

Манько Д. Г.,
доктор юридичних наук, професор,
завідувач кафедри державно-правових дисциплін
Міжнародного гуманітарного університету
<https://orcid.org/0000-0002-7677-397X>

Цховребов Р. Т.,
аспірант кафедри державно-правових дисциплін
Міжнародного гуманітарного університету
<https://orcid.org/0009-0002-1831-4668>

ОКРЕМІ АСПЕКТИ МІЖНАРОДНО-ПРАВОВОЇ РЕАКЦІЇ НА ГЛОБАЛЬНУ ЦИФРОВІЗАЦІЮ

CERTAIN ASPECTS OF THE INTERNATIONAL LEGAL RESPONSE TO GLOBAL DIGITALIZATION

У статті досліджено окремі аспекти міжнародно-правової реакції на процеси глобальної цифровізації. Проаналізовано ключові напрями правового реагування на цифрові трансформації, включаючи кібербезпеку, захист персональних даних, регулювання штучного інтелекту та цифрової економіки. Особливу увагу приділено діяльності міжнародних організацій (ООН, ЄС, Ради Європи тощо) у формуванні нормативних підходів до цифрових викликів. Обґрунтовано необхідність гармонізації національних і міжнародних правових механізмів для забезпечення ефективного, етично виваженого та людиноцентричного правового реагування на цифровізацію.

Встановлено, що інформаційно-комунікаційні технології (ІКТ) дедалі глибше проникають у правову сферу, змінюючи її структуру, функції та зміст. В умовах цифрової трансформації суспільства право не лише адаптується до нових реалій, а й стає активним чинником формування цифрового порядку. Це зумовлює появу нових правових наслідків, які мають комплексний, багатовимірний характер.

Цифрове середовище формує необхідність у юридичному визнанні автентичності електронних версій документів, нових підходів до систематизації, тлумачення й техніко-юридичного оформлення цифрових актів. Це також змінює архітектоніку і стиль нормативної мови, вимагаючи юридико-технологічної досконалості.

ІКТ породжують низку нових об'єктів правовідносин: цифрові дані, профілі, цифрові активи, алгоритми, ШІ-системи, блокчейн-мережі, інтернет речей. Встановлення правового статусу цих об'єктів є необхідною умовою забезпечення правової визначеності та стабільності. Особливої уваги набуває питання власності на дані, права на конфіденційність, на інформаційне самовизначення.

Звернено увагу на те, що сучасні тенденції правового регулювання інформаційно-комунікаційних відносин свідчать про поступовий перехід до моделі впливу, яка базується на принципах техногуманізму й технологічної нейтральності, екстериторіальності дії правових норм і превентивного захисту основоположних прав людини у цифровій сфері.

Зроблено висновок про актуальність розроблення універсальних стандартів правового регулювання у цифровій сфері, посилення співпраці держав у сфері глобального цифрового правопорядку.

Ключові слова: *Європейський союз, інформаційно-комунікаційні технології, міжнародне право, міжнародний правовий порядок, правова глобалізація, цифрова сфера.*

The article examines certain aspects of the international legal response to the processes of global digitalization. The key areas of legal response to digital transformations are analyzed, including cybersecurity, personal data protection, regulation of artificial intelligence and the digital economy. Particular attention is paid to the activities of international organizations (UN, EU, Council of Europe, etc.) in the formation of regulatory approaches to digital challenges. The need to harmonize national and international legal mechanisms to ensure an effective, ethically balanced and human-centered legal response to digitalization is substantiated.

It is substantiated that information and communication technologies (ICT) are increasingly penetrating the legal sphere, changing its structure, functions and content. In the conditions of digital transformation of society, law not only adapts to new realities, but also becomes an active factor in the formation of the digital order. This leads to the emergence of new legal consequences that are complex, multidimensional in nature.

The digital environment necessitates the legal recognition of the authenticity of electronic versions of documents, new approaches to systematization, interpretation and technical and legal registration of digital acts. This also changes the architecture and style of regulatory language, requiring legal and technological perfection.

ICTs generate a number of new objects of legal relations: digital data, profiles, digital assets, algorithms, AI systems, blockchain networks, the Internet of Things. Establishing the legal status of these objects is a necessary condition for ensuring legal certainty and stability. Particular attention is paid to the issues of data ownership, the right to confidentiality, and informational self-determination.

Attention is drawn to the fact that modern trends in the legal regulation of information and communication relations indicate a gradual transition to a model of influence based on the principles of technohumanism and technological neutrality, extraterritoriality of the action of legal norms and preventive protection of fundamental human rights in the digital sphere.

The conclusion is made about the relevance of developing universal standards of legal regulation in the digital sphere and strengthening cooperation between states within the global digital legal order.

Key words: *European Union, information and communication technologies, international law, international legal order, legal globalization, digital sphere.*

Стрімкий розвиток інформаційно-комунікаційних технологій, зокрема інтернету, а також масштабна цифровізація більшості сфер суспільного життя у глобальному вимірі стали ключовими чинниками формування єдиного цифрового простору. Сьогодні інтернет перестав бути лише комунікаційною платформою, перетворившись на складову поліфункціональної інфраструктури, що суттєво впливає на соціальні взаємодії. Ця трансформація часто відбувається поза межами національних регуляторних рамок, створюючи нові виклики для правових систем і суверенітету держав у контексті глобалізованого цифрового середовища.

Слід погодитися з міркуваннями науковців, що «XXI століття стало початком ери глобальної інформатизації та комп'ютеризації всього світу і інтеграції людства до нового інформаційного суспільства, в якому домінуючу роль в усіх сферах життя гратимуть інформаційно-телекомунікаційні ресурси та технології» [2, с. 8].

Мова сучасного права та міжнародних відносин поповнилася низкою нових понять, зокрема, пов'язаних із цифровізацією: «електронна демократія», «кібербезпека», «кіберзлочинність», «цифрова валюта», «цифрова ідентичність», «штучний інтелект» тощо. Значна частина цих понять вже отримала відповідну міжнародно-правову регламентацію.

Ще в 2003 році на міжнародному рівні було поставлено питання про правові наслідки впровадження інформаційно-комунікаційних технологій. Саме тоді, під час Всесвітнього саміту з питань інформаційного суспільства, організованого Міжнародним союзом електрозв'язку

у Женеві, було ухвалено Женевську декларацію принципів «Побудова інформаційного суспільства – глобальне завдання нового тисячоліття» [22]. У ній підкреслено важливість забезпечення рівного доступу до цифрових технологій, а також необхідність подолання технологічного розриву між розвиненими країнами і тими, що розвиваються, а також всередині самих держав.

У 2005 році в Тунісі відбувся другий етап Всесвітньої зустрічі на вищому рівні з питань інформаційного суспільства, який завершився ухваленням Туніського зобов'язання та Туніської програми щодо розвитку інформаційного суспільства. У рамках цього заходу вперше на глобальному рівні була актуалізована проблема управління інтернетом як одним із базових компонентів цифрового середовища. Питання стосувалося необхідності забезпечення більш справедливого, інклюзивного та міжнародного підходу до регулювання цифрового простору, що набуло особливої ваги для країн, які прагнули забезпечити рівний доступ до базових ІТ-технологій.

У Туніському зобов'язанні підкреслювалося, що інформаційно-комунікаційні технології (ІКТ) є ефективним інструментом сприяння миру, безпеці, стабільності, розвитку демократії, соціальній згуртованості, належному врядуванню та утвердженню верховенства права на національному, регіональному й міжнародному рівнях. Крім того, держави-учасниці саміту домовилися про початок процесу інтернаціоналізації управління інтернетом, результатом якого стало створення Форуму з питань управління Інтернетом (IGF) [22].

Перше його засідання відбулося в Афінах у 2006 році. Підтримку процесу інтернаціоналізації активно висловлювали країни, що розвиваються, а також Європейський Союз.

У Женеві в травні 2010 року на черговій Всесвітній зустрічі було заявлено, що кожна держава світу пов'язує своє соціально-економічне зростання з впровадженням ІКТ, розробляючи національні стратегії цифрового розвитку. У Посланні Генерального секретаря ООН з нагоди Всесвітнього дня телекомунікацій та інформаційного суспільства від 17 травня 2010 року наголошувалося, що телекомунікації та ІКТ перетворилися з базових сервісів на потужні засоби сприяння сталому розвитку, покращення якості життя й навіть збереження життя людей [20].

Розширення сфери застосування базових ІТ-технологій супроводжується активізацією міжнародного співробітництва. У цьому контексті Україна бере участь у діяльності профільних міжнародних організацій, спрямованих на розвиток правового регулювання цифрового середовища та інформаційної взаємодії.

Економічна і соціальна рада ООН, своєю чергою, готує аналітичні звіти та статистичні дані про рівень застосування ІКТ у країнах світу, що слугує базою для формування міжнародних стандартів розвитку цифрових технологій і рекомендацій для національних стратегій цифровізації.

Організація Об'єднаних Націй з питань освіти, науки і культури (ЮНЕСКО) є спеціалізованою установою ООН, що діє в галузі освіти, науки, культури та комунікації з метою зміцнення миру й безпеки шляхом міжнародного співробітництва. У сфері комунікацій ЮНЕСКО активно працює над подоланням цифрового розриву між розвиненими країнами та тими, що розвиваються, сприяючи безперешкодному доступу до інформації в усіх регіонах світу.

Ключовим пріоритетом діяльності ЮНЕСКО у цифрову епоху є перехід до «суспільства знань», що реалізується через утвердження принципів свободи слова, доступу до інформації, знань і освіти. У цьому контексті ЮНЕСКО впроваджує низку програм, пов'язаних із розвитком базових ІТ-технологій, зокрема: «Пам'ять світу», «Інформація для

всіх», Міжнародна програма розвитку комунікацій, Програма захисту цифрової спадщини [19].

Всесвітня організація інтелектуальної власності (ВОІВ) функціонує як міжнародна платформа, де формуються рекомендації й політики щодо правового врегулювання використання цифрових технологій у сфері інтелектуальної власності [21]. У її структурі діє Постійний комітет з інформаційних технологій, який готує пропозиції для Генеральної Асамблеї ВОІВ, а також забезпечує міждержавні консультації щодо проблематики цифрових послуг, включно з використанням штучного інтелекту (AI), AR/VR-технологій і хмарних сервісів у сфері авторського права.

Міжнародний союз електрозв'язку (МСЕ) ще з 1947 року працює над розробленням міжнародних стандартів у галузі телекомунікацій, зокрема забезпечує координацію використання радіочастот і розраховує Індекс розвитку ІКТ (ICT Development Index). Основною метою діяльності МСЕ є забезпечення доступності інформації та зв'язку для всіх людей світу як основи соціально-економічного зростання [17].

На сучасному етапі міжнародна спільнота визнає необхідність узгодження дій для захисту цифрових прав людини, забезпечення інформаційної безпеки, захисту критичних цифрових технологій від загроз несанкціонованого доступу та інших форм кіберзлочинності. Це особливо важливо в контексті зростання ролі базових ІТ-технологій у сфері оборони, охорони здоров'я, освіти, публічного адміністрування тощо.

Вплив глобалізації та цифровізації призводить до трансформації парадигми мислення, вдосконалення інститутів громадянського суспільства, органів влади та структур, а також правової системи. Тому цифровий простір потребує створення моделі правового регулювання, яка відповідатиме технологічній реальності [18, с. 130].

У сфері правового регулювання цифрових відносин існують дві концептуально протилежні моделі. Перша – концепція «інтернет-анархії», відповідно до якої віртуальний простір не має бути предметом жорсткого правового регулювання. Вона ґрунтується на позиції, що інтернет виник і розвивався

як відкритий простір без державного втручання, і ця модель має зберігатися й надалі. Представником такої концепції був Джон Перрі Барлоу, який у 1996 році опублікував «Декларацію незалежності кіберпростору», в якій виступив проти цензури та контролю з боку держав [4]. Друга концепція виходить із потреби системного нормативного врегулювання цифрових відносин, адже відсутність контролю призводить до зростання кількості правопорушень як у реальному, так і у віртуальному середовищі. Особливість таких правопорушень – ускладнена ідентифікація правопорушників, що знижує ефективність саморегуляції в інтернеті. Відтак прибічники цієї концепції наполягають на необхідності застосування публічного права для врегулювання інтернет-відносин, зокрема у сфері базових ІТ-технологій [1; 3].

Зіткнення цих двох концепцій вимагає пошуку балансу між інтересами свободи цифрового простору та забезпеченням цифрової безпеки. Проте з огляду на динамічний розвиток ІТ-середовища, досягти такого балансу складно.

Окремою проблемою міжнародного правового порядку залишається відсутність єдиних стандартів захисту даних у їх трансграничному обміні. Відмінності в підходах до конфіденційності, криптографії, прав споживачів і нагляду за обробкою персональної інформації в різних країнах створюють перешкоди для формування ефективного режиму правового захисту. Як наслідок, провідні міжнародні організації, зокрема ООН, ЮНЕСКО, МСЄ та ВОІВ, виступають за розроблення спільних правових механізмів, що дозволять гармонізувати вимоги до цифрової безпеки та захисту базових ІТ-технологій у глобальному масштабі.

Ці виклики ускладнюють досягнення консенсусу в питаннях формування міждержавних угод або створення єдиної міжнародної організації, яка б координувала розвиток і управління глобальними цифровими технологіями. У відповідь на це держави, в тому числі Україна, активно модернізують своє законодавство, зокрема шляхом узгодження стратегій кібербезпеки, цифрової трансформації та гармонізації з правом ЄС, що уможливило поступово долати фрагментованість регулювання і забезпечити захист прав людини у цифрову еру.

Дослідження правовідносин у сфері створення та використання базових ІТ-технологій з метою забезпечення цифрової безпеки в сучасному світі потребує комплексного аналізу національного та міжнародного законодавства, а також врахування наявного досвіду регулювання цієї сфери. Безпека цифрового середовища стала одним із найактуальніших викликів для всіх країн, оскільки безпосередньо впливає на темпи розвитку цифрової економіки, дотримання прав людини та забезпечення сталого функціонування держави в умовах глобальної цифровізації.

Європейський Союз протягом останніх двох десятиліть послідовно вибудовує комплексну нормативно-правову базу для цифрового середовища, прагнучи створити єдиний цифровий ринок і забезпечити баланс між інноваціями, конкуренцією та правами людини. Ще в 1990-х роках ЄС почав ухвалювати рамкові директиви у сфері телекомунікацій і захисту інформації (Директива 95/46/ЄС про захист персональних даних, Директива 2000/31/ЄС про електронну комерцію тощо), які заклали основу для гармонізації законодавства держав-членів.

У 2010-х роках ЄС перейшов до нової стратегії – «Цифрового єдиного ринку» (Digital Single Market Strategy, 2015–2020), результатом якої стало впровадження низки важливих актів прямої дії – регламентів і директив, що охоплюють практично всі аспекти цифрових відносин. Одним із наріжних каменів європейського підходу став «Загальний регламент про захист даних» (GDPR), що набув чинності у 2018 році [16]. GDPR встановив суворі вимоги до обробки персональних даних, екстериторіальний принцип дії та значні штрафи за порушення (до 4% світового обороту компанії).

У період 2023–2025 років практика застосування GDPR досягла нового рівня: національні органи щодо захисту даних активно штрафують транснаціональні корпорації за порушення, створюючи прецеденти. Наприклад, у 2023 році Ірландська комісія із захисту даних оштрафувала компанію «Meta» на рекордну суму €1,2 млрд за незаконне передання даних європейців до США всупереч правилам GDPR [6].

Це рішення стало можливим після того, як Суд ЄС скасував механізм «Privacy Shield» (справа Schrems II, 2020), визнавши, що США не забезпечують адекватний рівень захисту. У відповідь в 2023 році ЄС і США уклали нову рамкову угоду – «EU-US Data Privacy Framework», котру Європейська Комісія 10 липня 2023 р. визнала адекватною, відновивши законні шляхи трансферу даних через Атлантику [7]. Попри це увага до питання захисту даних залишається підвищеною: країни ЄС допрацьовують національні закони з урахуванням GDPR, створено Європейську раду щодо захисту даних для узгодження дій регуляторів, а також триває робота над новими інструментами регулювання даних у цифровій економіці.

Період 2023–2025 років ознаменувався в ЄС набуттям чинності двох масштабних регламентів, що докорінно змінюють правила гри для цифрових платформ, – Акту про цифрові послуги (DSA) та Акту про цифрові ринки (DMA). DSA (Регламент (ЄС) 2022/2065) встановлює комплекс обов’язків для онлайн-посередників щодо видалення незаконного контенту, прозорості алгоритмів, захисту прав користувачів і аудиту систем модерації. Особливо суворі вимоги висувуються до дуже великих онлайн-платформ (VLOPs) з аудиторією понад 45 млн користувачів – їх Єврокомісія визначила у квітні 2023 р. (17 платформ, серед яких Facebook, Google, TikTok, YouTube, Instagram та ін., а також 2 пошуковики). Для цих гігантів DSA передбачає незалежні перевірки та безпрецедентно високі штрафи за недотримання правил (до 6% глобального обороту). Уже наприкінці 2023 року Єврокомісія продемонструвала готовність застосовувати DSA: так, у грудні 2023 р. було відкрито офіційне провадження щодо соцмережі X (Twitter) за ймовірні порушення DSA стосовно дезінформації та шкідливого контенту [7].

Це сигналізує про серйозність намірів ЄС забезпечити безпечний цифровий простір для користувачів і притягати платформи до відповідальності за системні ризики.

DMA (Регламент (ЄС) 2022/1925), зі свого боку, спрямований на обмеження монополізму найбільших IT-компаній, які виконують роль «воратарів» основних цифрових послуг.

У вересні 2023 року Єврокомісія офіційно визначила шість корпорацій як *gatekeepers* – Alphabet (Google), Amazon, Apple, ByteDance (TikTok), Meta, Microsoft – які сумарно надають 22 ключові платформи (пошуковики, соцмережі, маркетплейси тощо).

З березня 2024 р. ці компанії зобов’язані виконувати перелік «обов’язків і заборон» DMA, зокрема: не нав’язувати власні сервіси користувачам, забезпечити можливість видалення попередньо встановлених додатків, ділитися даними з конкурентами на вимогу користувачів, гарантувати взаємодію месенджерів між платформами тощо.

Порушення DMA так само караються штрафами до 10% річного обороту, а в разі систематичного ігнорування – аж до примусового поділу бізнесу. Фактично, ЄС уперше запровадив *ex ante* регулювання для *Big Tech*, намагаючись запобігти зловживанням ще до їх настання. У поєднанні DSA і DMA формують нову «цифрову конституцію» єдиного ринку, що має глобальний вплив, оскільки великі компанії змушені адаптувати свої продукти під євронорми (наприклад, відмовитися від таргетингу реклами на основі чутливих даних, відкрити доступ до своїх магазинів додатків стороннім розробникам тощо).

У відповідь на зростання кіберзагроз і гібридних атак Європейський Союз послідовно розвиває правову базу кібербезпеки. Ще в 2016 році було ухвалено Директиву NIS щодо безпеки мереж та інформаційних систем [12], яка зобов’язала держав-членів створити національні стратегії кібербезпеки і запровадити обов’язки для операторів критичної інфраструктури. У 2022 році ухвалено Директиву NIS2 (ЄС) 2022/2555 [14], яка суттєво розширила сферу дії. Паралельно діє Регламент про кібербезпеку (Cybersecurity Act) [11], що започаткував європейську систему сертифікації безпеки IT-продуктів. У 2023 році запропоновано проєкт «Акту про кіберстійкість» (Cyber Resilience Act) [10].

У сфері електронної ідентифікації ЄС, спираючись на досвід Регламенту eIDAS 2014 року [15], у 2024 році ухвалив оновлений Регламент eIDAS 2.0. Новий регламент вводить поняття «європейський цифровий гаманець» [5], цей «гаманець» дозволить громадянам зберігати

електронні документи та використовувати їх на всій території ЄС.

У стратегічній перспективі Європейський Союз орієнтується на реалізацію цілей «Цифрового компаса 2030» [8], що передбачає розвиток цифрових навичок, безпечної інфраструктури, цифровізації бізнесу і державних послуг. Цілі закріплено у рішенні (ЄС) 2022/2481 [13].

Паралельно ЄС формує нормативно-правову базу для регулювання штучного інтелекту. У 2021 році було запропоновано Регламент про штучний інтелект (AI Act) [9], що встановлює вимоги залежно від рівня ризику використання ШІ.

Правові наслідки впровадження ІКТ мають системний характер і охоплюють усі рівні правової сфери. У відповідь на цифрові виклики формуються нові правові інститути, зокрема: право на цифрову недоторканність, право на автономне цифрове самовизначення та ін. Ці права доповнюють традиційні права людини, вони потребують чіткої нормативної фіксації та ефективних механізмів захисту, заснованих на принципах людиноцентричності цифрової трансформації та «поміркованості у використанні ІКТ», що має забезпечувати баланс між ефективністю та правовими й етичними цінностями.

Відтак забезпечення ефективної міжнародно-правової реакції на глобальну цифровізацію має поєднувати модернізацію нормативної бази, забезпечення етико-правового балансу між технологічною ефективністю та правами людини, чітку ідентифікацію прав,

обов'язків і відповідальності у цифровій сфері.

Висновки. Узагальнюючи викладене, можна констатувати, що правове регулювання відносин у цифровому середовищі дедалі більше набуває рис особливого правового феномену, який охоплює елементи міжнародного права, права Європейського Союзу та акти національного права окремих правових систем. У відповідь на глобалізацію цифрових процесів різні країни та міжнародні організації розробляють спеціалізовані правові акти, спрямовані на врегулювання питань кібербезпеки, цифрової ідентичності, захисту персональних даних, регулювання штучного інтелекту та базових ІТ-технологій.

Сучасні тенденції правового регулювання інформаційно-комунікаційних відносин свідчать про поступовий перехід до моделі впливу, яка базується на принципах техногуманізму й технологічної нейтральності, екстериторіальності дії правових норм і превентивного захисту основоположних прав людини у цифровій сфері. Україна, орієнтуючись на європейські стандарти, послідовно імплементує ключові положення права ЄС у національну правову систему, що є передумовою її інтеграції в єдиний цифровий ринок і підвищення стійкості до викликів інформаційної епохи.

Зазначені положення підкреслюють актуальність подальшого розроблення універсальних стандартів правового регулювання у цифровій сфері та посилення співпраці держав у сфері глобального цифрового правопорядку.

ЛІТЕРАТУРА:

1. Андрєєв К. О. Правове регулювання штучного інтелекту: світовий досвід та перспективи для України. Київ : Юрінком Інтер, 2022. 38 с.
2. Концептуальні основи захисту інформаційного суверенітету України : монографія / О. В. Задерейко, О. В. Троянський, Р. І. Чанишев, А. І. Дика. 2-ге вид., перероб. і доп. Одеса : Фенікс, 2022. 75 с. DOI: <https://doi.org/10.32837/11300.22733>
3. Лефтеров В. О. Психологічні особливості впливу цифрового середовища на особистість. *Психологія життєвого простору особистості в сучасних умовах кризи, глобалізації та цифрової трансформації суспільного життя* : матеріали міжнар. наук.-практ. конф. (м. Одеса, 14–15 верес. 2023 р.) / Міжнар. гуманіт. ун-т. Одеса, 2023. С. 187–190. DOI: <https://doi.org/10.32837/11300.26409>
4. Barlow, J. P. A Declaration of the Independence of Cyberspace. 1996. URL: <https://www.eff.org/cyberspace-independence>
5. Council of the European Union. European digital identity (eID): Council adopts legal framework on a secure and trustworthy digital wallet. In *Consilium*. URL: <https://www.consilium.europa.eu/en/press/press-releases/2024/03/26/european-digital-identity-eid-council-adopts-legal-framework-on-a-secure-and-trustworthy-digital-wallet/>
6. Data Protection Commission announces conclusion of inquiry into Meta Ireland. In Data Protection Commission.

Data Protection Commission. URL: <https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-announces-conclusion-of-inquiry-into-meta-ireland>

7. European Commission adopted an adequacy decision for the EU–U.S. Data Privacy Framework on 10 July 2023. URL: commerce.gov

8. 2030 Digital Compass: the European way for the Digital Decade. In *European Commission*. URL: <https://digital-strategy.ec.europa.eu/en/policies/digital-compass>

9. Proposal for a Regulation laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act). In *European Commission*. URL: <https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence>

10. Proposal for a Regulation on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act). In *European Commission*. URL: <https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act>

11. European Union Agency for Cybersecurity (ENISA). Cybersecurity Act. In *ENISA*. URL: <https://www.enisa.europa.eu/topics/cybersecurity-act>

12. Directive on security of network and information systems (NIS Directive). In *ENISA*. URL: <https://www.enisa.europa.eu/topics/nis-directive>

13. Decision (EU) 2022/2481 establishing the Digital Decade Policy Programme 2030. In *EUR-Lex*. URL: <https://eur-lex.europa.eu/eli/dec/2022/2481/oj>

14. Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). In *EUR-Lex*. URL: <https://eur-lex.europa.eu/eli/dir/2022/2555/oj>

15. Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions (eIDAS Regulation). In *EUR-Lex*. URL: <https://eur-lex.europa.eu/eli/reg/2014/910/oj>

16. General Data Protection Regulation (GDPR). (n.d.). In *Consilium.europa.eu*. URL: <https://www.consilium.europa.eu/en/policies/data-protection-regulation/>

17. Measuring digital development: ICT Development Index 2024. *Geneva: ITU*. URL: <https://www.itu.int/itu-d/reports/statistics/idi2024/>

18. Manko D., Zghama A., Atamanova N., Arabadzhy A., Ustinov D. Legal regulation of the digital environment: digitization of the state-legal and law enforcement sphere. *Amazonia Investiga*. 2023. Vol. 12, Iss. 70. P. 130.

19. Memory of the World: About the Programme. *UNESCO*. (n.d.). URL: <https://www.unesco.org/en/memory-world/about>

20. Message on World Telecommunication and Information Society Day. *United Nations Secretary-General*. 2010, May 17. URL: <https://www.un.org/en/events/telecommunicationday/2010/sgmessage.shtml>

21. Standing Committee on Information Technologies (SCIT). *World Intellectual Property Organization*. (n.d.). URL: https://www.wipo.int/meetings/en/topic.jsp?group_id=64

22. Declaration of Principles: Building the Information Society – A Global Challenge in the New Millennium. *Geneva: WSIS*. 2003. URL: <https://digitallibrary.un.org/record/533621>