УДК 342.9
DOI https://doi.org/10.32782/klj/2023.1.29

**Кравчук В. О.,**
аспірантка
Національного авіаційного університету

# РЕАЛІЗАЦІЯ ПРАВА НА НЕДОТОРКАНІСТЬ ПЕРСОНАЛЬНИХ ДАНИХ У СОЦІАЛЬНИХ МЕРЕЖАХ У СИСТЕМІ ПРАВ І СВОБОД ЛЮДИНИ І ГРОМАДЯНИНА

**Анотація.** Стаття присвячена питанню реалізації права на недоторканість персональних даних у соціальних мережах у системі прав і свобод людини і громадянина. Актуальність даної статті підтверджується швидкою зміною та розвитком інформаційно-комунікаційних технологій структури світу, що вплинуло на формування інформаційного суспільства в умовах глобалізаційних процесів. Тематика права на недоторканість персональних даних у соціальних мережах набуває нового змісту відповідно до тенденцій та викликів розвитку соціальних мереж в сучасному світі. Тому актуальність даної статті визначається необхідністю дослідження права на приватність в соціальних мережах до міжнародних стандартів.

Метою даної статті було виявити особливості розвитку права на недоторканість персональних даних у соціальних мережах в контексті складних інформаційних змін, та напрямки їх впливу на формування міжнародного інтернет права. Для досягнення мети була здійснений аналіз науково-теоретичних та практичних джерел в сфері дослідження права на недоторканість персональних даних у соціальних мережах Європейського Союзу та інших країн, а також аналіз впливу на політичну ситуацію та розвиток українських реалій. Для вирішення визначених завдань даної статті було застосовано загально правові та спеціально-правові методи: історичний метод, порівняльно-правовий метод, що дозволило здійснити дослідження. Більше того, застосовано методи аналізу та синтезу, а також систематизації, завдяки якому ми змогли проаналізувати закономірності права на недоторканість персональних даних у соціальних мережах у системі прав і свобод людини і громадянина. Автором було зроблено висновок про постійну динаміку в сфері розвитку права на недоторканість персональних даних у соціальних мережах у системі прав і свобод людини і громадянина, що пов'язано з розвитком технологій. Внаслідок порівняння досвіду ЄС та України, було визначено, що за останні роки політика права на недоторканість персональних даних у соціальних мережах у системі прав і свобод людини і громадянина стає складної міжнародної проблемою. Особливої уваги приділяється увага безпеці та захисту права на приватність в інтернет просторі.

***Ключові слова:*** *персональні дані, захист персональних даних, інформаційне право, інформаційне суспільство, недоторканність, приватність.*

**Kravchuk V. O. Implementation of the right to the invincibility of personal data in social networks in the system of human and citizen rights and freedoms**

**Abstract.** The article is devoted to the issue of implementing the right to inviolability of personal data in social networks in the system of human and citizen rights and freedoms. The relevance of this article is confirmed by the rapid change and development of information and communication technologies in the structure of the world, which influenced the formation of the information society in the conditions of globalization processes. The topic of the right to the inviolability of personal data in social networks acquires a new meaning in accordance with the trends and challenges of the development of social networks in the modern world. Therefore, the relevance of this article is determined by the need to research the right to privacy in social networks in accordance with international standards.

The purpose of this article was to reveal the peculiarities of the development of the right to privacy of personal data in social networks in the context of complex informational changes, and the direction of their influence on the formation of international Internet law. To achieve the goal, an analysis of scientific, theoretical and practical sources in the field of research on the right to privacy of personal data in social networks of the European Union and other countries was carried out, as well as an analysis of the impact on the political situation and the development of Ukrainian realities. To solve the defined tasks of this article, general legal and special legal methods were applied: historical method, comparative legal method, which allowed to carry out the research. Moreover, the methods of analysis and synthesis, as well as systematization, were applied, thanks to which we were able to analyze the patterns of the right to inviolability of personal data in social networks in the system of rights and freedoms of a person and a citizen. The author made a conclusion about the constant dynamics in the field of development of the right to inviolability of personal data in social

networks in the system of human and citizen rights and freedoms, which is connected with the development of technologies. As a result of comparing the experience of the EU and Ukraine, it was determined that in recent years the policy of the right to inviolability of personal data in social networks in the system of human and citizen rights and freedoms has become a complex international problem. Special attention is paid to security and protection of the right to privacy in the Internet space.

***Key words:*** *personal data, protection of personal data, information law, information society, inviolability, privacy.*

**Постановка проблеми.** Інформаційно-технічний прогрес і людська поведінка значною мірою впливають один на одного в епоху цифрових технологій і взаємно визначають майбутній економічний і соціальний розвиток світового суспільства. Соціальні мережі стали феноменом і новим інструментом комунікації, що змінив процес спілкування в усіх соціальних групах.

На сьогодні соціальні мережі набули величезної популярності, адже дозволяють користувачам завантажувати інформацію в загальнодоступний профіль, створювати список онлайн-друзів і переглядати профілі інших користувачів. Багато людей довіряють свої особисті дані цим мережам для спілкування в Інтернеті.

У сучасній цифровій епосі захист та безпека особистих даних потребують надійного захисту. Багато новітніх бізнес-моделей базуються на даних користувачів, а прибутковість цих моделей може бути продемонстрована фінансовим успіхом таких великих гравців, як Google і Facebook. І не тільки власники соціальних мереж вірять у «силу даних», оскільки майже всі суб'єкти господарювання збирають і аналізують дані своїх користувачів або купують набори даних на так званих ринках даних. У всьому світі налічується 3,6 мільярда активних користувачів соціальних мереж, тобто вони складають майже половину населення світу. Прогнозується, що до 2025 року це число зросте до 4,4 мільярди. У 2020 році витрати на рекламу в соціальних мережах досягли 132 мільярдів доларів і очікується, що загальна сума перевищить позначку в 200 мільярдів доларів у наступні два роки [1]. Велика кількість персональних даних, наданих цими користувачами, робить ці платформи одним із найефективніших маркетингових інструментів для компаній.

**Аналіз останніх досліджень і публікацій.** Тематику забезпечення інформаційних прав досліджувати такі вчені та практики, як: О.В. Басай, І.М. Берназюк, С.С. Єсімов, С.В. Ківалов, Л.Р. Біла-Тіунова, Т.А. Латковська, Г.М. Проскура, М.В. Різак, В.О. Серьогін, Б.В. Віліч, Кастерс, Л. Грест, С. Гутвірт, Е. Коста, К. Каллоніатіс, Б. Ковачич, М. Лукас, І. Раденковіч, С. Родота, Л. Риз, А. Скенджич та інші вчені. Таким чином, питання реалізації права на недоторканість персональних даних у соціальних мережах у системі прав і свобод людини і громадянина не лише залишається актуальним, а й поступово перетворюється в глобальну проблему людства.

**Метою статті** є дослідження особливостей реалізації права на недоторканість персональних даних у соціальних мережах у системі прав і свобод людини і громадянина на сучасному етапі розвитку інформаційного суспільства та цифрових технологій.

**Виклад основного матеріалу.** Факт існування у кіберпросторі можливостей збирати, зберігати, поширювати, відтворювати, публікувати та робити доступними для широкого кола людей особисті дані викликає відчуття незахищеності та відсутності безпеки та захисту [2]. Як визначають М.Г. Ісаков і В.Г. Паркулаб, у сучасному глобалізованому суспільстві більшість відносин здійснюється через Інтернет, тому основним соціальним регулятором має стати саме правове регулювання, основою якого є визнання принципів пріоритету прав і свобод людини, адекватного та виправданого державного контролю, забезпечення вибору варіантів захисту конфіденційності та анонімності інформації, забезпечення мінімізації збору та обробки персональних даних, реалізація яких не дозволить створити глобальну інформаційну базу, злочинцями якої будуть не тільки об'єкти спостереження [3]. У сучасній юридичній науці вченими неодноразово відзначалося, що соціальні мережі можуть відстежувати взаємодію користувачів на своїх сайтах і зберігати відповідну інформацію для подальшого використання,

що становить потенційну загрозу конфіденційності та приватності особи [4].

Отже, соціальні мережі стали засобом комунікації в Інтернеті, за допомогою яких користувачі діляться інформацією, ідеями, особистими повідомленнями та іншим вмістом.

Найперші форми соціальних медіа з'явилися майже відразу, як тільки технології змогли їх підтримувати. З випуском веббраузера Mosaic в 1993 році ці системи були об'єднані простим у використанні графічним інтерфейсом. Архітектура Всесвітньої павутини дозволяла переходити з одного сайту на інший одним клацанням миші, а швидші підключення до Інтернету дозволяли мати більше мультимедійного вмісту [5]. З розвитком технології Web 2.0 значення соціальних мереж стало стрімко зростати.

Серед важливих проблем забезпечення прав людини в мережі інтернет є забезпечення права на недоторканість персональних даних у соціальних мережах у системі прав і свобод людини і громадянина.

В академічних колах науковці часто сходяться на думці, що однозначно визначати приватність є недоцільним. Конфіденційність, як випливає з цього висновку, краще розглядати як суміш пов'язаних цінностей у різних контекстах. Наприклад, конфіденційність гарантує фізичну цілісність, контроль над особистою інформацією, недоторканність житла та конфіденційність спілкування. У свою чергу, ці принципи можуть ґрунтуватися на фундаментальному принципі автономії особистості на особистому, інтелектуальному та соціальному рівнях [6]. Дебати про схильність урядів і компаній збирати особисту інформацію, а також впровадження все нових і нових технологій привертають широкий громадський інтерес. Більше того, існує велика плутанина щодо того, що насправді означає конфіденційність. Ця плутанина іноді змушує нас забути, що може запропонувати конфіденційність як ідеал, особливо для індивідів у двадцять першому столітті.

Загроза, яку Інтернет та цифрові інформаційно-комунікаційні технології загалом створюють або створюватимуть для конфіденційності, є предметом багатьох дискусій як у пресі, так і на політичному рівні. Справа Сноудена у 2013 році, а потім ухвалення Загального регламенту захисту даних у 2016 році підвищили видимість цих суперечок у публічній сфері. Визначаючи «приватність» як об'єкт, що захищається нормативними текстами – законами, юриспруденцією та техніко-політичними стандартами Інтернету – які захищають право на приватність, можна емпірично вивчати їх еволюцію та протиріччя, які її супроводжують [7].

Як наслідок постало питання про визначення терміну "недоторканність персональних даних". Серед вчених немає єдиного погляду на розуміння даної категорії. У західній правовій доктрині для позначення правового інституту, яким охоплюється захист недоторканності приватного життя, використовується термін «прайвесі» [8]. Позиція Європейського суду з прав людини щодо несанкціонованого прослуховування телефонних розмов поліцією» зазначає: право на повагу до приватного та сімейного життя передбачено в ст. 8 Конвенції про захист прав людини і основоположних свобод. У рішеннях Європейського суду з прав людини немає юридичного визначення поняття «приватність» і чіткого визначення конфіденційної інформації та того, як ця категорія інформації співвідноситься з персональними даними [9].

Проте, як доцільно вказує Гуйван П. Д., право даної особи на захист її персональних даних у світі передбачається в рамках реалізації права на недоторканність приватного життя. Ці права тісно пов'язані між собою і співвідносяться як часткова та загальна категорії, оскільки персональні дані людини є невід'ємною частиною приватності [10].

За Р. Романскі, обсяг і зміст поняття «особисте життя» можна визначити відповідно до національної культури та індивідуальних особливостей населення, але є також загальні елементи, такі як недоторканність персональної інформації та її захист. У цьому сенсі кожна людина має право на захист персональних даних, що є частиною концепції приватності. Право на приватність формує загальну основу свободи вираження поглядів, права на особисту безпеку, права від-

мовитися від свідчень проти самого себе тощо [11].

За Басай О. В. неприпустимість свавільного втручання у сферу особистого життя особи означає вимогу забезпечення свободи особи, яку іноді називають «індивідуальним суверенітетом», включаючи в це поняття можливість особи визначати вид і характер своїх прав. поведінка, своє місце в суспільстві, в системі цивільних відносин на свій розсуд [12]. Як зазначає Е.А. Суханов, принцип неприпустимості свавільного втручання у сферу особистого життя людини характеризує цивільне право як приватне. Різак М.В. встановлено, що для створення ефективного механізму забезпечення недоторканності приватного життя в контексті обігу та обробки персональних даних в умовах правоохоронної діяльності необхідно на законодавчому рівні: визначити тривалість обіг та обробка персональних даних правоохоронними органами; встановити обов'язок знищення персональних даних після закінчення правоохоронної діяльності у зв'язку з вчиненням конкретного діяння, пов'язаного з їх збиранням для поширення та обробки; удосконалити положення правових норм щодо встановлення відповідальності у сфері обігу та обробки персональних даних [13].

На наш погляд, недоторканість персональних даних – це такий правовий режим персональної інформації, за яким унеможливлюється незаконний обіг та обробки особистих даних особи.

Межі приватності особи можна визначити як сферу діяльності виключно конкретної особи та інформацію про неї, які обмежені рамками законності, відсутністю норм які встановлюють обов'язкову поведінку в певних ситуаціях, що виникають у цій сфері, і особою, яка вживає заходів для її захисту [14].

На міжнародному рівні права на недоторканість персональних даних у соціальних мережах у системі прав і свобод людини і громадянина забезпечуються загальними нормами міжнародного права.

Загалом, поява нової концепції цифрових прав призвела до пошуку оптимальної моделі індивідуальної автономії, результатом чого стало право на захист даних, найбільш чітко сформульоване в Хартії основних прав Європейського Союзу. Показано, що декларація права на захист даних пов'язана з такими факторами: 1) спілкування з можливістю контролювати інформацію про себе; 2) еволюція права на недоторканність приватного життя, зміна в розвитку різноманітних технологій, розсунення меж права чи зміна підходів до його захисту; 3) поява нових цінностей та інформаційне самовизначення; 4) циркуляція інформаційних потоків відповідно до правил технологічної обробки, що впливають на зміст конкретних повноважень кожного громадянина в цифровому просторі [15].

У рішенні від 6 червня 2013 року ЄСПЛ зазначив, що захист персональних даних, у тому числі медичної інформації, має фундаментальне значення для реалізації гарантованого права людини на повагу до її приватного життя та сім'ї.

Водночас можливі варіанти, якщо виявиться, що національні інтереси важливіші. Справа «Gaugran проти Великої Британії» стосувалась скарги заявника щодо безстрокового зберігання його персональних даних. У рішенні від 13 лютого 2020 року у цій справі ЄСПЛ визнав непропорційний характер повноважень органів державної влади зберігати профіль, засудженої за вчинення злочину особи, оскільки безстрокове зберігання період таких даних встановлено без посилання на тяжкість правопорушення чи необхідність безстрокового тримання під вартою та за відсутності реальної можливості перегляду справи, що свідчить про недотримання справедливого балансу між конкуруючими державними та приватними інтересами. У цій справі Суд зазначив, що держава зберегла за собою дещо ширші дискреційні повноваження щодо зберігання відбитків пальців і фотографій, але цих широких дискреційних повноважень недостатньо для висновку, що збереження цих даних може бути пропорційним за обставин, включаючи відсутність будь-які відповідні гарантії, включаючи відсутність фактичної візуалізації. Слід зазначити, що подібний підхід був застосований ЄСПЛ у рішеннях від 34 січня 2019 року у справі «Kett v. Велика Британія» [16], від 13 лютого 2020 року у справі "Trajkovski and Chipovski v. Північна Македонія" та інші.

Більшість науковців, політиків і активістів дотримуються індивідуалістичних теорій конфіденційності та захисту даних. Соціальні мережі не лише загрожують своїм користувачам, відкриваючи їх для інших користувачів або громадськості. Вони становлять, насамперед, загрозу суспільству в цілому, збираючи інформацію про осіб, групи та організації з різних соціальних систем і об'єднуючи її в централізований банк даних [17].

Хоча існує суспільна згода щодо необхідності забезпечення конфіденційності, на практиці ставлення людей до конфіденційності їхньої особистої інформації складне. Наприклад, навіть, коли люди стверджують, що цінують конфіденційність своєї інформації, вони часто поширюють її заради матеріальної чи нематеріальної вигоди [18].

В Україні важливою складовою національної політики є забезпечення прав і свобод громадян, у тому числі інформаційних до статті 50 Конституції України [19].

Зарубіжна практика державної політики в окресленій сфері немає єдиного підходу до розуміння конфіденційності та приватності. Встановлення спеціального регулювання щодо розробки, створення, впровадження, продажу та обігу окремих цифрових технологій нерозривно пов'язане із встановленням спеціального порядку обробки знеособлених персональних даних з метою формування цілісної системи регулювання суспільних відносин, що виникають. у зв'язку з розвитком інформаційних технологій та їх використанням. Демократичні держави давно знайшли спільну мову у застосуванні основних принципів захисту персональних даних і підтвердили їх застосовність до цифрової сфери, але насправді їх реалізація суттєво відрізняється в різних країнах [20].

Загальний регламент захисту даних Європейського Союзу часто називають «золотим стандартом» для захисту інформації споживачів і конфіденційності даних у сучасну цифрову епоху [21]. За допомогою суворих заходів і жорстких покарань документ має на меті контроль за тим, як організації в будь-якій країні можуть збирати, використовувати та зберігати особисту інформацію суб'єктів даних ЄС. Ці правила також застосовуються до компаній, які збирають дані громадян ЄС за допомогою реклами в соціальних мережах, пікселів відстеження, веб-сайтів, файлів cookie тощо. Відповідність Регламенту є обов'язковою, а недотримання може призвести до суворих штрафів [22].

91 стаття та 11 розділів Регламенту спрямовані на те, щоб компанії не могли збирати, обробляти, зберігати або ділитися даними споживачів із ЄС без їхньої згоди. Це включає дані клієнтів соціальних мереж: файли cookie веб-браузера; IP-адреси; пікселі відстеження Facebook; фотографії в соціальних мережах; будь-яка інша ідентифікаційна інформація, пов'язана з публікаціями в соціальних мережах, інструментами чату, рекламою в соціальних мережах тощо. Щоб отримати згоду, компанії повинні встановити прапорці для згоди і розкрити умови збору та використання даних, які відвідувачі можуть переглянути та прийняти рішення щодо такої згоди.

У Китаї зростаюча популярність використання соціальних медіа, а також швидкий розвиток технологій спостереження на робочому місці полегшили роботодавцям доступ до великої кількості інформації в соціальних мережах працівників. Враховуючи, що китайське законодавство про конфіденційність і захист особистих даних є відносно слабким, у країні зростає кількість судових справ, пов'язаних із доступом роботодавців до вмісту соціальних мереж працівників і його використанням [23].

Конституція Бразилії у статті 5 забезпечує недоторканність приватного життя, інтимності та честі як фундаментальне право. Бразильський Білль про права в Інтернеті під назвою "Marco Civil da Internet" запровадив у Бразилії різноманітність принципів і параметрів регулювання Інтернету в країні. Існування прогалини в законодавчій системі, пов'язаної з законами та інфраструктурою для ефективної гарантії права на захист даних в Інтернеті, як виявлено в інших країнах, у поєднанні з відсутністю конкретної концептуальної точності конфіденційності в Інтернеті, виправдовує прийняття в цьому дослідженні інноваційної концепції «Прав на конфіденційність в Інтернеті», заснованої на Берналі (2014). Вона складається з чотирьох прав: право

шукати в Інтернеті з конфіденційністю; право стежити за тими, хто стежить за нами; право на видалення персональних даних; право на ідентифікацію в Інтернеті [24].

Для того, щоб людина могла активно реалізовувати своє право, їй необхідно повідомити, що її дані зберігаються вперше. Таким чином, особа має право в будь-який час отримати інформацію про тип і обсяг, а також зберігання своїх даних. Це право також включає можливість виправлення або оновлення даних. Це також стосується передачі даних третім особам. Особа має право знати, які дані, з якою метою та кому передаються, і мати можливість давати активну згоду на це. Якщо користувачі даних порушують захист даних, суб'єкт даних може відстоювати своє право на відшкодування збитків або компенсацію за біль і страждання [25].

Також важливою частиною права на приватність є право на забуття. Раніше ця ідея суперечила нав'язуванню технічної реальності щодо збереження персональних даних протягом невідомих періодів часу. Разом з тим, на сьогодні відомо, що дії користувачів в Інтернеті з поширення інформації, у тому числі особистої, супроводжуються процесом переходу контролю за цією інформацією інших користувачів і власників ресурсів. Цей процес переходу приніс користувачам Інтернету багато проблем і став явною загрозою для їх конфіденційності, а про їхнє право на доступ забули [26], [27].

Задля поваги конфіденційності та пов'язаних з нею прав постачальники онлайн-персоналізації повинні активно залучати користувачів до процесу персоналізації та дозволяти їм використовувати персоналізацію для особистих цілей [28]. Таким чином, доступ до баз персональних даних фізичних осіб підвищує ризик вторгнення у сферу приватного життя та порушення права на недоторканність. Комп'ютерна техніка значно загострила правові проблеми, пов'язані з дилемою розголошення чи конфіденційності та відсутністю традиційних правових засобів для забезпечення конфіденційності [29].

Таким чином, цифрові технології не змінюють фундаментальних цінностей, прав і свобод, закріплених в основному законі сучасної держави. Проте нові технологічні виклики вимагають підтвердження та роз'яснення фундаментальних прав щодо нових технологій. Численні проблеми цифрового середовища пов'язані із забезпеченням захисту персональних даних, що зумовлено недостатнім правовим регулюванням Загалом, законодавство різних країн розвивається по-різному та з різним ступенем розробленості питання захисту персональних даних. А персональні дані використовуються в економіці для різноманітних цілей, більш-менш відданих їх користувачам. Залишається відкритим питання про те, хто насправді «володіє» даними, тобто існує власність на персональні дані і кому ця власність належить, як її структурувати [30]. Автоматизована обробка персональних даних є основним джерелом загроз приватності. Важливо вирішити проблеми регулювання, накопичення, зберігання, використання та захисту персональної інформації. Це дозволить нам реалізувати потенціал і переваги інформаційних технологій для споживачів, мінімізуючи ризик втрати безпеки та конфіденційності [11].

Таким чином, стрімкий розвиток інформаційних технологій і процес глобалізації в останні десятиліття призвели до збільшення швидкості та ефективності поширення інформації. Чільне місце серед її негативних наслідків посідає інформаційна війна, яка передбачає використання різноманітних впливів. Необхідність захисту приватної інформації та даних, у тому числі від їхнього нецільового використання, обумовила необхідність детального вивчення проблеми обігу персональних даних у соціальних мережах та роботи з ними. Ця тема є предметом особливої уваги в контексті пандемії Covid-19 та воєнно-політичної ситуації в Україні. В сучасних суспільно політичних змінах і розвитку інформаційних технологій важливо забезпечити повагу до особистої свободи, прав та приватності кожної людини. В умовах інтернаціоналізації важко відстежити та відновити порушені права, що потребує постійного моніторингу та міжнародної співпраці стейкхолдерів різних рівнів.

**СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ:**

1. GDPR's Impact on Social Media – Everything You Need to Know. *Visitor Analytics* : website. URL: https://www.visitor-analytics.io/en/blog/gdpr-impact-on-social-media/ (Last accessed: 10.01.2023).

2. Ісаков М. Г., Паркулаб В. Г. Захист персональних даних у мережі Інтернет: загальнотеоретичні питання. *Науковий вісник публічного та приватного права*. 2018. Вип. 5, т. 1. С. 106–110.

3. Vilić V., Radenković I. The Right to Privacy, Informational Privacy and the Right to Information in the Cyberspace. *Sinteza 2017* : International Scientific Conference on Information Technology and Data Related Research. Belgrade : Singidunum University, 2017. P. 74–78. DOI: https://doi.org/10.15308/Sinteza-2017-74-78

4. Серьогін В. О. Соціальні мережі як загроза прайвесі. *Форум права.* 2011. № 2. С. 822–827. URL: http://nbuv.gov.ua/UJRN/FP_index (дата звернення: 10.01.2023).

5. Social media. *Encyclopedia Britannica* : website. URL: https://www.britannica.com/topic/social-media (Last accessed: 10.01.2023).

6. van Hoboken J. The Importance of Privacy: Confusion About the Civil Right of the Twenty-First Century. *Amsterdam Law School Legal Studies.* 2012. No 2012-37. URL: https://ssrn.com/abstract=2129751 (Last accessed: 10.01.2023).

7. Rossi J. Protection des données personnelles et droit à la vie privée: enquête sur la notion controversée de «donnée à caractère personnel». Science politique. Université de Technologie de Compiègne, 2020. URL: https://theses.hal.science/tel-03155480/ (Last accessed: 10.01.2023).

8. *Приватне право і підприємництво* : зб. наук. пр. / редкол.: Крупчан О. Д. (гол. ред.) та ін. Київ : Науково-дослідний інститут приватного права і підприємництва імені академіка Ф. Г. Бурчака Національної академії правових наук України, 2019. Вип. 19. 182 с.

9. Єсімов С. С. Персональні дані як предмет захисту права на недоторканність приватного життя. *Вісник Національного університету «Львівська політехніка». Сер. Юридичні науки.* 2017. № 884. С. 120–126.

10. Гуйван О., Гуйван П. Охорона персональних даних як потреба демократичного суспільства. *Підприємництво, господарство і право.* 2018. № 4. С. 34–40.

11. Radeiko R. The Right to Privacy in the Age of Digitalization. *Ehrlich's Journal.* Vol. 3. P. 52–61. URL: http://ehrlichsjournal.chnu.edu.ua/index.php?journal=ehrlichsjournal&page=article&op=view&path%5B%5D=43> (Last accessed: 10.01.2023).

12. Басай О. В. Неприпустимість свавільного втручання у сферу особистого життя як загальна засада цивільного законодавства України. *Часопис Національного університету «Острозька академія». Сер. Право.* 2013. № 2. URL: http://nbuv.gov.ua/UJRN/Choasp_2013_2_7 (дата звернення: 10.01.2023).

13. Різак М. В. Адміністративно-правове забезпечення відносин обігу та обробки персональних даних в Україні : автореф. дис. ... д-ра юрид. наук : 12.00.07 / МВС України ; Харк. нац. ун-т внутр. справ. Харків, 2017. 39 с.

14. Король І. Б. Охорона недоторканості приватного життя: кримінально-правові та кримінологічні аспекти : дис. … канд. юрид. наук : 12.00.08. Львів, 2015. 235 с.

15. Sultanov E. B., Romanovsky G. B., Kil'deev R. R. Transformation of the right to privacy in the context of the development of digital technologies. *BiLD Law Journal*. Vol. 7, No 2s. P. 223–228. URL: https://bildbd.com/index.php/blj/article/view/296 (Last accessed: 10.01.2023).

16. Берназюк І. М. Захист права на повагу до приватного й сімейного життя у практиці Європейського суду з прав людини. *Вчені записки ТНУ імені В. І. Вернадського. Сер. Юридичні науки.* 2020. Т. 31(70), № 4. С. 104–110.

17. Pohle J. Social Networks, Functional Differentiation of Society, and Data Protection. Cornell University, 2012. URL: https://arxiv.org/abs/1206.3027 (Last accessed: 10.01.2023).

18. Beldad A., de Jong M., Steehouder M. A Comprehensive Theoretical Framework for Personal Information-Related Behaviors on the Internet. *The Information Society*. 2011. Vol. 27, No 4. P. 220–232. DOI: https://doi.org/10.1080/01972243.2011.583802

19. Конституція України : Закон України від 28 черв. 1996 р. № 254к/96-ВР. URL: http://zakon.rada.gov.ua/cgibin/laws/main.cgi?page=1&nreg=254%EA%2F96-%E2%F0 (дата звернення: 10.01.2023).

20. Kalashnikova E. B. Personal Data Protection as a Basis of Digitalization. *Digital Technologies in the New Socio-Economic Reality* / eds. S. I. Ashmarina, V. V. Mantulenko. Cham : Springer, 2022. P. 73–79. DOI: https://doi.org/10.1007/978-3-030-83175-2_11

21. Загальний регламент про захист даних (GDPR) : Регламент Європейського Союзу № 2016/679. URL: https://ips.ligazakon.net/document/MU16144 (дата звернення: 10.01.2023).

22. GDPR: How Does it Affect Social Media? *Reciprocity* : website. URL: https://reciprocity.com/blog/gdpr-how-does-it-affect-social-media/ (Last accessed: 10.01.2023).

23. Zou M. Rethinking online privacy in the Chinese workplace: Employee dismissals over social media posts. *Made in China Journal*. Vol. 3, No 3. P. 50–55. URL: https://search.informit.org/doi/10.3316/informit.035341078913123 (Last accessed: 10.01.2023).

24. Fortes V. B., Oro Boff S., Galindo Ayuda F. The fundamental right to privacy in brazil and the internet privacy rights in regulating personal data protection. *Revista Eletrônica Do Curso De Direito Da UFSM.* 2016. Vol. 11, No 1. P. 24–48. DOI: https://doi.org/10.5902/1981369419706

25. Lemke C., Brenner W. Mensch und Gesellschaft im digitalen Zeitalter. *Einführung in die Wirtschaftsinformatik.* Heidelberg : Springer Gabler, 2015. DOI: https://doi.org/10.1007/978-3-662-44065-0_3

26. Al-Khalidy M. K. J., Aziz Y. M. The Applications of The Right to Be Forgetting. *Qalaai Zanist Journal*. 2022. Vol. 7, No 1. P. 938–955. DOI: https://doi.org/10.25212/lfu.qzj.7.1.37

27. Sadiya S., Hasan S. The Right to Privacy in Bangladesh in the Context of Technological Advancement. *International and Comparative Law Journal*. 2018. Vol. 1, No 2. DOI: http://dx.doi.org/10.2139/ssrn.3298069

28. Eskens S. The personal information sphere: An integral approach to privacy and related information and communication rights. *Journal of the Association for Information Science and Technology*. 2020. Vol. 71. P. 1116–1128. DOI: https://doi.org/10.1002/asi.24354

29. Heinemann M. J., Heinemann D. Postmortaler Datenschutz. *Datenschutz Datensich*. 2013. Vol. 37. P. 242–245. DOI: https://doi.org/10.1007/s11623-013-0085-2

30. Kathure M. The Confluence between Social Networking Sites, Data and Privacy. *SSRN* : website. DOI: http://dx.doi.org/10.2139/ssrn.3554250