, щоб розроблені механізми гарантували належний рівень свобод, необхідно, щоб зміст прав суб'єкта даних був достатньо широким, повним і всеохоплюючим. Тому вбачається актуальним і важливим визначити зміст тих інформаційних прав, що закріплені в українському законодавстві, проаналізувати зміст аналогічних приписів у праві ЄС і встановити той дух права, до якого прагнув український законодавець, зближуючі правове регулювання цих двох систем.

Стан опрацювання цієї проблематики. Дослідженню правової природи понять «інформаційні права і свободи громадян» присвячена достатня кількість праць цивілістів, конституціоналістів та науковців, що розроблюють поняття інформаційного права: І. Арістової, О. Баранова, І. Бачило, К. Бєлякова, В. Брижка, В. Бутузова, В. Гавловського, О. Гаврилова, Ю. Гелич, К. Калюжного, Р. Калюжного, Б. Кормича, Т. Костецької, О. Кохановської, В. Ліпкана, А. Марущака, О. Олійника, Є. Петрова, А. Тадеєва, Н. Ткачук.

Зазначені вчені провели ретельний аналіз змісту понять «інформаційні права», «права на інформацію»,«інформаційні свободи», надали класифікацію інформаційних прав людини, провели порівняння обсягів зазначених понять в національному і європейському законодавстві, проте зазначені науковці прагнули до аналізу змісту категорій, тоді як дослідження самих прав суб'єктів даних в науці майже не проводилось.

Відтак **метою** цієї праці бачимо необхідність проаналізувати актуальний підхід національного законодавця до розуміння свободи реалізації інформаційних прав громадянином та можливостей, наданих володільцям, розпорядникам та суб'єктам інформації в процесі реалізації громадянами своїх інформаційних прав.

Виклад основної частини: Поняття «інформаційні права людини» є досить спірним серед науковців через свій обсяг. Деякі вчені наголошують на тому, що «інформаційні права» належать до прав четвертого покоління, є новим явищем, пов'язаним з процесами цифрової трансформації суспільства в останні 20-30 років, і обумовлені виникненням нових об'єктів – цифрових продуктів, інформаційних мереж, тощо [1, с. 17]. Інші ж вчені доводять (П.М. Сухорольський, В.А. Ліпкан), що інформаційні

права як складова громадянських прав на свободу думки, слова, друку відомі ще творцям Французької декларації прав людини і належать до першого покоління прав [2, с. 155; 3]. Погодимось з науковцями, які зазначають про існування не тотожних понять «право на інформацію» та «інформаційні права» (В.А. Ліпкан, К.Р. Калюжний, Л. Вакарюк): поняття «інформаційні права людини» є ширшим поняттям, оскільки охоплює не лише можливість «вільно збирати, зберігати, використовувати і поширювати інформацію будь-яким способом, на свій вибір», а й усі права і свободи людини, що мають інформаційний характер [2, с. 156]. І до таких прав в найширшому розумінні відносимо закріплені в статтях 32, 34, 50 та інших статтях Конституції України права на невтручання в особисте життя, на свободу думки і слова, на інформацію про навколишнє середовище, на освіту та інші, що виникають в екологічній, економічній, фінансовій, політичній та інших сферах людського буття, які поєднані між собою і в своїй інтегративній сукупності становлять систему інформаційних прав і свобод. У цій концепції інформаційні права та право на інформацію співвідносяться між собою як загальне і часткове. Інформаційні права мають міжгалузевий характер та є в будь-якій сфері життєдіяльності суспільства [2, с. 158].

Відштовхуючись від такого підходу до розуміння інформаційних прав проведемо дослідження, спрямоване не аналіз порядку реалізації певних видів інформаційних прав, що відносно нещодавно почали отримувати специфічного правового регулювання (право на доступ до публічної інформації, право на захист персональних даних, право на «забуття» та інші).

В Законі України «Про інформацію» встановлено два режими доступу до інформації відкритий та обмежений [6]. Задекларовано вимогу, відповідно до якої інформація вважається відкритою, якщо інше не встановлено законом. Інформацією з обмеженим доступом є конфіденційна, таємна та службова інформація. З точки зору мети нашого дослідження, вбачаємо важливим проаналізувати інформаційні права людини, пов'язані з конфіденційної інформацією, тобто з інформацією, що може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, визначених законом. Конфіденційною є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень. Відповідно до положень пункту другого ст. 5 ЗУ «Про захист персональних даних» персональні дані можуть бути віднесені до конфіденційної інформації про особу законом або відповідною особою [7].

Визначення персональних даних в українському законодавстві міститься у ЗУ «Про захист персональних даних», відповідно до якого «персональні дані – відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована». При цьому поняття ідентифікації у зазначеному законі відсутнє. У ст. 3 Закону України «Про Єдиний державний демографічний реєстр та документ, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус» під «ідентифікацією» особи розуміється «встановлення особи шляхом порівняння наданих даних (параметрів), у тому числі біометричних, з наявною інформацією про особу в реєстрах, картотеках, базах даних тощо»; під «біометричними даними – сукупність даних про особу, зібраних на основі фіксації її характеристик, що мають достатню стабільність та істотно відрізняються від аналогічних параметрів інших осіб (біометричні дані, параметри – відцифрований підпис особи, відцифрований образ обличчя особи, відцифровані відбитки пальців рук)»; «ідентифікувати – здійснювати комплекс заходів, що дає змогу виконувати пошук за принципом «один до багатьох», зіставляючи дані (параметри) особи, у тому числі біометричні, з інформацією Реєстру» [5].

Отже, хоча і прямо не зазначено, які дані можуть бути визначені як ідентифікатори фізичної особи, проте з аналізу зазначених положень можна зробити висновок, що ідентифікаторами будуть відомості, які є в Реєстрі, з якими і буде проводитись зіставлення, і до яких, відповідно статті 7 зазначеного Закону належить інформація про ім'я особи, дату народження/смерті, місце народження, стать, дату внесення інформації про особу до Реєстру, відцифровані зразок підпису, образ обличчя, відбитки пальців рук особи, додаткова змінна інформація про народження дітей, про шлюб і розірвання та інша інформація як змістовного, так і організаційного характеру, визначена в цій статті.

Зазначені відомості можемо умовно назвати «ідентифікаторами» фізичної особи, тобто тими даними, які допоможуть встановити її особистість. Перелік таких ідентифікаторів не може бути виключний, тому що в будь-якому разі ідентифікувати людину можливо за будь-якими ознаками, які з огляду на умови, що склались, зможуть підтвердити відповідність між зразком, відібраним від певної визначеної людини, і зразком, що надається для порівняння (зразок почерку, голос, постава, медичні

дані тощо). Такої ж позиції дійшов і Конституційний суд України у своєму Рішенні [8], де зазначив, що перелік даних про особу, які визнаються як конфіденційна інформація, не є вичерпним.

Окремої уваги треба приділити поняттю ідентифікації людини в цифровому просторі, оскільки саме це середовище наразі є платформою і способом для вчинення юридично значущих дій, зокрема й реалізації своїх прав, а отже і потребує рівнозначного захисту. При цьому цифрове середовище якісно істотно відрізняється від реального буття людини. В українському законодавстві нами не знайдено вказівок на поняття інтернет – ідентифікаторів чи чогось схожого, проте у Регламенті Ради Європи 2016-769 (General Data Protection Regulation) (далі – GDPR) наведений приблизний перелік онлайн-ідентифікаторів. Так, у ст.30 GDPR зазначено, що «Фізичні особи можуть бути пов'язані з онлайн-ідентифікаторами за допомогою їхніх пристроїв, додатків, інструментів чи протоколів, зокрема IP-адрес, ідентифікаторів «cookie» (реп'яшків) або інших ідентифікаторів, таких як мітки радіочастотної ідентифікації. Це може залишити підказки, які, особливо в поєднанні з унікальними ідентифікаторами та іншою інформацією, отриманою з серверів, можна використати для створення профілів фізичних осіб та їхньої ідентифікації» [9].

Таким чином, для можливості здійснення подальшого дослідження порядку реалізації інформаційних прав людини нами встановлено відомості, які можуть бути конфіденційною інформацією і для обробки яких необхідна згода суб'єкта, а отже зміст інформаційних прав і особливості їх реалізаціє аналізуються в цій статті на прикладі прав на персональні дані.

Подальше дослідження полягає у встановленні змісту зазначених прав на підставі порівняння національного законодавства з європейськими вимогами до захисту персональних даних. Обрання такого підходу обумовлено розумінням необхідності виконання Україною статті 15 Угоди про асоціацію між Україною та ЄС, відповідно до якої «сторони домовились здійснювати співробітництво з метою забезпечення належного рівня захисту персональних даних відповідно до найвищих європейських та міжнародних стандартів, зокрема відповідних документів Ради Європи» [10]. На цей момент таким найвищим європейським стандартом у сфері захисту персональних даних є *Загальний регламент про захист даних* 2016/679 (*General Data Protection Regulation, далі – GDPR*) – регламент Ради Європи щодо захисту персональних даних усіх осіб у межах Європейського Союзу та Європейської економічної зони. GDPR спрямований на забезпечення контролю громадянам та резидентам ЄС за їхніми персональними даними та спрощення регуляторного середовища для міжнародного бізнесу шляхом уніфікації регулювання в межах ЄС. Регламент було прийнято 14 квітня 2016 року і відповідно до встановленого дворічного перехідного періоду 25 травня 2018 почалося його застосовування. GDPR, будучі регламентом, не вимагає від національних урядів прийняття законів, які уможливлюють його дію, і є безпосередньо застосовним. Юридично для України GDPR носить рекомендаційний характер, проте, враховуючі визначений в Преамбулі Конституції України курс на євроінтеграцію набуває для нашої держави цілевстановлювального значення.

Питання щодо встановлення змісту інформаційних прав суб'єктів персональних даних щодо своїх даних визначено в національному законодавстві як в профільному законі «Про захист персональних даних», так і в інших «інформаційних» актах (ЗУ «Про інформацію», «Про доступ до публічної інформації», «Про державну статистику» та інших).

Законом України «Про персональні данні» (далі – Законом) права суб'єкта персональних даних передбачені у статті восьмій, в якій сформульовано принцип невід'ємності та непорушності особистих немайнових прав на персональні дані кожної фізичної особи та міститься перелік з тринадцяти конкретних прав [7]. GDPR також має визначений перелік прав суб'єкта персональних даних, що міститься у главі третій, статтях з дванадцятої по двадцяту. Проведемо аналіз зазначених актів та надамо тлумачення змісту положень цих статей.

Право знати про джерела, місцезнаходження своїх персональних даних та інше, передбачене п. 1 ч. 2 ст. 8 Закону відповідає за змістом, але є набагато вужчим за обсягом статті 12 GDPR «*Прозора інформація, повідомлення та форми реалізації прав суб'єкта даних».* Зміст положень частин цієї статті зводяться до зобов'язання контролерів (особи, які контролюють обробку даних, за національним законодавством – володільці, тобто особи, які визначають мету та способи обробки персональних даних) інформувати суб'єктів про обробку їх особистої інформації. Контролери повинні заздалегідь інформувати суб'єктів даних про способи обробки даних в повідомленні про конфіденційність, доступному для невизначеного кола осіб, або у відповіді на індивідуальний запит, з яким до них може звернутися суб'єкт даних. У цій статті встановлюється вимога до форми інформації, яка надається як відповідь на запит суб'єкта даних: вона повинна бути передана «в лаконічній, прозорій, зрозумілій і

легкодоступній формі», контролери повинні використовувати у своєму спілкуванні «чітку і просту мову». Надамо короткі пояснення до цих вимог. Так лаконічність передбачає вимогу щодо того, що інформація повинна бути представлена коротко, але і всебічно. Контролери можуть мати велику кількість інформації, щоб надати людині в залежності від характеру запиту, але вони повинні представити її лаконічно, тому що, наприклад, включення неактуальної, зайвої або непотрібної інформації до відповіді має розглядатися як ще один спосіб порушення вимоги лаконічності.

Прозорість є одним з ключових принципів GDPR. Вона повинна розглядатися як загальне зобов'язання, що охоплює відкритість, чесність і правдивість. Компанія повинна активно розголошувати всю необхідну інформацію про те, як вона обробляє персональні дані або повідомляти про це, коли її просять.

Зрозумілість означає, що інформація, пов'язана з конфіденційністю, повинна бутилегко зрозумілою і представлена у формі, адаптованій для будь-якої аудиторії (дорослі, діти, професіонали, особливий контекст і т. ін.). Інформація повинна бути прямолінійною, уникати будь-якої двозначності і не залишати місця для інтерпретації.

Простота доступу означає, що інформація про захист даних повинна бути легкою для доступу. Спосіб надання інформації повинен бути адаптований до контексту або платформи, де вона представлена. Посилання на політику конфіденційності може бути помітно представлено внизу електронного листа або відображатися там, де особи зазвичай шукають його на веб-сайті, наприклад в нижньому колонтитулі. Воно не має бути «приховано» в контекстне меню в додатку, де користувачі ніколи не подумають його шукати.

Інформація відповідно до цих вимог повинна передаватися «письмово» або будь-якими «іншими засобами», наприклад через електронні форми, такі як додатки або веб-сайти. Вона може бути надана, якщо цього вимагає специфіка аудиторії,адаптована до ситуації, через малюнки, інфографіку або схеми (Керівні принципи щодо прозорості, викладені у п. 56 Преамбули).

Форма та структура інформації також розглядаються європейським регулюванням. Інформація, пов'язана з конфіденційністю, повинна чітко відрізнятися від іншої правової інформації, такої як загальні умови використання (п. 56 Преамбули). Допускається досягати такого розмежування навіть за допомогою синтаксичних і пунктуаційних засобів: використання заголовків, маркування, відступів тощо.

Положення п. 2, п. 3, п. 4, п. 8, п. 9 ч. 2 ст. 8 Закону, що передбачають права отримувати інформацію про умови надання доступу до персональних даних іншим особам, про доступ до своїх даних, отримувати відповідь про те, чи обробляються персональні дані, а також отримувати їх зміст**,** та право на застосування механізмів правового захисту прав суб'єкта персональних даних кореспондують статті 15 GDPR «*Право суб'єкта даних на доступ*»: суб'єкт даних повинен мати право на отримання від володільця підтвердження факту опрацювання його персональних даних і інформації про: цілі цього Регламенту; категорії відповідних персональних даних; одержувачі чи категорії одержувача, якому персональні дані були або будуть розкриті, зокрема, одержувачі в третіх країнах або міжнародні організації; за можливості, період, протягом якого передбачається, що персональні дані будуть зберігати, або, якщо це неможливо, – критерії визначення такого періоду існування права надсилати запит до контролера щодо виправлення чи стирання персональних даних, або обмеження опрацювання персональних даних про суб'єкта даних і заперечувати проти такого опрацювання; право подавати скаргу до наглядового органу якщо персональні дані не збирають від суб'єкта даних, будь-яку інформацію щодо їхнього джерела; наявність автоматизованого вироблення й ухвалення рішень, у тому числі профайлінгу, вказаного в статті 22(1) та (4) і, принаймні в таких випадках, достовірної інформації про логіку, значимість та передбачувані наслідки такого опрацювання для суб'єкта даних. Отже вбачається, що хоча положення національного та європейського актів зближені, однак підходи до їх викладення та їх зміст достатньо різниться: положення Регламенту є більш стратегічні і охоплюють більше ймовірних сфер поводження з персональними даними, зокрема й механізми запобігання порушенням при транскордонних передачах даних тощо.

Деякі з цих вимог бачимо також у статтях 16-17 Закону, наприклад, у ч. 6 ст. 16 Закону «Про захист персональних даних» з цього приводу також зазначено, що суб'єкт персональних даних має право на одержання будь-яких відомостей про себе у будь-якого суб'єкта відносин, пов'язаних з персональними даними, за умови надання інформації про прізвище, ім'я та по батькові, місце проживання (місце перебування) і реквізити документа, що посвідчує фізичну особу, яка подає запит (для фізичної особи – заявника), крім випадків, установлених законом. За ч. 1 ст. 17 відстрочення доступу суб'єкта персональних даних до своїх персональних даних не допускається.

Щодо органів державної влади, на які покладено повноваження нагляду та контролю у сфері забезпечення дотримання порядку обробки персональних даних, повноважень контролеру, то за національним законодавством такі повноваження покладено на Уповноваженого Верховної Ради України з прав людини. В Законі України «Про захист персональних даних» до суб'єктів відносин, пов'язаних із персональними даними (ст. 4) належить і Уповноважений Верховної Ради України з прав людини (далі – Уповноважений). Відповідно до п. 7 ст. 3 закону України «Про Уповноваженого Верховної Ради України з прав людини» одним з напрямів парламентського контролює сприяння правовій інформованості населення та захист конфіденційної інформації про особу [11]. В цій галузі Уповноваженим розроблено і прийнято низку правових актів, зокрема: Типовий порядок обробки персональних даних, Порядок здійснення Уповноваженим Верховної Ради України з прав людини контролю за додержанням законодавства про захист персональних даних, Порядок повідомлення Уповноваженого Верховної Ради України 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 при їх обробці, а також оприлюднення вказаної інформації, затверджені наказом Уповноваженого ВР з прав людини «Про затвердження документів у сфері захисту персональних даних» від 08.01.2014 № **1/02-14** [12].

Право пред'являти вмотивовану вимогу щодо зміни або знищення своїх персональних даних будь-яким володільцем та розпорядником персональних даних, якщо ці дані обробляються незаконно чи є недостовірними, передбачене п. 6 ч. 2 ст. 8 Закону є близьким за змістом до положень статті 16 GDPR «*Право на виправлення*», та статті 17 GDPR «*Право на забуття*». Право на виправлення передбачає право на виправлення неточних персональних даних, яке повинен здійснити контролер без будь-якої необґрунтованої затримки. Зважаючи на цілі опрацювання, суб'єкт даних повинен мати право заповнити незаповнені персональні дані, в тому числі, надавши додаткову заяву. У GDPR, як вбачається, зазначено право доповнити чи змінити дані, що є неточними, коли українське законодавство значно звужує таке право, обумовлюючи його наявність вже існуючим порушенням (використання недостовірних даних чи незаконна обробка) та залишаючи поза правовим полем вимогу суб'єкта даних щодо, наприклад, актуалізації інформації. Тлумаченні поняття недостовірної інформації надав Пленум Верховного Суду України в постанові від 27 лютого 2009 року № 1 «Про судову практику у справах про захист гідності та честі фізичної особи, а також ділової репутації фізичної та юридичної особи», де зазначено, що недостовірною вважається інформація, яка не відповідає дійсності або викладена неправдиво, тобто містить відомості про події та явища, яких не існувало взагалі або які існували, але відомості про них не відповідають дійсності (неповні або перекручені). Отже у випадку, коли навпаки подій не існувало, а потім вони відбулись (реєстрація шлюбу, народження дітей, отримання наукового ступеню тощо) суб'єкт не має підстав вимагати їх актуалізації.

Право на забуття є одним з найважливіших та обговорюваних прав суб'єкта даних, яку було реалізовано у ст. 17 GDPR. Потреба у «праві на забуття» зросла у зв'язку з розвитком світу високих технологій, в якому будь-які персональні дані можуть бути опубліковані у всесвітній мережі, що в свою чергу має обмежений рівень контролю [13]. Отже, відповідно до ст. 17 GDPR «Суб'єкт даних повинен мати право на стирання своїх персональних даних, яке повинен здійснити контролер без будь-якої безпідставної затримки, також контролер повинен бути зобов'язаним стерти персональні дані без будь-якої необґрунтованої затримки у разі виникнення однієї з наведених нижче підстав: **(a)** немає більше потреби в персональних даних для цілей, для яких їх збирали чи іншим чином опрацьовували; **(b)** суб'єкт даних відкликає згоду, на якій ґрунтується опрацювання, та якщо немає іншої законної підстави для опрацювання, **(c)** суб'єкт даних заперечує проти опрацювання, та немає жодних першочергових законних підстав для опрацювання, або суб'єкт даних заперечує проти опрацювання згідно зі статтею 21(2); **(d)** персональні дані опрацьовували незаконно; **(e)** персональні дані необхідно стерти для дотримання встановленого законом зобов'язання, закріпленого в законодавстві Союзу або держави-члена, яке поширюється на контролера **(f)** персональні дані збирали в зв'язку з пропонуванням послуг інформаційного суспільства, вказаних у статті 8(1).

Право не є абсолютним, а отже є випадки, коли воно не може бути реалізовано (наприклад, є законна вимога щодо збереження даних певний строк, або для надання певної послуги виконавцю потрібні такі дані, і суб'єкт даних від послуги не відмовився, для статистичних, наукових цілей, для цілей охорони здоров'я тощо).

В національному законодавстві це право розкривається у ст. 15 Закону, відповідно до якої персональні дані видаляються або знищуються в порядку, встановленому відповідно до вимог закону і

підлягають видаленню або знищенню у разі: закінчення строку зберігання даних, визначеного згодою суб'єкта персональних даних на обробку цих даних або законом; припинення правовідносин між суб'єктом персональних даних та володільцем чи розпорядником, якщо інше не передбачено законом; видання відповідного припису Уповноваженого, набрання законної сили рішенням суду щодо видалення або знищення персональних даних; встановлення факту зібрання персональних даних порушенням вимог закону. Однак, як вбачається зі змісту цієї статті, закон не передбачає можливості без наявних підстав звернутися з вимогою про видалення своїх персональних даних, всупереч положенням GDPR, де бажання суб'єкта даних є основною підставою.

Наступне право, близьке за змістом до «права на забуття» - це «*право на обмеження опрацювання*» (Стаття 18 GDPR). В національному Законі воно сформульоване як «право відкликати згоду на обробку персональних даних» і передбачене у п. 11 ч. 2 ст. 8 Закону.

Відповідно до ст. 18 GDPR «суб'єкт даних повинен мати право на обмеження працювання контролером у разі настання таких обставин: (a) точність персональних даних оскаржує суб'єкт даних, протягом періоду часу, що надає контролеру можливість перевірити точність персональних даних; (b) опрацювання є незаконним та суб'єкт даних виступає проти стирання персональних даних і натомість надсилає запит на обмеження їх використання; (c) контролеру більше не потрібні персональні дані для цілей опрацювання, але їх вимагає суб'єкт даних для формування, здійснення або захисту правових претензій; d) суб'єкт даних заперечив проти опрацювання згідно зі статтею 21(1) в очікуванні проведення перевірки щодо того, чи переважають законні підстави контролера над законними інтересами суб'єкта даних». Отже вбачається, що зазначене право дає можливість суб'єкту даних вимагати зупинення будь-якого поводження (обробки) з його даними, окрім зберігання.

В законі відсутні додаткові пояснення щодо цього права, проте в п. 2.15 Типового порядку обробки персональних даних, затвердженого наказом Уповноваженого ВРУ від 8.01.2014 № 1/02-14 зазначено, що особа має право відкликати згоду на обробку персональних даних без зазначення мотивів, у разі якщо єдиною підставою для обробки була її згода, при цьому володілець зобов'язаний припинити обробку персональних даних з моменту відкликання згоди.

Передбачене п. 5 ч. 2. ст. 8 Закону право пред'являти вмотивовану вимогу володільцю персональних даних із запереченням проти обробки своїх персональних даних корелює зі ст. 21 GDPR «*Право на заперечення*», відповідно до якої: «Суб'єкт даних повинен мати право заперечувати, на підставах, що пов'язані з його конкретною ситуацією, в будь-який час, проти опрацювання його персональних даних, у тому числі, проти профайлінгу. Контролер не повинен більше опрацьовувати персональні дані за винятком доведення ним наявності істотних законних підстав для опрацювання, що переважають над інтересами, правами та свободами суб'єкта даних або для формування, здійснення або захисту правових претензій». Частина третя цієї статті «якщо суб'єкт даних заперечує проти опрацювання для цілей прямого маркетингу, персональні дані не можна більше опрацьовувати для таких цілей» як виключення з загальної характеристики інформаційних прав щодо їх не абсолютності, є абсолютним. На наш погляд український законодавець намагався передбачити таку ж можливість, не зазначаючи на конкретну мету обробки даних, проте передбачаючи можливість встановлення застереження щодо мети обробки на початку відносин між сторонами – у п. 10 ч. 2 ст. 8 Закону зазначено, що суб'єкт даних має право вносити застереження стосовно обмеження права на обробку своїх персональних даних під час надання згоди.

І, нарешті, п. 12 та п. 13 ч. 2 ст. 8 Закону захищають суб'єкта персональних даних під час автоматизованої обробки даних. У зазначених пунктах передбачається право знати механізм автоматичної обробки персональних даних та забезпечується право на захист від автоматизованого рішення, яке має для нього правові наслідки. В GDPR схоже право закріплено у ст. 22 «*Автоматизоване індивідуальне вироблення й ухвалення рішень, у тому числі, профайлінг*»: «Суб'єкт даних повинен мати право не підлягати рішенню, що грунтується виняткова на автоматизованому опрацюванні, в тому числі, профайлінгу, що породжує правові наслідки для чи подібним чином істотно впливає на нього». Мова йде про те, що якщо для прийняття рішення щодо суб'єкта (отримання візи, отримання пенсії з урахуванням певного періоду страхового стажу тощо) обробка його персональних даних здійснюється програмою без участі людини, то суб'єкт завжди має право вимагати на перегляді цього рішення саме людиною. А отже при наявності автоматизованої обробки даних, що має юридичне значення, мають виконуватись три умови: 1) суб'єкт персональних даних має бути повідомлений про автоматизовану обробку, 2) суб'єкт повинен розуміти логіку обробки даних, 3) суб'єкт має право на втручання до автоматизованої системи прийняття рішення людиною.

Висновки: Отже, підбиваючи підсумки, зазначимо, що поняття «інформаційні права людини» за змістом є набагато ширшим поняттям ніж «право на інформацію».Інформаційні права людини є складовими її правового статусу, і ступінь їх закріплення та забезпечення реалізації є індикатором демократичності держави. Україна в преамбулі Конституції проголосила курс на євроінтеграцію, яка, зокрема, передбачає і співробітництва в галузі захисту інформаційних прав людини – захисту персональних даних на умовах наближення національного законодавства до найсуворіших регламентів ЄС. Таким регламентом на цей час є у Регламенті Ради Європи 2016-769 (General Data Protection Regulation) (далі – GDPR), зі змістом положень якого ми і порівнювали зміст національного законодавства у сфері захисту персональних даних. І хоча певна відповідність лексичних і змістовних конструкцій правового регулювання поводження з персональними даними в національному і європейському законодавстві спостерігається, проте залишається відмінність у «дусі» регулювання – Регламент ЄС є антропоцентричним, інтереси людини є пріоритетом регулювання, підставами для реалізації багатьох прав суб'єктів даних є їх воля, на відміну від національного законодавства, яке зберігає підхід, щодо якого підставою для виникнення і реалізації одних прав є факти порушення інших прав. Таким чином вважаємо, що трансформація українського законодавства в сфері захисту приватних даних ще не завершилась і буде продовжена, що дасть нові підстави для подальших досліджень.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Ткачук Н.І. Інформаційні права і свободи людини і громадянина в Україні: визначення термінів, співвідношення понять". *Інформація і право*. № 2(25)/2018. С. 17–30.
2. Вакарюк Л. Основні підходи до розуміння «Інформаційні права людини». *Підприємництво, господарство і право: Інформаційне право*. № 2/2018. С. 155–159.
3. Сухорольский П.М. Проблеми забезпечення та розвитку прав людини в умовах інформаційного суспільства. *Український часопис міжнародного права.* 2013. № 1. С. 18–23.
4. Марущак А.І. Визначення поняття "інформаційні права людини". *Інформація і право*. № 2(2)/2011. С. 21–26.
5. Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус: Закон України від 20.11.2012 № 5492-VI. URL: https://zakon.rada.gov.ua/laws/show/5492-17#Text (дата звернення 10.11.2023).
6. Про інформацію: Закон України від 02.10.1992 № **2657-XII**. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення 10.11.2023).
7. Про захист персональних даних : Закон України від 01.06.2010 № **2297-VI.** URL: https://zakon.rada.gov.ua/laws/show/2297-17#n170 (дата звернення 10.11.2023).
8. Рішення Конституційного Суду України у справі за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України: Рішення Конституційного Суду України від 20 січня 2012 року № 2-рп/2012. URL: https://zakon.rada.gov.ua/laws/show/v002p710-12#Text (дата звернення 10.11.2023).
9. Загальний Регламент Європейського Парламенту і Ради ЄС 2016/679 «Про захист даних» від 27.04.2016 р. URL: kmu.gov.ua/storage/app/media/uploaded-files/es-2016679.pdf
10. Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої [...] від 27.06.2014: УгодаСписок, Міжнародний документ / *Україна, Європейський Союз, Євратом [...]* URL: https://zakon.rada.gov.ua/laws/show/984_011#Text (дата звернення 10.11.2023).
11. Про Уповноваженого Верховної Ради України з прав людини: Закон України від 23.12.1997 № 776/97-ВР. URL: https://zakon.rada.gov.ua/laws/show/776/97-%D0%B2%D1%80#n10 (дата звернення 10.11.2023).
12. Про затвердження документів у сфері захисту персональних даних: Наказ від 08.01.2014 № 1/02-14. URL: https://zakon.rada.gov.ua/laws/show/v1_02715-14?test=n6HMfJRw7UpVmUn6ZilPzapnHI41gs80msh8Ie6#n11 (дата звернення 20.11.2023).
13. Аналіз законодавства про захист персональних даних України. Звіт, підготовлений АО «Саєнко Харенко» 14 вересня 2020 року. URL: https://ecpl.com.ua/wp-content/uploads/2020/09/UKR_09142020_CEP_Finalnyy-zvit.pdf (дата звернення 10.11.2023).