СЕКЦІЯ 1
ЦИФРОВІ ПРАВА ГРОМАДЯНИНА ЯК ЗДІЙСНЕННЯ УНІВЕРСАЛЬНИХ ПРАВ ЛЮДИНИ У ЦИФРОВОМУ СЕРЕДОВИЩІ: ДОСВІД ЄС ДЛЯ УКРАЇНИ

Модератори секції: Воронкова Валентина – д.філос.н., проф.,
Мар'єнко Вікторія – аспірантка спеціальності 033 «Філософія»,
Бугайчук Оксана – аспірантка спеціальності 033 «Філософія».

DOI https://doi.org/10.36059/978-966-397-447-7-1

УДК 342.727:004.738.5:004.056

ВОРОНКОВА ВАЛЕНТИНА ГРИГОРІВНА,
д.філос.н., проф., завідувач кафедри управління та адміністрування
Інженерний навчально-науковий інститут ім. Ю. М. Потебні
Запорізького національного університету (м. Запоріжжя, Україна)
E-mail: valentinavoronkova236@gmail.com
ORCID ID: http://orcid.org/ 0000-0002-0719-1546

НІКІТЕНКО ВІТАЛІНА ОЛЕКСАНДРІВНА,
д.філос.н., проф., проф. кафедри управління та адміністрування
Інженерний навчально-науковий інститут ім. Ю. М. Потебні
Запорізького національного університету (м. Запоріжжя, Україна)
E-mail: vitalina2006@ukr.net
ORCID ID: https://orcid.org/0000-0001-9588-7836

КИВЛЮК ОЛЬГА ПЕТРІВНА,
д.філос.н., проф., завідувач кафедри філософії та психології, Київський університет інтелектуальної власності та права Національного університету «Одеська юридична академія» (м. Київ, Україна)
E-mail: panyolga@ukr.net
ORCID ID: https://orcid.org/0000-0002-7900-9299 (м. Київ)

ЦИФРОВІ ПРАВА ЯК ЧИННИК ЦИФРОВІЗАЦІЇ СУСПІЛЬСТВА ТА ІНТЕГРАЦІЇ В ГЛОБАЛЬНИЙ ІНФОРМАЦІЙНИЙ ПРОСТІР

Актуальність дослідження цифрових прав людини має велике значення для захисту прав людини у цифрову епоху, так як має бути досягнутий міжкультурний діалог у суспільстві, проте, щоб реалізувалося дане право

необхідно реагувати на оцифрування, щоб правова система має бути відповідним чином реструктурована. В результаті розвитку цифрового права як науки деякі вчені почали досліджувати вплив інформаційних/цифрових технологій на людську онтологію та епістемологію. Сьогодні людське тіло є тілом постмодерністського суспільства у сенсі розвитку цифрового суспільства та культури. Існування людини у вимірі інформаційних/цифрових технологій – це існування «біологічної людини» з «цифровими атрибутами», у результаті чого формується «інформаційна особистість», яка є відображенням біологічної особистості в цифровому просторі і належить до інформаційної ідентичності [1].

«Портрет» особистості, що сформований з цифрових даних на просторах всесвітньої мережі Інтернет, використовується та узагальнюється для аналізу поведінки людей в цифровому суспільстві, що визначає сталий образ особистості – «інформаційно-цифровий портрет». Прискорення розвитку інформаційних/цифрових технологій, з одного боку, прискорює/спрощує життя людей, а з іншого боку, призводить до зростаючої залежності людей від цих технологій. Тому сьогодні цифровізація стала найактуальнішою темою на хвилі інформаційної революції, вона є динамічним процесом розвитку цифрового суспільства. Цифрове суспільство сформувалося як складний соціальний феномен і почало еволюціонувати – від двовимірного до тривимірного, від фрагментів до цілого, «розмиваючи» межі реального та віртуального. Цифрова «ерозія» на різних етапах стала проявлятися в існуванні, реалізації соціальної діяльності людини на основі інформації, даних та кодів, що поступово сформувало «цифрові атрибути» людини, які виявилися чинником посилення цифровізації та інтелектуалізації [2].

Процес розвитку цифрового суспільства насправді є процесом взаємної трансформації цифровізації соціальної діяльності людини та – «цифрових атрибутів» людини. Таким чином, цифровізація реалізувала накопичення інформаційних ресурсів/даних, циркуляцію та агрегацію цих ресурсів/даних, а інтелект здійснив інтеграцію. Цифровізація соціальної діяльності людини та її «цифрові атрибути» становлять два аспекти розвитку цифрового суспільства. Хоча цифровізація соціальної діяльності людей створила цифрове суспільство, вона також вплинула на самих людей [3].

Навколо концепції «цифрових прав людини» розгорнулися дискусії в академічних колах. Прихильники даної теорії зазначають, що «цифрові права людини» є оновленням та удосконаленням традиційних прав людини і становлять четверте покоління прав людини. Критики вважають, що «цифрові права людини» не мають нових характеристик, специфічної моральної основи, не можуть бути виправдані як основне право. Таким

чином, «цифрові права людини» стали представляти новий тип модернізації прав людини – як четвертого покоління прав людини, що походить від існуючого поняття прав людини». Ми намагалися проаналізувати питання про те, чи створюють «цифрові права людини» четверте покоління прав людини, чи певною мірою є питанням політичного судження, чи «цифрові права людини» вже мають характеристики нового типу прав людини. Деякі вчені наголошують, що «цифрові права людини» можуть задовольнити прагнення людей до кращого життя, посилити обов'язкову силу закону щодо наукової та технічної етики та зміцнити систему дискурсу юридичних кіл у міжнародному співтоваристві. Також існує думка, що «цифрові права людини» – це зовсім новий термін, новий тип права, який виник в епоху великих даних, цифрових послуг, цифрової інфраструктури тощо. Суб'єкти прав «цифрових прав людини» включають як окремих осіб, так і колективи, суб'єкти зобов'язань в основному вказують на підприємства і деякі державні установи з цифровими правами, а взаємодія суб'єктів прав і обов'язків являють собою синтез/інтеграцію відповідних процесів [4].

Перше покоління прав людини – це громадянські та політичні права, включаючи права на життя, рівність, свободу слова, релігії, власності та права голосу, які в основному відображені у статтях з 3 по 21 Загальної декларації прав людини 1948 року. Міжнародний пакт про громадянські та політичні права 1953 р. та Європейська конвенція про права людини 1953 р.

Права людини другого покоління – це економічні та соціальні права, у тому числі права на працевлаштування, права на соціальне забезпечення та права на добробут, які в основному відображені у статтях 22–28 Загальної декларації прав людини та Міжнародного пакту про економічні, соціальні та культурні права. Права прийняті в 1966 р.

«Права третього покоління – це колективні права і права солідарності, такі як право на самовизначення, екологічні права, права дітей і корінних народів, які в основному відображені в міжнародних договорах, таких як Стокгольмська декларація Конференції Організації Об'єднаних Націй, прийнятої в 1972 р.». Поділ К. Васака прав людини між трьома поколіннями має відносно різні політичні цілі.

Деякі вчені ставлять під сумнів дану теорію з погляду історичного поділу, природи прав та пріоритету прав. Вказують на те, що тимчасова вісь теорії прав людини між поколіннями не відповідає історії. Є точка зору, що еволюція – концепцій прав людини в історії не збігається з розвитком теорій прав людини в межах поколінь. Як свідчить аналіз, цифрові права – це права людини у всесвітній мережі Інтернет, що стосуються

доступу, участі, безпеки даних та конфіденційності, цінностей, орієнтованих на людину, таких як гідність, повага, рівність, справедливість, відповідальність, згода та екологічна стійкість. Існують різні глобальні, регіональні та місцеві ініціативи, які роз'яснюють різні елементи цифрових прав. Хартія прав людини в Інтернеті та Хартія прав людини та принципів в Інтернеті, розроблені Динамічною коаліцією з прав та принципів в Інтернеті на Форумі ООН з управління Інтернетом (IGF). Обидві хартії визначають, як слід інтерпретувати стандарти прав людини стосовно онлайнсередовища. Африканська декларація прав і свобод в Інтернеті – це загальнорегіональна декларація, в якій викладаються принципи, необхідні для захисту прав людей в Інтернеті, створення онлайн-середовища, яке найкраще відповідає потребам та цілям соціального та економічного розвитку Африки. У 2015 році громадянське суспільство на Філіппінах оприлюднило Філіппінську декларацію про права та принципи Інтернету, краудсорсингову декларацію, яка відображає мрії, надії та сподівання філіппінців щодо того, яким має бути Інтернет. Організація Об'єднаних Націй з питань освіти, науки та культури (ЮНЕСКО) у 2015 році фактично визначила понад 50 декларацій та структур, пов'язаних з Інтернетом. У тому ж році Центр досліджень Інтернету та суспільства Беркмана Кляйна визначив 30 таких конституцій та список із 42 прав, розділивши їх на сім тем. У цих рамках свобода вираження поглядів, право на недоторканність приватного життя і право на доступ до Інтернету були трьома темами, що найчастіше згадуються. Іншими важливими темами є свобода інформації, прозорість та відкритість процесів та мереж управління Інтернетом [5].

У 1997 році американський активіст Роберт Б. Гельман (Robert B. Gelman) висунув проєкт «Декларації прав людини в кіберпросторі», заснований на «Загальній декларації прав людини», висунув концепцію «прав людини в кіберпросторі». У 2014 році Європейська комісія прийняла «Посібник з прав людини користувачів Інтернету», який спрямований на захист прав та свобод користувачів Інтернету, що включає ряд мережевих прав для користувачів Інтернету. У грудні 2016 року 27 німецьких експертів опублікували Хартію цифрових основних прав Європейського Союзу (Charter of Digital Fundamental Rights of the European Union). Виходячи з цього, деякі країни (Іспанія) та міжнародні організації (Європейська комісія) послідовно видали «Декларації» та «Хартії» про цифрові права. В представленому дослідженні ми орієнтуємося на документи міжнародних організацій, які досліджують проблему цифрових прав людини, а також на праці українських та іноземних вчених: Р. Андрюкайтене, В. Воронкової, О. Кивлюк, В. Нікітенко, Р. Олексенка, А. Череп, О. Черепа, М. Гудмена, П. Діамандіса, Д. Левітіна, Роберт Б. Гельмана та інших.

Веклику роль сьогодні відіграє вирішення проблем цифрових прав людини та громадянина, що включають: 1) Конфіденційність і захист персональних даних, в основі якої захист приватності в умовах масового збору даних компаніями та державними органами: роль регуляторів (наприклад, GDPR у ЄС або законодавства України) у захисті персональної інформації: виклики у забезпеченні прозорості обробки даних і права «бути забутим». 2) Доступ до інтернету як базове право, так як Інтернет є невід'ємною частиною сучасного життя та базовим правом людини, що вимагає усунення цифрової нерівності між міськими і сільськими регіонами, для чого слід розвивати державні програми з розвитку цифрової інфраструктури та забезпечення доступу до інтернету. 3) Свобода вираження та боротьба з цензурою, в основі якої право громадян на вільне вираження думок у цифровому просторі; проблеми дезінформації, мови ненависті та маніпуляцій у соціальних мережах: регулювання контенту: баланс між свободою слова та необхідністю контролю. 4) Цифрова безпека та кіберзахист, що включає захист від кібератак, зломів і крадіжок даних: освітні програми для підвищення рівня кіберграмотності громадян, підвищення ролі держави та приватних компаній у забезпеченні цифрової безпеки. 5) Етичне використання технологій та штучного інтелекту, шо включає використання алгоритмів і штучного інтелекту, в основі яких захист від дискримінації та упередженості; відкритість та прозорість у роботі автоматизованих систем ухвалення рішень: забезпечення права на пояснення рішень, ухвалених технологіями [6]. Ці теми особливо актуальні в Україні в умовах активної цифровізації суспільства та економіки, а також інтеграції в глобальний інформаційний простір.

Список використаних джерел:

1. Воронкова Валентина, Кивлюк Ольга, & Андрюкайтене Регіна. Еволюція від активного відповідального громадянства до цифрового в контексті критичного мислення: досвід країн ЄС. *Humanities studies* : Collection of Scientific Papers / Ed. V. Voronkova. Zaporizhzhia : Publishing house"Helvetica", 2023. 14(91). P. 23–34.

2. Воронкова Валентина, Нікітенко Віталіна. Проблема трансформації людини у контексті трансгуманізму: методологія цифрової антропології. *Humanities studies :* Collection of Scientific Papers. Zaporizhzhia : Publishing house "Helvetica", 2023. Вип. 16(93). P. 9–17.

3. Воронкова В. Г., & Нікітенко В. О. Креативне місто як чинник розвитку цифрового суспільства. Комунальне господарство міст. Харків, 2022. Том 2. Вип169(2022): Серія: Економічні науки. С. 57–64.

4. Кивлюк Ольга, Воронкова Валентина, & Андрюкайтене Регіна. Інтелектуальна власність у контексті креативних індустрій, економіки та мислення (на прикладі країн Євросоюзу). *Humanities studies :* Collection of Scientific Papers. Zaporozhzhia : Publishing house "Helvetica", 2022. Вип. 13(90). P. 74–86.

5. Кивлюк О. П., Воронкова В. Г., Нікітенко В. О. Цифрові права людини як вираження цифрових атрибутів: соціально-філософське обґрунтування. Освітній дискурс: збірник наукових праць / голов. ред. О. П. Кивлюк. Київ : ТОВ Науково-інформаційне агентство «Наука-технології-інформація». 2023. Випуск 44(4–6). С. 7–22.

6. Коломоєць Тетяна, Верлос Наталя, Нікітенко Віталіна, Воронкова Валентина, Цифрові права в умовах розвитку штучного інтелекту та глобалізації: виклики та можливості. *Humanities studies :* Collection of Scientific Papers / Ed. V. Voronkova. Zaporizhzhia : Publishing house "Helvetica", 2024. 19(96). P. 207–217.

УДК 342.7

ГОСТІЧКО БОГДАН РУСЛАНОВИЧ,
студент І курсу факультету суспільних наук та міжнародних відносин
Дніпровський національний університет імені Олеся Гончара
(м. Дніпро, Україна)
E-mail: bogdan.gostichko@gmail.com
Науковий керівник: **Капітаненко Наталія Петрівна,**
д.юрид.н., доц., доцент кафедри теорії держави і права,
конституційного права та державного управління
Дніпровський національний університет імені Олеся Гончара
(м. Дніпро, Україна)
E-mail: kapitanenko.np@gmail.com
ORCID ID: http://orcid.org/0000-0002-1475-5784

ОСОБЛИВОСТІ ЗАХИСТУ СЛУЖБОВОЇ ІНФОРМАЦІЇ В УМОВАХ ВОЄННОГО СТАНУ

Захист службової інформації є одним із ключових аспектів забезпечення національної безпеки. В умовах воєнного стану в Україні, введеного відповідно до Закону України «Про затвердження Указу Президента України «Про введення воєнного стану в Україні» від 24 лютого 2022 р. [6] та Указу Президента України «Про введення воєнного стану в Україні» від 24 лютого 2022 р. № 64/2022 [4], важливість конфіденційності, цілісності та доступності інформації стає критичною для сфери публічного управління, ефективного управління військовими силами та іншими стратегічними установами. Враховуючи сучасні технологічні виклики та постійну загрозу з боку агресора, організація захисту службової інформації вимагає комплексного підходу, що включає як технічні, так і організаційні заходи,

спрямовані на мінімізацію ризиків і забезпечення стабільної роботи в екстремальних умовах.

Метою дослідження є аналіз особливостей захисту службової інформації в умовах воєнного стану на основі аналізу нормативно-правових актів та наукових джерел.

Інститут службової таємниці є одним з найбільш складних в інформаційних правовідносинах. Його розвиток супроводжується постійними змінами у термінології, практики застосування відповідних нормативно-правових норм та захисті інформації, що відноситься до службової. На цей час в українському законодавстві не можна знайти однозначного визначення службової інформації. Закон України «Про інформацію» від 2 жовтня 1992 року поділяє інформацію з обмеженим доступом на три види: а) конфіденційну інформацію, б) таємну інформацію, в) службову інформацію (ст. 21) [3]. У свою чергу відповідно до ст. 9 Закону України «Про доступ до публічної інформації» від 13 січня 2011 року, до службової інформації може належати, окрім зібраної в процесі оперативно-розшукової, контррозвідувальної діяльності та у сфері оборони країни, яку не віднесено до державної таємниці, лише інформація, що міститься в документах суб'єктів владних повноважень, які становлять внутрівідомчу службову кореспонденцію, доповідні записки, рекомендації, якщо вони пов'язані з розробкою напряму діяльності установи або здійсненням контрольних, наглядових функцій органами державної влади, процесом прийняття рішень і передують публічному обговоренню та/або прийняттю рішень [5].

У рекомендаціях Уповноваженого Верховної Ради України з прав людини з питань додержання конституційного права людини і громадянина зазначено, що під внутрішньовідомчою службовою кореспонденцією варто розуміти будь-який документ незалежно від його назви та реквізитів, який підготовлений будь-якою особою (службовцем) усередині суб'єкта владних повноважень та адресатом якого є інша особа чи структурний підрозділ цього суб'єкта владних повноважень. Отже, листування з іншим суб'єктом владних повноважень чи будь-якими іншими фізичними або юридичними особами не можна вважати «внутрішньовідомчою» кореспонденцією [7]. При цьому цей документ повинен мати службовий характер, тобто бути пов'язаним із роботою суб'єкта владних повноважень. Водночас під «відомством» варто розуміти не тільки центральний апарат органу влади, але і його територіальні підрозділи.

Відповідно до чинного законодавства кожен орган державної влади має право самостійно визначати інформацію, віднесену до службової. Документам, що містять інформацію, яка становить службову інформацію,

присвоюється гриф «для службового користування». Обов'язковість присвоєння грифу пояснюється необхідністю особливого обліку та зберігання таких документів. Гриф представляється як матеріальним носіям службової інформації, так і документам в електронній формі.

У вітчизняному законодавстві, визначають правники, закріплюється перелік орієнтовних критеріїв віднесення до службової інформації, які повинні: створюватися за кошти державного бюджету або перебувати у володінні, користуванні чи розпорядженні організації; використовуватися з метою забезпечення національних інтересів держави; не належати до державної таємниці; внаслідок розголошення такої інформації можливе: порушення конституційних прав і свобод людини та громадянина; настання негативних наслідків у внутрішньополітичній, зовнішньополітичній, економічній, військовій, соціальній, гуманітарній, науково-технологічній, екологічній, інформаційній сферах та у сферах державної безпеки і безпеки державного кордону; створення перешкод у роботі державних органів [2].

Робота з документами, які містять службову інформацію, здійснюється відповідно до Типової Інструкції про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію, затвердженої Постановою Кабінету Міністрів України від 19 жовтня 2016 р. № 736. Ця Інструкція визначає єдині вимоги до ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію, зібрану під час провадження оперативно-розшукової, контррозвідувальної діяльності, діяльності у сфері оборони держави, та іншу службову інформацію, в органах державної влади, інших державних органах, органах влади Автономної Республіки Крим [8].

Категорія службової інформації використовується не лише в Україні, а й у багатьох розвинених країнах для захисту внутрішньої інформації державних установ. Наприклад, у Німеччині діє гриф «для службового користування», а в США службова інформація охоплює також комерційну таємницю і ноу-хау. Поширення таких даних без дозволу карається застосуванням до правопорушника кримінальної відповідальності [1].

Незважаючи на відсутність чіткого регулювання службової інформації, її обіг частково регламентується українськими законами. Прийняття окремого закону, особливо в умовах воєнного стану, створило б правову основу для систематизації обігу та безпеки службових відомостей, сприяючи збалансуванню права громадян на доступ до інформації та захисту державної і приватної безпеки.

В умовах воєнного стану мають встановлюватися чіткі вимоги до обробки, зберігання та передачі службової інформації з додатковим

захистом окремих категорій даних; посилюватися відповідальність за розголошення чи неправомірне використання інформації, включаючи кримінальну відповідальність за дії, що загрожують національній безпеці; необхідно ввести обмеження на використання незахищених засобів зв'язку, програм та пристроїв. Співпраця з правоохоронними органами та військовими структурами забезпечуватиме оперативне реагування на загрози та правопорядок у сфері інформаційної безпеки.

Отже, захист службової інформації в умовах воєнного стану є критично важливим компонентом забезпечення національної безпеки. Наявні проблеми, зокрема недосконаліть законодавчої бази, застарілі методи захисту та недостатній рівень впровадження сучасних технологій, вимагають негайного реагування держави для забезпечення інформаційної безпеки суспільства.

Список використаних джерел:

1. Галинська К. Ю. Забезпечення безпеки службової інформації в Україні: правові аспекти. *Недержавний сектор безпеки: сучасний досвід та проблеми порівняльно-правового регулювання* : тези доп. учасників II Міжнар. наук.-практ. конф. 19 квіт. 2014 р. Харків, 2014. С. 21–23.
2. Жмур Н. Захист службової інформації: стан законодавства. *Підприємництво, господарство і право*. 2013. № 7. С. 158–161.
3. Про інформацію: Закон України від 02 жовтня 1992 р. *Відомості Верховної Ради України.* 1992. № 48. ст. 650.
4. Про введення воєнного стану в Україні : Указ Президента України від 24 лютого 2022 р. № 64/2022. URL: https://zakon.rada.gov.ua/laws/show/64/2022#Text (дата звернення: 18.11.2024).
5. Про доступ до публічної інформації : Закон України від 13.01.2011 р. *Відомості Верховної Ради України*. 2011. № 32. ст. 314.
6. Про затвердження Указу Президента України «Про введення воєнного стану в Україні : Закон України від 24 лютого 2022 р. URL: https://zakon.rada.gov.ua/laws/show/2102-20#Text (дата звернення: 18.11.2024).
7. Рекомендації Уповноваженого Верховної Ради України з прав людини з питань додержання конституційного права людини і громадянина. URL: https://rm.coe.int/recomendations-final-10-02-21/1680a165f7.
8. Типова інструкція про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію : затверджена Постановою Кабінету Міністрів України від 19 жовтня 2016 р. № 736. URL: https://zakon.rada.gov.ua/laws/show/736-2016-%D0%BF#Text (дата звернення: 18.11.2024).

УДК 342.7

КАПІТАНЕНКО НАТАЛЯ ПЕТРІВНА,
д.юрид.н., доц., доцент кафедри теорії держави і права,
конституційного права та державного управління
Дніпровський національний університет імені Олеся Гончара
(м. Дніпро, Україна)
E-mail: kapitanenko.np@gmail.com
ORCID ID: http://orcid.org/0000-0002-1475-5784

ОБМЕЖЕННЯ ІНФОРМАЦІЙНИХ ПРАВ: ЗАРУБІЖНИЙ ДОСВІД

Інформація як феномен цивілізації стала базою формування сучасного інформаційного суспільства. Кожен має право користуватися перевагами такого суспільства, реалізуючи права та свободи в інформаційній сфері. Стрімкий розвиток інформаційно-комунікаційних технологій та запровадження їх в життя сприяли появі, формуванню та подальшому розвитку інституту інформаційних прав, а в подальшому й інформаційного права. Інформація виступає як засіб реалізації прав та свобод людини. В той же час, в окремих випадках можуть встановлюватися обмеження прав та свобод, в тому числі й інформаційних, із зазначенням дії цих обмежень. Встановлення умов та підстав обмеження інформаційних прав з позицій верховенства права на основі аналізу норм міжнародних актів є важливим для українського суспільства. Для української спільноти в умовах воєнного стану актуально ознайомитися з умовами та підставами обмеження інформаційних прав для вдосконалення вітчизняного законодавства в зазначеній царині.

Серед науковців, що займалися дослідженнями інформаційних прав, слід назвати дослідження: І. Арістової, О. Баранова, І. Бачило, К. Бєлякова, В. Брижка, В. Бутузова, В. Воронкової, 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 та інших.

Метою дослідження є встановлення умов та підстав обмеження інформаційних прав на основі аналізу міжнародних і регіональних правових актів та наукових джерел.

Цивілізація як соціальна система, яка перебуває у стані постійного самовдосконалення, прагнучи гармонії, потребує соціального порядку. Для успішного подальшого саморегулювання цивілізація, її підсистеми та елементи повинні дотримуватись правових норм як найбільш ефективних

засобів соціального регулювання [2, с. 9]. Право на інформацію, як одне з основних прав людини, містили Декларація прав людини і громадянина (Déclaration des Droits de l'Homme et du Citoyen, 1789 р.) та Біль про права (Bill of Rights, 1791 р.), визнаючи їх важливість для людини, що підтверджує віднесення права на інформацію до основних загальновизнаних громадянських і політичних прав. Інформаційні права є відносно новим явищем, яке виникло завдяки розвитку інформаційно-комунікаційних технологій та формуванню інформаційного суспільства [6].

Встановлення умов та підстав обмеження інформаційних прав в умовах значної залежності сучасного суспільства від інформаційно-комунікаційних технологій є актуальним для глобального світу, держави, суспільства і людини. Чинні міжнародні акти містять відповідні положення. Так, ч. 2 ст. 29 Загальної декларації прав людини визнає загальні підстави для обмеження прав людини, зазначаючи, що «при здійсненні своїх прав і свобод кожна людина повинна зазнавати тільки таких обмежень, які встановлені законом виключно з метою забезпечення належного визнання і поваги прав і свобод інших та забезпечення справедливих вимог моралі, громадського порядку і загального добробуту в демократичному суспільстві» [1]. Міжнародний пакт про громадянські та політичні права (1966 р.) вже безпосередньо розглядає право кожної людини на безперешкодне дотримування своїх поглядів та вільне вираження свого погляду, визнаючи, що користування вказаними правами накладає особливі обов'язки та особливу відповідальність. Саме тому це право може бути пов'язане з певними обмеженнями, які «мають бути встановлені законом і бути необхідними: 1) для поважання і репутації інших осіб; 2) для охорони державної безпеки, громадського порядку, здоров'я чи моральності населення» (ст. 19) [5]. Відповідно, цим пактом було акцентовано увагу на особливості вказаних прав і конкретизовано перелік умов та підстав їх обмеження.

Європейська конвенція з прав людини (Конвенція про захист прав людини і основоположних свобод, 1950 р.) містить декілька статей, які визначають інформаційні права та умови їх обмеження, а саме: публічність проголошення судового рішення в умовах закритого судового засідання в демократичному суспільстві задля захисту моралі, громадського порядку, національної безпеки, інтересів неповнолітніх або приватного життя сторін; обмеження допускається лише за рішенням суду, якщо це строго необхідно для захисту правосуддя (ст. 6); втручання органів влади у здійснення права на повагу до приватного та сімейного життя дозволене лише законом і лише в інтересах безпеки, порядку, здоров'я, моралі чи захисту прав інших осіб і є необхідним в демократичному суспільстві (ст. 8); право на свободу вираження поглядів може підлягати обмеженню,

що встановлено законом і є необхідним в демократичному суспільстві «в інтересах національної безпеки, територіальної цілісності або громадської безпеки, для запобігання заворушенням чи злочинам, для охорони здоров'я чи моралі, для захисту репутації чи прав інших осіб, для запобігання розголошенню конфіденційної інформації або для підтримання авторитету і безсторонності суду» (ст. 10) [4]. Також Європейська конвенція з прав людини встановлює можливість для відступу для зобов'язань країнами під час війни чи іншої суспільної небезпеки відповідно до пропорційності загроз за умови, що такі заходи не протирічать іншим її зобов'язанням. Важливим є встановлення меж обмежень прав людини – лише для тих цілей, які визначені в законі.

Отже, здійснений аналіз вказаних міжнародних та регіональних правових актів надає можливість встановити умови та підстави обмеження інформаційних прав. Передусім, варто зазначити, що обмеження інформаційних прав в суспільстві може відбуватися лише з позицій верховенства права як одного з принципів демократичного суспільства і який полягає у пануванні права в суспільному житті [3].

До умов, за яких можливе обмеження інформаційних прав, варто віднести: 1) обмеження прав має встановлюватися законом; 2) закон має містити положення про строк обмеження прав; 3) обов'язково в законі має бути зазначена ціль обмеження прав і використання лише у відповідності до цілі; 4) пропорційність обмеження прав реальним загрозам в демократичному суспільстві; 5) застосування обмеження прав як необхідного, єдиного допустимого заходу для досягнення легітимної мети державою; 6) діяння в межах, необхідних для забезпечення громадського порядку.

Обмеження інформаційних прав можуть бути встановлені задля: поважання і репутації інших осіб; охорони державної безпеки, громадського порядку; охорони здоров'я чи моральності населення; захисту моралі, національної безпеки; захисту інтересів неповнолітніх або приватного життя сторін; територіальної цілісності або громадської безпеки; запобігання заворушенням чи злочинам; захисту репутації чи прав інших осіб; запобігання розголошенню конфіденційної інформації; підтримання авторитету і безсторонності суду.

Таким чином, норми міжнародних та регіональних правових актів передбачають умови та підстави обмеження інформаційних прав у суспільстві, які мають бути обґрунтованими, тимчасовими, пропорційними та підконтрольними. Важливо зберігати баланс між обмеженням інформаційних прав та забезпеченням безпеки людини, суспільства і держави. Українське законодавство щодо обмеження інформаційних прав має базуватися на положеннях міжнародних договорів, які є частиною національного законодавства України.

Список використаних джерел:

1. Загальна декларація прав людини від 10.12.1948 р. URL: https://zakon.rada.gov.ua/laws/show/995_015#Text (дата звернення: 19.11.2024).
2. Капітаненко Н. П. Адміністративно-правове регулювання у сфері реалізації права інтелектуальної власності: стан, проблеми, перспективи : монографія / Н. П. Капітаненко. Одеса : Видавничий дім «Гельветика», 2021. 412 с.
3. Каталог юридичних позицій Конституційного Суду України (за рішеннями, висновками). URL: https://ccu.gov.ua/storinka-knygy/34-verhovenstvo-prava (дата звернення: 19.11.2024).
4. Конвенція про захист прав людини і основоположних свобод, затверджена Радою Європи 4 листопада 1950 року. URL: https://zakon.rada.gov.ua/laws/show/995_004#Text (дата звернення: 19.11.2024).
5. Міжнародний пакт про громадянські та політичні права, затверджений Генеральною Асамблеєю ООН 16 грудня 1966 року. URL: https://zakon.rada.gov.ua/laws/show/995_043
6. Сухорольский П. М. Проблеми забезпечення та розвитку прав людини в умовах інформаційного суспільства. *Український часопис міжнародного права.* 2013. № 1. С. 18–23.

УДК 342.7

КОЗАКОВА МАША ОЛЕГІВНА,
студентка І курсу факультету суспільних наук та міжнародних відносин
Дніпровський національний університет імені Олеся Гончара
(м. Дніпро, Україна)
E-mail: kozakova.m.o@gmail.com
Науковий керівник: **Капітаненко Наталія Петрівна,**
д.юрид.н., доц., доцент кафедри теорії держави і права,
конституційного права та державного управління
Дніпровський національний університет імені Олеся Гончара
(м. Дніпро, Україна)
E-mail: kapitanenko.np@gmail.com
ORCID ID: http://orcid.org/0000-0002-1475-5784

РОЛЬ ІНФОРМАЦІЇ В ПРОФЕСІЙНІЙ ДІЯЛЬНОСТІ ДЕРЖАВНИХ СЛУЖБОВЦІВ

Значення інформації в сучасному суспільстві важко переоцінити. У даний час інформатизація суспільства проходить досить стрімко, а у сфері публічного управління помітно збільшується потік найрізноманітнішої

інформації, вдосконалюються засоби і способи її передачі, обробки та зберігання. Інформація є основним ресурсом для державних службовців, забезпечуючи обґрунтованість управлінських рішень. Збільшення обсягу даних та необхідність їх захисту, точності й доступності створюють нові виклики в умовах цифровізації публічного управління.

Науковці акцентують увагу на важливості інформаційної грамотності, сучасних технологій та управління даними у державному секторі. Однак практичні аспекти адаптації до цих змін ще потребують дослідження

Основна мета – аналіз значення інформації у діяльності держслужбовців, її впливу на рішення, визначення вимог до компетентності та факторів ефективного використання інформаційних ресурсів у державному управлінні.

Закон України «Про інформацію» від 2 жовтня 1992 року визначає інформацію як відомості або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді [4]. Важливо, що кожен має право на отримання, використання, поширення, зберігання та захист інформації для реалізації своїх прав, свобод і законних інтересів.

У силу розвитку процесів інформатизації публічного управління державні службовці залучені в цілу систему інформаційних правовідносин, що зумовлює необхідність вдосконалення інформаційного обміну, розробки нових моделей правового регулювання та підвищення прозорості діяльності органів влади.

Недоліки в інформаційному забезпеченні професійної діяльності державних службовців роблять їх роботу малоефективною. У зв'язку з цим інформаційну взаємодію державних службовців із громадянами та господарюючими суб'єктами повинно бути поставлено на принципово новий рівень, який буде відповідати розвитку процесів диджиталізації.

Однією з передумов сталого демократичного розвитку суспільства є інформаційна відкритість органів публічної влади. Саме прозорість дій влади є головною запорукою здійснення ефективної політики, уможливлення громадського контролю і зміцнення довіри до себе з боку людей. У всіх демократичних країнах влада зобов'язана виконувати чіткі процедури інформування громадян про свою діяльність і використовувати механізми залучення громадськості до формування державної політики та до оцінювання якості її реалізації [3, с. 6]. Однак публічність державної служби не має переходити межі службової інформації чи державної таємниці.

Впровадження інноваційних перетворень в Україні в умовах розвитку інформаційних технологій передбачає використання сучасних форм і методів роботи, які базуються на електронному обміні інформацією.

Швидка та якісна обробка інформації органами державної влади, органами місцевого самоврядування, комерційними та некомерційними суб'єктами господарювання надає можливість прискорити отримання інформації, її опрацювання та прийняття найбільш оптимального рішення [2].

Важливим моментом при використанні інформаційних технологій для управління державою є не тільки культура та інтелект суспільства в цілому, але й культура та інтелект державних службовців. В цьому контексті варто звернутися до важливості формування цифрових компетентностей у державних службовців відповідно до Концепції розвитку цифрових компетентностей, схваленої розпорядження Кабінету Міністрів України від 3 березня 2021 р. № 167-р. Відповідно до зазначеного розпорядження «цифровою компетентністю є динамічна комбінація знань, умінь, навичок, способів мислення, поглядів, інших особистих якостей у сфері інформаційно-комунікаційних та цифрових технологій, що визначає здатність особи успішно соціалізуватися, провадити професійну та/або подальшу навчальну діяльність із використанням таких технологій» [5].

Актуальність формування цифрових компетенцій для професійної діяльності державних службовців обумовлена: змінами ролі, місця, функцій та завдань органів публічної влади в умовах глобалізації, розбудови громадянського та інформаційного (цифрового) суспільства, побудови сервісної та цифрової держави; активізацією участі громадян і бізнесу у формуванні і реалізації публічної влади; масштабним впровадженням ІКТ в усі сфери життєдіяльності особи, суспільства та держави, у тому числі, в публічне управління та адміністрування, а також та новими можливостями щодо їх використання; пріоритетами та політики, у тому числі з використанням сучасних ІКТ, їх цифрових комунікацій з органами завданнями державної політики цифрових трансформацій та цифровізації, визначеними національним законодавством та міжнародними зобов'язаннями України; недостатнім рівнем обізнаності та готовністю публічних службовців та громадян до впровадження та застосування сучасних ІКТ, інструментів е-урядування та е-демократії.

Згідно дослідження ООН "E-Government Survey 2022» Україна у 2022 році за рейтингом е-уряду (індекс EGDI) Україна зайняла: у 2022 році 46 місце серед 193 країн світу, у 2020 році – 69, у 2018 році – 82 місце, у 2016 – 62 місце. Лідери 2022 року: Данія, Фінляндія та Південна Корея. EGDI формується на основі вимірів: надання онлайн-послуг, телекомунікаційне підключення та кадровий потенціал [1]. За рейтингом е-участі (індекс EPI) – Україна у 2022 році зайняла 57 місце зі 193 країн світу, 46 – у 2020 році, 75 – у 2018 році, 32 – у 2016 році [6].

Стратегія реформування державного управління України на 2022–2025 роки включає низку завдань щодо впровадження інструментів е-урядування: електронної системи управління документами, автоматизованого обміну даними між електронними інформаційними ресурсами органами виконавчої влади, надання адміністративних е-послуг, розвитку відкритих даних тощо

Отже, інформація є фундаментальним ресурсом у професійній діяльності державних службовців, безпосередньо впливаючи на ефективність управління та якість надання державних послуг. У сучасних умовах стрімкого розвитку інформаційних технологій значення інформаційного забезпечення державної служби неухильно зростає. Державні службовці працюють із великими обсягами різноманітної інформації, що є не лише предметом їхньої праці, але й основою для ухвалення управлінських рішень. Інтеграція сучасних інформаційно-комунікаційних технологій і дотримання принципів відкритості та оперативності інформаційного забезпечення сприятимуть створенню ефективного публічного управління, орієнтованого на потреби людини та суспільства.

Список використаних джерел:

1. Дослідження ООН “E-Government Survey 2022». URL: https://publicadministration.un.org/egovkb/Data-Center

2. Капітаненко Н. П. Правове забезпечення електронного документообігу. *Науковий вісник УжНУ. Серія: Право*. Випуск 84. Ч. 3. С. 130–138.

3. Пахнін М. Л. Вплив інформаційного суспільства на розвиток системи публічного управління». *Теорія та практика державного управління.* 2015. Вип. 4(51). URL: http://www.kbuapa.kharkov.ua/e-book/tpdu/2015-4/doc/1/09.pdf

4. Про інформацію: Закон України від 2 жовтня 1992 р. *Відомості Верховної Ради Україн*и. 1992. № 48. Ст. 650.

5. Про схвалення Концепції розвитку цифрових компетентностей та затвердження плану заходів з її реалізації : Розпорядження Кабінету Міністрів України від 3 березня 2021 р. № 167-р. URL: https://zakon.rada.gov.ua/laws/show/167-2021-р#Text

6. E-Participation Index. URL: https://publicadministration.un.org/egovkb/en-us/About/Overview/E-Participation-Index#

УДК 340.1

МЕТЕЛЕНКО НАТАЛЯ ГЕОРГІЇВНА,
д.е.н., проф., директор
Інженерний навчально-науковий інститут ім. Ю. М. Потебні
Запорізького національного університету (м. Запоріжжя, Україна)
E-mail: natalia.metelenko@gmail.com
ORCID/Researcher ID 0000-0002-6757-3124

ОГЛОБЛІНА ВІКТОРІЯ ОЛЕКСАНДРІВНА,
к.е.н., доцент, доцент кафедри інформаційної економіки,
підприємнитцва та фінансів
Інженерний навчально-науковий інститут ім. Ю. М. Потебні
Запорізького національного університету (м. Запоріжжя, Україна)
E-mail: va.ogloblina@gmail.com
ORCID/Researcher ID 0000-0001-6627-0255

БЕЗРУКОВА ВАЛЕРІЯ СЕРГІЇВНА,
бакалавр гр. 6.0723-фдпс-с2
Інженерний навчально-науковий інститут ім. Ю. М. Потебні
Запорізького національного університету (м. Запоріжжя, Україна)

АІ ЯК ІНСТРУМЕНТ ЗАБЕЗПЕЧЕННЯ ПРАВ ГРОМАДЯНИНА В УМОВАХ РОЗВИТКУ ЦИФРОВОЇ ЕКОНОМІКИ

З появою і стрімким розвитком цифрової економіки виникають нові виклики щодо захисту прав громадянина. Цифрові права громадянина є адаптацією фундаментальних прав людини до умов сучасного цифрового світу. Ці права включають захист персональних даних, конфіденційність, свободу вираження, право на доступ до інформації та нові права, які виникли з розвитком інтернету. Наприклад, право на видалення даних («право на забуття») є важливим для захисту конфіденційності в умовах, коли особисті дані можуть зберігатися на сервері десятиліттями. У Європейському Союзі права громадян у цифровому середовищі захищаються такими нормативними актами, як Загальний регламент захисту даних (GDPR). Цей документ вимагає, щоб організації мали обґрунтовані підстави для обробки персональних даних та забезпечували їх захист.

В епоху розвитку цифрової економіки, Україна, як держава з високим рівнем цифровізації та розширенням цифрових послуг, таких як «Дія», потребує законодавчих механізмів для забезпечення безпеки та

конфіденційності цифрових прав своїх громадян. Удосконалення регулятивної бази не тільки зміцнить довіру громадян до цифрових послуг, але й сприятиме адаптації України до європейських стандартів у цій сфері, що є важливим аспектом євроінтеграції. Питання захисту цифрових прав особливо актуальні на тлі глобальних тенденцій до зростання використання особистих даних у комерційних та державних цілях, тому прозорі та чіткі регулятивні механізми допоможуть забезпечити ефективний захист громадян [1].

Одним з найпотужніших інструментів для забезпечення захисту цифрових прав громадян у сучасному суспільстві є штучний інтелект (AI). AI дозволяє автоматизувати процеси збору, обробки та аналізу великих обсягів даних у реальному часі, що надає можливість швидше реагувати на загрози порушення конфіденційності та кібербезпеки. AI-системи вже сьогодні широко використовуються для моніторингу та аналізу даних, що дозволяє попереджати витік інформації та своєчасно виявляти можливі загрози, що є особливо важливим для захисту прав громадян у цифровому середовищі.

Окрім цього, AI здатен забезпечити персоналізований підхід до захисту даних, адже системи можуть самостійно визначати, які дані потребують додаткового захисту. Наприклад, у багатьох країнах AI-системи використовуються для контролю та аналізу доступу до конфіденційних даних. Це дозволяє швидше виявляти спроби несанкціонованого доступу та зменшувати ризик витоку даних. AI також може допомогти у наданні доступу до інформації особам з обмеженими можливостями, створюючи адаптовані інтерфейси та послуги.

Впровадження AI у сферу захисту цифрових прав потребує нормативного регулювання, яке б гарантувало відповідальність, прозорість та етичність використання технології. В ЄС вже розроблені етичні норми для AI-систем, зокрема, принципи прозорості та неприпустимості дискримінації. Україна може скористатися цим досвідом, щоб розробити національні стандарти для використання AI, які б враховували місцеві умови та особливості цифрової інфраструктури [2].

Історія розвитку штучного інтелекту розпочалася у 1950-х роках. Тоді вчені почали розробляти перші алгоритми, здатні імітувати людське мислення. Проте розвиток AI проходив не рівномірно; у 1970–1980-х роках дослідження значною мірою припинилися через обмеження у потужностях комп'ютерів та відсутність достатнього фінансування. Лише у 2000-х роках з появою нових обчислювальних потужностей штучний інтелект почав активно використовуватися у різних галузях, таких як медицина, фінанси, кібербезпека тощо. Сьогодні AI вже використовується у багатьох

аспектах життя, і його розвиток вимагає відповідного регулювання, особливо з огляду на конфіденційність і безпеку даних.

Для ЄС питання регулювання AI є одним з пріоритетів. У 2021 році Європейська комісія запропонувала законодавство, яке класифікує технології AI за рівнем ризику і встановлює вимоги для кожного з рівнів. Наприклад, AI-системи з високим ризиком мають бути прозорими та підлягати обов'язковому контролю. Це дозволяє зменшити ризики порушення прав громадян у цифровому середовищі. Для України адаптація цього досвіду може стати корисною, оскільки дозволить створити національні стандарти для захисту громадян у цифровому середовищі [3].

Штучний інтелект має великий потенціал для забезпечення цифрових прав громадян, особливо в умовах швидкої цифровізації суспільства. AI дозволяє автоматизувати процеси виявлення та реагування на порушення, що робить систему захисту більш ефективною. Наприклад, AI-системи можуть використовуватися для аналізу великої кількості запитів на доступ до персональних даних, що дозволяє знизити навантаження на людський ресурс і прискорити процес надання послуг.

AI також може забезпечити прозорість цифрових послуг, дозволяючи громадянам відстежувати використання своїх даних і краще контролювати, хто і як отримує доступ до їхньої інформації. Це особливо важливо у сфері охорони здоров'я, де AI-системи можуть допомагати забезпечити конфіденційність даних пацієнтів, або в державних послугах, де AI може відстежувати обробку заявок та гарантувати, що процес є прозорим та безпечним [4].

Отже, питання цифрових прав громадян є надзвичайно важливим для сучасного суспільства, особливо в умовах стрімкого розвитку цифрової економіки і збільшення обсягів даних, що зберігаються в цифровому середовищі. В Україні, де цифровізація набирає обертів, питання захисту прав громадян у цифровому середовищі має бути пріоритетним. Використання досвіду ЄС дозволить Україні створити правову базу, яка буде відповідати європейським стандартам і забезпечить надійний захист прав громадян.

Розробка національної стратегії, яка врахує досвід ЄС та адаптує його до українських реалій, допоможе Україні забезпечити права громадян у цифровому середовищі та підвищить рівень довіри до державних цифрових послуг. Це сприятиме зміцненню правової бази для захисту персональних даних, забезпечення конфіденційності та боротьби з кіберзагрозами, а також підтримуватиме основоположні права людини у цифровому середовищі.

Інтеграція AI у процес захисту цифрових прав громадян також відкриє нові можливості для підвищення ефективності цифрової економіки. Це дозволить автоматизувати багато процесів з надання державних послуг, що допоможе знизити навантаження на держслужбовців і забезпечить

швидший та надійніший захист прав громадян. Зокрема, штучний інтелект дозволить громадянам отримувати більш персоналізований підхід у вирішенні їхніх запитів, а також забезпечить більшу прозорість у використанні їхніх даних.

Список використаних джерел:

1. Оглобліна В. О., Попова А. О., Р. П. Афонов, А. І. Сілін. Цифровий інструментарій фінансового управління: інформаційно-аналітичне забезпечення. *Цифрова трансформація промислового менеджменту: теорія і практика* : монографія за ред. д.філософ.н., проф В. Г. Воронкової, д.е.н., проф. Н. Г. Метеленко. Львів – Торунь : Ліга-Прес, 2023. С. 221–304.

2. Dobrosotskaya, L. The Role of AI in Digital Transformation of Government Services. *Ukrainian Journal of Digital Rights*, 2023.

3. European Commission. Proposal for a Regulation on Artificial Intelligence. Brussels: European Commission, 2021.

4. Castelluccia, C., Le Métayer, D. Understanding AI and its Impact on Data Privacy. *European Journal of Law and Technology*, 2022.

УДК 342.7

НІКІТЕНКО ВІТАЛІНА ОЛЕКСАНДРІВНА,
д.філос.н., проф., проф. кафедри управління та адміністрування
Інженерний навчально-науковий інститут ім. Ю. М. Потебні
Запорізького національного університету (м. Запоріжжя, Україна)
ORCID ID: https://orcid.org/0000-0001-9588-7836

ВОРОНКОВА ВАЛЕНТИНА ГРИГОРІВНА,
д.філос.н., проф., завідувач кафедри управління та адміністрування
Інженерний навчально-науковий інститут ім. Ю. М. Потебні
Запорізького національного університету (м. Запоріжжя, Україна)
ORCID ID: http://orcid.org/0000-0002-0719-1546

СОЦІАЛЬНО-ФІЛОСОФСЬКИЙ ДИСКУРС ЕВОЛЮЦІЇ ЛЮДИНИ ВІД БІОЛОГІЧНОЇ ДО ЦИФРОВОЇ, ВІД ЦИФРОВИХ АТРИБУТІВ ДО ЦИФРОВИХ ПРАВ

Цифрова доба створила цифрове суспільство, у якому люди використовують «сировину», таку як інформація, дані та коди для створення віртуального простору, що існує паралельно фізичному світу. Цей простір став

п'ятим стратегічним простором після землі, океану, неба та космосу. Коли люди входять у цей віртуальний простір для здійснення різних соціальних дій, подібно до того, як Гідденс описує заміну аграрного суспільства на індустріальне суспільство, цифрове виживання робить життя людей більше не прив'язаним до землі. Людина виходить з фізичного поля та порушує межі регіону, поля чи клану. Існування людей у віртуальному цифровому суспільстві формує нові «цифрові атрибути», людина еволюціонує від біологічної людини до «цифрової людини», «цифрові атрибути» людини стають домінуючими.

В епоху цифрових технологій, зіткнувшись з такими інформаційними технологіями, як великі дані, блокчейн, штучний інтелект та Інтернет речей, людям важко зрозуміти, що діючий суб'єкт здійснює свою діяльність в одному куточку землі, а його поведінка може змінюватися в кількох місцях одночасно за допомогою передачі даних. У вимірі інформаційних технологій формою існування людини є вже не традиційна «біологічна людина», а «інформаційна людина» з «цифровими атрибутами». «Інформаційні люди» з «цифровими атрибутами» у цифровому просторі постають переважно у двох формах: статичній та динамічній. Динамічна «інформаційна людина» є модернізацією статичної «інформаційної людини», являє собою соціальну особистість з «цифровими атрибутами».

Так звана динамічна «інформаційна людина» відноситься до автономної біологічної людини, яка використовує інформаційні технології для виконання низки соціальних дій, тим самим досягаючи ефекту відокремлення поведінки від фізичного тіла. Тим більше, що сьогоднішній світ зазнає серйозних змін, яких не спостерігалося за сторіччя, відбувається перетворення ресурсів – трансформація від «цифровізації офісу» до «цифровізації суспільства», людина починає рухатися до «цифровізації всього». Люди взаємодіють і формують один одного, що робить «цифрове» суспільство» стабільним.

«Цифрові атрибути» людей зародилися в період «цифровізації всього» завдяки поглибленню цифровізації соціальної діяльності людини. Оцифрування сприяло еволюції від біологічної людини до «інформаційної» та завершує серію соціальних перетворень у цифровому просторі. Цифровізація соціальної діяльності людей та розширення «цифрових атрибутів» людей є двома аспектами розвитку цифрового суспільства. Хоча цифровізація соціальної діяльності людини створила цифрове суспільство, вона також вплинула на самих людей. З настанням цифрової епохи реалізована низка соціальних дій, таких як розпізнавання осіб або відбитків пальців для входу в співтовариство та виходу з нього,

онлайн-голосування за президента, навчання та розвага, спілкування та взаємодія, купівля та продаж.

Спосіб виживання зробив життя людей мобільними та адаптованими, що призвело до збільшення залежності людей від інформаційних технологій. Так, в епоху «Веб 2.0» люди почали висловлювати думки та спілкуватися з іншими у цифровому просторі, в епоху «Веб 3.0» – розвиваються блокчейн, великі дані, штучний інтелект, Інтернет речей, що дозволило людям поступово оцифрувати різні види соціальної поведінки. Соціальна діяльність людей змінюється від простої до складної, від двовимірного до тривимірного формату, від фрагментів до цілого, «розмитого» у цифровому вигляді.

Процес розвитку цифрового суспільства – це по суті процес взаємної еволюції та трансформації між цифровізацією соціальної діяльності людини та «цифровими атрибутами» людини. Наявність стабільних «цифрових атрибутів» – це просунутий цифровий стан людини, від її динамічного оцифрування до статичних цифрових атрибутів. Рівень технологічного розвитку визначає процес цифровізації соціальної діяльності людей, стабільність системи, ступінь «цифрових атрибутів» соціальної діяльності людей.

Специфічний людський сенс полягає не просто в оцифруванні особистої інформації та передачі її в Інтернет, а в наданні цій інформації соціальної значущості, щоб люди могли безперешкодно з'єднуватись та взаємодіяти у рамках дворівневої структури цифрового та фізичного простору. У вік інформації всі суспільства фактично пронизані універсальною логікою інформаційно-мережевого та цифрового суспільства з різним ступенем інтенсивності, його динамічне розширення поступово поглинає і підпорядковує собі всі соціальні форми. Система справжніх імен у цифровому просторі дозволяє людям встановити свою «ідентичність даних» та перетворитися з біологічних людей на інформаційних людей завдяки цифрових атрибутів [1].

Соціально-філософський дискурс еволюції людини від біологічної до цифрової охоплює кілька ключових аспектів, які стосуються змін у природі людського буття, соціальних взаємодій і нормативних підходів у контексті цифрової трансформації.

1. Еволюція від біологічної до цифрової людини відбувається на основі біологічної основи та технологічного впливу. Людина як біологічна істота завжди еволюціонувала у зв'язку з впливом зовнішнього середовища, але технології надали нового імпульсу цій трансформації. Розвиток штучного інтелекту, біотехнологій і кібернетики поставив питання про поєднання біологічного і технологічного (кіборгізація).

2. Цифровий габітус розгортається у контексті того, що людська ідентичність дедалі більше пов'язана з цифровими атрибутами (наприклад, профілями в соціальних мережах), які формують спосіб самопрезентації та соціальну взаємодію.

3. У контексті еволюцій від цифрових атрибутів до цифрових прав формується цифрова ідентичність, у контексті якої у людини цифрового світу формуються унікальні атрибути: облікові записи, дані, віртуальну репутацію. Цифрова ідентичність уже прирівнюється до реальної, і її захист стає нагальною потребою.

Зі зростанням ролі цифрового середовища виникла концепція цифрових прав:

1) Право на конфіденційність та захист персональних даних.
2) Право на доступ до інформації та технологій.
3) Право на «цифрове забуття» (видалення даних).
4) Право на кібербезпеку та захист від маніпуляцій.
5) Соціальні та філософські виклики.

Цифрові технології одночасно розширюють можливості людини та створюють ризики відчуження, втрати емоційних зв'язків і перетворення людини на «цифрову функцію». Цифрова нерівність. Доступ до цифрових технологій залишається нерівномірним, що посилює соціальну нерівність. Людина розглядається як істота, яка постійно змінюється під впливом технологій, і можливий перехід до нової форми життя – симбіозу біологічного та цифрового.

Необхідна розробка етичних принципів використання технологій, які б забезпечували гідність і права людини в цифрову епоху. Цифрове законодавство повинно адаптуватися до викликів часу, забезпечуючи баланс між інноваціями та захистом прав людини. Еволюція від біологічної до цифрової людини ставить перед суспільством завдання не тільки технологічного розвитку, але й осмислення того, якою має бути людина в умовах цифрової реальності. Цей дискурс потребує інтеграції філософії, соціології, права та технологій.

Практичне значення теми еволюції людини від біологічної до цифрової, від цифрових атрибутів до цифрових прав, охоплює низку важливих аспектів, які мають прямий вплив на життя сучасного суспільства. Основні напрями її практичного застосування:

1. Захист цифрової ідентичності, в основі якої розробка механізмів захисту персональних даних. Зважаючи на широке використання цифрових платформ, необхідно створювати більш досконалі інструменти для захисту цифрових атрибутів людини: облікових записів, паролів, банківських даних. Цифрове право на забуття, яке дозволяє видаляти застарілі

або некоректні дані з інтернету, що важливо для управління репутацією в цифровій епосі.

2. Цифрові права у законодавстві, що базуються на основі розробки правової бази, в основі якої створення та вдосконалення законів, які регулюють право людини на доступ до цифрових технологій, конфіденційність і захист від кіберзагроз. Міжнародні угоди, націлені на необхідність інтегрувати цифрові права до глобальних норм, враховуючи, що цифрове середовище не має кордонів.

3. Освіта і адаптація до цифрового світу, що включає підвищення цифрової грамотності. Люди повинні вміти користуватися сучасними технологіями, розуміти ризики цифрового світу і знати, як захистити свої дані; навчання етичному використанню цифрових технологій, особливо важливо для молоді, щоб уникнути кібербулінгу та інших форм цифрового насильства.

4. Бізнес і економіка, що включає адаптацію бізнесу до цифрової трансформації; розвиток цифрових платформ і продуктів для кращої взаємодії з клієнтами та створення нових економічних можливостей. Управління даними., що включає збір, аналіз і використання даних стають важливим аспектом для створення конкурентних переваг у бізнесі.

5. Охорона здоров'я, що включає використання цифрових атрибутів у медицині; електронні медичні записи, телемедицина, застосунки для моніторингу здоров'я – це приклади цифровізації охорони здоров'я, які покращують якість і доступність медичних послу; біометричні системи, в основі яких інтеграція біологічних та цифрових даних для діагностики та лікування.

6. Створення цифрових платформ для збереження культурної спадщини, в основі якої архіви, музеї та інші установи використовують цифрові інструменти для збереження історичних і культурних цінностей. Практичне значення теми полягає в тому, що вона дозволяє суспільству краще адаптуватися до нових умов існування, використовуючи можливості цифрового світу для досягнення соціальної гармонії, економічного розвитку та індивідуального самореалізації.

Список використаних джерел:

1. Воронкова Валентина, Кивлюк Ольга, & Андрюкайтене Регіна. Еволюція від активного відповідального громадянства до цифрового в контексті критичного мислення: досвід країн ЄС. *Humanities studies :* Collection of Scientific Papers / Ed. V. Voronkova. Zaporizhzhia : Publishing house "Helvetica", 2023. 14(91). P. 23–34.

2. Воронкова В. Г., Кивлюк О. П. Відповідальне цифрове громадянство в епоху цифрових технологій. Modern scientific strategies of development : collective

monograph / Compiled by V. Shpak; Chairman of the Editorial Board S. Tabachnikov. Sherman Oaks, California : GS Publishing Services, 2022. C. 226–249.

3. Коломоєць Тетяна, Верлос Наталя, Нікітенко Віталіна Воронкова Валентина, Цифрові права в умовах розвитку штучного інтелекту та глобалізації: виклики та можливості. *Humanities studies :* Collection of Scientific Papers / Ed. V. Voronkova. Zaporizhzhia : Publishing house "Helvetica", 2024. 19(96). P. 207–217.

4. Кивлюк О. П., Воронкова В. Г., Нікітенко В. О. Цифрові права людини як вираження цифрових атрибутів: соціально-філософське обґрунтування. *Освітній дискурс* : збірник наукових праць / голов. ред. О. П. Кивлюк. Київ : ТОВ Науково-інформаційне агентство «Наука-технології-інформація». 2023. Випуск 44(4–6). С. 7–22.

УДК 342.9

ОГЛОБЛІНА ВІКТОРІЯ ОЛЕКСАНДРІВНА,
к.е.н., доцент, доцент кафедри інформаційної економіки,
підприємнитцва та фінансів
Інженерний навчально-науковий інститут ім. Ю. М. Потебні
Запорізького національного університету (м. Запоріжжя, Україна)
E-mail: va.ogloblina@gmail.com
ORCID ID: http://orcid.org/0000-0001-6627-0255

ПЛИСКА ВЛАДИСЛАВ ВІКТОРОВИЧ,
аспірант спеціальності 073 «Менеджмент»
Інженерний навчально-науковий інститут ім. Ю. М. Потебні
Запорізького національного університету (м. Запоріжжя, Україна)
ORCID ID: http://orcid.org/0009-0008-6062-1833

ОДАРЮК ІГОР ОЛЕГОВИЧ,
магістр гр. 8.0724-уфпс
Інженерний навчально-науковий інститут ім. Ю. М. Потебні
Запорізького національного університету (м. Запоріжжя, Україна)
E-mail: odaryukigor@gmail.com

ЗАХИСТ ЦИФРОВИХ ПРАВ ГРОМАДЯНИНА: ЄВРОПЕЙСЬКІ ПРАКТИКИ ДЛЯ УКРАЇНИ

Тема цифрових прав громадянина є надзвичайно актуальною в умовах швидкої цифровізації, коли технології стають невід'ємною частиною

суспільного життя. Однак універсальні права людини, такі як право на приватність, доступ до інформації та свобода вираження, потребують адаптації до цифрових умов. Досвід Європейського Союзу є важливим джерелом для формування відповідної нормативної бази, яка може стати моделлю для України. Впровадження європейських норм в Україні сприятиме створенню законодавчих рамок, що забезпечать захист прав громадян у цифровому середовищі [1].

Європейський Союз уже тривалий час вважається лідером у питаннях захисту прав людини, зокрема й цифрових прав. Регламент ЄС щодо захисту персональних даних (GDPR), запроваджений у 2018 році, став одним із найяскравіших прикладів інструментів, які надають громадянам можливість контролювати свої дані, забезпечуючи права на конфіденційність та захист від неправомірного використання інформації.

Впровадження GDPR дозволило забезпечити високу прозорість у роботі з персональними даними, що сприяє формуванню нових стандартів у світі. Принципи GDPR включають право на доступ до даних, право на виправлення інформації, право на видалення («право на забуття»), а також право на обмеження обробки даних. Ці принципи стали зразком для законодавств багатьох країн, у тому числі й для України, яка прагне імплементувати найкращі європейські практики у своє правове поле.

Цифрові права громадянина у ЄС не обмежуються лише захистом персональних даних. Європейські держави розглядають цифрові права як невід'ємну частину демократичного суспільства, де кожен громадянин має право не тільки на приватність, але й на свободу вираження думок, доступ до інформації та право на безпеку в цифровому середовищі. Наприклад, під час роботи з великими обсягами даних чи із соціальними мережами громадяни мають можливість бути інформованими про те, як саме їхні дані використовуються. Це дозволяє захищати людей від непрозорих алгоритмів, які можуть впливати на доступ до інформації або на процес прийняття рішень [2].

На шляху Євроінтеграції для України важливим завданням є забезпечення захисту цифрових прав своїх громадян на рівні, близькому до європейського. Попри те, що Україна вже має Закон «Про захист персональних даних», він потребує суттєвого оновлення для відповідності сучасним європейським стандартам. Успішне впровадження принципів GDPR в українське законодавство сприятиме зміцненню довіри громадян до державних інституцій, що обробляють персональні дані, а також забезпечить більш високий рівень безпеки при взаємодії з державою та бізнесом у цифровому середовищі.

Однак, запозичення лише законодавчих норм недостатньо. Важливим є також створення механізмів контролю за їх дотриманням та освітня робота з населенням, що допоможе сформувати культуру безпечної поведінки в інтернеті. Адже, згідно з дослідженнями, лише близько половини українських громадян повністю обізнані про свої права у сфері захисту персональних даних. Важливо, щоб громадяни не лише знали про свої права, але й мали доступ до інструментів, які дозволяють їх реалізовувати, а також до юридичної підтримки у разі порушення прав.

Захист цифрових прав включає не тільки контроль за обробкою даних, а й протидію кіберзлочинності. Зокрема, в країнах ЄС існують спеціалізовані відділи кібербезпеки, які працюють над тим, щоб захищати громадян від кіберзлочинів та несанкціонованого доступу до їхніх даних. У цьому напрямі Україна також повинна розвивати відповідну інфраструктуру, адже рівень кіберзлочинності залишається високим, і багато громадян все ще є недостатньо захищеними від можливих загроз в інтернеті.

Важливо розуміти, що цифрові права також є частиною більшої концепції прав людини. Їх дотримання у цифровому середовищі допомагає реалізувати такі фундаментальні права, як свобода слова, право на безпеку та право на приватність. Це особливо актуально в сучасних умовах, коли цифрові технології охоплюють все більше аспектів життя людини. Таким чином, створення умов для реалізації цифрових прав стає обов'язковим елементом побудови демократичного суспільства.

Прийнятий у ЄС у 2018 році Регламент GDPR став важливим кроком у захисті цифрових прав громадян. Дослідження показують, що введення GDPR сприяло підвищенню прозорості у сфері обробки даних та дало громадянам більший контроль над своєю інформацією. Серед основних положень GDPR – право громадян на доступ до своїх даних, право на виправлення, право на идалення («право на забуття»), право на обмеження обробки, право на переносимість даних та право на заперечення. Це надає громадянам можливість ефективніше захищати свої права.

У той же час, досвід таких країн, як Німеччина та Франція, які адаптували GDPR у свої національні законодавства, показує позитивні наслідки впровадження таких стандартів. Наприклад, у Німеччині були прийняті додаткові закони, що посилюють захист персональних даних, особливо у сфері державного управління та комерційних організацій. Ці заходи стали відповіддю на виклики цифрового суспільства, де конфіденційність та приватність стають базовими цінностями. Водночас, в Україні Закон «Про захист персональних даних» залишається недостатньо адаптованим до європейських стандартів, що підкреслює необхідність проведення додаткових реформ у цій сфері, спрямованих на захист прав громадян

у цифровому середовищі, а також інтеграція технологічних інструментів для забезпечення прозорості та безпеки обробки даних [3].

Для забезпечення захисту цифрових прав громадян Європейський Союз застосовує суворі вимоги, що регулюють обробку персональних даних. Одним із ключових принципів GDPR є прозорість, який передбачає обов'язок компаній та організацій надавати користувачам чітку інформацію про те, як, для чого і на який термін їхні дані збираються та використовуються. Це включає обов'язкову згоду користувача на обробку даних, право на доступ до своєї інформації та можливість заперечити проти її використання.

У зв'язку з цим, важливу роль у забезпеченні цифрових прав відіграють технологічні інструменти, такі як шифрування, багаторівневий захист та інструменти контролю доступу, що сприяють безпеці та конфіденційності даних. Наприклад, у деяких країнах ЄС впроваджено механізми автоматичного моніторингу обробки даних, які дозволяють органам контролю швидко виявляти порушення та реагувати на них. Ці практики можуть бути корисними і для України, зважаючи на актуальність питання захисту персональних даних у цифровому просторі [4].

Отже, адаптація європейських стандартів захисту цифрових прав є важливим завданням для України. Запозичення принципів GDPR дозволить покращити рівень захисту персональних даних, підвищити довіру до цифрових послуг та забезпечити прозорість обробки даних. У довгостроковій перспективі, це сприятиме розвитку інформаційного суспільства, підвищенню рівня цифрової грамотності та посиленню кібербезпеки на державному рівні. Крім того, це відкриє нові можливості для міжнародного співробітництва України з країнами ЄС, що позитивно вплине на інтеграційні процеси.

Список використаних джерел:

1. Оглобліна В. О., Попова А. О., Р. П. Афонов, А. І. Сілін. Цифровий інструментарій фінансового управління: інформаційно-аналітичне забезпечення. *Цифрова трансформація промислового менеджменту: теорія і практика* : монографія за ред. д.філософ.н., проф В. Г. Воронкової, д.е.н., проф. Н. Г. Метеленко. Львів – Торунь : Ліга-Прес, 2023. С. 221–304.

2. Захарова О. В. Цифрові права громадян в ЄС: уроки для України. *Вісник Київського національного університету*. 2022. № 3. С. 14–20.

3. Smith, J. Digital Rights in the European Union: Perspectives and Challenges. *Journal of Digital Law*. 2021. Vol. 12, Issue 4. P. 45–56.

4. Бойко П. М. Захист персональних даних в Україні в контексті європейської інтеграції. Київ : Юридичний вісник, 2021.

УДК 347.78:004.056:341.24

СІРА КСЕНІЯ ВОЛОДИМИРІВНА,
студентка 3 курсу бакалаврату спеціальності 073 «Промисловий менеджмент»
Інженерний навчально-науковий інститут ім. Ю. М. Потебні
Запорізького національного університету (м. Запоріжжя, Україна)

ВОРОНКОВА ВАЛЕНТИНА ГРИГОРІВНА,
д.ф.н. завідувач кафедри управління та адміністрування
Інженерний навчально-науковий інститут ім. Ю. М. Потебні
Запорізького національного університету (м. Запоріжжя, Україна)
ORCID ID: http://orcid.org/0000-0002-0719-1546

ЗАХИСТ АВТОРСЬКИХ ПРАВ І ЗМІСТУ ЦИФРОВИХ ДАНИХ

Під захистом авторських прав слід розуміти передбачені законом заходи щодо визнання авторського права, запобігання його порушенням і притягнення до юридичної відповідальності винних. Захист особистих немайнових і майнових прав суб'єктів авторського права здійснюється в порядку, встановленому адміністративним, цивільним і кримінальним законодавством. Захист авторських прав – це комплекс заходів, спрямованих на забезпечення виключних прав автора на його творчий твір. Основна мета такого захисту – гарантувати, що лише автор або правовласник може контролювати використання свого твору, отримувати винагороду за його використання, а також запобігати його несанкціонованому використанню іншими. Захист авторських прав і змісту цифрових даних – це сукупність правових, технологічних та організаційних заходів, спрямованих на забезпечення збереження інтелектуальної власності в цифровому середовищі та на захист прав творців і власників контенту. З розвитком цифрових технологій та інтеграцією інформаційних систем у повсякденне життя виникає необхідність у формуванні нової концепції цифрових прав людини, яка б відповідала сучасним викликам, таким як загроза конфіденційності, доступ до інформації, цензура та цифровий розрив.

Авторські права – це права, які захищають твори літератури, музики, мистецтва, науки, програмне забезпечення, відео та інші продукти творчої діяльності, надаючи авторам контроль над тим, як їхні роботи використовуються. У цифрову епоху захист авторських прав ускладнюється, оскільки контент легко копіюється, змінюється і розповсюджується через Інтернет. Цифрові права на контент = вони регулюють використання інтелектуальної власності в цифровому просторі, включаючи електронні

книги, цифрову музику, фільми, фотографії, бази даних, програмне забезпечення, а також публікації в Інтернеті. Ці права встановлюють, хто має право зберігати, копіювати, передавати чи змінювати ці дані.

Права поділяються на немайнові (право вимагати визнання авторства або залишатись анонімним, обирати псевдонім, захищати твір від його перекручення або спотворення тощо) та майнові (право на використання твору та право дозволяти іншим особам використовувати свій твір).

Ось основні аспекти захисту авторських прав:

1. Реєстрація авторських прав. У багатьох країнах, щоб полегшити захист прав, автор може зареєструвати свій твір у відповідних державних органах. Хоча авторське право виникає автоматично в момент створення твору, реєстрація може спростити процес підтвердження авторства.

2. Економічні права. Це права на комерційне використання твору: право на його відтворення, розповсюдження, адаптацію, публічний показ тощо. Автор може передавати ці права іншим особам або організаціям за винагороду.

3. Моральні права. Вони включають право автора на визнання його авторства (право на ім'я) та на захист твору від спотворення. Ці права є невідчужуваними і залишаються у автора навіть у разі передачі економічних прав.

4. Ліцензії. Автор або правовласник може видавати ліцензії, що надають іншим особам право використовувати твір у певних умовах. Ліцензії бувають винятковими (тільки одна особа має право на використання) і невинятковими (декілька осіб можуть використовувати твір).

5. Термін дії авторського права. У більшості країн авторське право діє протягом усього життя автора і певний період після його смерті (наприклад, 70 років). Після закінчення цього терміну твір переходить у суспільне надбання і може вільно використовуватися будь-ким.

6. Захист у разі порушень. Автор має право звертатися до суду, якщо його права порушуються, і вимагати відшкодування збитків, припинення порушень та інші заходи захисту. Важливо, що авторське право має свої особливості залежно від країни. Тому для ефективного захисту своїх творів авторам варто враховувати законодавство як своєї країни, так і тих країн, де передбачається використання їх творів.

Захист авторських прав і змісту цифрових даних є надзвичайно актуальним у наш час, коли цифрова інформація може легко копіювати:

1. Право на інтелектуальну власність захищає оригінальний контент, зокрема тексти, зображення, аудіо, відео, програмне забезпечення та інше. Щоб контент мав юридичний захист, необхідно чітко ідентифікувати автора і дату створення.

2. Ліцензування дозволяє авторам контролювати, як їхні роботи використовуються. Наприклад, можна обмежити використання лише для некомерційних цілей або дозволити тільки часткове копіювання. Поширені ліцензії, такі як Creative Commons, дають змогу авторам встановити умови використання контенту.

3. Цифрові водяні знаки та DRM (Digital Rights Management): уе технічні методи захисту, які забезпечують контроль за доступом до цифрового контенту. Водяні знаки можуть використовуватися для збереження авторства, а DRM дозволяє обмежити копіювання, редагування чи розповсюдження контенту.

4. Шифрування та захист доступу: для захисту конфіденційної інформації часто використовується шифрування. Це знижує ризик викрадення даних або їхнього несанкціонованого доступу. Двофакторна аутентифікація та складні паролі також допомагають захистити цифрові активи.

5. Дотримання законів: У різних країнах діють свої закони щодо авторських прав і захисту цифрових даних (як-от Закон про цифрове тисячоліття у США чи GDPR у Європі). Компанії мають дотримуватись цих стандартів для захисту прав авторів і користувачів. Захист цифрового контенту забезпечує контроль над його розповсюдженням і зменшує ризик порушення авторських прав, що є важливим для підтримки справедливості та стимулювання інновацій.

Проблеми захисту:

1. Піратство – несанкціоноване копіювання, розповсюдження та використання цифрового контенту без згоди автора або власника прав.

2. Цифровий водяний знак та DRM (Digital Rights Management) – методи, що застосовуються для захисту авторських прав. DRM обмежує можливості копіювання чи поширення цифрових матеріалів, а водяні знаки дозволяють ідентифікувати джерело контенту.

3. Проблеми доступу та конфіденційності – використання контенту часто вимагає балансу між правами власника і правом користувачів на доступ до інформації.

4. Роль законодавства – міжнародні договори та національне законодавство (наприклад, Бернська конвенція, DMCA у США, GDPR в ЄС) забезпечують правовий захист авторських прав, накладаючи санкції за їх порушення.

Законодавчі норми вимагають дотримання авторських прав у цифровому середовищі, а також передбачають процедури для видалення контрафактного контенту. У глобальному цифровому просторі регулювання авторських прав має міжнародний характер. Важливою є гармонізація

законів, оскільки національні правові системи можуть мати відмінності в підходах до захисту авторського контенту.

Перспективи захисту авторських прав у цифрову епоху:

1. Автоматизація та штучний інтелект – можуть допомогти виявляти порушення прав у мережі шляхом моніторингу використання контенту.

2. Розвиток блокчейн-технологій – забезпечує прозорість транзакцій з інтелектуальною власністю та дозволяє відстежувати володіння контентом.

3. Удосконалення нормативно-правових актів – адаптація законодавства до нових технологій сприятиме більш ефективному захисту авторських прав. Захист інтелектуальної власності.

Розробка та впровадження механізмів захисту авторських прав сприяє збереженню прав на творчі продукти, запобігає незаконному копіюванню та поширенню контенту. Це важливо для авторів, компаній і творців контенту, які можуть втрачати значні прибутки через піратство. Підтримка креативних індустрій. Ефективний захист авторських прав стимулює розвиток творчих галузей – літератури, музики, кіно, програмного забезпечення, дизайну. Це створює сприятливі умови для інновацій і збільшує цінність культурного продукту, який стимулює економічне зростання і створює робочі місця. Підвищення довіри до цифрових платформ. Наявність дієвих інструментів захисту авторських прав та цифрових даних сприяє створенню довірливого середовища на цифрових платформах. Користувачі та творці контенту відчувають більшу захищеність і комфорт, знаючи, що їхні права будуть забезпечені. Юридична безпека та зменшення правових ризиків. Забезпечення відповідності нормативним вимогам щодо захисту авторських прав знижує ризик судових позовів і фінансових санкцій для компаній. Це особливо важливо для бізнесів, які займаються розповсюдженням цифрового контенту, таких як стрімінгові платформи, видавництва та рекламні агенції. Адаптація бізнес-процесів до сучасних викликів. Для компаній, які створюють або використовують контент, ця тема дозволяє розробити стратегії захисту власного цифрового продукту, зменшуючи загрози від несанкціонованого доступу та копіювання. Це включає використання таких технологій, як DRM (управління цифровими правами) та блокчейн, що дозволяє ефективніше управляти правами на контент. Стимулювання міжнародної співпраці. Оскільки проблема захисту авторських прав у цифровому середовищі має глобальний характер, розробка універсальних підходів та методів захисту сприяє міжнародній співпраці, гармонізації законодавств і спільній боротьбі з цифровим піратством. У результаті, практичне значення цієї теми полягає у підтримці авторів та бізнесів, збереженні економічної цінності контенту, формуванні прозорого цифрового простору і підвищенні правової відповідальності в цифрову епоху.

Список використаних джерел:

1. Воронкова В. Г., Заїка О. В. Концепція електронного управління та електронної демократії в епоху цифрового розвитку. “Vectors of the development of science and education in the modern world ” («Вектори розвитку науки і освіти на сучасному світі») / Compiled by V. Shpak; Chairman of the Editorial Board S. Tabachnikov. Sherman Oaks, California : GS Publishing Services, 2023. С. 287–307. DOI: 10.51587/9798-9866-95976-2023-014-287-30

2. Воронкова Валентина, Кивлюк Ольга, & Андрюкайтене Регіна. Еволюція від активного відповідального громадянства до цифрового в контексті критичного мислення: досвід країн ЄС. *Humanities studies :* Collection of Scientific Papers / Ed. V. Voronkova. Zaporizhzhia : Publishing house “Helvetica”, 2023. 14(91). P. 23–34. doi: https://doi.org/10.32782/hst-2023-14-91-03. http://humstudies.com.ua/article/view/277846/272597

3. Коломоєць Тетяна, Верлос Наталя, Нікітенко Віталіна Воронкова Валентина, Цифрові права в умовах розвитку штучного інтелекту та глобалізації: виклики та можливості. *Humanities studies :* Collection of Scientific Papers / Ed. V. Voronkova. Zaporizhzhia : Publishing house “Helvetica”, 2024. 19(96). P. 207–217. DOI: https://doi.org/10.32782/hst-2024-20-97-24; URL: http://humstudies.com.ua/article/view/312143/303213

4. Захист авторських прав: Особливості правового регулювання в Україні та закордоном. URL: https://armada.law/blog/zakhyst-avtorskykh-prav-osoblivosti-pravovogo-regulyuvannya-v-ukraini-ta-za-kordonom/

5. DRM (керування цифровими правами). URL: https://gsmhub.com.ua/glossary/drm-keruvannia-cifrovimi-pravami

6. Захист авторських прав,порушених в мережі Інтернет internetlaw. URL: https://dspace.onua.edu.ua/server/api/core/bitstreams/a10d229c-85ef-4edd-b4ca-47b6fa0b79e4/content

УДК 342.7

СОЛЯНЕНКО ЄВГЕНІЯ ВІКТОРІВНА,
студентка І курсу факультету суспільних наук та міжнародних відносин
Дніпровський національний університет імені Олеся Гончара
(м. Дніпро, Україна)
E-mail: eugeniasoljanenko@gmail.com
Науковий керівник: **Капітаненко Наталія Петрівна,**
д.юрид.н., доц., доцент кафедри теорії держави та права,
конституційного права та державного управління
Дніпровський національний університет імені Олеся Гончара
(м. Дніпро, Україна)
E-mail: kapitanenko.np@gmail.com
ORCID ID: http://orcid.org/0000-0002-1475-5784

РЕАЛІЗАЦІЯ ІНФОРМАЦІЙНИХ ПРАВ ГРОМАДЯН В УМОВАХ ВОЄННОГО СТАНУ

Інформація є ключовим елементом людського існування, адже кожна людина є носієм певних знань і даних. Розвиток особистості відбувається через постійне засвоєння, застосування та обмін інформацією. У мирний час це поняття зазвичай асоціюється з доступом до необхідних даних, перевіркою їх достовірності та реалізацією прав, пов'язаних із інформаційною свободою. На сьогодні, актуальним постає питання реалізації та охорони інформаційних прав спільноти в умовах воєнного стану. Особливо, коли інформаційна складова є ключовим об'єктом маніпуляції в умовах гібридної війни. Наразі інформація виконує роль стратегічного ресурсу, здатного впливати на перебіг воєнних дій, формувати суспільну думку та забезпечувати безпеку громадян. В умовах воєнного стану критично важливим є зберігання балансу між захистом демократичних прав і свобод та їх обмеженням на основі впровадження ефективних механізмів інформаційної безпеки.

Метою дослідження є встановлення особливостей реалізації інформаційних прав громадян в умовах воєнного стану на основі аналізу нормативно-правових актів, наукових джерел та статистичних даних.

У період воєнного стану можливості громадян щодо збору, зберігання, обробки та розповсюдження інформації можуть бути обмежені через контроль за змістом та поширенням інформації, допускається тимчасова зупинка роботи державних реєстрів і баз даних, введення особливого режиму роботи і посилена охорона об'єктів критичної інфраструктури тощо. Це дозволяє державі контролювати інформаційний простір

та забезпечувати захист інтересів громадян, впроваджуючи різноманітні заходи в межах інформаційної безпеки. Проте подібні заходи можуть значно ускладнити доступ громадян до публічної інформації.

В таких умовах результативність управління на державному та муніципальному рівнях потребує застосування соціальних інновацій, зокрема, комунікаційних технологій публічного управління [3, с. 117]. Важливо, щоб держава, застосовуючи такі заходи, враховувала принципи пропорційності і обґрунтованості та не порушувала права громадян на доступ до інформації. Так, Уповноважений Верховної Ради України з прав людини в щорічній доповіді про стан додержання та захисту прав і свобод людини і громадянина в Україні у 2023 році зазначає, що впродовж 2023 року надійшло 652 повідомлення від громадян про незаконну обробку персональних даних, які стосувалися незаконної обробки персональних даних, розголошення та оприлюднення персональних даних на вебсайтах в інтернеті, соціальних мережах, мобільних додатках, дошках оголошень, неправомірного поширення персональних даних у відповідь на запити та ін. [8].

Проблема реалізації інформаційних прав у воєнний час набуває особливої актуальності, адже, не досягаючи успіхів на полі бою, окупанти дедалі частіше вдаються до кібервійни. Це проявляється у кібератаках на сайти органів державної влади та органів і місцевого самоврядування, фальшивих дзвінках «від імені української влади» громадянам, поширенні дезінформації через українські медіа, запуску вірусних атак, зламі сторінок у соціальних мережах тощо. Так, Статистичний звіт за результатами роботи Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки в 2023 році Державного центру кіберзахисту державної служби зв'язку та захисту інформації України визнає, що у 2023 року кількість зареєстрованих в Україні кіберінцидентів зросла на 62,5 % порівняно з попереднім, 2022 роком [7].

Окрім цього, війна в Україні виявила ще одну форму порушення інформаційних прав – обмеження права на публікацію цифрового контенту. Після повномасштабного вторгнення російської федерації такі соціальні платформи, як Instagram та Facebook, почали маркувати матеріали про війну в Україні як "sensitive content" [1, с. 92]. На наш погляд, це є порушенням права на публікацію в медіа. Крім того, відповідно до ст. 19 Загальної декларації прав людини «кожна людина має право на свободу переконань і їхнє вільне вираження, що включає можливість шукати, отримувати та поширювати інформацію й ідеї будь-якими засобами, незалежно від державних кордонів» [2].

Важливо зауважити, що після введення воєнного стану в країні були внесені відповідні зміни до вітчизняного законодавства з питань

регулювання інформаційних відносин. Відповідно, 24 березня 2022 року Верховна Рада України ухвалила Закон України «Про внесення змін до Кримінального та Кримінального процесуального кодексів України щодо забезпечення протидії несанкціонованому поширенню інформації про направлення, переміщення зброї, озброєння та бойових припасів в Україну, рух, переміщення або розміщення Збройних Сил України чи інших утворених відповідно до законів України військових формувань, вчиненому в умовах воєнного або надзвичайного стану» з метою встановлення справедливого покарання для осіб, які вчиняють вказані дії [6]. Крім того, набули чинності Закон України «Про внесення змін до деяких законодавчих актів України щодо посилення кримінальної відповідальності за виготовлення та поширення забороненої інформаційної продукції» від 03 березня 2022 року [4] та Закон України «Про внесення змін до Кримінального процесуального кодексу України та Закону України «Про електронні комунікації» щодо підвищення ефективності досудового розслідування «за гарячими слідами» та протидії кібератакам» від 15 березня 2022 року [5]. Отже, внесені зміни до законодавства посилювали відповідальність за кримінальні правопорушення в інформаційній сфері.

Забезпечення захисту інформації в сучасних умовах є гарантією національної, а також інформаційної безпеки України. Перемога в інформаційній війні є не менш важливою, ніж воєнні успіхи. У разі програшу в інформаційній сфері, ситуація на передовій та в тилу країни стане більш критичною. Відтак, Україна має продовжувати інвестувати у розбудову інформаційного фронту, забезпечуючи стійкість держави перед викликами гібридної війни.

Отже, в умовах воєнного стану важливо забезпечити баланс між захистом національної безпеки та дотриманням інформаційних прав громадян, оскільки заходи інформаційної безпеки можуть обмежувати доступ до публічної інформації. Протидія кібератакам та дезінформації є важливими напрямками національної та інформаційної безпеки. Інвестування в інформаційну безпеку забезпечить захист інформаційного простору України та дотримання конституційних прав особи на вільне вираження своїх поглядів і переконань, захист приватного життя в умовах інформаційних війн.

Список використаних джерел:

1. Денисенко К. В., Борко І. С., Косов О. М. Реалізація цифрових та інформаційних прав людини в умовах воєнного стану. *Науковий вісник Ужгородського національного університету. Серія: Право.* 2023. Вип. 77(1). С. 90–94.

2. Загальна декларація прав людини від 10.12.1948 р. URL: https://zakon.rada.gov.ua/laws/ show/995_015#Text (дата звернення: 19.11.2024).

3. Капітаненко Н. П. Комунікаційні технології публічного управління: правовий аспект. *Право та державне управління*. 2018. № 2. С. 116–119.

4. Про внесення змін до деяких законодавчих актів України щодо посилення кримінальної відповідальності за виготовлення та поширення забороненої інформаційної продукції : Закон України від 03.03.2022 р. № 2110-IX. URL: https://zakon.rada.gov.ua/laws/show/2110-20#Text

5. Про внесення змін до Кримінального процесуального кодексу України та Закону України «Про електронні комунікації» щодо підвищення ефективності досудового розслідування «за гарячими слідами» та протидії кібератакам : Закон України 15.03.2022 р. № 2137-IX. URL: https://zakon.rada.gov.ua/laws/show/2137-20#Text

6. Про внесення змін до Кримінального та Кримінального процесуального кодексів України щодо забезпечення протидії несанкціонованому поширенню інформації про направлення, переміщення зброї, озброєння та бойових припасів в Україну, рух, переміщення або розміщення Збройних Сил України чи інших утворених відповідно до законів України військових формувань, вчиненому в умовах воєнного або надзвичайного стану : Закон України від 24.03.2022 р. № 2160-IX. URL: https://zakon.rada.gov.ua/laws/show/2160-20#Text

7. Статистичний звіт за результатами роботи Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки в 2023 році Державного центру кіберзахисту державної служби зв'язку та захисту інформації України. URL: https://scpc.gov.ua/uk/articles/334.

8. Щорічна доповідь Уповноваженого Верховної Ради України з прав людини про стан додержання та захисту прав і свобод людини і громадянина в Україні у 2023 році. URL: https://ombudsman.gov.ua/report-2023/rozdil-9-informatsiini-prava

УДК 342.7

ЦИМБАЛОВА СВІТЛАНА СЕРГІЇВНА,
студентка IV курсу факультету української й іноземної філології
та мистецтвознавства
Дніпровський національний університет імені Олеся Гончара
(м. Дніпро, Україна)
E-mail: svetlanazimbalova@gmail.com
Науковий керівник: **Капітаненко Наталія Петрівна,**
д.юрид.н., доц., доцент кафедри теорії держави і права,
конституційного права та державного управління
Дніпровський національний університет імені Олеся Гончара
(м. Дніпро, Україна)
E-mail: kapitanenko.np@gmail.com
ORCID ID: http://orcid.org/0000-0002-1475-5784

РЕАЛІЗАЦІЯ ІНФОРМАЦІЙНИХ ПРАВ У КРАЇНАХ ЄС У КОНТЕКСТІ ЦИФРОВІЗАЦІЇ

Технологічний прогрес відіграє все більшу роль у всіх сферах життєдіяльності людини, через що він безпосередньо впливає на еволюцію універсальних прав людини та громадянина, які переходять у віртуальний простір. Наразі багато вчених зацікавленні питанням особливостей інформаційних прав, зокрема цифрових прав, викликів щодо їх забезпечення та можливими заходами для їх захисту. З іншого боку, концепція цифрових прав на даний момент не є достатньо визначеною та дослідженою, у зв'язку з чим під час прийняття законів на регіональному, національному та міжнародному рівнях виникають труднощі з правовим регулюванням цифровізації.

Країни Європейського Союзу є достатньо адаптованими до сучасних технологій, що означає своєчасну трансформацію законодавства та відповідні дії для забезпечення інформаційних прав людини в контексті цифровізації. Цей досвід Україна може прийняти до уваги з урахуванням своїх особливостей та інплементувати. Вказані обставини визначають актуальність роботи.

Метою роботи є дослідження особливостей реалізації інформаційних прав у країнах ЄС в контексті цифровізації на основі аналізу нормативно-правових актів, наукових джерел з оглядом на їх впровадження в українському законодавстві.

Вчені не дійшли одностайної згоди щодо тлумачення поняття «цифрові права». О. Братасюк та Н. Ментух розуміють цифрові права як окрему категорію прав людини, що пов'язані з використанням мережі

Інтернет. Дослідники виділяють шість таких прав: право на доступ до інтернету, право на свободу у вираженні поглядів, право на приватність та захист персональних даних, право на свободу та особисту безпеку онлайн (що передбачає гарантії захисту від насильства, нетерпимості, дискримінації та ворожнечі), право на мирні зібрання і використання електронних інструментів демократії (можливість використовувати електронні сервіси для зібрань), право на цифрове самовизначення [4, с. 59].

Н. Верлос зазначає, що цифрові права можуть інтерпретуватися дослідниками як умовна категорія прав, яка стосується безпосередньо їх реалізації у віртуальному просторі. Варто розглядати цифрові права як окрему групу, адже через стрімкий розвиток цифрових технологій виникають нові права, які до недавнього часу не були юридично осмисленими та закріпленими: право на користування електронними пристроями, право на захист персональних даних, право на забуття, право на анонімність тощо [5, с. 130]. З іншого боку, фундаментальні права людини і громадянина також трансформуються у зв'язку з цифровізацією, тож їхня реалізація в сучасних умовах потребує юридичних змін.

Європейський Союз (ЄС) вже зробив низку кроків для оновлення законодавства у відповідності до вимог сучасності. Так, у 2012 році Європейська комісія опублікувала Кодекс прав ЄС в Інтернеті (Code of EU Online Right), призначений для навчання громадян їхніх основних прав під час підключення та використання Інтернету [7]. В подальшому Європейська комісія затвердила цифрові ініціативи держав-членів ЄС, такі як Талліннська декларація про електронний уряд (6 жовтня 2017 року), Берлінська декларація про цифрове суспільство та цифровий уряд, заснований на цінностях (8 грудня 2020 року), Лісабонська декларація – Цифрова демократія. У якості основоположної у цих документах проводилася ідея збалансування технологічного розвитку з повагою до етичних принципів і заохоченням прав людини [3].

9 березня 2021 року Європейська Комісія виклала своє бачення цифрової трансформації Європи до 2030 року у програмі про «Цифровий компас: європейський шлях до цифрового десятиліття», яка передбачає виконання таких чотирьох пунктів: освоєння населенням цифрових навичок і наявність людей, що володіють цими навичками на професійному рівні; безпечна та продуктивна цифрова інфраструктура; цифрова трансформація бізнесу; цифровізація державних послуг [1]. Планується, що до 2030 року всі європейські домогосподарства будуть охоплені гігабітною мережею, а населені пункти будуть охоплені мережею 5G. Також прогнозується, що до 2030 року можна досягти 100 % надання онлайн ключових державних послуг для європейських громадян та бізнесу, всі громадяни

ЄС матимуть доступ до медичних записів в електронному режимі, і 80 % громадян ЄС будуть використовувати цифрове посвідчення [6].

European Declaration on Digital Rights and Principles for the Digital Decade (Європейська декларація про цифрові права та принципи цифрового десятиліття), прийнята в грудні 2022 року та підписана в урочистій обстановці Головою Єврокомісії, Головами Європарламенту та Європейської Ради [9], гарантує додержання таких принципів, як розміщення людей в центрі цифрової трансформації, солідарність та інклюзивність, свобода вибору, участь в цифровому громадському просторі, безпека і сталий розвиток. Дана декларація проголошує обов'язком Європейського Союзу забезпечити рівний доступ до мережі Інтернет, можливість набути цифрових навичок, безпечний і справедливий цифровий робочий простір, доступ до ключових державних послуг, захист дітей і молоді в цифровому середовищі тощо [1, с. 3–7]. З цього випливає, що Європейський парламент виокремив основні принципи, що не мають бути порушені під час пропозиції нових законів, і охарактеризував основні права людини в цифровому середовищі.

Важливою міжнародною мережею, що зробила значний внесок у врегулювання цифрових прав і свобод, є European Digital Rights (EDRi). Ця мережа поєднує більше ніж 40 організації, що працюють в 21 європейській державі. Звіт за 2023 рік свідчить про роботу мережі в напрямі боротьби проти шпигунських програм, надмірного державного нагляду, запам'ятовування даних. Також група працює над гарантіями вільного програмного забезпечення, конфіденційності, свободи самовираження. Наприклад, EDRi просуває акт про європейську медійну свободу, покликаний захистити журналістів та медійних працівників від стороннього нагляду [8, с. 24–41]. Такі заходи спрямовані на забезпечення прав і свобод громадян, а також збереження демократичного устрою в ЄС.

Важливими документами в сфері регуляції цифрового простору також є Загальний регламент захисту персональних даних (GDPR) та Закон про цифрові послуги (DSA). Регламент установлює чіткі норми опрацювання і руху персональних даних та захист прав фізичних осіб. Правники зазначають, що цей документ діє і на компанії, не засновані в Європейському Союзі, у випадку обробки даних громадян ЄС, і охоплює широкий спектр діяльності. Натомість Закон про цифрові послуги детально визначає регулювання всіх електронних платформ, що зробить ці платформи більш зрозумілими та ускладнить поширення шкідливої інформації [2, с. 335]. Ці закони зробили значний внесок у правозахисній практиці та підготували Європу до цифрового десятиліття.

Позитивний досвід рівня правового регулювання прав людини у сфері цифрового середовища в країнах ЄС має слугувати прикладом для України.

Зокрема потенційними заходами є створення мережі організацій для захисту цифрових прав, складання плану з чіткими цілями щодо реалізації можливостей громадян використовувати Інтернет та інші електронні ресурси, видання нових законів стосовно регулювання процесу цифровізації у правозахисному контексті. Деякі заходи країн ЄС вже вплинули на оновлення та переосмислення прав людини і громадянина в контексті віртуального світу. Наприклад, Закон України «Про захист персональних даних» від 1 червня 2010 року, що також встановлює норми з опрацювання персональних даних, спирається на принципи GDPR [1, с. 113]. В той же час чинне законодавство не врегульовує багато питань, які виникають в практичній діяльності. Це зумовлено швидким технологічним розвитком в порівнянні з темпами змін законодавства. Саме тому виникла потреба у прийнятті Закону України «Про захист персональних даних» в новій редакції шляхом імплементації Регламенту (ЄС) 2016/679 Європейського Парламенту і Ради від 27 квітня 2016 року про захист фізичних осіб щодо обробки персональних даних та про вільний рух таких даних; Директиви (ЄС) 2016/680 Європейського Парламенту та Ради від 27 квітня 2016 року про захист фізичних осіб щодо обробки персональних даних компетентними органами з метою запобігання, розслідування, виявлення чи переслідування за кримінальні правопорушення або для виконання кримінальних покарань, а також щодо вільного переміщення таких даних; Директиви 2002/58 Європейського Парламенту та Ради від 12 липня 2002 року стосовно обробки персональних даних та захисту конфіденційності у сфері електронних комунікацій (Директива про конфіденційність та електронні комунікації). Відповідний законопроєкт включено до порядку денного парламенту України 3 вересня 2024 року.

В умовах воєнного стану імплементація європейського досвіду ускладнюється. Втрати досвідчених працівників в області цифрових технологій не дозволяють швидко проводити інновації, пошкоджується інфраструктура і проводяться кібератаки [2, с. 336].

Отже, для ефективного правового захисту в цифровому просторі необхідно оновити законодавство, щоб юридично визначити ці права. Досвід країн ЄС у створенні механізму реалізації інформаційних прав в контексті цифровізації є прикладом для проведення реформування вітчизняного законодавства в зазначеній сфері суспільного життя. Сучасні умови українського буття спонукають ефективно привносити зміни з урахуванням європейського досвіду та власних особливостей цифровізації на основі принципу верховенства права.

Список використаних джерел:

1. Бєлов Д. М. Цифрові права людини: доктринальні засади / Д. М. Бєлов, І. Є. Переш, І. Покорба. *Аналітично-порівняльне правознавство.* 2024. № 2. С. 110–115.

2. Бондаренко О. С., Думчиков М. О. Захист цифрової особистості: вивчення досвіду Європейського Союзу та України. *Юридичний науковий електронний журнал.* 2024. № 1. С. 334–338.

3. Бочарова Н. В., Биков О. М. Праволюдинний зміст сучасної цифрової стратегії Європейського Союзу. *Вісник університету іменІ Альфреда Нобеля. Серія: Право.* 2022. № 1(4). С. 34–42.

4. Братасюк О. Б., Ментух Н. Ф. Поняття та класифікація цифрових прав в Україні. *Юридичний науковий електронний журнал.* 2021. № 10. С. 58–61.

5. Верлос Н. В. Конституціоналізація цифрових прав людини: вітчизняна практика та зарубіжний досвід. *Часопис Київського університету права.* 2020. № 2. С. 129–133.

6. 2030 Digital Compass: the European way for the Digital Decade URL: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021DC0118

7. Code of EU Online Right. Publications Office of the European Union. Luxembourg, 2012. URL: https://op.europa.eu/en/publication-detail/-/publication/50d06da2-18bb-40b2-9e97-7d19527f2c88

8. EDRi annual report 2023 URL: https://edri.org/wp-content/uploads/2024/06/EDRi_AR_2023.pdf

9. European Declaration on Digital Rights and Principles for the Digital Decade URL: https://eur-lex.europa.eu/legal-content/EN/TXT//?uri=CELEX: 32023C0123(01)