

УДК 340.13:004.9:004.8

КОСТЕНКО О., *Ph.D. в галузі права, старший науковий співробітник, завідувач лабораторії теорії цифрової трансформації та права Державної наукової установи «Інститут інформаційної безпеки і права» Національної академії правових наук України*
ORCID: <https://orcid.org/0000-0002-2131-0281>

ЦИФРОВА ЮРИСДИКЦІЯ: МОДЕЛЬ

DOI: [https://doi.org/10.37750/2616-6798.2025.4\(55\).346297](https://doi.org/10.37750/2616-6798.2025.4(55).346297)

Анотація. Стаття пропонує методологічну схему побудови цифрової юрисдикції на основі модульного підходу, який дозволяє інтегрувати її до системи національного та міжнародного права. Особливу увагу приділено інституційним і процедурним компонентам — цифровим судам, омбудсменам, транскордонному арбітражу, а також принципам алгоритмічної легітимності та етико-центричного управління. Цифрова юрисдикція інтерпретується як інструмент цивілізаційної адаптації права до доби Web 4.0, блокчейн-юридичних протоколів і штучного інтелекту.

Це дослідження не лише систематизує напрацьовану теорію, а й пропонує концептуальний зсув від декларативного рівня до моделювання операційної правової системи майбутнього, відкриваючи перспективи створення цифрових кодексів, реєстрів і міжнародних нормативних платформ.

Ключові слова: цифрова юрисдикція, Metaverse, електронна юрисдикція, AI, цифровий суверенітет, Web 3.0.

Summary. The article proposes a methodological scheme for building a digital jurisdiction based on a modular approach that allows it to be integrated into the system of national and international law. Special attention is paid to the institutional and procedural components: digital courts, ombudsmen, cross-border arbitration, as well as the principles of algorithmic legitimacy and ethical-centric management. Digital jurisdiction is interpreted as a tool for civilizational adaptation of law to the age of Web 4.0, blockchain legal protocols and artificial intelligence.

This study not only systematizes the developed theory, but also offers a conceptual shift from the declarative level to the modeling of the operational legal system of the future, opening up prospects for the creation of digital codes, registers and international regulatory platforms.

Keywords: Digital Jurisdiction, Metaverse, Electronic Jurisdiction, AI, Digital Sovereignty, Web 3.0.

1. *Вступ.* Сьогодні людство увійшло у епоху електронної комунікації, у якій цифрові технології не лише поєднують, а й трансформують усі попередні форми інформаційного обміну. Від перших обчислювальних машин до Метавсесвіту (Metaverse), де Metaverse розуміється як електронне середовище, що утворено сукупністю електронних суб'єктів та об'єктів, які взаємодіють між собою, а також електронні або інші технології, що забезпечують їх взаємодію [1].

2. *Код як Конституція кіберпростору: від Лессіга до архітектури електронної юрисдикції.* Транскордонні цифрові простори формують новий тип правової реальності, у якій традиційні інструменти аналогового права не працюють належним чином. Саме тому виникає необхідність у новій правовій конструкції — цифровій юрисдикції, що

покликана стати відповіддю на виклики цифрової епохи. Нині такий підхід не має аналогів. У фундамент цифрової юрисдикції покладено “Декларацію про незалежність кіберпростору” Дж. П. Барлоу [2], а також “Код та інші закони кіберпростору” та “Код” Л. Лессіґа [3, 4]. Саме **код** визначає способи, межі та порядок взаємодії користувачів у кіберпросторі, подібно до того, як у фізичному світі соціальні відносини регулюються нормами державного управління та права. Л. Лессіґ обґрунтовує тезу, що у фундаментальному вимірі код є своєрідною “Конституцією” кіберпростору, оскільки саме він встановлює правила доступу до цифрових середовищ, визначає межі приватності, безпеки, свободи дії користувачів і формує алгоритмічні режими контролю.

Таким чином, код постає як форма цифрового суверенітету, що створює автономний порядок, альтернативний традиційним моделям правового і державного регулювання у фізичному світі.

3. Проблеми правового регулювання суспільних відносин у Metaverse

Відмінність сучасного кіберпростору Web 2.0 від Metaverse Web 3.0-4.0 полягає у зміні самої природи правовідносин. У системі Web 2.0 переважна більшість процесів регулюється чинними нормативно-правовими актами, які охоплюють визначене коло суспільних відносин. Натомість у Metaverse виникають нові типи цифрової взаємодії, що не мають чітких аналогів у традиційному праві. Вони спрямовані на визначення їх змісту, спрямованості й правового статусу — тобто на створення основи для формування адекватних механізмів їх регулювання. Ключовими питаннями залишаються: який зміст слід вкладати в поняття “*суспільні відносини в Metaverse*” та “*відносини в Metaverse*”; за яких умов електронні суб’єкти й об’єкти можуть бути наділені правами, притаманними людині; які форми правосуддя можуть бути застосовані у віртуальному середовищі; яку відповідальність матимуть електронні суб’єкти й об’єкти, наділені правами людини.

Сучасний Metaverse еволюціонує від імітації реального світу до самостійного розвитку, формуючи нову систему цінностей, правових норм і навіть соціальних ієрархій, які поступово починають впливати на реальний світ. Основною проблемою залишається відсутність єдиного правового механізму регулювання суспільних відносин у Metaverse. Більшість національних правових систем базуються на нормативних актах, створених без урахування технологічної природи Метавсесвіту. У кращому випадку чинне законодавство лише частково охоплює окремі аспекти цифрової взаємодії, залишаючи значні сфери у стані правової невизначеності.

Спроби модернізувати правову систему часто зводяться до ухвалення тимчасових підзаконних актів або відомчих інструкцій, які не забезпечують системного підходу. Судова практика лише починає формувати прецеденти електронного правосуддя, застосовуючи чинні норми аналогового права до цифрових кейсів. Це формує підґрунтя для майбутньої цифрової юстиції, однак на сьогодні такі рішення мають фрагментарний характер.

Різноманіття правових культур і державних інтересів створює асиметрію регулювання: те, що в одній країні розглядається як правопорушення, в іншій може розглядатися як правомірна дія. У результаті навіть прогресивні нормативні акти часто мають декларативний характер і не забезпечують реальної юридичної дії.

Попри це, технології Metaverse уже сьогодні породжують нові типи правовідносин, що вимагають регулювання. Саме тому постає завдання створення системного правового каркасу Metaverse, який забезпечить узгоджене співіснування людини, технологій та алгоритму в межах єдиного цифрового правопорядку [5].

4. Юридична ентропія: деградація класичних опор права у цифрових екосистемах.

Тотальна цифровізація демонструє кризову неспроможність аналогового права у цифрових екосистемах — аналогове право історично спирається на три “опори”: територіальність (*lex loci*), матеріальність об’єктів (*res*) і централізовані інституції примусу. У цифрових екосистемах ці опори системно дефлектують. Територіальність втрачає визначальний характер: “місце” події замінює топологія мережі (вузли, кластери, зони доступності, блокчейн-реєстри), а не географічні координати. Матеріальність поступається цифровим речам або квазіречам — станам програмного коду (токени, ончейн-записи, доступи, ноди), для яких класичні речово-правові конструкції не працюють без спеціальних модифікацій. Примус дедалі частіше реалізується протоколами самовиконання (смартконтракти, оракули, списки доступу), що діють поза традиційною вертикаллю “суд — виконавець”. Виникає регуляторний лаг: нормотворчий цикл держав — роки; тоді як цикл цифрових протоколів — тижні [6].

Класичні колізійні прив’язки (місце укладення/виконання, громадянство сторін, місцезнаходження речі) втрачають релевантність, якщо сторони — мережеві ідентичності (DID/VC), а “річ” — стан розподіленого реєстру. Процесуальні гарантії доказування також залишаються недостатніми: прийнятність криптографічних підписів, журналів транзакцій, часових міток і *chain of custody* потребує автономної процесуальної рамки, яка описує криптографічну верифікацію, реплікацію та фінальність записів.

Транскордонна природа електронних екосистем (е-екосистем) і Metaverse формує нові принципи функціонування суспільства [7].

Е-екосистеми та Metaverse за своєю суттю є транскордонними й міжнародними, оскільки організовані за протокольними принципами, а не за державними кордонами. Їхні базові принципи функціонування визначаються так:

- 1) юрисдикція даних і протоколів замість виключно територіальної юрисдикції;
- 2) протокольне врядування (*on-chain* голосування, багатопідпис, делегування) поряд із публічно-правовими вертикалями;
- 3) самовиконання та “м’який примус” через зміну прав доступу, замороження активів тощо;
- 4) ідентичність як набір атрибутів, що потребує правового статусу аватарів, агентів AI та DAO;
- 5) об’єкти як стани коду (*on-chain* активи, токенизовані права, ліцензії доступу);
- 6) економіка подій (*event-driven*), яка вимагає правових оркестрацій, мапованих на подієві шини протоколів.

Відповідно, право має функціонувати на рівні протоколів і даних, що обґрунтовує появу цифрової юрисдикції як спеціальної нормативної оболонки з новими “юридичними якорями”: *provenance*-якорі (походження та якість даних), інфраструктурні (розташування вузлів, HSM/TEE), ідентифікаційні (DID/VC), економічні (*on-chain activity nexus*), а також — *lex protocolli* як спеціальна форма *lex specialis* для смартконтрактів і консенсусних механізмів.

5. Кінець вестфальського світу: право у добу протоколів і платформ.

Вестфальська парадигма виходила з принципів територіальної цілісності та монополії держави на право і примус [8]. У цифрову добу вона деградує через: розмивання кордонів потоками даних; появу паралельних правопорядків (платформи, протоколи, приватні стандарти); асиметрію спроможностей між державами та транснаціональними технологічними мережами. Як реакція формується феномен, який можна означити як “балканський кіберсуверенітет”. Це — мозаїчна фрагментація мережевого простору

(кіберсуверенітет) за ознаками локалізації даних, національних криптолагун, ліцензування дата-центрів, бар'єрів транскордонної передачі інформації та “цифрових кордонів” для AI та криптоінфраструктур.

Ознаки цього стану: регуляторне “залізне шатро” (data localization, суверенні хмари); юрисдикційне маневрування (вибір сприятливих режимів для протоколів); сплінтернет (несумісні технічні й правові стандарти); проксі-суверенітет платформ (правила спільнот і терміни сервісу, що фактично виконують квазі-державні функції); санкційні режими як інструменти кібергеополітики.

Наслідок — блокування інтероперабельності та зростання транзакційних витрат для інновацій. Відтак цифрова юрисдикція має запровадити “мости довіри”: взаємне визнання DID/VC, міжюрисдикційні правила прийнятності цифрових доказів, стандарти сумісності для смартконтрактів і “хмарні апеляції” (cloud AI-judiciary) як наднаціональні механізми вирішення спорів.

6. Digital Jurisdiction

Цифрова юрисдикція — це багатовимірна правова форма здійснення юрисдикційних повноважень у цифровому середовищі, що забезпечує повноцінне функціонування правової системи у віртуальному просторі Metaverse та е-екосистемах.

Отже, сформулюємо базову авторську дефініцію: *“Цифрова юрисдикція — це посттериторіальна правова конструкція, що регулює соціальні, економічні, інформаційні та алгоритмічні відносини у цифрових екосистемах — кіберпросторі, блокчейн-мережах, середовищах штучного інтелекту та Metaverse. Вона охоплює сукупність технічних, процедурних, нормативних та етичних принципів, які визначають порядок доступу, взаємодії, ідентифікації, цифрових соціальних відносин, цифрових прав, цифрових обов'язків, цифрової відповідальності, а також функціонування цифрової судової системи в цифровому середовищі”*.

У концептуальному сенсі цифрова юрисдикція є розширеною формою електронної юрисдикції. Якщо *електронна* визначає технологічну основу — електронні документи, транзакції, інфраструктуру, — то *цифрова* охоплює повний життєвий цикл даних, алгоритмів, прав і етичних норм, включаючи автономні штучні системи, децентралізовані організації (DAO) та віртуальні ідентичності.

Отже, digital включає electronic як технічний рівень, але розширює його до алгоритмічного, правового, семантичного та етико-соціального виміру, формуючи нову архітектуру правового суверенітету — *Meta-Legal OS*.

На відміну від класичних територіальних форм правосуддя, цифрова юрисдикція спирається на принцип функціональної присутності: правові наслідки дій визначаються не географією, а цифровим місцем, де відбулася активність або зберігаються дані, що породжують юридичні наслідки. Такий підхід забезпечує екстериторіальність, гнучкість і здатність держави захищати права своїх громадян у глобальному кіберпросторі, де межі визначаються не кордонами, а даними, мережевими зв'язками та цифровими ідентичностями.

Держава забезпечує легітимність, публічність і прозорість електронної юрисдикції; створює інституції, що реалізують правосуддя у цифровому форматі; гарантує ідентифікацію та верифікацію кожного суб'єкта у віртуальному середовищі, а також зберігає його правову суб'єктність у разі транскордонної взаємодії.

До таких інституцій належать електронні суди, цифрові арбітражі, онлайн-нотаріат, реєстри електронних рішень, системи автоматизованої верифікації доказів і сервіси юридичного моніторингу. Вони функціонують на основі смарт-контрактів, блокчейн-

записів та алгоритмів прозорого прийняття рішень із залученням штучного інтелекту під контролем людини.

Цифрова юрисдикція функціонує на засадах цифрового суверенітету, верховенства права, поваги до прав людини, алгоритмічної справедливості, сумісності правових систем, етичної відповідальності та міжнародного співробітництва. Вона передбачає обов'язкове забезпечення відкритого доступу до правових актів, процедур апеляції в електронному форматі та механізмів транскордонного виконання рішень через міжнародні платформи цифрового права.

Цифрова юрисдикція поширюється на:

- правовідносини, що виникають у межах цифрових платформ, блокчейн-мереж, Метавсесвітів, децентралізованих автономних організацій (DAO), віртуальних офісів, державних порталів, смарт-екосистем, цифрових бірж, освітніх і комунікаційних середовищ, включно з імерсивними платформами, що забезпечують взаємодію між людиною та штучними агентами;

- електронні правочини, адміністративні процедури, судочинство, сертифікацію, ліцензування, реєстрацію, електронне нотаріальне посвідчення, цифрові транзакції та інші юридично значущі дії, що здійснюються у віртуальному середовищі та породжують правові наслідки в цифровому або змішаному форматі;

- електронні докази, цифрову ідентичність, смарт-контракти, децентралізовані угоди, блокчейн-записи, електронні архіви, цифрові сертифікати, біометричні підтвердження та інші форми взаємодії, що мають юридичну значущість і забезпечують автентичність, достовірність та відтворюваність правових фактів у цифровому середовищі.

8. Принципи функціонування електронної юрисдикції

Принципи функціонування електронної юрисдикції включають:

Принцип екстериторіальності. Дія електронної юрисдикції поширюється на всі цифрові події, транзакції, правочини або інформаційні процеси, незалежно від фізичного місця перебування їхніх учасників чи технічного розміщення серверів [9]; якщо така подія створює правові наслідки, впливає на права, обов'язки чи інтереси осіб у правовому полі держави, вона підпадає під дію національного законодавства [10]. Цей принцип забезпечує можливість держави захищати своїх громадян, цифрових резидентів та інституції у глобальному кіберпросторі, долаючи обмеження фізичної території [11, 12]. Він формує основу для юридичного визнання транскордонних дій у блокчейн-мережах, Метавсесвітах і хмарних середовищах, визначаючи, що цифровий простір є продовженням національної правової системи, де діють норми Конституції, міжнародних договорів і принципи цифрового суверенітету [13, 14].

Принцип правової ідентичності. Кожен учасник електронних правовідносин має підтверджену цифрову ідентичність [15], що визнається рівнозначною особистій присутності та забезпечує його правовий статус у всіх формах цифрової взаємодії [16, 17]. Цифрова ідентичність створюється через систему багаторівневої автентифікації, цифрових підписів, біометричних параметрів і криптографічних ключів, які гарантують унікальність та недоторканність особистих даних [18]. Вона має юридичну силу для укладання договорів, участі у судових процедурах, подання заяв і отримання адміністративних послуг [19]. Правова ідентичність виступає фундаментом електронного громадянства, дозволяє встановлювати відповідальність за дії у кіберпросторі, запобігає шахрайству та забезпечує верифікацію правомірності цифрових транзакцій [20]. Її наявність є обов'язковою умовою легітимності будь-яких дій у межах електронної юрисдикції Держави [21].

Принцип алгоритмічної справедливості. Рішення, що приймаються за участю штучного інтелекту, мають бути прозорими, перевірюваними, підконтрольними людині та відповідати принципам законності, пропорційності й захисту прав людини [22]. У межах електронної юрисдикції алгоритмічна справедливість передбачає можливість аудиту моделей прийняття рішень [23], публічну доступність описів логіки функціонування систем, забезпечення можливості оскарження результатів, створених за участю AI, та обов'язкове втручання людини у випадках, що мають правові наслідки [24]. Держава гарантує, що використання штучного інтелекту у правових процесах не призводить до дискримінації, викривлення фактів чи маніпулювання доказами, а всі алгоритмічні інструменти проходять незалежну сертифікацію етичної та правової відповідності [25].

Принцип децентралізованої відповідальності. Суб'єкти цифрового права зобов'язані забезпечувати відповідність своїх дій нормам національного, міжнародного та етичного права незалежно від технічної форми їх реалізації або місця розташування технологічної інфраструктури [26]. Цей принцип передбачає, що відповідальність за наслідки цифрової діяльності несуть не лише фізичні чи юридичні особи, але й оператори платформ, власники алгоритмів, розробники смарт-контрактів, адміністратори децентралізованих систем та інші учасники цифрової екосистеми [27]. Децентралізована відповідальність означає колективний обов'язок суб'єктів забезпечувати прозорість, достовірність і безпечність транзакцій, запобігати порушенням прав людини, кіберзлочинам, маніпуляціям або створенню ризиків для цифрового суверенітету держави [28].

Принцип інтероперабельності. Цифрова юрисдикція Держави узгоджується з правовими режимами ЄС, Ради Європи, ООН, ISO та інших міжнародних інституцій, забезпечуючи можливість транскордонного визнання електронних документів, цифрових підписів і рішень судових або арбітражних органів [29]. Інтероперабельність охоплює технічну, правову та етичну сумісність систем [30]. Цей принцип створює основу для інтеграції електронної юрисдикції Держави у світовий цифровий правопорядок, де взаємне визнання даних і рішень гарантує довіру, прозорість і ефективність правових процесів [31].

9. Судова система цифрової юрисдикції. Держава забезпечує створення та функціонування цифрових судів, арбітражів і трибуналів нового покоління, які здійснюють правосуддя у повністю електронному форматі. Ці інституції уповноважені розглядати спори, що виникають з електронних правочинів, блокчейн-транзакцій, операцій із цифровими активами, діяльності у Метавсесвітах, DAO, смарт-контрактах та інших імерсивних середовищах, де взаємодіють люди, аватари або автономні агенти.

Рішення цифрових судів ухвалюються колегіально із застосуванням алгоритмічної підтримки аналізу доказів, проте остаточне рішення залишається за людиною-суддею. Такі рішення мають повну юридичну силу, підписуються цифровим підписом, автоматично реєструються у національному реєстрі та можуть бути виконані через смарт-контракти у межах електронної юрисдикції Держави.

Усі спори між суб'єктами цифрового права, незалежно від їхньої фізичної локації, виду технологій чи способу комунікації, підлягають вирішенню відповідно до норм електронної юрисдикції Держави, якщо інше прямо не передбачено міжнародними договорами або угодами про взаємне визнання юрисдикційних процедур.

Цифрова юрисдикція охоплює як спори між фізичними та юридичними особами, так і між автономними агентами, цифровими аватарами, роботизованими системами або гібридними штучними утвореннями, якщо їхня діяльність створює наслідки в

національному правовому полі. Такі спори можуть виникати у сфері виконання смарт-контрактів, розподілу цифрових активів, користування інтелектуальними технологіями, захисту персональних даних, інформаційної безпеки, кіберправопорушень, порушення умов цифрових ліцензій або алгоритмічних угод.

Цифрова юрисдикція поширюється також на ситуації, коли дії штучних агентів чи алгоритмічних систем спричиняють наслідки для прав, свобод або обов'язків людини — зокрема ухвалення автоматизованих рішень, управління цифровими об'єктами власності або створення цифрових зображень особи без згоди.

У межах цифрової юрисдикції забезпечується повна процесуальна рівність сторін, незалежно від їхньої природи — людської чи цифрової, — із правом на представництво, захист, апеляцію та виконання рішень у цифровій формі.

Держава створює та підтримує інтегровану цифрову екосистему цифрового правосуддя, що включає публічний реєстр електронних юрисдикційних рішень, систему електронного нотаріату, онлайн-свідчення, цифровий арбітраж, електронне засвідчення доказів і механізми миттєвого виконання рішень через смарт-контракти.

Публічний реєстр електронних рішень є відкритим блокчейн-ресурсом, що гарантує автентичність, незмінність і доступність рішень для всіх учасників цифрового правового процесу. Кожне рішення має унікальний криптографічний ідентифікатор, який дозволяє перевірити його походження, час ухвалення та юридичну силу.

Система електронного нотаріату забезпечує засвідчення дій, правочинів і цифрових підписів у повністю електронному форматі, а онлайн-свідчення передбачає можливість віддаленої участі сторін, свідків і експертів у процесуальних діях із дотриманням стандартів кібербезпеки та автентифікації.

Механізми миттєвого виконання рішень через смарт-контракти забезпечують автоматичне виконання судових або арбітражних актів у цифровому середовищі без необхідності додаткових адміністративних процедур. Уповноважені органи зобов'язані гарантувати повну прозорість процедур, захист персональних і комерційних даних, а також відповідність усіх рішень принципам справедливості, відкритості, підзвітності та міжнародної сумісності.

10. Відповідальність у електронній юрисдикції. Порушення законів цифрової юрисдикції, маніпуляції даними, спотворення цифрових доказів, несанкціоноване втручання у блокчейн-записи, знищення або підроблення електронних документів, а також відмова виконати електронне судове чи арбітражне рішення є підставою для настання юридичної відповідальності.

До таких порушень належать дії, що підривають довіру до систем електронного правосуддя, перешкоджають виконанню рішень або створюють ризики для національної безпеки в цифровому просторі. Вони тягнуть за собою застосування заходів у вигляді блокування цифрових ідентифікаторів, тимчасового обмеження доступу до цифрових ресурсів, анулювання реєстрацій, відкликання сертифікатів автентичності, накладення адміністративних санкцій, а в окремих випадках — ініціювання кримінального провадження.

Держава зобов'язується створити механізми моніторингу, фіксації та розслідування таких правопорушень із використанням цифрової криміналістики, систем аудиту даних і автоматизованих інструментів відстеження порушень для забезпечення прозорості та невідворотності відповідальності.

Разом з тим Держава розвиває культуру правового мислення у цифровому середовищі як складову національної ідентичності та інтелектуальної безпеки. Вона забезпечує підготовку та підвищення кваліфікації фахівців з електронного права,

кіберправа, цифрової етики та інформаційної безпеки, створює освітні програми нового покоління для юристів, суддів, прокурорів, державних службовців і технічних спеціалістів, які працюють у сфері цифрового врядування.

Розвиток правової освіти у межах цифрової юрисдикції включає запровадження спеціалізованих курсів, симуляцій електронних судових процесів, практику в цифрових лабораторіях права, дослідження алгоритмічних рішень і моделювання судових процесів у Метавсесвітах.

Також Держава сприяє створенню наукових, аналітичних і практичних платформ, що забезпечують адаптацію юриспруденції до нових форм електронного правосуддя, та підтримує міжнародну співпрацю у сфері правового регулювання штучного інтелекту, Метавсесвітів і цифрової економіки.

Важливим напрямом є формування етичних кодексів для юристів цифрової доби, розвиток правових досліджень у сфері нейромереж, автономних систем і алгоритмічних судових технологій, що забезпечують справедливість, прозорість і гуманність у застосуванні електронного правосуддя.

11. Ключові категорії електронної юрисдикції. Цифрова присутність — розширена правова категорія сучасного цифрового права, що означає юридично значущий факт активності суб'єкта чи об'єкта правовідносин у цифровому середовищі, незалежно від його фізичного місця перебування [32]. Вона охоплює як безпосередню участь у транзакціях, так і непрямі форми активності — створення цифрових профілів, функціонування аватарів [33], застосування смарт-пристроїв і сенсорних систем, присутність у Метавсесвітах чи XR-платформах. Цифрова присутність стає підставою для набуття прав і обов'язків, визначає можливість притягнення до юридичної відповідальності та є юридично значущим елементом у процесі встановлення електронної юрисдикції [34]. Вона враховує не лише факт, а й тривалість, інтенсивність і характер цифрової активності, а у випадку автономних агентів — алгоритмічну поведінку, яка прирівнюється до дій фізичних або юридичних осіб [35].

Віртуальна локалізація — розширена правова категорія, що означає механізм визначення належності цифрових транзакцій, даних чи правочинів до конкретної юрисдикції шляхом криптографічної та протокольної фіксації. Вона враховує географію серверів, структуру блокчейн-мереж, технічні протоколи передачі інформації та стандарти сертифікації та інші чинники, які визначають умовне “місце” існування цифрової події. Віртуальна локалізація дозволяє прив'язати дії у віртуальному середовищі до конкретної правової системи, навіть якщо вони здійснюються у децентралізованому чи транскордонному форматі. Вона забезпечує юридичну визначеність для електронних правочинів, унеможливорює анонімне ухилення від правових режимів та створює умови для інтеграції державних і міжнародних стандартів у єдину систему електронного правосуддя.

Алгоритмічне місцезнаходження — розширена правова категорія, що визначає юрисдикцію не за фізичною територією, а за тим, у межах якої цифрової мережі, протоколу чи блокчейну здійснено транзакцію, дію або правочин [36]. Це поняття відображає логіку розподілених систем, у яких правові наслідки визначаються архітектурою алгоритму та закладеними у нього правилами. Алгоритмічне місцезнаходження передбачає, що саме код і протокол виконують функцію нормативної “правової території”, коли географічна юрисдикція не здатна повноцінно регулювати цифрові правовідносини [37]. Алгоритмічне місцезнаходження забезпечує передумови для формування нових моделей електронного арбітражу, визнання рішень смарт-контрактів і становлення цифрового суверенітету спільнот [38].

Мультиюрисдикційний процес — розширена правова категорія, що охоплює сукупність правових відносин, які одночасно підпадають під дію кількох правових систем у цифровому середовищі. Це стосується ситуацій, коли транзакція або правочин здійснюються у глобальних блокчейн-мережах, Метавсесвітніх просторах чи хмарних інфраструктурах, а їхні наслідки одночасно регулюються різними національними та наднаціональними правовими режимами. Мультиюрисдикційний процес передбачає узгодження норм, запобігання правовим колізіям, визначення пріоритету застосування тієї чи іншої системи права та створення механізмів спільного вирішення спорів між суб'єктами різних юрисдикцій.

Транскордонна цифрова правосуб'єктність — розширена категорія правового статусу, що означає набуття фізичними чи юридичними особами прав та обов'язків одночасно у кількох цифрових правопорядках. Вона враховує участь суб'єктів у транскордонних блокчейн-мережах [39], Метавсесвітніх екосистемах, глобальних дата-хмарах і децентралізованих автономних організаціях (DAO), де правові наслідки формуються поза межами класичних територіальних кордонів держав [40]. Такий статус передбачає одночасне підпорядкування нормам різних юрисдикцій, визнання електронних ідентифікацій та правочинів у кількох правових системах, а також створення механізмів запобігання колізіям і подвійній відповідальності [41]. Транскордонна цифрова правосуб'єктність формує основу для глобальної інтероперабельності цифрового права та сприяє гармонізації правових режимів у сферах даних, контрактів і цифрової ідентичності [42].

Юрисдикція даних — розширений правовий режим, що визначає застосування права залежно від місця зберігання, обробки, передачі чи походження даних, у тому числі в умовах розподілених реєстрів і багаторівневих хмарних систем. Вона охоплює питання контролю за транскордонним рухом даних, застосування правових норм до глобальних дата-центрів, відповідальності за витоки чи маніпуляції з інформацією, а також забезпечення цифрового суверенітету держави [43]. Юрисдикція даних враховує як технічні параметри — геолокацію серверів, маршрутизацію трафіку, алгоритми шифрування — так і правові чинники: національне законодавство, міжнародні договори, політику локалізації та обміну даних. Її мета — гарантувати захист прав суб'єктів, прозорість обробки та сумісність національних режимів із міжнародними стандартами, зокрема у сфері GDPR, ISO/IEC і угод про вільний рух даних [44].

Віртуальний арбітражний форум — розширена правова конструкція, що означає спеціально створений цифровий простір або протокол, у межах якого сторони домовляються вирішувати спори незалежно від географічного розташування та національної юрисдикції [45, 46]. Такий форум може функціонувати у вигляді блокчейн-платформи, децентралізованої автономної організації (DAO) чи смарт-контрактної системи, яка автоматично забезпечує виконання арбітражних рішень на основі алгоритмічних правил [47, 48]. Віртуальний арбітражний форум гарантує нейтральність, прозорість і оперативність розгляду спорів, дозволяє застосовувати комбіновані методи доказування — цифрові сліди, блокчейн-записи, імерсивні реконструкції — та забезпечує юридичну визначеність і формування глобальної довіри у транскордонних цифрових відносинах [49].

Гібридна юрисдикція — це інтегрований правовий режим, що поєднує елементи фізичної, цифрової та алгоритмічної юрисдикції для врегулювання комплексних спорів [50, 51]. Вона застосовується у випадках, коли один правовий конфлікт охоплює одночасно фізичні дії, цифрові транзакції та алгоритмічні процеси, які взаємодіють у межах єдиної правової події [52]. Прикладом є ситуація, коли угода укладається у

віртуальному середовищі, підтверджується смарт-контрактом у блокчейні та має наслідки у фізичному світі (поставка товару чи надання послуги) [53]. Гібридна юрисдикція забезпечує єдність правозастосування, запобігає колізіям і дозволяє використовувати змішані механізми доказування: від класичних документів до блокчейн-записів і даних з Метавсесвіту. Вона також передбачає створення спеціалізованих арбітражних і судових інстанцій, здатних інтегрувати різні рівні доказів і забезпечувати комплексне техніко-правове вирішення спорів.

Протокольна юрисдикція — правовий режим, що визначається не територією, а стандартом чи технічним протоколом, на базі якого функціонує цифровий сервіс або мережа. Вона встановлює, що застосування норм права залежить від обраної архітектури протоколу комунікації: наприклад, якщо транзакція здійснена через Ethereum чи Hyperledger, саме ці протоколи задають базовий правовий каркас виконання зобов'язань. Протокольна юрисдикція враховує особливості мережових стандартів — ISO, W3C, TCP/IP, блокчейн-протоколи — їхню сумісність і правила безпеки, а також формує підстави для вирішення спорів у межах конкретного технологічного середовища.

Електронні особистості та аватари — правова категорія, що визначає правовий статус цифрових копій людини (аватарів, електронних особистостей, цифрових гуманоїдів), здатних самостійно діяти у Метавсесвіті [54]. Вона передбачає наділення їх частковою правоздатністю, визначення меж відповідальності за дії, виконані від імені власника чи автономно, встановлення порядку автентифікації ідентифікаційних даних та забезпечення легітимності їх існування в системі електронної юрисдикції.

Віртуальні немайнові активи — правова категорія, що охоплює цифрові об'єкти у Метавсесвіті (віртуальні земельні ділянки, NFT, цифровий контент), які не мають матеріальної форми, але визнаються цінністю та підлягають правовому регулюванню. Вона визначає правила володіння, користування, розпорядження, встановлює механізми підтвердження права власності та захисту від незаконного привласнення через смарт-контракти і блокчейн-реєстри.

Електронні правопорушення — особлива правова категорія, що фіксує дії, які мають протиправний характер виключно у цифровому середовищі (наприклад, маніпуляції з цифровими аватарами, шахрайство з NFT, зловживання імерсивними технологіями та інші дії, що не мають аналогів у фізичному просторі). Вона передбачає відмежування від аналогових правопорушень і встановлення нових стандартів юридичної кваліфікації та відповідальності у межах електронної юрисдикції [55].

Ідентифікаційні дані — правова категорія, що регулює порядок використання ідентифікаційних та персональних даних для створення, автентифікації та функціонування у Метавсесвіті віртуальних аватарів, цифрових двійників та електронних гуманоїдів. Вона передбачає застосування біометричних параметрів, IoT-ідентифікаторів та квантових криптографічних сертифікатів для забезпечення правової безпеки, автентичності та довіри у цифрових правовідносинах [56].

Режим електронного правосуддя — розширена правова категорія, що охоплює судові та квазі-судові механізми здійснення правосуддя у Метавсесвіті: від локальних віртуальних трибуналів до наднаціональних арбітражних палат. Вона визначає правила юрисдикційної підсудності, процедурного статусу учасників, гарантії справедливого процесу та алгоритмічні механізми оскарження рішень у цифровому чи змішаному середовищі правозастосування [57].

12. *Юридична архітектура цифрової юрисдикції.* Юридична архітектура цифрової юрисдикції:

Конституція Metaverse (Велика хартія законів, GLM) — це базовий метаправовий документ, що визначає засади цифрового суверенітету, гарантує права, свободи та обов'язки користувачів, а також регулює правовий статус алгоритмічних агентів, автономних систем і цифрових аватарів [58, 59]. Конституція задає структуру цифрового врядування, процедури арбітражу й координації міждержавних цифрових платформ, забезпечуючи стабільність і справедливість у всіх вимірах Metaverse [60].

GLM виступає архітектурним ядром електронної юрисдикції Metaverse, формуючи її як Meta-Legal Operating System — динамічну багаторівневу платформу для правового управління цифровими відносинами. Основними функціями GLM є: забезпечення сумісності між національними та алгоритмічними системами права; створення єдиної семантичної бази цифрових норм (Smart Law Ontology); підтримання етикоцентричної легітимності цифрових процесів; формування умов для глобальної міждержавної співпраці у сфері електронного правосуддя [61].

Загальні норми і структура законів Великої хартії визначають принципи цифрового нормотворення, методи узгодження між національними, корпоративними та глобальними правовими стандартами, а також встановлюють порядок створення, оновлення й валідації електронних норм [62].

Загальне право Metaverse (правовий, інституційний та технологічний простір Metaverse) формує систему прецедентів, норм поведінки та механізмів алгоритмічної справедливості [63]. Воно встановлює принципи рівності доступу до цифрового правосуддя, визначає алгоритми розгляду електронних спорів і стандарти поведінки у віртуальних середовищах. Загальне право Metaverse (WM) також регламентує умови створення, накопичення та застосування правових прецедентів у смарт-контрактах, визначає механізми узгодження норм між цифровими суб'єктами та національними правовими системами, забезпечуючи гнучкість, ефективність і справедливість у застосуванні електронного права [64, 65].

Судова система Metaverse — це багаторівнева архітектура електронного правосуддя, що охоплює цифрові суди, арбітражні протоколи, омбудс-агентів і модулі Smart Justice. Вона забезпечує справедливість і прозорість електронного правосуддя, охоплюючи як повністю автоматизовані, так і гібридні судові процеси, у межах яких рішення формуються за участю штучного інтелекту та людини. У межах Smart Justice реалізуються модулі цифрової медіації, автоматизованого арбітражу та моніторингу виконання судових рішень, що забезпечує ефективне, достовірне і безперервне функціонування електронного правосуддя у Metaverse.

Закон про електронний Офіс Metaverse (E-Office Act) регулює адміністративні, процедурні та організаційні аспекти управління діяльністю електронних суб'єктів, визначає механізми цифрової підзвітності, обліку та координації взаємодії між інституційними агентами у Metaverse [66]. Він установлює стандарти електронного документообігу, управління даними, порядок автентифікації посадових осіб, а також правила використання цифрових підписів. Крім того, E-Office Act створює правову основу для впровадження автоматизованих адміністративних процесів, систем електронного ліцензування, аудиту та контролю за діяльністю алгоритмічних адміністрацій у межах Metaverse [67].

Режим транскордонної взаємодії у Metaverse встановлює правові засади обміну даними, електронними доказами, міжюрисдикційного арбітражу та цифрової дипломатії [68]. Він визначає порядок взаємного визнання електронних ідентифікаторів, процедур автентифікації та застосування цифрових підписів між різними юрисдикціями,

забезпечуючи правову сумісність на рівні протоколів даних і транскордонних смарт-контрактів.

Кодекс фундаментальних технічних регламентів Metaverse визначає базові стандарти безпеки, сертифікації, криптографії, кіберзахисту та інтероперабельності.. Кодекс регламентує застосування стандартів ISO, IEEE, ITU та інших міжнародно визнаних норм, інтегруючи їх у єдину техно-правову екосистему Metaverse. Окремо передбачено положення щодо квантової стійкості криптографії, управління ризиками даних, енергетичної ефективності обчислень і надійності інфраструктур штучного інтелекту.

Регламент управління ідентифікацією Metaverse (Identity Governance Certificate) визначає порядок створення, верифікації та захисту цифрових ідентичностей [69, 70]. Він установлює процедури цифрової автентифікації, управління правами доступу та делегування ідентифікаційних повноважень у межах електронної юрисдикції [71, 72]. Сертифікат також передбачає механізми захисту персональних даних, запобігання підробкам, застосування децентралізованих ідентифікаторів (DID) і верифікованих облікових даних (VC), забезпечуючи безпечну взаємодію між людиною, організацією та алгоритмічними суб'єктами у середовищі Metaverse [73, 74].

Кодекс немайнових електронних активів Metaverse регулює обіг NFT, віртуальних земель, цифрових творів і даних як об'єктів права власності [75]. Він визначає правовий статус нематеріальних активів, порядок їх реєстрації, підтвердження авторства та передачі прав у цифровій формі. Кодекс встановлює правила обігу токенизованих об'єктів інтелектуальної власності, умови створення та використання цифрових сертифікатів володіння, а також механізми розв'язання спорів між власниками, платформами та розробниками [76]. Окрему увагу приділено питанням спадкування немайнових електронних активів, їх збереженню в децентралізованих реєстрах, а також захисту від маніпуляцій та фальсифікації метаданих. Таким чином, Кодекс створює правову основу для легітимного функціонування цифрової економіки власності у Metaverse [77].

Кримінальний електронний кодекс Metaverse визначає види злочинів у сфері кіберпростору, встановлює відповідальність за дії алгоритмічних агентів і забезпечує цифрову безпеку особи [78]. Кодекс охоплює норми, що регламентують запобігання, розслідування та притягнення до відповідальності за кіберзлочини. Він встановлює рівні відповідальності між людиною, розробником і автономною системою, визначає механізми електронного слідства, цифрової експертизи та доказової верифікації [79,80]. Крім того, Кодекс передбачає систему цифрової реабілітації, гарантії захисту прав жертв кіберзлочинів і принципи гуманного поводження в умовах електронного правосуддя у Metaverse [81,82].

Кодекс кіберзахисту Metaverse забезпечує правові режими кібероборони, реагування на інциденти та захист критичної цифрової інфраструктури [83]. Він визначає принципи кіберстійкості, управління ризиками та безперервності цифрових операцій, встановлює стандарти реагування на кібератаки й порядок координації між державними та приватними структурами у сфері кібербезпеки [84]. Кодекс передбачає створення системи раннього попередження, запровадження правового режиму кібермоніторингу, проведення аудиту безпеки критичних об'єктів і впровадження протоколів взаємодії у разі надзвичайних цифрових загроз [85].

Військовий регламент Metaverse встановлює норми цифрової оборони, алгоритмічного командування та гуманітарного права в умовах кіберконфліктів. Він визначає принципи застосування кіберсил, порядок взаємодії між військовими та

цивільними цифровими структурами, а також стандарти безпеки під час проведення віртуальних операцій. Регламент регламентує процедури управління автономними оборонними системами, здійснення контролю за використанням штучного інтелекту у військових цілях, правила ведення інформаційних операцій та захисту цивільного населення у кіберпросторі.

Великий електронний судовий кодекс Metaverse унормовує процедури електронного правосуддя, смарт-рішень і доказової аналітики на основі AI. Він деталізує процеси подання та розгляду електронних позовів, автоматизовану фіксацію доказів, алгоритмічне оцінювання обставин справи та порядок ухвалення рішень із використанням систем штучного інтелекту. Кодекс визначає стандарти цифрового процесуального права, регламентує роботу віртуальних судових залів, цифрових присяжних та арбітражних платформ, а також установлює правила електронної апеляції та перевірки справедливості смарт-рішень. Особливу увагу приділено забезпеченню прозорості, реалізації права на захист і дотриманню принципу людського контролю в умовах функціонування змішаних систем електронного судочинства Metaverse.

13. Регуляторні механізми. Легітимація цифрових доказів. Електронні документи, блокчейн-записи, цифрові сліди, дані з Метавсесвіту, телеметричні сигнали, біометричні показники, записи сенсорних пристроїв та результати діяльності автономних систем визнаються допустимими доказами за умови дотримання трьох ключових критеріїв: автентичність, цілісність, юридична придатність.

До категорії цифрових доказів також належать цифрові свідчення з Метавсесвіту, аудіо- та відеодані XR-середовищ, машинні журнали автономних систем, криптографічні лог-файли та результати алгоритмічного аналізу подій. Порядок їх легітимації визначається спеціальним протоколом Цифрового Кодексу, який забезпечує можливість подання, перевірки та оскарження таких доказів у межах алгоритмічної юрисдикції.

Віртуальні правочини. Укладення угод у цифровому середовищі — включно зі смарт-контрактами, DAO-рішеннями, алгоритмічними зобов'язаннями, цифровими меморандумами та автоматизованими транзакційними сценаріями — визнається рівнозначним офлайн-правочинам за умови дотримання комплексу вимог, визначених Цифровим Кодексом. До категорії віртуальних правочинів належать не лише економічні транзакції, а й управлінські рішення DAO, юридично значущі дії в метавсесвітах, алгоритмічні угоди між штучними агентами та взаємодії «людина – машина», які породжують зобов'язання або зміну правового статусу. Усі такі дії регулюються принципом **lex algorithmica**, за яким цифрові коди набувають правового значення за умови їх сертифікації та інтегрованості у систему електронної юрисдикції.

Відповідальність у мультиюрисдикційному середовищі. Учасники цифрових правовідносин несуть комбіновану, багаторівневу відповідальність залежно від цифрової приналежності, юрисдикційного статусу та характеру вчинених дій. Така відповідальність включає три взаємопов'язані рівні:

- первинна (національна) відповідальність — регулюється нормами держави реєстрації цифрового суб'єкта або юрисдикції, у межах якої розміщено його ключі, сервери чи інші засоби автентифікації;

- вторинна (транскордонна) відповідальність — застосовується у випадках впливу на права іноземних громадян, активів або цифрових платформ з урахуванням положень міжнародних договорів, цифрових конвенцій і принципів взаємного визнання;

– алгоритмічна відповідальність — покладається на розробників або власників автономних систем, чий код або штучний інтелект спричинили шкоду, збитки чи порушення прав.

Додатково передбачається принцип **екстериторіальної дії цифрових норм**, за яким національне законодавство може поширюватися на цифрові дії, що мають наслідки для громадян або національної інфраструктури, незалежно від місця виконання алгоритму чи зберігання даних.

Алгоритмічна юрисдикція. У справах, що виникають із застосування смарт-контрактів, блокчейн-протоколів, автономних агентів або гібридних систем штучного інтелекту, визначальними є логіка коду, механізм консенсусу та цифровий слід виконання алгоритму. Такі спори розглядаються в межах спеціального правового поля — **алгоритмічної юрисдикції**, що базується на принципах техноправової нейтральності, прозорості та відповідності міжнародним етичним стандартам. Алгоритмічна юрисдикція включає три основні рівні:

– технічний рівень — фіксація, аудит та відтворення алгоритмічних дій у блокчейні, перевірка цифрових підписів, хеш-ідентифікаторів і журналів транзакцій;

– юридичний рівень — правове тлумачення алгоритмічного коду, його еквівалентність традиційним нормам і визначення моменту настання правових наслідків;

– етичний рівень — оцінка рішень автономних систем на предмет дискримінації, непрозорості чи порушення принципу людського контролю.

Цифровий правовий аудит. Кожна цифрова система, що впливає на права осіб, обробляє персональні чи поведінкові дані, ухвалює рішення на основі алгоритмів або здійснює автоматизоване управління, підлягає періодичному комплексному правовому аудиту. Аудит проводиться міждисциплінарною комісією за участю юристів, технічних фахівців, етиків, аудиторів з кібербезпеки та представників громадськості. Процедура аудиту включає такі етапи: ідентифікація ризиків, техно-правова перевірка, етична оцінка (*human-in-the-loop*), оцінка кіберстійкості та безпеки, публічна звітність тощо.

Результати цифрового правового аудиту публікуються в Національному реєстрі аудиторських висновків, що забезпечує прозорість, підзвітність і можливість незалежної перевірки. Виявлені порушення можуть бути підставою для призупинення дії алгоритму або застосування регуляторних санкцій. Така система гарантує сталу відповідність технологій принципам етичності, прозорості, кіберстійкості та верховенства права.

14. Інституційна архітектура.

Національна комісія з електронної юрисдикції — це центральний координаційний орган цифрової державності, уповноважений забезпечувати системне впровадження, узгоджене тлумачення та належне застосування норм електронної юрисдикції в межах національного правового простору. Комісія здійснює функції стратегічного управління цифровим правопорядком, координує діяльність органів державної влади, судових інституцій, регуляторних структур і приватних цифрових платформ у сфері електронного врядування. До її повноважень входить: розроблення та експертиза проєктів нормативно-правових актів у сфері електронної юрисдикції; сертифікація і моніторинг безпеки національних цифрових інфраструктур; аудит транскордонних цифрових операцій і протоколів обміну даними; нагляд за дотриманням принципів цифрової етики, прав людини та кіберсуверенітету. Комісія формує та реалізує Національну стратегію електронної юрисдикції, координує державну участь у міжнародних цифрових ініціативах, а також забезпечує зворотний зв'язок між урядом, громадянським суспільством і цифровими суб'єктами через відкриті платформи

електронного консультування. Крім того, Комісія виконує функції національного центру арбітражної медіації у справах, що виникають між громадянами, державними системами, суб'єктами господарювання та алгоритмічними агентами в межах електронної юрисдикції.

Транснаціональний цифровий арбітраж — це міжнародна інституція нового покоління, створена як незалежна судова платформа для розгляду спорів у транскордонному цифровому просторі. Його архітектура побудована на технології блокчейну, що забезпечує повну прозорість, відкритість і неможливість зовнішнього втручання у процес ухвалення рішень. Арбітраж функціонує як цифровий суд з глобальною юрисдикцією щодо спорів, що виникають з використання смарт-контрактів, DAO-угод, криптоактивів, NFT-прав, кіберінцидентів і алгоритмічних порушень. Його діяльність ґрунтується на принципах техно-правової нейтральності, цифрової доброчесності та автоматизованої легітимації рішень. До складу Арбітражу входять міжнародні судді-експерти, сертифіковані етичні моделі AI та представники цифрових держав. Така гібридна структура забезпечує баланс між людською компетентністю, алгоритмічною неупередженістю та цифровим суверенітетом учасників процесу.

Цифрові омбудсмени — незалежні агенти, що діють у системі електронної юрисдикції з метою забезпечення захисту прав людини у цифровому середовищі. Вони функціонують у двох форматах: людські омбудсмени — представляють інтереси користувачів у правових процедурах; алгоритмічні е-омбудсмени — працюють у реальному часі, відстежують потенційні порушення цифрових прав і генерують превентивні рекомендації.

Цифрова прокуратура та AI-наглядові органи — це спеціалізовані інституції, відповідальні за виявлення, розслідування та переслідування порушень цифрових прав, зловживань даними, кіберзлочинів і неправомірних дій штучних агентів. Вони діють на засадах відкритого алгоритмічного права, використовують власні аналітичні системи для виявлення ризиків у цифрових транзакціях, проводять судово-технічні експертизи та координують діяльність з національними і міжнародними правоохоронними структурами.

Науково-експертна рада з цифрових технологій і права — постійно діючий міждисциплінарний орган, який забезпечує експертизу, прогнозування та розроблення стратегій цифрової трансформації правової системи. До її складу входять фахівці у сфері права, штучного інтелекту, етики, кібербезпеки, соціології та філософії. Рада здійснює правовий аналіз нових технологій, надає рекомендації щодо законодавчого регулювання, проводить оцінку соціального впливу (FRIA) та формує концепції правових інновацій у цифровій сфері.

Міжнародний офіс правового контролю — інституція, що забезпечує аудит та нагляд за дотриманням міжнародних стандартів цифрового права. Офіс здійснює моніторинг виконання рішень Транснаціональних цифрових арбітражів, координує діяльність цифрових судів, оцінює ефективність національних цифрових регуляторів та сприяє уніфікації практик електронної юрисдикції в міжнародному масштабі.

Центр цифрової медіації та алгоритмічної дипломатії — інституція, що поєднує правові, комунікаційні та техноетичні підходи до врегулювання конфліктів між цифровими державами, корпораціями, DAO-спільнотами та користувачами. Центр займається попередженням кризових ситуацій у кіберпросторі, організовує й проводить переговори між суб'єктами цифрових суперечок, а також розробляє дипломатичні протоколи та етичні кодекси для алгоритмічних взаємодій.

Академія цифрового права і юрисдикційних інновацій — освітньо-наукова платформа для підготовки фахівців нового покоління — юристів-конструкторів, експертів з електронної юрисдикції (е-юрисдикції) та аналітиків права штучного інтелекту. Академія впроваджує програми підготовки суддів і слідчих до роботи з цифровими доказами, організовує й проводить стажування в цифрових судах і створює міжнародні дослідницькі лабораторії з футуроюриспруденції.

15. Транскордонний режим електронної юрисдикції.

Принцип глобальної сумісності. Транскордонний режим цифрової юрисдикції базується на взаємному визнанні цифрових актів, сертифікатів, смарт-контрактів і судових рішень між державами — учасниками міжнародних конвенцій у сфері електронного права. Його мета — усунути прогалини між національними правовими режимами та сформувати єдиний цифровий простір правової довіри. Режим передбачає технічну інтероперабельність даних, правову гармонізацію та автоматизований обмін рішеннями між юрисдикціями через децентралізовану систему міждержавних реєстрів.

Принцип глобальної сумісності. Транскордонний режим цифрової юрисдикції — це комплексна система гармонізації цифрових правових норм, процедур і технічних стандартів між державами, корпораціями та міжнародними інституціями.

Він передбачає поєднання трьох взаємопов'язаних рівнів сумісності:

1. **Технічний рівень** — уніфікація форматів даних, алгоритмів шифрування, протоколів верифікації та кіберзахисту (зокрема відповідно до стандартів ISO 20022, W3C, ITU, NIST, ETSI тощо).

2. **Юридичний рівень** — гармонізація законодавства у сфері цифрових підписів, електронних документів, блокчейн-записів, смарт-контрактів, управління ідентифікаційними даними, XR-технологій, цифрової ідентичності тощо.

3. **Інституційний рівень** — створення мережі міждержавних органів координації, які забезпечують спільну правову політику, моніторинг та нагляд за її виконанням.

Режим глобальної сумісності реалізується через децентралізовану систему міждержавних реєстрів, яка забезпечує автоматизований обмін рішеннями, сертифікатами, доказами та транзакціями між юрисдикціями. Ці реєстри функціонують за принципом багаторівневого доступу: публічний — для відкритих актів, урядовий — для міждержавних угод, зашифрований — для конфіденційних справ.

Алгоритм визнання і виконання цифрових рішень. Визнання судових і арбітражних рішень, ухвалених у межах електронної юрисдикції, здійснюється через багаторівневу систему цифрової атестації: перевірка автентичності цифрового підпису та смарт-контрактного коду рішення; ідентифікація цифрового суб'єкта, проти якого винесено рішення; автоматичне внесення рішення до міжнародного реєстру з фіксацією дати, хеш-ідентифікатора та правового статусу.

Після проходження процедури верифікації рішення набуває юридичної сили на території інших учасників транскордонного режиму без потреби у додатковому судовому розгляді.

Цифрові угоди про взаємну юридичну співпрацю. Держави, корпорації та наднаціональні органи можуть укладати цифрові угоди про спільне врегулювання спорів, обмін доказами, проведення спільних розслідувань кіберінцидентів і взаємне виконання судових актів. Такі угоди зберігаються у міжнародному блокчейн-реєстрі й мають статус транскордонних смарт-договорів, що набувають чинності автоматично у разі виконання визначених умов співпраці.

Транскордонні цифрові угоди є базовим інструментом міжнародного правового партнерства між державами, корпораціями, наднаціональними структурами та

міжнародними організаціями. Вони спрямовані на координацію дій у сфері розслідування кіберінцидентів, обміну цифровими доказами, врегулювання спорів між суб'єктами різних юрисдикцій, а також на забезпечення взаємного визнання судових і арбітражних рішень.

Електронна ідентичність у транскордонному просторі. Для суб'єктів, що здійснюють діяльність у кількох юрисдикціях, запроваджується система уніфікованої цифрової ідентичності (Global DID), яка забезпечує автентифікацію, верифікацію та захист персональних даних під час транскордонних цифрових операцій і міждержавної взаємодії. Global DID є універсальним ключем доступу до сервісів транскордонного правосуддя, електронного нотаріату, арбітражу та цифрової медіації.

Протоколи транскордонного цифрового правосуддя визначають особливий порядок розгляду справ із міжнародним елементом. Для забезпечення технологічної сумісності та правової визначеності у таких справах діють спеціальні процесуальні стандарти:

1. Віддалене подання позову через електронну платформу юрисдикції походження з автентифікацією заявника засобами цифрової ідентичності;
2. Використання квантових ключів для шифрування доказів і захищеної передачі процесуальних документів між юрисдикціями;
3. Проведення судових засідань у форматі XR-середовищ з повною фіксацією цифрових даних, біометричних ідентифікаторів та доказових матеріалів;
4. Автоматизоване виконання судових рішень через децентралізований механізм виконання, інтегрований до міжнародного цифрового реєстру.

Ці протоколи забезпечують швидкість, прозорість і взаємне визнання правових процедур між державами, формуючи новий рівень алгоритмічної довіри у сфері електронного правосуддя.

Етичний і безпековий контур транскордонної взаємодії. Режим цифрової юрисдикції враховує питання цифрового суверенітету, захисту персональних даних, конфіденційності та недопущення використання транскордонних механізмів для кіберманіпуляцій або контролю над особистістю. З цією метою створюються спільні етичні ради, технічні комітети з питань кіберстійкості та механізми швидкого реагування на транскордонні інциденти.

Висновки. Цифрова юрисдикція як нова правова парадигма – це вже наближена реальність. Проведене дослідження підтверджує, що Цифрова юрисдикція є не просто похідною від інформаційного права, а самостійною системною категорією, яка поєднує правові, технічні, етичні та управлінські компоненти. Вона формує власний контур нормативної автономії — особливу сферу права, у межах якої виникають нові суспільні відносини, діють цифрові суб'єкти, алгоритмічні інституції та смарт-контракти, що виконують регуляторну функцію, замінюючи або доповнюючи класичні правові процедури.

Модель цифрової юрисдикції являє собою структурну правову модель, що складається з чотирьох взаємопов'язаних рівнів. Така модель забезпечує можливість реалізації концепції цифрової правотворчості шляхом використання смарт-контрактів, модульного оновлення норм і забезпечення транскордонної інтероперабельності правових систем. Її впровадження сприятиме формуванню універсального правового простору Metaverse, у межах якого врегулювання спорів, захист прав і легітимація дій здійснюватимуться в електронній площині.

Цифрова юрисдикція постає не лише об'єктом наукового дослідження, а інструментом цивілізаційного оновлення права, здатним інтегрувати гуманістичні

цінності в логіку штучного інтелекту та перетворювати правопорядок на гнучку, прозору й саморегульовану систему.

This article is published as open access under the Creative Commons Attribution 4.0 International License (CC BY 4.0), allowing the author to retain copyright. The CC BY 4.0 License permits the content to be copied, adapted, displayed, distributed, republished, or reused for any purpose, including adaptation and commercial use, as long as proper attribution is provided. Original: <https://sciformat.ca/journals/index.php/mssl/article/view/23>

Список використаної літератури:

1. Kostenko O.V. Electronic Jurisdiction, Metaverse, Artificial Intelligence, Digital Personality, Digital Avatar, Neural Networks: Theory, Practice, Perspective. World Science. 2022. 1(73). P. 1-13.
2. Barlow, J. P. (1996). Declaration of the Independence of Cyberspace. Available at: <https://www.eff.org/cyberspace-independence>.
3. Lessig, L. (1999). Code and other laws of cyberspace. New York: Basic Books.
4. Lessig, L. (1998). The Laws of Cyberspace. Taiwan Net '98 Conference. Available at: https://cyber.harvard.edu/works/lessig/laws_cyberspace.pdf.
5. Kaddoura, S., & Husseiny, F. (2023). The rising trend of Metaverse in education: challenges, opportunities, and ethical considerations. *PeerJ Computer Science*, 9. <https://doi.org/10.7717/peerj-cs.1252>.
6. Dwivedi, Y., Hughes, L., Baabdullah, A., Ribeiro-Navarrete, S., Giannakis, M., Al-Debei, M., Dennehy, D., Metri, B., Buhalis, D., Cheung, C., Conboy, K., Doyle, R., Dubey, R., Dutot, V., Felix, R., Goyal, D., Gustafsson, A., Hinsch, C., Jebabli, I., Janssen, M., Kim, Y., Kim, J., Koos, S., Kreps, D., Kshetri, N., Kumar, V., Ooi, K., Papagiannidis, S., Pappas, I., Polyviou, A., Park, S., Pandey, N., Queiroz, M., Raman, R., Rauschnabel, P., Shirish, A., Sigala, M., Spanaki, K., Tan, G., Tiwari, M., Viglia, G., & Wamba, S. (2022). Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. *Int. J. Inf. Manag.*, 66, 102542. <https://doi.org/10.1016/j.ijinfomgt.2022.102542>.
7. Mascitti, M. (2024). The Metaverse impact on the politics means. *Comput. Law Secur. Rev.*, 55, 106037. <https://doi.org/10.1016/j.clsr.2024.106037>.
8. Johnson, David Reynold and Post, David G., Law and Borders - the Rise of Law in Cyberspace. Stanford Law Review, Vol. 48, p. 1367, 1996, Available at SSRN: <https://ssrn.com/abstract=535> or <http://dx.doi.org/10.2139/ssrn.535>
9. Wang, Y. (2024). Do not go gentle into that good night: The European Union's and China's different approaches to the extraterritorial application of artificial intelligence laws and regulations. *Comput. Law Secur. Rev.*, 53, 105965. <https://doi.org/10.1016/j.clsr.2024.105965>.
10. Yang, Y. (2024). Analysis on the Extraterritorial Expansion and Conflict of Digital Prescriptive Jurisdiction. *Dispute Settlement*. <https://doi.org/10.12677/ds.2024.101017>.
11. Hildebrandt, M. (2013). Extraterritorial jurisdiction to enforce in cyberspace?: Bodin, Schmitt, Grotius in cyberspace. *University of Toronto Law Journal*, 63, 196-224. <https://doi.org/10.3138/UTLJ.1119>.
12. Li, K. (2022). Reconceiving Extraterritorial Jurisdiction. *German Yearbook of International Law*. <https://doi.org/10.5771/9783748933212>.
13. Ryngaert, C. (2023). Extraterritorial Enforcement Jurisdiction in Cyberspace: Normative Shifts. *German Law Journal*, 24, 537-550. <https://doi.org/10.1017/glj.2023.24>.
14. Leontiev, L. (2024). Conceptualising Extraterritoriality. Public International Law and Private International Law Considerations. *Global Jurist*, 24, 119-155. <https://doi.org/10.1515/gj-2023-0128>.
15. Sullivan, C., & Tyson, S. (2023). A global digital identity for all: the next evolution. *Policy Design and Practice*, 6, 433-445. <https://doi.org/10.1080/25741292.2023.2267867>.
16. Sullivan, C. (2018). Digital identity - From emergent legal concept to new reality. *Comput. Law Secur. Rev.*, 34, 723-731. <https://doi.org/10.1016/J.CLSR.2018.05.015>.

17. Vardanyan, L., Hamul'ák, O., & Kocharyan, H. (2024). Fragmented Identities: Legal Challenges of Digital Identity, Integrity, and Informational Self-Determination. *European Studies*, 11, 105-121. <https://doi.org/10.2478/eustu-2024-0005>.
18. Sedlmeir, J., Smethurst, R., Rieger, A., & Fridgen, G. (2021). Digital Identities and Verifiable Credentials. *Business & Information Systems Engineering*, 63, 603-613. <https://doi.org/10.1007/s12599-021-00722-y>.
19. Sullivan, C. (2023). Digital Identity as an International Legal Concept – New Disturbing Developments. *Georgetown Journal of International Affairs*, 24, 29-35. <https://doi.org/10.1353/gia.2023.a897698>.
20. Michałkiewicz-Kądziela, E., & Milczarek, E. (2022). Legal boundaries of digital identity creation. *Internet Policy Review*. <https://doi.org/10.14763/2022.1.1614>.
21. Wang, Y., Su, Z., Zhang, N., Liu, D., Xing, R., Luan, T., & Shen, X. (2022). A Survey on Metaverse: Fundamentals, Security, and Privacy. *IEEE Communications Surveys & Tutorials*, 25, 319-352. <https://doi.org/10.1109/COMST.2022.3202047>.
22. Sachan, S., & Liu, X. (2024). Blockchain-based auditing of legal decisions supported by explainable AI and generative AI tools. *Eng. Appl. Artif. Intell.*, 129, 107666. <https://doi.org/10.1016/j.engappai.2023.107666>.
23. Chiao, V. (2019). Fairness, accountability and transparency: notes on algorithmic decision-making in criminal justice. *International Journal of Law in Context*, 15, 126-139. <https://doi.org/10.1017/S1744552319000077>.
24. Rong, S. (2024). A legal study of transparency and fairness in algorithm-driven legal decision support systems. *Applied Mathematics and Nonlinear Sciences*, 9. <https://doi.org/10.2478/amns-2024-3386>.
25. Lee, M., Jain, A., Cha, H., Ojha, S., & Kusbit, D. (2019). Procedural Justice in Algorithmic Fairness. *Proceedings of the ACM on Human-Computer Interaction*, 3, 1 - 26. <https://doi.org/10.1145/3359284>.
26. Napieralska, A., & Kepczynski, P. (2024). Redefining Accountability: Navigating Legal Challenges of Participant Liability in Decentralized Autonomous Organizations. *ArXiv*, abs/2408.04717. <https://doi.org/10.48550/arXiv.2408.04717>.
27. Dwivedi, V., Pattanaik, V., Deval, V., Dixit, A., Norta, A., & Draheim, D. (2021). Legally Enforceable Smart-Contract Languages. *ACM Computing Surveys (CSUR)*, 54, 1-34. <https://doi.org/10.1145/3453475>.
28. Truong, N., Lee, G., Sun, K., Guitton, F., & Guo, Y. (2021). A Blockchain-based Trust System for Decentralised Applications: When trustless needs trust. *ArXiv*, abs/2101.10920. <https://doi.org/10.1016/J.FUTURE.2021.05.025>.
29. Djuraev, I., Baratov, A., Khujayev, S., Yakubova, I., Rakhmonova, M., Mukumov, B., & Abdurakhmanova, N. (2025). The Impact of Digitization on Legal Systems in Developing Countries. *Qubahan Academic Journal*. <https://doi.org/10.48161/qaj.v5n1a1246>.
30. Jimenez-Gomez, C. (2012). Implementing Interoperability in E-Justice's Criminal Area.
31. Malik, V., Mittal, R., Mavaluru, D., Narapureddy, B., Goyal, S., Martin, R., Srinivasan, K., & Mittal, A. (2023). Building a Secure Platform for Digital Governance Interoperability and Data Exchange Using Blockchain and Deep Learning-Based Frameworks. *IEEE Access*, 11, 70110-70131. <https://doi.org/10.1109/ACCESS.2023.3293529>.
32. Kalyvaki, M. (2023). Navigating the Metaverse Business and Legal Challenges: Intellectual Property, Privacy, and Jurisdiction. *Journal of Metaverse*. <https://doi.org/10.57019/jmv.1238344>.
33. Raposo, V. (2024). Beyond pixels and profiles: unveiling the legal identity of avatars in the metaverse. *Interactive Entertainment Law Review*. <https://doi.org/10.4337/ielr.2024.02.04>.
34. Noval, S., & Maaruf, I. (2024). Toward a Comprehensive Cyber Law Framework: Assessing Avatar Legal Liability. *China and WTO Review*. <https://doi.org/10.52152/cwr.2024.10.1.07>.
35. Barfield, W., & Williams, A. (2018). The law of virtual reality and increasingly smart virtual avatars. 2-43. <https://doi.org/10.4337/9781786438591.00008>.

36. Watters, C. (2023). When Criminals Abuse the Blockchain: Establishing Personal Jurisdiction in a Decentralised Environment. *Laws*. <https://doi.org/10.3390/laws12020033>.
37. Musthafa, A., Putri, R., Farizki, A., & Alma, S. (2024). Lex Cryptographia: Legal Extensions to Smart Contract Breaches and Governance in Blockchain Systems. *Jurnal Kajian Pembaruan Hukum*. <https://doi.org/10.19184/jkph.v4i2.53366>.
38. De Filippi, P., & Hassan, S. (2016). Blockchain Technology as a Regulatory Technology: From Code is Law to Law is Code. *First Monday*, 21. <https://doi.org/10.5210/FM.V21I12.7113>.
39. Garcia-Teruel, R., & Simón-Moreno, H. (2021). The digital tokenization of property rights. A comparative perspective. *Comput. Law Secur. Rev.*, 41, 105543. <https://doi.org/10.1016/J.CLSR.2021.105543>.
40. Tumakov, A. (2024). Digital and Virtual Objects of Modern Civil Turnover: The Issue of Differentiation of Concepts. *Lex Russica*. <https://doi.org/10.17803/1729-5920.2024.212.7.030-038>.
41. Glasze, G., Cattaruzza, A., Douzet, F., Dammann, F., Bertran, M., Bômont, C., Braun, M., Danet, D., Desforges, A., Géry, A., Grumbach, S., Hummel, P., Limonier, K., Münßinger, M., Nicolai, F., Pétiñaud, L., Winkler, J., & Zanin, C. (2022). Contested Spatialities of Digital Sovereignty. *Geopolitics*, 28, 919-958. <https://doi.org/10.1080/14650045.2022.2050070>.
42. Quinn, J. (2021). Geo-location technology: restricting access to online content without illegitimate extraterritorial effects. *International Data Privacy Law*. <https://doi.org/10.1093/idpl/ipab016>.
43. Ryngaert, C. (2023). Extraterritorial Enforcement Jurisdiction in Cyberspace: Normative Shifts. *German Law Journal*, 24, 537-550. <https://doi.org/10.1017/glj.2023.24>.
44. Quinn, J. (2021). Geo-location technology: restricting access to online content without illegitimate extraterritorial effects. *International Data Privacy Law*. <https://doi.org/10.1093/idpl/ipab016>.
45. (2021). OUP accepted manuscript. *Journal of International Dispute Settlement*. <https://doi.org/10.1093/jnlids/idab025>.
46. Okezie, P. (2024). Resolving Smart Contract Disputes Through Blockchain Arbitration. *Arbitration: The International Journal of Arbitration, Mediation and Dispute Management*. <https://doi.org/10.54648/amdm2024013>.
47. Wiegandt, D. (2022). Blockchain and Smart Contracts and the Role of Arbitration. *Journal of International Arbitration*. <https://doi.org/10.54648/joia2022029>.
48. Gabuthy, Y. (2023). Blockchain-Based Dispute Resolution: Insights and Challenges. *Games*, 14, 34. <https://doi.org/10.3390/g14030034>.
49. Aouidef, Y., Ast, F., & Deffains, B. (2021). Decentralized Justice: A Comparative Analysis of Blockchain Online Dispute Resolution Projects. 4, 1-8. <https://doi.org/10.3389/fbloc.2021.564551>.
50. Allouzi, A., & Alomari, K. (2023). Adequate legal rules in settling metaverse disputes: Hybrid legal framework for metaverse dispute resolution (HLFMDR). *International Journal of Data and Network Science*. <https://doi.org/10.5267/j.ijdns.2023.8.001>.
51. Gronic, I. (2023). Transforming Digital Dispute Resolution in India. *RUDN Journal of Law*. <https://doi.org/10.22363/2313-2337-2023-27-4-1113-1124>.
52. Atiyah, G., Ibrahim, A., & Jasim, A. (2024). Enforcement of smart contracts in cross-jurisdictional transactions. *International Journal of Law and Management*. <https://doi.org/10.1108/ijlma-06-2024-0220>.
53. Szabo, J., Bernard, C., & Philip, L. (2024). Legal Implications and Challenges of Blockchain Technology and Smart Contracts. *Computer Life*. <https://doi.org/10.54097/ztn2w848>.
54. Global, R., Oleksii, A., Oleksii, D., & Dmytro, Z. (2024). METAVERSE: ENSURING LEGAL RECOGNITION OF AVATARS AND ELECTRONIC PERSONALITIES THROUGH A CROSS-BORDER PERSONALIZED ID-CODE. *International Journal of Innovative Technologies in Social Science*. https://doi.org/10.31435/rsglobal_ijitss/30062024/8141.
55. Qin, H., Wang, Y., & Hui, P. (2022). Identity, Crimes, and Law Enforcement in the Metaverse. *ArXiv*, abs/2210.06134. <https://doi.org/10.1057/s41599-024-04266-w>.

56. Svantesson, D. (2013). A 'layered approach' to the extraterritoriality of data privacy laws. *International Data Privacy Law*, 3, 278-286. <https://doi.org/10.1093/IDPL/IPT027>.
57. Kostenko, O., Furashev, V., Zhuravlov, D., & Dniprov, O. (2022). Genesis of Legal Regulation Web and the Model of the Electronic Jurisdiction of the Metaverse. *Bratislava Law Review*. <https://doi.org/10.46282/blr.2022.6.2.316>.
58. Kostenko, O., Furashev, V., Zhuravlov, D., & Dniprov, O. (2022). Genesis of Legal Regulation Web and the Model of the Electronic Jurisdiction of the Metaverse. *Bratislava Law Review*. <https://doi.org/10.46282/blr.2022.6.2.316>.
59. Dwivedi, Y., Hughes, L., Baabdullah, A., Ribeiro-Navarrete, S., Giannakis, M., Al-Debei, M., Dennehy, D., Metri, B., Buhalis, D., Cheung, C., Conboy, K., Doyle, R., Dubey, R., Dutot, V., Felix, R., Goyal, D., Gustafsson, A., Hinsch, C., Jebabli, I., Janssen, M., Kim, Y., Kim, J., Koos, S., Kreps, D., Kshetri, N., Kumar, V., Ooi, K., Papagiannidis, S., Pappas, I., Polyviou, A., Park, S., Pandey, N., Queiroz, M., Raman, R., Rauschnabel, P., Shirish, A., Sigala, M., Spanaki, K., Tan, G., Tiwari, M., Viglia, G., & Wamba, S. (2022). Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. *Int. J. Inf. Manag.*, 66, 102542. <https://doi.org/10.1016/j.ijinfomgt.2022.102542>.
60. Bibri, S., & Allam, Z. (2022). The Metaverse as a virtual form of data-driven smart cities: the ethics of the hyper-connectivity, datafication, algorithmization, and platformization of urban society. *Computational Urban Science*, 2. <https://doi.org/10.1007/s43762-022-00050-1>.
61. Djuraev, I., Baratov, A., Khujayev, S., Yakubova, I., Rakhmonova, M., Mukumov, B., & Abdurakhmanova, N. (2025). The Impact of Digitization on Legal Systems in Developing Countries. *Qubahan Academic Journal*. <https://doi.org/10.48161/qaj.v5n1a1246>.
62. Uddin, M., Manickam, S., Ullah, H., Obaidat, M., & Dandoush, A. (2023). Unveiling the Metaverse: Exploring Emerging Trends, Multifaceted Perspectives, and Future Challenges. *IEEE Access*, 11, 87087-87103. <https://doi.org/10.1109/ACCESS.2023.3281303>.
63. Allouzi, A., & Alomari, K. (2023). Adequate legal rules in settling metaverse disputes: Hybrid legal framework for metaverse dispute resolution (HLFMDR). *International Journal of Data and Network Science*. <https://doi.org/10.5267/j.ijdns.2023.8.001>.
64. Watts, J. (2025). Law in the Metaverse. . <https://doi.org/10.5040/9781526530783>.
65. Tan, A. (2023). Metaverse Realities: A Journey Through Governance, Legal Complexities, and the Promise of Virtual Worlds. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.4393422>.
66. Chen, Z. (2023). Metaverse office: exploring future teleworking model. *Kybernetes*, 53, 2029-2045. <https://doi.org/10.1108/k-10-2022-1432>.
67. Ryu, J., Son, S., Lee, J., Park, Y., & Park, Y. (2022). Design of Secure Mutual Authentication Scheme for Metaverse Environments Using Blockchain. *IEEE Access*, 10, 98944-98958. <https://doi.org/10.1109/ACCESS.2022.3206457>.
68. Kalyvaki, M. (2023). Navigating the Metaverse Business and Legal Challenges: Intellectual Property, Privacy, and Jurisdiction. *Journal of Metaverse*. <https://doi.org/10.57019/jmv.1238344>.
69. Kostenko, O. (2021). IDENTIFICATION DATA MANAGEMENT: LEGAL REGULATION AND CLASSIFICATION. *Scientific Journal of Polonia University*. 43(6), 198-203. DOI: <https://doi.org/10.23856/4325>
70. Akramov, A., Rakhmonkulova, N., Khazratkulov, O., Inamdjanova, E., Imamalieva, D., Tuychieva, S., Ibodullaev, S., Ergashev, A., Khamidov, S., & Rustamova, N. (2024). The Impact of Digitalization in Inheritance Law. *Qubahan Academic Journal*. <https://doi.org/10.48161/qaj.v4n3a863>.
71. Kostenko, O. (2021). V. Identification of IoT: Origins of the Problem of Legal Regulation of Identity Data Management. *Juris Europensis Scientia*, 1, 77-83. DOI: <https://doi.org/10.32837/chern.v0i1.177.org/10.32837/chern.v0i1.177>
72. Kostenko, O. (2021). Management of Identification Data: Legal Regulation and Classification. *Young scientist*. 3(91), 90-94. DOI: <https://doi.org/10.32839/2304-5809/2021-3-91-21>
73. Chen, Z. (2025). Building a Legal Framework for the Metaverse: Digital Identity, NFT Property Rights, and Global Legal Structures. *Digital Society & Virtual Governance*. <https://doi.org/10.6914/dsvg.010104>.

74. Kostenko, O. (2021). Paradigms of identity data management in the light of the development of IoT devices and artificial intelligence. *Amparo*. 3, 42-47. DOI: <https://doi.org/10.26661/2616-9444-2021-3-06>
75. Wyczik, J. (2024). The rise of the metaverse: tethering effect and intellectual property of crypto tokens. *Journal Of Intellectual Property Law and Practice*. <https://doi.org/10.1093/jiplp/jpad124>.
76. García, R., Cedié, A., Teixidó, M., & Gil, R. (2022). Semantics and Non-fungible Tokens for Copyright Management on the Metaverse and Beyond. *ACM Transactions on Multimedia Computing, Communications and Applications*, 20, 1-20. <https://doi.org/10.1145/3585387>.
77. Limongelli, R., & Sposini, L. (2025). The (virtual) battle for intellectual property rights in the metaverse: The case of copyright, trademarks and the NFT technology. *Metaverse*. <https://doi.org/10.54517/m3056>.
78. Qin, H., Wang, Y., & Hui, P. (2022). Identity, Crimes, and Law Enforcement in the Metaverse. *ArXiv*, abs/2210.06134. <https://doi.org/10.1057/s41599-024-04266-w>.
79. Sallavaci, O. (2020). Rethinking Criminal Justice in Cyberspace: The EU E-evidence Framework as a New Model of Cross-Border Cooperation in Criminal Matters, 1-58. https://doi.org/10.1007/978-3-030-50613-1_1.
80. Casino, F., Pina, C., López-Aguilar, P., Batista, E., Solanas, A., & Patsakis, C. (2022). SoK: Cross-border Criminal Investigations and Digital Evidence. *ArXiv*, abs/2205.12911. <https://doi.org/10.48550/arXiv.2205.12911>.
81. Kostenko, O., Zhuravlov, D., Dniprov, O., & Korotiuk, O. (2023). METAVERSE: MODEL CRIMINAL CODE. *Baltic Journal of Economic Studies*. <https://doi.org/10.30525/2256-0742/2023-9-4-134-147>.
82. Arnell, P., & Fatureti, B. (2023). The prosecution of cybercrime – why transnational and extraterritorial jurisdiction should be resisted. *International Review of Law, Computers & Technology*, 37, 29-51. <https://doi.org/10.1080/13600869.2022.2061888>.
83. Pooyandeh, M., Han, K., & Sohn, I. (2022). Cybersecurity in the AI-Based Metaverse: A Survey. *Applied Sciences*. <https://doi.org/10.3390/app122412993>.
84. Fiaz, F., Sajjad, S., Iqbal, Z., Yousaf, M., & Muhammad, Z. (2024). MetaSSI: A Framework for Personal Data Protection, Enhanced Cybersecurity and Privacy in Metaverse Virtual Reality Platforms. *Future Internet*, 16, 176. <https://doi.org/10.3390/fi16050176>.
85. Srinivas, J., Das, A., & Kumar, N. (2019). Government regulations in cyber security: Framework, standards and recommendations. *Future Gener. Comput. Syst.*, 92, 178-188. <https://doi.org/10.1016/j.future.2018.09.063>.

~~~~~ \* \* \* ~~~~~