

Editori

Alexandru STANCIU, Carmen-Elena CÎRNU, Ionuț PETRE

Conexiuni în Metavers. Governanța Datelor



EDITURA 

Conexiuni în Metavers. Guvernanța Datelor



Notă editorială

În procesul de redactare și editare a acestui volum, au fost utilizate tehnologii Generative AI pentru optimizarea clarității textului și verificarea coerenței terminologice. Toate modificările și sugestiile AI au fost supuse unei revizuirii umane pentru a asigura conformitatea cu standardele academice și rigurozitatea științifică a lucrării. Ilustrațiile din această carte au fost realizate cu ajutorul tehnologiei de generare a imaginilor Midjourney.

Editori

Alexandru Stanciu, Carmen-Elena Cîrnu, Ionuț Petre

Autori

**Alexandru Stanciu, Carmen-Elena Cîrnu, Ionuț Petre
Ion-Alexandru Marinescu, Monica Barbu, Mădălina-Cornelia Zamfir
Ionuț-Emanuel Giura, Ella-Magdalena Ciupercă, Dragoș Iordache**

**Conexiuni în Metavers.
Guvernanța Datelor**

EDITURA 

București, 2025

Copyright © 2025, Editura ICI
Toate drepturile asupra acestei ediții sunt rezervate editurii.



Procesare PC
Alexandru Mihai Manolescu

Copertă
Imaginea a fost generată cu Midjourney
(<https://midjourney.com>) după un prompt definit de
Alexandru Stanciu & ChatGPT

Corectură Redacțională
Mihaela Căliment

Layout & Prepress
Iuliana Panciu

ISBN 978-606-95858-3-2

Cuprins

Cuvânt înainte	7
I. Metavers - guvernanta și reglementări	13
1. Metaversul între noi oportunități și provocări	15
Definiții și interpretări ale Metaversului	19
Servicii publice, educație și gaming în Metavers: direcții de dezvoltare	22
Viziune versus pragmatism în Metavers	40
2. Guvernanța datelor și reglementarea Inteligenței Artificiale	45
Rolul datelor în Metavers	46
Guvernanța datelor în sisteme bazate pe Inteligența Artificială	52
Reglementări referitoare la Inteligența Artificială și guvernanța datelor	64
II. Tehnologiile emergente: factor-cheie în transformarea societății	81
3. Utilizarea Metaversului în administrația publică	83
Aplicații potențiale ale Metaversului în administrația publică	86
Cercetare pe baza unui focus grup	90
4. Ar putea fi Metaversul o soluție pentru orașele inteligente?	101
Tranziția orașelor către neutralitatea climatică	101
Agricultura urbană ca posibilă soluție inovatoare?	114
Considerații privind guvernanța datelor	130
III. Guvernanța datelor în Metavers	165
5. De ce este importantă guvernanța datelor?	167
Rolul și importanța datelor în organizații	167
Provocări în gestionarea și utilizarea eficientă a datelor	171
Context tehnologic și organizațional	176
Principalele abordări în guvernanța datelor	177
Definiția și rolul guvernanței datelor	178
Rolul și responsabilitățile în guvernanța datelor	181
Introducere în conceptul de Data Governance Framework (DGF)	183
Guvernanța datelor în Metavers: de la principii clasice la spații virtuale interconectate	187

6. Modele și exemple de cadre de guvernanță a datelor	191
Prezentare generală a principalelor cadre de guvernanță a datelor	191
Analiză detaliată a principalelor cadre de guvernanță a datelor	194
Analiză comparativă a modelelor de guvernanță a datelor	203
7. Componentele de bază ale unui cadru de guvernanță a datelor în Metavers	209
Principii de guvernanță a datelor în Metavers	209
Pilonii care susțin cadrul de guvernanță a datelor în Metavers	213
Componentele de bază ale unui cadru de guvernanță a datelor în Metavers	234
IV. Perspective finale	245
8. Arhitectura încrederii într-un viitor imersiv	247
Bibliografie	253
Despre autori	267

Cuvânt înainte

De-a lungul istoriei, tehnologia a fost un catalizator al transformării umane. De la revoluția industrială la revoluția digitală, fiecare nouă paradigmă a redefinit modul în care trăim, lucrăm și interacționăm.

Astăzi, ne aflăm în pragul unei noi metamorfoze, una care ne permite nu doar să navigăm în lumi virtuale, ci să le modelăm, să le locuim și să le transformăm după propriile noastre aspirații.

Metaversul reprezintă următoarea frontieră a spațiului virtual, un mediu în care granițele dintre real și digital se estompează, iar posibilitățile devin aproape infinite.

Într-un context în care tehnologii precum realitatea virtuală și inteligența artificială devin tot mai performante și interconectate, Metaversul se redefineste prin valențe noi și surprinzătoare: dacă la început s-a manifestat prin simple jocuri și platforme de socializare, astăzi ajunge să includă spații de lucru virtuale, medii de învățare și creativitate, precum și zone dedicate divertismentului sau chiar comerțului. Într-o epocă marcată de inovații tehnologice accelerate, Metaversul începe să se contureze ca o nouă dimensiune a interacțiunilor umane.

Dincolo de definițiile riguroase și de entuziasmul generat de amploarea posibilităților sale, se conturează o întrebare inedită: poate fi Metaversul văzut ca un sistem viu, cu propriile sale mecanisme de creștere și adaptare? În ce măsură, în funcție de perspectivele pe care le adoptăm, își poate găsi această analogie justificări în caracteristicile comune dintre un ecosistem virtual și un organism viu?

Într-adevăr, privind potențialul de transformare și evoluție continuă a Metaversului, am putea fi tentați să îl asociem cu un fluture — un simbol al renașterii și al libertății. Asemenea acestuia, ideea unui spațiu virtual comun a trecut printr-un proces de metamorfoză. A pornit ca o omidă, fragilă și limitată de tehnologiile primitive ale realității virtuale. Ulterior, prin progresul continuu și interconectarea globală, s-a transformat într-un fluture, simbol al frumuseții, libertății și conectivității. La fel cum unii fluturi migrează pe distanțe lungi, creând punți între ecosisteme diferite, Metaversul depășește barierele geografice, culturale și economice, aducând oamenii împreună într-o realitate partajată.

Însă, pe măsură ce ne aprofundăm explorarea, descoperim că Metaversul nu este doar un spațiu de transformare, ci și unul de adaptare continuă. Nu este un simplu fluture, ci mai degrabă un cameleon - un cameleon cibernetic. Asemenea

acestui fascinant animal, Metaversul are capacitatea de a se ajusta la mediul în care se află, de a se integra organic în diverse contexte și de a oferi experiențe unice fiecărui utilizator.

Cameleonul își schimbă culoarea pentru a se adapta la mediul înconjurător, iar acest mecanism reflectă exact flexibilitatea Metaversului. Acesta nu este un simplu spațiu de divertisment, ci un mediu multifuncțional, capabil să se modeleze în funcție de necesitatea utilizatorilor. Poate deveni o sală de clasă virtuală în educație, un instrument de simulare pentru politici urbane în administrația publică sau o piață digitală pentru economie. Adaptabilitatea sa este esențială pentru viitorul nostru digital.

O caracteristică remarcabilă a cameleonului este vederea sa independentă, similar modului în care Metaversul permite explorarea simultană a mai multor realități. Utilizatorii pot interacționa prin diverse avatururi, pot participa la experiențe variate și pot colabora indiferent de distanța fizică. Metaversul nu oferă doar o simplă fereastră către o lume virtuală, ci o rețea imersivă în care percepția noastră asupra realității se extinde dincolo de limitele tradiționale.

Cameleonul nu rămâne niciodată static, ci se adaptează permanent la condițiile mediului în care trăiește. În mod similar, Metaversul este un sistem viu, aflat într-o continuă evoluție. De la progresele din inteligența artificială, la blockchain, cloud computing și realitatea mixtă, tehnologiile emergente modelează Metaversul în moduri imprevizibile. Nu este un produs finit, ci un ecosistem care se transformă odată cu utilizatorii săi.

Această carte explorează multiplele fațete ale Metaversului, analizând impactul său asupra societății, economiei, educației și inovației. Cameleonul cibernetic nu se limitează la o singură formă sau funcție, ci continuă să se reinventeze, adaptându-se la nevoile și aspirațiile cetățenilor digitali.

Pe măsură ce ne aventurăm în acest univers digital, să nu uităm că Metaversul nu este doar o destinație, ci un proces continuu de explorare, adaptare și transformare. Aceasta nu este o promisiune a evadării din cotidian, ci mai degrabă o invitație la explorarea posibilităților nelimitate create de interacțiunea dintre tehnologie, imaginație și nevoile umane. Dincolo de limitele spațiului fizic, Metaversul și universurile virtuale adiacente oferă o privire în viitor, unde fiecare idee sau proiect poate fi dezvoltat în moduri până acum imposibile.

În acest nou „teren de joacă” digital, valorile cu care ne-am obișnuit – precum creativitatea, colaborarea și inovația – devin resurse primare, iar barierele clasice se dizolvă. Aici, granițele geografice dispar și răsar noi oportunități pentru învățare, afaceri, divertisment și, nu în ultimul rând, pentru exprimare personală. Realitatea obișnuită devine doar o platformă de start, un cadru care își extinde limitele prin realitatea virtuală și augmentată, prin inteligența artificială și prin tehnologii a căror evoluție rapidă ne provoacă să ne adaptăm în permanență.

Într-o astfel de lume, orașele pot fi gândite ca spații flexibile, interconectate, în care inovația și sustenabilitatea nu mai sunt concepte teoretice, ci instrumente reale pentru dezvoltare. Politicile publice, serviciile educaționale și chiar practicile comerciale se regândesc din temelii pentru a se potrivi noului cadru digital, deschizând astfel calea unor colaborări internaționale și a unei implicări civice sporite.

Totodată, acest orizont extins pune în prim-plan importanța guvernancei datelor și a eticii, deoarece informațiile devin noul „aur” al societății conectate. Într-o lume în care realitatea nu mai este limita, ci doar un punct de pornire, modul în care colectăm, stocăm și utilizăm datele poate influența puternic felul în care se dezvoltă noile ecosisteme digitale. A construi încredere și a proteja drepturile individuale în timp ce valorificăm tehnologiile emergente, reprezintă una dintre cele mai mari provocări pe care viitorul ni le rezervă.

Astfel, a explora Metaversul și a înțelege complexitatea guvernancei datelor echivalează cu a face primii pași într-o nouă eră a umanității – una în care limitele realității sunt reconceptuate, iar posibilitățile devin infinite

Reflectând asupra problematicii guvernancei datelor, ne putem gândi că aceasta se poate rezuma prin răspunsul la întrebarea „Cine are autoritate și control asupra datelor și cum se manifestă aceasta?”

Scena complexă a datelor este guvernată de o rețea interconectată de entități, fiecare exercitând autoritate și control prin diverse mecanisme. Nu există o singură entitate care să dețină puterea absolută, ci mai degrabă un echilibru dinamic și adesea tensionat între diferiți actori.

Guvernele stabilesc cadrul legal general pentru protecția și circulația datelor. Printr-o legislație adaptată la societatea digitală, precum Regulamentul General privind Protecția Datelor (GDPR) în Uniunea Europeană, guvernele impun reguli stricte companiilor și instituțiilor publice privind colectarea, stocarea și prelucrarea datelor personale, astfel încât agențiile guvernamentale pot accesa date doar în scopuri de securitate națională, în condițiile legale prevăzute.

Corporațiile exercită un control semnificativ prin intermediul politicilor interne și a termenilor și condițiilor pe care utilizatorii trebuie să le accepte. Companiile mari de tehnologie, în special, colectează volume uriașe de date despre utilizatori, pe care le folosesc pentru a-și personaliza serviciile, pentru publicitate țintită și pentru dezvoltarea de noi produse. Ele dețin infrastructura tehnică (servere, centre de date) unde datele sunt stocate și procesate.

Indivizii au, teoretic, dreptul fundamental la protecția datelor lor. Legislația modernă le conferă drepturi specifice, cum ar fi dreptul de a fi informat, dreptul de

acces, de rectificare și de ștergere a datelor („dreptul de a fi uitat”). Cu toate acestea, exercitarea efectivă a acestor drepturi poate fi dificilă, necesitând cunoștințe tehnice și juridice.

Controlul asupra datelor se manifestă printr-o serie de mecanisme tehnice, legale și administrative care reglementează modul în care datele sunt gestionate și protejate. Astfel, legile și reglementările formează fundamentul controlului datelor, stabilind drepturi și obligații clare. GDPR este un exemplu de referință, impunând principii precum limitarea scopului, minimizarea datelor și responsabilitatea operatorului.

Totodată însă, fiecare companie își definește propriile reguli interne pentru gestionarea datelor. Aceste politici acoperă aspecte precum clasificarea datelor, controlul accesului, procedurile de răspuns la incidente de securitate și perioadele de retenție.

Pentru a facilita transferul de date între diferite jurisdicții (de exemplu, între UE și SUA), sunt necesare acorduri speciale care să garanteze un nivel adecvat de protecție. Aceste acorduri, precum fostul „Privacy Shield”, sunt esențiale pentru economia digitală globală.

Controlul efectiv este imposibil fără măsuri tehnice robuste. Acestea includ criptarea datelor (atât în repaus, cât și în tranzit), pseudonimizarea, autentificarea multi-factor și auditurile regulate de securitate. Mecanismele prin care indivizii își pot exercita controlul direct includ portaluri de confidențialitate, posibilitatea de a descărca propriile date și proceduri clare pentru a depune plângeri la autoritățile de supraveghere.

Tensiunile dintre actorii implicați generează o serie de provocări complexe care definesc dezbaterile actuale privind controlul datelor. Spre exemplu, statele doresc să își afirme autoritatea asupra datelor generate pe teritoriul lor (suveranitatea datelor), uneori impunând ca acestea să fie stocate local. Acest lucru intră în conflict cu natura globală a internetului și cu modelul de afaceri al multor companii multinaționale, care se bazează pe fluxul liber de date.

De asemenea, există un conflict inerent între dreptul la viață privată al individului și dorința companiilor de a monetiza datele, precum și interesul guvernelor de a le utiliza pentru supraveghere și aplicarea legii. Găsirea unui echilibru just între aceste interese este una dintre cele mai mari provocări.

Nu în ultimul rând, dezvoltarea rapidă a tehnologiilor precum inteligența artificială (AI) și Internetul lucrurilor (IoT) generează noi modalități de colectare și prelucrare a datelor, adesea depășind capacitatea cadrului legal de a se adapta. Asigurarea că inovația se desfășoară într-un mod care respectă drepturile fundamentale este esențială pentru a menține încrederea publicului.

Lucrarea este organizată în patru părți distincte, fiecare contribuind la construirea unui cadru conceptual, practic și etic. Prima parte, „Metavers – guvernanta și reglementări”, fundamentează conceptul de Metavers și investighează implicațiile juridice și sociale ale acestuia. Sunt analizate principalele tehnologii convergente – de la realitate virtuală la blockchain – și reglementările esențiale, precum GDPR sau AI Act, într-un efort de a înțelege nu doar ce este Metaversul, ci și în ce limite legale și etice trebuie să funcționeze. Această secțiune oferă o privire clară asupra tensiunii dintre inovație și reglementare, propunând o abordare echilibrată între entuziasmul tehnologic și responsabilitatea juridică.

A doua parte, „Tehnologiile emergente – factor-cheie în transformarea societății”, face tranziția de la teorie la practică. Sunt examinate modurile concrete prin care Metaversul poate contribui la transformarea serviciilor publice, administrației urbane și educației. Prin studii de caz și inițiative internaționale, se demonstrează că aceste tehnologii nu sunt doar instrumente speculative, ci soluții reale pentru provocări contemporane. Se conturează astfel o viziune pragmatică, în care tehnologiile imersive devin catalizatori pentru orașe inteligente și guvernanta participativă.

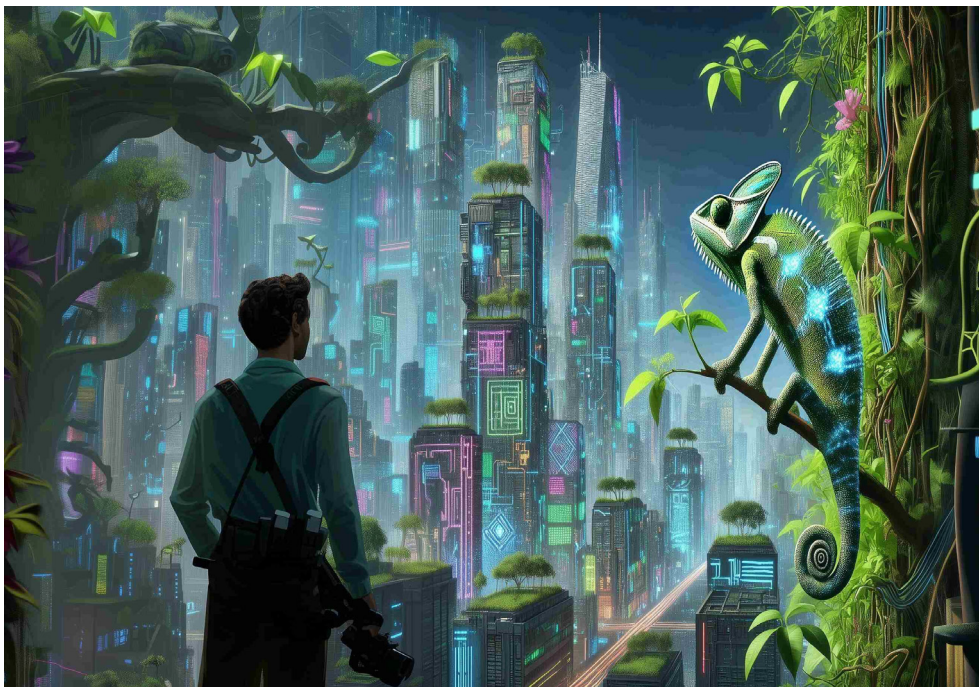
Partea a treia, „Guvernanta datelor în Metavers”, reprezintă nucleul metodologic și aplicativ al cărții. Aici este definită în mod riguros noțiunea de guvernanta a datelor și sunt prezentate principalele modele internaționale, de la DAMA DMBOK la ISO/IEC 38500. În această secțiune propunem un cadru inovator, specific pentru Metavers, adaptat particularităților sale: identitate digitală, date biometrice, interacțiuni în timp real. Se pune accent pe principii precum etica, interoperabilitatea și reziliența digitală, oferind un model scalabil și transparent pentru gestionarea datelor în noile spații virtuale.

Partea a patra, „Perspective finale” oferă o viziune integratoare asupra universului analizat. Conceptul de „arhitectură a încrederii” devine central: fără o guvernanta solidă a datelor și fără instituții credibile, Metaversul riscă să devină un spațiu al haosului și al manipulării. Este subliniată importanța colaborării între guverne, companii și cetățeni, dar și nevoia unei educații digitale care să permită utilizatorilor să navigheze acest nou mediu în mod informat și responsabil. În loc de concluzie, această secțiune lansează o invitație: să construim un Metavers etic, sigur și incluziv, în care tehnologia să servească binele comun.

Partea I.
Metavers - guvernarea și reglementări



1. Metaversul între noi oportunități și provocări



În era digitală modernă, inovațiile tehnologice au transformat profund modul în care interacționăm, lucrăm și învățăm. Unul dintre cele mai revoluționare concepte emergente în acest context este Metaversul care promite să redefinească limitele realității virtuale (Aspen Institute, 2024). Acest spațiu virtual nu se limitează doar la replicarea lumii fizice, ci oferă oportunități nelimitate pentru explorare, creativitate și eficiență, integrând tehnologii avansate precum realitatea augmentată (AR), realitatea virtuală (VR), inteligența artificială (AI) și Internetul lucrurilor (IoT) (OECD, 2022; Huang et al., 2023; Aspen Institute, 2024)

Cuvântul Metavers provine din alipirea prefixului „meta”, ce simbolizează „dincolo” cu sufixul „vers”, prescurtarea pentru „univers”. În acest sens, se referă literalmente la un univers dincolo de lumea fizică. Mai precis, acest „univers de dincolo” simbolizează o lume generată de computer, deosebindu-l de concepțiile metafizice sau spirituale specific umane. De asemenea, Metaversul se referă la un mediu digital tridimensional complet imersiv, în contrast cu conceptul mai incluziv de spațiu cibernetic care reflectă totalitatea spațiului online partajat în toate

dimensiunile reprezentării. Viziunea asupra structurii și organizării Metaversului a evoluat semnificativ de-a lungul timpului. Inițial, perceput ca o extensie singulară și amplificată a unei lumi virtuale individuale, Metaversul este acum conceptualizat ca o rețea complexă și interconectată de lumi virtuale, care formează un ecosistem digital vast și dinamic. Neal Stephenson, care a inventat termenul în romanul său din 1992 intitulat *Snow Crash*, a oferit o descriere vizionară a acestuia, imaginându-l ca o formă de reprezentare virtuală complexă a unui univers digital. În viziunea lui Stephenson asupra Metaversului, accesul utilizatorilor, reprezentați sub forma avatarurilor digitale, se realizează prin intermediul unor terminale computerizate. Aceste dispozitive proiectează imagini de realitate virtuală pe lentile speciale și transmit sunet stereo digital prin căști integrate, care se conectează discret la urechile utilizatorului, oferind o experiență imersivă completă. Utilizatorii Metaversului beneficiază de posibilitatea de a-și personaliza avatarurile, singura limitare fiind impusă asupra înălțimii pentru a preveni reprezentările excesiv de disproportionale. Aceștia pot explora spațiul virtual fie pe jos, fie utilizând vehicule virtuale, pot construi structuri pe terenuri digitale achiziționate și se pot implica într-o gamă variată de activități sociale și funcționale care reflectă complexitatea interacțiunilor umane. În esență, Metaversul pe care Stephenson l-a imaginat este, atât în formă, cât și în funcționare, o lume virtuală întinsă și puternic populată, care funcționează nu ca un mediu de joc cu parametri și obiective specifice, ci ca o cultură digitală deschisă care operează în paralel cu domeniul fizic. De când a apărut romanul lui Stephenson, progresele tehnologice au permis implementarea în viața reală a lumilor virtuale și au fost dezvoltate concepții mai complexe și mai extinse despre Metavers.

Pentru a înțelege stadiul actual și viitorul spațiilor virtuale 3D, analizăm evoluția istorică a lumilor virtuale, incluzând jocurile video și progresele tehnologice care au modelat Metaversul. Aceste perspective sunt considerate elemente structurale ale progresului tehnologic, depășind statutul de manifestări culturale izolate.

Lumile virtuale sunt medii digitale persistente, create de computer, care permit utilizatorilor din locații fizice distincte să interacționeze în timp real, fie pentru activități profesionale, fie pentru divertisment. Acestea reprezintă un subset al aplicațiilor de realitate virtuală, un concept mai larg ce desemnează simulări computerizate ale obiectelor sau mediilor tridimensionale, oferind utilizatorilor o interacțiune aparent autentică și intuitivă.

Studiul primelor forme de Metavers a demarat încă din anii 1950, când oamenii de știință au început să fie preocupați de augmentarea simțurilor omului, de transpunerea caracteristicilor realității în diferite formate. În anul 1956, Morton Geiling a creat *Sensorama* - prima mașină de realitate virtuală, capabilă să afișeze imagini în spațiul tridimensional. În anul 1970, MIT (Massachusetts Institute of Technology) a creat *Aspen Movie Map*, o cameră cu capacități de măsurare a

distanței, cu senzor optic ce înregistra și transpunea casele în spațiul 3D. Începând cu anii 1990, Sega a introdus conceptul de realitate virtuală, dezvoltând o pereche de ochelari VR care predimensiona spațiul vizual al jucătorilor. În anul 2010, Palmer Luckey a creat primul prototip VR Oculus Rift ce permitea utilizatorului să vizualizeze datele multimedia către unghiuri de 90 grade.

Dezvoltarea lumilor virtuale cuprinde o istorie detaliată în care actele de imaginație literară și inovațiile în jocuri au dus la progrese în platformele virtuale deschise, orientate social. Istoria aceasta poate fi împărțită în cinci faze definitorii:

În faza inițială, începând cu sfârșitul anilor 1970, lumile virtuale bazate pe text au apărut în două modalități:

MUD-urile (Multi-User Dungeons) au implicat crearea de realități fantastice care semănau cu Stăpânul Inelelor al lui Tolkien sau cu jocul de rol cu zaruri Dungeons and Dragons. Opera de bază a literaturii fantastice din secolul al XX-lea a lui Tolkien servește drept sursă de inspirație pentru multe dintre jocurile și mediile lumii virtuale care au fost dezvoltate ulterior. Pe de altă parte, Dungeons and Dragons, proiectat inițial de Gary Gygax și Dave Arneson este considerat pe scară largă drept începutul jocurilor de rol moderne (Dionisio et al., 2013).

MUSH-urile (Multi-User Shared Hallucinations) au reprezentat medii digitale mai puțin structurate, concepute pentru a încuraja explorarea deschisă și colaborarea creativă. Aceste spații ofereau utilizatorilor posibilitatea de a contribui împreună la construcția unui univers virtual, experimentând noi forme de interacțiune și creație colectivă.

A doua fază de dezvoltare a avut loc aproximativ un deceniu mai târziu, atunci când Lucasfilm a fost inspirat parțial de publicarea romanului cyberpunk al lui William Gibson, *Neuromancer* (1984), care a popularizat conceptul timpuriu al spațiului cibernetic, ca de exemplu „Matrix”. Astfel, Lucasfilm a introdus Habitat pentru Commodore 64 în 1986 și platforma Fujitsu în 1989. Habitat a fost prima aplicație comercială de mare profil a lumii virtuale tehnologice și prima lume virtuală care încorporează o interfață grafică. Această interfață grafică inițială era totuși bidimensională, în 2D, comparativ cu spațiul tridimensional, iar mediul online prezenta utilizatorului o viziune asemănătoare cu o animație primitivă care funcționează la viteze mici prin modemuri de tipul dial-up. Habitat a fost, de asemenea, prima lume virtuală care a folosit termenul „avatar”, termen preluat din sanscrită care înseamnă „apariția sau manifestarea deliberată a unei zeități pe pământ” (Dionisio et al., 2013) pentru a descrie rezidenții sau utilizatorii săi digitali. Această utilizare contemporană a termenului de avatar implică o transpunere a conștiinței într-o nouă formă, mai exact de la un corp uman la o reprezentare digitală. Munca de pionierat în sistemele de realitate virtuală și interfețele utilizator marchează, tranziția de la această fază de dezvoltare la următoarea etapă.

A treia fază de dezvoltare, începută la mijlocul anilor 1990, definită de progrese accelerate în capacitatea de procesare și în tehnologiile grafice, care au impulsionat dezvoltarea în numeroase domenii cheie, inclusiv introducerea conținutului creat de utilizatori, grafica 3D, socializarea deschisă și integrarea de conținut audio. În 1994, Web World a introdus o lume digitală 2.5D, cu o perspectivă izometrică, oferind pentru prima dată utilizatorilor posibilitatea de a contribui activ la construcția mediului virtual. Această inovație a marcat o schimbare de paradigmă semnificativă, trecând de la setările virtuale predefinite, create în totalitate de dezvoltatori, la medii online dinamice, modelate în timp real de către participanți. Prin integrarea unor instrumente de creare a conținutului, personalizate pe baza preferințelor utilizatorilor, Web World a deschis calea către o nouă eră de colaborare creativă și interacțiune participativă în spațiile virtuale. În 1995, Worlds Inc. a devenit prima lume virtuală disponibilă publicului cu grafică tridimensională completă. Această lume a reînviat genul deschis, care nu se bazează pe jocuri (open-ended non-game-based), găsit inițial în MUSH-uri bazate pe text. În acest fel, utilizatorilor li s-a permis să socializeze în spații 3D și, prin urmare, lumile virtuale au evoluat tot mai mult de la un model de joc spre un mediu focalizat pe furnizarea unui cadru sau cultură alternativă, pentru a exprima întreaga gamă și complexitatea comportamentului uman (Dionisio et al., 2013). În acest fel, amploarea și diversitatea activităților din lumile virtuale au ajuns să fie paralele cu cele ale întregului Internet existent, cu posibilitatea reprezentării tridimensionale și cu moduri de interacțiune corespunzătoare. În anul 1995 a fost introdusă și Activeworlds, o lume virtuală bazată în întregime pe viziunea exprimată în romanul Snow Crash al lui Neal Stephenson. Activeworlds se aștepta în mod explicit ca utilizatorii să personalizeze și să construiască împreună un mediu virtual 3D complet. În cele din urmă, un an mai târziu, în anul 1996, OnLive! Traveler a devenit primul mediu virtual 3D disponibil pentru publicul larg, care a inclus opțiunea de chat vocal spațial utilizat nativ și mișcarea buzelor avatarului prin procesarea fonemelor (Dionisio et al., 2013).

A patra fază de dezvoltare a debutat la începutul acestui mileniu. Această perioadă a fost caracterizată de o creștere a bazei de utilizatori a lumilor virtuale comerciale, cum a fost în cazul Second Life. De asemenea, s-a remarcat implicarea crescută a instituțiilor majore din lumea reală - corporații, universități, organizații nonprofit, îmbunătățirea instrumentelor de creare a conținutului din lumea virtuală, îmbunătățirea treptată a fidelității grafice, precum și dezvoltarea unei economii virtuale avansate. Jocul Blue Mars dezvoltat de Avatar Reality, lansat în 2009, a implicat cea mai ambițioasă încercare de a încorpora un nivel mult mai ridicat de realism grafic în lumile virtuale, prin utilizarea CryEngine 2, de ultimă generație la momentul respectiv, dezvoltat inițial de Crytek pentru aplicații de jocuri. Avatar Reality a permis, în plus, să fie create obiecte 3D în afara lumii, atâta timp cât este posibilă salvarea acestora într-unul dintre mai multe formate deschise („open”). Cu

toate acestea însă, efortul de a obține un realism grafic mai ridicat a crescut în mod semnificativ cerințele de sistem pentru mașinile utilizatorilor, într-o măsură care nu a fost rentabilă pentru baza de utilizatori țintă a Blue Mars. Astfel, această depășire a necesitat restructurarea masivă a unei inițiative inițial promițătoare.

Cea de-a cincea fază de dezvoltare a fost marcată de suprapunerea introducerii Second Life și Blue Mars. Această ultimă fază, care a debutat începând cu anul 2007 și este încă în curs de desfășurare, implică contribuții descentralizate de tipul „open-source” la dezvoltarea lumilor virtuale tridimensionale. Solipsis este remarcabil nu numai ca unul dintre primele sisteme open-source din lumea virtuală, ci și pentru arhitectura sa „peer-to-peer”. De atunci, au urmat o serie de alte proiecte open-source, inclusiv Open Cobalt, Open Wonderland și OpenSimulator (Dionisio et al., 2013). Dezvoltarea descentralizată a dus la decuplarea părților reprezentate de către client și server ale unui sistem din lumea virtuală, facilitată de convergența asupra protocolului de rețea folosit de Linden Lab pentru Second Life ca standard de facto. Vizualizatorul open-source Imprudence/Kokua a marcat primul „vizualizator terț parte” pentru Second Life, o categorie de aplicații care a crescut pentru a include proiecte precum Phoenix și mai târziu Kirstens, Firestorm, Nirans, și Singularity. Pe partea de server, OpenSimulator, menționat anterior, a apărut ca o alternativă similară la Second Life și a dat naștere la proiecte complementare, cum ar fi Aurora-Sim și realXtend. Protocolul Second Life în sine a rămas proprietar sub controlul deplin al Linden Lab. Multiplicitatea emergentă de clienți sau spectatori și servere interoperabile vor reprezenta finalul celei de-a cincea faze. Aceasta se caracterizează prin interoperabilitate și interschimbabilitate deplină între servere și clienți din lumea virtuală, în același mod în care World Wide Web este compus din mai multe opțiuni de client, sau browsere și servere, centrate în jurul protocolului standard HTTP(S). Disponibilitatea open-source a condus la apariția de noi posibilități de integrare, cum ar fi găzduirea lumilor virtuale prin folosirea paradigmei de cloud computing și autentificarea folosind acreditările rețelelor sociale.

Definiții și interpretări ale Metaversului

Metaversul utilizează tehnologiile VR (Virtual Reality), AR (Augmented Reality), AI (Artificial Intelligence), XR (Mixed Reality), Web 3.0, IoT (Internet of Things) și social media pentru a simula medii virtuale 3D. Aici, utilizatorii pot interacționa atât cu mediul virtual, cât și cu utilizatorii, pot crea conținut, întreprinde diverse activități profesionale sau recreative. Totodată, există numeroase definiții ale termenului de Metavers, începând din anul 1984, acesta fiind considerat un concept al Cyberspace-ului. Fondatorul Facebook, Mark Zuckerberg, îl consideră „Următoarea generație a Internetului (...), un mediu virtual în care te poți întâlni cu oameni în spații digitale”.

Fiind încă în faza incipientă și în continuă dezvoltare, definiția conceptului de Metavers suferă modificări continue, astfel că definițiile se schimbă cu rapiditate. În lucrarea lor, S.-M. Park et al., 2022, au selectat o serie de definiții, prezente în lucrări de specialitate, ce încadrează lumea Metavers:

- O lume virtuală rezidentă în care geografia și caracteristicile fizice ale lumii reale sunt modelate într-un spațiu digital în care utilizatorul este reprezentat sub forma unui avatar (Schroeder et al., 2001);
- Un mediu captivant care utilizează o rețea media digitală universală și partajată ce înlătură barierele timpului și ale spațiului, înșelând simțurile vizuale ale utilizatorilor (Jaynes et al., 2003);
- Un mediu în care utilizatorii își pot crea personalitatea, pot vizita rapid diferite locuri, explora clădiri și pot face cumpărături (Rymaszewski, 2007);
- Pun bazele unor afaceri, divertisment și rețele interactive cu medii virtuale 3D continue, captivante și accesibile (Collins, 2008);
- Un mediu video-realistic complet bazat pe realitatea virtuală ce permite interacțiunea captivantă între participanți (Prisco, 2009);
- O lume continuă, concepută pentru a oferi utilizatorilor control aproape complet al fiecărui aspect al lumii virtuale, creând obiectul pe care și-l doresc (Papagiannidis et al., 2010);
- O lume virtuală 3D captivantă în care oamenii interacționează între ei și cu mediul, lor folosind metafore din lumea reală fără limitări fizice (Owens et al., 2011);
- Un mediu asincron la care utilizatorii se conectează și o lume conectată cu un avatar care este un proxy pentru ființa umană reprezentată digital (Hughes, 2012);
- O rețea integrată de lumi virtuale 3D într-o lume virtuală independentă sau un tărâm alternativ pentru interacțiunea socio-culturală umană (Dionisio et al., 2013);
- O comunitate virtuală online care permite utilizarea simulărilor și a obiectelor pentru a interacționa cu alți utilizatori prin intermediul avatarurilor (Ko et al., 2014);
- O lume a informațiilor în care orice îți poți imagina astăzi este conectat la Internet și simulează intens simțurile (Yoon et al., 2015);
- O lume care poate exista sub diferite forme temporale, politice și culturale prin interacțiunile om-mașină și permite agenților jocului

să rezolve probleme prezente, să redefinească trecutul și să inventeze viitorul (Zackery et al., 2016);

- Un spațiu creat prin fuziunea realității virtuale și a realității augmentate ca o lume compusă de concepte meta abstracte și univers (Choi et al., 2017);
- O simulare interactivă mediată de om și calculator a unui mediu artificial ca un spațiu permanent, sintetic, 3D, care nu este centrat pe jocuri și separă jocurile de spațiul social (Nevelsteen, 2018);
- Un spațiu în care lumile virtuale integrează realitatea virtuală imersivă cu actori umani, obiecte fizice, interfețe și rețele, conturând o nouă formă a Internetului. O lume digitală paralelă, cu o dimensiune socială puternică, care ajunge să reflecte și, în unele privințe, să înlocuiască – realitatea. (Huggett, 2020);
- O rețea persistentă interoperabilă de medii virtuale partajate în care oamenii pot interacționa sincron prin avatarurile lor cu alți agenți și obiecte (Kim, 2021);
- Un mediu virtual ce îmbină mediul fizic și mediul digital prin convergența dintre Internet și tehnologiile web (Lee et al., 2021);
- O lume virtuală, captivantă și partajată în care sunt permise diferite activități pentru utilizatorii săi, reprezentați ca avataruri (Vidal-Tomás, 2022);
- O lume virtuală 3D, captivantă în care utilizatorii, indiferent de locația lor, se pot angaja în interacțiuni sociale și economice, ce sunt computaționale (Akour et al., 2022);
- Conceptul unei lumi virtuale complet imersive în care oamenii se adună pentru a socializa, a se juca și a lucra (Laeq, 2022);
- Metaversul reprezintă o nouă evoluție a Internetului, Internetul în 3D, o rețea interconectată, persistentă, de lumi virtuale, unde oamenii se pot transpune în lumi virtuale prin dispozitive XR. Metaversul reprezintă o rețea scalată și interoperabilă, cu crearea 3D-ului instant a lumii virtuale ce poate fi experimentată sincron de către un număr nelimitat de utilizatori, fiecare putând fi identificat în mod unic prin identitate, istorie, plăți, evenimente (Ball, 2022);
- O multitudine de lumi interconectate (Morgado, 2009);
- Un set de spații virtuale în care poți crea și explora împreună cu alți oameni care nu se află în același spațiu virtual ca și tine (Bosworth et al., 2021);

Nu în ultimul rând, Metavers-as-a-Service (MaaS) care este o platformă specială, similar cu Software-as-a-Service (SaaS), și care permite întreprinderilor să-și stabilească și să-și îmbunătățească prezența într-un mediu virtual 3D care îmbină fizicul și digitalul, facilitat de convergența dintre tehnologiile Internet și Web și Realitatea Extinsă (XR) (Bian et al., 2022). În acest context, Metavers-as-a-Service poate fi descris ca o soluție de interoperabilitate care va permite companiilor să pătrundă ulterior în Metavers cu propriile lumi virtuale pentru o varietate de cazuri de utilizare, de la asistență medicală și finanțe la divertisment, învățare și multe altele.

Analizând aceste definiții, putem constata că Metavers definește o realitate paralelă, persistentă, colectivă și interactivă creată prin sintetizarea unor lumi virtuale. Astfel, Metaversul reprezintă o transpunere digitală a spațiului și timpului real, iar prin folosirea dispozitivelor periferice de augmentare a simțurilor, utilizatorii se pot regăsi ca indivizi prin istorie, spațiul în care își desfășoară activitatea, plățile efectuate, remunerații, deținere de obiecte digitale. Nucleul unui Metavers este format dintr-o rețea de lumi virtuale interconectate în spațiul cibernetic unde utilizatorii sunt reprezentați prin avataruri iar majoritatea activităților care se pot desfășura în lumea reală se pot desfășura și aici. Este o fuziune dintre o lume virtuală și cea reală unde se pot experimenta ambele. Metaversul este în continuă dezvoltare, fiind de presupus că, în timp, multe activități desfășurate pe Internetul 2D precum socializare, recreație, educație, activități profesionale și altele, vor migra către un spațiu 3D.

Metaversul este și o viziune a ceea ce mulți specialiști consideră a fi următoarea iterație a Internetului: un spațiu virtual 3D unic, partajat, captivant, persistent, în care oamenii experimentează viața în moduri în care nu ar putea-o în lumea fizică.

Metaversul este mai mult decât o tehnologie sau o aplicație software, este un concept de spațiu virtual ce folosește mai multe tehnologii care facilitează interacțiunile între utilizatori și activitățile ce pot fi desfășurate. Tehnologia Web 3.0 permite interoperabilitatea între lumile Metavers și implicit, tranzacții Blockchain și NFT. Interoperabilitatea în Metavers are rolul de a permite ca bunurile deținute și create de utilizatori să poată fi folosite dintr-un Metavers în altul datorită conceptului de descentralizare. Web 3.0 permite ca bunurile digitale să fie create de către comunitate, companii sau dezvoltatori, iar în Web

2.0 doar companiile sau dezvoltatorii pot crea bunuri digitale. Fără tehnologia Blockchain, ar fi extrem de dificil de a evalua valoarea economică a resurselor și a bunurilor virtuale din Metavers (Güven et al., 2024).

Servicii publice, educație și gaming în Metavers: direcții de dezvoltare

Integrarea serviciilor publice specifice administrației publice, educației și industriei de gaming în Metavers, alături de facilitarea interacțiunilor prin intermediul avatarurilor, poate contribui semnificativ la optimizarea modului în care cetățenii

interacționează cu instituțiile guvernamentale. Odată cu evoluția tehnologiei Blockchain, care contribuie la întărirea securității serviciilor guvernamentale prin intermediul mai multor mecanisme-cheie precum transparență și trasabilitate, autentificare descentralizată și audit automatizat, accesul la serviciile virtuale din aceste trei sectoare de activitate devine considerabil mai facil.

Administrație publică



Metaversul deschide noi perspective pentru extinderea serviciilor administrației publice, atât la nivel central, cât și local.

Integrarea tehnologiilor Metavers în sfera administrației publice promise nu doar să eficientizeze interacțiunile dintre cetățeni și instituții, ci să sporească transparența proceselor administrative. În acest context digital extins, gestionarea responsabilă a datelor devine determinantă, având în vedere cantitatea mare de informații sensibile aflate în custodia autorităților administrative (Hutagalung et al., 2024).

Pentru cetățenii din zonele greu accesibile, Metaversul propune o alternativă modernă la interacțiunea clasică cu administrația publică. Prin intermediul unei platforme guvernamentale virtuale, aceștia pot obține documente necesare direct de pe un dispozitiv conectat la Internet, beneficiind de suport profesional pe întreaga durată a procesului. În plus, pot participa virtual la ședințe ale consiliilor locale, pot vota în alegeri și pot contribui la consultări publice, fără a fi nevoiți să se deplaseze.

Birourile digitale oferă acces facil la servicii precum emiterea sau reînnoirea actelor oficiale și permit transmiterea rapidă a cererilor sau a solicitărilor de

informații, iar totul trebuie să se petreacă într-un mediu sigur și eficient. Protejarea datelor personale necesită tehnologii de criptare avansată și sisteme robuste de autentificare, pentru a preveni riscurile de securitate și a asigura încrederea în procesele administrative digitale.

Cetățenii pot vizualiza în Metavers simulări 3D ale orașelor și regiunilor pentru planificare urbanistică, în cadrul proiectelor de dezvoltare, și pot contribui cu opinii. Și în acest caz, guvernanța datelor este importantă deoarece datele obținute din proiectele de dezvoltare trebuie protejate, iar managementul acestora va trebui să fie realizat conform reglementărilor de confidențialitate și transparență.

Un sondaj internațional desfășurat în anul 2022 în 29 de țări (Yfantis et al., 2022) a arătat că, jumătate dintre adulți (52%) erau deja familiarizați cu ideea de Metavers. Interesant este că locuitorii țărilor în curs de dezvoltare s-au arătat mai entuziasmați de potențialul acestuia, exprimând speranțe pozitive legate de modul în care tehnologiile Metaversului ar putea influența viața cotidiană în următorul deceniu.

În același context, tehnologiile conexe Metaversului nu erau deloc străine publicului: 80% dintre participanți cunoșteau conceptul de Realitate Virtuală, iar 61% erau familiarizați cu Realitatea Augmentată. Aceste date sugerează o deschidere tot mai mare către noile forme de interacțiune digitală, în special în rândul celor care văd în tehnologie o oportunitate de transformare personală și socială.

Familiaritatea cetățenilor cu mediul virtual și tehnologiile specifice Metavers a inspirat multe orașe din întreaga lume să adopte acest concept cu scopul extinderii și îmbunătățirii serviciilor publice. Astfel că, în Coreea de Sud, în orașul Seul s-a stabilit fundamentul pentru un mediu Metavers care poartă numele „Metaverse Seoul”, o replică virtuală a orașului Seul, și care are în vedere fiecare sector din administrația locală, având ca scop îmbunătățirea serviciilor municipale, a activităților de management și turismului virtual. Strategia de implementare implică tehnologii precum gemeni digitali, Realitate Virtuală și Realitate Augmentată.

Datele generate și gestionate în Metavers reprezintă o prioritate. În acest context, guvernul din Coreea de Sud a elaborat ghiduri privind bunele practici în etica utilizării Metavers, fără a fi desemnată o autoritate competentă pentru stabilirea reglementărilor specifice acestui mediu virtual.

În Statele Unite, un grup reprezentativ al orașelor și comunităților, cunoscut sub numele de National League of Cities (NLC), explorează noi modalități de a transforma modul în care cetățenii interacționează cu serviciile publice. Una dintre inițiativele inovatoare vizează utilizarea Metaversului ca platformă pentru dezvoltarea acestor servicii, dar și pentru organizarea adunărilor publice într-un spațiu digital accesibil. Scopul este de a extinde accesul la aceste resurse esențiale, în special pentru persoanele cu dizabilități sau pentru cei care, din diverse motive, nu pot participa fizic. Mai mult, la nivel național, autoritățile americane iau în

considerare posibilitatea de a adopta pe scară largă Metaversul ca mijloc de furnizare a anumitor tipuri de servicii publice, deschizând astfel calea către o administrație mai incluzivă și mai eficientă.

Cerințele fundamentale pentru utilizarea aplicațiilor Metavers în sectorul public se referă la incluziune, transparență și responsabilitate, ceea ce presupune că toți cetățenii trebuie să aibă dreptul de a beneficia de aceste servicii, indiferent de nivelul de cunoștințe informatice, problemele de sănătate sau dificultățile financiare.

Tot mai multe administrații publice din întreaga lume își îndreaptă serviciile către platforme digitale care integrează tehnologii emergente precum Realitatea Virtuală, Realitatea Augmentată, Inteligența Artificială, Internetul lucrurilor (IoT), Blockchain sau rețelele 5G. Această tranziție nu mai este o posibilitate ipotetică, ci o realitate concretă în cazul țărilor care dispun de infrastructura tehnologică necesară și sunt hotărâte să îmbunătățească modul în care cetățenii interacționează cu instituțiile publice.

Majoritatea aplicațiilor din mediul virtual destinate sectorului public vizează domenii precum turismul, sănătatea, serviciile sociale, administrația locală, ambasadere virtuale, consulatere și planificarea urbană (Lnenicka et al., 2024). Gradul de acceptare din partea populației este hotărător în succesul acestor inițiative, alături de strategiile adoptate de guverne pentru transformarea sectorului public și de resursele TIC disponibile la nivel național. În acest context, predicțiile experților indică o direcție clară: conform unui raport Gartner (Lnenicka et al., 2024), până în anul 2026, aproximativ 25% dintre utilizatori, din diverse țări, vor petrece cel puțin o oră pe zi în Metavers — un spațiu digital care promite să redefinească experiența cotidiană, inclusiv în relația cu serviciile publice.

Guvernul insulei Barbados a făcut un pas revoluționar în domeniul diplomației internaționale, devenind prima țară din lume care a decis să înființeze o ambasadă în Metavers. Aceasta a fost lansată pe platforma Decentraland sub denumirea de Barbados Metaverse Embassy și simbolizează o inițiativă ambițioasă de transpunere a diplomației într-un spațiu virtual. Prin acest demers, Barbados își propune nu doar să își extindă prezența digitală, ci și să construiască relații bilaterale inovatoare cu alte guverne, la nivel global, într-un mediu complet nou.

Republica Indonezia, de asemenea și-a exprimat intenția fermă de a pătrunde în Metavers (Yfantis et al., 2022). Ca parte a acestui demers, țara a încheiat un parteneriat strategic cu WIR Group, o companie specializată în tehnologii de Realitate Augmentată, marcând astfel primii pași concreți în direcția integrării lumii virtuale în viziunea sa guvernamentală și diplomatică.

În efortul de a dezvolta modalități inovatoare pentru o comunicare mai eficientă între administrația publică și cetățeni, aplicațiile digitale destinate acestui sector trebuie să țină cont nu doar de oportunitățile oferite de tehnologii emergente, ci și de

provocările pe care acestea le presupun. În special în contextul utilizării Metaversului, aspecte precum securitatea datelor, confidențialitatea, sănătatea mintală a utilizatorilor și implicațiile etice trebuie abordate cu responsabilitate și claritate.

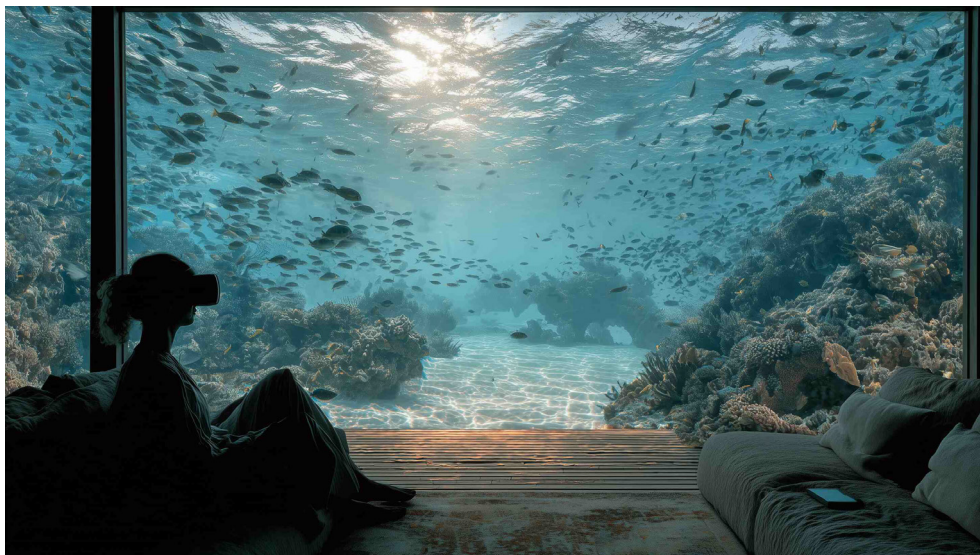
Tehnologiile gemenilor digitali se conturează ca un viitor instrument determinant în planificarea urbană și dezvoltarea orașelor inteligente. Un exemplu elocvent vine din Coreea de Sud, unde, în cadrul proiectului de urbanism al orașului Jeonju, au fost create modele digitale detaliate ale infrastructurii și clădirilor existente. Acestea au fost îmbunătățite cu ajutorul gemenilor digitali, permițând autorităților să simuleze și să monitorizeze în timp real funcționarea orașului, contribuind astfel la luarea unor decizii mai informate și mai eficiente în gestionarea spațiului urban.

Accesul la spațiile urbane și participarea la evenimente sociale capătă o nouă dimensiune odată cu integrarea Metaversului și gemenilor digitali. În orașe precum Seul (J. Park et al., 2023), această transformare devine realitate. Locuitorii au posibilitatea de a folosi dispozitive de realitate virtuală (VR) și realitate augmentată (AR) pentru a interacționa cu orașul într-un mod inovator, chiar și din confortul propriului cămin. Prin intermediul Metaversului, cetățenii pot accesa servicii publice, pot depune sesizări administrative sau pot vizita virtual parcuri, muzee și alte spații culturale, extinzând astfel granițele experienței urbane dincolo de lumea fizică.

Metaversul aduce un plus de valoare sectorului turistic, în special prin capacitatea sa de a reduce costurile (Lnenicka et al., 2024) și de a extinde accesul la experiențe diverse. Conștient de acest potențial, Ministerul Economiei din Emiratele Arabe Unite a inaugurat un sediu virtual în Metavers. Prin această inițiativă, ministerul își propune să consolideze colaborarea cu parteneri din întreaga lume — de la guverne și corporații, până la cetățeni (Kshetri et al., 2024) — oferindu-le posibilitatea de a interacționa în medii de realitate virtuală. Astfel, turismul și dialogul economic se redefinesc într-un spațiu digital care transcende granițele fizice și deschide noi oportunități de cooperare globală.

Într-o lume în care tehnologia redefinesc constant modul în care explorăm, Thailanda își deschide porțile către vizitatori printr-o experiență complet nouă: turismul virtual. Autoritatea de Turism din Thailanda a lansat o aplicație care le permite utilizatorilor să descopere frumusețea acestei țări prin intermediul realității virtuale. Cu ajutorul căștilor VR, turiștii pot explora destinații emblematiche precum Bangkok sau Phuket, bucurându-se de imagini spectaculoase și atmosferă autentică, fără a părăsi propria locuință. Această inițiativă nu doar că sporește atractivitatea Thailandei pe scena turismului global, ci contribuie și la reducerea impactului ecologic asociat cu deplasările fizice. În același timp, ea consolidează angajamentul Thailandei față de sustenabilitate și inovație în industria turismului¹.

¹ Tamer T. (2024), *Real Examples and Use Cases of Metaverse in Tourism*, Disponibil la: <https://capsulesight.com/metaverse/real-examples-and-use-cases-of-metaverse-in-tourism/> [Accesat: 18 Aug. 2025].



Metaversul poate simplifica planificarea călătoriilor, permițând turiștilor să exploreze virtual hoteluri, restaurante și atracții turistice, ajutându-i să ia decizii informate cu privire la itinerariile lor. Companii precum Amadeus (Amadeus Navigation Solutions) utilizează realitatea virtuală pentru a oferi previzualizări imersive ale cazărilor și zborurilor cu scopul de a crește încrederea clienților de a reduce ezitățile la rezervare².

Realitatea Augmentată transformă modul în care turiștii experimentează locurile pe care le vizitează, adăugând un strat interactiv peste lumea reală. Prin integrarea de informații în timp real, această tehnologie oferă acces facil la detalii istorice fascinante, asistență pentru orientare și chiar servicii de traducere, îmbunătățind considerabil calitatea experienței turistice.

Un exemplu în acest sens este compania ARtGlass, care implementează soluții AR în cadrul siturilor de patrimoniu cultural. Prin reconstituiri istorice, reconstrucții arhitecturale virtuale și narațiuni disponibile în mai multe limbi, ARtGlass adaugă profunzime vizitelor, sporind atât valoarea educațională, cât și cea culturală. Astfel, tehnologia nu doar că facilitează accesul la informație, dar reușește să creeze o conexiune mai profundă între vizitatori și istoria locurilor explorate³.

Metaversul personalizează experiențele de călătorie pentru persoanele cu dizabilități, oferind previzualizări virtuale ale destinațiilor și opțiunilor de transport pentru a asigura accesibilitatea. Aplicațiile de tip „Tururi virtuale fără bariere”

² Ibid.

³ Ibid.

permit persoanelor cu mobilitate redusă sau deficiențe de vedere și auz să exploreze destinații globale, oferind conținut VR personalizat și accesibil⁴.

Realitatea virtuală din Metavers nu este doar un instrument de divertisment sau explorare turistică, ci devine tot mai mult o platformă eficientă de instruire pentru profesioniștii din domeniul ospitalității. Prin simulări realiste ale unor scenarii diverse, angajații pot fi pregătiți într-un mod interactiv și sigur pentru provocările pe care le-ar putea întâlni în relația cu turiștii.

Un exemplu concludent vine din partea lanțului hotelier Marriott, care a integrat tehnologia VR în programele sale de formare. Prin intermediul acestor simulări, angajații sunt puși în situații autentice de servire a clienților, învățând să gestioneze eficient cerințele acestora, să rezolve probleme pe loc și să își perfecționeze abilitățile de comunicare. Astfel, realitatea virtuală contribuie direct la creșterea calității serviciilor și la formarea unei echipe mai bine pregătite pentru interacțiunile din lumea reală⁵.

Într-un pas considerat revoluționar pentru sistemul de justiție, Columbia a devenit una dintre primele țări care a desfășurat un proces judiciar în Metavers⁶. Participanții la acest caz au fost prezenți în mod virtual, utilizând căști de realitate virtuală și avatare personalizate în cadrul platformei Horizon Workrooms, dezvoltată de Meta. Întregul eveniment a fost transmis live pe YouTube, marcând un moment de referință în digitalizarea procedurilor judiciare.

Magistrata care a condus ședința a solicitat verificarea identității tuturor celor implicați și, într-un gest care subliniază integrarea inteligenței artificiale în sistemele moderne, a consultat ChatGPT în legătură cu posibilitatea organizării procesului într-un spațiu virtual. Participanții au utilizat ochelari Oculus Quest 2, configurându-și avatarele pentru a participa la audieri într-un mediu digital. Acest caz nu doar că evidențiază o deschidere semnificativă către noile tehnologii, dar reflectă și o tendință globală tot mai pronunțată - aceea ca instanțele de judecată să adopte soluții emergente pentru a răspunde provocărilor unei lumi aflate într-o transformare rapidă.

Această transformare digitală poate fi extinsă cu succes și în domeniul sănătății, creând premisele unei transformări fundamentale în modalitatea de furnizare a serviciilor medicale. Într-un ecosistem virtual, pacienții pot interacționa cu medicii prin intermediul avatarurilor, beneficiind de consultații la distanță într-un spațiu tridimensional sigur și intuitiv. Accesul ghidat la dosarul medical electronic devine mai facil, iar tratamentele sau investigațiile pot fi explicate și simulate într-un mod interactiv, care ajută la înțelegerea și acceptarea lor. În același timp, cadrele medicale

⁴ Ibid.

⁵ Ibid.

⁶ IHussainA. (2023), *Court case held in the metaverse*, Disponibil la: <https://www.legalcheek.com/2023/02/court-case-held-in-the-metaverse/> [Accesat: 19 Aug. 2025].

pot participa la sesiuni de instruire avansate, desfășurate în medii virtuale realiste, unde pot exersa proceduri și pot răspunde la situații complexe, fără riscuri pentru pacienți.

Sistemul medical, care cuprinde rețeaua de spitale, clinici, cabinete medicale, medici de familie, și structuri critice precum Casa Națională a Asigurărilor de Sănătate (CNAS), serviciile de ambulanță și unitățile de urgență, poate fi extins în Metavers prin crearea de spații virtuale și integrarea planurilor de tratament într-un cadru digital tridimensional. Acest spațiu imersiv oferă oportunități unice pentru simulări medicale avansate care nu doar sprijină procesul de învățare, ci contribuie activ la îmbunătățirea calității actului medical și a comunicării dintre toți cei implicați (M.-C. Zamfir et al., 2024).

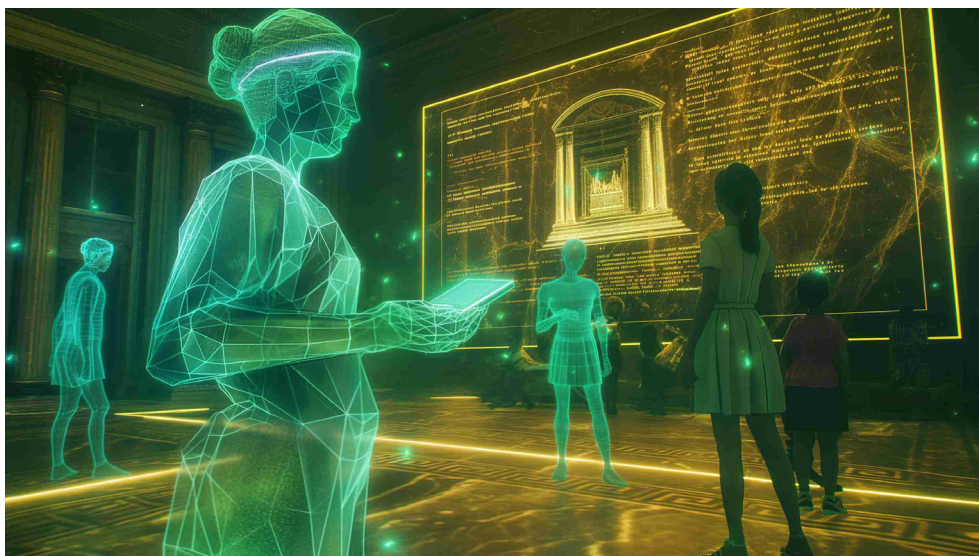
În acest context al digitalizării accelerate și al migrării serviciilor publice în spațiul virtual, gestionarea corectă a datelor capătă o importanță strategică, mai ales în condițiile în care autoritățile administrează volume tot mai mari de informații sensibile și personale.

Educație

Într-o lume din ce în ce mai conectată digital, Metaversul începe să își lase amprenta și asupra educației, deschizând uși către posibilități care până nu demult păreau de domeniul science fiction-ului. Imaginați-vă o sală de clasă fără pereți, unde granițele geografice dispar, iar elevii și studenții din colțuri opuse ale lumii pot învăța împreună, ca și cum ar fi în același loc. Aici, lecțiile nu se mai limitează la manuale sau prezentări statice – totul prinde viață prin simulări realiste, jocuri interactive și resurse educaționale variate, menite să transforme învățarea într-o experiență captivantă și profund imersivă.

Instituțiile de învățământ, de la școlile generale și licee până la universități, își pot extinde activitatea dincolo de granițele fizice, pătrunzând în mediul digital prin intermediul claselor virtuale. În acest spațiu interactiv, elevii și studenții pot accesa metode de predare moderne, participând la lecții imersive care transformă procesul de învățare într-o experiență adaptată noii generații de utilizatori digitali. Se remarcă o creștere constantă în adoptarea acestor soluții la nivelul universităților, transformând Metaversul într-un spațiu virtual inovator, unde educația devine interactivă și colaborativă (Sim et al., 2024). Prin integrarea acestor medii digitale dinamice, se oferă un sprijin real cadrelor didactice în procesul de predare și o experiență de învățare adaptată nevoilor și curiozității noilor generații. Un exemplu relevant este realizarea unui geamăn digital al unei universități, o replică virtuală tridimensională a campusului fizic, care permite digitizarea aplicațiilor academice sub forme vizuale atractive. Acest campus digital reflectă structura și funcționalitatea instituției, devenind un spațiu în care lecțiile, laboratoarele și interacțiunile studențești

capătă o dimensiune nouă și accesibilă. Tehnologiile Metavers și gemenii digitali pot recrea reprezentări complexe, de cele mai multe ori costisitoare în viața reală, iar transmiterea cunoștințelor poate fi îmbunătățită cu ajutorul simulărilor de instruire. Rezultatele unei astfel de implementări au evidențiat faptul că utilizatorii au apreciat posibilitatea de a înțelege și experimenta diferite concepte de studiu într-un interval de timp mai redus, în comparație cu metodele tradiționale de învățare. De asemenea, a fost evidențiat faptul că instruirea pe echipamente dificil de manevrat în spațiul fizic oferă, în mediul virtual, un nivel ridicat de siguranță pentru studenți, cu respectarea strictă a protocoalelor de utilizare. În plus, instruirea în cadrul unei săli de curs din Metavers nu este limitată temporal, permițând studenților să exerseze și să repete procedurile ori de câte ori este necesar. Pentru o desfășurare optimă a activităților în cadrul claselor virtuale, trebuie asigurată siguranța tuturor utilizatorilor și protecția documentelor utilizate de aceștia. Prin urmare, utilizatorii platformelor Metavers trebuie să fie pregătiți să înțeleagă riscurile și beneficiile asociate mediului virtual, pentru a putea lua decizii corecte privind protecția datelor lor personale⁷.



Platformele Metavers, precum VRChat, Minecraft Education Edition, Roblox Education și Second Life Education, furnizează soluții pentru învățarea virtuală, oferind acces la clase virtuale, laboratoare, muzee și medii alternative imersive destinate educației (Nguyen et al., 2024). Utilizarea căștilor de realitate virtuală nu este obligatorie în aceste aplicații, iar utilizatorii au posibilitatea de a crea și încărca

⁷ *Minecraft (2020), New Study: Understanding the Impact of Minecraft in the Math Classroom*, Disponibil la: <https://education.minecraft.net/en-us/blog/new-study-understanding-the-impact-of-minecraft-in-the-math-classroom> [Accesat: 19 Aug. 2025].

propriile avatururi personalizate. Aceste platforme facilitează accesul la resurse educaționale de înaltă calitate, incluzând cursuri online, materiale interactive, simulări și biblioteci virtuale. În plus, integrarea experiențelor sub formă de jocuri și a interacțiunilor (M. Zamfir et al., 2023) cu alți utilizatori, contribuie semnificativ la creșterea nivelului de implicare și motivație în procesul de învățare.

În mediul educațional al Metaversului, protejarea datelor reprezintă o necesitate reală. Pe măsură ce rețelele de învățare virtuală se extind, cresc și tipurile de informații gestionate – de la conturi de utilizatori și plăți online, până la accesul la cursuri și resurse. Toate aceste procese generează date sensibile, care trebuie protejate cu responsabilitate, respectând normele legale și principiile etice. Instituțiile implicate în acest ecosistem formează un cadru extins și interconectat, unde proprietatea și controlul datelor trebuie gestionate cu maximă responsabilitate. Fiecare informație stocată sau transferată trebuie protejată nu doar prin tehnologie, ci și prin politici clare și riguroase, pentru a asigura securitatea și integritatea întregului proces educațional în Metavers. Astfel, viitorul digital al educației poate fi construit pe o fundație solidă, în care inovația merge mână în mână cu responsabilitatea⁸.

În mediul educațional digital din Metavers, unde elevii își desfășoară activitatea prin avatururi și interacționează constant cu conținutul virtual, urmărirea progresului devine parte din procesul de învățare. Dar, oricât de utilă ar fi pentru profesori, această monitorizare trebuie făcută corect, cu reguli clare și protecție solidă a datelor. Informațiile despre performanțele elevilor – rezultate, evoluție, comportament în spațiul virtual trebuie protejate împotriva accesului neautorizat și gestionate cu grijă. În acest context, apare o întrebare fundamentală: cine deține cu adevărat datele generate de aceste interacțiuni virtuale? Este utilizatorul – elevul sau profesorul – cel care are controlul asupra propriilor date, sau furnizorul platformei care găzduiește întregul univers educațional? Stabilirea clară a acestor responsabilități și drepturi devine nu doar o chestiune juridică, ci și una etică. Numai prin definirea acestor limite și asigurarea unei guvernări corecte a datelor se poate construi un mediu educațional virtual sigur, echitabil și de încredere.

Aceeași nevoie de claritate și securitate se extinde și asupra modului în care sunt realizate plățile în acest nou ecosistem digital. Dacă în sistemele tradiționale de educație, înscrierea la programele de studiu și achitarea taxelor se realizează prin intermediul unor furnizori de soluții software integrate cu agregatori de plăți, în Metavers apar opțiuni complet noi, cu un potențial transformator. Criptomonede, NFT-urile și portofelele digitale devin instrumente alternative pentru efectuarea tranzacțiilor, aducând cu ele nu doar flexibilitate, ci și noi provocări legate de reglementare, transparență și securitatea datelor financiare. Având în vedere estimarea că numărul portofelelor digitale unice

⁸ Kulkarni A. (2019), 28. *Payments in — Education Sector*, Disponibil la: <https://medium.com/authncapture/28-industry-education-3ace3b973342> [Accesat: 19 Aug. 2025].

a atins 4,3 miliarde în anul 2024, utilizarea acestora și în lumea virtuală implică preocupări legate de determinarea proprietății datelor în Metavers⁹.

În acest demers, tehnologia Blockchain se conturează ca un aliat strategic, capabil să rezolve o serie de ineficiențe care încă afectează sistemele educaționale tradiționale. Prin integrarea Blockchain-ului, diplomele, certificările și rezultatele academice pot fi stocate și verificate într-un mod complet securizat, transparent și imuabil. Fără a mai fi nevoie de intermediari pentru validarea autenticității, se reduce drastic riscul de falsificare, iar procesele administrative devin mult mai eficiente și rapide. Această transparență sporită oferă siguranță instituțiilor și angajatorilor și încredere absolvenților privind recunoașterea și protejarea oriunde în lume a realizărilor lor. Blockchain deschide drumul către platforme de învățare descentralizată, în care profesorii și elevii pot interacționa direct, într-un cadru digital autonom. Eliminarea intermediarilor din procesul educațional stimulează implicarea activă a participanților, care pot fi recompensați cu tokeni pentru contribuțiile lor – fie că este vorba despre predare, participare activă sau rezultate academice¹⁰. Tehnologia Blockchain va contribui și la crearea de identități digitale unice pentru studenți, îmbunătățind gestionarea acestora și simplificând procesele de admitere și transfer între instituții. De asemenea, Blockchain asigură transparență și eficiență în gestionarea burselor, facilitând distribuirea directă a fondurilor către studenții eligibili, fără intermediari, iar contractele inteligente vor automatiza procesele administrative, reducând birocrăția și întârzierile. Un alt avantaj important al utilizării Blockchain este protejarea proprietății intelectuale în educație, garantând drepturile autorilor, autentificarea materialelor și prevenirea pirateriei. De exemplu profesorii își vor putea securiza lucrările de cercetare sau alte resurse educaționale.

În ceea ce privește proprietatea intelectuală în Metavers, vor trebui reevaluate cadrele legale și reglementările existente, pentru a preveni la situațiile de încălcare a acestor drepturi. De exemplu, un caz de utilizare a conținutului terților privind drepturile de autor în Metavers, fără permisiunea sau licențele corespunzătoare¹¹, complicând aplicarea drepturilor de proprietate intelectuală este cazul Hermès versus Mason Rothschild, în care crearea și vânzarea NFT-urilor MetaBirkin de către Rothschild au fost contestate de Hermès pentru încălcarea drepturilor sale de marcă. Preocupările legale incluse au fost cybersquatting (înregistrarea unui nume de

⁹ Michael Greenwood (2024), *Digital Wallets Market Report: Growth, Trends 2024-2029*, Disponibil la: <https://www.juniperresearch.com/research/fintech-payments/core-payments/digital-wallet-research-report/> [Accesat: 19 Aug. 2025].

¹⁰ Jhan A. S. (2024), *Unexplored Use Cases of Blockchain in Education*, Disponibil la: <https://medium.com/@arshanshajhan214/unexplored-use-cases-of-blockchain-in-education-c5c002cd6e60> [Accesat: 19 Aug. 2025].

¹¹ Nitu A. (2024), *Metaversul : Provocări și Oportunități pentru Protecția și Aplicarea Drepturilor de Proprietate Intelectuală*, Disponibil la: <https://infocons.ro/metaversul-provocari-si-oportunitati-pentru-protectia-si-aplicarea-drepturilor-de-proprietate-intelectuala/> [Accesat: 19 Aug. 2025].

domeniu identic sau similar cu numele companiei cu intenția de a profita de bunăvoința proprietarului mărcii), diluarea mărcii (reducerea caracterului distinctiv și impactului unei mărci comerciale) și încălcarea drepturilor de marcă. Instanța a dat câștig de cauză companiei Hermès, stabilind că Rothschild se face vinovat și dispunând plata unei despăgubiri în valoare de aproape 133.000 de dolari. Această hotărâre a stabilit un precedent pentru protejarea mărcilor în Metavers și a ridicat întrebări despre protecția NFT-urilor în cadrul legislației privind proprietatea intelectuală.

Gaming

Metaversul își face simțită influența în mod spectaculos în industria jocurilor. Având la bază tehnologii avansate precum realitatea virtuală (VR) și realitatea augmentată (AR), poate transforma complet modul în care jucătorii experimentează divertismentul. În acest spațiu virtual imersiv, jucătorii își pot crea propriile avataruri, se pot conecta între ei, pot participa la evenimente live și pot interacționa într-un univers digital care continuă să existe și să evolueze, chiar și atunci când utilizatorii se deconectează. Astfel, Metaversul oferă o experiență de joc unică și rescrie regulile socializării online, aducând comunitățile virtuale mai aproape ca niciodată. Totuși, pe măsură ce aceste lumi digitale devin tot mai complexe, apare și nevoia unei guvernări clare a datelor, pentru a oferi protecție adecvată informațiilor personale ale jucătorilor, o gestionare eficientă a economiilor virtuale și prevenirea fraudelor¹².



¹² Barnes A. (2023), *Metaverse in Gaming: Revolution in Gaming industry With Next-Generation Experience*, Disponibil la: <https://www.datasciencecentral.com/metaverse-in-gaming-revolution-in-gaming-industry-with-next-generation-experience/> [Accesat: 19 Aug. 2025].

Gamingul în Metavers: aplicații și tehnologii emergente

Metaversul aduce o transformare profundă în industria jocurilor, printr-o serie de aplicații și tehnologii care schimbă fundamental modul în care jucătorii interacționează, colaborează și se raportează la experiențele digitale. La baza acestei revoluții stă promovarea jocurilor sociale și multiplayer, care permit crearea de comunități virtuale active și colaborarea în timp real, accentuând componenta socială a gamingului¹³.

Un alt element definitoriu este modelul play-to-earn (P2E) care, prin integrarea tehnologiei Blockchain și a NFT-urilor, oferă jucătorilor posibilitatea de a câștiga și tranzacționa active digitale cu valoare reală – fie că este vorba despre skin-uri, monede sau terenuri virtuale. În acest cadru, portabilitatea resurselor permite jucătorilor să dețină și să transfere bunuri între diverse platforme din Metavers, păstrând valoarea acestor obiecte dincolo de granițele unui singur joc. Experiențele devin tot mai imersive și personalizate, datorită combinației dintre realitatea virtuală (VR), augmentată (AR) și mixtă (MR), care deschid un spectru larg de posibilități – de la jocuri VR complete până la interacțiuni augmentate integrate în lumea fizică. În spatele acestor schimbări se află o infrastructură tehnologică complexă: Blockchain-ul și criptomonede susțin economii virtuale descentralizate, în timp ce Internetul lucrurilor leagă universul virtual de cel real, permițând, de exemplu, adaptarea obiectelor din joc la condițiile meteo din lumea fizică. De asemenea, reconstrucția 3D contribuie la crearea de spații digitale fidele realității, aducând un plus de autenticitate și detaliu în mediile de joc¹⁴. Această evoluție tehnologică deschide noi oportunități de monetizare și personalizare, oferindu-le dezvoltatorilor un cadru flexibil pentru a crea jocuri de nouă generație. Jucătorii, la rândul lor, beneficiază de un nivel ridicat de libertate creativă și control asupra propriului parcurs în Metavers.

În spatele ascensiunii spectaculoase a Metaversului în domeniul gamingului se află o serie de companii-cheie care contribuie semnificativ la conturarea și extinderea acestui univers digital. Fiecare dintre ele aduce inovații distincte, tehnologii avansate și viziuni diferite asupra modului în care jucătorii pot experimenta lumi virtuale tot mai complexe și captivante¹⁵. Decentraland se numără printre pionierii Metaversului construit pe tehnologia Blockchain. Cu propriul său token, LAND, platforma oferă o economie virtuală funcțională, în care utilizatorii pot cumpăra terenuri digitale, construi spații interactive și participa la jocuri multiplayer. Parteneriatele strategice, cum ar fi colaborarea cu Decentral Games, adaugă un plus de dinamism și atractivitate acestui ecosistem descentralizat.

¹³ Ibid.

¹⁴ Barnes A. (2023), *Metaverse in Gaming: Revolution in Gaming industry With Next-Generation Experience*, Disponibil la: <https://www.datasciencecentral.com/metaverse-in-gaming-revolution-in-gaming-industry-with-next-generation-experience/> [Accesat: 19 Aug. 2025].

¹⁵ Ibid.

The Sandbox duce conceptul de creativitate colaborativă la un alt nivel, permițând utilizatorilor nu doar să exploreze lumi virtuale, ci și să le creeze și să le monetizeze prin NFT-uri. Platforma a atras atenția globală prin colaborări spectaculoase cu branduri și personalități din cultura pop, precum Snoop Dogg sau Standard Chartered, transformând spațiile virtuale în adevărate centre de divertisment și exprimare artistică.

Epic Games, binecunoscut pentru succesul Fortnite, a depășit granițele unui joc convențional, transformându-l într-un veritabil hub cultural. Cu evenimente live, concerte și parteneriate emblematice, cum ar fi cele cu Timberland sau MTV, platforma a redefinit intersecția dintre gaming, muzică și lifestyle.

În ceea ce privește componenta tehnologică, Meta Platforms rămâne dominant, datorită investițiilor masive în realitatea virtuală. Casca VR Quest și platforma Horizon Worlds permit crearea de jocuri imersive și experiențe sociale extinse, consolidând poziția Meta ca lider în dezvoltarea infrastructurii necesare Metaversului.

Nu în ultimul rând, Improbable se implică în construirea fundamentelor tehnice ale Metaversului. Specializată în dezvoltarea infrastructurii pentru lumi virtuale masive, folosește tehnologii de conectivitate avansate pentru a susține interacțiuni fluide între mii de utilizatori simultan.

Împreună, aceste companii modelează un viitor în care granițele dintre real și virtual devin tot mai greu de distins.

Viitorul gamingului în Metavers

Industria gamingului evoluează rapid sub influența Metaversului, redefinind interacțiunea, monetizarea și creativitatea în spațiul virtual. Astfel că este urmărită adopția pe scară largă: acest lucru înseamnă că, platforme populare precum Minecraft și Fortnite atrag zilnic peste 200 de milioane de utilizatori, care participă la concerte, evenimente sociale și interacționează în economii virtuale complexe. Apoi sunt folosite tehnologii imersive¹⁶: inovații precum Google Starline, ce permite comunicarea prin holograme 3D fără echipamente speciale, promit să revoluționeze atât gamingul, cât și modul în care utilizatorii interacționează în mediile virtuale. Monetizarea și expresia creativă se referă la faptul că Metaversul transformă jocurile într-un ecosistem economic sustenabil, oferind oportunități de câștig prin NFT-uri și active digitale portabile. În același timp, jucătorii beneficiază de un control sporit asupra propriilor experiențe, având posibilitatea de a modela lumi virtuale personalizate. Aceste evoluții marchează un nou capitol în gaming, unde granițele dintre realitate și virtual devin tot mai fluide, iar utilizatorii devin nu doar consumatori, ci și creatori ai universurilor digitale.

¹⁶ Barnes A. (2023), *Metaverse in Gaming: Revolution in Gaming industry With Next-Generation Experience*, Disponibil la: <https://www.datasciencecentral.com/metaverse-in-gaming-revolution-in-gaming-industry-with-next-generation-experience/> [Accesat: 19 Aug. 2025].

Metaversul redefinește experiența gamingului creând lumi digitale imersive și interconectate în care jucătorii nu doar explorează aceste universuri, ci și dețin, tranzacționează și monetizează active digitale, transformând fundamental paradigma gamingului tradițional. Gamingul în Metavers nu mai este doar o formă de divertisment, ci o experiență complexă, în care tehnologia, economia digitală și interacțiunea socială se contopesc creând un nou univers de posibilități. Acest spațiu virtual evoluează rapid, susținut de o serie de caracteristici cheie ce îl diferențiază fundamental de jocurile clasice¹⁷.

Unul dintre cele mai remarcabile aspecte este imersiunea avansată. Prin intermediul tehnologiilor VR și AR, jucătorii pot pătrunde direct în universul jocului, experimentând medii 3D realiste care le oferă senzația de prezență fizică în lumea digitală. Fiecare mișcare, sunet sau interacțiune devine parte integrantă a unei realități virtuale tot mai convingătoare.

Pe lângă acest nivel ridicat de imersiune, interconectivitatea extinsă schimbă complet modul în care este trăită experiența din Metavers. Lumea virtuală nu mai este fragmentată în jocuri izolate, ci devine un ecosistem unificat, unde avatarurile și bunurile digitale pot fi transferate liber între platforme. Un obiect câștigat într-un joc nu mai rămâne blocat acolo — poate fi folosit și în alte spații virtuale, păstrându-și valoarea și funcționalitatea, indiferent de context.

Această mobilitate a activelor este susținută de economii virtuale descentralizate, alimentate de tehnologiile Blockchain și NFT. Jucătorii pot deține, vinde și cumpăra obiecte digitale în piețe virtuale reale, participând la o economie în care timpul și creativitatea investite în joc sunt recompensate material. Totodată, Metaversul devine și un spațiu efervescent de socializare digitală, în care interacțiunile umane capătă noi forme. Comunități globale se reunesc pentru a organiza evenimente, concerte, competiții sau pur și simplu pentru a explora împreună lumi virtuale, creând legături autentice dincolo de ecrane.

Pe măsură ce jucători din întreaga lume adoptă experiențele imersive ale Metaversului, iar dezvoltatorii explorează potențialul tehnologiilor emergente, se conturează o piață din ce în ce mai competitivă și inovatoare. Totodată, companiile investesc masiv în infrastructură, conținut și soluții de monetizare, anticipând un nou val de oportunități comerciale și sociale. Astfel, se modelează un ecosistem dinamic, în care granițele dintre joc, afacere și comunitate devin tot mai greu de distins¹⁸.

¹⁷ Kelly A. (2024), *Future Of Metaverse In Gaming Industry, Section: Game Development*, Disponibil la: <https://euphoriaxr.com/metaverse-in-gaming-industry-the-future-of-gaming/> [Accesat: 19 Aug. 2025].

¹⁸ Kelly A. (2024), *Future Of Metaverse In Gaming Industry, Section: Game Development*, Disponibil la: <https://euphoriaxr.com/metaverse-in-gaming-industry-the-future-of-gaming/> [Accesat: 19 Aug. 2025].

Referitor la numărul utilizatorilor activi, platforme precum Fortnite și Roblox atrag zilnic peste 200 de milioane de utilizatori, consolidând Metaversul ca spațiu central pentru gaming, socializare și economie digitală. Scena gamingului din Metavers este modelată de câțiva actori-cheie care, prin inovație și investiții strategice, conturează viitorul acestui univers digital. Fiecare dintre aceștia contribuie în mod distinct la dezvoltarea unui ecosistem virtual complex, în care creativitatea, economia digitală și experiențele sociale se împletesc¹⁹.

Exemple de jocuri în Metavers

Unele dintre cele mai reprezentative jocuri din Metavers sunt²⁰:

Axie Infinity – Joc play-to-earn bazat pe NFT-uri, unde jucătorii colecționează, cresc și luptă cu creaturi digitale;

Decentraland – Lume virtuală descentralizată, oferind terenuri digitale, evenimente interactive și o economie bazată pe criptomonede;

Farmers World – Simulator agricol în care resursele sunt reprezentate sub formă de NFT-uri și pot fi tranzacționate pe piețe digitale;

Pokémon Go – Un exemplu timpuriu de integrare a realității augmentate (AR), conectând lumea fizică cu cea virtuală prin explorare interactivă.

Jocurile din Metavers integrează o serie de inovații tehnologice care redefinesc modul în care utilizatorii interacționează cu lumea virtuală, oferind o experiență tot mai realistă, atrăgătoare și profitabilă. Printre cele mai remarcabile progrese se numără realismul avansat, adus de tehnologiile haptice și de realitatea virtuală cu rezoluție 4K, ce permit jucătorilor să simtă și să perceapă mediul virtual într-un mod aproape senzorial, sporind considerabil nivelul de imersiune. O altă direcție puternic susținută este modelul play-to-earn, prin care jucătorii pot genera venituri reale participând la misiuni, creând conținut digital sau tranzacționând NFT-uri. Astfel, gamingul devine nu doar un mijloc de divertisment, ci și o formă de activitate economică. În plus, se pune tot mai mult accent pe accesibilitate universală și compatibilitate extinsă, cu jocuri disponibile pe console, PC, dispozitive mobile și căști VR. Această versatilitate permite o experiență fluidă, indiferent de platforma aleasă de utilizator.

Potențialele riscuri sociale ale Metaversului

Cercetările evidențiază că jocurile video, inclusiv cele bazate pe realitate virtuală, precum VRChat sau Meta Horizon Worlds, pot prezenta riscuri sociale semnificative, agravate de lipsa unor reglementări adecvate. Studiile anterioare au arătat că aceste platforme pot contribui la normalizarea violenței, obiectificarea femeilor și pot fi exploatate de grupuri extremiste pentru recrutare, radicalizare și

¹⁹ Ibid.

²⁰ Ibid.

propagandă. În plus, mediile de gaming online sunt utilizate pentru diseminarea ideologiilor extremiste și chiar pentru antrenamente tactice. Spre exemplu, Anders Breivik, autorul atacului din Norvegia, a declarat că s-a antrenat folosind jocul Call of Duty: Modern Warfare. Cu toate acestea, aceste riscuri rămân insuficient studiate în contextul emergent al Metaversului (Ortiz, 2022).

Gamingul este una dintre cele mai mari industrii la nivel global, cu aproximativ 2,8 miliarde de jucători și venituri de 180 de miliarde de dolari în 2024. Deși jocurile video oferă beneficii importante, precum facilitarea interacțiunilor sociale, dezvoltarea colaborării și stimularea creativității, ele ridică și provocări majore în ceea ce privește siguranța utilizatorilor. Jocurile video reprezintă un mediu propice pentru formarea comunităților, crearea de prietenii și colaborarea în proiecte tehnologice. Cu toate acestea, odată cu avansul tehnologic, cresc și riscurile, amenințările și dilemele etice asociate.

În timp ce Metaversul promite o lume virtuală a conectării și explorării libere (Ortiz, 2022), realitatea arată și o fațetă întunecată a acestor spații digitale. Platforme precum VRChat, accesibile prin Steam, au ajuns să fie folosite nu doar pentru socializare și divertisment, ci și pentru propagarea ideologiilor extremiste. În astfel de medii, grupuri radicale își diseminează mesajele, incitând la ură și violență sub masca anonimatului oferit de avataruri și interacțiuni virtuale.

Cercetările recente atrag atenția asupra prezenței active a unor comunități afiliate organizațiilor extremiste violente, nu doar pe platforma Steam, ci și pe alte platforme populare precum Discord. Mai îngrijorător este faptul că, în aceste grupuri online de extremă dreaptă, vârsta medie a utilizatorilor este de doar 15 ani, evidențiind o reală vulnerabilitate a minorilor în fața fenomenului de radicalizare digitală. Această tendință subliniază necesitatea unui cadru solid de reglementare, monitorizare și educație digitală, pentru a proteja spațiile virtuale și, mai ales, pentru a apăra tinerii de influențe periculoase care se infiltrează din ce în ce mai subtil în universurile online.

În ciuda acestor riscuri, există puține studii care analizează în profunzime modul în care platformele de gaming sunt utilizate pentru recrutare și radicalizare, iar o întrebare persistă: de ce părinții și tutorii nu reușesc să își protejeze copiii mai eficient? Printre obstacolele principale se numără decalajul digital, lipsa educației tehnologice și dificultățile economice, care îngreunează supravegherea activităților online ale minorilor.

Pe lângă vârsta utilizatorilor, există și factori psihologici și sociali care pot favoriza radicalizarea, precum izolarea, depresia, sentimentul de excludere sau furia față de societate. Aceste realități subliniază necesitatea unor reglementări mai stricte, a unei monitorizări mai atente a platformelor din Metavers și a unei mai bune conștientizări a riscurilor asociate cu gamingul online.

Studiu de caz. Analiza UX și gamificare în Metavers

Succesul unei platforme depinde din ce în ce mai mult de experiența utilizatorului și de cât de bine funcționează totul. Un studiu recent a analizat exact asta - cum influențează interfața, ușurința în utilizare și funcțiile oferite, calitatea interacțiunilor digitale și viabilitatea pe termen lung a platformelor virtuale (Cheremnykh, 2024).

Pentru a evalua eficiența și gradul de accesibilitate al acestor medii, analiza a fost realizată pe baza a zece principii de utilizabilitate, ce acoperă aspecte precum mecanicile de joc, suportul comunitar, securitatea, compatibilitatea multiplatformă și modelele de guvernare descentralizată.

Printre factorii analizați s-au numărat (Cheremnykh, 2024):

- Mecanici de Joc (Primary Play) – Crearea unui mediu interactiv, care să faciliteze explorarea și generarea de conținut
- Compatibilitate multiplatformă – Optimizarea funcționalității pe diverse dispozitive, de la desktop și mobile la VR;
- Modelul de monetizare – Oferirea unor opțiuni flexibile de abonamente și servicii personalizate;
- Designul avatarurilor și elementele vizuale – Un stil minimalist și intuitiv, care îmbunătățește reprezentarea digitală a utilizatorilor;
- Instrumente de comunicare – Implementarea chat-ului vocal și text pentru o interacțiune eficientă în timp real;
- Suport comunitar – Prezența unor echipe dedicate pentru asistență și rezolvarea problemelor utilizatorilor;
- Colaborare și interoperabilitate – Funcționalități care permit schimbul de informații și colaborarea între utilizatori;
- Securitate și confidențialitate – Măsuri solide de protecție a datelor, care să confere încredere utilizatorilor;
- Integrare pentru Dezvoltatori – API-uri și ecosisteme flexibile, menite să faciliteze interoperabilitatea și extinderea platformelor;
- Guvernare și Descentralizare – Promovarea unui model democratic care asigură transparență și sustenabilitate pe termen lung.

Analiza a fost completată cu un cadru de gamificare bazat pe Game UX Framework, alături de teorii precum Self-Determination Theory (SDT), Social Learning Theory (SLT) și sisteme de recompense și progresie²¹.

²¹ Kelly A. (2024), *Future Of Metaverse In Gaming Industry, Section: Game Development*, Disponibil la: <https://euphoriaxr.com/metaverse-in-gaming-industry-the-future-of-gaming/> [Accesat: 19 Aug. 2025].

Aceste concepte au fost aplicate în evaluarea comportamentului și motivației utilizatorilor în hărțile Fortnite, demonstrând cum elementele de gamificare pot îmbunătăți angajamentul și experiența acestora.

Studiul a subliniat că succesul unei platforme din Metavers depinde de integrarea unei UX intuitive și funcționale, alături de mecanici de joc bine definite și elemente de gamificare. Această combinație nu doar că oferă o experiență captivantă pentru utilizatori, dar sprijină și dezvoltatorii, asigurând un ecosistem sustenabil pentru creatori și comunități.

Aceste criterii conturează un cadru de referință pentru dezvoltarea platformelor din Metavers, având ca obiectiv nu doar crearea unor medii captivante, ci și asigurarea unei experiențe interactive, sigure și sustenabile pentru utilizatori și dezvoltatori deopotrivă.

Viziune versus pragmatism în Metavers

Metaversul a captat imaginația publicului ca o paradigmă revoluționară a viitorului digital. Cu toate acestea, deși a fost promovat ca următoarea generație a Internetului (“NextG Internet”), numeroasele promisiuni legate de Metavers nu au fost întru totul realizate până în prezent. În continuare analizăm principalele predicții făcute despre Metavers, discrepanțele dintre viziuni și realitate, precum și factorii care contribuie la aceste lacune.

Lipsa interoperabilității

Una dintre cele mai ambițioase promisiuni ale Metaversului a fost crearea unui spațiu digital interoperabil, în care utilizatorii și conținutul pot tranzita fără bariere între diferite platforme. Realitatea actuală arată că majoritatea platformelor Metaversului sunt silozuri izolate, fără standarde comune care să permită transferul ușor al activelor digitale și al identităților utilizatorilor (R. Cheng et al., 2022).

Lipsa interoperabilității afectează nu doar experiența utilizatorilor, dar și potențialul de colaborare între diferite ecosisteme virtuale. Un exemplu clar în acest sens este dependența utilizatorilor de un ecosistem unic, cum ar fi Meta sau Roblox, unde bunurile digitale achiziționate sau create sunt limitate exclusiv la acea platformă. Acest lucru îngreunează libertatea creativă și limitează valoarea economică a activelor virtuale. Soluțiile propuse includ dezvoltarea unor standarde deschise și a unor protocoale comune care să permită interoperabilitatea, așa cum sugerează (Chen et al., 2023).

Adoptarea limitată și integrarea zilnică

Metaversul a fost anticipat ca o tehnologie care va deveni parte integrantă a vieții cotidiene, similar smartphone-urilor (Pew Research Center, 2022). Adoptarea

pe scară largă a Metaversului este frânată de mai mulți factori. Printre aceștia se numără lipsa unui conținut diversificat și a aplicațiilor relevante, care diminuează atractivitatea Metaversului pentru diverse categorii de utilizatori. Integrarea acestuia în activitățile zilnice, precum munca, educația sau divertismentul, rămâne insuficientă. Soluțiile propuse includ dezvoltarea de aplicații cu un impact practic ridicat și crearea de conținut personalizat, care să răspundă unor nevoi variate (Chen et al., 2023).

Realismul imersiv

O altă promisiune cheie a fost crearea de experiențe virtuale aproape fotorealiste. Deși tehnologiile grafice și dispozitivele XR (Realitate Extinsă) au îmbunătățit considerabil calitatea vizuală și interactivitatea, acestea nu reușesc încă să atingă nivelul de realism necesar pentru a oferi o experiență cu adevărat imersivă (Mystakidis, 2022). Lipsa unui echilibru între fidelitatea vizuală și costurile accesibile reprezintă principala barieră pentru adoptarea pe scară largă.

Un alt obstacol îl reprezintă lipsa dispozitivelor haptice avansate care să completeze experiența vizuală cu feedback tactil. De exemplu, soluțiile actuale precum controlerele de VR, sunt limitate în a reda cu precizie senzațiile fizice dintr-un mediu virtual (Chen et al., 2023). De asemenea, multe platforme Metavers nu sunt capabile să susțină interacțiuni complexe în timp real, cum ar fi simulările fizice detaliate sau reprezentările dinamice ale avatarurilor umane. Pentru a depăși aceste provocări, este necesară integrarea tehnologiilor emergente, precum ray-tracing-ul în timp real, inteligența artificială pentru animații faciale autentice și dispozitive care să permită utilizatorilor să interacționeze cu mediul digital într-un mod cât mai natural (R. Cheng et al., 2022).

Accesibilitatea tehnologică

Una dintre promisiunile fundamentale ale Metaversului a fost democratizarea accesului la tehnologiile necesare pentru a explora pe deplin acest spațiu virtual. Totuși, realitatea a demonstrat că prețurile ridicate ale dispozitivelor VR și AR (precum Meta Quest sau HoloLens) rămân un obstacol important, limitând accesul la acest mediu doar unui segment restrâns al populației (Chen et al., 2023). Pentru a oferi o experiență fluidă, aceste echipamente costisitoare au nevoie de computere performante, ceea ce crește semnificativ povara financiară asupra utilizatorului.

Un alt aspect important este lipsa diversității în opțiunile hardware, care afectează adoptarea pe scară largă. Majoritatea dispozitivelor sunt încă voluminoase, inconfortabile pentru utilizare îndelungată și nu reușesc să integreze pe deplin funcționalități necesare, cum ar fi senzori avansați pentru mișcare sau haptică sofisticată (Mystakidis, 2022). Aceste limitări tehnice contribuie la o experiență

fragmentată, departe de viziunea inițială a unui Metavers fluid și accesibil tuturor. În plus, infrastructura globală joacă un rol critic. În multe regiuni mai puțin dezvoltate, vitezele Internetului și stabilitatea conexiunii nu sunt suficient de ridicate pentru a susține experiențe VR/AR de calitate (R. Cheng et al., 2022), creând astfel o segregare digitală între, țările cu infrastructuri tehnologice avansate și cele care nu pot beneficia pe deplin de potențialul Metaversului.

Soluțiile propuse pentru a depăși aceste bariere includ dezvoltarea unor dispozitive mai accesibile din punct de vedere financiar, bazate pe tehnologii open-source și investiții în miniaturizarea și îmbunătățirea confortului hardware-ului existent. De asemenea, adoptarea rețelelor 5G și a tehnologiilor emergente, cum ar fi edge computing, ar putea sprijini o accesibilitate mai mare, reducând cerințele hardware de pe dispozitivele utilizatorilor (Pew Research Center, 2022; Chen et al., 2023).

Economia digitală instabilă

Pentru a se putea susține, Metaversul trebuie să fie un spațiu cu economie digitală robustă. Această economie trebuia să fie susținută de bunuri virtuale, NFT-uri și tranzacții bazate pe criptomonede. Cu toate acestea, realitatea a demonstrat că piața bunurilor virtuale este extrem de volatilă, fiind adesea caracterizată de speculații financiare și fluctuații majore în valoare ceea ce face investițiile imprevizibile. (X. Cheng et al., 2022).

De exemplu, valoarea NFT-urilor, considerate un pilon important al economiei Metaversului, a scăzut drastic după un vârf inițial, punând sub semnul întrebării sustenabilitatea pe termen lung a acestor active digitale. O altă problemă majoră este lipsa încrederii utilizatorilor în tranzacțiile digitale din Metavers, alimentată de fraude și lipsa unor reglementări clare. Studiile arată că, în absența unor cadre legale bine definite, utilizatorii ezită să investească sume semnificative în active virtuale, ceea ce limitează creșterea economică a acestui ecosistem (R. Cheng et al., 2022).

Mai mult, disparitățile de acces la resursele digitale accentuează inegalitățile economice în cadrul Metaversului. Utilizatorii din regiunile mai puțin dezvoltate au acces limitat la oportunitățile economice oferite de acest spațiu virtual, amplificând diviziunile existente dintre economiile globale²².

Pentru a atenua aceste probleme, experții propun dezvoltarea unor mecanisme de reglementare internaționale care să protejeze utilizatorii și să stabilească standarde pentru tranzacțiile din Metavers. De asemenea, se recomandă investiții în educație digitală pentru a ajuta utilizatorii să înțeleagă riscurile și oportunitățile asociate cu economia digitală (X. Cheng et al., 2022).

²² Pew Research Center (2022), *The Metaverse in 2040*, Disponibil la: <https://www.pewresearch.org/internet/2022/06/30/the-metaverse-in-2040/> [Accesat: 28 Ian. 2025].

Conexiuni sociale și incluziune

Deși Metaversul a fost promovat ca un spațiu în care limitările sociale din lumea fizică pot fi depășite, realitatea actuală arată că aceste idealuri sunt încă departe de a fi atinse. Multe platforme din Metavers au probleme persistente legate de comportamentele toxice, cum ar fi hărțuirea online, excluderea socială și crearea de medii nesigure pentru utilizatori²³.

Una dintre provocările majore este lipsa unor mecanisme eficiente de moderare și reglementare a interacțiunilor sociale. Spre exemplu, multe platforme bazate pe VR permit o libertate extinsă a utilizatorilor, dar nu dispun de instrumente adecvate pentru a preveni sau sancționa comportamentele abuzive. Studiile arată că hărțuirea și agresiunea virtuală au un impact direct asupra dorinței utilizatorilor de a participa la astfel de medii, reducând astfel potențialul social al Metaversului și limitând interacțiunile pozitive între utilizatori.(Mystakidis, 2022).

De asemenea, problemele de accesibilitate și reprezentare contribuie la excluderea anumitor grupuri din Metavers. Utilizatorii din medii socio-economice defavorizate sau utilizatorii cu dizabilități se confruntă cu bariere tehnologice și economice care limitează accesul la aceste platforme. În plus, reprezentarea diversității culturale, etnice și de gen în avataruri și interfețe rămâne insuficient dezvoltată, perpetuând inegalitățile din lumea fizică în cea virtuală. Pentru a aborda aceste probleme, experții recomandă implementarea unor politici clare de moderare, crearea unor cadre etice pentru interacțiuni sociale și dezvoltarea unor mecanisme de raportare eficientă a abuzurilor. De asemenea, este importantă dezvoltarea de tehnologii incluzive, care să asigure participarea egală a tuturor utilizatorilor, indiferent de mediul lor socio-economic sau de particularitățile lor fizice (X. Cheng et al., 2022).

Integrarea inteligenței artificiale pentru moderarea în timp real a interacțiunilor și dezvoltarea unor norme sociale acceptate în spațiul virtual sunt următorii pași pentru transformarea Metaversului într-un mediu mai sigur și mai primitor. Totodată, promovarea diversității și incluziunii prin design participativ și crearea unor avataruri care să reflecte identitatea diverselor grupuri sociale pot contribui la consolidarea unui spațiu digital mai echitabil și mai incluziv.

Sustenabilitate

Deși Metaversul a fost prezentat ca o alternativă sustenabilă pentru numeroase activități din lumea fizică, impactul său ecologic actual contrazice multe dintre aceste promisiuni. Teoretic, tranziția unor activități precum întâlnirile, educația sau divertismentul în mediul virtual ar trebui să reducă utilizarea resurselor fizice,

²³ Ibid.

precum transportul sau construirea infrastructurilor. Cu toate acestea, infrastructura necesară pentru funcționarea Metaversului este extrem de intensivă din punct de vedere energetic.

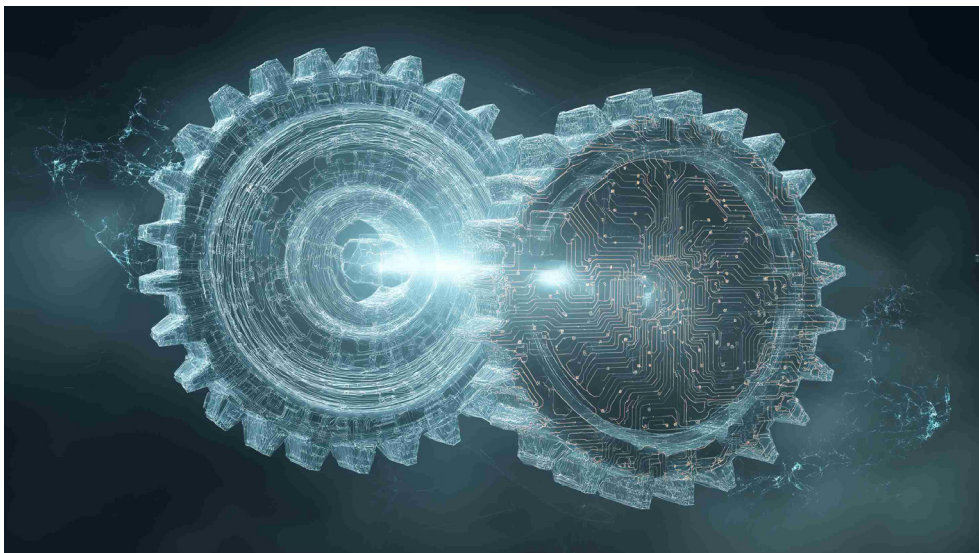
Centrele de date care susțin Metaversul, rețelele Blockchain folosite pentru active digitale și dispozitivele hardware de înaltă performanță consumă cantități semnificative de energie. Tehnologiile Blockchain, utilizate frecvent pentru tranzacțiile cu NFT-uri și criptomonede, contribuie semnificativ la emisiile globale de carbon (X. Cheng et al., 2022). De exemplu, mineritul de criptomonede necesar pentru susținerea economiilor digitale din Metavers are un impact ecologic comparabil cu consumul energetic anual al unor țări mici (R. Cheng et al., 2022). Mai mult, dispozitivele VR și AR necesare pentru accesarea Metaversului conțin piese din materiale rare și dificil de reciclat, ceea ce contribuie la creșterea deșeurilor electronice. Lipsa unor inițiative globale pentru reciclarea acestor dispozitive accentuează problema, limitând sustenabilitatea pe termen lung a Metaversului²⁴.

Pentru a aborda aceste provocări, experții propun câteva soluții strategice. În primul rând, adoptarea surselor de energie regenerabilă pentru alimentarea centrelor de date ar putea reduce semnificativ impactul ecologic al infrastructurii digitale. În al doilea rând, implementarea unor protocoale eficiente de utilizare a energiei în Blockchain ar putea contribui la diminuarea emisiilor de carbon asociate cu tranzacțiile digitale. De asemenea, dezvoltarea dispozitivelor hardware cu un ciclu de viață mai lung și posibilitatea reciclării componentelor ar putea contribui la reducerea deșeurilor electronice.

Pentru a reduce acest decalaj, este necesară o puternică colaborare interdisciplinară și intersectorială între industrie, mediul academic și autoritățile publice. Industria poate accelera dezvoltarea tehnologică prin inovare, în timp ce mediul academic poate oferi soluții privind gestionarea etică a datelor, impactul psihologic al interacțiunilor virtuale și dezvoltarea unor standarde globale care să reglementeze acest spațiu digital emergent. În paralel, guvernele trebuie să joace un rol activ în crearea unor politici și cadre legislative adaptate, menite să asigure incluziunea socială, protecția drepturilor digitale și reducerea inegalităților tehnologice dintre regiuni. Totodată, sprijinirea inițiativelor de educație digitală și investițiile strategice în infrastructura tehnologică vor permite participarea echitabilă a tuturor la această transformare.

²⁴ Pew Research Center (2022), *The Metaverse in 2040*, Disponibil la: <https://www.pewresearch.org/internet/2022/06/30/the-metaverse-in-2040/> [Accesat: 28 Ian. 2025].

2. Guvernanța datelor și reglementarea Inteligenței Artificiale



Metaversul este o platformă care își propune să pătrundă în multe domenii ale vieții noastre, de la cele societale la cele personale. Infrastructura sa de date, modul în care este guvernat și sistemul său economic sunt concepute pentru a se adapta și a funcționa în aceste diverse contexte (Bibri et al., 2022). Pe măsură ce acest domeniu evoluează, guvernanța datelor are un rol important pentru a asigura un mediu digital sigur și de încredere pentru toți participanții.

Pentru a putea merge mai departe, este necesar să înțelegem terminologia cuvintelor guvernare, guvernanță și management.

Din punct de vedere al terminologiei, cuvintele „governing” (guvernare), „governance” (guvernanță) și „management” au sensuri distincte.

„Governance” se referă la organizarea logică prin care se gestionează datele, incluzând colectarea, stocarea, procesarea, utilizarea, partajarea și distrugerea acestora.

„Governing” cuprinde acțiunile necesare pentru a implementa această organizare, incluzând modul de utilizare a datelor și identificarea responsabilităților cu privire la date. Conceptual, guvernanța datelor presupune autoritatea și controlul asupra managementului datelor. Structural, aceasta se exercită prin reguli, stimulente și sancțiuni, creând o cultură organizațională care subliniază importanța datelor și impune consecințe pentru încălcarea regulilor de gestionare a datelor.

Un aspect cheie al acestei guvernante este utilizarea Big Data, care reprezintă o resursă critică pentru Metavers, oferind companiilor și utilizatorilor informații valoroase pentru a înțelege și a răspunde mai bine nevoilor și preferințelor acestora. Cantitățile mari de date colectate în Metavers pot fi transformate în informații pentru afaceri. Analiza acestor date ajută companiile să înțeleagă mai bine clienții, să profileze soluțiile și să ia decizii mai bune. Totodată, este necesară dezvoltarea unor reguli de guvernanta a datelor care să fie auto adaptative și auto optimizabile, capabile să gestioneze volumele de date în creștere dinamică și să se adapteze la o gamă largă de medii virtuale. Cu timpul, Big Data va deveni indispensabilă pentru dezvoltarea unui Metavers centrat pe nevoile umane (Sun et al., 2022).

În plus, caracteristicile unice ale Metaversului - creșterea rapidă a cantității datelor, tipurile diverse de date, partajarea sporită și interacțiunile complexe - ridică întrebări cu privire la proprietatea și confidențialitatea datelor. Acestea sunt provocări care pot fi depășite doar printr-o reglementare de guvernanta solidă a datelor. Crearea unui mediu digital de încredere pentru utilizatori începe prin gestionarea și utilizarea eficientă a datelor din Metavers într-un mod echitabil, sigur, eficient și legal (Ooi et al., 2022).

În Metavers, unde tipurile de date sunt extrem de variate și mediile virtuale tot mai interconectate, este necesară elaborarea unei paradigme de management al datelor care să fie atât securizată, cât și verificabilă. Această infrastructură digitală complexă, poate fi susținută de un model de guvernanta eficient, capabil să gestioneze date diverse în contexte virtuale interoperabile. În plus, reglementările juridice și sistemele de securitate se cer adaptate, aliniat și consolidate, mai ales în cazul organizațiilor care își desfășoară activitatea dincolo de granițe și gestionează date transfrontaliere. (Ooi et al., 2022).

Rolul datelor în Metavers

În cadrul Metaversului, datele joacă un rol fundamental atât pentru utilizatori, cât și pentru companii, oferind baza necesară pentru personalizarea lumilor virtuale. Această personalizare aduce o gamă largă de caracteristici și funcționalități care transformă interacțiunile obișnuite în experiențe profund imersive. Procesele de instruire și învățare capătă un caracter mult mai atractiv și dinamic, în timp ce strategiile de marketing devin tot mai eficiente, adaptându-se în mod inteligent preferințelor fiecărui utilizator și creând campanii personalizate și impactante¹.

Odată conectați în Metavers, utilizatorii din lumea reală pătrund într-un spațiu vast, unde își pot explora creativitatea și pot interacționa cu alții în timp real,

¹ Stefanic D. (2025), *Unlocking the Power of Data in Metaverse Experiences*, Disponibil la: <https://hyperspace.mv/data-in-metaverse/> [Accesat: 19 Aug. 2025].

prin intermediul avatarurilor lor. Fie că este vorba de socializare, educație, afaceri sau divertisment, tehnologiile avansate din Metavers permit desfășurarea unor activități similare celor din lumea fizică, dar cu un plus de libertate și posibilități creative nelimitate².

În esență, formatul datelor constituie fundamentul ecosistemului Metaversului, facilitând interoperabilitatea și oferind utilizatorilor o experiență continuă și fără întreruperi. Indiferent de platforma pe care se conectează, aceștia își pot utiliza și partaja avatarurile și activele digitale fără restricții de compatibilitate, contribuind astfel la crearea unui univers virtual armonizat și interconectat.

Pe măsură ce Metaversul se dezvoltă, devine tot mai imperativă adoptarea unor formate de date deschise și accesibile utilizatorilor. Standardizarea acestora reprezintă un aspect fundamental pentru asigurarea coerenței și atractivității mediului digital, contribuind la eliminarea obstacolelor care ar putea restricționa interacțiunea socială și procesul de inovare.

Tehnologiile avansate integrate în Metavers asigură experiențe imersive, interactive și sigure. Realitatea virtuală (VR), realitatea augmentată (AR) și realitatea mixtă (MR), combinate cu feedback-ul haptic, sunt folosite pentru a spori nivelul de realism al experiențelor virtuale, făcându-le mai tangibile și mai captivante. În anii recenti, Inteligența Artificială are o contribuție tot mai pregnantă în dezvoltarea entităților digitale inteligente și în optimizarea modului în care utilizatorii interacționează între ei, creând astfel un mediu virtual mai natural și mai intuitiv. În cadrul acestui ecosistem complex, infrastructurile de calcul cloud și edge asigură gestionarea eficientă a stocării și procesării datelor, facilitând interconectarea dintre spațiile imersive 3D, dispozitivele și echipamentele utilizate, avatarurile și platformele digitale. Aceste tehnologii permit utilizatorilor să creeze și să exploreze experiențe virtuale avansate, oferind suport pentru operarea și gestionarea activelor digitale (Gadekallu et al., 2023).

În ecosistemul Metavers, unde se întâlnesc utilizatori, tehnologii și platforme variate, adoptarea unor formate de date standardizate va deveni indispensabilă pentru asigurarea continuității și interoperabilității acestui univers virtual complex. Modul în care aceste formate sunt alese va impacta direct modul în care conținuturile digitale sunt create, distribuite și experimentate, iar rolul lor este explorat în detaliu în cele ce urmează.

1. Asigurarea interoperabilității între platforme. Utilizarea formatelor standardizate de date permite ca activele digitale create pe o platformă să fie compatibile și utilizabile pe alte platforme, asigurând portabilitatea acestora în întregul ecosistem virtual.

² Ibid.

2. Menținerea uniformității în experiența utilizatorului. Prin adoptarea formatelor de date standardizate, obiectele virtuale și avatarurile își păstrează aspectul și funcționalitatea în diverse medii din Metavers. Totodată, aceste formate elimină întreruperile în animațiile avatarurilor personalizate, permițând utilizatorilor să își mențină identitatea digitală indiferent de spațiul virtual accesat.
3. Optimizarea colaborării și a distribuției de conținut. Dezvoltatorii și creatorii de conținut beneficiază de posibilitatea de a partaja modele 3D, animații și texturi între diferite instrumente software, fără riscul erorilor de conversie sau al pierderii calității. Standardizarea formatelor de date facilitează accesul la active și conținuturi digitale atât pentru dispozitivele de ultimă generație, cât și pentru cele mobile, eliminând dependența utilizatorilor de aplicații software și echipamente specifice pentru a interacționa în Metavers.
4. Asigurarea scalabilității. Încărcarea rapidă a mediilor virtuale și funcționarea fără erori reprezintă cerințe primordiale pentru a permite interacțiunea în timp real a unui număr mare de utilizatori. Utilizarea formatelor de date standardizate contribuie la atingerea acestor obiective, optimizând eficiența rețelei și reducând latența. Acest aspect este deosebit de important pentru îmbunătățirea calității utilizării în cazul utilizatorilor care folosesc dispozitive cu performanțe reduse.
5. Promovarea inovării. Adoptarea unor standarde deschise și larg acceptate facilitează dezvoltarea de noi instrumente și aplicații, contribuind la diversificarea și îmbunătățirea experiențelor din Metavers. Un avantaj major al acestor formate este flexibilitatea lor, permițând integrarea rapidă a noilor funcționalități și îmbunătățiri fără a fi restricționate de tehnologii sau formate proprietare.
6. Asigurarea longevității datelor. Utilizarea formatelor de date standardizate garantează păstrarea pe termen lung a activelor digitale și menținerea unui conținut persistent într-un mediu tehnologic în continuă evoluție. Aceste formate durabile asigură compatibilitatea pe termen lung a obiectelor 3D, avatarurilor și mediilor virtuale, prevenind situațiile în care activele digitale devin inaccesibile din cauza dependenței de platforme sau tehnologii proprietare. Astfel, investițiile și munca depuse în Metavers sunt protejate, iar utilizatorii și dezvoltatorii beneficiază de posibilitatea de a transfera liber activele digitale între diverse platforme, indiferent de schimbările tehnologice viitoare.
7. Asigurarea interacțiunii în timp real. Utilizarea formatelor de date standardizate pentru reprezentarea comportamentului și interacțiunilor în

spațiile 3D permite o interacțiune fluidă și precisă între avatare și obiecte virtuale, asigurând un răspuns corect în diverse medii digitale. În special pentru spațiile de lucru colaborative din domeniul educației și al companiilor, aceste formate de date sunt folosite pentru facilitarea colaborării asupra obiectelor digitale partajate. Astfel, toți participanții pot vizualiza, manipula și adnota modele 3D ale produselor în timp real, indiferent de instrumentele software utilizate.

8. Asigurarea confidențialității, securității și guvernancei datelor. Standardizarea formatelor de date pentru reprezentarea avatarurilor și identităților digitale (precum JSON-LD) contribuie la protecția datelor personale, indiferent de platforma utilizată (Hansson, 2024). În plus, informațiile utilizatorilor și tranzacțiile financiare din Metavers, cum ar fi achiziționarea, vânzarea sau transferul de bunuri virtuale, sunt securizate împotriva fraudei și furtului prin utilizarea protocoalelor criptografice standardizate, precum SSL (Secure Socket Layer) și TLS (Transport Layer Security).

În cele ce urmează, explorăm principalele contexte în care adoptarea formatelor de date standardizate devine determinantă pentru funcționarea coerentă și eficiență a Metaversului:

1. Fișierele și modelele 3D. Formatele standardizate pentru avataruri și obiectele 3D asigură posibilitatea de a crea și modifica fișierele și de a fi folosite pe diferite platforme din Metavers. Formatele utilizate aici (Nam et al., 2019) sunt GLTF (Graphics Library Transmission Format), USD (Universal Scene Description) și FBX (Filmbox). Formatul GLTF este de tip open-source și este utilizat de obicei pentru transmiterea scenelor și a modelelor 3D în aplicații în timp real, fiind ideal pentru lumile virtuale din Metavers. Formatul USD este un framework pentru descrierea scenelor complexe 3D, incluzând geometrie, texturi și animații. Este un format des folosit pentru gestionarea conținutului 3D în mediile de colaborare. FBW este formatul obișnuit pentru schimbul de modele 3D și animații în mediile virtuale, oferind o reprezentare de calitate a acestora și este utilizat mai ales în jocuri și filme, precum și în alte medii digitale. Formatul OBJ este un format simplu, utilizat pentru obiectele 3D, pentru schimbul între platformele software și modele.
2. Identitate virtuală și avataruri. Avatarurile în Metavers reprezintă identitățile digitale ale utilizatorilor pe diferite platforme și lumi virtuale, iar interoperabilitatea avatarurilor depinde de utilizarea formatelor standardizate. În acest context, formatele de date asigură utilizatorilor identități și personalizări compatibile în lumile virtuale. Aceste formate asigură că avatarurile pot fi

create, personalizate și folosite pe diferite platforme. Sunt întâlnite aici formatele VRM (Virtual Reality Model), X3D (Extensible 3D) și BVH (Biovision Hierarchy). VRM este folosit pentru portabilitatea avatarurilor, personalizarea și includerea de metadate, precum mișcarea și expresiile faciale. X3D este folosit la reprezentarea grafică 3D și a interacțiunilor, fiind util pentru aplicațiile 3D bazate pe web din Metavers. BVH este un format care stochează date de captură a mișcării pentru caracterele 3D și este folosit în mișcările și interacțiunile din spațiile virtuale.

3. Texturi și iluminare. În contextul creării și redării unor lumi virtuale complexe în Metavers este nevoie de formate standard pentru manipularea datelor spațiale, texturilor și elementelor care țin de mișcare. Texturile definesc aspectul realist și coerent al obiectelor 3D din Metavers. Formatele utilizate sunt PNG, JPEG, DDS (DirectDraw Surface), PBR (Physically-Based Rendering) și HDRI (High Dynamic Range Imaging). Aceste formate asigură încărcarea și redarea texturilor în mediile virtuale sau pot fi utilizate împreună cu formatele GLTF și USD (Universal Scene Description) pentru crearea suprafețelor realiste în mediile 3D. USD este un format din ce în ce mai utilizat în descrierea scenelor 3D și a unor active complexe. OpenEXR este un format pentru texturi și imagini, esențial în menținerea unor lumi virtuale, asigurând iluminare / reflexii. Formatele BIM (Building Information Modeling) și IFC (Industry Foundation Classes) sunt standarde utilizate în domeniile arhitectură și construcții pentru crearea de modele 3D. Aceste formate ar putea fi folosite în Metavers pentru proiectarea și administrarea proprietăților imobiliare virtuale, de la simple locuințe până la orașe. Formatele de date geospațiale (cum ar fi GeoJSON) sunt necesare pentru maparea lumilor fizice și virtuale, odată ce Metavers poate utiliza datele obținute din serviciile bazate pe locație.
4. Animații și interacțiuni. Pentru asigurarea unei experiențe coerente și fluide a utilizatorilor pe platforme, este nevoie de formate standardizate pentru animații și interacțiuni precum, Collada (Collaborative Design Activity) și Alembic. Formatul Collada stochează date fizice, modele 3D și animații, fiind utilizat la transferul fișierelor între diferite instrumente 3D și platforme în Metavers. Alembic este un format utilizat pentru schimbul de scene și modele animate complexe.
5. Proprietate digitală și Blockchain. În Metavers proprietatea asupra bunurilor digitale (precum avataruri, terenuri virtuale și obiecte de colecție) este legată de tehnologiile Blockchain și jetoanele NFT (Non-Fungible Tokens). Aceste NFT-uri se bazează pe formate de date standard pentru a verifica metadatele,

securitatea și integritatea tranzacțiilor și dreptul de proprietate al activelor virtuale (Far et al., 2022). Odată ce activele virtuale sunt protejate împotriva falsificării sau fraudei, încrederea în folosirea activelor crește și implicit economia Metavers se poate dezvolta. Formatele de date se referă în acest caz la modul în care aceste active sunt reprezentate, stocate și transferate în rețelele descentralizate. Standardele ERC-721 și ERC-1155 sunt standarde token Ethereum, care permit crearea, cumpărarea și vânzarea de active digitale unice în mediul virtual. Standardul ERC-721 oferă fiecărui token ERC-721 unicitate și caracteristica de a nu fi interschimbabil, ceea ce îl face ideal pentru reprezentarea activelor de tip colecție, artă digitală sau domeniu imobiliar. Standardul ERC-1155 este de tip multi-token și permite crearea de jetoane nefungibile și semi-fungibile într-un contract. În contextul portabilității și standardizării, protocolul descentralizat de stocare a fișierelor IPFS (InterPlanetary File System) este dedicat stocării și accesării activelor digitale mari (cum ar fi obiecte 3D de înaltă rezoluție). Acest lucru permite utilizatorilor să își transfere articolele virtuale între diferite lumi virtuale sau să le vândă pe o piață descentralizată.

6. Comunicarea audio și sunetul spațial. Comunicarea audio se referă la tehnologiile utilizate de dispozitivele electronice, de aplicații sau platforme care permit participanților să audă și să vorbească cu alți participanți în timp real, indiferent de locația lor fizică. În contextul experiențelor imersive de înaltă calitate, formatele standard Ogg, MP3 și AAC sunt folosite la transmisiile live sau audio din mediile virtuale. Formatele Ambisonics și formatele 3D audio sunt utilizate la crearea de peisaje sonore captivante care urmăresc mișcările fizice ale unui utilizator. Aceste formate reglează calitatea sunetului ca și când ar proveni din direcții și distanțe adecvate.
7. Colaborări și schimb de date. În contextul integrării conținutului sau al simulărilor interactive pe diferite platforme Metavers, colaborarea între utilizatori necesită în Metavers utilizarea de formate compatibile pentru a-și putea distribui cu ușurință datele. Formatul X3D (Extensible 3D) reprezintă un format de fișier pentru redarea scenelor 3D, a obiectelor și interacțiunilor între obiecte. Formatele de colaborare pot cuprinde formatele tradiționale întâlnite la locul de muncă (cum ar fi doc, pdf și xls) și formate de date colaborative în timp real.

Guvernanța datelor în sisteme bazate pe Inteligența Artificială

Procesul de colectare și pregătire a datelor pentru un sistem de Inteligență Artificială (IA) este unul complex și deosebit de laborios, deși adesea nu i se acordă importanța cuvenită. Volumul uriaș de informații preluate din surse diverse poate conduce la probleme legate de calitatea datelor, ceea ce, implicit, generează provocări în ceea ce privește gestionarea și guvernanța acestora (Janssen et al., 2020).

Evaluarea calității datelor se bazează pe mai mulți factori relevanți, precum acuratețea, actualitatea, completitudinea, consistența, obiectivitatea, credibilitatea și relevanța. Acești indicatori determină în ce măsură datele sunt adecvate pentru un anumit scop și influențează eficiența sistemelor de Inteligență Artificială (Janssen et al., 2020).

Evoluțiile tehnologice au transformat procesul de colectare a datelor într-unul extrem de rapid și eficient, facilitând agregarea informațiilor dintr-o varietate de surse simultan. Totuși, această capacitate sporită aduce și provocări, deoarece, alături de date de înaltă calitate, sunt colectate și informații eronate sau incomplete, care pot compromite acuratețea sistemelor care le utilizează. Pe măsură ce volumul de date crește, variația calității acestora face ca gestionarea și structurarea lor să devină din ce în ce mai complexă (Janssen et al., 2020). Chiar și în ipoteza ideală în care toate datele colectate ar avea un nivel ridicat de calitate, rămâne o problemă: discrepanța dintre realitatea actuală și informațiile înregistrate. Spre exemplu, o adresă stocată într-o bază de date devine irelevantă în momentul în care persoana respectivă își schimbă domiciliul, iar informația nu este actualizată în timp util.

În prezent, majoritatea instituțiilor guvernamentale conștientizează importanța datelor și necesitatea educării societății în acest domeniu. Cu toate acestea, implementarea unei astfel de inițiative este dificilă, deoarece datele sunt adesea fragmentate între multiple entități, fiecare având politici și standarde proprii privind gestionarea acestora. Lipsa unei abordări unitare poate afecta calitatea sistemelor IA care se bazează pe aceste date. Astfel, un obiectiv fundamental al guvernanței datelor pentru IA ar trebui să fie nu doar menținerea calității acestora, ci și utilizarea lor într-un mod corect și eficient.

Provocările actuale ne arată cât de importantă este guvernanța riguroasă a datelor, pentru a menține informațiile folosite de sistemele de inteligență artificială corecte, actualizate și relevante. O administrare bine gândită poate transforma IA într-un instrument cu adevărat valoros, reducând riscurile generate de date inexacte. Totuși, una dintre marile probleme este lipsa unui model universal de guvernanță, care să ofere tuturor organizațiilor un cadru comun și eficient (Janssen et al., 2020). În acest sens, există trei abordări principale care pot fi adoptate pentru a asigura gestionare eficientă și conformă. Prima abordare vizează modelul de planificare și

control. Acest model stabilește politici și proceduri clare pentru gestionarea datelor și introduce mecanisme de verificare care garantează calitatea și integritatea lor. Alocarea bugetelor și resurselor se face în funcție de priorități, pentru a evita risipa și pentru a menține coerența..

A doua abordare este axată pe modelul organizațional. Acesta pornește de la structura internă a companiei. Definirea rolurilor și responsabilităților, echipe dedicate și leadership clar sunt elemente care ajută la implementarea și menținerea unei guvernante eficiente.

A treia este abordarea bazată pe riscuri. Acest model urmărește identificarea și reducerea problemelor legate de date. Prin evaluarea vulnerabilităților și introducerea unor măsuri preventive, organizațiile pot proteja datele și pot respecta mai ușor reglementările.

Îmbinând aceste trei abordări, organizațiile pot construi un sistem de guvernanță a datelor solid și totuși flexibil, care să le ajute să folosească datele în mod eficient, să reducă riscurile și să rămână conforme cu standardele legale și etice.

Alegerea și aplicarea unui model potrivit de guvernanță a datelor este de dorit pentru orice organizație care vrea să-și gestioneze informațiile eficient și să evite capcanele date de inconsistență și fragmentare. Un astfel de cadru nu doar că aduce coerență și acces mai ușor la date, ci și ajută la desființarea silozurilor informaționale – acele zone moarte unde datele zac nefolosite și inaccesibile.

O guvernanță solidă în IA presupune măsuri concrete pentru a preveni derapajele tehnologice. De la filtre împotriva bias-ului, la mecanisme clare de trasabilitate și intervenție, toate acestea contribuie la o utilizare mai sigură și mai responsabilă a IA³. Iar pe termen lung, ele sunt cheia pentru a construi încredere – atât din partea utilizatorilor, cât și a partenerilor și autorităților. Prin urmare, investiția în guvernanța IA nu reprezintă doar o obligație etică și legală, dar și o oportunitate de a stimula responsabil inovația și progresul.

Principii de bază ale guvernantei IA

Guvernanța Inteligenței Artificiale se bazează pe câteva principii fundamentale, menite să asigure o implementare responsabilă și sigură a acestei tehnologii⁴. Dintre acestea menționăm:

- Principii etice care prevăd respectarea drepturilor fundamentale ale omului și integrarea unor criterii etice clare în toate aplicațiile IA;

³ Modulos (2025), *A Guide to AI Governance*, Disponibil la: <https://www.modulos.ai/guide-to-ai-governance/> [Accesat: 19 Aug. 2025].

⁴ Snowflake (2024), *AI Governance, Threat Intelligence and Anomaly Detection*, Disponibil la: <https://www.snowflake.com/content/snowflake-site/global/en/fundamentals/ai-governance-threat-intelligence-and-ml-anomaly-detection> [Accesat: 19 Aug. 2025].

- Asigurarea transparenței modului de funcționare a sistemelor, astfel încât utilizatorii și părțile interesate să poată înțelege și evalua tehnologia;
- Asumarea responsabilității de către dezvoltatori și implementatori pentru eventualele efecte negative produse de sistemele IA;
- Promovarea corectitudinii și prevenirea discriminării prin reducerea bias-ului în procesele de dezvoltare și utilizare;
- Managementul riscurilor, cu măsuri concrete pentru a limita posibilele consecințe nedorite;
- Auditabilitatea sistemelor IA și mecanisme de trasabilitate a raționamentului deciziilor generate de acestea;
- Menținerea unui nivel de supervizare umană care să garanteze controlul și utilizarea etică a tehnologiilor.

Guvernanța IA la nivel național, regional și internațional

Guvernanța IA se desfășoară pe mai multe niveluri: național, regional și internațional, fiecare având propriile domenii de aplicare, obiective, provocări și oportunități. Diferențele dintre aceste niveluri se reflectă în politici publice, legislație, activități de cercetare și finanțare, dar și în elaborarea de standarde și mecanisme de conformitate.

La nivel național, guvernele dezvoltă strategii adaptate la contextul socio-economic, la nivelul de pregătire tehnologică și la specificul reglementărilor interne. Din cauza ritmului accelerat de integrare a IA în diverse sectoare, apar probleme sensibile legate de etică, securitate și impact economic. Legislația urmărește să găsească un echilibru între stimularea inovației și asigurarea siguranței, responsabilității și corectitudinii.

În funcție de priorități, de la creștere economică la sănătate publică sau securitate, guvernele direcționează fonduri pentru cercetare și dezvoltare, iar organismele naționale de standardizare definesc și aplică reguli pentru utilizarea responsabilă a tehnologiilor IA.

Guvernanța IA la nivel național

Elaborarea strategiilor de guvernanță pentru Inteligența Artificială presupune integrarea mai multor elemente precum principii etice, cadre de reglementare clare, investiții în cercetare-dezvoltare, dezvoltarea unei forțe de muncă bine pregătite, stabilirea de standarde și cooperare internațională, precum și cultivarea încrederii publice în sistemele IA.

Principiile etice pentru IA vin în sprijinul transparenței (procesele de luare a deciziilor sunt explicabile), corectitudinii (prevenirea discriminării în algoritmi)

IA când afectează grupurile marginalizate), responsabilității (responsabilizarea dezvoltatorilor și utilizatorilor pentru rezultatele IA, cu mecanisme de remediere), siguranței și securității (atenuarea riscurilor cum ar fi utilizarea necorespunzătoare, amenințările de securitate cibernetică și consecințele neintenționate), drepturilor omului (asigurarea că sistemele IA respectă drepturile individuale, inclusiv viața privată, libertatea de exprimare). Cadrele de reglementare abordează protecția datelor și confidențialitatea, siguranța și certificarea IA, răspunderea și responsabilitatea, reglementările antidiscriminare (stabilirea standardelor de testare a algoritmilor IA pentru minimizarea rezultatelor discriminatorii, în special în domenii precum finanțe sau justiție).

Investițiile în activitățile de cercetare-dezvoltare în IA sunt necesare pentru a păstra spiritul competitiv la nivel global. Acestea includ finanțările pentru inovare în IA (sub formă de granturi, stimulente și resurse pentru instituțiile academice, start-up-uri și companii pentru dezvoltarea de tehnologii IA de ultimă oră), parteneriatele public-privat, infrastructurile pentru IA (precum AI Factories și AI GigaFactories).

Pregătirea forței de muncă înalt calificate este parte integrantă în strategiile naționale de IA, fiind urmărite aspectele legate de educația STEAM (îmbunătățirea educației în știință, tehnologie, artă, inginerie și matematică), alfabetizare în IA pentru publicul larg, programe de perfecționare și recalificare. Standardele, cooperarea internațională și încrederea publică în sistemele IA nu pot fi separate, de aceea sunt necesare politici incluzive, cu implicarea tuturor actorilor relevanți: cetățeni, industrie, mediul academic și organizații civice. Totodată, utilizarea IA de către guverne, mai ales în domenii sensibile precum sănătate, securitate sau justiție, este important să fie transparentă și deschisă controlului public. În paralel, campaniile de informare au rolul de a familiariza cetățenii cu beneficiile și riscurile IA și de a le clarifica drepturile atunci când aceste tehnologii influențează direct deciziile care îi privesc.

Exemple de strategii de guvernanță IA la nivel național:

Statele Unite. Au adoptat o abordare orientată pe piață, încurajând inovarea în inteligență artificială, bazându-se pe reglementările specifice fiecărui sector. Discuțiile recente s-au concentrat pe crearea unor reglementări federale privind IA pentru a aborda probleme precum discriminarea, responsabilitatea și siguranța. Actul Național de Inițiativă IA și Declarația drepturilor IA conturează obiectivele strategice și principiile etice pentru dezvoltarea IA;

China. A făcut din IA o prioritate națională, integrând-o în strategia sa industrială și investind masiv în infrastructură și în cercetare. Recent, se concentrează și pe reglementarea utilizării etice a inteligenței artificiale, în special în domenii precum recunoașterea facială și luarea deciziilor algoritmice, deși modelul său de guvernanță este mai mult de tip top-down și se aliniază cu prioritățile mai răspândite

de supraveghere și control ale guvernului. Planul de dezvoltare a IA Noua Generație, cu accent pe controlul statului, țintește în a transforma China într-un lider global în inteligență artificială până la finele acestui deceniu;

Marea Britanie. Strategia IA a Marii Britanii se concentrează pe inovare, cadre de reglementare și colaborări internaționale, având ca scop poziționarea Regatului Unit ca lider global în IA;

Canada. A fost una dintre primele țări care a adoptat o strategie națională de IA. Se concentrează pe sprijinirea cercetării IA și pe asigurarea dezvoltării IA responsabile. Strategia pancanadiană de Inteligență Artificială pune accent pe colaborarea dintre cercetătorii IA, utilizarea etică a IA și construirea încrederii publice.

Guvernanța IA la nivel internațional

La nivel regional, guvernanța IA se concentrează în principal pe trei direcții: armonizarea politicilor, cercetarea colaborativă și orientările etice. Organismele regionale urmăresc să alinieze politicile și reglementările statelor membre pentru a evita fragmentarea și pentru a asigura interoperabilitatea. Ele facilitează inițiative comune de cercetare și dezvoltare, punând în comun resurse și expertiză. Totodată, cadrele regionale pun accent pe valori și principii etice împărtășite, adaptate contextelor culturale și politice ale fiecărei regiuni.

Uniunea Europeană este un exemplu proeminent. Prin AI Act, UE își propune să reglementeze sistemele IA în funcție de nivelul de risc. Regulamentul stabilește cerințe stricte pentru aplicațiile cu risc ridicat, precum recunoașterea facială sau utilizările medicale, și interzice anumite practici, cum ar fi supravegherea în masă. În paralel, Regulamentul General privind Protecția Datelor (GDPR) rămâne un element de bază în guvernanța datelor care alimentează aceste sisteme.

Un alt exemplu este Asociația Națiunilor din Asia de Sud-Est (ASEAN), care dezvoltă un cadru regional de IA pentru a promova inovarea în IA, abordând în același timp provocările etice și de reglementare în mod colectiv.

În secolul XXI, Inteligența Artificială a devenit un nou teatru al interacțiunilor dintre statele-națiune, modelat de ambiții de supremație și viziuni divergente asupra guvernării sale, în care competiția pentru dominanță între marile puteri, precum Statele Unite, China și Uniunea Europeană, este o realitate definitorie a peisajului tehnologic actual. Această întrecere nu este doar o chestiune de prestigiu tehnologic, ci are profunde implicații economice, militare și de influență la nivel mondial.

Națiunea care va reuși să stăpânească și să implementeze cel mai eficient IA va beneficia de un avantaj economic considerabil, prin optimizarea industriilor, crearea de noi piețe și creșterea productivității. Mai mult, capacitățile IA sunt din ce în ce mai integrate în strategiile de apărare și securitate, alimentând o cursă pentru dezvoltarea de sisteme autonome și instrumente de intelligence superioare.

Această rivalitate acerbă generează în mod firesc o reticență profundă față de cooperarea deschisă. Fiecare percepe distribuirea liberă a tehnologiilor avansate, a seturilor masive de date (pentru antrenarea algoritmilor) sau a cadrelor de dezvoltare ca pe o potențială cedare a avantajului competitiv.

Teama că inovațiile proprii ar putea fi preluate și utilizate de competitori pentru a le submina poziția, duce la o politică de protejare strictă a proprietății intelectuale și la investiții masive în cercetare și dezvoltare „in-house” sau în ecosisteme naționale închise. Acest climat de neîncredere poate duce la duplicarea eforturilor la nivel global și la încetinirea progresului în domenii unde colaborarea ar fi benefică, cum ar fi cercetarea fundamentală sau abordarea provocărilor globale cu ajutorul IA.

Pe măsură ce IA pătrunde în tot mai multe aspecte ale societății, nevoia de reglementare devine stringentă. Totuși, statele abordează această provocare din perspective fundamentale diferite. Uniunea Europeană, de exemplu, a adoptat o poziție proactivă și axată pe valori, prin propunerea AI Act. Aceasta urmărește respectarea unor standarde stricte, în special pentru aplicațiile considerate cu risc ridicat, cu scopul de a proteja drepturile fundamentale, siguranța cetățenilor și de a consolida încrederea acestora în noua tehnologie. Abordarea UE este una bazată pe risc, încercând să moduleze cerințele în funcție de impactul potențial al sistemelor IA.

În contrast, alte națiuni, punând un accent mai mare pe viteza inovației și pe beneficiile economice imediate, optează pentru cadre de reglementare mai flexibile sau chiar pentru o abordare de tip „așteaptă și vezi”. Aceste state se tem că o reglementare prea strictă și prematură ar putea înăbuși creativitatea și ar putea plasa companiile autohtone într-un dezavantaj competitiv pe piața globală.

Această divergență filozofică – între prudența bazată pe valori și agilitatea orientată spre inovație – creează un peisaj fragmentat din punct de vedere al reglementărilor. Armonizarea standardelor internaționale devine astfel extrem de dificilă, fiecare regiune dezvoltându-și propriile norme și cerințe.

Pentru companiile care operează la nivel global, acest mozaic de reguli înseamnă costuri de conformitate mai mari și incertitudine juridică, putând frâna adopția pe scară largă a unor soluții IA și creând provocări în ceea ce privește fluxurile internaționale de date și servicii digitale.

Astfel, în peisajul complex al guvernării globale a inteligenței artificiale, diverse organizații și cadre multilaterale joacă roluri distincte, reflectând simultan dorința de cooperare și precauție pentru protecția inovației.

Națiunile Unite și căutarea unui consens global pentru etica IA

Organizația Națiunilor Unite (ONU), prin vocația sa universală, reprezintă un for esențial în eforturile de a stabili linii directoare etice globale pentru inteligența artificială.

Agenții specializate precum UNESCO (Organizația Națiunilor Unite pentru Educație, Știință și Cultură) au fost deosebit de active, elaborând recomandări privind etica IA care să ghideze dezvoltarea și implementarea acestei tehnologii într-un mod care respectă drepturile omului, promovează pacea și dezvoltarea durabilă. Aceste eforturi urmăresc să creeze un cadru normativ internațional care să prevină abuzurile și să asigure că beneficiile IA sunt partajate echitabil.

Cu toate acestea, drumul către un consens unanim în cadrul ONU este anevoios. Cele 193 de state membre au adesea interese naționale, priorități economice, viziuni culturale și niveluri de dezvoltare tehnologică extrem de variate.

Obținerea unui acord asupra unor standarde etice obligatorii și universal aplicabile se lovește de aceste divergențe, transformând adesea inițiativele în declarații de principii și recomandări, mai degrabă decât în tratate cu forță juridică. Provocarea majoră rămâne transpunerea acestor idealuri înalte în practici concrete și verificabile la nivel național și internațional.

ITU - International Telecommunication Union

ITU este o agenție a Națiunilor Unite dedicată tehnologiilor digitale⁵, dezvoltării de standarde tehnice și conectării la nivel internațional în rețelele de comunicații, în a cărei componență intră 193 state membre și peste 1000 de organizații regionale și internaționale, universități și companii.

Obiectivele strategice ale statelor membre se referă la conectivitate universală și transformare digitală durabilă pentru populația țărilor în curs de dezvoltare care nu beneficiază încă de conexiune la Internet.

Inițiatiile demarate de ITU joacă un rol important în conturarea Metaversului⁶:

Inițiativa Globală privind Lumile Virtuale - Descoperirea CitiVerse este o inițiativă lansată de ITU, Digital Dubai și UNICC (United Nations International Computing Centre - Centrul Internațional de Calcul al Națiunilor Unite) în iunie 2024, care își propune să exploreze și să valorifice potențialul lumilor virtuale și al conceptului CitiVerse. Această inițiativă servește ca o platformă globală privind dezvoltarea urbană, unde pot fi imaginate lumi virtuale deschise, interoperabile, care îmbunătățesc lumile fizice și care pot fi utilizate în siguranță și cu încredere de către oameni, companii și serviciile publice.

Conceptul CitiVerse reprezintă o cale de dezvoltare a cadrelor normative care abordează principii, facilitatori și guvernanță pentru aplicarea soluțiilor Metavers în orașe. CitiVerse oferă un mediu și controlat pentru testarea și experimentarea diferitelor scenarii Metavers pentru orașele din întreaga lume. Astfel că pot fi realizate

⁵ ITU (2025a), *About ITU*, Disponibil la: <https://www.itu.int:443/en/about/Pages/default.aspx> [Accesat: 19 Aug. 2025].

⁶ ITU (2025b), *AI-powered virtual worlds and Metaverse*, Disponibil la: <https://www.itu.int/metaverse/> [Accesat: 19 Aug. 2025].

activități de tip instruire și găzduire de evenimente pentru diseminarea cunoștințelor, creșterea gradului de conștientizare și împărtășirea celor mai bune practici ori soluții la nivel de orașe.

Înființarea grupului focus ITU Focus Group pentru Metavers (FG-MV) s-a realizat cu scopul de a sprijini activitățile de pre-standardizare pentru Metavers⁷. Acestea se referă la analiza cerințelor tehnice ale Metavers pentru identificarea de terminologii de lucru și definiții, concepte, viziune, cazuri de utilizare, cerințe și framework-uri tehnice (cum ar fi identificarea tehnologiilor fundamentale), aspecte legate de securitatea și protecția informațiilor cu caracter personal, aspecte legate de interoperabilitate, determinarea infrastructurii de rețea și conectivitate.

Grupul a funcționat pe o perioadă de un an și jumătate, iar activitățile sale au constat în forumuri și sesiuni speciale, având ca rezultat aprobarea a 52 de Rapoarte Tehnice și Specificații Tehnice⁸. Grupul a facilitat dialogul în vederea identificării părților interesate pentru potențiale colaborări și identificarea cazurilor de utilizare importante cu ajutorul forumurilor, sesiunilor speciale și webinarilor. Acestea au explorat în profunzime elementele cheie care definesc Metaversul și rolul gemenilor digitali în modelarea evoluției Metavers. Au fost analizate cerințele și studiile de caz pentru Metavers pe baza gemenilor digitali, care să permită integrarea celor două lumi: fizică și virtuală. A fost analizat modelul de referință pentru Metavers bazat pe un geamăn digital care permite integrarea lumilor virtuale și fizice. Modelul de referință servește ca un framework pentru integrarea fără probleme între lumile virtuale și fizice.

Organizația pentru Cooperare și Dezvoltare Economică (OCDE)

OCDE este dedicată elaborării de politici inovatoare pentru îmbunătățirea vieții oamenilor. Cu peste șase decenii de experiență, din 1961, OCDE se concentrează pe promovarea prosperității, oportunității, egalității și bunăstării prin dezvoltarea de politici bazate pe date și analize aprofundate⁹.

Structura OCDE constă în trei părți principale:

Consiliul. Consiliul este corpul de decizie al OCDE, fiind compus dintr-un reprezentant din fiecare țară membră și din Uniunea Europeană. Președinția Consiliului este asigurată de Secretarul General, care oferă direcții strategice pentru organizație și pentru activitățile sale. Întâlnirile anuale ale Consiliului Ministerial, prezidate de unul sau mai mulți membri, aduc împreună guvernele pentru a discuta cele mai importante provocări de politică globală și pentru a stabili prioritățile OCDE pentru anul următor.

⁷ ITU (2025c), *FG-MV Outcomes – Metaverse*, Disponibil la: https://www.itu.int/metavers_e/fg-mv-outcomes/ [Accesat: 19 Aug. 2025].

⁸ Ibid.

⁹ OECD (2025a), *The Organisation for Economic Co-operation and Development*, Disponibil la: <https://www.oecd.org/en.html> [Accesat: 19 Aug. 2025].

Comitetele de fond. Peste 300 de comitete de fond propun soluții, dezvoltă standarde, evaluează datele și succesul politicilor și revizuiesc acțiunile politice. Concentrate pe provocări politice majore, cum ar fi schimbările climatice și economia comerțului și a impozitelor, aceste comitete includ specialiști din diverse țări, domeniul academic, sectorul de afaceri și grupuri ale societății civile, care joacă un rol vital în crearea de standarde globale pentru reglementările publice.

Secretariatul. Compus din peste 3500 de angajați din diverse direcții și condus de Secretarul General, acesta coordonează activitățile OCDE din sediul de la Paris. Economisti, avocați, oameni de știință, analiști politici, experți în tehnologia informației, statisticieni și alți specialiști lucrează împreună cu experți ai guvernului pentru a oferi perspective și expertiză în sprijinul elaborării de politici bazate pe dovezi, în strânsă coordonare cu membrii organizației¹⁰.

Misiunea principală a OCDE este de a ghida crearea de standarde internaționale și de a asista țările în construirea unor societăți mai puternice și mai echitabile, pentru a asigura un viitor mai bun pentru toată lumea.

Colaborând cu factori de decizie politică, părți interesate și cetățeni, OCDE creează standarde internaționale bazate pe statistici și abordează aspecte sociale, economice și de mediu. De la îmbunătățirea performanței economice și educației până la combaterea schimbărilor climatice și evaziunii fiscale internaționale, OCDE acționează ca un forum pentru date, analize și cele mai bune practici în reglementările publice.

În colaborare cu peste 100 de țări, OCDE este atât un forum, cât și un centru de cunoștințe care dezvoltă reglementări mai eficiente prin standardele sale, statistici și analize de încredere, platforme pentru dialoguri și suport pentru reforme politice.

OCDE furnizează cunoștințe membrilor și partenerilor săi, ajutându-i să ia decizii mai bine fundamentate în procesul de elaborare a noilor reglementări. Analizele realizate de OCDE sunt concretizate în peste 500 de rapoarte majore și evaluări ale țărilor, precum și de peste 5 miliarde de puncte de date publicate anual. Organizația produce, de asemenea, sute de note de informare politică, articole și conținut digital referitor la problemele legate de reglementare. Ca una dintre cele mai mari surse de statistici comparabile, date și analize de reglementări din lume, OCDE contribuie la informarea în cadrul dezbaterilor în parlamente, media și cercetare.

OCDE analizează evenimente economice, evenimente privitoare la mediu și schimbări sociale, oferind analize personalizate la cererea guvernelor. Organizația are ca rol ghidarea și informarea dezbaterilor internaționale de politică în forumuri globale, contribuind la toate direcțiile de lucru ale G20 cu date, rapoarte analitice, recomandări de reglementări și standarde. De asemenea, este implicată în G7,

¹⁰ Ibid.

parteneriatul Deauville, Asia-Pacific Economic Cooperation (APEC), Comisia Uniunii Africane și multe altele¹¹.

OCDE oferă leadership în domenii cheie, la cererea guvernelor, cum ar fi evitarea impozitelor, lupta împotriva corupției și transformarea digitală, probleme care necesită soluții transfrontaliere. Prin promovarea unei cooperări internaționale eficiente, OCDE contribuie la îmbunătățirea rezultatelor economice și a vieții de zi cu zi.

Principiile OCDE de promovare a unei Inteligențe Artificiale de încredere

Organizația pentru Cooperare și Dezvoltare Economică (OCDE), un grup ce reunește preponderent economii dezvoltate, a jucat un rol pionierat în articularea unor principii pentru o inteligență artificială responsabilă și centrată pe om.

Adoptate în 2019, Principiile IA ale OCDE – primele de acest fel la nivel interguvernamental – promovează transparența, robustețea, securitatea, responsabilitatea și protecția drepturilor omului și a valorilor democratice în proiectarea și utilizarea sistemelor IA¹².

Acestea sunt concepute pentru a ghida guvernele și industria în efortul de a stimula inovația, asigurând în același timp că IA este demnă de încredere. Numai că acestea au un caracter non-obligatoriu. Deși influente și adoptate ca referință de multe țări membre și chiar non-membre în elaborarea strategiilor naționale, ele nu dispun de mecanisme de constrângere. Aderarea și implementarea efectivă depind de voința politică a fiecărui stat. Mai mult, sfera de acoperire a OCDE, deși extinsă, nu este universală, ceea ce înseamnă că aceste principii nu sunt automat îmbrățișate la nivel global, lăsând loc pentru abordări divergente în alte părți ale lumii.

România a făcut pași importanți spre aderarea la OCDE. După ce a devenit candidată oficială în 2022, țara a început să urmeze foaia de parcurs stabilită pentru integrare. Din cele 25 de comitete care verifică dacă standardele organizației sunt respectate, mai mult de jumătate și-au încheiat deja analiza cu rezultate pozitive. Acest lucru arată un progres solid în mai multe domenii – de la guvernanța corporativă, până la politicile fiscale și sociale. Totuși, drumul nu e complet lipsit de provocări. România mai are de lucrat la reforma pensiilor private, la modul în care funcționează companiile de stat, dar și la îmbunătățirea colectării taxelor. În plus, agricultura, mediul și energia trebuie adaptate la regulile și recomandările OCDE. La fel de importanți sunt și pașii în direcția independenței instituțiilor publice și a consolidării justiției. Dacă aceste reforme sunt duse la capăt, România își poate atinge obiectivul ambițios de a adera la OCDE în primăvara lui 2026.

¹¹ OECD, 2025a.

¹² OECD (2025b), *AI Principles Overview*, Disponibil la: <https://oecd.ai/en/principles> [Ac-cesat: 19 Aug. 2025].

Considerăm că guvernanța Inteligenței Artificiale trebuie să fie construită pe principii clare, precum etică, transparență, responsabilitate, corectitudine, gestionarea riscurilor și supraveghere umană. Dar totul începe cu guvernanța datelor, fără date curate și sigure, IA nu poate funcționa în mod responsabil. Guvernanța datelor se sprijină pe câteva aspecte fundamentale, cum ar fi protecția vieții private, calitatea și corectitudinea informațiilor, trasabilitate și auditabilitate, asumarea responsabilității și reguli clare pentru circulația datelor între state.

Observăm că, la nivel global, abordările diferă. Unele state, precum SUA sau China, pun accent pe interese proprii ca securitate sau economie, în timp ce Europa a ales să meargă pe un drum mai echilibrat, precum GDPR și AI Act. Organizațiile internaționale (cum ar fi ONU, ITU, OCDE) încearcă să creeze principii comune, dar acestea nu sunt întotdeauna obligatorii, ceea ce lasă loc fragmentării și inegalităților. Cele mai mari provocări vin din fragmentarea legislativă, tensiunea dintre suveranitatea digitală și cooperarea internațională, riscurile de securitate și, nu în ultimul rând, din încheitățile care pot lăsa statele mai puțin pregătite în urmă.

Uniunea Europeană a elaborat un cadru legislativ complex și coerent. Astfel că, Data Governance Act (DGA) are scopul de a aduce transparență și de a crea o piață unică a datelor, Data Act are scopul de a clarifica accesul și utilizarea acestor date, în timp ce primul cadru european dedicat Inteligenței Artificiale - AI Act, sare rolul de a clasifica riscurile. Nu în ultimul rând, GDPR rămâne fundamentul protecției datelor personale și oferă cadrul necesar pentru a face față noilor provocări aduse de Metavers și tehnologiile imersive. Acest pachet normativ plasează Europa în avangardă, însă regulile trebuie adaptate permanent la ritmul tehnologiei. Guvernanța datelor reprezintă esența guvernanței IA și este elementul-cheie care ne permite să împăcăm inovația tehnologică cu protecția drepturilor fundamentale.

Forumurile G7/G20: dialog la nivel înalt despre guvernanța IA

Grupurile G7 (cele mai industrializate șapte democrații) și G20 (cele mai mari 20 de economii ale lumii) au devenit platforme importante pentru discuții la nivel înalt privind guvernanța inteligenței artificiale.

În cadrul summiturilor lor anuale și al reuniunilor ministeriale, liderii acestor națiuni abordează provocările și oportunitățile generate de IA, încercând să identifice puncte de convergență și să stabilească obiective comune. Discuțiile acoperă o gamă largă de subiecte, de la stimularea inovației responsabile și dezvoltarea talentelor, la promovarea unei IA etice și sigure, combaterea dezinformării generate de IA și asigurarea unei concurențe loiale pe piața digitală.

Deși aceste forumuri nu au autoritatea de a crea legi internaționale, ele joacă un rol în stabilirea agendei globale și în coordonarea politicilor între marile puteri economice. Angajamentele asumate în declarațiile G7 și G20 pot impulsiona acțiuni la nivel național și pot facilita cooperarea în domenii specifice, cum ar fi cercetarea

sau standardizarea, contribuind la conturarea unui cadru internațional mai coerent pentru IA, chiar și în absența unor tratate formale.

Implicarea sectorului privat și a societății civile

În epicentrul dezvoltării IA se află giganții tehnologici precum Google, Microsoft sau Alibaba. Aceștia nu sunt doar furnizori de inovație, ei influențează considerabil politicile și standardele globale. Expertiza și capacitatea lor tehnică greu de egalat, capacitatea de lobby și anvergura operațiunilor la nivel mondial le conferă un rol determinant, dar și controversat, în modelarea guvernării IA, adesea forțând granițele dintre interesul public și cel corporativ. Ca o contrapondere necesară, societatea civilă militează activ pentru o dezvoltare etică și responsabilă a IA. Aceasta aduce în prim-plan preocupări critice legate de potențialul discriminatoriu al algoritmilor, impactul IA asupra locurilor de muncă, erodarea confidențialității și necesitatea de a încorpora drepturile omului și principiul echității în arhitectura sistemelor de guvernare globală.

Pe un palier tehnic, dar cu implicații etice profunde, organisme internaționale de standardizare precum IEEE (Institute of Electrical and Electronics Engineers) și ISO (International Organization for Standardization) depun eforturi considerabile pentru a elabora standarde tehnice globale pentru IA. Inițiative precum „IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems” urmăresc să uniformizeze practicile etice în dezvoltarea și implementarea IA la nivel transfrontalier¹³. Cu toate acestea, provocarea majoră constă în asigurarea adoptării și implementării uniforme a acestor standarde, în contextul unor interese și capacități naționale divergente.

Prin armonizarea eforturilor la nivel național, regional și internațional, guvernarea inteligenței artificiale poate fi orientată într-o direcție care maximizează beneficiile, reduce riscurile și promovează o dezvoltare echilibrată și incluzivă. O astfel de colaborare oferă cadrul necesar pentru ca IA să evolueze în mod responsabil, în slujba societății. Totuși, calea către o astfel de armonie este presărată cu obstacole semnificative

Principalele provocări în calea guvernării globale a IA

Complexitatea sarcinii de a governa IA la nivel global este amplificată de o serie de provocări interconectate.

În primul rând, valorile și interesele naționale divergente duc la o fragmentare a reglementărilor – Europa prioritizează confidențialitatea și etica (GDPR, Legea IA), în timp ce China accentuează rolul IA în securitatea statului și creșterea economică. Această viziune a IA ca activ strategic național complică eforturile de cooperare în favoarea siguranței globale.

¹³ IEEE SA (2024), *The IEEE Global Initiative 2.0 on Ethics of Autonomous and Intelligent Systems*, Disponibil la: <https://standards.ieee.org/industry-connections/activities/ieee-global-initiative/> [Accesat: 19 Aug. 2025].

În al doilea rând, se resimte acut lipsa unor mecanisme globale eficiente de coordonare și aplicare. Majoritatea cadrelor internaționale, precum Principiile OCDE, sunt non-obligatorii, iar reticența statelor de a ceda suveranitate națională în favoarea unor standarde globale obligatorii limitează drastic eficacitatea acestora.

Complexitatea tehnologică și etică intrinsecă IA reprezintă un alt nod gordian. Implicațiile sociale și etice asupra ocupării forței de muncă sau a drepturilor omului variază cultural, iar evoluția fulgerătoare a tehnologiei face ca orice cadru de guvernare să riște o perimare rapidă.

Guvernanța datelor și preocupările privind confidențialitatea sunt, de asemenea, centrale. Reguli conflictuale privind fluxurile transfrontaliere și localizarea datelor (ex. Legea Securității Cibernetice din China vs. GDPR) și utilizarea controversată a IA pentru supraveghere de stat tensionează eforturile de standardizare.

Problematika discriminării, corectitudinii și responsabilității este stringentă, algoritmi putând perpetua prejudecăți, iar stabilirea răspunderii pentru erorile sistemelor autonome fiind o provocare juridică globală.

Nu în ultimul rând, riscurile de securitate și potențiala militarizare a IA, inclusiv utilizarea în atacuri cibernetice sau dezvoltarea armelor autonome letale, generează temeri privind o nouă cursă a înarmărilor, subminând eforturile de control.

În final, asigurarea incluziunii și a unei reprezentări echitabile în procesul de guvernare este vitală. Dominanța țărilor dezvoltate în conturarea acestor cadre riscă marginalizarea nevoilor țărilor în curs de dezvoltare, adâncind decalajul digital și inechitățile globale.

Reglementări referitoare la Inteligența Artificială și guvernanța datelor

Într-o eră digitală aflată într-o dezvoltare continuă, reglementările privind Inteligența Artificială (IA) și guvernanța datelor contribuie la menținerea unui echilibru optim între inovare, securitate și protecția drepturilor fundamentale. Expansiunea volumului de date generate de tehnologiile emergente și utilizarea tot mai extinsă a IA subliniază necesitatea instituirii unor cadre legislative clare și eficiente, atât la nivel național, cât și internațional.

Uniunea Europeană a adoptat un set de reglementări menite să asigure atât protecția și accesibilitatea datelor, cât și utilizarea responsabilă a Inteligenței Artificiale. Printre cele mai semnificative acte legislative se numără: (a) Data Governance Act (DGA), care instituie un cadru unitar pentru partajarea și reutilizarea datelor la nivelul UE, (b) EU Data Act, ce reglementează accesul și utilizarea datelor generate în spațiul economic european, și (c) Artificial Intelligence Act (AI Act), primul cadru juridic cu acoperire largă, destinat reglementării utilizării sistemelor

de inteligență artificială. În acest context, Regulamentul General privind Protecția Datelor (GDPR), rămâne un element de bază completând aceste inițiative prin asigurarea confidențialității și protecției datelor cu caracter personal.

Impactul implementării acestor reglementări poate determina transformări în ceea ce privește relațiile dintre factorii de decizie, mediul de afaceri și societatea civilă, prin stimularea inovației, consolidarea competitivității și creșterea încrederii în soluțiile digitale, în domenii multiple – de la sănătate și educație, până la servicii financiare și administrație publică. În paralel, progresele recente în domeniul Metaversului și al tehnologiilor de realitate imersivă generează noi provocări juridice și etice, impunând adaptarea cadrului de reglementare existent.

În acest context, cooperarea între organizații internaționale precum Uniunea Internațională a Telecomunicațiilor (ITU, International Telecommunication Union) și Organizația pentru Cooperare și Dezvoltare Economică (OCDE, Organisation for Economic Co-operation and Development) sprijină elaborarea de standarde comune și promovarea bunelor practici în domeniul guvernării datelor și al Inteligenței Artificiale, dincolo de limitele sistemelor juridice naționale. Din această perspectivă, analiza contribuției reglementărilor la consolidarea guvernării datelor în spațiul european se poate extinde către noile frontiere tehnologice, precum Metavers.

EU Data Governance Act (DGA)

Creșterea continuă a volumului de date generate de dispozitivele și serviciile digitale impune un cadru eficient de gestionare și partajare la nivelul Uniunii Europene. În acest scop, Actul privind Guvernanța Datelor (DGA), adoptat în 2020 prin Regulamentul UE nr. 2022/868, urmărește crearea unei piețe unice a datelor și facilitarea accesului internațional, consolidând rolul UE ca lider al economiei globale bazate pe date¹⁴.

Parte centrală a strategiei digitale europene, DGA este complementat de Data Act, care stabilește drepturi clare privind accesul și controlul asupra anumitor tipuri de date. În timp ce DGA reglementează guvernarea și încrederea în partajarea datelor, Data Act definește cine le poate utiliza. Aliniat Strategiei Europene pentru Date din 2020, DGA sprijină dezvoltarea spațiilor comune de date și introduce măsuri orizontale aplicabile tuturor sectoarelor, lăsând loc regulilor specifice domeniilor particulare. Conform Articolului 1, acesta reglementează reutilizarea datelor publice, monitorizarea serviciilor de schimb și promovarea altruismului în utilizarea datelor (Baloup et al., 2021).

¹⁴ Cyber Risk GmbH (2024), *Data Governance Act (DGA) | Updates, Compliance, Training*, Disponibil la: <https://www.european-data-governance-act.com/> [Accesat: 19 Aug. 2025].

Strategia digitală a Comisiei Europene include, alături de Actul privind Guvernanța Datelor (DGA), două inițiative legislative majore: Actul privind Piața Digitală (DMA) și Actul privind Serviciile Digitale (DSA). DGA introduce o nouă definiție a datelor — „orice reprezentare digitală a actelor, faptelor sau informațiilor, inclusiv înregistrări sonore, vizuale sau audiovizuale” — diferită de standardul ISO, care pune accent pe reprezentarea formalizată, interpretabilă și procesabilă a informațiilor, precum datele meteorologice sau de cercetare (Baloup et al., 2021).

Pe baza acestei definiții, DGA se sprijină pe trei piloni principali: (1) regim obligatoriu de notificare pentru anumite servicii de partajare a datelor; (2) mecanism voluntar de înregistrare a serviciilor dedicate altruismului în domeniul datelor, pentru creșterea încrederii în proces și în intermediari; (3) cadru legal pentru reutilizarea datelor din sectorul public protejate de drepturi ale terților, complementar Directivei privind Datele Deschise (Baloup et al., 2021).

Acești piloni se leagă strâns de două concepte centrale. Primul este cel al intermediarilor de date — entități independente care facilitează schimbul de date între deținători și utilizatori, fără a le exploata comercial. Prin neutralitate și transparență, aceștia pot stimula apariția unor ecosisteme de date echitabile, ferite de influența actorilor dominanți, și pot sprijini agregarea și partajarea eficientă a datelor¹⁵.

Al doilea concept este altruismul datelor, care încurajează partajarea voluntară a datelor, de către persoane sau companii, în beneficiul societății. Protejând drepturile și interesele participanților, acest principiu contribuie la crearea unui spațiu deschis și echilibrat al datelor, cu beneficii reciproce pentru toți cei implicați¹⁶.

Articolul 11 din DGA stabilește condițiile pentru furnizorii de servicii de partajare a datelor: existența unor entități juridice separate, acces echitabil și nediscriminatoriu, precum și standarde ridicate de securitate în stocarea și transmiterea datelor. Din 9 august 2023, acești furnizori și organizațiile de altruism de date recunoscute de UE utilizează sigle speciale, vizibile pe toate publicațiile, pentru a spori transparența și încrederea pe piața de date. Sigla dedicată altruismului de date include un cod QR ce direcționează către registrul public european, disponibil din 24 septembrie 2023, iar utilizarea lor este reglementată strict pentru a preveni abuzurile¹⁷. Prin consolidarea încrederii și eliminarea barierelor tehnice, DGA stimulează inovația prin crearea de spații europene comune de date — platforme strategice pentru colectarea și schimbul de date în diverse domenii — bazate pe intermediere și altruism de date¹⁸.

¹⁵ Ibid.

¹⁶ DG CONNECT (2024), *Data Governance Act explained | Shaping Europe's digital future*, Disponibil la: <https://digital-strategy.ec.europa.eu/en/policies/data-governance-act-explained> [Accesat: 18 Iul. 2024].

¹⁷ Cyber Risk GmbH (2024), *Data Governance Act (DGA) | Updates, Compliance, Training*, Disponibil la: <https://www.european-data-governance-act.com/> [Accesat: 19 Aug. 2025].

¹⁸ Ibid.

1. Spațiul comun european de date industriale (de producție). Este urmărită valorificarea datelor industriale co-generate (de exemplu, date IoT) prin drepturi clare de utilizare și partajare echitabilă, stimulând produse inteligente și protejând interesele utilizatorilor.
2. Spațiul comun european de date pentru Green Deal. Este urmărită sprijinirea obiectivelor climatice, economiei circulare, reducerii poluării, protecției biodiversității și combaterii defrișărilor.
3. Spațiul comun european de date privind transportul. Este urmărită digitalizarea și integrarea datelor din toate modurile de transport în sistemul european, inclusiv vehicule conectate.
4. Spațiul comun european de date privind sănătatea. Este urmărită reutilizarea securizată a datelor medicale pentru inovație, reglementare, îmbunătățirea îngrijirii și reducerea costurilor, cu protecția etică a datelor.
5. Spațiul european comun de date financiare. Este urmărit schimbul îmbunătățit de date financiare pentru serviciile bancare deschise, inovare și susținerea politicilor UE.
6. Spațiul comun european de date energetice. Este urmărit accesul transparent la datele de consum, partajarea obligatorie a datelor de rețea, securitatea cibernetică și sprijinul pentru decarbonizare.
7. Spațiul comun european de date agricole. Un spațiu comun de date va crea o platformă neutră de partajare a datelor agricole pentru sustenabilitate, competitivitate și reducerea sarcinilor administrative.
8. Spații comune europene de date pentru administrațiile publice. Este urmărită utilizarea și îmbunătățirea calității datelor în domenii de interes public, sporind transparența și eficiența.
9. Spațiul comun european de date privind competențele. Sunt necesare datele de calitate privind calificările și oportunitățile de învățare, cu standarde și interoperabilitate prin Europass.
10. European Open Science Cloud. Este susținut accesul și reutilizarea datelor de cercetare pentru știință, inovare și conectarea spațiilor sectoriale de date.

Implementarea spațiilor europene comune de date creează un cadru standardizat și interoperabil care facilitează reutilizarea și transferul internațional al datelor, menținând protecția conform normelor europene. Aceste spații accelerează accesul la informații valoroase, amplificând beneficiile economice și sociale ale datelor și sprijinind cercetarea, inovația și creșterea economică.

DGA, parte a strategiei europene pentru date, promovează reutilizarea datelor din sectorul public, precum cele de sănătate, prin intermediari de încredere și mecanisme sigure de partajare. Încurajând schimbul transsectorial și transfrontalier, actul urmărește crearea unui spațiu unic de date care să stimuleze economia și să reducă impactul asupra mediului¹⁹.

EU Data Act

Actul european privind datele (EU Data Act) este inițiativa Comisiei Europene de a proteja tehnologia și suveranitatea datelor, stabilind reguli clare pentru accesul și utilizarea acestora în toate sectoarele Spațiului Economic European. Complementar Regulamentului GDPR, care vizează datele personale, Data Act extinde protecția și asupra datelor non-personale²⁰.

Prin norme uniforme de distribuire, stocare și prelucrare, actul urmărește modelarea spațiului digital european și facilitarea accesului la datele generate de companii, industrii și utilizatori prin Internetul Lucrurilor. Acest acces extins poate sprijini IMM-urile, consumatorii și dezvoltarea tehnologiilor emergente, inclusiv a aplicațiilor Web 3.0 și a Metaversului. Propunerea include măsuri prin care atât persoanele fizice, cât și companiile pot accesa diferite tipuri de date pentru a dezvolta servicii inovatoare, consolidând astfel competitivitatea digitală a Uniunii Europene²¹:

- Măsuri referitoare la dreptul utilizatorilor de dispozitive conectate de a accesa datele generate și de a distribui aceste date cu părți terțe;
- Măsuri care să garanteze o negociere echitabilă a clauzelor contractuale privind partajarea datelor între IMM-uri și alte entități, cu scopul de a preveni eventualele abuzuri din partea celor aflați într-o poziție de forță în procesul de negociere;
- Modalități prin care organismele publice pot obține și utiliza datele din sectorul privat în situații de urgență și pentru asigurarea siguranței;
- Reguli care să asigure protecția utilizatorilor împotriva transferului ilegal de date atunci când își schimbă serviciul de procesare a datelor în cloud;
- Aspecte legate de aplicabilitatea Directivei privind bazele de date în contextul protecției juridice a datelor generate de dispozitivele IoT.

¹⁹ DG CONNECT (2024), *Data Governance Act explained | Shaping Europe's digital future*, Disponibil la: <https://digital-strategy.ec.europa.eu/en/policies/data-governance-act-explained> [Accesat: 18 Iul. 2024].

²⁰ Schenker J. L. (2022), *What Business Needs To Know About The EU Data Act*, Disponibil la: https://medium.com/@jennifer_45057/what-business-needs-to-know-about-the-cu-data-act-ad6d961830ad [Accesat: 19 Aug. 2025].

²¹ Ibid.

Legea Datelor 2023/2854 (EU Data Act) introduce reglementări cu impact direct asupra arhitecturii software, vizând accesibilitatea, interoperabilitatea și securitatea datelor²². În cele ce urmează, sunt prezentate principalele aspecte relevante:

- Aspecte privind portabilitatea și accesibilitatea datelor. Conform prevederilor Legii Datelor, furnizorii de servicii de procesare a datelor au obligația de a facilita transferul și schimbul acestora, inclusiv prin specificarea detaliată a metodelor, formatelor, restricțiilor și limitărilor tehnice aplicabile (Articolul 26). Acest cadru legislativ impune utilizarea unor arhitecturi software care să asigure o manipulare flexibilă a datelor și posibilitatea exportului acestora în formate variate;
- Aspecte privind cerințele de interoperabilitate. Legea evidențiază importanța interoperabilității datelor, a mecanismelor de distribuire și a serviciilor din cadrul spațiilor de date europene comune (Articolul 33). În acest context, proiectarea sistemelor software pornește de la respectarea cerințelor de interoperabilitate (precum structuri de date coerente, formate standardizate și protocoale de acces adecvate);
- Aspecte tehnice privind schimbul de date. Furnizorii de servicii de procesare a datelor au obligația de a facilita migrarea utilizatorilor către servicii similare, asigurând echivalența funcțională a serviciului de procesare a datelor de destinație (Articolul 30). În acest sens, arhitecturile software trebuie să fie concepute astfel încât să susțină aceste procese de migrare, inclusiv prin furnizarea instrumentelor adecvate și a suportului tehnic necesar;
- Aspecte privind contractele inteligente pentru distribuirea datelor. Legea stabilește cerințe pentru contractele inteligente utilizate în implementarea acordurilor de distribuire a datelor (Articolul 36). Arhitecturile software care integrează astfel de contracte au rolul de a asigura robustețea acestora, gestionarea accesului, posibilitatea rezilierii în condiții de siguranță, arhivarea datelor și conformitatea cu termenii acordurilor de distribuire a datelor;
- Aspecte privind protecția împotriva accesului ilegal. Conform legislației, furnizorii de servicii de procesare a datelor sunt obligați să implementeze măsuri de securitate menite să prevină accesul neautorizat al entităților guvernamentale internaționale sau transferul neautorizat de date fără

²² Pino De Francesco MSc (2024), *EU Data Act: how it impacts Solution and Software Architecture?*, Disponibil la: <https://medium.com/law-and-software-architecture/eu-data-act-how-it-impacts-solution-and-software-architecture-125a210d4fd8> [Accesat: 19 Aug. 2025].

caracter personal stocate în UE, dacă acestea contravin legislației europene sau naționale (Articolul 32). În acest context, arhitecturile software vor fi dezvoltate ținând cont de protecția împotriva accesului ilegal și să respecte cerințele legale aplicabile;

- Aspecte privind interoperabilitatea deschisă. Legea impune elaborarea unor specificații de interoperabilitate deschise și a unor standarde armonizate pentru serviciile de procesare a datelor (Articolul 35). Aceste cerințe pot influența dezvoltarea viitoare a software-ului, determinând necesitatea ca arhitecturile software să fie compatibile cu specificațiile și standardele stabilite.

EU Artificial Intelligence Act

Guvernanța Inteligenței Artificiale se referă la ansamblul de cadre de reglementare, politici și organisme implicate în dezvoltarea și implementarea IA, cu respectarea unor principii precum etica, securitatea și beneficiile pentru societate. Ritmul accelerat al progresului tehnologic în domeniul IA și al conștientizării impactului pe care IA îl are asupra societății, au determinat evoluția rapidă a peisajului guvernantei IA²³.

Legea Uniunii Europene privind Inteligența Artificială reglementează dezvoltarea, implementarea și utilizarea IA în spațiul european. Ea definește clar rolurile și responsabilitățile celor implicați — furnizori, utilizatori, importatori, distribuitori și producători — pe întregul lanț de aprovizionare. Adoptată de Parlamentul European la 13 martie 2024, legea urmărește: siguranța și încrederea în sistemele IA, respectarea drepturilor și valorilor fundamentale, stimularea inovației și a investițiilor și armonizarea pieței UE²⁴.

Guvernanța IA este un domeniu dinamic, influențat de politici naționale și internaționale, cadre etice, instituții de reglementare, standarde și inițiative publice și private. Exemple relevante se referă la OCDE (care promovează utilizarea inovatoare și responsabilă a IA, cu respectarea drepturilor omului) și la UE (care dezvoltă un cadru legislativ bazat pe gestionarea riscurilor și clasificarea aplicațiilor IA în funcție de risc). Statele Unite ale Americii, China, Canada, Marea Britanie au strategii proprii axate pe finanțare, cercetare și etică, iar organizații internaționale (IEEE, Parteneriatul pentru IA) și mari companii (Microsoft, IBM, Google) stabilesc principii etice pentru utilizarea responsabilă a IA.

²³ Modulos (2025), *A Guide to AI Governance*, Disponibil la: <https://www.modulos.ai/guide-to-ai-governance/> [Accesat: 19 Aug. 2025].

²⁴ NayaOne (2024), *The EU AI Act and Its Impact on Businesses*, Disponibil la: <https://meadium.com/@NayaOne/the-eu-ai-act-and-its-impact-on-businesses-f2d4eb2f66df> [Accesat: 19 Aug. 2025].

Un pilon al guvernării Inteligenței Artificiale îl constituie cadrele și ghidurile etice, elaborate atât la nivel instituțional, cât și privat. Organizații precum IEEE și Parteneriatul pentru IA au definit principii menite să asigure dezvoltarea responsabilă a IA, în acord cu valorile fundamentale ale umanității. Mari companii tehnologice – Microsoft, IBM, Google – și-au creat propriile coduri etice pentru a ghida cercetarea și inovația. Instituțiile de reglementare includ agenții specializate în supravegherea dezvoltării și aplicării IA, unele deja active, altele operate prin colaborări internaționale, cum este GPAI (Global Partnership on AI), ce sprijină cercetarea și politicile în domeniu.

Certificările și standardele – precum ISO/IEC – garantează interoperabilitatea, siguranța și fiabilitatea sistemelor IA. Programele de certificare urmăresc să asigure conformitatea cu normele tehnice și etice.

Viitorul guvernării Inteligenței Artificiale va depinde de găsirea unui echilibru între inovație și etică, pentru a valorifica potențialul tehnologiei în beneficiul societății și a limita riscurile asociate. Acest proces va fi ghidat de direcții majore: îmbunătățirea reglementărilor, armonizarea standardelor internaționale, dezvoltarea responsabilă, implicarea publicului, progresul infrastructurii și integrarea IA în procesele decizionale. Cadrele de reglementare sunt caracterizate de adaptabilitate, de răspunsul la ritmului rapid al progresului tehnologic, de evaluarea constantă a riscurilor emergente și de sprijinirea experimentării într-un mediu controlat.

Dezvoltarea IA într-un mod etic și responsabil presupune integrarea principiilor fundamentale de echitate, transparență, responsabilitate și respect al drepturilor omului, care sunt îndeplinite prin implementarea la nivel de organizații de evaluări de impact, publicarea de rapoarte de transparență și implicarea activă a părților interesate în luarea deciziilor. Participarea publicului – prin consultări, adunări cetățenești sau alte mecanisme – este importantă pentru politici incluzive și echitabile.

Progresul tehnologic se bazează pe instrumente avansate de audit și de mecanisme solide de securitate și protecție a datelor. Integrarea IA în administrația publică poate îmbunătăți procesele decizionale prin analize predictive și simulări de politici, cu condiția asigurării transparenței, supravegherii și posibilității de contestare a deciziilor automate.

La scară globală, un cadru de guvernare eficient presupune trei piloni: standarde tehnice clare, integrarea valorilor fundamentale ale Națiunilor Unite și consolidarea capacităților instituționale și tehnologice. Țări din diverse regiuni ale lumii au subliniat necesitatea unei guvernări centrate pe om și adaptate contextelor locale.

În Europa, Actul privind Inteligența Artificială, adoptat în mai 2024, stabilește reguli stricte pentru utilizarea sigură și etică a IA. Aceste reglementări se aplică tuturor din ecosistem – de la dezvoltatori și furnizori la utilizatori finali – indiferent

de originea tehnologiei. Prin acest cadru, Uniunea Europeană urmărește crearea unui mediu în care IA să fie sigură, echitabilă și aliniată cu drepturile fundamentale consacrate de Carta Drepturilor Fundamentale a Uniunii Europene²⁵.

Furnizorii / dezvoltatorii sunt cei care creează și oferă pe piață sisteme IA. Furnizorii de sisteme IA sunt companiile care dezvoltă sisteme IA în vederea introducerii lor pe piață sau a punerii în funcțiune sub propriul nume sau marcă comercială, cu plată sau gratuit. Aceștia au obligații stricte.

Utilizatorii / implementatorii implementează sistemele într-un spațiu profesionist. Utilizatorii au obligații, însă nu așa stricte ca furnizorii.

Implementatorii IA au obligația să se asigure că implementările lor respectă cadrul de reglementare IA stabilit de legea IA.

Utilizatorii finali sunt persoanele care interacționează direct cu un sistem de inteligență artificială (IA) prin utilizarea unui produs sau serviciu bazat pe această tehnologie. Spre deosebire de dezvoltatori sau implementatori, utilizatorii finali nu au obligații specifice în ceea ce privește conformitatea cu reglementările. Totuși, este esențial ca tehnologiile IA să fie implementate într-un mod sigur, etic și benefic pentru societate, respectând standardele legale și protejând drepturile și interesele utilizatorilor.

Restricții și obligații impuse de EU AI Act

Potrivit AI Act, sistemele de Inteligență Artificială sunt clasificate în patru niveluri de risc, fiecare fiind supus unor reglementări specifice în funcție de impactul său asupra societății. În plus, sistemele de Inteligență Artificială cu scop general (General Purpose AI – GPAI) beneficiază de un cadru de reglementare dedicat, adaptat complexității și versatilității acestora²⁶.

Restricții în funcție de categoriile de risc și aplicații

Risc inacceptabil. Sistemele de Inteligență Artificială care prezintă un risc inacceptabil sunt strict interzise, din cauza impactului lor critic asupra siguranței și drepturilor fundamentale ale omului. Această categorie include următoarele tipuri de sisteme:

- Sistemele care utilizează tehnici subliminale sau manipulative. Acestea sunt proiectate pentru a influența comportamentul uman și procesele de luare a deciziilor;

²⁵ Jurcys P. (2022), *Prifina Comments to the Proposed EU Data Act: What Will Data Access, Interoperability, and Data...*, Disponibil la: <https://medium.com/prifina/prifina-comment-s-to-the-proposed-eu-data-act-what-will-data-access-interoperability-and-data-5900e2bb4ed1> [Accesat: 19 Aug. 2025].

²⁶ Casalegno F. (2024), *The EU AI Act — A Complete Guide to Laws and Regulations on AI*, Disponibil la: <https://medium.com/@francesco.casalegno/the-eu-ai-act-a-complete-guide-to-laws-and-regulations-on-ai-61f630fcc1be> [Accesat: 19 Aug. 2025].

- Sistemele care exploatează vulnerabilitățile umane pentru a influența comportamentul. Aceste sisteme țintesc indivizii cu caracteristici specifice, cum ar fi vârsta, dizabilități sau alte condiții personale, pentru a induce comportamente specifice;
- Sistemele care utilizează identificarea biometrică la distanță în timp real pentru aplicarea legii în spațiile publice. Aceste tehnologii, folosite pentru aplicarea legii sau monitorizare, reprezintă o amenințare gravă la intimitate și libertatea individuală, fiind interzise în cadrul public;
- Sistemele care permit identificarea informațiilor sensibile (etnie, orientare sexuală, etc). Aceste sisteme permit recunoașterea și extragerea de date confidențiale despre persoane, cum ar fi etnia sau orientarea sexuală. Astfel de tehnologii reprezintă o încălcare gravă a intimității și drepturilor individuale;
- Sistemele bazate pe scoruri sociale în evaluarea comportamentului și personalității persoanelor. Acestea utilizează evaluări ale comportamentului și personalității pentru a determina accesul la diverse servicii. Astfel de practici pot duce la discriminare și inechități, afectând libertatea și oportunitățile indivizilor;
- Sistemele de estimare a probabilității infracțiunilor în funcție de personalitate. Aceste tehnologii își propun să prevină criminalitatea prin analiza trăsăturilor de personalitate, însă ridică serioase probleme etice și pot conduce la stigmatizarea unor persoane sau grupuri;
- Sistemele pentru identificarea emoțiilor în mediile educaționale sau profesionale. Utilizate în școli sau la locurile de muncă, aceste sisteme monitorizează stările emoționale ale indivizilor, ceea ce poate aduce atingere libertății personale și unui mediu de lucru sănătos.

Risc ridicat. Aceste sisteme urmează a fi evaluate înainte de lansarea pe piață și monitorizate pe întregul lor ciclu de viață, furnizorii și cei care le pun în aplicare având responsabilități clar definite. Furnizorii sistemelor IA cu risc ridicat au nevoie de aprobări pentru sistemele de gestionare a riscurilor, guvernarea datelor, documentația tehnică și standardele de calitate. În același timp, cei care implementează aceste tehnologii sunt obligați să asigure conformitatea cu normele în vigoare și să garanteze supravegherea umană.

Sistemele IA cu risc ridicat sunt cele care pot genera pericole pentru sănătate și siguranță dacă nu sunt utilizate adecvat. Printre acestea se numără:

- Sistemele care reglementează accesul la infrastructura critică, cum ar fi apă, gaze;

- Sistemele care reglementează accesul la educația și evaluarea elevilor;
- Sistemele utilizate la selectarea și recrutarea locurilor de muncă, precum și evaluarea angajaților pe baza comportamentului și a personalității;
- Sistemele folosite în procesele de aplicare a legii sau în procesele de justiție pentru a determina exactitatea dovezilor, riscul de recidivă, etc;
- Sistemele folosite la graniță pentru controlul imigrației și al frontierelor, pentru determinarea eligibilității vizelor.

Risc limitat. Rolul sistemelor IA este de a asigura transparența, ceea ce presupune ca dezvoltatorii și implementatorii să informeze corect utilizatorii finali atunci când interacționează cu un sistem IA.

Impactul acestor sisteme este semnificativ doar dacă utilizatorii nu sunt conștienți că interacționează cu un sistem IA. În această categorie sunt incluse:

- Sistemele care utilizează programe chatbot și asistenți vocali. Acestea interacționează direct cu utilizatorii, iar lipsa transparenței poate duce la confuzie sau eroare;
- Sistemele care utilizează deepfakes și generare IA de imagini și sunete. Acest tip de sisteme pot crea conținut realist care, dacă nu este recunoscut ca atare, poate fi folosit în scopuri frauduloase sau dăunătoare.

Risc minim. Sistemele IA nu sunt supuse unor restricții majore. Conform legii IA, sistemele IA cu risc minim sunt sistemele care nu se încadrează mai sus și sunt sistemele utilizate în jocurile video și în filtrele de spam.

Sistemele IA cu scop general (GPAI): această categorie de sisteme a fost introdusă pentru a aborda preocupările legate de IA generativă și acoperă sisteme caracterizate prin:

- Capacitatea de a efectua diferite sarcini, precum dialog, generarea de imagini sau cod;
- Instruire pe seturi mari de date. GPAI necesită cantități substanțiale de date pentru a învăța și funcționa corespunzător;
- Instruire cu resurse mari de calcul. Dezvoltarea acestor sisteme cere resurse computaționale substanțiale.

Furnizorii sistemelor GPAI au obligația de a realiza documentația tehnică privind procesele și datele utilizate în fazele de instruire și testare și, în conformitate cu Directiva privind drepturile de autor: sunt necesare măsuri pentru a respecta legile privind proprietatea intelectuală, evitând încălcarea drepturilor de autor.

Regulamentul General privind Protecția Datelor (GDPR)

Regulamentul general privind protecția datelor (GDPR) a fost adoptat de Uniunea Europeană (UE) cu scopul de a consolida confidențialitatea și protecția datelor cetățenilor europeni. Acesta se aplică tuturor entităților care prelucrează date cu caracter personal ale persoanelor fizice rezidente în UE.

Principalul obiectiv al GDPR este de a oferi indivizilor un control sporit asupra propriilor date personale, asigurând totodată că organizațiile care colectează, prelucrează sau stochează aceste date respectă principiile transparenței și responsabilității.

Regulamentul GDPR, în vigoare din 25 mai 2018, a înlocuit Directiva 95/46/CE din 1995. Principala diferență între o directivă și un regulament este aceea că o directivă oferă statelor membre flexibilitatea de a o adapta legislației naționale, în timp ce un regulament este aplicat direct și în mod uniform în toate statele membre ale UE (Tiliute, 2020).

GDPR constă în 99 de articole și se ocupă de protecția datelor personale și a informațiilor sensibile ale tuturor cetățenilor individuali din UE și ale celor din Spațiul Economic European, atât din interiorul, cât și din afara comunității UE (Proniewska et al., 2021).

Acesta este aplicabil în toate statele membre ale Uniunii Europene, iar țările din afara UE care își desfășoară activitățile în această regiune sunt obligate să respecte acest regulament. GDPR acordă o atenție deosebită datelor personale, definite ca informații care permit identificarea unei persoane fizice, cum ar fi locația geografică, numele sau adresa IP. Aceste date includ, de asemenea, informațiile stocate și accesate prin diverse aplicații, inclusiv modulele cookie. Regulamentul GDPR reglementează și categorii speciale de date, cum ar fi informațiile cu privire la opiniile politice, convingerile religioase, originea etnică sau datele biometrice, care necesită măsuri suplimentare de protecție (Tiliute, 2020).

GDPR reprezintă un factor de transformare important pentru platformele tehnologice și arhitecturile de date care se ocupă cu colectarea, stocarea și gestionarea datelor personale. Acest regulament impune cerințe stricte pentru operatorii de date, obligându-i să adopte măsuri de protecție a datelor, încă din faza de proiectare.

De asemenea, organizațiile au obligația de a înregistra toate activitățile de prelucrare a datelor și de a efectua evaluări amănunțite ale platformelor tehnologice și arhitecturilor de date pe care le utilizează.

Acest proces de auto-evaluare va implica analiza sistemelor informatice, site-urilor web, bazelor de date, depozitelor de date și platformelor de prelucrare a datelor, cu scopul de a înțelege exact ce date personale au fost colectate și unde sunt stocate.

După finalizarea acestei evaluări interne, organizațiile vor fi probabil nevoite să adapteze sau chiar să reprojeteze integral sistemele și platformele existente pentru a îndeplini cerințele GDPR. Acest proces poate implica modificări substanțiale ale infrastructurii lor tehnologice, dar va asigura, în cele din urmă, protecția adecvată a datelor personale și conformitatea cu regulamentul european (Li et al., 2019).

Se poate afirma că GDPR influențează dezvoltarea și implementarea tehnologiilor emergente, precum Inteligența Artificială, blockchain-ul sau cloud computing, toate fiind piloni esențiali pentru progresul economic și inovația globală. Aceste tehnologii, prin natura lor inovatoare, oferă soluții eficiente pentru creșterea performanței și productivității. Ele reprezintă un motor puternic al competitivității internaționale, împingând granițele tehnologice și deschizând noi oportunități în diverse domenii. Cu toate acestea, succesul lor depinde în mare măsură de capacitatea de a utiliza și prelucra date, element cheie care este acum supus unor reguli stricte impuse de GDPR.

GDPR, prin intermediul articolelor sale precum 13, 17 și 22, introduce noi provocări pentru dezvoltatorii și utilizatorii acestor tehnologii. De exemplu, în domeniul IA, reglementările cresc costurile și limitează aplicabilitatea sistemelor algoritmice. Articolul 22 impune revizuirea anumitor decizii luate de algoritmi, ceea ce poate perturba echilibrul între precizie și transparență, afectând în mod direct eficiența și funcționalitatea sistemelor IA. Mai mult, dreptul utilizatorilor de a-și șterge datele personale, conform Articolului 17, poate conduce la destabilizarea bazei de date necesare pentru antrenarea și funcționarea algoritmilor, reducând astfel eficiența și precizia lor.

La nivelul tehnologiei cloud computing, GDPR adaugă un strat suplimentar de complexitate. Furnizorii de servicii cloud sunt responsabili de furnizarea informațiilor detaliate despre prelucrarea datelor, conform Articolelor 13 și 14, ceea ce complică operațiunile zilnice și majorează costurile. Această cerință intră în contradicție cu principiul fundamental al eficienței cloud computing, bazat pe alocarea dinamică și optimă a resurselor în funcție de sarcini, proces dificil de anticipat și planificat în avans.

Astfel, GDPR, în timp ce își propune să protejeze confidențialitatea și securitatea datelor, ridică semne de întrebare importante cu privire la impactul său asupra inovației tehnologice. Balanța dintre reglementarea necesară pentru protecția datelor și libertatea de inovare rămâne un subiect deschis de dezbatere, în special în domeniul dinamice precum IA și cloud computing. În acest context, este esențial să găsim o cale de mijloc care să permită atât protejarea datelor cu sensibilitate, cât și stimularea continuă a progresului tehnologic (Li et al., 2019).

GDPR stabilește șase principii fundamentale pentru prelucrarea datelor personale: legalitate, echitate și transparență prin procesarea în mod legal, echitabil și

într-o manieră transparentă; limitarea scopului prin colectarea datelor doar în scopuri specificate, explicite și legitime, dar arhivarea și folosirea acestora pentru cercetări științifice, istorice sau statistice nu se consideră incompatibile cu scopul inițial; minimizarea datelor prin colectarea datelor relevante și limitate la minimumul necesar pentru scopul în care sunt colectate; acuratețea datelor prin colectarea datelor clare, precise și, care sunt mereu actualizate și necesitatea măsurilor pentru a se asigura că datele colectate nu sunt greșite și că acestea sunt șterse sau modificate în cazul unei greșeli în timp foarte scurt; limitarea stocării și asigurarea integrității și confidențialității prin păstrarea datelor personale doar cât timp este necesar pentru scopurile pentru care au fost colectate, excepție făcând doar datele care sunt folosite pentru arhivare în interes public, cercetare științifică sau istorică, sau în scopuri statistice²⁷.

Odată cu apariția Metaversului, un spațiu virtual în care utilizatorii pot interacționa, crea și tranzacționa cu active digitale, peisajul juridic devine tot mai complex. Proprietatea intelectuală, confidențialitatea și jurisdicția sunt doar câteva dintre provocările juridice majore aduse de Metavers. Deși Metaversul reprezintă tehnologii și concepte relativ noi, legislația existentă, cum ar fi GDPR și Directiva UE privind comerțul electronic, poate fi aplicată activităților din acest mediu virtual (Kalyvaki, 2023).

Realitatea virtuală (VR) și realitatea augmentată (AR) aduc provocări pentru cadrele juridice existente, în special în domenii precum dreptul antitrust și dreptul contractual, deoarece acestea estompează granițele dintre obiectele tangibile și cele virtuale și remodelează conceptele de personalitate.

Integrarea tot mai profundă a obiectelor virtuale în mediul real și importanța tot mai mare a avatarurilor în spațiile virtuale ridică întrebări juridice complexe legate de protecția datelor, dreptul de proprietate și drepturile individuale. Pe măsură ce mediile virtuale devin tot mai interconectate cu viața de zi cu zi – prin spații de lucru virtuale, interacțiuni sociale și comerț – natura juridică și protecția avatarurilor, care reprezintă identitatea personală, se impune a fi revizuită.

Natura globală a platformelor virtuale face dificilă reglementarea și controlul eficient al comportamentului de către sistemele juridice naționale, ceea ce duce la provocări în distribuirea responsabilității între operatorii platformelor și utilizatori. Acest lucru creează o nevoie urgentă de discuții între părțile interesate cu privire la modul în care legile viitoare pot gestiona relația în evoluție dintre drepturile personale și puterea economică a operatorilor de platforme în cadrul unei societăți hibride digital-fizice (Dwivedi et al., 2022).

Este de așteptat ca în viitor Metaversul să fie un sistem deschis, scalabil și de mari dimensiuni. Acest sistem este creat simultan, acoperind spațiul cibernetic,

²⁷ Intersoft Consulting (2024), *Art. 5 GDPR – Principles relating to processing of personal data*, Disponibil la: <https://gdpr-info.eu/art-5-gdpr/> [Accesat: 1 Oct. 2024].

terminalele hardware, diferiți producători și utilizatori și oferind o gamă largă de scenarii de aplicare în realitatea virtuală și augmentată (medii AR/VR). Fără o reglementare legală adecvată, teritoriul „libertății virtuale” se poate transforma într-un instrument distructiv. Doar cu sprijinul legii este posibil să se asigure reglementarea juridică a relațiilor sociale în Metavers.

În prezent, funcționează câteva meta-lumi diferite: Horizon Worlds, Ceek City, Baidu Xi Rang, Metaverse Facebook, Decentraland (Ethereum), Emirates Metaverse, Expanded Virtual World, tehnologii Qualcomm Nvidia Omniverse, AI, AR/VR, holograme, platforme XR, registre distribuite, rețele neuronale, tehnologii cuantice și alte soluții tehnice (Kostenko et al., 2022).

Tehnologiile imersive, precum realitatea virtuală (VR), realitatea augmentată (AR) și realitatea mixtă (MR), îmbină lumea reală cu cea generată de computer, oferind o vedere compusă. AR este o versiune îmbunătățită a lumii fizice prin utilizarea diferiților stimuli, cum ar fi audio sau vizual. Aplicarea de elemente suplimentare imaginilor virtuale tridimensionale (3D) ar trebui să se desfășoare în timp real, să fie interactivă și să permită utilizatorilor, care poartă de obicei un dispozitiv montat pe cap, libertatea de mișcare în afișajele 3D. Realitatea mixtă este un hibrid între realitatea augmentată și cea virtuală. Dispozitivele AR/VR/MR oferă o nouă calitate în domeniile artei și divertismentului, mentenanței, arhitecturii, industriei, serviciilor de sănătate și educației în medicină (Proniewska et al., 2021).

Senzorii din headset-urile VR (HMD), folosite pentru a accesa Metaversul, colectează și procesează o gamă largă de date personale, inclusiv informații biometrice și comportamentale. Aceste date sunt analizate cu ajutorul Inteligenței Artificiale pentru a asigura o experiență realistă în Metavers. Întrucât Metaversul Meta operează în Uniunea Europeană, regulamentul GDPR este aplicabil pentru a asigura protecția datelor personale ale utilizatorilor (Xynogalas et al., 2024).

Avatarurile virtuale create pentru a participa în Metavers pot conține informații sensibile despre utilizatori, iar conturile asociate acestora nu sunt întotdeauna anonime. Transferul datelor între diferite platforme Metavers este o altă problemă de confidențialitate, expunând datele la riscuri precum breșe de securitate sau fraude. Colaborarea între platforme este esențială pentru stabilirea unor metodologii de transfer sigur al datelor²⁸.

Metaversul este unic deoarece procesează date personale extinse și extrem de sensibile, legate de drepturi și libertăți fundamentale, ceea ce îl face riscant. În mod specific, datele biometrice sunt definite de GDPR ca date personale rezultate dintr-o procesare tehnică specifică referitoare la caracteristicile fizice, fiziologice sau

²⁸ Weingarden G. et al. (2022), *Metaverse and privacy* | IAPP, Disponibil la: <https://iapp.org/g/news/metaverse-and-privacy-2> [Accesat: 19 Aug. 2025].

comportamentale ale unei persoane fizice, care permit sau confirmă identificarea unică a acelei persoane fizice. Dacă Meta procesează astfel de date utilizând inteligența artificială (IA), de exemplu, într-un mod care permite identificarea unică, atunci aceste date vor fi considerate biometrice (Xynogalas et al., 2024).

GDPR reglementează procesarea datelor personale în Metavers și oferă utilizatorilor anumite drepturi, precum accesul, corectarea și ștergerea datelor. Utilizatorii platformelor Meta, cum ar fi Metaversul, sunt considerați „persoane vizate”, iar datele lor pot include informații sensibile, cum ar fi date biometrice. Acestea sunt definite de GDPR ca date rezultate din procesări tehnice ce permit identificarea unică a unei persoane (Xynogalas et al., 2024).

Organizațiile și națiunile nu sunt în prezent pregătite să abordeze provocările complexe legate de confidențialitate și securitate din Metavers, parțial din cauza lipsei de profesioniști calificați și a dificultății de a monitoriza și detecta atacurile pe aceste platforme noi.

Regulamentele existente, precum GDPR-ul UE, sunt insuficiente pentru a gestiona confidențialitatea în Metavers, unde granițele jurisdicționale sunt neclare, ceea ce face dificilă aplicarea regulilor privind transferul și procesarea datelor. Platformele din Metavers colectează cantități mari de date biometrice și personale, ridicând probleme legate de proprietatea datelor, securitatea și posibila manipulare a acestora.

Soluțiile viitoare sunt așteptate să găsească un echilibru între îmbunătățirea experienței utilizatorilor și protecția confidențialității, iar cercetările rămân esențiale pentru dezvoltarea unor instrumente de detectare timpurie a riscurilor legate de confidențialitate. (Dwivedi et al., 2022).

Deoarece Metaversul este accesibil la nivel global, el este supus unei varietăți de legi privind confidențialitatea și protecția datelor. Acest lucru face necesară crearea unor reglementări internaționale uniforme, care, însă, ar putea intra în conflict cu reglementările locale din anumite țări²⁹.

Guvernanța datelor este astăzi o condiție necesară pentru a construi un mediu digital sigur, de încredere și orientat spre utilizator, mai ales odată cu dezvoltarea rapidă a Metaversului și a Inteligenței Artificiale. Deși multe guverne și organizații internaționale au început să lucreze la politici și standarde, realitatea arată că datele sunt încă fragmentate, lipsesc reguli comune clare și există prea puțină trasabilitate și responsabilitate. Reglementarea este necesară nu doar pentru a proteja drepturile utilizatorilor, precum confidențialitatea și transparența, ci și pentru a crește încrederea și a sprijini inovația fără riscul erorilor sau al abuzurilor.

²⁹ Weingarden G. et al. (2022), Metaverse and privacy | IAPP, Disponibil la: <https://iapp.org/g/news/a/metaverse-and-privacy-2> [Accesat: 19 Aug. 2025].

Pentru ca Metaversul să evolueze într-un mod echilibrat, este nevoie de date deschise și standardizate, reguli clare de acces și protecție, mecanisme de verificare și curățare a informațiilor, dar și de o guvernanță adaptivă, capabilă să țină pasul cu schimbările rapide. Exemplele din alte țări arată că, trebuie adoptate certificări pentru algoritmi, audituri independente și platforme publice de date curate, toate însoțite de reguli stricte privind responsabilitatea.

Uniunea Europeană poate avea un rol-cheie prin armonizarea standardelor, finanțarea infrastructurilor și sprijinirea alfabetizării digitale, în timp ce forumuri internaționale precum OCDE sau G20 pot facilita cooperarea globală și prevenirea ecosistemelor digitale izolate.

Responsabilitatea este împărțită: sectorul privat trebuie să implementeze principii de etică și transparență, societatea civilă are rolul de a monitoriza și educa, iar guvernele trebuie să ofere un cadru coerent și adaptat. Astfel, România și partenerii europeni pot crea o guvernanță a datelor care să asigure un Metavers sigur, interoperabil și centrat pe oameni, unde inovația merge mână în mână cu respectarea drepturilor și a încrederii publice.

Partea II.
*Tehnologiile emergente: factor-cheie în
transformarea societății*



3. Utilizarea Metaversului în administrația publică



În primul capitol a fost evidențiat modul în care Metaversul își găsește aplicabilitatea în multiple domenii, precum educația, industria jocurilor video sau administrația publică. Exemplele prezentate au arătat potențialul acestei tehnologii emergente de a transforma procese instituționale și sociale, de a genera noi modalități de interacțiune între actori și de a crește eficiența în desfășurarea unor activități care, până în trecutul recent, aveau loc exclusiv în spațiul fizic.

Prezentul capitol își propune să aprofundeze analiza asupra unei dimensiuni de interes major pentru societatea contemporană: integrarea Metaversului în administrația publică. Obiectivul principal constă în identificarea modalităților prin care această tehnologie poate fi încorporată în procesele administrative, examinarea beneficiilor potențiale pentru cetățeni și personalul administrativ, precum și evaluarea provocărilor și limitărilor inerente acestei implementări

Demersul analitic va fi structurat pe două axe complementare. În prima parte, vor fi prezentate câteva direcții de utilizare potențială a Metaversului în administrația publică, urmate de analiza a două studii de caz relevante – implementările din Seul și Dubai –, menite să ilustreze concret modul în care această tehnologie poate fi aplicată în practică, cu accent pe rezultatele obținute și lecțiile desprinse din aceste experiențe. În cea de-a doua parte, va fi prezentată o investigație calitativă bazată pe un focus-grup cu experți în administrație publică. Datele obținute vor fi

analizate în vederea surprinderii percepțiilor și evaluărilor formulate de aceștia cu privire la oportunitatea, utilitatea și fezabilitatea adoptării Metaversului în context administrativ, precum și pentru conturarea unei perspective critice asupra direcțiilor de dezvoltare viitoare.

Introducerea Metaversului în sfera publică promite, și amenință, să reconfigureze fundamental natura relației dintre stat și cetățean și să modifice psihologia interacțiunilor civice. De aceea, este necesară o distincție conceptuală între e-guvernare și ceea ce am putea numi *meta-guvernanță*.

E-guvernarea (Electronic Governance), în forma sa actuală, reprezintă în principal utilizarea tehnologiilor informaționale și de comunicații (TIC) pentru a optimiza și a oferi online serviciile guvernamentale existente. Este un model predominant tranzacțional: cetățeanul accesează un portal web pentru a plăti o taxă, a depune o cerere sau a consulta o informație. Interfața este bidimensională (ecranul), iar interacțiunea este mediată prin formulare și text.

Meta-guvernanța (Metaverse Governance) propune o paradigmă fundamental diferită. Ea implică utilizarea spațiilor virtuale imersive și persistente pentru a transforma interacțiunea, participarea și colaborarea. Logica nu mai este una de „serviciu”, ci de „experiență și «co-creare»”. Cetățeanul nu mai este un simplu utilizator al unui serviciu, ci un participant activ într-un mediu virtual. De exemplu, în loc să citească un raport despre un proiect de infrastructură, el poate „vizita” virtual șantierul, poate interacționa cu un model 3D al proiectului final și poate oferi feedback într-un context spațial.

Metaversul, privit ca o rețea persistentă și interoperabilă de lumi virtuale tridimensionale, nu reprezintă doar o evoluție a internetului, ci o transformare fundamentală a interfeței dintre stat și cetățean, trecând de la un model tranzacțional, bazat pe formulare (e-guvernare), la un model experiențial, spațial și imersiv (meta-guvernanță).

Această tranziție are potențialul de a schimba dinamica puterii. Pe de o parte, poate duce la o democratizare sporită, oferind cetățenilor un acces mai direct și mai intuitiv la informații și la procesele decizionale. Pe de altă parte, gradul de imersiune și datele colectate pot crea noi și subtile forme de control și monitorizare.

Există două viziuni principale care modelează dezvoltarea Metaversului: o viziune centralizată, care dezvoltă ecosisteme închise (cunoscute și ca „walled gardens”), în care controlul asupra datelor ține de compania dezvoltatoare, și o viziune descentralizată, bazată pe principiile Web3, care promovează platforme deschise, interoperabile și controlul utilizatorului asupra datelor și activelor digitale. Pentru sectorul public, înțelegerea acestei dihotomii are implicații asupra deciziilor strategice privind suveranitatea digitală și dependența sau independența de platforme private. Metaversul este o evoluție majoră a interfeței prin care cetățeanul interacționează

cu statul. Dacă e-guvernarea a reprezentat digitalizarea proceselor birocratice existente, meta-guvernanța propune o trecere de la o interacțiune bidimensională, tranzacțională, la una tridimensională, spațială și experiențială. De exemplu, în loc de a consulta un plan urbanistic zonal (PUZ) sub forma unui document PDF, un cetățean ar putea „păși” într-un model 3D al cartierului său pentru a vizualiza direct impactul noilor construcții. Această modificare a naturii interacțiunii de la una pur informațională la una participativă și imersivă necesită o regândire completă a modului în care serviciile publice sunt proiectate și livrate.

Există o contradicție între viziunea corporatistă, centralizată, a Metaversului și nevoile sectorului public. O administrație publică ce își construiește prezența pe o platformă proprietară, cum ar fi cea dezvoltată de Meta, devine dependentă de standardele tehnice, modelele de afaceri și, cel mai important, de politicile de colectare a datelor ale unei entități private. Acest lucru poate intra în conflict direct cu principiile de transparență, suveranitate digitală și protecție a datelor cetățenilor, care ar trebui să ghideze acțiunea guvernamentală. Alternativa, bazată pe tehnologii Web3, oferă un model teoretic mai aliniat cu interesul public, dar se confruntă cu provocări semnificative de maturitate tehnologică, scalabilitate și complexitate în implementare. Prin urmare, prima decizie

strategică pentru orice guvern nu este „*ce construim?*”, ci „*pe ce fundație tehnologică și ideologică construim și care sunt compromisurile pe termen lung?*”. Două concepte aplicative se disting prin relevanța lor directă și potențialul

transformator pentru administrația publică - Gemenii Digitali și Identitatea Descentralizată. Un geamăn digital este mai mult decât un simplu model 3D; este o replică virtuală a unui obiect, proces sau sistem fizic, care este actualizată constant cu date în timp real de la senzori din lumea fizică (tehnologia Internet of Things - IoT). Un „Geamăn digital al unui Oraș” (City Digital Twin) integrează date din multiple surse – senzori de trafic, rețele de utilități, date GIS, modele meteorologice – pentru a crea un model virtual, dinamic și cuprinzător al mediului urban. Valoarea sa pentru administrație nu constă doar în vizualizare, ci în capacitatea sa de a funcționa ca un instrument analitic și de simulare. Administratorii publici pot folosi un geamăn digital pentru a testa scenarii „what-if” (de exemplu, „care va fi impactul asupra traficului dacă închidem acest bulevard pentru un eveniment?”) și pentru a lua decizii bazate pe date, nu pe intuiție. Standardizată de consorțiul World Wide Web (W3C), *identitatea descentralizată* reprezintă o schimbare de paradigmă în managementul identității digitale. Într-un sistem tradițional, identitatea noastră digitală (contul de Google, contul bancar) este emisă și controlată de o terță parte. DID-urile permit crearea unei identități digitale „auto-suverane”, care este generată și controlată direct de utilizator, independent de orice registru centralizat. Această identitate este verificabilă criptografic. Pentru serviciile publice în Metavers, DID-

urile sunt esențiale, deoarece ar permite unui cetățean să-și dovedească identitatea sau anumite atribute (de exemplu, „sunt major”, „sunt rezident al acestui oraș”) fără a dezvălui alte informații personale, asigurând interacțiuni sigure și private (un concept cunoscut sub numele de „zero-knowledge proofs”).

Aplicații potențiale ale Metaversului în administrația publică

Una dintre cele mai directe și discutate aplicații ale Metaversului în administrația publică este crearea de „primării virtuale” sau „ghișee unice imersive”. Acestea ar fi spații virtuale tridimensionale unde cetățenii, prin intermediul avatarurilor, pot naviga și interacționa cu diverse departamente ale administrației publice.

Într-un astfel de mediu, un cetățean ar putea interacționa cu funcționari publici, fie că sunt reprezentați de alte avataruri controlate de oameni, fie de asistenți virtuali bazați pe inteligență artificială. Cetățenii pot discuta, pune întrebări și primi consultanță personalizată într-un mod mai natural și interactiv decât prin chat-uri text sau apeluri telefonice. Totodată, ei pot depune documente, parcurge fluxuri administrative sau efectua plăți prin sisteme de plată integrate ce permit achitarea taxelor și impozitelor direct în mediul virtual. Acest model oferă accesibilitate sporită, în special pentru persoanele cu mobilitate redusă, cele care locuiesc în zone rurale sau izolate, sau pentru cetățenii din diaspora.

Conceptul de geamăn digital al unui oraș reprezintă probabil cea mai puternică aplicație a Metaversului pentru meta-guvernanță. Acesta este o platformă de simulare dinamică, alimentată cu date în timp real, care poate revoluționa modul în care orașele sunt planificate și gestionate.

În domeniul planificării urbane, gemenii digitali permit urbanistilor și arhitecților să modeleze și să simuleze impactul proiectelor de dezvoltare înainte ca acestea să fie construite. Se pot analiza scenarii complexe precum modificarea fluxurilor de trafic ca urmare a construirii unui nou complex rezidențial; impactul umbririi noilor clădiri înalte asupra spațiilor publice și a clădirilor învecinate; eficiența energetică a unui nou cartier sau impactul implementării unor noi surse de energie regenerabilă; simularea poluării fonice și a calității aerului în diferite scenarii de dezvoltare.

În managementul crizelor, capacitatea de simulare a gemenilor digitali este utilă în pregătirea pentru situații de urgență. Echipele de intervenție pot simula dezastre naturale precum inundații, cutremure sau incendii de vegetație pentru a testa și optimiza planurile de evacuare și de răspuns; pot aloca resurse (ambulante, mașini de pompieri) în timp real într-un mediu virtual pentru a identifica cele mai eficiente strategii de desfășurare pot antrena personalul în scenarii realiste, dar complet sigure.

Rolul gemenilor digitali este de a funcționa ca o infrastructură de date pentru o guvernare proactivă. În loc să reacționeze la probleme precum ambuteiajele sau aglomerarea serviciilor publice, prin gemeni digitali se pot anticipa și preveni astfel de probleme prin simulări predictive. Metaversul devine interfața de vizualizare și interacțiune cu acest „creier” digital al orașului, transformând date complexe în informații intuitive și acțiuni concrete.

Augmentarea gemenilor digitali cu tehnologii imersive, în special Realitatea Virtuală (VR), oferă oportunități pentru formarea și perfecționarea personalului din sectorul public, în special în domenii unde instruirea în lumea reală este periculoasă, costisitoare sau dificil de replicat. De exemplu, pompierii pot exersa proceduri de stingere a incendiilor în diferite tipuri de clădiri sau de gestionare a unor scurgeri de substanțe periculoase, fără niciun risc fizic. Platforme precum Response Simulator de la VSTEP sunt deja utilizate în acest scop, permițând instructorilor să modifice scenariul în timp real, în funcție de acțiunile cursanților.

Un avantaj important al Metaversului poate fi revitalizarea implicării civice, prin noi canale pentru participare și deliberare, depășind limitările geografice și logistice ale ședințelor publice clasice. Cetățenii pot participa la dezbateri privind bugetele locale, proiecte de legi sau strategii de dezvoltare, direct de acasă. Anonimizarea oferită de un avatar poate încuraja mai multe persoane să își exprime liber opiniile. Platformele de Metavers pot găzdui procese colaborative în care cetățenii oferă feedback și participă activ la proiectare. De exemplu, locuitorii unui cartier ar putea explora mai multe variante de reamenajare a unui parc într-un model 3D interactiv și ar putea vota sau chiar propune modificări.

Deși guvernarea virtuală poate amplifica participarea, există și riscul să exacerbeze polarizarea și camerele de ecou, probleme deja omniprezente în social media. Interacțiunile mediate prin avatare pot reduce anumite inhibiții dar și dezinhiba comportamentele toxice. În acest caz pot fi aplicate mecanisme de moderare, de facilitare a dialogului constructiv și de expunere la perspective diverse, pentru a nu replica aspecte dăunătoare ale Web 2.0 într-un mediu 3D cu un impact psihologic mult mai puternic.

Pionierii guvernării virtuale: studii de caz globale – Seul și Dubai

Printre primele inițiative concrete prin care guvernele au început deja să exploreze Metaversul, două studii de caz se remarcă prin anvergură, viziune strategică și stadiu avansat de implementare: „Metaverse Seoul”¹ și „Dubai

¹ Dong-hwan K. (2023), *Seoul gov't launches world's 1st public services platform in metaverse - The Korea Times*, Disponibil la: <https://www.koreatimes.co.kr/business/tech-science/20230117/seoul-govt-launches-worlds-1st-public-services-platform-in-metaverse> [Accesat: 19 Aug. 2025].

Metaverse Strategy”². Acestea nu reprezintă doar proiecte tehnologice, ci și două modele ideologice distincte de abordare a guvernanței în era digitală imersivă.

Guvernul Metropolitan din Seul a fost prima administrație locală din lume care a anunțat o foaie de parcurs pentru integrarea serviciilor sale în Metavers, lansând prima fază a platformei în ianuarie 2023. Proiectul „Metaverse Seoul” a fost conceput ca un răspuns strategic la tendințele accelerate de pandemie, precum stilul de viață contactless, și ca o modalitate de a interacționa cu generațiile tinere, native digital. Obiectivul pe termen lung, stabilit pentru 2026, este ambițios: migrarea tuturor serviciilor administrative cheie – economice, culturale, turistice, educaționale și civice – într-un mediu virtual unificat. Viziunea este aceea de a crea un „spațiu creativ pentru comunicare, un spațiu nediscriminatoriu, unde realitatea întâlnește cyberspațiu”.

Chiar din prima fază, platforma a oferit o gamă variată de funcționalități concrete, demonstrând o abordare axată pe utilitate imediată pentru cetățeni:

- *Servicii administrative.* Cetățenii pot solicita și obține șapte tipuri de documente oficiale, pot primi consultanță virtuală pe probleme fiscale și pot depune plângeri sau petiții.
- *Implicare civică.* O replică virtuală a biroului primarului permite cetățenilor să trimită propuneri direct edilului, creând un nou canal de comunicare.
- *Suport economic și social.* Platforma include un „Fintech Lab” pentru promovarea companiilor din domeniu, un „Centru de Suport pentru Întreprinderi” care oferă consultanță pe probleme de management, legale și de resurse umane, și un serviciu de consiliere și mentorat pentru tineri, numit „Metaforest”.
- *Cultură și turism.* Utilizatorii pot explora virtual replici ale principalelor 10 atracții turistice din Seul și pot participa la activități sociale în spații virtuale precum o replică a Pieței Seul.

Una dintre provocările majore identificate timpuriu a fost gestionarea și interpretarea feedback-ului public pentru a ghida dezvoltarea ulterioară a platformei. Pentru a asigura un mediu sigur și a preveni hărțuirea, au fost implementate măsuri tehnice proactive, precum filtrarea automată a limbajului licențios și interzicerea contactului fizic între avatare. De asemenea, se depun eforturi pentru a asigura accesibilitatea platformei pentru cetățenii mai în vârstă, care ar putea întâmpina dificultăți în utilizarea noilor tehnologii.

² TDRA (2023), *Dubai Metaverse Strategy | The Official Portal of the UAE Government*, Disponibil la: <https://u.ae/en/about-the-uae/strategies-initiatives-and-awards/strategies-plans-and-visions/government-services-and-digital-transformation/dubai-metaverse-strategy> [Accesat: 19 Aug. 2025].

Lansată în iulie 2022, Strategia Metaverse a Dubaiului reflectă ambiția emiratului de a se poziționa ca un lider global nu doar în tehnologie, ci și într-o nouă paradigmă economică. Abordarea este mai puțin centrată pe livrarea de servicii publice și mai mult pe crearea unui ecosistem economic vibrant.

Scopul declarat este de a plasa Dubaiul în top 10 economii de Metavers la nivel mondial și de a deveni un hub global pentru comunitatea și companiile din acest domeniu. Obiectivele cuantificabile sunt clare: adăugarea a 4 miliarde USD la PIB-ul anual până în 2030, atragerea a peste 1.000 de companii specializate în blockchain și Metavers, și susținerea creării a 40.000 de locuri de muncă virtuale.

Strategia se fundamentează pe dezvoltarea și adoptarea unui set de tehnologii de bază: realitatea extinsă (XR), gemenii digitali, Web3, inteligența artificială și blockchain. Toate acestea sunt susținute de o infrastructură de conectivitate de ultimă generație, bazată pe 5G și edge computing, considerată esențială pentru a permite experiențe imersive de înaltă calitate.

Deși serviciile guvernamentale sunt menționate ca un domeniu de aplicare, accentul principal cade pe sectoarele economice cu potențial de creștere: turism, educație, retail, imobiliare și sănătate. Inițiativele concrete, precum lansarea de către Ministerul Sănătății și Prevenției (MoHAP) a unui „centru de servicii pentru fericirea clienților” în Metavers, sunt adesea pilotate ca exemple de inovație care pot fi replicate în sectorul privat.

O componentă distinctivă a strategiei Dubaiului este accentul pus pe crearea unui cadru de guvernare agil și pro-inovație. Viziunea este ca autoritățile să acționeze mai degrabă ca „arbitri” care stabilesc reguli clare pentru protecția datelor, a proprietății intelectuale și a utilizatorilor, decât ca „portari” care încetinesc inovația prin birocrăție. Acest lucru este conceput pentru a atrage talente și companii din întreaga lume.

Analiza comparativă a celor două abordări relevă două filosofii fundamentale diferite. Seul adoptă un model în care guvernul este principalul actor și furnizor, utilizând Metaversul ca un nou canal pentru a-și îndeplini misiunea de a servi cetățenii. Discursul public este centrat pe concepte precum „incluziune”,

„comunicare” și „accesibilitate”. În contrast, Dubai promovează un model în care guvernul este un facilitator și un catalizator. Rolul său principal este de a crea condițiile – infrastructură, reglementări favorabile, finanțare – pentru ca sectorul privat să poată inova și prospera. Discursul public este dominat de termeni economici: „PIB”, „locuri de muncă”, „investiții”.

Această distincție, evidențiată și în analize academice, este de o importanță capitală pentru orice altă administrație, inclusiv cea din România, care ia în considerare o strategie pentru Metavers. Decizia fundamentală care trebuie luată la nivel strategic nu este una tehnologică, ci una de viziune: este scopul principal

eficientizarea aparatului administrativ și îmbunătățirea directă a serviciilor pentru cetățeni (modelul Seul), sau este stimularea unui nou sector economic, cu beneficii indirecte pentru societate (modelul Dubai)? Răspunsul la această întrebare va dicta alocarea resurselor, designul politicilor publice și parteneriatele strategice care vor fi urmărite.

Alte inițiative, precum cele din Finlanda (Tampere și Helsinki), se află încă într-o fază incipientă, de cercetare și elaborare a strategiei, concentrându-se pe identificarea domeniilor cheie de aplicare, cum ar fi mobilitatea, sănătatea și siguranța publică. Acestea reprezintă un model mai prudent, de tip „așteaptă și vezi”, care poate fi, de asemenea, o opțiune validă.

Această tranziție deschide un orizont de oportunități, de la crearea de servicii publice mai accesibile și intuitive în „primării virtuale”, la simulări avansate pentru planificare urbană și managementul crizelor prin intermediul „gemenilor digitali”, și până la platforme inovatoare pentru implicare civică și formare profesională imersivă.

Cercetare pe baza unui focus grup

Întregul demers teoretic anterior nu are doar o motivație epistemică, ci și un obiectiv pragmatic - de a înțelege abordarea pe care o au decidenții din administrația publică față de o potențială platformă de lucru în Metavers și de a formula sugestii de optimizare a modului actual de lucru în domeniul guvernanței datelor. Din acest motiv, experți din diferite sfere ale administrației publice, respectiv din ministere conexe domeniului, din primării și consilii județene, din cadrul autorităților care reglementează domeniul IT, precum DNSC, ANCOM, Consiliul Concurenței au fost invitați să-și exprime opiniile referitoare la practicile curente și la modul în care consideră că ar trebui să fie reglementată guvernanța datelor în Metavers.

Această schimbare potențială de paradigmă deschide noi oportunități pentru guverne și cetățeni, modificând total modul de interacțiune și de furnizare a serviciilor publice, sporind transparența și eficiența și reducând în același timp costurile și complexitatea.

Metaversul nu înseamnă obligatoriu furnizarea unor noi servicii de e-guvernare, ci schimbă total nivelul de interacțiune guvern-cetățean. Astfel, prin intermediul avatarurilor, cetățenii vor putea să participe la elaborarea politicilor, să obțină informații și servicii de la reprezentanții virtuali guvernamentali activați de inteligență artificială care vor oferi o experiență umană pentru cetățeni sau utilizatori.

Guvernanța datelor este un subiect critic în Metavers, iar părerile experților invitați referitoare la provocările specifice, riscurile asociate și demersurile care ar trebui demarate sunt de importanță mare și pot constitui fundamentul unei viitoare abordări coerente.

Având în vedere noutatea și complexitatea subiectului abordat, am decis că cea mai corectă abordare ar fi o discuție semistructurată pe baza unui ghid de interviu monofocal, în locul unui interviu multidimensional, centrat pe problematica guvernancei datelor în viitoarea platformă Metavers.

Rezultatele acestui studiu credem că vor constitui un punct de plecare pentru concretizarea preocupărilor pe care administrația publică ar trebui să le aibă în legătură cu subiectul Metavers și cu aplicabilitatea lui în domeniul public.

Metodologia de cercetare

Metaversul va însemna o schimbare de paradigmă cu consecințe pe care încă nu le înțelegem; de aceea, prin acest focus grup am încercat să provocăm experții invitați să își valorifice imaginația și spiritul critic într-un exercițiu intelectual necesar pentru trasarea unor scenarii ale viitorului.

OBIECTIVUL CERCETĂRII

Explorarea și înțelegerea perspectivelor, preocupărilor și așteptărilor utilizatorilor cu privire la gestionarea, confidențialitatea și securitatea datelor în Metavers.

ALEGEREA METODEI

Metoda focus grup a fost aleasă pentru că permite discutarea detaliată a subiectelor propuse, cu ajustări reciproce între participanți, pe tema guvernancei datelor în Metavers. Spre deosebire de metodele individuale de colectare a datelor, cum ar fi interviurile sau chestionarele, focus grupul permite interacțiunea între membrii grupului, stimulând dezbateră și exprimarea unor opinii diverse. În contextul unui subiect complex și relativ nou precum guvernancea datelor în Metavers, această metodă este ideală pentru a explora percepțiile colective și pentru a identifica atitudini și preocupări comune.

Focus grupul a fost preferat în locul altor metode, deoarece acesta poate oferi nu doar informații despre ce gândesc participanții, ci și despre de ce gândesc astfel. În timp ce un sondaj ar putea măsura nivelul de încredere în guvernancea datelor, focus grupul permite explorarea mai profundă a motivelor din spatele acestor niveluri de încredere sau neîncredere, dezvăluind factori subiectivi precum experiențele anterioare, temerile sau opiniile despre securitatea datelor în spațiile virtuale.

Focus grupul este o metodă excelentă pentru a colecta perspective autentice, încurajând participanții să vorbească deschis și spontan în cadrul unei discuții moderate de un facilitator. Într-un mediu de grup, oamenii sunt adesea inspirați să-și împărtășească experiențele personale și să dezvăluie opinii mai nuanțate decât ar face-o într-un cadru individual. În cazul guvernancei datelor în Metavers, această

autenticitate este importantă, deoarece arată în mod direct ce anume își doresc utilizatorii în ceea ce privește protecția datelor lor.

Focus grupul s-a desfășurat online, prin intermediul platformei Webex, iar sesiunea a durat 2 ore.

PROCESUL DE SELECȚIE A PARTICIPANȚILOR

Pentru a asigura o diversitate a perspectivei și a experienței în discuții, selecția participanților a fost realizată în funcție de criteriile predefinite, precum vechimea în activitate și derularea activității într-un domeniu de activitate conex guvernancei datelor în Metavers.

La focus grup au fost invitați să participe 10 experți, un număr optim pentru a permite fiecărui participant să își exprime părerea, dar și pentru a menține o coerență în discuții. Condiția ca un participant să fie selectat pentru eșantionul vizat era ca aceștia să dețină o vechime de minim 10 ani în domeniul administrației publice. Deși poate părea o perioadă redusă pentru eticheta de expert, am avut în vedere noutatea subiectului la care ne referim. Astfel, au fost acceptați ca experți cei familiarizați cu subiectul, adică implicați în administrația publică, cu specializări în domenii precum informatică, științe inginerești, matematică/statistică, științe juridice și științe sociale.

Am invitat să participe la studiu, în mod echilibrat, experți cu funcții de conducere în instituțiile de apartenență, dar și cu funcții de execuție. Motivația din spatele acestei alegeri derivă din faptul că ambele perspective au puncte forte importante de care este necesar să ținem seama în elaborarea unui cadru de guvernare. Dacă managerii sunt cei care dețin o privire de ansamblu asupra domeniului și se pot referi la abordarea macro a guvernancei datelor în Metavers, persoanele din sfera de execuție cunosc mai bine provocările care apar în fiecare zi în implementarea politicilor și gestionarea concretă a situației de pe teren.

Pentru a respecta principiile etice și pentru a crea un mediu de siguranță pentru participanți, s-au luat măsuri speciale de protecție a confidențialității acestora. Informațiile personale au fost păstrate anonime, iar interpretarea răspunsurilor a fost realizată prin referințe la Subiectul nr. 1 - 10 (S1 – S10).

ÎNTREBĂRILE DE CERCETARE

Pentru a ghida răspunsurile experților către segmentele de interes pentru subiectul de cercetare, am construit un ghid cu întrebări semistructurate în funcție de care va fi condusă discuția, dar care va permite și aprofundarea unor idei, pe măsură ce sunt exprimate de experți. Întrebările sunt orientative și se referă la guvernancea datelor, confidențialitate și securitate în Metavers și au fost concepute astfel încât să încurajeze reflecția și să permită participanților să dezvăluie opinii nuanțate, precum și să răspundă liber, fără a fi limitați de răspunsuri predefinite.

1. Care sunt principalele direcții de care ar trebui să ținem cont în privința guvernancei datelor în Metavers?
2. Cum se pot aplica reglementările GDPR pentru platforma Metavers?
3. Cum pot fi prevenite și contracarate utilizările abuzive ale datelor colectate în Metavers, astfel încât să se evite riscurile de manipulare sau alte scopuri rău intenționate?
4. Ce autorități ar trebui să se ocupe de protejarea datelor în Metavers în plan național? Dar în Uniunea Europeană?
5. Ce amenințări de securitate cibernetică credeți că sunt mai probabile în Metavers? Cum ar trebui contracarate riscurile și amenințările de securitate cibernetică în Metavers? De către cine?
6. Ce drepturi ar trebui să aibă utilizatorii în Metavers pentru a controla modul în care sunt colectate, utilizate și partajate datele lor?
7. Cum ar trebui să se împartă controlul datelor în Metavers între diferiții stakeholders (instituții publice, entități private, utilizatori, autorități ale statului)?
8. Cum pot fi protejate drepturile categoriilor vulnerabile (copii, adolescenți, minorități etnice, de gen, persoane aflate în dificultate, marginalizați etc.) în Metavers?
9. Cum poate administrația publică să folosească Metaversul pentru a îmbunătăți serviciile publice și participarea cetățenilor în mod etic și sigur?
10. Care sunt riscurile și beneficiile economice și sociale legate de prezența administrației publice în Metavers și cum intenționați să le gestionați?

Prezentarea și analiza datelor

Datele obținute au fost transcrise și codificate în funcție de tematici fiind utilizate metode de analiză a textului precum harta mentală. Ulterior, au fost extrase categoriile care reflectă temele majore și subtemele relevante, așa cum reies acestea din opiniile respondenților asupra subiectelor propuse.

REZULTATELE CERCETĂRII

Preocupările experților referitoare la viitoarea platformă Metavers au fost sintetizate în răspunsurile pe care le-au oferit la întrebarea Care sunt principalele direcții de care ar trebui să ținem cont în privința guvernancei datelor în Metavers?, interesul predominant al grupului fiind axat pe următoarele teme:

- securitatea datelor cu accent asupra confidențialității datelor personale ale utilizatorilor, și controlul asupra datelor (S2, S3, S4, S7, S10) și pe protejarea infrastructurii și datelor utilizatorilor (S1, S3, S4);

- stabilirea unor standarde de securitate și trasabilitate pentru a permite auditarea și monitorizarea coerentă a datelor (S5, S8);
- transparența proceselor și responsabilitățile clare privind modul în care datele sunt gestionate, procesate și utilizate de către platformele din Metavers (S2, S3, S7), definirea clară a categoriilor de date care pot fi partajate și a regulilor de utilizare a datelor publice (S8), monitorizarea conformității și răspunderea platformelor pentru protejarea datelor (S2, S4), consimțământul explicit și detaliat în colectarea și utilizarea datelor (S7, S10);
- nevoia de informare a utilizatorilor despre drepturile lor și riscurile asociate datelor în Metavers (S3, S4);
- interoperabilitatea între platforme pentru o experiență fluidă a utilizatorului (S2, S5) și standardizarea platformelor;
- promovarea unei utilizări etice a datelor, care să respecte drepturile utilizatorilor și să evite abuzurile (S3).

Au fost înregistrate și opinii mai puțin comune în discursul public, precum nevoia de a menține principiul proporționalității utilizării datelor obținute în Metavers: folosirea datelor în limite rezonabile, astfel încât colectarea să fie proporțională cu nevoile platformei (S7), încurajarea „data sharing-ului” între organizații pentru a sprijini dezvoltarea de produse și servicii inovatoare, evitarea situațiilor de monopol asupra datelor pentru a permite diversitatea și competiția pe piață (S10) sau implementarea blockchain-ului pentru trasabilitatea datelor și auditarea entităților generatoare de date (S5). Odată exprimate, aceste idei au captat interesul participanților și au generat convergență.

În privința modului de aplicare a reglementărilor GDPR (General Data Protection Regulation) în platforma Metavers, experții au fost unanim de acord că prevederile legislative existente pot fi acoperitoare pentru situațiile generate de viitorul digital:

„Prin aplicarea principiilor ce stau la baza reglementării în general, în sensul că acele companii sau platforme înregistrate în Uniunea Europeană care colectează date ce pot conduce la realizarea unei legături cu identitatea unei persoane trebuie să fie ținute responsabile de respectarea aceluiași obligații privind protecția datelor în Metavers ca și în lumea fizică” (S8),

cu minime nuanțe în privința faptului că sunt necesare evaluări ale riscurilor legate de prelucrarea datelor sensibile precum cele biometrice și de localizare (S3, S4), fiind făcută precizarea explicită că: *„în ceea ce privește prelucrarea datelor biometrice, aceasta trebuie să se încadreze în excepțiile de la art. 9 alin. (2) GDPR” (S7)*. De asemenea, a fost subliniată de către experți nevoia de armonizare a legislației internaționale, inclusiv între UE și SUA (S4, S8, S9). Participanții au reiterat un

principiu care ar trebui avut în vedere în permanență, pentru a nu relua procesele de reglementare de fiecare dată când tehnologia transformă spațiul digital:

„Putem porni de la aceleași idei de la care a pornit DSA: what is illegal offline is also illegal online. Astfel, ceea ce e privat în viața reală ar trebui să fie privat și în viața din Metavers. Crearea unor mecanisme de tipul «dreptul de a fi uitat» și «dreptul de a fi lăsat în pace» care să stea la baza dezvoltării de lumi virtuale, adică stimularea dezvoltării lumilor virtuale cu ajutorul principiului «privacy by design» ar fi principala cale spre asigurarea aplicării GDPR în viața reală. De asemenea, de ținut cont de interzicerea «dark patterns» ca posibilă pistă de nerespectare a reglementărilor legate de minimizarea colectării datelor personale.” (S10).

Înțelegerea faptului de netăgăduit că oamenii vor fi vulnerabili în mediul online al Metaversului a determinat în mod firesc adresarea întrebării următoare: *Cum pot fi prevenite și contracarate utilizările abuzive ale date-lor colectate în Metavers, astfel încât să se evite riscurile de manipulare sau alte scopuri rău intenționate?*

Răspunsurile subiecților au accentuat nevoia de clarificare și particularizare a măsurilor de control și securitate în sensul existenței unor proceduri clare de restricționare a accesului, astfel încât doar persoanele autorizate să poată accesa datele colectate în platformă (S1, S4). Aportul tehnologic pentru rezolvarea acestei probleme se regăsește în sfera tehnicilor de pseudonimizare, criptare și securitate cibernetică (S2, S3, S4, S6).

De asemenea, experții au considerat important ca utilizatorilor să le fie solicitat consimțământul într-o manieră clară, verificabilă și aferentă fiecărui tip de date colectat (S3, S4, S7) și ca aceștia să aibă posibilitatea de a-și gestiona datele (prin modificarea sau ștergerea lor), dar și de a raporta abuzul (S4, S6). S10 a atras atenția și asupra nevoii de a interzice practicile de tip *dark patterns* (manipulatoare) care ar putea determina utilizatorii să ofere date suplimentare, în mod involuntar: *Prin obligații de privacy by design, interzicerea explicită a dark patterns și supravegherea instituțională* (S10). În context, S4 a atras atenția asupra nevoii de instruire a utilizatorilor cu privire la securitatea datelor, precum și asupra importanței unui mecanism de feedback din partea utilizatorilor, unde să poată fi raportate problemele întâmpinate. Respectarea reglementărilor este un alt topic considerat important de toți experții, concomitent cu un control riguros al modului de funcționare al platformelor prin audituri periodice (S2, S3, S4, S8, S9, S10).

„Ar fi necesară utilizarea unor registre de acces și existența unor loguri care atestă acțiunile executate de respectivul utilizator. Contracararea se poate realiza prin acțiunile specifice ale Ministerului Public, care poate cerceta aspectele de infracționalitate comise și sesiza Parchetul. Procurorii sesizează instanța, în mod corespunzător, potrivit legii. Este obligatoriu să existe un cadru legal corespunzător (S9).”

Evaluările experților referitoare la instituțiile care ar trebui să fie responsabile cu protejarea datelor în Metavers la nivel național și în Uniunea Europeană au indicat, în mod special, autoritățile de protecție a datelor la nivel național - Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP) (S2, S4, S10) sau la nivel european - Autoritatea Europeană pentru Protecția Datelor (EDPS) (S2, S4, S10):

„În plan național, ANSPDCP, iar în Uniunea Europeană, aceasta ar trebui să fie gestionată de Autoritatea Europeană pentru Protecția Datelor (EDPS) și autoritățile naționale de supraveghere din statele membre (S2).”

Totodată, alți experți au menționat și autoritățile cu responsabilități pe zona de securitate cibernetică: Directoratul Național de Securitate Cibernetică (DNSC) (S1, S4, S9), Serviciul de Telecomunicații Speciale (STS) (S9), European Union Agency for Cyber Security (ENISA) (S4) și Europol (S3, S4). A existat o unanimitate a părerilor referitoare la nevoia de cooperare între instituțiile competente pentru a identifica cele mai importante dimensiuni ale protecției utilizatorilor în Metavers (S3, S4, S6, S7, S8), dar și pentru asigurarea efectivă a protecției acestora printr-un mix de responsabilitate (S10).

„Ar trebui să lucreze împreună mai multe instituții - Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal, DNSC, Ministerul Comunicațiilor și Digitalizării, European Data Protection Board, ENISA, Comisia Europeană și organisme de asigurare a aplicării legii (S4).”

Așa cum era de așteptat, aceleași instituții au fost considerate responsabile și pentru combaterea amenințărilor și riscurilor care pot apărea în Metavers (S9, S4), în paralel cu o implicare activă pe direcția creșterii capacității utilizatorilor de discriminare a atacurilor prin educație cibernetică (S2, S10): operatorii platformelor Metavers ar trebui să fie responsabilizați, iar autoritățile de protecție a datelor și ENISA pot oferi îndrumare tehnică și pot colabora cu operatorii de platforme pentru a stabili standarde de securitate adecvate (S4).

De asemenea, standardizarea și conceperea unor reglementări valabile la nivel internațional (inclusiv prin colaborarea între utilizatori și dezvoltatori) (S3, S4) sunt considerate fundamentale pentru combaterea amenințărilor și riscurilor. Referitor la riscuri, experții atrag atenția asupra faptului că în Metavers vor exista atât amenințările cibernetică de tip tradițional, precum phishing, malware, ransomware (S2, S8), cât și riscuri de natură psihologică și socială, exemple fiind manipularea comportamentală, clonarea avatarurilor, furtul de identitate (S2, S4, S10):

„Având în vedere că este vorba despre o experiență completă, riscurile pot fi audio, senzitive, psihologice sau fizice. Se lucrează, din cunoștințele mele la elaborarea unor standarde de securitate la nivel ITU” (S7).

Desigur, riscurile și amenințările sunt conforme cu tehnologiile care vor fi utilizate pentru funcționalitatea platformelor. De exemplu, dispozitivele IoT sau wearables pot fi mai vulnerabile la atacuri (S4, S6). La fel, utilizarea blockchain ar conduce la:

„...riscul compromiterii unor noduri în rețea sau al unor entități ce pot oferi diferite produse sau servicii. Tipologia celor care ar avea astfel de inițiative poate fi diversă, dar e important să ținem cont de motivație, care nu este de cele mai multe ori financiară. Poate fi de manipulare, de compromitere, ideologică, religioasă” (S5).

Referitor la întrebarea Ce drepturi ar trebui să aibă utilizatorii în Metavers pentru a controla modul în care sunt colectate, utilizate și partajate datele lor?, subiecții se referă prioritar la:

- dreptul de informare și consimțământ informat (S2, S4, S7);
- dreptul de cunoaștere a fiecărei vizualizări a datelor lor de către terți (S1, S2, S7);
- dreptul la retragerea consimțământului (S3, S4);
- dreptul de rectificare sau de ștergere (dreptul de a fi uitat) în sensul ca utilizatorii să aibă posibilitatea de a corecta informațiile și de a solicita ștergerea datelor personale (S2, S3, S4);
- dreptul de a se opune utilizării datelor proprii de către algoritmi de profilare și în decizii luate automat în baza unor astfel de analize și de a contesta, în general, utilizările abuzive ale datelor proprii (S4).

Ca o concluzie, la această întrebare, experții au fost de acord că utilizatorii ar trebui să beneficieze de aceleași drepturi de care se bucură în mediul fizic în relația cu operatorii de date cu caracter personal și cu autoritățile de supraveghere (S8).

Un capitol esențial al guvernancei datelor obținute în Metavers se referă la modul în care ar trebui să se împartă controlul datelor între diferiții stakeholders (instituții publice, entități private, utilizatori, autorități ale statului) (întrebarea 7). Răspunsurile experților includ cu precădere elemente procedurale precum nevoia unei legislații coerente (S9) și a unor protocoale clar definite pentru fiecare instituție implicată în proces, controlul asupra derulării corecte a utilizării datelor colectate și monitorizarea permanentă (S1), stabilirea bine definită a responsabilităților fiecărui operator, în acord cu cele existente în lumea fizică (S2, S3, S4, S6, S8).

„Utilizatorul să aibă dreptul la expresă și completa informare privind datele furnizate, la retragerea nemotivată și în orice moment a consimțământului în ceea ce privește deținerea/prelucrarea datelor sale, autoritățile publice să dețină pârghii de supraveghere și control eficiente, iar entitățile private, rolul de notificatori de încredere (model DSA) (S7).”

Având în vedere riscurile discutate anterior, un subiect de interes este alegerea unor reglementări potrivite pentru a garanta protejarea drepturilor unor categorii vulnerabile care pot accesa platforma, precum copii, adolescenți, minorități etnice, de gen, persoane aflate în dificultate, marginalizați etc. Unele soluții asupra cărora au insistat experții au fost: configurarea platformei astfel încât să permită identificarea utilizatorilor și clasificarea adecvată a acestora, urmată de măsuri customizate de protecție a respectivelor categorii, cu limitarea accesului la informații care ar putea fi dăunătoare (S1), crearea de zone cu conținut adecvat fiecărei categorii (S2), configurări specifice:

„Tehnologia blockchain ar permite configurarea diferențiată a accesului pentru orice tip de categorie vulnerabilă, precum și tipul de produse sau servicii ce pot fi accesate sau utilizate (S5).”

Îmbunătățirea cadrului legal existent prin definirea clară a activităților potrivite a fi derulate în mediul online și posibilitatea utilizatorilor de a raporta abuzurile au fost, la rândul lor, considerate importante de către subiecți pentru a veni în sprijinul categoriilor vulnerabile.

„Aplicând principiul minimizării datelor personale, crearea unor limite de vârstă și de utilizare pentru tineri, promovarea incluziunii în interiorul Metaversului prin crearea de servicii/produse adaptate acestor categorii, crearea unor cadre legale de raportare și monitorizare a respectării drepturilor (S10).”

Administrația publică este parte importantă din viața de zi cu zi a oamenilor și, probabil, va deveni parte importantă a viitoarei lumi virtuale Metavers. Întrebarea Cum poate administrația publică să folosească Metaversul pentru a îmbunătăți serviciile publice și participarea cetățenilor în mod etic și sigur? a primit răspunsuri diferențiate în funcție de oportunitățile pe care le-au sesizat experții care au participat la discuții. Principalele preocupări ale acestora s-au îndreptat către dimensiuni precum crearea unor platforme interactive pentru consultări publice și pentru implicarea cetățenilor în procesul de guvernare (S2), organizarea de evenimente virtuale cu accesibilitate largă a cetățenilor indiferent de categoria socială sau de localizarea geografică (S2, S3): *„se pot crea pârgii eficiente pentru integrarea unor categorii sociale mai defavorizate (economic, geografic etc) și reduce decalajul economic și social” (S7) și mergând până la părerea că „oricare dintre serviciile oferite tradițional online acum, vor putea fi oferite și în Metavers” (S3).*

Este adevărat că au existat și efecte ale iluziei de distanțare temporală determinată de o percepție a viitorului ca fiind incert și plin de obstacole, dar din care răzbate și o amărăciune a lucrurilor trenate, din păcate, în țara noastră:

„Cred că la nivel de România mai avem mult până să discutăm despre servicii publice în Metavers. Deci, e prematur pentru această întrebare. Prima dată să discutăm măcar despre o strategie de data governance și mai vedem apoi (S10).”

În privința riscurilor legate de prezența administrației publice în Metavers și referitor la modul de gestionare a acestora, experții au readus în atenție importanța unei securități cibernetice puternice, evitarea manipulării și dezinformării, dar se referă și la riscurile economice care derivă din costurile mari de implementare și, probabil, de mentenanță. Pe de altă parte, beneficiile economice și sociale sunt mari în principal din perspectiva eficienței administrative, accesibilității, transparenței sau colaborării dintre sectorul public și cel privat.

„Riscurile pot fi identificate în legătură cu securitatea cibernetică, cu discriminarea sau cu protecția datelor personale. Beneficiile s-ar putea regăsi atât în educație, în materia drepturilor fundamentale (creșterea accesului la curțile de judecată internaționale), a dreptului la sănătate, a dreptului muncii (acces extins la locuri de muncă), a dreptului penal (extinderea, de ex., a supravegherii Europol) etc. (S7).”

Existența unor politici și reglementări clare care să permită echilibrarea riscurilor și beneficiilor ar putea fi o soluție pentru utilizarea unei astfel de platforme în administrația publică.

„Gestionarea riscurilor și beneficiilor se poate realiza prin angajarea specialiștilor. Prezența administrației publice în Metavers este aducătoare de mari beneficii economice și sociale, acesta fiind trendul de evoluție al societății (S9).”

Concluzii și recomandări

Studiul realizat cu experții din administrația publică a reliefat faptul că viitoarea platformă Metavers va reprezenta o provocare, nu doar din perspectiva implementării sau efectelor sociale pe care le va produce, cât și pentru maniera în care va redimensiona caracteristicile administrației publice. Toți experții implicați au fost de acord că existența acesteia va însemna modificări de substanță ale caracteristicilor administrației publice și că modul în care va fi concepută guvernanta acestei platforme reprezintă poate cel mai important pas pentru atingerea obiectivelor de eficiență a administrației publice.

Guvernanța va trebui să fie una flexibilă și adaptată noilor nevoi generate, de un mediu imersiv în totalitate nou, dar axată pe principii precum transparența, securitatea, respectul pentru confidențialitatea datelor utilizatorilor și pe drepturile acestora. Necesitatea de a implementa reguli clare și responsabilități bine definite referitoare la colectarea, stocarea și utilizarea datelor, mai ales că acestea pot fi senzoriale și biometrice, a fost accentuată în mod repetat de către experții implicați.

Participanții au considerat utilă valorificarea legislației actuale, precum GDPR, în contextul Metavers, dar nu au exclus și formularea unor texte legislative noi, care

să fie valabile la nivel internațional, nu doar în România sau Uniunea Europeană. Deoarece Metaversul este un spațiu virtual global, este importantă coordonarea transfrontalieră și implementarea standardelor comune prin colaborarea dintre țări.

Prevenirea utilizărilor abuzive ale datelor în Metavers trebuie să se concentreze pe măsuri proactive, inclusiv tehnologii de criptare avansată, monitorizare continuă și audituri de securitate, pentru a evita riscurile de manipulare sau abuz. De asemenea, este esențial ca autoritățile naționale și europene să colaboreze cu platformele din Metavers pentru a stabili un cadru de sancțiuni și măsuri corective rapide împotriva celor care încalcă reglementările. Drepturile utilizatorilor în Metavers ar trebui să fie bine definite și adaptate pentru acest mediu virtual, incluzând accesul și controlul asupra datelor personale, dreptul de a solicita ștergerea datelor, transparență totală cu privire la metodele de colectare și utilizare a datelor și protecție sporită pentru categoriile vulnerabile. Controlul datelor ar trebui să fie împărțit în mod echitabil între stakeholderi, cu garanții clare pentru utilizatori și măsuri de supraveghere strictă din partea autorităților. Aceste inițiative vor contribui la construirea unei structuri de încredere și responsabilitate în Metavers, încurajând utilizarea sigură și etică a tehnologiilor imersive.

Desigur, acest studiu este unul explorativ și principala constrângere a prezentei cercetări derivă din organizarea unui singur focus-grup din considerente derivate preponderent din dificultatea identificării experților potriviți pentru evaluări pe acest subiect. Aducerea în discuție a rezultatelor oferite în mai multe runde de discuții ar putea nuanța opiniile prezentate cu această ocazie. La fel, o altă dinamică de grup ar putea determina aprofundări ale unor subiecte conexe. Dincolo de aceste aspecte, experții au permis identificarea unor preocupări de interes pentru domeniul guvernantei în Metavers, pe care intenționăm să le aprofundăm prin studii suplimentare și prin propunerea unui draft de White paper privind guvernarea datelor în Metavers.

4. Ar putea fi Metaversul o soluție pentru orașele inteligente?

În contextul urbanizării accelerate și al imperativului eficienței, conceptul de „oraș inteligent” (smart city) s-a impus ca un model proeminent al dezvoltării urbane contemporane. Aceste metropole, fundamentate pe interconectivitatea tehnologică și pe analiza datelor, au ca obiectiv optimizarea calității vieții, creșterea siguranței și promovarea sustenabilității pentru cetățeni.

Simultan, un alt concept de mare anvergură tehnologică, Metaversul, a intrat în prim-planul discursului tehnologic. Definit ca un univers virtual persistent, în care interacțiunile umane sunt mediate de avataruri și de tehnologii imersive precum realitatea augmentată, Metaversul este frecvent teoretizat ca fiind următoarea etapă evolutivă a internetului.

În acest context, devine pertinentă și tot mai presantă tema privind posibila convergență a acestor două viziuni asupra viitorului. Ar putea Metaversul, prin potențialul său imersiv și interconectat, să ofere soluții viabile la provocările sistemice cu care se confruntă orașele inteligente? Analiza acestei probleme este complexă, cu multe nuanțe, implicând o evaluare critică a beneficiilor potențiale în raport cu obstacolele tehnice, etice și de guvernare.

Tranziția orașelor către neutralitatea climatică

În ultimele decenii, orașele s-au impus ca motoare ale dezvoltării economice și sociale, atrăgând investiții substanțiale, o forță de muncă diversificată și stimulând creativitatea. Din ce în ce mai multe companii își mută sediile în marile centre urbane, contribuind la creșterea numărului de locuri de muncă și la diversificarea industriilor. De asemenea, migrarea rapidă a populației către orașe oferă oportunități multiple în domenii precum tehnologia, cercetarea sau serviciile financiare.

Totuși, pe fondul acestor evoluții remarcabile, devine tot mai evident faptul că dezvoltarea necontrolată și consumul masiv de resurse exercită presiuni considerabile asupra mediului înconjurător. Un factor determinant al acestei presiuni îl constituie schimbările climatice, a căror intensitate și frecvență a efectelor sunt tot mai evidente. Fenomene meteorologice extreme – canicule prelungite, inundații devastatoare sau furtuni violente – afectează regiunile urbane cu o intensitate fără precedent, punând în pericol atât infrastructura, cât și sănătatea locuitorilor.

Principala sursă de poluare în zonele metropolitane o reprezintă emisiile provenite din transport, industrie și producerea de energie. Creșterea numărului de autovehicule a dus la amplificarea congestiilor rutiere și, implicit, la sporirea emisiilor

de dioxid de carbon. În același timp, industriile care se dezvoltă în apropierea zonelor urbane folosesc, de multe ori, tehnologii învechite și resurse fosile, contribuind suplimentar la degradarea calității aerului. Această problemă devine cu atât mai îngrijorătoare cu cât există o cerere crescândă de produse și servicii într-un context urban aflat în expansiune rapidă. Conform datelor IPCC (Intergovernmental Panel on Climate Change)¹, aproximativ 70% din emisiile globale de gaze cu efect de seră provin din mediul urban, astfel încât orașele nu mai pot ignora responsabilitatea pe care o au în atingerea obiectivului mondial de neutralitate climatică².

În acest context, tot mai multe localități caută să adopte strategii menite să reducă emisiile și să îmbunătățească calitatea vieții urbane. Exemple de bune practici în acest sens pot fi Copenhaga, recunoscută pentru rețeaua extinsă de piste pentru bicicliști și proiectele de energie regenerabilă, Singapore, care își propune să devină un „oraș inteligent” prin implementarea sistemelor Internet of Things (IoT), și Vancouver, cu ambiția sa de a fi cea mai „verde” metropolă din lume. Dar totul se bazează pe noile tehnologii digitale și gestionarea inteligentă a datelor. Prin colectarea de informații din surse diverse, de la niveluri de trafic și consum energetic până la calitatea aerului și feedback-ul locuitorilor, autoritățile pot lua decizii bazate pe argumente solide, concentrând resursele în zonele cu impact maxim asupra mediului și a populației.

În continuare, vor fi analizate principalele provocări cu care se confruntă orașele fiind evidențiate diverse exemple de bune practici care pot contribui la dezvoltarea sustenabilă a acestora. Discuția va fi structurată în patru direcții-cheie:

- Transportul – modul în care orașele pot trece de la un trafic intens și poluant la soluții de mobilitate verde, accesibile și eficiente;
- Clădirile – consumul energetic al infrastructurii urbane și potențialul major de reducere a emisiilor prin metode de eficientizare și modernizare;
- Gestionarea resurselor – provocările legate de apă, energie și alte resurse vitale, precum și soluțiile inovatoare care pot asigura o utilizare mai responsabilă și mai durabilă a acestora;
- Guvernanța datelor – importanța colectării și analizării eficiente a informațiilor, pentru a fundamenta deciziile și a implementa politici urbane cu impact real.

¹ IPCC (2018), *Global Warming of 1.5 °C*, Disponibil la: <https://www.ipcc.ch/sr15/> [Accesat: 19 Aug. 2025].

² United Nations (2024), *Net Zero Coalition*, Publisher: United Nations, Disponibil la: <http://www.un.org/en/climatechange/net-zero-coalition> [Accesat: 19 Aug. 2025].

Transportul – de la trafic intens la mobilitate verde

În multe orașe, transportul rămâne principala sursă de emisii poluante. Mașinile personale, flotele de autobuze diesel și traficul de marfă au o contribuție majoră la poluarea atmosferică.

Transportul, fiind un element vital al oricărei comunități, influențează direct modul în care oamenii locuiesc, muncesc și își petrec timpul liber. O mobilitate verde, susținută de infrastructuri digitale ar putea fi catalizatorul unei transformări mai ample, care să îmbunătățească inclusiv sănătatea publică, coeziunea socială și reziliența orașelor în fața efectelor schimbărilor climatice. Idealul către care tind majoritatea orașelor care își propun neutralitatea climatică este acela a unui mediu urban unde cetățenii se deplasează rapid și în siguranță, având la dispoziție multiple opțiuni nepoluante, unde aerul este curat, iar spațiile verzi abundă, unde tehnologia simplifică procesele de planificare și utilizare a serviciilor, și unde, în cele din urmă, cetățenii nu mai sunt constrânși de traficul intens, ci se bucură de libertatea oferită de o mobilitate cu adevărat sustenabilă.

Un exemplu în acest sens poate fi considerat Oslo, în Norvegia, care a investit masiv în infrastructură pentru vehicule electrice și a implementat un „buget climatic” anual³. Prin această inițiativă, autoritățile stabilesc obiective de reducere a emisiilor

³ Oslo City Council (2024), *Climate Budget 2024*, Disponibil la: <https://www.klimaoslo.no/wp-content/uploads/sites/2/2024/08/Climate-budget-2024.pdf> [Accesat: 19 Aug. 2025].

pentru fiecare sector, inclusiv transportul, și monitorizează constant progresul. Oslo a devenit unul dintre orașele cu cea mai mare rată de adopție a mașinilor electrice din lume. Stațiile de încărcare sunt răspândite în tot orașul, iar taxele și subvențiile sunt gândite pentru a face trecerea la vehicule nepoluante cât mai atrăgătoare pentru locuitori. Un alt exemplu este Copenhaga⁴, care și-a propus să devină primul oraș neutru din punct de vedere al carbonului până în anul 2025. Transportul pe bicicletă este parte integrantă a vieții de zi cu zi, cu piste extinse și servicii de închiriere accesibile. Și în acest caz, provocarea rămâne în continuare gestionarea traficului rutier și tranziția către autobuze electrice sau alimentate cu biogaz. Astfel, un sistem complex de colectare și analiză a datelor despre rutele cele mai aglomerate, orele de vârf și preferințele cetățenilor pentru anumite moduri de transport face diferența între o simplă intenție și o transformare reală. Cu toate acestea, o tranziție eficientă se bazează întotdeauna pe analiza datelor din diverse sectoare de activitate, fie că vorbim despre fluxurile de trafic, consumul de energie sau gradul de ocupare a parcarilor. O gestionare eficientă și securizată a informațiilor asigură o direcționare eficientă a investițiilor în infrastructura verde.

În Berlin, de exemplu, administrația locală a inițiat proiecte de colectare a datelor despre traficul rutier și fluxurile de navetiști, pentru a putea identifica exact zonele cele mai congestionate și intervalele orare în care apar blocajele majore⁵. Analiza acestor date a dus la optimizarea rețelei de transport, cu accent pe dezvoltarea de rute prioritare pentru autobuze electrice și tramvaie, precum și pe îmbunătățirea accesului la metrou în zone rezidențiale slab deservite. În Hamburg, un alt oraș german cu ambiții în materie de sustenabilitate, conceptul de „mobilitate ca serviciu” începe să se contureze prin dezvoltarea unor platforme integrate, unde cetățenii pot alege și combina diverse opțiuni de transport – autobuze, trenuri regionale, trotinete electrice, un sistem de biciclete partajate – astfel încât să găsească soluția de deplasare potrivită fiecărei situații, în același timp contribuind la reducerea emisiilor totale⁶.

Strategiile urbane orientate către neutralitate climatică au început să se extindă și dincolo de marile capitale sau metropole. De pildă, în orașe precum Graz (Austria), Utrecht (Olanda) ori Freiburg (Germania), abordarea durabilă a transportului nu este doar un concept teoretic, ci un plan concret care vizează limitarea accesului vehiculelor poluante în zonele centrale și transformarea locurilor de parcare stradală în spații verzi ori piste pentru biciclete. Odată cu aceste inițiative, dispare progresiv

⁴ Technical and Environmental Administration, City of Copenhagen (2025), *The CPH 2025 Climate Plan | Urban Development*, Disponibil la: <https://urbandevelopmentph.kk.dk/climate> [Accesat: 19 Aug. 2025].

⁵ VMZ Berlin (2025), *Traffic Planning and Consulting – VMZ Berlin*, Disponibil la: <https://www.vMZberlin.com/kompetenzbereiche/verkehrsplanung/> [Accesat: 19 Aug. 2025].

⁶ Hamburg Invest (2025), *Transport and mobility in Hamburg | Hamburg Business*, Disponibil la: <https://hamburg-business.com/en/future-hamburg/mobility-traffic> [Accesat: 19 Aug. 2025].

dependența de mașinile personale, iar transportul public este regândit pentru a fi mai accesibil, mai frecvent și mai prietenos cu mediul. Freiburg, de exemplu, a mizat pe implementarea unor linii de tramvai moderne, alimentate cu energie verde, care să străbată cartiere nou-construite, proiectate astfel încât locuitorii să nu fie nevoiți să folosească zilnic automobilul⁷.

În orașe-port precum Rotterdam sau Anvers, logistica de transport a bunurilor este o parte importantă a economiei locale și regionale. În acest caz, obiectivele de neutralitate climatică pot fi atinse prin soluții de transport ce permit conectarea navelor electrice sau cu hidrogen cu trenuri de marfă și vehicule de livrare nepoluante. O gestionare inteligentă a datelor despre traseele de livrare, orele de descărcare și consumul energetic conduce către diminuarea traficului și evitarea emisiilor poluante inutile.

Electrificarea masivă a flotelor de transport are sens doar dacă energia provine, pe cât posibil, din surse regenerabile, precum eoliana, solară sau hidroelectrică. În Norvegia, unde producția de electricitate se bazează preponderent pe hidrocentrale, tranziția către mașini electrice a fost naturală, iar Oslo a beneficiat din plin de acest avantaj, reușind să reducă într-un mod substanțial amprenta de carbon a sectorului de transport. Alte orașe însă, care încă depind de cărbune sau gaze naturale pentru generarea electricității, se confruntă cu un efect de tip „deplasare a emisiilor”, în care poluarea este mutată din zona urbană spre zonele unde sunt amplasate centralele electrice.

În plus, merită amintite și eforturile de reducere a necesității de transport prin reconfigurarea spațiului urban. Conceptul de „oraș de 15 minute”, promovat în special în Paris⁸, dar și în alte părți ale lumii, urmărește să ofere locuitorilor acces facil la majoritatea serviciilor de bază (sănătate, educație, aprovizionare) în apropierea locuinței, pentru ca aceștia să nu mai fie nevoiți să se deplaseze zilnic pe distanțe lungi. Transportul public și infrastructura pentru mersul pe jos ori cu bicicleta devin coloana vertebrală a mobilității urbane, în timp ce mașinile private sunt folosite mult mai rar, pentru deplasări specifice sau pentru cei care au nevoie reală de ele. O asemenea restructurare urbană presupune o planificare complexă care să implice arhitecți, urbaniști, sociologi și economiști, toate deciziile fiind ghidate de date și de analize preliminare asupra comportamentului populației și a fluxurilor de mobilitate existente. Evident, există și provocări: implementarea orașului de 15 minute poate duce la creșterea prețului locuințelor din zonele bine conectate și la

⁷ European Bank for Reconstruction and Development (2024), *Incentives to use public and active transport: Freiburg, Germany – EBRD*, Disponibil la: <https://www.ebrdgreencities.com/policy-tool/incentives-to-use-public-and-active-transport-freiburg-germany-2/> [Accesat: 19 Aug. 2025].

⁸ Brecht M. (2025), *How 15-Minute City Paris Became the Role Model for Urban Transformation* | MOTION Magazine | *Electric Mobility Lifestyle*, Disponibil la: <https://www.motion-mag.com/articles/how-15-minute-city-paris-became-the-role-model-for-urban-transformation> [Accesat: 19 Aug. 2025].

riscul de gentrificare, ceea ce demonstrează încă o dată că tranziția climatică trebuie întotdeauna privită prin lentilele sociale și economice, evitând concentrarea exclusivă pe componenta tehnologică.

Dincolo de granițele Europei, orașe precum Seul, Singapore sau Vancouver experimentează, de asemenea, politici avansate de mobilitate durabilă, în care digitalizarea, inteligența artificială și tehnologiile IoT transformă felul în care se planifică și se administrează infrastructura de transport. În Seul, s-au introdus benzi rutiere inteligente, dotate cu senzori care transmit în timp real informații despre gradul de ocupare și viteza de rulare, iar inteligența artificială reglează semafoarele pentru a minimiza blocajele⁹. În Vancouver, progresul se vede în investițiile masive în rețeaua de transport public SkyTrain¹⁰, care operează cu trenuri automate, alimentate cu electricitate curată provenită din hidrocentrale, și în proiectele de dezvoltare a infrastructurii pentru biciclete. Mai mult, autoritățile colaborează cu diverse startup-uri pentru a introduce vehicule autonome de mici dimensiuni, care pot asigura livrări rapide în zonele centrale, eliminând astfel necesitatea folosirii camioanelor clasice pe drumuri scurte și aglomerate.

Nu trebuie uitată dimensiunea socială a acestor transformări, căci nu toate categoriile de cetățeni au acces la tehnologii noi sau au abilitățile necesare pentru a adopta alternative durabile de transport. Unele orașe au introdus stimulente sub forma unor abonamente de transport public la prețuri reduse ori a unor scheme de tip „bike to work”, prin care angajații primesc beneficii financiare dacă aleg mersul pe bicicletă în locul autoturismului. Pentru ca astfel de inițiative să aibă impact real, autoritățile trebuie să colaboreze cu angajatorii, cu organizațiile comunitare și cu cetățenii înșiși, creând mecanisme de feedback și participare civică. Modelul de guvernare locală devine relevant, deoarece deciziile privind infrastructura de transport nu mai pot fi luate doar de un grup restrâns de experți, ci necesită consultări publice și analize multidisciplinare care să includă mediul academic, sectorul privat și societatea civilă.

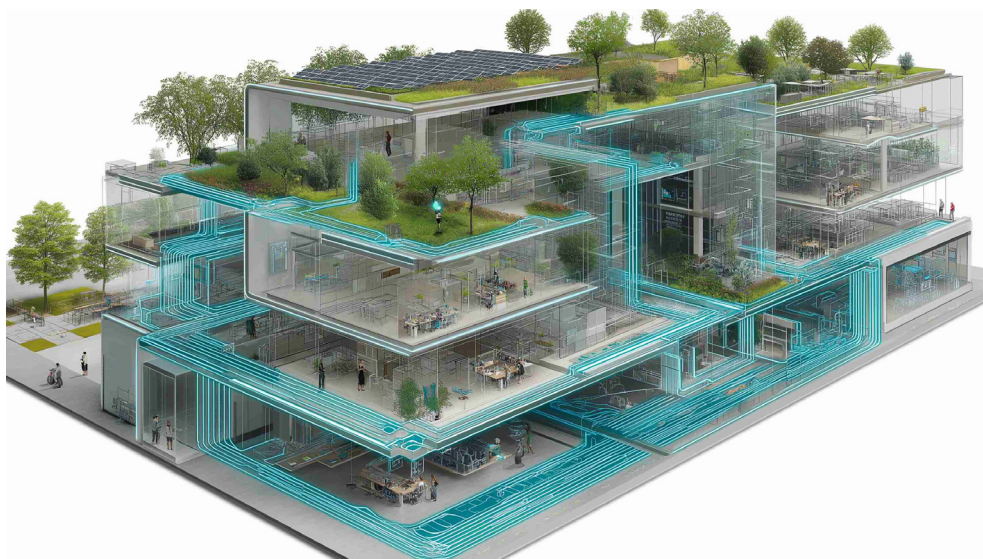
Datele și tehnologiile digitale oferă fundația pe care se pot construi politici coerente și bine fundamentate. De la simplele contoare de trafic rutier și până la sisteme avansate de monitorizare a calității aerului și a zgomotului, orașele colectează o cantitate impresionantă de informații care pot fi folosite pentru a modela scenariul viitoare, a prognoza cererea de transport și a evalua riscurile asociate cu schimbările climatice. În plus, platformele de tip open data permit dezvoltatorilor independenți să creeze aplicații și servicii utile pentru cetățeni, precum planificatoare de rute personalizate, instrumente de tip „car-sharing” și soluții de micro-mobilitate. Dar, pentru a asigura

⁹ Kavipriya (2023), *Seoul unveils smart intersection testbed to enhance urban mobility – Telematics Wire*, Disponibil la: <https://telematicswire.net/seoul-unveils-smart-intersection-testbed-to-enhance-urban-mobility/> [Accesat: 19 Aug. 2025].

¹⁰ Green City Times (2017), *What are Transit Options in Vancouver?*, Disponibil la: <https://www.greencitytimes.com/vancouver-alternative-transit/> [Accesat: 19 Aug. 2025].

eficiența unor astfel de abordări, trebuie să existe un cadru clar de guvernare a datelor, care să stabilească cine colectează informațiile, cum sunt ele stocate, cine le poate utiliza și în ce scop. În absența unei reglementări adecvate, există riscul ca datele sensibile să fie folosite abuziv sau ca anumite companii să dețină monopol asupra fluxurilor informaționale, distorsionând astfel piața și limitând inovația.

Clădirile – consum energetic și potențial de reducere



Orașele nu poluează doar prin transport, ci și prin clădiri ineficiente energetic. Conform C40 Cities (rețea globală de orașe care colaborează pentru reducerea emisiilor, clădirile sunt responsabile pentru până la 50-60% din emisiile directe și indirecte de gaze cu efect de seră în marile metropole¹¹, iar o mare parte a acestor emisii provine din încălzire, răcire și iluminat. Doar prin procese complexe de modernizare, prin implementarea senzorilor și a platformelor digitale de management, prin sancționarea ineficienței și răsplătirea comportamentelor responsabile, orașele pot reduce considerabil poluarea și își pot consolida reziliența în fața provocărilor tot mai mari legate de climă și de costurile energetice.

Un caz de succes este Vancouver, Canada, care a lansat „Greenest City Action Plan”, un proiect ambițios care include modernizarea clădirilor existente și

¹¹ C40 Cities (2025), *C40 Cities - A global network of mayors taking urgent climate action*, Disponibil la: <https://www.c40.org/> [Accesat: 19 Aug. 2025].

standarde stricte pentru cele nou construite¹². Prin colectarea și analizarea datelor despre consumul de energie al fiecărei clădiri publice, administrația a putut identifica prioritățile de modernizare: izolarea termică, ferestre cu eficiență sporită, sisteme de încălzire bazate pe pompe de căldură și, nu în ultimul rând, folosirea surselor regenerabile de energie.

Alte exemple de măsuri se referă la monitorizarea consumului de curent electric la nivel de cartier, compararea între tipuri de clădiri și introducerea unor tarife diferențiate pentru energie în funcție de orele de consum^{13,14}. Centralizarea informațiilor din diverse surse – companii de utilități, proprietari de imobile, date meteo, au condus la soluții adaptate la nevoile reale ale locuitorilor. Marile metropole investesc tot mai mult în infrastructuri digitale care să permită colectarea și procesarea rapidă a datelor despre consum. Clădirile inteligente folosesc platforme de tip IoT pentru a trimite informații continue către un centru de comandă, unde algoritmi de învățare automată pot analiza tiparele de consum și pot recomanda ajustări fine ale sistemelor de climatizare sau iluminat. Prin senzori și sisteme de monitorizare în timp real, administrațiile pot descoperi unde se pierd cele mai mari cantități de căldură, cum pot fi reglate automat nivelurile de iluminat în funcție de lumina naturală ori cum pot fi sincronizate instalațiile de răcire și de încălzire cu comportamentul real al ocupanților. Astfel, o clădire devine capabilă să reacționeze aproape instant la modificările de temperatură exterioară sau la creșterea numărului de persoane dintr-un spațiu, reducând consumul inutil de energie și oferind totodată un nivel adecvat de confort.

Pe lângă investițiile în soluții tehnologice, sunt necesare politici publice clare și coerente, care să stabilească standarde minime de eficiență energetică pentru toate imobilele, fie ele rezidențiale, comerciale sau industriale. În unele locuri, se aplică obligativitatea unor audituri energetice periodice, iar proprietarii care nu își modernizează clădirile în termenul impus riscă amenzi sau penalități. În altele, administrația locală preferă stimulentele financiare – subvenții, credite cu dobândă redusă sau reduceri de impozite – pentru cei care aleg să investească în izolație termică, în sisteme moderne de încălzire ori în instalarea de panouri fotovoltaice. Vancouver a reușit să combine ambele abordări, deopotrivă presând sectorul construcțiilor să respecte standarde de sustenabilitate și oferind beneficii notabile

¹² City of Vancouver (2012), *Greenest City 2020 Action Plan - the City's Sustainability Plan*, Disponibil la: <https://vancouver.ca/files/cov/greenest-city-action-plan.pdf> [Accesat: 19 Aug. 2025].

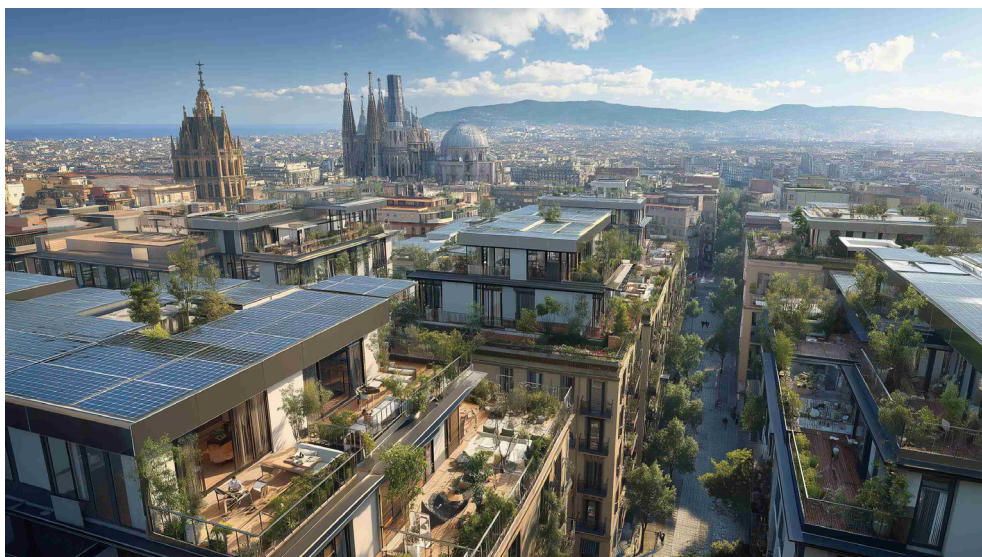
¹³ Environment Bureau (2015), *Energy Saving Plan for Hong Kong Built Environment*, Disponibil la: <https://www.eeb.gov.hk/sites/default/files/pdf/EnergySavingPlanEn.pdf> [Accesat: 19 Aug. 2025].

¹⁴ Bourbonnais Cecile A. F. (2020), *Time of Use Rates: An International Perspective*, Disponibil la: <https://energyregulationquarterly.ca/articles/time-of-use-rates-an-international-perspectives> [Accesat: 19 Aug. 2025].

celor care adoptă imediat noile directive, iar rezultatele se văd deja în scăderea treptată a emisiilor provenite din clădiri.

Un alt aspect important constă în modul în care orașele pot integra eficiența energetică a clădirilor cu politica de dezvoltare urbană și de planificare teritorială. Unele inițiative vizează, de pildă, crearea unor cartiere noi proiectate de la zero pentru a fi eficiente energetic, folosind concepte de oraș inteligent și principii de design bioclimatic. Acolo, clădirile sunt orientate astfel încât să valorifice la maximum lumina naturală și să reducă nevoia de încălzire pe timp de iarnă ori de răcire pe timp de vară, folosesc plante și materiale ecologice pentru fațade și sisteme de colectare și reutilizare a apei pluviale. Însă, chiar și în cartierele vechi, există potențial ridicat de reducere a emisiilor prin modernizarea așa-numitului stoc de clădiri existente, care adesea suferă de pierderi masive de căldură și de un consum exagerat de electricitate. În acest proces, analiza datelor colectate prin comparații sistematice ale performanțelor energetice înainte și după lucrările de renovare, pot identifica practicile cele mai eficiente și abordări replicabile la scară largă.

Gestionarea resurselor: provocări și soluții inovatoare



Tranziția orașelor către neutralitate climatică înseamnă mai mult decât adoptarea unor tehnologii avansate: este necesară inclusiv o remodelare completă a modului în care se gestionează resursele naturale, se produce și se consumă energie

și se asigură hrană pentru populația în continuă creștere. Schimbările climatice, urbanizarea rapidă și obiectivul general de a atinge neutralitatea climatică până la jumătatea secolului obligă administrațiile locale, sectorul privat și comunitățile să caute noi soluții. În acest proces, datele joacă un rol cheie, întrucât permit anticiparea și gestionarea crizelor, optimizarea fluxurilor de apă și energie și reorganizarea sistemului alimentar.

Exemplele concrete din diferite orașe evidențiază modul în care aceste provocări sunt abordate și arată că succesul depinde de strategiile integrate și de participarea tuturor actorilor implicați.

Gestionarea apei a devenit una dintre cele mai stringente probleme, așa cum s-a văzut în Cape Town, când autoritățile au avertizat locuitorii despre „Day Zero”, ziua în care robinetele urmau să fie închise din cauza secetei¹⁵.

Cu o populație de peste patru milioane de oameni, regiunea, altădată renumită pentru peisajele sale și turismul prosper, a intrat într-o criză acută de aprovizionare cu apă din cauza secetei prelungite și a creșterii cererii. Autoritățile au reacționat prin măsuri drastice de raționalizare, reducând timpul petrecut la duș la 90 de secunde și încurajând reciclarea apei pentru diverse activități domestice. Un factor decisiv a fost infrastructura de monitorizare, bazată pe senzori care transmiteau în timp real informații despre nivelurile din baraje și rezervoare, astfel încât administrația să poată impune restricții diferențiate și să ofere populației o imagine clară asupra situației. Datele au fost integrate într-o platformă comună, unde sectorul public, companiile private și ONG-urile puteau corela informații despre consum, infrastructură și prognoze meteo. Deși Cape Town a evitat în ultima clipă dezastrul, a lăsat lumii întregi un avertisment privind fragilitatea resurselor de apă, chiar și în zone care nu păreau expuse în mod tradițional secetei.

Singapore, ilustrează modul în care limitările geografice pot determina generarea soluții tehnologice inedite: insula-oraș-stat cu resurse de apă reduse a dezvoltat programul NEWater¹⁶, bazat pe microfiltrare, osmoză inversă și tratarea cu raze ultraviolete pentru a transforma apa uzată în apă potabilă. Informațiile colectate permanent permit ajustări fine în tratare și în aprovizionare, asigurând un grad ridicat de independență față de importurile de apă.

Energia reprezintă un alt pilon de bază, având în vedere că orice creștere urbană vine la pachet cu o cerere sporită. În trecut, majoritatea localităților depindeau de combustibili fosili, dar tranziția energetică spre surse regenerabile capătă amploare și pune accent pe orașele inteligente, care folosesc contoare și rețele de distribuție

¹⁵ Baker A. (2018), *I Knew We Were in Trouble. 'What It's Like to Live Through Cape Town's Massive Water Crisis*, Disponibil la: <https://time.com/cape-town-south-africa-water-crisis/> [Accesat: 19 Aug. 2025].

¹⁶ Singapore's National Water Agency (2024), *NEWater*, Disponibil la: <https://www.pub.gov.sg/Public/WaterLoop/OurWaterStory/NEWater> [Accesat: 19 Aug. 2025].

capabile să comunice între ele. Barcelona a adoptat micro-rețelele urbane¹⁷, instalând panouri fotovoltaice pe clădiri publice și stimulând cetățenii să devină prosumatori, adică atât producători, cât și consumatori de energie. Toate datele referitoare la producție și consum sunt centralizate digital, astfel încât surplusul dintr-un cartier poate fi redirecționat către zonele cu cerere mai mare. O atare flexibilitate, bazată pe fluxuri de date corelate cu precizie, contribuie la stabilitatea rețelei și sporește reziliența în fața penelor de curent. În plus, locuitorii participă direct prin instalarea de panouri solare și utilizarea contoarelor inteligente, aspect care îi apropie de dinamica energetică a orașului. De asemenea, componentele de tip „smart home” optimizează în timp real consumul din locuințe, gestionând eficient termostatele, electrocasnicele și încărcarea mașinilor electrice pentru un consum echilibrat și sustenabil.

După apă și energie, alimentele sunt a treia resursă esențială pentru orașele mari, care sunt de obicei foarte dependente de importuri. Orașele dens populate pot suferi rapid dezechilibre în situații de criză. Singapore, neavând teren agricol, a inovat din nou prin ferme verticale¹⁸, unde legumele și fructele sunt cultivate hidroponic sau acvaponic în medii închise și controlate.

Pe verticală se pot obține recolte impresionante într-un spațiu restrâns, cu consum redus de apă și energie, grație senzorilor care monitorizează parametrii de creștere și algoritmi de inteligență artificială care ajustează lumina și nutriția. Rata ridicată de productivitate și scăderea drastică a risipei asigură orașului o bună parte din consumul alimentar de bază, diminuând dependența de importuri.

La polul opus, Detroit a pierdut masiv din populație odată cu declinul industriei auto, rămânând cu mari terenuri abandonate. Acestea au devenit însă suportul pentru grădini comunitare¹⁹ în care locuitorii produc hrană proaspătă și refac legătura dintre oameni și pământ. Date despre tipurile de culturi, calitatea solului și volumul recoltelor sunt colectate și folosite pentru planificare. Grădinile funcționează ca un spațiu de socializare și schimb de cunoștințe și îi ajută pe oameni să se unească în jurul unui scop comun. Chiar dacă tehnologiile nu sunt la fel de sofisticate ca în Singapore, implicarea comunitară și monitorizarea resurselor transformă inițiativele în proiecte de succes.

În toate aceste exemple, datele joacă un rol central. Autoritățile, companiile private, ONG-urile și cetățenii trebuie să colaboreze astfel încât datele să fie folosite în mod transparent, securizat și responsabil. În plus, politicile publice trebuie să ofere un cadru legislativ și fiscal adecvat, cu standarde stricte de securitate cibernetică, reglementări privind anonimizarea datelor și protocoale de partajare.

¹⁷ Barcelona Energia (2025), *Strategy for energy transition | Urban Planning, Ecological Transition, Urban Services and Housing*, Disponibil la: <https://ajuntament.barcelona.cat/ecologiaurbana/en/what-we-do-and-why/energy-and-climate-change/strategy-energy-transition> [Accesat: 19 Aug. 2025].

¹⁸ SFA (2024), *Singapore Food Agency*, Disponibil la: <https://www.sfa.gov.sg/> [Accesat: 19 Aug. 2025].

¹⁹ Detroit Future City (2024), *Detroit Future City: Think Tank, Policy Advocate, Innovation Engine*, Disponibil la: <https://detroitfuturecity.com/> [Accesat: 19 Aug. 2025].

Colaborarea intersectorială este necesară, mai ales la nivel financiar, deoarece dezvoltarea de rețele de apă inteligente, micro-rețele energetice sau ferme verticale necesită investiții mari și expertiză tehnică avansată. Comunicarea transparentă, așa cum s-a întâmplat în Cape Town, are puterea de a mobiliza comunități întregi, iar inițiativele de grădini urbane din Detroit demonstrează cum angajarea cetățenilor poate genera coeziune socială. Prin educație, locuitorii înțeleg mai bine implicațiile propriilor acțiuni, sunt dispuși să economisească apă, să-și instaleze panouri solare sau să cultive produse locale. Politicile publice au rolul de a stabili și a veghea la respectarea regulilor jocului: standarde de eficiență energetică pentru clădiri noi, subvenții pentru energii regenerabile, facilități fiscale pentru instalarea de panouri fotovoltaice, impunerea unor norme de economisire a apei și programe de sprijin pentru agricultura urbană. Lecțiile din Cape Town, Singapore, Barcelona și Detroit confirmă faptul că orașele pot trece de la vulnerabilitate la reziliență printr-o abordare integrată, în care se îmbină cercetarea științifică, finanțarea adecvată, parteneriatele durabile și, mai ales, implicarea efectivă a locuitorilor

Guvernanța datelor – puntea dintre inovație și rezultate concrete



Indiferent că vorbim despre vehicule electrice, clădiri „verzi” sau sisteme de reciclare performante, toate inițiativele de reducere a emisiilor de gaze cu efect de seră au la bază colectarea și analiza unor volume uriașe de informații. Guvernanța datelor asigură că aceste date sunt fiabile, securizate și utilizate în mod etic.

În inițiativele C40 Cities, de exemplu, există platforme comune de partajare a datelor între orașe, astfel încât fiecare să poată învăța din experiența celuilalt²⁰. Totuși, pentru ca aceste informații să fie utile, e nevoie de standarde și protocoale clare: cum se colectează datele, cine are acces la ele, în ce formate sunt stocate și cum se respectă confidențialitatea cetățenilor. Fără o guvernare consistentă, datele riscă să devină fie redundante, fie contradictorii.

De la sistemele inteligente de distribuție a apei în Cape Town sau Singapore, până la rețelele micro-grid din Barcelona, toate presupun gestionarea unor seturi uriașe de date. În absența unui cadru clar de guvernare, aceste date ar putea rămâne fragmentate sau subutilizate, pierzându-se oportunități majore de eficientizare și inovare. Mai mult, aspectele legate de confidențialitate și securitate trebuie integrate de la bun început în proiecte, pentru a menține încrederea publicului.

De asemenea, un plan ambițios de reducere a emisiilor urbane nu poate avea succes fără implicarea locuitorilor. În Suedia, spre exemplu, compania Svalna a lansat o aplicație pentru dispozitive mobile prin care cetățenii sunt încurajați să afle, în timp real, cum le afectează transportul sau consumul de energie amprenta de carbon, transformând astfel datele complexe în grafice și indicatori ușor de înțeles, generând un sentiment de responsabilitate personală²¹.

Fiecare dintre exemplele discutate ilustrează, la nivel practic, faptul că locuitorii orașelor joacă un rol hotărâtor în gestionarea resurselor. Nu este suficient ca administrațiile să elaboreze strategii și să investească în infrastructură dacă mentalitatea generală rămâne aceea a consumului nechibzuit.

În Cape Town, populația a fost nevoită să se implice activ prin măsuri radicale de economie a apei. În Copenhaga, alegerea transportului public sau a bicicletei este mai degrabă o normă socială decât o obligație. La Detroit, grădinile comunitare au readus speranță și apartenență, implicându-i pe cetățeni în producția alimentară locală.

Inițiativele de tip „open data” sau platformele de tip „civic tech” pot contribui la creșterea transparenței și la stimularea implicării cetățenilor. Când oamenii au acces la informații despre cum este folosită apa, câtă energie se consumă în cartierul lor sau care este sursa alimentelor din magazine, devin mai conștienți și, implicit, mai responsabili. Tehnologii emergente precum Metaversul pot fi folosite și în scop educațional, permițându-le locuitorilor să exploreze, într-un mediu virtual, scenarii de tip „ce-ar fi dacă?” și să înțeleagă mai bine impactul alegerilor lor.

Măsurile de tip gamificare – puncte de fidelitate, recompense pentru cei care folosesc bicicleta sau transportul public – se bazează tot pe o bună gestiune

²⁰ C40 Cities Climate Leadership Group (2025), C40 Knowledge Hub, Disponibil la: https://www.c40knowledgehub.org/s/?language=en_US [Accesat: 19 Aug. 2025].

²¹ Svalna (2024), *Calculate your climate impact*, Disponibil la: <https://svalna.se/web/en> [Accesat: 19 Aug. 2025].

a datelor. Pe lângă faptul că trebuie să existe o infrastructură sigură de colectare a informațiilor, e important și ca aceste date să fie interpretate corect și comunicate eficient publicului. Numai așa oamenii pot vedea progresul și pot înțelege clar că fiecare gest, oricât de mic, contribuie la un obiectiv mai mare.

Agricultura urbană ca posibilă soluție inovatoare?



Am discutat faptul că schimbările climatice reprezintă una dintre cele mai mari provocări ale secolului XXI, iar orașele, fiind responsabile pentru o mare parte din emisiile de gaze cu efect de seră, se află în centrul acestei probleme.

În căutarea soluțiilor pentru reducerea emisiilor, creșterea rezilienței și îmbunătățirea calității vieții, ne putem întreba dacă nu cumva agricultura urbană (Orsini et al., 2013; Specht et al., 2014; Hallett et al., 2016) nu se poate contura astfel ca o posibilă opțiune inovatoare?

Prin integrarea cultivării alimentelor în mediul construit, orașele pot beneficia de numeroase avantaje, de la reducerea amprente de carbon și până la îmbunătățirea coeziunii sociale. Una dintre principalele modalități prin care agricultura urbană contribuie la diminuarea emisiilor de gaze cu efect de seră este prin reducerea distanței pe care alimentele o parcurg până la consumator. În mod tradițional, alimentele sunt produse în zone rurale, apoi transportate pe distanțe lungi până la centrele urbane. Acest sistem, deși bine pus la punct, generează costuri energetice ridicate, atât prin transportul propriu-zis, cât și prin depozitarea și ambalarea suplimentară necesare. În schimb, cultivarea alimentelor în oraș sau la periferie reduce semnificativ amprenta de carbon asociată transportului.

Un exemplu elocvent este modelul fermelor urbane din New York, precum Brooklyn Grange²², care produce anual tone de legume și verdețuri chiar pe acoperișurile clădirilor din metropolă. Prin vânzarea directă în comunitate, se elimină necesitatea unor transporturi de lungă distanță, ceea ce duce la economii importante de combustibil fosil și la reducerea poluării.

Agricultura urbană nu înseamnă doar grădini comunitare la sol sau pe acoperișuri, ci și sisteme complexe de agricultură verticală și hidroponie, care maximizează productivitatea pe suprafețe mici. Asemenea instalații se pot integra în clădiri comerciale sau rezidențiale, transformându-le în „centre de producție” alimentară. Prin folosirea unor tehnologii avansate de iluminat cu LED-uri și prin controlul atent al climatului interior, aceste ferme verticale pot produce legume proaspete tot timpul anului, fără a necesita acces la suprafețe întinse de teren agricol. În plus, datorită sistemelor de recirculare a apei și îngrășămintelor, consumul de resurse este mult mai mic decât în cazul agriculturii convenționale.

Un exemplu cunoscut la nivel mondial este Sky Greens din Singapore²³, unde turnuri agricole hidroponice reutilizează apa și utilizează energie minimă pentru a crește plante în mod sustenabil. Prin astfel de inițiative, se reduce presiunea asupra terenurilor agricole tradiționale și se creează un sistem mult mai eficient din punct de vedere energetic.

O altă componentă fundamentală a agriculturii urbane este legată de posibilitatea valorificării deșeurilor organice provenite din gospodăriile urbane. Resturile alimentare, frunzele și crengile rezultate din întreținerea spațiilor verzi pot fi colectate și transformate în compost, care să fie ulterior folosit în grădinile urbane. Astfel se închide un cerc al resurselor, contribuind la scăderea cantității de deșeuri trimise la gropile de gunoi și, implicit, la reducerea emisiilor de metan. De exemplu, în San Francisco, colectarea separată a deșeurilor organice permite obținerea unui compost de înaltă calitate, utilizat ulterior de fermierii locali și în grădinile urbane din zonă. Prin gestionarea inteligentă a deșeurilor organice, orașele pot crea un sistem circular, în care resursele sunt valorificate constant, în loc să fie risipite.

Agricultura urbană, în special sub forma grădinilor pe acoperișuri și a fermelor verticale, contribuie la reglarea temperaturilor locale, prin generarea de umbră și prin procesele naturale de evapotranspirație. De asemenea, vegetația ajută la captarea pulberilor în suspensie și la îmbunătățirea calității aerului. În orașe precum Basel (Elveția), se oferă subvenții proprietarilor de clădiri care își „înverzesc” acoperișurile, iar unele dintre aceste spații sunt transformate în adevărate grădini urbane²⁴. Pe lângă

²² Brooklyn Grange (2024), *Brooklyn Grange | Green Roof System & Eco-Friendly Landscaping In Brooklyn*, Disponibil la: <https://www.brooklyngrangefarm.com> [Accesat: 19 Aug. 2025].

²³ Sky Urban Solutions (2014), *Sky Greens*, Disponibil la: <https://www.skygreens.com/> [Accesat: 19 Aug. 2025].

²⁴ UrbanizeHub (2023), *Orașul Basel vrea ca locuințele să fie protejate de acoperișuri verzi*, Disponibil la: <https://urbanizehub.ro/orasul-basel-vrea-ca-locuintele-sa-fie-protejate-de-acoperisuri-verzi/> [Accesat: 19 Aug. 2025].

beneficiile de mediu, aceste proiecte aduc un plus de biodiversitate și creează zone de relaxare pentru locuitori.

Pe măsură ce populația urbană crește, iar fenomenul de urbanizare se accelerează, securitatea alimentară devine o temă de maxim interes. Agricultură urbană poate contribui la consolidarea rezilienței orașelor în fața șocurilor climatice și a întreruperilor în lanțurile de aprovizionare globală. Prin producerea de hrană la nivel local, orașele devin mai puțin dependente de importuri și au capacitatea să asigure resurse vitale chiar și în situații de criză. Mai mult, grădinile comunitare îmbină utilul cu plăcutul: pe de o parte produc alimente proaspete și sănătoase, iar pe de altă parte, creează spații pentru interacțiune socială, educație și schimb de cunoștințe.

Un exemplu relevant este rețeaua de *allotments* din Marea Britanie, unde fiecare familie poate avea o mică bucată de teren pentru a cultiva legume și fructe. Aceste inițiative îmbunătățesc relațiile dintre vecini, dezvoltă un sentiment de apartenență la comunitate și oferă oportunități de a învăța despre mediu și agricultură sustenabilă.

Pentru ca agricultura urbană să își atingă potențialul maxim, este necesară o integrare atentă în politicile de planificare urbană. Este necesar să existe o colaborare strânsă între autoritățile locale, dezvoltatorii imobiliari și comunități pentru identificarea celor mai potrivite amplasamente și pentru crearea infrastructurii necesare. De pildă, în orașe precum Montréal sau Detroit, clădirile abandonate sau terenurile virane au fost transformate în spații agricole productive, ducând la revitalizarea cartierelor și la creșterea valorii proprietăților din proximitate. De asemenea, politicile fiscale favorabile, cum ar fi reducerea taxelor pentru spațiile verzi sau oferirea de subvenții pentru proiecte de fermă urbană, stimulează companiile și asociațiile să investească în astfel de inițiative.

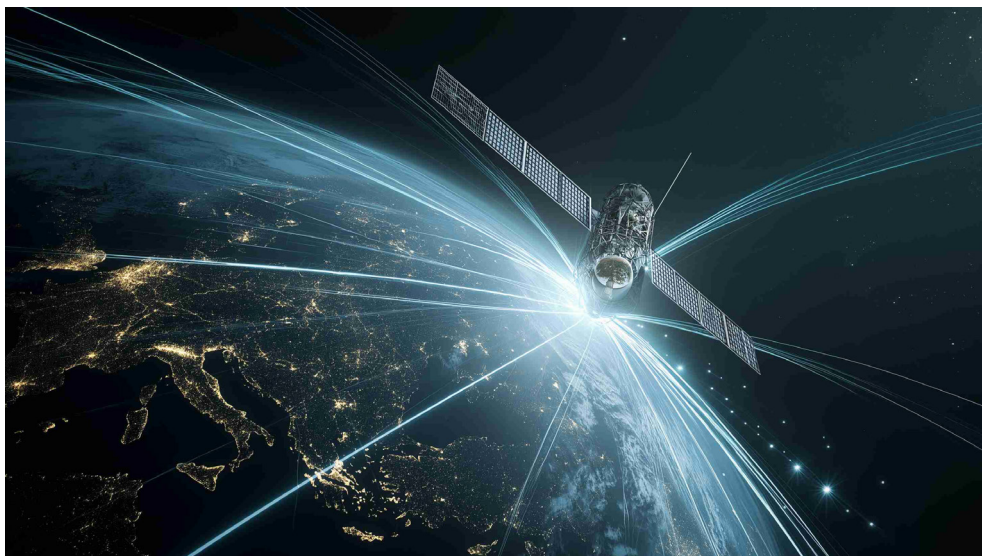
Dezvoltarea agriculturii urbane este strâns legată de progresul tehnologic. Sistemele de irigare inteligente, senzorii de umiditate, aplicațiile de monitorizare a nutrienților și iluminatul cu LED de ultimă generație permit cultivarea controlată a plantelor, cu un consum minim de apă și energie. Surplusul de energie din panourile fotovoltaice instalate pe clădiri poate alimenta fermele verticale, iar apa de ploaie colectată poate fi direcționată către grădinile urbane. Un exemplu interesant este proiectul Farm One din Manhattan²⁵, unde senzorii și datele colectate sunt utilizate pentru a optimiza producția în fiecare etapă a ciclului de creștere, obținându-se un randament ridicat pe suprafețe reduse. Dincolo de beneficiile ecologice evidente, agricultura urbană poate fi o sursă de dezvoltare economică. Pe de o parte, creează oportunități de antreprenoriat pentru micii producători și pentru start-up-urile din domeniul tehnologiei agricole. Pe de altă parte, poate avea un impact pozitiv asupra economiei locale prin crearea de locuri de muncă și prin stimularea turismului. Din ce în ce mai multe orașe organizează tururi ghidate ale fermelor urbane, oferind

²⁵ Farm.One (2025), *Indoor Farm*, Disponibil la: <https://www.farm.one/> [Accesat: 19 Aug. 2025].

astfel vizitatorilor posibilitatea de a înțelege cum funcționează aceste sisteme și cum contribuie ele la viața comunității. Prin urmare, orașele care susțin și promovează agricultura urbană investesc în viitorul lor, nu doar din perspectiva mediului, ci și din perspectiva prosperității locale.

Proiectele de agricultură urbană pot contribui la reducerea emisiilor de gaze cu efect de seră prin scurtarea lanțurilor de aprovizionare, și pot îmbunătăți eficiența energetică prin tehnologiile de cultivare verticală. Totodată, ele facilitează gestionarea responsabilă a deșeurilor organice, sprijină dezvoltarea biodiversității și scad efectul de insulă termică din mediul urban. Mai mult, prin oferirea unor surse locale de hrană, orașele devin mai reziliente și mai capabile să facă față fluctuațiilor și șocurilor externe. Agricultura urbană stimulează și coeziunea socială, creând spații de interacțiune și educație pentru locuitori, indiferent de vârstă sau statut social. Desigur, agricultura urbană nu poate rezolva de una singură toate dificultățile generate de schimbările climatice, dar, integrată inteligent alături de alte măsuri sustenabile precum promovarea transportului în comun și a mobilității electrice, creșterea eficienței energetice a clădirilor, extinderea spațiilor verzi și reformarea sistemelor de gestionare a deșeurilor poate accelera considerabil tranziția către neutralitate climatică.

Utilizarea imaginilor în sprijinul dezvoltării agriculturii urbane



Imaginile satelitare oferă date complexe și actualizate despre suprafața Pământului. Aceste date, colectate la intervale regulate, pot fi folosite pentru a evalua o gamă largă de variabile: de la structura fizică a zonelor urbane până la variațiile de

temperatură, umiditate și poluanți. În cazul agriculturii urbane, imaginile satelitare devin extrem de valoroase, deoarece permit fermierilor, planificatorilor și autorităților locale să obțină o viziune de ansamblu asupra spațiilor disponibile și a potențialului acestora. Mai mult, în contextul dezvoltării tehnologice, imaginile satelitare pot fi integrate cu soluții XR și cu platforme tip Metavers. Practic, se pot crea „gemeni digitali” (digital twins) ai orașelor, în care datele satelitare sunt suprapuse peste modele 3D ale clădirilor și infrastructurii.

În acest fel, dezvoltatorii, planificatorii urbani și cetățenii interesați au posibilitatea să exploreze în mod interactiv spațiile existente, identificând potențiale locații pentru grădini comunitare sau ferme urbane verticale, evaluând simultan factori precum poluarea, densitatea clădirilor și nivelul de lumină solară. O astfel de abordare interactivă nu doar îmbogățește procesul de planificare, ci înlesnește comunicarea între toți actorii implicați. Cu ajutorul algoritmilor de inteligență artificială și învățare automată, pot fi clasificate tipurile de acoperire a terenului (beton, spațiu verde, apă etc.), pot fi identificate zonele cu vegetație bogată și pot fi detectate semnele de degradare a solului sau de poluare a apei.

Integrarea cu tehnologii XR (precum realitatea augmentată și realitatea virtuală) îi ajută pe decidenți să vizualizeze ce tip de intervenție agricolă este potrivită într-un anumit spațiu. Prin simpla îndreptare a unui dispozitiv mobil către o clădire, un utilizator poate vedea o simulare a modului în care ar arăta o seră urbană sau o grădină hidroponică pe terasa superioară.

Identificarea și evaluarea spațiilor potrivite pentru agricultură urbană - unul dintre primele obstacole în dezvoltarea agriculturii urbane este găsirea terenurilor potrivite pentru implementarea proiectelor: poate fi vorba despre terenuri abandonate, despre zone aflate în stare de degradare sau despre clădiri și acoperișuri plate care nu sunt utilizate. Imaginile satelitare, combinate cu hărți digitale ale orașului și cu date despre proprietăți, permit identificarea rapidă a acestor spații. De exemplu, pot fi analizate zonele din jurul unor foste fabrici sau depozite, determinându-se dacă solul este suficient de stabil pentru a susține culturi. Ori, printr-o simplă scanare a suprafețelor de acoperiș, se pot găsi clădirile cu potențial pentru grădini pe acoperiș sau pentru sere hidroponice.

În marile metropole, unde terenul este foarte scump și limitat, astfel de tehnologii pot face diferența între a identifica sau a rata oportunități prețioase pentru agricultura urbană. Odată identificate terenurile potențiale, urmează etapa de evaluare a calității și stabilității acestora. Aici, imaginile satelitare pot oferi informații despre topografie (relieful local), drenajul natural al apei și chiar despre compoziția solului, prin analize multispectrale. De exemplu, anumite benzi spectrale pot sugera prezența humusului sau a sărurilor. Totodată, datele topografice indică zonele cu risc de inundații sau terenurile prea abrupte, nepotrivite pentru agricultură.

Astfel, fermierii urbani pot decide ce tip de agricultură se potrivește: dacă un teren are un drenaj natural bun și o expunere optimă la soare, poate fi folosit pentru

culturi clasice în sol. Dacă însă există riscul de poluare sau dacă solul nu reține apa, se poate opta pentru sisteme de agricultură în paturi ridicate sau metode hidroponice. Prin urmare, imaginile satelitare ajută la reducerea riscului de investiție pe un teren nepotrivit și la creșterea eficienței planificării. Expunerea suficientă la lumina solară este vitală pentru creșterea plantelor.

Într-un oraș, clădirile înalte și infrastructura pot crea umbre persistente, iar fermierii urbani trebuie să știe cum se deplasează soarele de-a lungul zilei și al anotimpurilor. Imaginile satelitare și simulările 3D, corelate cu datele despre poziția soarelui, permit cartografierea zonelor umbrite și a celor bine luminate. Această analiză e cu atât mai relevantă pentru acoperișuri, unde structurile adiacente pot obstrucționa parțial lumina la anumite ore. De asemenea, se pot folosi modele digitale de suprafață (Digital Surface Model – DSM) generate din imagini satelitare sau din scanări LIDAR, care arată înălțimea construcțiilor, a copacilor și altor elemente urbane. Cu ajutorul lor, se creează hărți de insolație pentru fiecare oră a zilei, în fiecare sezon. Astfel, un potențial proiect poate fi planificat în zonele cu expunere optimă, iar acolo unde lumina este mai redusă, se pot implementa sisteme de iluminat artificial sau se pot cultiva plante care tolerează umbra.

Identificarea contaminărilor - una dintre cele mai sensibile probleme legate de agricultura urbană este riscul de poluare a solului și a apei. Imaginile satelitare multispectrale și hiperspectrale pot detecta prezența unor compuși chimici nocivi, precum și a unor metale grele, prin semnătura spectrală specifică. Deși această metodă are nevoie în general de validare la fața locului, ea poate servi drept un prim pas de triere a zonelor cu potențial poluat. În plus, istoricul industrial al unui oraș poate fi corelat cu datele satelitare pentru a determina dacă un anumit teren a fost anterior zonă industrială cu reziduuri, depozit de deșeuri sau locul unor activități care lasă reziduuri toxice. Astfel, fermierii urbani pot evita încă de la început terenurile care prezintă un grad mare de contaminare și pot lua în calcul metode alternative de cultivare (paturi ridicate, hidroponie) acolo unde există potențial, dar solul nu este sigur pentru plante alimentare. Mai mult, în unele cazuri, se pot implementa strategii de fitoremediere, folosindu-se plante capabile să absoarbă metale grele și să detoxifice treptat solul, proces monitorizat ulterior prin noi analize satelitare și prelevări la teren.

Analiza microclimatului urban (identificarea insulelor de căldură urbană) - efectul de insulă termică urbană (heat island) este un fenomen prin care, din cauza betonului și asfaltului, orașele au temperaturi mai mari decât zonele rurale înconjurătoare.

Cu ajutorul imaginilor termice furnizate de sateliți (precum cei din seria Landsat sau Sentinel), se pot cartografia zonele cu temperaturi anormal de ridicate. Autoritățile locale pot integra datele obținute din satelit cu planurile de extindere a zonelor verzi. Agricultura urbană devine astfel parte a strategiei de reducere a insulelor de căldură, oferind atât beneficii alimentare, cât și ameliorarea microclimatului.

Monitorizarea calității aerului - poluarea aerului este un alt factor care poate influența randamentul culturilor și siguranța alimentelor obținute din agricultura urbană. Anumiți sateliți (precum Sentinel-5P) furnizează date despre concentrațiile de dioxid de azot, dioxid de sulf și alte gaze poluante. Aceste informații, combinate cu date la sol, pot oferi o imagine cuprinzătoare a calității aerului la nivelul unor zone extinse. Fermierii urbani pot astfel să își adapteze culturile, să implementeze filtre de aer în sere sau să aleagă specii de plante capabile să absoarbă anumite categorii de poluanți.

Planificarea și gestionarea sustenabilă a terenurilor (integrarea în sisteme GIS) - Sistemele Informaționale Geografice (GIS) reprezintă coloana vertebrală a unei planificări spațiale coerente. Datele satelitare se pot importa în platforme GIS, unde sunt combinate cu informații demografice, socioeconomice și urbanistice. De pildă, se pot crea hărți tematice care să arate venitul mediu pe cartier, accesul la piețe și magazine alimentare, precum și nivelul de poluare, toate suprapuse cu potențialele locații identificate pentru agricultura urbană. În felul acesta, fermierii urbani, ONG-urile, administrațiile locale și comunitățile pot lua decizii bazate pe analize complexe, direcționând investițiile spre zonele care au cea mai mare nevoie de acces la hrană proaspătă și care prezintă cele mai bune condiții de mediu. Mai mult, prin integrarea acestor date într-o platformă XR sau într-un mediu de tip Metavers, părțile interesate pot participa la ateliere de planificare virtuală, explorând datele GIS într-o manieră imersivă. Astfel, se pot testa diferite scenarii de dezvoltare, cum ar fi extinderea unei ferme urbane, transformarea unei parcuri în grădină comunitară sau reconversia unor zone abandonate în livezi urbane. O astfel de abordare colaborativă și interactivă crește gradul de acceptare publică și asigură o planificare mai adaptată nevoilor reale.

Monitorizarea și evaluarea schimbărilor în timp (analiza temporală) - unul dintre marile avantaje ale imaginilor satelitare este disponibilitatea lor periodică.

Prin comprarea mai multor imagini în momente diferite de timp se poate urmări evoluția spațiilor urbane și a proiectelor agricole. O serie de imagini preluate la interval de câteva luni poate arăta cum se extinde o fermă urbană, cum se modifică vegetația sau cum se reface un sol supus programelor de fitoremediere. Astfel de monitorizări oferă date reale despre eficiența investițiilor în agricultura urbană. Analiza NDVI (Normalized Difference Vegetation Index) sau a altor indici de vegetație ajută la cuantificarea nivelului de creștere a plantelor și la estimarea stării lor de sănătate.

Detectarea tendințelor climatice - schimbările climatice și încălzirea globală pot afecta în mod direct randamentul culturilor urbane. Pe termen lung, datele satelitare permit identificarea tendințelor locale în privința temperaturii, precipitațiilor și nivelului de poluare. În felul acesta, fermierii urbani și autoritățile locale se pot pregăti din timp pentru scenarii nefavorabile: secete prelungite, episoade de ploi abundente ori valuri de căldură. Strategiile de adaptare precum introducerea unor culturi rezistente la stres termic sau construirea unor rezerve de

apă etc. Detectarea timpurie a unor fenomene meteo extreme poate asigura inclusiv un răspuns rapid, protejând culturile prin acoperirea lor cu structuri temporare sau prin reglarea sistemelor de irigație. Această abordare reduce riscul de pierderi și consolidează reziliența agriculturii urbane care, în ultimă instanță, joacă un rol important în securitatea alimentară locală. Într-un oraș populat, chiar și o mică scădere sau creștere a producției alimentare locale se poate traduce prin avantaje sau dezavantaje economice și sociale considerabile.

Evaluarea impactului intervențiilor - pe lângă monitorizarea generală a condițiilor, imaginile satelitare sunt excelente pentru a evalua impactul înainte și după al unor proiecte de agricultură urbană. De pildă, dacă o zonă abandonată a fost transformată într-o fermă comunitară, imaginile satelitare din perioada anterioară și ulterioară amenajării evidențiază creșterea suprafeței de vegetație și eventualele modificări ale temperaturilor locale (analiză termică). Totodată, se poate urmări și starea infrastructurii verzi învecinate și felul în care cultura agricolă influențează biodiversitatea sau capacitatea de drenare a apei.

Utilizarea tehnologiilor IoT



Tehnologiile IoT (Internet of Things) au declanșat o adevărată revoluție în agricultură, iar acest lucru se vede din plin și în spațiile urbane, unde terenurile sunt mai limitate și resursele trebuie gestionate cu precizie maximă. Prin conectarea diverselor dispozitive și senzori la internet și prin colectarea automată de date în timp real, fermierii urbani pot lua decizii rapide și bine fundamentate, pot crește eficiența consumului de energie și apă și pot crea medii optime pentru creșterea plantelor pe tot parcursul anului.

Tehnologiile IoT își dovedesc potențialul în agricultură prin capacitatea de a colecta și transmite date despre orice aspect al procesului de cultivare, de la temperatură și umiditate, până la calitatea apei și consumul de energie. De pildă, dispozitivele IoT pot fi amplasate în diverse puncte ale unei ferme verticale, astfel încât să se asigure monitorizarea unitară a parametrilor de creștere a plantelor în toate zonele. Datele colectate sunt centralizate într-o platformă digitală, analizate și convertite în rapoarte ușor de înțeles, care permit fermierilor să ajusteze strategiile de cultivare în timp real. Această transparență ridicată nu doar că îmbunătățește productivitatea, ci și reduce semnificativ risipa de resurse.

Monitorizarea condițiilor de mediu - senzorii de temperatură și umiditate sunt probabil cele mai răspândite dispozitive IoT folosite în agricultura urbană. Amplasați în sol, acești senzori detectează nivelul de umiditate și trimit datele către o platformă digitală, unde sunt procesate în timp real. Dacă umiditatea scade sub nivelul optim, sistemul poate declanșa automat irigația, evitând astfel situația în care plantele suferă de stres hidric. În același mod, senzorii de temperatură din aer semnalizează când climatul devine prea cald sau prea rece, permițând reglarea ventilării ori a încălzirii. Această abordare reduce considerabil intervențiile manuale și facilitează stabilirea unor setări precise pentru fiecare tip de cultură. Practic, se creează microclimate personalizate, mai ales în ferme verticale sau sere urbane, unde diferite zone pot avea cerințe climatice specifice.

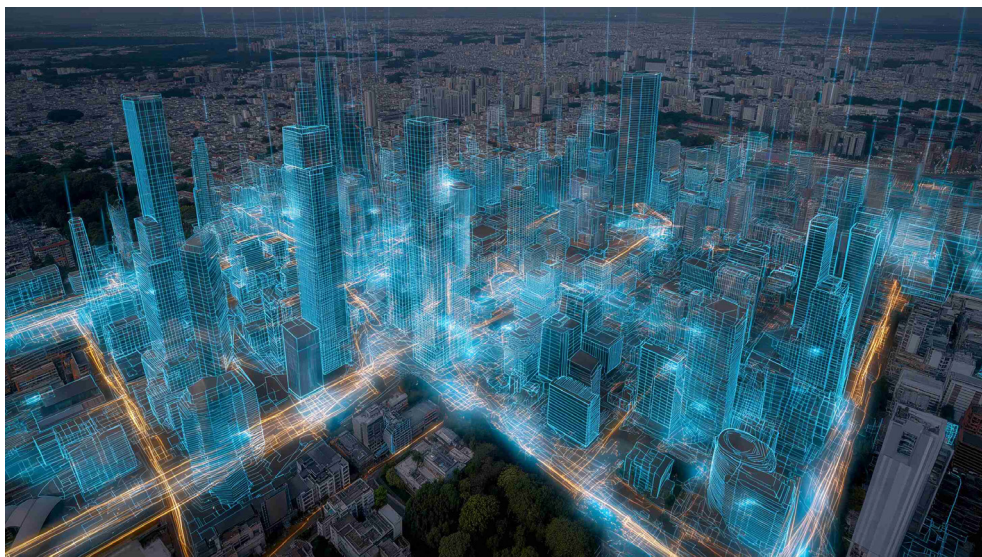
În sisteme de agricultură urbană, lumina naturală poate fi insuficientă din cauza clădirilor înalte și a umbrelor proiectate. Senzorii IoT care măsoară intensitatea luminoasă și durata de expunere la lumină pot fi instalați la diferite înălțimi și poziții. Datele colectate sunt transmise către un sistem de control al iluminatului, care își ajustează intensitatea și spectrul de lumină artificială în funcție de nevoile momentului.

Sisteme de irigare automatizate - o altă componentă importantă a agriculturii urbane este irigarea eficientă, mai ales în contextul secetelor urbane și al prețului ridicat al apei. Datele privind umiditatea solului, corelate cu prognozele meteo colectate prin intermediul IoT, permit sistemelor automate să fie pornite exact când plantele au nevoie de apă și în cantitățile potrivite. Prin urmare, risipa de apă se reduce masiv, iar plantele nu sunt supuse stresului generat de supra-irigare. În același timp, fermierii urbani pot urmări de la distanță parametrii de irigare pe dispozitive mobile și pot interveni manual dacă observă anomalii. Mai mult, istoricul de consum de apă este stocat, permițând analize și comparații între sezoane diferite, culturi diferite sau tehnologii de irigare testate.

Utilizarea surselor regenerabile - o strategie des întâlnită în rândul fermelor urbane este integrarea de panouri solare sau alte surse regenerabile. Senzorii IoT pot monitoriza producția de energie și pot regla automat consumul în funcție de disponibilitatea sursei regenerabile. Astfel, când soarele este puternic, o fermă verticală poate folosi prioritar energia solară, iar când cerul este noros, sistemul comută pe rețeaua tradițională sau pe un acumulator.

Gestionarea apei și resurselor de apă - calitatea apei este un factor critic pentru succesul oricărui proiect de agricultură urbană, mai ales în sisteme precum hidroponia sau acvaponia, unde apa face parte din mediul direct de creștere a plantelor. Cu ajutorul senzorilor IoT, se pot măsura parametri precum pH-ul, nivelul de oxigen dizolvat sau prezența contaminanților. Dacă un senzor detectează valori anormale, sistemul poate alerta fermierul și poate activa procedurile necesare, precum înlocuirea apei sau adăugarea de substanțe care să restabilească echilibrul chimic. Astfel, se elimină riscul ca plantele să fie afectate de boli sau de stres, iar recoltele rămân sigure pentru consumatori. Integrarea cu platformele digitale și Big Data (analize predictive) - datele colectate în timp real de zecile sau chiar sutele de senzori IoT dintr-o fermă urbană sunt mai mult decât un instantaneu al condițiilor curente. Ele devin bază pentru modele predictive atunci când sunt agregate și analizate. Într-o platformă de tip Big Data, se pot identifica tipare și corelații care scapă analizei umane, precum relația dintre variațiile de temperatură și ratele de creștere a diferitelor soiuri. Aceste informații pot anticipa potențiale probleme, precum apariția dăunătorilor, bolile plantelor sau perioadele de secetă. De exemplu, prin corelarea datelor IoT despre umiditatea solului cu modelele meteo, un fermier poate primi o alertă de tipul: „În următoarele 48 de ore sunt șanse crescute de temperaturi foarte ridicate, iar solul tău se va usca rapid. Ar trebui să crești frecvența irigației pentru a evita scăderea randamentului”.

Digital Twin în agricultura urbană



Tehnologia Digital Twin (geamăn digital) se bazează pe crearea unei replici virtuale ale unui sistem, obiect sau proces fizic, care poate fi monitorizată, simulată și optimizată în timp real. Această replică digitală cuprinde atât infrastructura fizică

a spațiilor de cultivare, cât și datele despre plante, mediu, resurse și echipamente, permițând o gestionare mult mai precisă, flexibilă și eficientă. Datorită capacității sale de a unifica surse multiple de date și de a oferi vizualizări și simulări avansate, geamănul digital poate deveni inima procesului decizional într-o fermă urbană modernă.

În cele ce urmează, vom explora modul în care un Digital Twin poate facilita monitorizarea în timp real, simularea și optimizarea operațiunilor, planificarea și designul asistate de XR, precum și gestionarea colaborativă și susținerea deciziilor privind politicile publice.

Crearea unui geamăn digital pentru agricultură urbană implică modelarea digitală a întregului ecosistem: de la clădirile și spațiile unde se cultivă plante (acoperișuri, sere, grădini verticale etc.) până la rețelele de irigare și senzorii care monitorizează parametrii de mediu. Acest model digital este actualizat permanent cu date provenite din rețele de senzori IoT, imagini satelitare, surse climatice și alte canale de informare, astfel încât să reflecte în timp real starea fizică a fermei urbane. În plus față de simpla monitorizare, un Digital Twin oferă și capacitatea de a realiza simulări și previziuni. De pildă, poate prezice evoluția randamentului unei culturi pe baza datelor despre temperatură, luminozitate și umiditate, sau poate semnaliza din timp riscurile asociate cu schimbările climatice ori invaziile de dăunători.

Monitorizare în timp real - senzorii IoT, plasați strategic în diferite puncte ale fermei urbane (în sol, în aer, la nivelul rădăcinilor plantelor, în rețeaua de irigare etc.), colectează date despre temperatură, umiditate, nivel de nutrienți, dăunători, dar și despre consumul de energie sau starea echipamentelor. Transmise în timp real către platforma de geamăn digital, aceste informații oferă o imagine clară și actualizată a stării fiecărei zone de cultivare.

Simulare și optimizare a operațiunilor - una dintre cele mai valoroase funcționalități ale unui geamăn digital este abilitatea de a rula simulări înainte ca problemele să apară în realitate. Spre exemplu, fermierul poate simula ce s-ar întâmpla dacă temperaturile medii cresc cu 2° Celsius peste nivelul obișnuit, identificând astfel potențialele culturi mai rezistente și ajustând planul de irigare pentru a face față unei evaporări accentuate. În același mod, se pot explora diferențele dintre diverse soiuri de plante sau metode de fertilizare, testându-se impactul acestora asupra randamentelor, fără a risca compromiterea efectivă a întregii culturi.

Geamănul digital poate sugera soluții de optimizare. Algoritmii de analiză pot recomanda schimbări fine, cum ar fi ajustarea programului de irigare în funcție de gradul de însorire sau reglarea dozelor de fertilizant pentru a corela creșterea plantelor cu stadiul lor de dezvoltare. Pe termen lung, sistemul poate învăța din propriile observații, aplicând un model de tip machine learning pentru a îmbunătăți permanent strategia agricolă. De pildă, dacă geamănul digital constată că o anumită combinație de nutrienți și condiții de umiditate generează producții mai mari,

recomandările viitoare vor integra aceste concluzii, ducând la o creștere continuă a eficienței și productivității.

Gestionarea colaborativă și suport pentru decizii - Digital Twin-ul reunește date din diverse surse (IoT, imagini satelitare, date meteo, informații istorice) într-un singur model, oferind o percepție unificată și cuprinzătoare asupra fermei urbane. Această analiză multisursă permite detectarea corelațiilor subtile care altfel ar fi greu de identificat. De pildă, se poate observa că producția scade ușor în perioadele cu trafic intens, corelată cu creșterea nivelului de poluanți. Prin înțelegerea acestor conexiuni, fermierii pot interveni punctual, adoptând măsuri precise de contracarare, cum ar fi amplasarea de bariere verzi pentru filtrarea aerului sau ajustarea sistemelor de ventilație în funcție de orele de vârf ale traficului.

Suport pentru politici publice - în cele din urmă, datele și analizele obținute prin geamănul digital pot fi prezentate factorilor de decizie politică, pentru a fundamenta reglementări și programe de sprijin pentru agricultura urbană. De exemplu, un consiliu local poate folosi aceste informații pentru a desemna zone prioritare pentru transformarea în grădini comunitare, pentru a subvenționa construcția de sere urbane sau pentru a stabili taxe și facilități pentru proprietarii care își amenajează acoperișurile în scop agricol.

Participarea comunitară și planificarea colaborativă - succesul inițiativelor de agricultură urbană depinde adesea de susținerea și implicarea locuitorilor, care pot deveni beneficiari direcți (prin acces la hrană proaspătă, spații de relaxare și educație) sau pot resimți schimbări în peisajul urban. Prin AR și VR, proiectele pot fi prezentate într-o manieră accesibilă și captivantă, permițând publicului să își facă o idee clară despre beneficiile și posibilele provocări, astfel:

- Consultarea publică prin expoziții VR: În cadrul unor evenimente sau întâlniri comunitare, locuitorii pot explora, cu ajutorul căștilor VR, modul în care ar putea arăta viitoarea lor grădină comunitară sau fermă pe acoperiș. Aceștia pot schimba unghiul de vizualizare, se pot „plimba” prin spațiu și pot discuta direct cu organizatorii despre posibile îmbunătățiri.
- Aplicații AR pe telefon: Chiar și fără echipamente costisitoare, AR poate fi implementată prin aplicații mobile. Un locuitor poate îndrepta camera telefonului către o parcelă virană sau către un acoperiș, iar aplicația va suprapune modele 3D ale viitoarei ferme urbane. Dacă ceva pare nepotrivit – de exemplu, pare să blocheze un spațiu de agrement sau să afecteze aspectul arhitectural al clădirii –, utilizatorii pot lăsa feedback.

Planificarea infrastructurii verzi a orașului - în efortul de a dezvolta orașe mai verzi și mai reziliente, administrațiile publice și planificatorii urbani iau în considerare rețele complexe de spații verzi: parcuri, grădini comunitare, coridoare ecologice, perdele forestiere și, nu în ultimul rând, ferme urbane. AR devine un instrument foarte valoros în integrarea tuturor acestor elemente într-o viziune de ansamblu coerentă.

Atunci când se dorește amenajarea unui parc cu componente agricole (de exemplu, zone pentru cultivarea legumelor sau livezi urbane în apropierea cartierelor dens populate), AR poate proiecta cum anume se va conecta noul parc cu infrastructura existentă – căi de acces, piste de biciclete, zone pietonale, depozite de compost, sisteme de colectare a apei pluviale. În același timp, specialiștii pot evidenția coridoarele ecologice care leagă diferite sectoare ale orașului, arătând clar zonele în care ar fi utilă implementarea de ferme verticale pe fațade sau pe acoperișuri, astfel încât să se maximizeze continuitatea ecologică și să se ofere habitate adiționale pentru polenizarea plantelor.

Prin AR, factorii de decizie pot vedea imediat dacă există suprapuneri sau conflicte între proiectele de infrastructură verde (de pildă, un coridor ecologic care trece printr-o zonă propusă pentru extinderea traficului auto) și pot lua măsuri de adaptare. De asemenea, pot fi analizate beneficiile ecologice și sociale: capacitatea de a reduce insula termică urbană, potențialul de educare a populației, îmbunătățirea calității aerului, și oportunitățile economice create din vânzarea locală a produselor proaspete.

Implementarea Metaversului ca mediu integrator

Metaversul reprezintă un mediu virtual colectiv și persistent, unde utilizatorii pot interacționa între ei, precum și cu obiecte și informații digitale, într-un mod imersiv, intensificat de tehnologii emergente precum realitatea virtuală (VR), realitatea augmentată (AR) și realitatea mixtă (MR).

În contextul agriculturii urbane, Metaversul deschide o serie de oportunități ce pot fi valorificate pentru a eficientiza, educa și implica mai bine atât fermierii, cât și comunitatea locală. Această lume digitală paralelă permite accesul la date, proiecte, simulări și soluții tehnologice într-un cadru colaborativ, fără a fi constrâns de limitările fizice. Prin intermediul tehnologiilor XR (VR, AR, MR) integrate în Metavers, fermierii urbani și specialiștii pot avea acces la date și informații în timp real. Aceștia pot să vizualizeze condițiile agrometeorologice, să analizeze problemele care apar în culturi și să ia decizii informate folosind modele 3D interactive.

Totodată, același spațiu virtual poate funcționa drept un mediu educațional, oferind cursuri, tutoriale și experiențe imersive despre bunele practici în agricultură, gestionarea resurselor, agroecologie, permacultură și alte concepte relevante.



O componentă importantă o reprezintă colaborarea extinsă la nivel global, pe care Metaversul o face posibilă. Experții și fermierii urbani din diferite orașe ale lumii pot împărtăși în timp real cunoștințe, strategii și tehnologii, pentru a sprijini dezvoltarea unor modele de agricultură urbană rezistente, eficiente și flexibile. Totodată, Metaversul poate asigura și o platformă de socializare, unde publicul larg poate interacționa cu fermele urbane într-un mod captivant, descoperind beneficiile acestui tip de agricultură și implicându-se activ în proiecte. Nu în ultimul rând, Metaversul servește drept catalizator pentru dezvoltarea infrastructurii digitale, necesară implementării pe scară largă a soluțiilor de tip Internet of Things (IoT) și a sistemelor avansate de inteligență artificială (AI) în agricultură.

Platformă colaborativă pentru planificare și design - unul dintre avantajele definitorii ale Metaversului constă în posibilitatea de a crea spații de colaborare virtuală, unde diferiți actori, de la experți în agricultură, arhitecți și planificatori urbani, până la fermieri și cetățeni interesați, pot lucra împreună pentru a concepe și planifica ferme urbane. Aceste spații de lucru comune oferă un nivel de interactivitate sporit, facilitând discuții și sesiuni de brainstorming în timp real, indiferent de localizarea geografică a participanților.

Într-un mediu tradițional, colaborarea pentru proiectarea unei ferme urbane implică planuri 2D, randări și, eventual, modele 3D statice. Metaversul duce acest

proces la un alt nivel, oferind posibilitatea de a genera modele 3D interactive ale terenului disponibil, infrastructurii urbane și potențialelor constrângeri de mediu. Participanții pot explora și modifica aceste modele la scară, pot ajusta parametrii precum tipul de culturi, modul de dispunere a plantelor, soluțiile de irigare, sistemele de lumină și ventilație, dar și elemente estetice sau funcționale. În orice moment, modificările pot fi vizualizate instantaneu, ceea ce accelerează procesul decizional și reduce foarte mult riscul de erori costisitoare.

Piață virtuală și economie agricolă digitală - agricultura urbană nu se rezumă doar la producția de hrană, ci implică și procese de distribuție, comercializare și relaționare cu consumatorul. În Metavers, dezvoltarea unei piețe virtuale pentru produsele fermelor urbane poate redefini întregul lanț valoric, facilitând tranzacții rapide, transparente și bazate pe încredere.

Să ne imaginăm un spațiu virtual în care fermierii urbani își pot expune produsele sub forma unor standuri 3D, fiecare cu informații detaliate despre metoda de cultivare, valorile nutriționale, trasabilitatea semințelor și impactul ecologic. Consumatorii pot „vizita” aceste standuri la orice oră, pot interacționa cu fermierii, pot pune întrebări și pot comanda produse, totul într-un cadru digital intuitiv. Mai mult, tururile virtuale ale fermelor oferă clienților posibilitatea de a vedea exact cum sunt cultivate legumele și fructele pe care le cumpără, sporind astfel transparența și încrederea. O astfel de piață virtuală poate fi adaptată pentru a reflecta nevoile și preferințele locale. De exemplu, pot exista zone dedicate produselor ecologice, fermelor care folosesc doar energie solară sau producătorilor care urmează principiile de permacultură. Consumatorii pot filtra ofertele în funcție de criterii precum certificări, localizare, preț sau disponibilitate sezonieră. În plus, pot fi organizate evenimente de tip „târg virtual”, unde mai mulți fermieri își lansează simultan noile produse sau unde se prezintă inovații tehnologice în domeniul agriculturii urbane.

Tokenizare și economie digitală - un alt aspect interesant îl reprezintă posibilitatea de a tokeniza produsele agricole sub formă de NFT-uri (Non-Fungible Tokens).

De exemplu, un fermier urban poate crea un NFT care să reprezinte dreptul de proprietate asupra unei anumite recolte sau a unui produs de nișă, cum ar fi sortimente rare de plante aromatice sau roșii mai puțin obișnuite. Clienții care cumpără aceste NFT-uri pot intra în posesia produselor fizice la recoltare, iar între timp, pot tranzacționa tokenurile pe diverse platforme de Blockchain.

Nu în ultimul rând, o piață virtuală bazată pe Metavers și Blockchain poate integra și mecanisme de finanțare participativă. Comunitățile locale și investitorii interesați de agricultura sustenabilă pot cumpăra „tokenuri” sau acțiuni într-un proiect agricol urban, contribuind astfel la dezvoltarea infrastructurii, achiziționarea de echipamente sau cercetarea de noi tehnici. În schimb, aceștia pot beneficia de acces prioritar la recoltă sau de alte beneficii asociate.

Monitorizarea și gestionarea fermelor în timp real - în mediul urban, spațiile destinate agriculturii sunt adesea limitate, iar resursele precum apa, energia și spațiul de creștere trebuie gestionate cu mare atenție. Unul dintre aspectele cheie pentru succesul fermelor urbane este capacitatea de a monitoriza în timp real parametrii de mediu și de a reacționa prompt la schimbări. Metaversul, integrat cu dispozitive IoT și tehnologii AR, oferă un cadru ideal pentru această monitorizare și gestionare. Tehnologia IoT permite colectarea permanentă de date despre umiditatea solului sau a mediului de cultură, temperatură, nivelul de nutrienți, calitatea aerului, luminozitate și consumul de apă ori energie. Aceste date sunt trimise în cloud, unde pot fi procesate și afișate în Metavers sub forma unor reprezentări 3D ușor de interpretat. Fermierii sau specialiștii pot intra în acest spațiu virtual și pot observa starea fiecărei culturi, pot compara datele istorice cu cele actuale și pot identifica rapid zonele cu probleme, cum ar fi deficitul de nutrienți sau un nivel necorespunzător de umiditate.

Prin AR, aceste informații digitale pot fi suprapuse direct peste plantele reale. De pildă, un tehnician care se plimbă printr-o seră urbană poate purta ochelari inteligenți care afișează datele culese de senzorii IoT. Astfel, atunci când se uită la o anumită cultură, acesta vede imediat nivelul de umiditate, istoricul de fertilizare și eventualele alerte despre posibile boli sau dăunători. În acest mod, deciziile sunt luate în cunoștință de cauză și pot fi executate mai rapid și mai precis.

Realitatea mixtă (MR) combină elemente de VR și AR, permițând interacțiunea cu obiecte digitale într-un mediu real. În cazul fermelor urbane, MR poate fi folosită pentru a modifica parametrii de funcționare a sistemului de irigare sau de iluminare direct din teren. Fermierul poate trasa, cu un simplu gest, noi direcții pentru furtunurile de picurare sau poate regla intensitatea luminilor LED în zonele mai umbrite. Această abordare „hands-on” în mediul virtual reduce erorile, pentru că modificările sunt vizibile imediat și pot fi comparate cu starea reală a culturilor.

Integrarea MR în Metavers asigură, de asemenea, posibilitatea de a „teleporta” experți din alte regiuni pentru a oferi consultanță în timp real. De exemplu, un specialist dintr-o universitate poate „vedea” live datele unui sistem acvaponic dintr-un alt oraș și poate sugera ajustări pentru un pH optim sau pentru temperatura apei, ca și cum s-ar afla fizic în acea fermă. Aceasta deschide perspective incredibile pentru cooperare globală și pentru dezvoltarea unui know-how colectiv, menit să îmbunătățească eficiența și sustenabilitatea agriculturii urbane.

Implicarea comunității și participarea publicului - unul dintre avantajele majore ale agriculturii urbane este potențialul său de a consolida legăturile din comunitate și de a educa cetățenii cu privire la importanța hranei locale, proaspete și sustenabile. În Metavers, pot fi create „cartiere” sau „centre culturale” virtuale dedicate agriculturii urbane. Aceste spații pot găzdui ateliere, dezbateri, cursuri și prezentări interactive despre diverse teme: compostarea în oraș, reciclarea apei,

crearea grădinilor verticale pe balcoane etc. Participanții pot veni cu idei, pot prezenta proiecte locale și pot primi feedback din partea altor membri ai comunității. De asemenea, pot exista zone speciale unde fermierii urbani își împărtășesc succesele și provocările, creând astfel un sentiment de solidaritate și colaborare.

Una dintre provocările actuale ale agriculturii urbane este armonizarea intereselor diverse: cetățeni care doresc spații verzi, dezvoltatori imobiliari care vizează profitul maxim, autorități locale cu strategii de urbanism și organizații non-guvernamentale care promovează sustenabilitatea. Metaversul poate integra platforme de vot și feedback, permițând cetățenilor să fie consultați și să își exprime preferințele într-un mod simplu și transparent. De exemplu, pentru un proiect de amenajare a unui acoperiș verde destinat cultivării legumelor, autoritatea publică poate încărca un model 3D al clădirii în Metavers, oferind mai multe variante de proiect. Cetățenii pot explora virtual fiecare variantă, pot analiza costurile, beneficiile ecologice și estetice, apoi pot vota direct pentru soluția preferată. Astfel, deciziile se iau într-un mod participativ, iar implicarea comunitară contribuie la acceptarea mai ușoară a proiectelor și la crearea unui sentiment de mândrie locală.

Considerații privind guvernanța datelor

Așa cum am discutat în secțiunea precedentă, în ultimii ani, dezvoltarea accelerată a tehnologiilor de realitate imersivă (XR), Internet of Things (IoT), precum și utilizarea conceptelor de Digital Twin și a analizelor avansate ale imaginilor satelitare au creat noi oportunități pentru orașe de a face tranziția spre neutralitate climatică.

Metaversul, ca mediu virtual integrator, oferă la rândul său un suport critic pentru promovarea unor strategii de planificare urbană mai eficiente, inclusiv pentru dezvoltarea agriculturii urbane. Toate aceste tehnologii generează și utilizează cantități masive de date, a căror guvernanță devine o prioritate pentru actorii implicați în administrația publică, sectorul privat, domeniul academic și societatea civilă.

Guvernanța datelor implică o serie de procese, politici și reglementări prin care se asigură colectarea, stocarea, analiza, partajarea și utilizarea responsabilă a informațiilor. Așa cum am văzut în capitolele precedente, într-un peisaj urban inteligent, datele provin dintr-o multitudine de surse. Datorită complexității și a volumului tot mai mare de informații, asigurarea confidențialității, securității, acurateței și valorificării datelor devine un subiect de interes strategic.

În cele ce urmează vom discuta despre principalii actori (stakeholderi) implicați în această ecuație a guvernanței datelor, cu un accent deosebit pe rolul fiecăruia în contextul planificării urbane și al utilizării Metaversului. Vom particulariza analiza pentru România și, în mod specific pentru București, pentru a oferi un cadru cât

mai complet al provocărilor și oportunităților locale. De asemenea, vom discuta și despre principalele provocări și oportunități cu care se confruntă guvernanta datelor în Metavers, precum și despre principiile cheie și cele mai bune practici.

În primul rând, gestionarea eficientă a datelor în acest mediu virtual implică o serie de dificultăți legate de protecția confidențialității, securitatea informațiilor, interoperabilitate și standardizare tehnologică. Pe lângă aceste aspecte, creșterea exponențială a volumului de date provenite dintr-o gamă foarte largă de interacțiuni virtuale, necesită stabilirea unor mecanisme clare de reglementare și supraveghere, pentru a preveni abuzurile sau distorsiunile generate de colectarea și utilizarea necontrolată a informațiilor. Totodată, se conturează și o serie de oportunități: Metaversul poate facilita procesele de planificare urbană și dezvoltare a infrastructurii digitale, poate duce la îmbunătățirea colaborării între diverse instituții și actori, precum și la apariția unor noi industrii și modele de business bazate pe inovație.

Pentru a răspunde eficient provocărilor, cele mai bune practici recomandă adoptarea unui cadru solid de guvernanta, care să includă reguli clare privind accesul la date, respectarea drepturilor fundamentale ale utilizatorilor și mecanisme periodice de audit și control. De asemenea, se impune o colaborare strânsă între autorități, operatori de platforme, dezvoltatori de aplicații și societatea civilă, astfel încât reglementările să fie adaptate în mod flexibil la schimbările rapide din domeniu, dar și suficient de ferme pentru a proteja echilibrul dintre inovație și interesele legitime ale indivizilor și comunităților.

Rolul utilizatorilor în guvernanta datelor

Utilizatorii finali, fie că sunt cetățeni simpli, organizații, instituții de cercetare sau antreprenori, ocupă o poziție centrală în orice discuție despre guvernanta datelor din Metavers, deoarece rolul lor este fundamental în generarea, consumul și validarea informațiilor care circulă în acest spațiu virtual din ce în ce mai dinamic.

În Metavers, mulți dintre acești utilizatori pot adopta identități digitale sau avatururi prin intermediul cărora explorează lumi virtuale, participă la activități socio-economice, interacționează cu obiecte și infrastructuri urbane simulate ori contribuie la proiecte ce țin de agricultură urbană și de reducerea emisiilor de carbon. Faptul că prezența lor generează date comportamentale, preferințe de consum, localizare virtuală, istoricul interacțiunilor și alte informații relevante face ca ei să fie atât sursă de date, cât și beneficiari ai proceselor de colectare și analiză. În plus, ei utilizează dispozitive inteligente și soluții IoT care amplifică fluxul de informații, conectând și mai mult viața cotidiană de mediul virtual. Această participare constantă și integrată oferă utilizatorilor o poziție unică, deoarece orice acțiune, fie ea și cea mai mică

mișcare a avatarului, poate fi înregistrată și transformată ulterior în date valoroase pentru analize urbane, studii sociologice, modele de consum sau optimizări ale politicilor publice.

Din perspectiva protecției datelor, drepturile lor devin fundamentale, ceea ce înseamnă că fiecare individ care pătrunde în Metavers trebuie să aibă posibilitatea de a-și exercita opțiunile legale: dreptul de a fi informat cu privire la ce date se colectează și în ce scop, dreptul de a-și da și de a-și retrage consimțământul, dreptul de a corecta date inexacte sau de a fi uitat, atunci când circumstanțele o impun.

Într-un context digital, aplicarea acestor drepturi poate fi mai complexă decât în mediile tradiționale, fiindcă pot exista multiple platforme, fiecare cu propriile reguli și infrastructuri, iar avatarul unui utilizator poate circula dintr-un mediu virtual în altul. De aceea, interesul acestora de a înțelege ce se întâmplă cu informațiile generate de activitățile lor devine un subiect critic de guvernare, iar operatorii platformelor au obligația de a elabora politici clare și instrumente intuitive pentru ca oricine să poată gestiona cu ușurință gradul de acces pe care-l oferă.

La rândul lor, utilizatorii nu sunt doar creatori pasivi de date, ci și participanți activi ce pot influența modul în care se desfășoară întregul proces de guvernare. Ei pot oferi feedback determinant, pot ridica probleme legate de transparența operatorilor, pot contesta deciziile pe care le consideră injuste și se pot implica în consultări publice organizate de autoritățile locale, de consorții de dezvoltatori sau de grupuri civice. Un exemplu concret ar fi implicarea cetățenilor în proiecte de planificare urbană desfășurate în Metavers: aceștia pot explora modele digitale ale unui cartier, pot analiza cum se proiectează clădirile și spațiile verzi, pot propune idei pentru rezolvarea congestiilor de trafic, pot semnala deficiențe legate de accesibilitate și pot sugera amplasarea unor grădini urbane pe acoperișuri ori în curțile interioare.

Dincolo de implicarea directă în planificare, utilizatorii Metaversului dețin și un rol educațional, deoarece prin interacțiunile lor pot demonstra altor persoane modul în care tehnologia poate fi valorificată în procese participative. Cei care aleg să se informeze despre drepturile de protecție a datelor și să le exercite responsabil pot da un exemplu pozitiv de implicare, încurajându-i și pe ceilalți să conștientizeze importanța consimțământului informat și a protejării vieții private. O comunitate care își susține reciproc eforturile de monitorizare și de raportare a abuzurilor contribuie la crearea unui mediu virtual mai sigur, în care datele nu sunt folosite în mod excesiv sau abuziv, iar confidențialitatea rămâne un parametru central în orice activitate digitală. De asemenea, utilizatorii pot semnala mecanisme de colectare agresivă a datelor, pot solicita clarificări despre modul în care companiile le analizează comportamentul și pot să ceară modificări ale politicilor, inclusiv prin petiții, campanii de conștientizare și cereri de transparență.

De asemenea, ei reprezintă o forță motrică în adoptarea sau respingerea unor tehnologii, putând alege să utilizeze doar dispozitive care le inspiră încredere, care

au demonstrat practici etice și care le permit să dețină controlul asupra informațiilor generate. Prin urmare, puterea de decizie a utilizatorilor, exprimată prin practicile lor de consum, influențează direct modul în care actorii mari din industrie își dezvoltă infrastructurile și afacerile. Dacă un operator de platformă nu respectă drepturile utilizatorilor și nu garantează securitatea datelor, este probabil să piardă utilizatori care își vor îndrepta atenția spre alte medii virtuale mai transparente și mai sigure. În plus, utilizatorii pot crea la rândul lor inițiative dedicate guvernantei, pot forma grupuri independente care să se implice în elaborarea de standarde, pot stabili parteneriate cu experți, activiști și legiuitori, devenind astfel protagoniști ai schimbărilor structurale ce guvernează Metaversul.

Într-un spațiu virtual, nu doar marile companii pot colecta date personale, ci și alți utilizatori care ar putea încerca să stocheze ori să distribuie materiale fără acordul persoanelor implicate. Din acest punct de vedere, fiecare individ devine un potențial operator de date și are obligația să se asigure că nu încalcă intimitatea altor participanți sau că nu utilizează necorespunzător datele obținute în timpul interacțiunilor virtuale.

Implicarea oamenilor în procese de autoreglementare și conștientizarea asupra faptului că orice încălcare a confidențialității poate fi raportată este un pas important pentru a cultiva o etică a responsabilității reciproce. De altfel, cu cât mai mulți participanți cunosc și respectă principiile de guvernantă, cu atât scad șansele de apariție a unor practici abuzive de supraveghere, de colectare excesivă sau de manipulare a datelor personale. Așadar, utilizatorii nu sunt doar beneficiari ai serviciilor din Metavers, ci și părți interesate ce dețin control asupra unor aspecte esențiale.

Furnizori / Operatori de platforme Metavers

Furnizorii sau operatorii de platforme Metavers, reprezentați ai companiilor consacrate la nivel internațional și ai startup-urilor inovatoare, joacă un rol major în configurarea, întreținerea și dezvoltarea mediilor virtuale care alcătuiesc acest ecosistem digital în continuă expansiune. Ei asigură fundația tehnică pe care se construiesc numeroase activități sociale, economice și culturale, fiind responsabili de tot ceea ce înseamnă infrastructură, reguli de utilizare, securitate și interoperabilitate cu alte platforme. Aceștia pot fi giganți din domeniul tehnologiei, precum Meta sau Microsoft, care investesc considerabil în soluții de realitate virtuală și augmentată, dar și organizații mai mici, specializate pe nișe foarte specifice, cum ar fi furnizarea de modele digitale pentru orașe inteligente, dezvoltarea de medii educaționale sau crearea de ecosisteme bazate pe Blockchain și criptomonede.

Indiferent de anvergura lor, operatorii de platforme au un set de responsabilități comune ce pornesc de la colectarea și stocarea datelor despre utilizatori și modul în

care aceștia interacționează cu spațiul virtual, până la definirea normelor de conținut și a modalităților de raportare a abuzurilor ori încălcărilor de securitate. În momentul în care un avatar pătrunde într-o lume virtuală pentru a explora, a tranzacționa bunuri digitale sau a participa la evenimente, platforma înregistrează date care pot varia de la detalii despre comportamentul avatarului, preferințe și istoricul interacțiunilor, până la informații despre tranzacțiile economice desfășurate, în special acolo unde există elemente de tip NFT sau criptomonede.

Pentru a stoca și procesa aceste date, operatorii au nevoie de centre de date performante, de soluții robuste de cloud și de mecanisme de management al informațiilor care să asigure acuratețea și integritatea seturilor de date. Pe lângă gestionarea datelor, securitatea cibernetică este o altă provocare majoră pentru furnizorii de platforme, deoarece un sistem amplu și deschis poate fi tentant pentru atacatorii informatici, fie că scopul acestora este furtul de identitate, accesul la fonduri virtuale ori perturbarea operării normale a platformei.

Implementarea protocoalelor de criptare a datelor, a sistemelor de detectare a comportamentelor suspecte, verificări constante ale vulnerabilităților software și, nu în ultimul rând, proceduri clare prin care utilizatorii să poată raporta orice activitate dubioasă, fac parte din panelul de măsuri pentru prevenirea breșelor de securitate. Existența unor mecanisme de autentificare puternice contribuie, de asemenea, la diminuarea riscurilor compromiterii conturilor de utilizator și expunerea de date sensibile. Pentru a stabili reguli clare de utilizare și conținut, operatorii de platforme Metavers elaborează politici ce vizează toate aspectele interacțiunii digitale, de la tipul de limbaj permis, la modul de relaționare dintre participanți și conținutul considerat inadecvat sau ilegal.

Dincolo de aceste prevederi, care pot apărea sub formă de termeni și condiții generali, există și dispoziții care abordează punctual situații noi, precum crearea și vânzarea de obiecte virtuale, încălcările drepturilor de autor sau hărțuirea între avatururi, un fenomen dificil de gestionat când spațiul virtual este gândit să încurajeze libertatea de exprimare și creativitatea. În același timp, operatorii trebuie să prevadă metode de raportare a neregulilor, astfel încât utilizatorii să poată semnala rapid orice comportament ilicit sau conținut abuziv și să se asigure că reacționează prompt și imparțial prin proceduri de moderare și, când este cazul, prin suspendarea ori blocarea conturilor care încalcă în mod repetat regulile stabilite.

Într-un Metavers cu adevărat funcțional, interoperabilitatea între diferitele spații virtuale devine un criteriu cheie pentru succes, iar furnizorii de platforme se află în prima linie a acestui efort de standardizare. Fie că e vorba despre dezvoltarea unor protocoale comune de schimb de date, despre stabilirea unor formate recunoscute pentru obiectele virtuale 3D sau despre crearea de mecanisme de tranzacționare care pot funcționa la nivel cross-platform, operatorii au interesul

să coopereze între ei și să pună bazele unor instrumente care să permită avatarurilor să se deplaseze, împreună cu bunurile lor virtuale, dintr-un mediu virtual în altul. În absența acestei colaborări, Metaversul riscă să se fragmenteze în numeroase insule digitale, fiecare cu propriile reguli și standarde, iar utilizatorii vor fi nevoiți să-și fragmenteze la rândul lor experiența, ceea ce reduce atractivitatea și potențialul economic al acestor universuri.

Un alt aspect în care rolul operatorilor devine deosebit de vizibil este colaborarea cu autoritățile locale și cu experții în dezvoltare urbană, în situațiile în care platformele sunt folosite pentru a crea replici digitale ale orașelor sau pentru a derula simulări urbane complexe. Deoarece marile aglomerări urbane se confruntă cu probleme precum poluarea, mobilitatea deficitară și supraaglomerarea spațiilor, operatorii platformelor pot construi gemeni digitali în care specialiștii să introducă date colectate de la senzori de trafic până la imagini satelitare, informații privind calitatea aerului și consumul de energie. Aceste spații virtuale, realizate cu sprijinul dezvoltatorilor de software și al experților din domeniul administrării orașelor, permit simularea unor scenarii de planificare și testare pe termen lung a impactului unor decizii, înainte ca ele să fie aplicate în realitate, unde costurile și riscurile sunt mult mai mari.

Astfel, decidenții politici și urbanisții se pot servi de un set de instrumente avansate de vizualizare 3D pentru a anticipa efectele unor schimbări de infrastructură, precum construirea unor noi piste pentru biciclete, amenajarea de parcuri și grădini comunitare sau mutarea unor zone industriale departe de centrul orașului. Ei pot urmări cum se modifică fluxurile de trafic, nivelul emisiilor de CO₂ sau indicii privind calitatea vieții, și pot lua decizii fundamentate pe analize detaliate. Prin aceste funcționalități, operatorii se poziționează ca parteneri strategici ai administrațiilor publice, care pot îmbunătăți calitatea politicilor urbane și pot inspira inițiative de agricultură urbană sau de combatere a schimbărilor climatice. Rolul lor nu se limitează la furnizarea infrastructurii tehnice, ci se extinde spre zona de facilitare a interacțiunii și a dialogului, iar acest lucru implică, în mod inevitabil, stabilirea unor bune practici privind gestionarea datelor care se generează în astfel de procese participative.

Pe de altă parte, operatorii de platforme Metavers se confruntă cu provocări legate de capacitatea de a menține stabilitatea tehnică a platformelor pe măsură ce acestea cresc rapid în popularitate. Un exemplu îl reprezintă momentele când are loc un eveniment virtual masiv, cum ar fi un concert într-o lume 3D, care poate atrage sute de mii de participanți simultan. Pentru a susține un asemenea flux și a evita întreruperile sau întârzierile mari care afectează experiența utilizatorilor, operatorii trebuie să investească în arhitecturi distribuite, să utilizeze servicii de cloud scalabile și să monitorizeze în timp real performanța rețelelor.

Un alt factor cu impact major în activitatea furnizorilor este respectarea legislației și a reglementărilor în materie de confidențialitatea, concurența, proprietatea intelectuală și protecția consumatorilor. Fiind în mare parte responsabili de colectarea, stocarea și analizarea unor cantități considerabile de date personale și comportamentale, trebuie să țină cont de cerințele impuse de GDPR în Europa, de regulile impuse de alte state sau regiuni și de principiile de securitate a datelor la nivel internațional. Furnizorii se văd astfel în situația de a juca un rol de arbitru, stabilind politici interne care pot fi contestate de entități guvernamentale sau de grupuri de utilizatori. Colaborarea permanentă cu legiuitorii și cu organizațiile de reglementare devine necesară, mai ales când se ajunge la subiecte precum colectarea datelor biometrice sau introducerea unor mecanisme de recunoaștere facială în spațiile virtuale.

Cu toate aceste provocări, operatorii de platforme Metavers ocupă totuși o poziție privilegiată, din care pot schimba modul în care oamenii, companiile și administrațiile publice interacționează în mediul digital. Ei pot experimenta soluții inovatoare, pot stabili noi standarde de interoperabilitate, pot contribui la eforturile de gestionare durabilă a resurselor prin simulări realiste și pot susține inițiative de educație și de formare în realitatea virtuală, accesibile unui public larg.

De modul în care își exercită responsabilitățile și își echilibrează interesele economice cu nevoile comunității va depinde dacă Metaversul va rămâne un loc sigur, incluziv și fertil pentru inovație. În cele din urmă, furnizorii și operatorii de platforme sunt, în același timp, pionieri ai acestui nou mediu digital și gardieni ai integrității lui. Deciziile pe care le iau în privința guvernării datelor, a normelor de utilizare și a cooperării cu alte platforme sau instituții vor continua să dea forma Metaversului în anii ce vin.

Organisme de supervizare, reglementare, legiferare

Organismele de supervizare, reglementare și legiferare reprezintă un pilon fundamental în menținerea echilibrului dintre inovație și protecția interesului public, un factor major mai ales într-un domeniu atât de complex precum gestionarea datelor în contextul Metaversului, al tehnologiilor IoT, XR, Digital Twin sau al oricăror platforme digitale avansate.

Din momentul în care s-a constatat că evoluția tehnologiilor informaționale tinde să devină mai rapidă decât capacitatea legiuitorilor de a reacționa, a apărut nevoia unor instituții capabile să înțeleagă și să supravegheze procesele prin care se colectează, stochează și utilizează datele, stabilind criterii de legalitate și legitimitate, precum și un cadru etic menit să protejeze viața privată și drepturile

fundamentale ale indivizilor. În fapt, evoluția societății umane este inevitabil legată de datele care circulă între actori publici, entități private și spațiul civic, iar fără existența unor instrumente de reglementare se poate instaura rapid un dezechilibru în care datele sunt folosite în mod abuziv, fie în scopuri comerciale îndoielnice, fie în scopuri de supraveghere nelegitimă. În Metavers, dimensiunea acestei probleme crește exponențial, deoarece datele devin și mai detaliate, incluzând informații cu privire la comportamentul și mișcările utilizatorilor, la reacțiile lor emoționale, la preferințele lor de consum, la interacțiunile sociale ori la patrimoniul digital de care dispun. Prin urmare, aceste structuri de supervizare au un rol care depășește simplele competențe de a emite legi, mergând până la un dialog permanent cu industrie, mediul academic și societatea civilă, pentru a se asigura că inovația progresează, iar drepturile și libertățile persoanelor sunt respectate.

În plan global, observăm o serie de organisme internaționale și transnaționale care și-au propus să ofere linii directoare privitoare la securitatea și confidențialitatea datelor, precum și la etica utilizării inteligenței artificiale. Printre acestea se numără, de exemplu, Consiliul European, care stabilește convenții internaționale în materie de protecție a datelor și viață privată, sau organizații precum OCDE, ce propun principii și ghiduri privitoare la fluxurile transfrontaliere de date și la guvernanta inteligentă.

La nivelul Uniunii Europene, Regulamentul General privind Protecția Datelor (GDPR) reprezintă probabil cea mai cunoscută inițiativă legislativă care a încercat să echilibreze libertatea fluxului de date cu nevoia de protecție și control individual. GDPR a impus obligații clare pentru operatorii de date, a oferit drepturi sporite persoanelor vizate și a stabilit amenzi severe pentru cei care încalcă regulile, totul cu scopul de a preveni abuzurile care ar putea apărea odată cu colectarea masivă de informații.

În momentul în care Metaversul devine o arenă în care date sensibile, precum cele biometrice sau cele care descriu comportamentul psihologic al indivizilor, sunt puse în circulație, importanța GDPR și a altor reglementări complementare devine mai mare ca niciodată, iar autoritățile de supervizare naționale, cum ar fi agențiile guvernamentale de protecție a datelor, primesc responsabilități suplimentare.

De altfel, aceste autorități joacă un rol central în a monitoriza conformitatea entităților care operează în Metavers și în a investiga reclamațiile utilizatorilor. Ele pot dispune măsuri corective sau pot aplica sancțiuni, pot iniția acțiuni în instanță și pot stabili bune practici.

Pe lângă zona strictă a confidențialității, organismele de reglementare intervin și în domeniul concurenței, al protecției consumatorului și al eticii, mai ales atunci când se discută despre algoritmi de inteligență artificială care pot modela opiniile sau comportamentele utilizatorilor, atunci când se vehiculează sume mari de bani în cadrul tranzacțiilor de tip NFT ori criptomonede, sau atunci când apar riscuri de

monopol în rândul marilor operatori de platforme Metavers. Autoritățile antitrust, de exemplu, pot analiza dacă un jucător care deține controlul asupra unei infrastructuri critice folosește această poziție pentru a bloca inovația sau pentru a restricționa accesul altor dezvoltatori. În plus, consiliile de etică în inteligența artificială, fie că vorbim despre consilii la nivelul Comisiei Europene, fie despre entități la nivelul unor state membre, au început să elaboreze ghiduri privind modul în care algoritmiile pot fi proiectați pentru a evita discriminarea, pentru a respecta demnitatea umană și pentru a fi transparenți în deciziile lor automate.

În planul securității naționale și strategice, organismele guvernamentale ce gestionează informații sensibile sau protecția infrastructurilor critice au un interes major în a se asigura că fluxurile de date urbane dintr-un Metavers nu pot fi deturnate sau exploatare de entități ostile.

În contextul planificării urbane și al agriculturii urbane, dacă operatorii de platforme colectează cantități masive de date despre infrastructura unui oraș, despre fluxurile de trafic, despre rețeaua de alimentare cu apă și energie, despre rețelele de transport public ori despre activitatea companiilor și a populației, devine crucial ca aceste informații să nu ajungă în mâinile actorilor care pot să le folosească pentru a lansa atacuri cibernetice sau alte tipuri de ingerințe.

Din acest motiv, legislația ce reglementează accesul la date, condițiile de stocare și transfer transfrontalier, precum și politicile de securitate cibernetică trebuie să fie foarte clar definite. Organismele naționale de apărare și instituțiile responsabile de gestionarea infrastructurilor critice colaborează frecvent cu autoritățile de supraveghere a protecției datelor și cu alte entități de reglementare, pentru a se asigura că interesul public primează și că nu se creează riscuri pentru stabilitatea țării.

În același timp, aceste autorități nu pot ignora necesitatea de a stimula inovația și competitivitatea, ceea ce implică găsirea unui echilibru delicat: prea multe restricții pot îngreuna inițiativele private și pot încetini progresul tehnologic, prea puține restricții pot pune în pericol datele și pot crea haos pe piață. De aceea, instituțiile de supervizare și reglementare acționează adesea prin consultări publice, apeluri la experți, colaborări cu organizații profesionale și parteneriate cu universități, pentru a elabora politici bazate pe cunoaștere aprofundată și pentru a anticipa posibilele efecte secundare ale reglementărilor. Cadrul pe care aceste instituții îl creează se extinde dincolo de protecția strictă a datelor. Ele stabilesc inclusiv reglementări privind protecția consumatorului atunci când vine vorba de tranzacții virtuale: într-un Metavers care oferă posibilitatea de a achiziționa obiecte digitale, spații virtuale ori NFT-uri, instituțiile de supraveghere se asigură că există reguli transparente de rambursare, de mediere a conflictelor și de informare asupra costurilor.

De asemenea, se au în vedere aspecte ce țin de reclamă și marketing în medii imersive, unde consumatorii pot fi expuși unor forme noi de publicitate

personalizată, care poate fi intruzivă sau poate genera forme subtile de influențare a comportamentului.

În momentul în care se adaugă și tema imaginilor satelitare, devine relevant ca instituțiile de reglementare să stabilească limitele și condițiile pentru utilizarea acestor date, cu atât mai mult cu cât ele pot dezvălui informații sensibile despre structurile strategice ale unui oraș, pot fi folosite pentru studii de mediu și planificare urbană, dar pot fi și exploatate în scopuri mai puțin onorabile, precum monitorizarea neautorizată a populației sau spionarea unor facilități militare. Astfel, există linii directoare privind rezoluția maximă a imaginilor, modul în care pot fi stocate și cui pot fi distribuite, pentru a asigura un echilibru între beneficiile deschiderii și riscul scurgerilor de informații strategice.

Instituțiile de supervizare pot susține, de asemenea, planificarea urbană cât și agricultura urbană prin promovarea unor programe de open data, menite să ofere publicului acces la datele colectate de administrațiile publice, astfel încât antreprenorii și cercetătorii să poată dezvolta aplicații inovatoare, iar cetățenii să poată monitoriza transparența și eficiența instituțiilor locale.

Acest lucru sporește gradul de implicare și încurajează proiectele de tip civic tech, în care voluntarii sau startup-urile colaborează cu municipalitățile și creează soluții ce îmbunătățesc calitatea vieții, de la reducerea poluării până la creșterea suprafețelor verzi disponibile pentru comunitate. Desigur, politica de date deschise trebuie dublată de asigurarea protecției confidențialității atunci când datele pot dezvălui informații personale despre indivizi, de exemplu despre modul în care se deplasează într-un cartier ori despre ce tipuri de servicii accesează. Din această cauză, anonimizarea și agregarea datelor devin tehnici obligatorii pentru instituțiile care publică seturi de date.

Instituțiile de supervizare și reglementare joacă un rol important și în promovarea transparenței și responsabilității furnizorilor de platforme Metavers și a dezvoltatorilor de aplicații. Ele pot să impună obligații de raportare, cerând companiilor să prezinte periodic informații despre volumele de date colectate, despre incidentele de securitate, despre solicitările de acces la date din partea autorităților și despre modul în care răspund cererilor utilizatorilor de a-și exercita drepturile de confidențialitate.

Prin aceste rapoarte, se poate evalua gradul de respectare a prevederilor legale și se pot identifica posibile zone de risc. Totodată, autoritățile pot solicita ca marile companii să-și publice politicile de utilizare a datelor într-un limbaj clar și să ofere interfețe accesibile, astfel încât cetățenii să înțeleagă efectiv ce se întâmplă cu datele lor. Dacă utilizatorii sunt informați și au la dispoziție mecanisme rapide de reclamare, e mai puțin probabil să apară situații de abuz sistematic.

Prin acest cadru de reglementare, instituțiile respective stimulează, de asemenea, colaborarea dintre municipalități, universități și sectorul privat. De pildă, atunci când se dorește implementarea unor proiecte ambițioase de smart-city, companiile și cercetătorii pot beneficia de licențe speciale care să le permită prelucrarea unor date relevante și experimentarea de soluții la scară mică, cu condiția să respecte protocoalele de securitate și confidențialitate.

Dacă proiectele se dovedesc a fi viabile și sigure, pot fi extinse la nivelul întregului oraș. În acest mod, cercetarea academică și antreprenoriatul primesc sprijin, iar autoritățile publice se asigură că interesul general este protejat.

La nivel național, în România, există instituții cheie, printre care, Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP), care are rolul principal în aplicarea legislației privind protecția datelor, conform GDPR și altor acte normative.

Atunci când platformele Metavers colectează date ale utilizatorilor români, ANSPDCP poate investiga modul în care acestea aplică principiile de legalitate, corectitudine și transparență, putând dispune amenzi sau corecții acolo unde sunt nereguli.

Pe de altă parte, Ministerul Cercetării, Inovării și Digitalizării (MCID) poate orienta politicile publice astfel încât să se creeze un mediu favorabil dezvoltării tehnologiilor XR, IoT și Metavers, oferind fonduri pentru cercetare și inovare, stabilind linii directe pentru interoperabilitate și colaborând cu mediul privat.

O altă instituție cu atribuții semnificative este Autoritatea Națională pentru Administrare și Reglementare în Comunicații (ANCOM), care se asigură că infrastructura de comunicații – pilonul principal al oricărei platforme online, inclusiv Metavers – funcționează în condiții de concurență loială și că accesul la Internet se extinde uniform, oferind astfel șanse egale pentru inovatori și utilizatori.

La nivel local, Primăria Municipiului București și Consiliul General al Municipiului București pot adopta politici ambițioase de tip smart-city, inclusiv integrate cu Metavers, colaborând cu specialiști pentru a pune la dispoziție date despre trafic, poluare, utilizarea spațiilor publice și eficiența energetică, astfel încât să creeze un context de testare pentru proiecte pilot.

De asemenea, pot stabili parteneriate public-private cu operatori de platforme care creează gemeni digitali ai orașului și pot iniția consultări publice prin care cetățenii să-și exprime preferințele legate de extinderea spațiilor verzi, reconfigurarea transportului urban ori integrarea agriculturii urbane în planurile de dezvoltare.

În toate aceste inițiative, instituțiile de supervizare și reglementare păstrează un ochi atent asupra modului în care datele generate de locuitori și de infrastructurile urbane sunt colectate, asigurând protecția identității și a drepturilor fundamentale, evitând potențialele excese de supraveghere și sancționând organizațiile care nu

respectă legile și regulile de etică. O chestiune specială care se conturează ține de regimul juridic al datelor sensibile și de aspectele transfrontaliere. Dacă un Metavers e găzduit de o companie cu sediul în altă țară sau chiar pe mai multe servere răspândite în diverse zone geografice, apare întrebarea în ce măsură legislația națională se aplică și ce instrumente au la dispoziție autoritățile de supraveghere pentru a-și impune cerințele.

Adesea, cooperarea internațională devine imperativă, bazându-se pe tratate bilaterale sau multilaterale, pe recunoașterea reciprocă a deciziilor administrative sau pe mecanisme cum ar fi Consiliul European pentru Protecția Datelor.

Dacă societatea-gază are filiale în UE și tratează datele cetățenilor europeni, ea este supusă normelor GDPR, ceea ce oferă un instrument solid de enforcement, însă rămân zone de incertitudine ori de conflict atunci când operatorul rezidă într-un stat care nu recunoaște aceleași standarde privind confidențialitatea.

Astfel, instituțiile de supervizare au sarcina dificilă de a naviga în acest peisaj legislativ fragmentat și de a găsi soluții care să păstreze protecția individului la un nivel înalt, fără să închidă calea colaborării transfrontaliere.

În plus, rolul consiliilor de etică pentru inteligența artificială devine mai proeminent, deoarece tot mai multe operațiuni din Metavers implică algoritmi care prelucrează date masive, de exemplu pentru recunoaștere gestuală, analiză comportamentală, personalizarea conținutului, publicitate contextuală sau recomandări de rute de transport. Acești algoritmi pot genera fenomene de discriminare indirectă, de manipulare psihologică sau de polarizare socială, ceea ce ridică probleme spinoase cu privire la legitimitatea și impactul lor.

Consiliile de etică dezvoltă standarde și bune practici privind transparența, explicarea și responsabilizarea algoritmilor, iar instituțiile de supraveghere le pot integra în setul lor de cerințe, solicitând operatorilor să demonstreze conformitatea.

Dacă, în planul agriculturii urbane, deciziile cu privire la distribuirea resurselor de apă, amplasarea serelor sau selecția culturilor se fac prin algoritmi antrenați pe date istorice, devine obligatoriu ca acești algoritmi să fie supravegheați, pentru a nu introduce bias-uri care să favorizeze anumite categorii de zone urbane și să le discrimineze pe altele, consolidând inegalități existente. Consiliile de etică pot formula metodologii de audit algoritmic, astfel încât decidenții publici și operatorii privați să poată verifica la intervale regulate modul în care funcționează sistemele automate și să corecteze eventualele deficiențe. Observăm și un interes din ce în ce mai pronunțat al acestor instituții de reglementare pentru educarea populației și a actorilor implicați în Metavers, considerându-se că regulile, oricât de bine elaborate, nu pot fi eficiente dacă cei vizați nu le înțeleg și nu le pun în aplicare în spiritul lor.

Prin urmare, se recomandă campanii publice de informare, ghiduri pentru companii, cursuri de formare pentru specialiști și crearea unor puncte de contact

unde utilizatorii pot afla rapid ce drepturi au și cum să reacționeze dacă se consideră prejudiciați. De pildă, un cetățean care constată că datele sale sunt colectate fără consimțământ explicit ar trebui să aibă la îndemână o modalitate ușoară de a sesiza autoritățile, iar acestea să reacționeze prompt, clarificând situația și, dacă este cazul, ordonând măsuri reparatorii. Astfel, se construiește un climat de încredere care stimulează adoptarea largă a Metaversului în serviciile publice și private, asigurând totodată că drepturile fundamentale nu sunt compromise.

În lumina acestor considerente, instituțiile de supervizare, reglementare și legiferare devin arhitecții unui spațiu digital în care inovația și protecția interesului general merg mână în mână. Mai mult decât niște simpli emitenți de reguli, ele dobândesc rolul de coordonatori între diverse paliere de guvernare: local, național și internațional, între instituții publice și private, între interese economice și drepturile cetățenilor, între nevoia de a stimula competitivitatea și dorința de a preveni abuzurile și discriminarea.

Un exemplu concret îl reprezintă situația în care un startup din București vrea să lanseze o aplicație de planificare urbană în Metavers, bazată pe date colectate de la mii de senzori amplasați în cartiere și integrată cu imagini satelitare. Fără un cadru legal clar, startup-ul s-ar putea lovi de interdicții privind prelucrarea datelor personale, de neclarități despre cui aparțin datele sau despre cum să le partajeze cu altă platformă care dorește să ofere o soluție de agricultură urbană comunitară.

În schimb, dacă există linii directe emise de ANSPDCP, de Ministerul Cercetării, Inovării și Digitalizării și de Primăria București, care să definească pașii de urmat, condițiile de conformitate și instrumentele de colaborare, startup-ul poate să se dezvolte într-un mod sigur și legal. Această sinergie dintre reglementare și inovație devine, așadar, un factor cheie care determină calitatea proiectelor digitale dintr-un oraș inteligent.

Dincolo de reglementările curente, se prefigurează și noi teme care vor necesita o implicare mai profundă a acestor organisme: extinderea realității mixte și a device-urilor care pot citi date biologice direct de pe corpul utilizatorului, evoluția rețelelor 5G și, pe viitor, 6G, ce permit latențe extrem de reduse și un transfer fulgerător al unor volume mari de date, ascensiunea tehnologiilor cuantice și a criptografiei de nouă generație, care vor schimba radical modul în care se asigură confidențialitatea și securitatea fluxurilor de informații.

Fiecare dintre aceste inovații cere ajustări în legislație, definirea de standarde, cooperare internațională extinsă și, nu în ultimul rând, o atenție sporită la posibile efecte adverse. De pildă, dacă rețelele ultra-rapide facilitează telemedicina avansată și intervențiile chirurgicale la distanță în Metavers, cum asigurăm protecția datelor medicale sensibile și integritatea actului medical în fața unor posibile atacuri cibernetice?

Răspunsurile la asemenea întrebări revin parțial instituțiilor de reglementare, însă nu pot fi oferite cu adevărat decât printr-o muncă de echipă, în care aceste organisme antrenează experți tehnici, companii, mediul academic și societatea civilă pentru a discuta, a experimenta și a conveni asupra celor mai bune practici. La fel de importantă rămâne și capacitatea sistemului judiciar de a înțelege și a aplica legile în situații concret legate de Metavers, de exemplu în caz de litigii privind drepturile de proprietate intelectuală asupra unor obiecte virtuale, în caz de fraudă legată de criptomonede sau atunci când se comit infracțiuni grave ce implică defăimare ori încălcarea vieții private în medii digitale.

Judecătorii și procurorii trebuie să fie la curent cu modul în care funcționează aceste tehnologii, iar legislația procedurală trebuie să permită obținerea, prezentarea și validarea probelor în instanță, chiar dacă ele sunt de natură digitală și pot fi stocate în registre distribuite. În absența unei convergențe între sistemul de reglementare, organele de anchetă, sistemul judiciar și operatorii de platforme, Metaversul riscă să devină un fel de „Wild West” virtual, în care legea nu poate fi aplicată în mod eficient.

De altfel, un alt aspect controversat este jurisdicția, fiindcă Metaversul este prin definiție global, iar un utilizator poate să opereze într-un spațiu digital găzduit fizic pe alte continente, supus altor legislații. Din acest motiv, o parte din eforturile organismelor internaționale se îndreaptă către armonizarea regulilor și crearea unor standarde minime, general acceptate, astfel încât entitățile care acționează în Metavers să nu-și poată ascunde practicile abuzive sub scutul lacunelor legislative dintr-o anumită țară. Totuși, nu se poate nega existența diferențelor culturale și politice care fac dificilă obținerea unui consens deplin, ceea ce înseamnă că, pe termen scurt și mediu, vom continua să ne confruntăm cu fragmentarea normativă. Prin această perspectivă, un rol major revine organizațiilor neguvernamentale și asociațiilor profesionale ce pot exercita presiune asupra guvernelor și companiilor, cerând practici mai transparente și responsabile, lansând campanii de advocacy și participând la consultări publice.

Ele pot semnala eventualele abuzuri și pot iniția acțiuni colective pentru apărarea drepturilor utilizatorilor, iar organismele de supervizare pot fi receptive la aceste semnale, ajustându-și strategia de control și prioritățile de monitorizare. De asemenea, institutele de cercetare și think-tank-urile specializate pot contribui la elaborarea unor scenarii privind viitorul Metaversului și la evaluarea impactului social și economic al tehnologiilor emergente. Astfel, importanța organismelor de supervizare, reglementare și legiferare într-un univers dominat de tehnologii digitale nu poate fi subestimată, și cu atât mai mult când discutăm despre Metavers, unde granița dintre real și virtual se estompează, iar datele devin materia primă a majorității activităților.

Importanța colaborării dintre stakeholderi

Importanța colaborării dintre stakeholderi în guvernanța datelor devine evidentă atunci când ne uităm la amploarea și complexitatea transformărilor prin care trec orașele, mai ales în contextul digitalizării accelerate și al provocărilor climatice. Fiecare categorie de actori – fie că vorbim despre utilizatori, furnizori de platforme Metavers, dezvoltatori de aplicații, antreprenori, autorități publice și organisme de reglementare – intră în acest ecosistem cu propriile competențe, interese și obiective specifice. De pildă, dacă ne uităm la stabilirea unor obiective comune privind neutralitatea climatică și dezvoltarea sustenabilă a orașelor, devine limpede că niciuna dintre părțile implicate nu poate aborda singură magnitudinea acestor provocări. Autoritățile publice pot emite strategii generale și pot asigura un cadru legal, însă au nevoie de parteneriat cu furnizori de platforme care să faciliteze colectarea și analiza datelor despre trafic, consum de resurse ori calitatea aerului. Dezvoltatorii de aplicații și antreprenorii, la rândul lor, pot folosi aceste date pentru a crea instrumente care optimizează mobilitatea, reduc costurile energetice și sporesc calitatea vieții, însă depind de implicarea utilizatorilor și de feedbackul lor pentru a ajusta soluțiile la nevoile reale ale comunității.

Dincolo de aceste scopuri generale, există și nevoia de a elabora politici de date echitabile și transparente, ceea ce impune un nivel ridicat de cooperare, deoarece guvernanța datelor se referă atât la aspecte tehnice – precum structura bazelor de date, algoritmi de securitate, protocoalele de interoperabilitate – cât și la probleme etice și juridice. Utilizatorii, de exemplu, au drepturi privind confidențialitatea și controlul asupra propriilor informații, însă aceste drepturi trebuie să fie implementate și protejate de furnizori de platforme care stabilesc regulile de colectare și stocare, de dezvoltatori de aplicații care creează instrumentele de analiză și de autoritățile care pot interveni atunci când apar abuzuri sau neconformități legislative.

Într-o lume ideală, colaborarea dintre toți acești actori se manifestă încă din fazele incipiente ale proiectării unor soluții urbane inteligente, astfel încât mecanismele de protecție a datelor să fie integrate nativ și să nu apară, ulterior, ca simple remedieri impuse după ce anumite vulnerabilități ies la iveală. Simetric, cooperarea conferă un cadru propice pentru evaluarea riscurilor și impactului asupra diferitelor grupuri de populație, evitând amplificarea inechităților sociale prin tehnologii care ar putea, dacă sunt prost gestionate, să dezavantajeze cetățenii din zonele cu infrastructură digitală precară sau pe cei care nu au cunoștințele necesare pentru a folosi noile platforme.

Pe lângă coerența în elaborarea și aplicarea politicilor, prin colaborarea dintre stakeholderi se creează un ecosistem de inovație în care ideile și soluțiile noi sunt

testate rapid, iar feedbackul din partea utilizatorilor ajunge imediat la dezvoltatori și autorități, care pot remedia curențele de securitate sau de funcționalitate. Un exemplu relevant ar fi dezvoltarea de aplicații de tip Digital Twin pentru orașe, în care datele satelitare, informațiile oferite de senzori IoT și simulările 3D din Metavers se îmbină pentru a reda, în timp real, comportamentul unei zone urbane.

Pentru fiecare nevoie identificată, soluțiile trebuie validate și monitorizate, iar acest proces devine o buclă de feedback permanent, în care colaborarea între toți actorii scurtează timpul de răspuns și îmbunătățește calitatea deciziilor. Însă, pentru toate aceste beneficii, există în egală măsură provocări majore care solicită aprofundarea și extinderea colaborării dintre stakeholderi. Una dintre aceste provocări este interoperabilitatea între platforme: astăzi, Metaversul este un concept fragmentat, cu multiple ecosisteme care nu comunică eficient între ele și care potențează inegalități tehnologice. Fără un efort comun de standardizare, cu implicarea marilor companii tehnologice, a universităților și a grupurilor de lucru internaționale, riscăm să avem un număr mare de aplicații incapabile să facă schimb de date într-un mod coerent, ceea ce limitează puterea de acțiune a planificării urbane sau a agriculturii urbane inteligente. În plus, securitatea cibernetică devine un subiect care nu mai poate fi lăsat la latitudinea unei singure companii, pentru că scurgerile de date sau atacurile ransomware nu cunosc granițe și pot sabota simulări vitale pentru gestionarea traficului, pentru distribuția apei sau pentru strategii de evacuare în situații de urgență.

Transparența în acest domeniu poate salva atât resurse cât și vieți, deoarece o breșă de securitate într-un sistem de management urban care coordonează semafoarele poate avea consecințe asupra ordinii publice, iar un atac asupra unei platforme de partajare a datelor despre poluare poate induce decidenților politici concluzii greșite, cu rezultate potențial dezastruoase pentru mediul înconjurător.

Un alt subiect delicat care necesită o abordare colaborativă îl reprezintă etica inteligenței artificiale, deoarece algoritmi care interpretează date despre comportamentul uman în mediul urban și în Metavers pot introduce, dacă nu sunt atent reglați, forme subtile de discriminare sau segregare. Această discriminare poate apărea atunci când seturile de date istorice prezintă deja inechități sociale sau geografice, pe care algoritmul, nefiind proiectat să le recunoască și să le corecteze, le perpetuează. Spre exemplu, un sistem automat de planificare a infrastructurii, antrenat pe date provenite din zone centrale bogate, poate emite recomandări care favorizează în continuare dezvoltarea acelor zone, neglijând cartierele defavorizate. O soluție la asemenea probleme nu poate fi găsită decât prin colaborare între experții în tehnologie care înțeleg modul de funcționare a algoritmilor, autoritățile publice care au interesul să asigure echitatea socială, și comunitățile direct afectate care pot semnală când se simt nedreptățite sau marginalizate.

Tot cooperarea devine critică pentru a rezolva problema accesului echitabil la tehnologii, deoarece disparitățile digitale se mențin sau chiar se accentuează, pe măsură ce platformele avansează către soluții XR, realitate augmentată ori rețele 5G și 6G. Dacă nu există politici coerente prin care să se asigure acces la internet de bandă largă și echipamente minime, o mare parte a populației riscă să rămână în urmă, neputând utiliza serviciile urbane inteligente și neputând profita de oportunitățile de angajare ori de învățare pe care Metaversul le poate facilita. Actorii privați, stimulați de oportunități de afaceri, pot investi în infrastructura digitală a zonelor prospere, însă este nevoie de efortul autorităților și al organizațiilor non-profit pentru a direcționa investiții și către zonele rurale sau cartierele sărace. Fără un mecanism de sprijin și fără programe specifice de reducere a decalajului digital, orice evoluție tehnologică va accentua, în loc să atenueze, disfuncționalitățile urbane și va crea noi falii în rândul populației.

Pe lângă asigurarea accesului, colaborarea este importantă și în ceea ce privește educația și conștientizarea publică, pentru că oricât de bine ar fi concepute aplicațiile și infrastructurile digitale, totul depinde de gradul în care oamenii sunt pregătiți să le adopte și să le integreze în viața lor cotidiană. O municipalitate poate colabora cu universitățile și cu asociațiile civice pentru a organiza ateliere, demonstrații și cursuri despre cum se utilizează Metaversul în planificarea urbană sau despre cum pot fi administrate ferme urbane inteligente care folosesc senzori IoT.

Școlile și liceele pot introduce module de formare care să stimuleze interesul copiilor și tinerilor pentru tehnologiile XR și pentru noțiunile de bază legate de protecția datelor și securitatea online. Într-un asemenea efort integrat, firmele private pot sponsoriza hackathoane și concursuri, instituțiile publice pot oferi date deschise pentru exerciții practice, iar organizațiile non-profit pot anima comunitățile locale, astfel încât cei implicați să învețe prin practică avantajele colaborării și să recunoască potențialul social și economic al noilor tehnologii.

Prin acest tip de conlucrare, oamenii capătă încredere în Metavers și în aplicațiile inteligente, iar implementarea devine mult mai lină, deoarece sunt diminuate rezistențele cauzate de temeri legitime sau de dezinformare. În mod evident, guvernanța datelor este piatra de temelie ce permite ca impactul inovației tehnologice să fie benefic și de lungă durată. Prin adoptarea unor principii comune – cum ar fi transparența, responsabilitatea, consimțământul informat și minimizarea colectării de date – fiecare stakeholder își poate exercita rolul fără a încălca drepturile celorlalți.

Mai mult, cooperarea stimulează apariția unui mecanism de autoreglare, în care operatorii de platforme sunt motivați să mențină standarde ridicate de securitate, dezvoltatorii de aplicații implementează modele de design etic și optimizat pentru confidențialitate, autoritățile publice se asigură că procesele de planificare și decizie includ componenta digitală și perspectivele cetățenești, iar utilizatorii știu că se pot

baza pe un ansamblu de reguli clare pentru a-și proteja și valorifica propriile date. Astfel, colaborarea dintre stakeholderi este, în realitate, un proces de negociere continuă care asigură un echilibru între diverse interese: economice, sociale, de mediu și juridice.

Un exemplu tipic se întâmplă atunci când se dorește implementarea unei soluții XR pentru managementul traficului urban: autoritățile doresc să reducă emisiile și aglomerația, firmele de transport vor să-și optimizeze costurile și să crească numărul de curse, dezvoltatorii de aplicații caută să propună interfețe prietenoase cu utilizatorul și să colecteze date care să permită predicții sofisticate, iar cetățenii vor un oraș mai respirabil și un sistem de transport care să funcționeze fără blocaje. Printr-un demers comun, se poate dezvolta o aplicație mobilă care colectează date despre fluxurile de trafic, le corelează cu semafoarele inteligente și încurajează folosirea transportului public sau a vehiculelor ecologice, totul realizându-se cu un nivel ridicat de securitate a datelor, astfel încât oamenii să nu se simtă supravegheați în mod nejustificat.

În lipsa unei colaborări puternice, acest proiect ar putea să se blocheze fie din cauza reticenței cetățenilor, fie din cauza lipsei de resurse tehnice, fie din cauza unui cadru legislativ inadecvat care nu reglementează clar drepturile și responsabilitățile fiecărui partener. Din fericire, există deja exemple și modele de bună practică, în care stakeholderii reunesc cunoștințele și resursele lor, generând rezultate notabile în domeniul eficientizării energetice, al reorganizării spațiului urban, al dezvoltării agriculturii inteligente și al promovării economiei circulare.

Pentru a aplica aceleași standarde de protecție a datelor, de etică a inteligenței artificiale și de interoperabilitate, este nevoie de dialog între guverne, companii multinaționale, organizații internaționale și rețele de cercetare, astfel încât soluțiile testate la scară locală să poată fi transferate și adaptate altor contexte. Numai astfel se pot reduce costurile, se pot disemina inovări tehnologice și se poate accelera tranziția globală spre orașe mai prietenoase cu mediul și cu locuitorii lor.

Pe termen lung, construirea unei culturi a colaborării reprezintă o investiție cu beneficii multiple, deoarece consolidează reziliența orașelor și a comunităților în fața șocurilor de natură economică, sanitară sau climatică și pregătește terenul pentru adaptările viitoare pe care progresul tehnologic le va cere. Nu trebuie uitat faptul că acest progres tehnologic este doar o componentă dintr-un ansamblu mai larg, în care factorul uman, politic și cultural joacă un rol la fel de vital. Cu cât stakeholderii reușesc să își sincronizeze demersurile și să comunice într-o manieră deschisă, cu atât mai mult pot orienta inovația spre scopuri colective, respectând nevoile individuale și protejând mediul.

Prin astfel de eforturi, orașele se pot transforma în spații vii, în care tehnologiile de ultimă generație lucrează în beneficiul tuturor, iar guvernarea datelor se impune

ca fundament pentru dezvoltarea sustenabilă, pentru coeziune socială și pentru respectul față de drepturile omului. Aceasta este puterea colaborării într-un domeniu în care niciun actor nu are monopol asupra cunoașterii, ci fiecare poate contribui cu ceva unic la construcția unei societăți mai bune, mai reziliente și mai incluzive.

Provocările guvernancei datelor în Metavers

Metaversul în esență este o rețea interconectată de lumi virtuale și medii digitale accesibile prin tehnologii de realitate virtuală, augmentată sau mixtă, ridică o serie complexă de provocări privind guvernancea datelor, mai ales într-un context în care platformele și aplicațiile sunt dezvoltate de entități diverse, iar utilizatorii sunt din ce în ce mai numeroși și activi.

Una dintre cele mai importante probleme privește proprietatea și controlul datelor, fiind dificil de stabilit cine deține drepturile asupra informațiilor generate în medii virtuale și cum se exercită efectiv acest control atunci când infrastructura este descentralizată prin tehnici de tip Blockchain sau prin rețele distribuite.

Într-un model clasic, datele sunt găzduite pe serverele unei entități centrale care are autoritatea de a decide ce se întâmplă cu aceste informații, însă tranziția spre un Metavers alimentat de multiple platforme concurente și interoperabile face ca rolul actorilor să devină mult mai fluid. De exemplu, un creator de conținut care își publică lucrările sub forma unor obiecte 3D sau NFT-uri într-o lume virtuală poate pretinde o anumită formă de proprietate intelectuală asupra acestor elemente, însă datele despre comportamentul utilizatorilor, modul în care interacționează cu obiectele sau despre parametrii tehnici din spate revin, de multe ori, fie platformei centrale, fie se află într-un ledger comun gestionat de participanții rețelei.

Această fragmentare a responsabilităților duce la o necesitate stringentă de clarificare a drepturilor de folosire a datelor și de consimțământ, dar și la definirea unor mecanisme de guvernance care să permită o administrare corectă și echitabilă a informațiilor, inclusiv a datelor personale sau a metadatelor care ar putea dezvălui comportamente și preferințe ale utilizatorilor. În plus, implicațiile juridice sunt foarte variate întrucât anumite jurisdicții pot recunoaște forme de proprietate digitală, în timp ce altele nu oferă un cadru legal clar, iar acest lucru îngreunează și mai mult construcția unui model global de guvernance pentru datele din Metavers.

Concomitent, în Metaversul contemporan și emergent, confidențialitatea și securitatea datelor reprezintă cele mai sensibile subiecte, având în vedere volumul enorm de informații colectate și caracterul potențial invaziv al interacțiunilor virtuale. Avatarele, de pildă, nu mai sunt simple reprezentări grafice, ci pot fi strâns legate de datele biometrice ale utilizatorilor, fie că este vorba de expresii faciale, mișcări

oculare, tipare vocale ori ritm cardiac detectat de dispozitive portabile. Integrarea acestor date în mecanismele de feedback și personalizare a experiențelor virtuale generează riscuri majore de confidențialitate, în special dacă operatorii platformelor nu implementează măsuri avansate de criptare și de protecție a identității digitale.

Într-un Metavers cu multiple lumi virtuale, breșele de securitate pot deveni un coșmar pentru utilizatori, care s-ar putea confrunta cu scurgeri de informații sensibile, cu furt de identitate sau cu diverse forme de manipulare a comportamentului, în funcție de scopul rău intenționat al unor actori. Mai mult decât atât, spre deosebire de mediile digitale tradiționale, Metaversul se apropie de conceptul de prezență imersivă și participare corporală, ceea ce înseamnă că datele colectate pot fi mult mai bogate și pot dezvălui aspecte intime, imposibil de protejat prin metode clasice de anonimizare. Astfel, dezbaterea despre confidențialitate capătă o nouă dimensiune, iar soluțiile tehnice și organizatorice trebuie să țină pasul cu complexitatea interacțiunilor: criptarea end-to-end a comunicațiilor și datelor de telemetrie, controlul granular al accesului la date, implementarea principiilor de privacy by design și privacy by default, asigurarea că orice colectare și prelucrare are un temei legal solid și un scop clar, toate devin fundamentale. Chiar dacă un furnizor de platformă promite securitate maximă, utilizarea standardelor actuale poate fi insuficientă în fața unor vectori de atac rafinați, astfel că e necesară o abordare holistică ce implică monitorizare constantă, actualizări frecvente, audit extern și protocoale stricte de răspuns la incidente.

Pe lângă aceste teme legate de proprietate, control, securitate și confidențialitate, interoperabilitatea și portabilitatea datelor constituie un alt obstacol major în calea unei guvernante eficiente și transparente a Metaversului. Pentru ca Metaversul să devină cu adevărat un spațiu în care utilizatorii își pot muta fără dificultăți avatarurile, inventarele de obiecte virtuale, istoricul interacțiunilor sau datele de progres între diverse medii virtuale și platforme, este nevoie de standarde comune și protocoale clare de schimb de date.

În prezent, numeroase proiecte și platforme adoptă propriile formate de fișiere și structuri de date, fapt care blochează transferul simplu și rapid al informațiilor, generând așa-numitele insule digitale în care datele rămân captive. La nivel conceptual, noțiunea de interoperabilitate și portabilitate se leagă strâns de ideea că utilizatorul ar trebui să dețină controlul efectiv asupra propriilor date și să poată decide să le folosească în orice ecosistem virtual dorește, fără a fi constrâns de limitări tehnice sau de politici restrictive impuse de un operator.

Un scenariu ideal ar fi cel în care un avatar, cu toate însușirile sale vizuale, abilitățile și bunurile virtuale, poate tranzita dintr-o platformă de joc sau socializare în alta, păstrându-și identitatea și istoricul. Însă, în absența unor protocoale recunoscute la scară largă, implementarea acestui ideal rămâne dificilă, fiind nevoie

de colaborări extinse între dezvoltatorii de software și furnizorii de servicii și, totodată, de un cadru de reglementare care să stipuleze modul în care datele sunt gestionate, actualizate și protejate pe parcursul transferului. Dacă interoperabilitatea are o dimensiune tehnică, portabilitatea are și o componentă juridică și economică, întrucât accesul la datele de pe o platformă terță poate fi privit ca un avantaj competitiv și, prin urmare, unii operatori pot fi reticenți să deschidă porțile pentru concurenți. În plus, datele despre obiecte virtuale și avataruri pot să aibă o valoare monetară ridicată în anumite ecosisteme, îngreunând și mai mult negocierea unor standarde comune. Cu toate acestea, lipsa interoperabilității subminează potențialul creativ și economic al Metaversului, întrucât limitează posibilitatea utilizatorilor de a-și folosi conținutul și datele în mod liber în diverse contexte și constrânge inovația la nivelul dezvoltatorilor independenți.

A patra mare provocare este conformitatea cu reglementările, un aspect care decurge organic din celelalte trei, dar care necesită o atenție deosebită atât din partea autorităților, cât și din partea entităților care operează platforme sau dezvoltă tehnologii asociate Metaversului. În momentul de față, cele mai relevante cadre de reglementare privesc protecția datelor personale și confidențialitatea, în mod special Regulamentul General privind Protecția Datelor (GDPR) la nivel european și alte legi naționale ori regionale, cum ar fi California Consumer Privacy Act (CCPA) în Statele Unite ale Americii.

Aceste acte normative au fost concepute într-un context dominat de platforme web și aplicații mobile, însă Metaversul extinde radical tipul și cantitatea de date colectate, precum și modalitățile prin care utilizatorii își pot da sau retrage consimțământul. De pildă, colectarea datelor biometrice sau a datelor despre comportamentul emoțional în timpul unei experiențe de realitate virtuală ridică întrebări noi cu privire la categorii speciale de date care necesită protecție suplimentară, iar conceptul de pseudonimizare devine mult mai complicat dacă elementele observate în mediu virtual pot duce cu ușurință la reidentificarea persoanei. În plus, apar dificultăți în stabilirea jurisdicției și a competenței teritoriale, deoarece, într-un Metavers cu adevărat global, utilizatorii interacționează în spații virtuale care pot fi operate de companii înregistrate în diverse țări, cu legislații diferite și nearmonizate. Astfel, dacă o persoană dintr-o țară europeană își creează un avatar și interacționează cu un alt utilizator din Statele Unite pe o platformă cu sediul în Asia, devine foarte complicat să se determine care autoritate de supraveghere are competența de a reglementa folosirea datelor și care legislație trebuie aplicată. În acest sens, conformitatea cu reglementările devine nu doar o chestiune de respectare a unor principii generale de protecție a datelor, ci și o problemă de cooperare internațională, care să asigure un minimum de standarde comune acceptate de toate părțile implicate.

Pe lângă regulile existente, se prefigurează și noi reglementări care vizează aspecte precum inteligența artificială, conținutul generat de utilizatori, drepturile de proprietate intelectuală aplicate mediilor virtuale și responsabilitățile platformelor în combaterea dezinformării sau a abuzurilor. Așadar, pentru a respecta aceste cerințe și a evita sancțiunile, operatorii Metaversului și dezvoltatorii trebuie să adopte strategii avansate de guvernare a datelor, să investească în formarea echipelor juridice și în sisteme de conformitate, să implementeze mecanisme de trasabilitate și audit, precum și să creeze instrumente transparente prin care utilizatorii pot gestiona, modifica, exporta sau șterge datele proprii.

În concluzie, proprietatea și controlul datelor, confidențialitatea și securitatea acestora, interoperabilitatea și portabilitatea, precum și conformitatea cu reglementările constituie patru piloni majori ai guvernării datelor în Metavers, fiecare dintre ei aducând un set specific de provocări tehnice, juridice și etice.

Oportunități pentru guvernarea datelor în Metavers

Guvernarea datelor în Metavers nu se rezumă la rezolvarea unor probleme de natură tehnică sau juridică, ci oferă și numeroase oportunități care pot transforma acest mediu virtual într-un spațiu mai echitabil, mai sigur și mai propice dezvoltării inovației. Unul dintre cele mai mari avantaje ale unei guvernări eficiente este posibilitatea de a oferi utilizatorilor un control sporit asupra propriilor date, întrucât realitatea virtuală imersivă face ca datele despre comportamentul și preferințele lor să fie mult mai diverse și cu un potențial mai mare de a dezvălui aspecte sensibile ale identității personale.

În mod tradițional, platformele sociale și de gaming colectau masiv informații despre utilizatori, însă cu o guvernare concepută în spiritul controlului individual, se poate crea cadrul prin care fiecare persoană să poată alege cum și când își partajează datele, cum dorește să își gestioneze identitatea virtuală și care sunt setările de confidențialitate pe care le consideră potrivite. Astfel, un avatar ar putea fi asociat cu un minim de date personale sau, dimpotrivă, cu date precise și biometrice, în funcție de scopul experienței și de preferințele celui care utilizează platforma. Acest control mai bun se poate traduce, spre exemplu, în posibilitatea de a decide ce informații sunt disponibile în profilul public, cui i se permite accesul la istoricul interacțiunilor virtuale și cum sunt stocate înregistrările audio sau video ale discuțiilor, toate acestea având un rol determinant în construirea unei încrederi de lungă durată între platforme și comunitățile de utilizatori. Un alt aspect al acestui control sporit asupra datelor se referă la dreptul de portabilitate, care devine mai simplu de exercitat atunci când există proceduri clare și interfețe tehnice unificate, prin care oamenii pot exporta și importa informațiile despre ei și despre obiectele virtuale deținute.

Dacă, în trecut, utilizatorii aveau un sentiment de captivitate în interiorul unei platforme, lipsiți de posibilitatea de a-și muta progresul sau resursele virtuale într-un alt mediu, o guvernare modernă poate prevedea mecanisme prin care aceștia să poată face tranziția fără a-și pierde datele, dând naștere unei noi ere a libertății digitale. Aceste practici consolidează ideea că datele personale nu sunt un bun exclusiv al platformei, ci aparțin în primul rând persoanei în cauză, iar controlul exercitat de aceasta contribuie la prevenirea abuzurilor și la dezvoltarea unui climat de transparență și bună-credință. Prin concentrarea pe protecția datelor și definirea clară a responsabilităților fiecărui actor implicat, se reduc șansele ca datele să fie valorificate necorespunzător, de exemplu în scopuri publicitare intruzive sau pentru profilare excesivă. În același timp, controlul mai mare asupra datelor personale devine un factor care poate stimula creativitatea și adoptarea unor forme noi de interacțiune: avatarele personalizate, obiectele virtuale cu valoare simbolică sau artistică, mecanisme de storytelling în care utilizatorul poate gestiona gradul de implicare emoțională și identitatea afișată într-un anumit context.

O a doua oportunitate remarcabilă adusă de o guvernare solidă este creșterea calității și a utilității datelor disponibile în Metavers. Atunci când nu există reguli clare și standarde comune privind colectarea, validarea și stocarea informațiilor, datele pot deveni incoerente, incomplete sau contradictorii, fapt care poate periclita puterea analitică a platformelor și poate îngreuna procesele de luare a deciziilor. Prin adoptarea unor politici de guvernare care să insiste asupra acurateței și relevanței, se pot stabili fluxuri de lucru menite să verifice și să coreleze datele din surse multiple, să le actualizeze constant și să elimine redundanțele. Această abordare aduce beneficii atât utilizatorilor individuali, care vor avea parte de experiențe mai personalizate și mai bine adaptate nevoilor lor, cât și organizațiilor care activează în Metavers, de la companii și instituții culturale, până la universități și centre de cercetare.

Oricine dorește să construiască aplicații peste infrastructura Metaversului se poate baza pe un depozit de date robust și consistent, ceea ce contribuie la dezvoltarea de soluții care să fie viabile pe termen lung și să răspundă unor nevoi reale. Prin îmbunătățirea calității datelor, partenerii interesați pot obține analize predictive mai precise, pot proiecta modele comportamentale mai apropiate de realitate și pot propune scenarii avansate de interacțiune virtuală, cum ar fi simulări pentru managementul traficului într-un oraș virtual, abordări noi ale telemedicinii sau forme inovatoare de educație digitală.

Calitatea și utilitatea datelor nu țin doar de dimensiunile tehnice, ci și de abordările etice și sociale pe care le încurajează guvernarea, în sensul că o platformă responsabilă va încuraja raportarea și înlăturarea conținutului dăunător, va implementa mecanisme pentru reducerea bruiajului informațional și va cultiva în rândul participanților o cultură a acurateței și fiabilității. Această cultură poate crește

loialitatea față de platformă și gradul de implicare în proiecte comune, deoarece utilizatorii vor avea mai multă încredere că datele pe care le oferă sunt administrate corect, iar datele pe care le primesc în schimb sunt pertinente și valoroase.

În final, o a treia mare oportunitate desprinsă dintr-o guvernare eficientă a datelor în Metavers ține de stimularea inovației și facilitarea colaborării între actori diferiți.

Tranziția spre un mediu virtual complex, în care barierele spațiale dispar și unde ideile pot fi implementate rapid, favorizează apariția unor parteneriate transdisciplinare: artiști care se asociază cu ingineri și designeri de jocuri, companii de software care colaborează cu instituții medicale, startup-uri care caută să rezolve probleme urbane prin simulări virtuale și modele predictive.

Aceste interacțiuni pot lua amploare doar dacă există un cadru clar care să reglementeze cum se partajează datele, cum se împart drepturile de proprietate intelectuală, și ce reguli de confidențialitate și utilizare se aplică, astfel încât niciunul dintre parteneri să nu se simtă expus sau dezavantajat. În lipsa unor politici de guvernare coerente, colaborarea poate fi încetinită de temeri privind scurgerile de informații sensibile, privind furtul de date sau privind folosirea neautorizată a rezultatelor comune.

Pe de altă parte, când există politici care încurajează interoperabilitatea și definirea unor standarde pentru formate de date și protocoale de comunicare, devine mult mai simplu pentru dezvoltatori să creeze punți tehnice între diferite lumi virtuale, să creeze aplicații complementare și să favorizeze un flux liber de informații benefic întregului ecosistem.

Această deschidere duce la o accelerare a progresului tehnologic, fiindcă specialiști din multiple domenii pot lucra împreună la proiecte ample, fără a se izbi de obstacole cauzate de lipsa unor formate unificate sau de absența unor reglementări ferme cu privire la cine poate avea acces la seturi de date comune. Iar inovația nu se rezumă doar la aspectul tehnic, ci și la aplicațiile sociale și culturale, întrucât Metaversul oferă un cadru propice pentru forme de artă colaborativă, expoziții virtuale participative, metodologii educaționale avangardiste și multe alte manifestări la care poate contribui o întreagă rețea globală de creatori. O guvernare încurajatoare și transparentă poate permite chiar și celor fără cunoștințe tehnice avansate să se implice în aceste procese, consolidând sentimentul de apartenență la comunitate și dezvoltând încrederea reciprocă. În plus, datorită unor reguli clare cu privire la drepturile de autor, la recunoașterea contribuției și la remunerarea corectă a creatorilor, talentele nou intrate în ecosistem nu se vor teme că munca lor ar putea fi exploatăată abuziv de terți. Dincolo de colaborarea directă între creatori, guvernarea robustă a datelor deschide calea cooperării între companii și instituții publice, care pot împărtăși seturi de date pentru cercetări științifice, pentru analize de piață,

pentru testarea unor politici publice într-un mediu virtual sau pentru dezvoltarea unor soluții comune de securitate cibernetică. Dacă, spre exemplu, orașele doresc să implementeze un sistem de urbanism inteligent, pot folosi Metaversul ca pe un laborator în care să simuleze scenarii de infrastructură și trafic, având la dispoziție date reale, anonimizate și corect guvernate, ceea ce le permite să extrapoleze rezultate fără a pune în pericol confidențialitatea cetățenilor.

Odată identificate ideile cele mai eficiente, acestea pot fi transpuse în planul real, reducând costurile și riscurile asociate cu experimentele urbane. Astfel, inovația devine nu doar un termen vag, ci un proces concret, alimentat de date de calitate și catalizat de un regim de guvernare care pune accent pe transparență, cooperare și respect față de drepturile tuturor participanților.

Conectând aceste trei beneficii – control sporit pentru utilizatori, calitate crescută a datelor și încurajarea colaborării și inovației – se conturează imaginea unui Metavers mai matur și mai bine articulat, unde factorii de interes, de la indivizi la corporații și guverne, se pot întâlni într-un spațiu imersiv creat pentru a servi obiective comune, fără a sacrifica însă valorile fundamentale ale protecției vieții private și ale echității.

Fiecare pas către o guvernare coerentă sporește stabilitatea și atractivitatea mediului virtual, atât pentru investitori, care pot identifica oportunități de afaceri sustenabile, cât și pentru dezvoltatorii de tehnologie, care pot proiecta soluții scalabile, și mai ales pentru utilizatori, care beneficiază de siguranță sporită, de autonomie și de posibilitatea de a face tranziții fluide între lumi virtuale interconectate.

Pe măsură ce aceste oportunități sunt exploatate, s-ar putea crea noi modele de business bazate pe economia datelor, noi tipare de consum cultural și de producție artistică, precum și rețele de parteneriat, mai ales în domeniile educației și cercetării, în care schimbul de date devine un factor esențial pentru progresul științific.

În plus, dezvoltarea normelor de guvernare poate duce la apariția unor profesii și roluri noi: specialiști în compliance și audit pentru lumi virtuale, consultanți în materie de protecție a datelor și inteligență artificială, moderatori care să asigure respectarea standardelor etice și a reglementărilor în rândul participanților la Metavers, dar și facilitatori de colaborări public-privat menite să creeze soluții comune pentru problemele complexe ale societății.

Dintr-o perspectivă globală, un Metavers guvernat corect poate favoriza incluziunea, deoarece persoanele care trăiesc în zone dezavantajate sau care au limitări fizice pot participa în mod egal la activități economice, sociale și educaționale, cu condiția să li se asigure infrastructura minimă de acces. Dacă datele sunt administrate într-un mod transparent și deschis, iar instrumentele de protecție a confidențialității sunt integrate în mod nativ, atunci și grupurile vulnerabile pot beneficia de oportunitățile acestui spațiu virtual, fără teamă că datele lor personale

ar putea fi folosite împotriva lor sau fără riscul de a fi excluse din cauza unor limitări tehnice ori economice.

Poate că, în acest sens, cea mai mare oportunitate constă exact în capacitatea guvernantei de a fi un catalizator pentru cooperare și experimentare, de a găsi puncte comune între entități aparent diferite și de a oferi o structură unitară prin care datele să devină mai mult decât simple active digitale – să devină resurse de evoluție, cunoaștere și creștere incluzivă.

Principiile cheie ale guvernantei datelor în Metavers

Guvernanța datelor în Metavers devine un subiect tot mai important pe măsură ce tot mai multe persoane, utilizatori și organizații își extind activitățile în universuri virtuale interconectate, folosind tehnologii de realitate virtuală, augmentată sau mixtă și dezvoltând platforme complexe în care datele circulă pe multiple canale. Într-un asemenea mediu, principiile cheie ale guvernantei datelor au menirea de a asigura că drepturile utilizatorilor sunt protejate, că inovația și colaborarea sunt încurajate, iar riscurile legate de securitate și confidențialitate sunt gestionate eficient.

Unul dintre aceste principii fundamentale este transparența și responsabilitatea, deoarece utilizatorii, creatorii de conținut și dezvoltatorii de platforme trebuie să știe clar ce tipuri de date sunt colectate, în ce scop, cum sunt prelucrate, cine le accesează și ce se întâmplă cu ele pe termen lung. Dacă într-un mediu digital clasic, precum rețelele sociale sau aplicațiile web, au existat deja numeroase scandaluri legate de lipsa de informare și de modul netransparent în care companiile au gestionat datele personale, în Metavers riscurile cresc exponențial, mai ales pentru că volumul și varietatea datelor colectate sunt mult mai mari.

Vorbim nu doar despre simpla înregistrare a numelui, adresei de e-mail sau datelor financiare, ci și despre date de natură biometrică, despre comportamentul și mișcările utilizatorilor în spații virtuale, despre preferințe, reacții emoționale detectate prin senzori și dispozitive portabile, toate acestea putând genera o imagine extrem de fidelă a personalității fiecăruia. Prin urmare, este necesar ca platformele care pun la dispoziție astfel de servicii să ofere politici de confidențialitate redactate într-un limbaj clar, să implementeze panouri de control ușor de înțeles și să raporteze orice eveniment de securitate sau încălcare a drepturilor.

Transparența adevărată nu înseamnă doar publicarea unor termeni și condiții cu un limbaj complex pe care puțini au timp sau răbdare să-l citească, ci implică și comunicarea proactivă și accesibilă despre ce date se colectează, de ce sunt necesare și către cine vor fi partajate. Această abordare stimulează responsabilitatea tuturor

actorilor din Metavers, fie că sunt operatori mari de platforme globale, fie că sunt creatori de conținut independenți sau parteneri de afaceri.

Responsabilitatea presupune existența unor mecanisme clare de trasabilitate și de audit, prin care să se poată verifica dacă datele au fost folosite conform scopului declarat, dacă au fost protejate în mod corespunzător și dacă există un cadru de sancțiuni pentru orice entitate care nu respectă regulile stabilite.

În același timp, responsabilitatea se conectează și cu nevoia de definire a unor standarde etice și a unor organisme de supraveghere care să poată interveni când apar conflicte între diverse părți implicate și să poată rezolva sesizările ori reclamațiile. Mai mult, transparența și responsabilitatea au un impact direct asupra gradului de încredere al utilizatorilor, care reprezintă fundamentul oricărui ecosistem digital sănătos: dacă oamenii nu se simt în siguranță să împărtășească date sensibile sau să își pună la dispoziție resursele creative, proiectele de anvergură din Metavers nu vor putea fi susținute pe termen lung. Un alt principiu fundamental este controlul și consimțământul utilizatorului, care pune accent pe ideea că orice persoană care intră în Metavers are dreptul să decidă ce date pot fi colectate despre ea, cum sunt folosite și cât de mult dorește să își dezvăluie identitatea. Întrucât Metaversul se vrea a fi un mediu mult mai personal și mai captivant decât internetul tradițional, riscul de a colecta date intruzive despre intimitatea oamenilor este mai mare, astfel că asigurarea controlului devine o necesitate în gestionarea datelor. Consimțământul nu trebuie să fie unul formal, obținut prin căsuțe bifate, ci unul informat, care să permită fiecărui utilizator să înțeleagă implicațiile și să aibă oricând posibilitatea de a-și retrage acordul.

Sistemele de guvernanță a datelor bine proiectate trebuie să ofere instrumente practice, cum ar fi panouri de confidențialitate în care să poți alege ce tip de informații permiți să fie colectate (localizarea, tipul de mișcări corporale, reacțiile fiziologice sau datele despre microexpresii faciale) și cum vor fi folosite sau partajate aceste date. Tot la acest capitol, controlul se manifestă și sub forma accesului la datele deja colectate și a posibilității de a le șterge sau rectifica dacă sunt inexacte, precum și a dreptului de portabilitate, prin care utilizatorul își poate lua toate datele și le poate transfera pe o altă platformă. Într-o lume virtuală descentralizată, aceste drepturi devin și mai dificile de aplicat, deoarece pot exista structuri bazate pe Blockchain care stochează înregistrări în mod distribuit, iar ștergerea completă a unei informații poate fi imposibilă din punct de vedere tehnic. Cu toate acestea, un cadru robust de guvernanță ar trebui să stabilească mecanisme prin care datele personale sensibile să fie gestionate într-un mod care respectă cerințele de protecție a vieții private și să existe, pe cât posibil, căi de anonimizare sau pseudonimizare a datelor, dacă ștergerea lor definitivă nu este realizabilă.

Astfel, controlul și consimțământul oferă utilizatorilor siguranța că deciziile lor contează și le permite să participe la Metavers în condițiile pe care ei le consideră acceptabile, ducând la o mai mare diversitate și o mai mare incluziune a publicului în aceste medii virtuale.

Al treilea principiu, și anume minimizarea datelor și limitarea scopului, este o consecință directă a conceptului de confidențialitate încă din faza de proiectare, formulat în legislație, precum Regulamentul General privind Protecția Datelor (GDPR) din Uniunea Europeană, dar devine cu atât mai relevant în Metavers, unde tentația sau chiar necesitatea tehnologică este de a colecta cantități uriașe de informații despre fiecare mișcare și reacție a utilizatorului.

Minimizarea datelor se referă la ideea că platformele și aplicațiile ar trebui să colecteze doar acele informații strict necesare pentru a furniza serviciul promis sau pentru a îmbunătăți experiența utilizatorului, fără a cădea în capcana supravegherii totale și a profilării excesive. Limitarea scopului adaugă la acest concept cerința ca datele să fie folosite doar pentru motivele comunicate inițial, adică dacă cineva își dă consimțământul ca datele legate de modul în care își mișcă brațele în realitatea virtuală să fie folosite pentru a calibra mai bine interfața, aceste date nu ar trebui ulterior folosite pentru a deduce informații despre starea sa de sănătate sau pentru a alimenta campanii publicitare țintite. Prin adoptarea unui principiu strict de minimizare a datelor, se reduce automat și suprafața de atac, deoarece cu cât se acumulează mai puține informații sensibile, cu atât consecințele unei eventuale breșe de securitate sunt mai mici. Totodată, dacă datele sunt adunate doar când este nevoie și pentru un scop clar, șansele ca acestea să fie stocate haotic, să devină redundante și să creeze confuzie sunt mult mai mici.

Pentru dezvoltatorii de conținut și pentru companiile care administrează platforme de Metavers, aplicarea acestui principiu poate părea un obstacol, deoarece unii pot dori să folosească cât mai multe date pentru a-și rafina algoritmi de inteligență artificială, însă abordarea contrară, bazată pe colectarea nelimitată, nu mai este viabilă într-un ecosistem global tot mai sensibil la confidențialitate și securitate.

Pe termen lung, minimizarea datelor și limitarea scopului contribuie la consolidarea încrederii dintre platforme și utilizatori și permite o gestionare mai eficientă a resurselor de stocare și procesare, evitând acumularea de date inutile care îngreunează analizele sau expune companiile la riscuri de reglementare și reputație.

În continuare, un al patrulea principiu esențial în guvernanta datelor pentru Metavers este securitatea și integritatea informațiilor, ceea ce înseamnă că trebuie luate măsuri tehnice și organizatorice robuste pentru a preveni pierderea, alterarea, accesul neautorizat sau folosirea abuzivă a acestora.

Într-o lume virtuală, amenințările cibernetice pot lua forme noi și variate, de la atacuri de tip phishing concepute special pentru spațiul tridimensional, până

la infiltrații în dispozitivele care citesc semnale biometrice, la manipulări ale identității avatarurilor și la breșe în rețelele de tip Blockchain care stochează istoricul tranzacțiilor din Metavers.

Prin urmare, securitatea nu mai poate fi tratată ca un capitol secundar, ci devine parte integrantă a arhitecturii oricărui sistem care operează într-un Metavers sau îl susține. Aceasta implică metode avansate de criptare, testare regulată a vulnerabilităților, implementarea unor protocoale de autentificare multifactor, monitorizare în timp real și reacție promptă la incidente, precum și pregătirea personalului care gestionează infrastructura și a utilizatorilor care trebuie să fie conștienți de riscuri și de regulile de bună conduită online.

Tot la capitolul securitate intră și protecția împotriva comportamentelor abuzive și a hărțuirii, întrucât datele se pot scurge nu doar prin hacking direct, ci și prin tehnici de inginerie socială și manipulare a utilizatorilor. Pentru a menține integritatea datelor, guvernanța trebuie să prevadă mecanisme prin care datele să fie stocate în formate standardizate și fiabile, cu posibilitatea de verificare a autenticității și cu menținerea unui istoric al modificărilor.

În plus, metadatele care descriu sursa și evoluția unui obiect digital ar trebui să fie la rândul lor protejate, pentru ca oricine să poată identifica cu certitudine dacă un document, un fișier sau un bun virtual a fost alterat sau asociat cu altă identitate. Cu cât platformele își dezvoltă mai mult infrastructura bazată pe contracte inteligente (smart contracts) ori pe registre distribuite, cu atât e mai mare nevoia de reguli explicite care să asigure că aceste mecanisme automate nu pot fi exploatate în mod malițios și că datele rămân exacte și de încredere pe întregul parcurs al tranzacțiilor.

Integrarea tuturor acestor principii într-un singur cadru coerent de guvernanță a datelor în Metavers implică un efort comun al actorilor majori din industrie, al autorităților de reglementare, al comunităților de dezvoltatori și de utilizatori, precum și al organizațiilor care promovează drepturile omului și libertățile civile în mediul digital. Transparența și responsabilitatea, controlul și consimțământul utilizatorului, minimizarea datelor și limitarea scopului, plus securitatea și integritatea informațiilor creează un set de repere care, aplicate consecvent, pot face diferența între un Metavers dominat de practici opace și riscante și unul care să fie un model de inovație etică și sustenabilă.

Bune practici pentru guvernanța datelor în Metavers

Din ce în ce mai multe organizații, dar și persoane fizice, își extind activitățile în spații virtuale guvernate de tehnologii avansate de realitate virtuală și augmentată, rețele distribuite și soluții bazate pe inteligență artificială. Pentru a administra într-un

mod adecvat cantitățile masive de date generate într-un asemenea context și a asigura un mediu sigur și corect pentru toți participanții, sunt necesare măsuri puternice de securitate, cooperare între diferiți factori interesați, educația utilizatorilor și, nu în ultimul rând, definirea unui cadru coerent și adaptat particularităților Metaversului.

Una dintre cele mai importante practici de guvernare a datelor în Metavers este dezvoltarea unor politici clare și cuprinzătoare care să răspundă provocărilor unice pe care acest mediu virtual le implică. Într-un spațiu în care limitele dintre real și virtual se estompează și în care avatarurile, obiectele virtuale și interacțiunile sociale pot genera date mult mai detaliate și sensibile decât în mediile digitale convenționale, simplul fapt de a transpune regulile clasice privind protecția datelor cu caracter personal nu mai este suficient. Politicile de guvernare trebuie să facă distincția între tipurile de date colectate și între scopurile diferite în care acestea pot fi utilizate, abordând și modul în care datele biometrice, informațiile de localizare în timp real sau comportamentul utilizatorilor (manifestat sub forma mișcărilor, reacțiilor și chiar indicilor fiziologici detectați de dispozitive portabile) urmează să fie stocate și prelucrate.

O guvernare adecvată trebuie să abordeze și problema drepturilor de proprietate asupra datelor generate în Metavers, fiindcă nu este întotdeauna clar dacă datele aparțin furnizorului platformei, utilizatorului, dezvoltatorului de conținut sau unui partener terț care a creat anumite elemente. În absența unor linii directoare clare și a unor proceduri de gestionare a conflictelor, riscul de a apărea dispute privind drepturile de utilizare și de comercializare a datelor este foarte ridicat, ceea ce ar putea submina încrederea participanților și stabilitatea ecosistemului. Prin urmare, politicile trebuie să enunțe explicit principiile de partajare, să definească procese de arbitraj și să permită oricărui actor să înțeleagă rapid ce drepturi și obligații îi revin atunci când intră în Metavers și interacționează cu ceilalți. În plus, politicile solide de guvernare a datelor trebuie să acopere și situațiile neprevăzute, cum ar fi proiectele-pilot care testează tehnologii emergente sau integrarea unor rețele distribuite care funcționează pe bază de Blockchain, tehnologii ce pot complica procesele de ștergere ori de anonimizare a datelor.

Stabilirea de bune practici privind colectarea, reținerea și eliminarea informațiilor în aceste contexte contribuie la evitarea unor blocaje legale și la consolidarea transparenței în fața utilizatorilor și a partenerilor de afaceri. După conturarea unor politici clare, o altă practică necesară pentru o guvernare eficientă este implementarea unor măsuri solide de securitate a datelor, care să protejeze informațiile de accesul, utilizarea sau divulgarea neautorizată.

Într-un Metavers populat de milioane de utilizatori, care interacționează prin dispozitive VR sau AR, se transmit constant pachete de date prin rețele complexe ce pot fi oricând ținta unor atacuri cibernetice. Astfel, investițiile în tehnologii avansate

de criptare și protecție reprezintă o cerință minimă pentru orice furnizor de platformă ce dorește să-și mențină reputația și să evite consecințe financiare și legale grave. Deși fiecare organizație sau dezvoltator are strategii proprii privind securitatea, există bune practici recunoscute la nivel internațional, precum criptarea end-to-end a fluxurilor de date, protecția conexiunilor cu certificate digitale și implementarea de protocoale robuste de autentificare multifactor pentru conturile de acces la platformă. Colaborarea și comunicarea între părțile interesate este un alt element definitoriu al unor practici eficiente de guvernanță a datelor în Metavers, deoarece un ecosistem complex implică dezvoltatori independenți, furnizori de infrastructură, creatori de conținut, organisme de reglementare, agenții guvernamentale și comunități de utilizatori cu așteptări diferite. Abordarea izolată, în care fiecare platformă își stabilește propriile reguli, ignorând standardele globale și fără a dialoga cu actorii cheie, conduce la fragmentare, la incompatibilități tehnice și la confuzie în rândul celor care doresc să-și mute activitățile între diverse lumi virtuale sau să creeze punți între platforme. Pentru a încuraja colaborarea, pot fi organizate grupuri de lucru care reunesc reprezentanți ai industriei și factorilor de decizie, astfel încât politicile de guvernanță să fie aliniate cu reglementările naționale și internaționale privind protecția datelor, securitatea cibernetică și drepturile utilizatorilor.

Standardele de interoperabilitate și formatele comune de fișiere pot fi stabilite prin acorduri la nivel de consorțiu, în ideea de a permite avatarurilor, obiectelor virtuale și istoricului de date să circule într-o manieră cât mai fluidă, sporind valoarea economică și socială a Metaversului. Cooperarea constructivă poate conduce și la abordări comune în privința luptei împotriva comportamentelor abuzive, a conținutului ilicit și a încălcărilor de proprietate intelectuală, probleme care riscă să escaladeze rapid într-un univers virtual masiv și diversificat.

Un alt aspect major pe care guvernanța datelor în Metavers trebuie să îl abordeze cu prioritate este educația și împuternicirea utilizatorilor, prin care aceștia să fie conștienți de drepturile lor asupra datelor și să poată lua decizii informate cu privire la modul în care informațiile lor sunt colectate, prelucrate sau partajate. În absența unei înțelegeri de bază a riscurilor și a posibilităților de control, mulți utilizatori pot fi manipulați cu ușurință, pot furniza date sensibile fără să conștientizeze consecințele sau pot deveni victime ale atacurilor ciberneticе.

Bunele practici în acest sens includ campanii de conștientizare și materiale educaționale, integrate direct în platformele de Metavers și prezentate într-un limbaj accesibil, care să le explice pas cu pas cum să își seteze parametrii de confidențialitate, cum să își gestioneze permisivitatea accesului la date și cum să sesizeze orice încălcare a drepturilor lor. Este important ca utilizatorii să înțeleagă că pot oricând să își retragă consimțământul, că au posibilitatea de a solicita ștergerea sau rectificarea datelor și că beneficiază de mecanisme de rezolvare a disputelor sau chiar de despăgubiri în

cazul unor încălcări grave. Când utilizatorii se simt împuterniciți, ei devin parteneri activi în menținerea unui mediu virtual echilibrat, raportând abuzurile și contribuind la rafinarea politicilor și instrumentelor de protecție a datelor, contribuție care poate fi inestimabilă pentru operatorii de platforme care nu au întotdeauna o viziune completă asupra tuturor interacțiunilor ce au loc în timp real.

Pentru a aduna și integra toate aceste bune practici într-un ansamblu coerent, este necesar un cadru de guvernare a datelor specific Metaversului, un concept care să conțină în mod explicit regulile, standardele, procedurile și instrumentele tehnice prin care informațiile sunt colectate, partajate și gestionate. Un asemenea cadru ar trebui să ia în considerare complexitatea deosebită a spațiilor virtuale, unde avatarurile, obiectele, mediile interactive și componentele hardware sunt distribuite în rețele ce pot traversa multiple jurisdicții și pot fi supuse unor legislații diferite.

În mod ideal, cadrul de guvernare ar stabili procese de acreditare sau de certificare pentru platformele care doresc să-și afirme aderența la standarde înalte de protecție a datelor, astfel încât utilizatorii să poată alege în cunoștință de cauză mediul virtual care le conferă siguranță și transparență.

De asemenea, un cadru matur de guvernare descrie metodologiile de audit și monitorizare continuă a practicilor de manipulare a datelor, garantând că politicile sunt puse în aplicare efectiv și sunt revizuite ori de câte ori tehnologia și contextul social evoluează. S-ar putea chiar prevedea obligația publicării unor rapoarte periodice privind conformitatea, astfel încât orice eventuală lacună să poată fi reparată rapid, iar comunitatea să aibă un nivel ridicat de încredere. În plus, cadrul ar trebui să fie deschis inovației, permițând testarea de noi soluții tehnice precum criptografia avansată, metode de anonimizare automată, mecanisme de control granular al accesului la date și moduri de a asigura portabilitatea datelor între platforme, fără a compromite securitatea sau confidențialitatea.

Printre cele mai bune practici pentru consolidarea guvernării datelor în Metavers se numără și implementarea unor politici clare privind proprietatea datelor. Astfel, fiecare tip de date generate, fie că este vorba despre conținut creat de utilizator, date personale ale acestuia, date operaționale despre sistem sau informații rezultate din analize avansate, ar trebui să fie asociat cu un set de drepturi și obligații. Dacă un creator de conținut dezvoltă un obiect 3D vândut ulterior sub formă de NFT, este necesar să se stabilească dacă datele privind utilizarea acelui obiect rămân la dispoziția creatorului, sunt exclusiv ale operatorului platformei sau pot fi partajate cu terți pentru scopuri de marketing sau analiză. Prin acest tip de clarificare, confuziile se reduc și pot fi prevenite situații în care un dezvoltator revendică datele generate de alți utilizatori asupra creațiilor sale, încălcând astfel drepturile de confidențialitate.

Totodată, stabilirea controalelor și permisiunilor de acces la date este vitală, pentru că într-un mediu în care interacțiunile se desfășoară la scară mare și în timp

real, gestionarea greșită a permisiunilor poate deschide uși pentru atacuri cibernetice sau pentru încălcări sistematice ale confidențialității. Printr-o segmentare atentă a datelor, un design bine structurat al bazelor de date și o gestionare stratificată a accesului (care să țină cont de rolurile și competențele fiecărei persoane sau entități), platformele pot asigura că doar cei cu nevoi legitime pot vedea ori modifica anumite informații. În plus, pentru a garanta transparența în activitățile de procesare a datelor, orice modificare majoră a politicilor, orice colectare suplimentară de date și orice parteneriat prin care datele sunt transmise unor terți trebuie comunicat în mod clar, în prealabil, astfel încât utilizatorii și partenerii să poată lua măsuri. Comunicarea acestei transparențe nu ar trebui să se rezume la documente juridice stufoase, ci să se facă prin interfețe ușor de înțeles, mesaje explicite și instrumente de tip panou de control, care să ofere vizibilitate și control concret asupra operațiunilor de prelucrare.

Pentru a menține integritatea și calitatea guvernantei, auditarea și actualizarea regulată a practicilor ar trebui să fie o rutină, mai ales că Metaversul se află într-o perpetuă schimbare și inovațiile tehnologice apar rapid. Un audit periodic poate scoate la iveală inconsistențe în respectarea politicilor, probleme tehnice de securitate, lacune de conformitate cu reglementările și nevoia de a ajusta procedurile pentru a ține pasul cu cerințele în continuă evoluție ale comunităților virtuale. Practicile de audit pot implica experți independenți, pot folosi instrumente automate de verificare a setărilor de securitate și pot încuraja chiar și o formă de „bug bounty”, prin care experții în securitate cibernetică să fie recompensați dacă descoperă vulnerabilități. Dincolo de problemele tehnice și legale, auditarea regulată are și un aspect cultural, punând presiune pe operatorii de platformă să își asume cu adevărat responsabilitatea gestionării datelor și să nu trateze aspectele de confidențialitate doar ca pe niște cerințe formale. Toate aceste inițiative și soluții trebuie să acționeze sinergic pentru a construi un Metavers în care datele sunt administrate cu grijă, iar inovația și creativitatea nu sunt frânate de temeri legate de securitate sau de posibile abuzuri.

Astfel, dezvoltarea unor politici clare de guvernare, combinată cu implementarea de măsuri avansate de securitate, se susțin reciproc cu un efort colectiv de colaborare între părțile interesate și cu educarea continuă a utilizatorilor, totul fiind încadrat într-un cadru cuprinzător de guvernare a datelor, care să fie revizuit periodic și adaptat pe măsura extinderii și transformării acestui univers virtual.

Rezultatul final al aplicării acestor practici ar trebui să fie un spațiu digital dinamic, dar și responsabil, în care companiile pot dezvolta noi modele de afaceri, artiștii și creatorii se pot exprima fără teamă de furt intelectual, instituțiile publice pot exploata potențialul realității virtuale pentru educație și servicii comunitare, iar utilizatorii pot explora aceste lumi 3D având convingerea că datele lor sunt respectate și că pot exercita un control real asupra vieții lor digitale.

În concluzie, capitolul a arătat că valoarea Metaversului pentru orașele inteligente nu constă doar în spectaculozitatea tehnologică, ci în capacitatea de a transforma date eterogene — din IoT, imagini satelitare, gemeni digitali și interacțiuni imersive — în decizii publice corecte și măsurabile. Această transformare este imposibilă fără un cadru matur de guvernare a datelor, care să asigure calitatea, integritatea și trasabilitatea informațiilor pe tot lanțul lor de viață. Fără guvernare, riscurile de fragmentare, biasul algoritmic, lock-in tehnologic și intruziune în viața privată subminează exact obiectivele de neutralitate climatică, echitate socială și eficiență operațională. Cu o guvernare a datelor solidă, Metaversul devine infrastructură critică de interes public: un spațiu în care scenariile urbane pot fi simulate, validate și auditate transparent, iar indicatorii de impact (energie, mobilitate, calitate a aerului, acces la alimentație) pot fi urmăriți în mod reproductibil.

Importanța guvernării datelor în Metavers se traduce în cerințe operaționale clare: „privacy/security by design”, minimizarea și limitarea scopului prelucrării datelor, standarde deschise pentru interoperabilitate și portabilitate, definiții explicite ale proprietății și accesului la date, precum și mecanisme de audit tehnic și etic (inclusiv audit algoritmic). La acestea se adaugă instituții și procese: registre de date urbane guvernate ca bun comun, consilii de etică pentru AI, acorduri de partajare cu responsabilități și SLA-uri între administrații, operatori de platforme și dezvoltatori, plus panouri de control pentru cetățeni care să facă efectivă exercitarea drepturilor (informare, consimțământ, portabilitate, ștergere). Doar în acest cadru, datele devin comparabile și reutilizabile, iar gemenii digitali din Metavers pot furniza dovezi solide care să ghideze investițiile publice și private, reducând risipa și accelerând reducerea emisiilor.

Pentru România și pentru municipii precum București, prioritatea este instituirea unui „contract digital” între stakeholderi — autorități, operatori de platforme, mediul academic, antreprenori și comunități — care să ancoreze proiectele Metavers în standarde comune și indicatori de monitorizare-raportare-verificare. Un portofoliu de proiecte-pilot (mobilitate, clădiri eficiente, agricultură urbană) ar trebui lansat cu guvernarea datelor inclusă încă din faza de proiectare, cu rezultate publice și replicabile. Investiția în capacitate instituțională (competențe de date, securitate cibernetică, audit), în standarde deschise și în instrumente de participare civică va determina dacă Metaversul rămâne o sumă de insule tehnologice sau devine stratul integrator care convertește date credibile în politici urbane legitime și eficiente. Pe scurt, fără guvernare a datelor, Metaversul riscă să amplifice problemele orașelor; cu o guvernare riguroasă, el poate deveni acceleratorul lor către sustenabilitate și reziliență.

Partea III.
Gubernanța datelor în Metavers



5. De ce este importantă guvernarea datelor?

În lumea modernă, datele au devenit unul dintre cele mai valoroase active ale unei organizații, asemănătoare cu resursele tradiționale precum capitalul sau forța de muncă. De fapt, termenul de „noul petrol” este adesea folosit pentru a sublinia rolul critic pe care datele îl joacă în economia digitală globală. În acest context, conceptul de guvernare a datelor reprezintă toate măsurile, procesele și politicile implementate pentru a asigura o gestionare eficientă și etică a datelor.

Guvernarea datelor a evoluat ca răspuns la nevoia de a administra datele de o manieră organizată și responsabilă, nu doar în ceea ce privește volumul și complexitatea, ci și pentru a asigura calitatea, securitatea și conformitatea acestora cu reglementările legale. Prin intermediul guvernării, organizațiile își definesc cine are acces la date, cum sunt datele colectate, stocate și utilizate, și cum sunt protejate împotriva pierderilor, breșelor de securitate sau utilizării abuzive.

Acest capitol explorează evoluția și importanța guvernării datelor, subliniind aspectele sale principale și modul în care a devenit un factor central în strategia organizațiilor moderne.

Rolul și importanța datelor în organizații

Ritmul alert de dezvoltare și integrare a noilor tehnologii digitale emergente determină transformări profunde atât în economie cât și în societate, influențând structura și dinamica acestora¹. Aceste tehnologii sunt fundamentate pe analiza și utilizarea avansată a datelor (Odunayo Josephine Akindote et al., 2023), contribuind astfel la optimizarea proceselor de afaceri existente și la crearea unor modele de afaceri complet noi. Prin urmare, datele constituie un activ valoros pentru organizații, sprijinind politicile acestora, fundamentând deciziile și practicile organizaționale și, în final, contribuind la crearea de valoare adăugată. (Murphy, 2022). Dar principalul avantaj al datelor constă în furnizarea de servicii ce pot fi reproduse sistemic fără costuri marginale adiționale. În plus, acestea permit o varietate largă de aplicații care pot fi implementate pe o gamă extinsă de dispozitive diferite, rezultând astfel un grad înalt de flexibilitate și scalabilitate (Veit et al., 2014).

În acest context, activități precum analiza și gestionarea eficientă a datelor capătă noi valențe în siajul dezvoltării unor tehnologii de prelucrare a volumelor mari de date precum Big Data. Obținerea unor informații relevante este strâns corelată cu disponibilitatea organizațiilor de a acorda prioritate integrării tehnologiilor

¹ Commission E. (2020), *A European strategy for data*, Brussels, Disponibil la: <https://digital-strategy.ec.europa.eu/en/policies/strategy-data> [Accesat: 22 Iul. 2024].

avansate de analiză predictivă și prescriptivă. Astfel de instrumente sunt utilizate la optimizarea operațiunilor și strategiilor de afaceri, cu scopul de a îmbunătăți performanța și competitivitatea (Berndtsson et al., 2018; Shahadat et al., 2023). Proportional cu creșterea volumului și diversității datelor, apare o serie întreagă de provocări legate de calitatea, securitatea și confidențialitatea acestora².

În prezent, analiza datelor nu mai este doar apanajul marilor companii³. Dincolo de cifre și statistici, datele permit extragerea de informații relevante pentru orientarea strategiilor, optimizarea proceselor și stimularea inovației. În acest context, luarea deciziilor bazate pe date a evoluat dintr-o tendință într-o necesitate⁴. Un studiu realizat în 2018 de Forbes arată că peste 52% dintre companii folosesc diverse forme de analiză a datelor, de la curățare și optimizare, până la aplicarea rezultatelor în strategii de piață (Forbes, 2018). Conform unui studiu similar realizat de Deloitte⁵, 49% dintre participanți asociază analiza datelor cu decizii mai bune, 16% cred că ajută la inițiativa strategice, iar 10% spun că îmbunătățește relațiile cu clienții și partenerii. Organizațiile care își bazează activitatea pe date au de 23 de ori mai multe șanse de a atrage noi clienți, de șase ori mai multe șanse de a menține clienții existenți și de 19 ori mai multe șanse de a înregistra profituri în creștere⁶. Aceste statistici subliniază tendința globală în care tot mai multe organizații, indiferent de domeniu, se bazează pe date pentru a-și îmbunătăți deciziile operaționale și strategice, prin procese bine structurate de colectare și analiză a informațiilor (Chidera Victoria Ibeh et al., 2024).

Datele sunt valoroase din cel puțin două motive, și anume caracterul lor omniprezent și potențialul de a fi colectate și analizate. În plus, datele sunt reutilizabile: odată generate, pot fi refolosite pentru diverse scopuri, cum ar fi analiza sau dezvoltarea de modele analitice⁷. Importanța datelor pentru organizații este evidențiată prin următoarele beneficii: o mai bună înțelegere a pieței; îmbunătățirea bazelor de date pentru consumatori; îmbunătățirea strategiilor de marketing;

² Forbes (2022), *The Age Of Analytics And The Importance Of Data Quality*, Disponibil la: <https://www.forbes.com/sites/forbesagencycouncil/2019/10/01/the-age-of-analytics-and-the-importance-of-data-quality/#7e16ab8d5c3c> [Accesat: 22 Iul. 2024].

³ Marr B. (2019), *How Can Small Businesses Use Big Data?*, Disponibil la: <https://bernardmarr.com/how-can-small-businesses-use-big-data-here-are-6-practical-examples/> [Accesat: 22 Iul. 2024].

⁴ Medium (2023), *The Importance of Data Strategy in Today's Business Landscape*, Disponibil la: <https://medium.com/@data.pilot/the-importance-of-data-strategy-in-todays-business-landscape-deb4140365bb> [Accesat: 22 Iul. 2024].

⁵ Deloitte (2018), *The Analytics Advantage*, Disponibil la: <https://www2.deloitte.com/ro/ro/pages/deloitte-analytics/articles/the-analytics-advantage.html> [Accesat: 24 Iul. 2024].

⁶ McKinsey Global Institute (2020), *Data Strategy Session*, Disponibil la: <https://www.datadeology.com/data/data-driven-organizations-are-23-times-more-likely-to-acquire-customers-six-times-as-likely-to-retain-customers-and-19-times-as-likely-to-be-profitable-as-a-result/> [Accesat: 24 Iul. 2024].

⁷ IIBA (2022), *The Critical Role of Data*, Disponibil la: <https://www.iiba.org/business-analysis-blogs/the-critical-role-of-data/> [Accesat: 22 Iul. 2024].

comunicare personalizată cu clienții; înțelegerea consumatorilor; sprijin în rezolvarea problemelor; îmbunătățirea proceselor interne⁸.

Într-un mod mai elaborat, organizația The Council on Quality and Leadership (CQL)⁹ enumeră un set de beneficii determinate de utilizarea datelor într-un context economic și social mai larg:

1. *Îmbunătățirea calității vieții*: un sistem eficient de analiză a datelor permite organizațiilor nu doar să monitorizeze cu acuratețe diferite aspecte relevante ale activității lor, dar și să adopte măsuri de corecție bazate pe informațiile astfel obținute. Această capacitate de intervenție proactivă, contribuie semnificativ la îmbunătățirea calității vieții persoanelor vizate prin optimizarea serviciilor și resurselor oferite.
2. *Suport în luarea deciziilor*: datele de calitate oferă informații clare și precise, esențiale pentru luarea deciziilor informate. În contrast, deciziile bazate pe dovezi ambigue sau presupuneri pot conduce la irosirea resurselor și la acțiuni eronate.
3. *Prevenirea transformării problemelor incipiente în crize*: datele permit monitorizarea continuă a sistemelor importante, ajutând organizațiile să identifice și să rezolve problemele înainte ca acestea să devină crize majore. Astfel, organizațiile pot fi proactive, nu reactive, și pot menține cele mai bune practici în timp.
4. *Obținerea rezultatelor preconizate*: datele permit măsurarea eficacității strategiilor implementate. Colectarea de date ajută la evaluarea performanței soluțiilor aplicate și la ajustarea abordărilor pe termen lung, dacă este necesar.
5. *Identificarea de soluții la probleme existente*: datele facilitează identificarea cauzelor problemelor. Analiza datelor ajută la vizualizarea relațiilor între evenimentele din diferite locații, departamente și sisteme. De exemplu, creșterea erorilor pe partea de productivitate poate indica probleme legate de fluctuația personalului, ajutând la formularea unor teorii mai precise și la implementarea soluțiilor mai eficiente.
6. *Fundamentarea argumentelor în schimbările sistemice*: datele permit construirea unui raționament solid pentru realizarea unor schimbări disruptive precum solicitarea de fonduri suplimentare sau modificarea reglementărilor,

⁸ Truyo (2024), *The Importance of Data: The Top Benefits of Collecting Customer Data*, Disponibil la: <https://truyo.com/blog/the-importance-of-data-the-top-benefits-of-collecting-customer-data/> [Accesat: 22 Iul. 2024].

⁹ CQL (2018), *12 Reasons Why Data Is Important*, Disponibil la: <https://www.c-q-l.org/resources/guides/12-reasons-why-data-is-important/> [Accesat: 24 Iul. 2024].

- oferind dovezi clare și analize detaliate care justifică necesitatea schimbărilor și sprijină inițiativele de reformă.
7. *Evitarea speculațiilor*: datele ajută la explicarea deciziilor, fie ele pozitive sau negative, către părțile interesate. Indiferent de rezultatul anticipat al strategiilor și deciziilor, datele oferă o bază solidă, în loc de presupuneri.
 8. *Abordare strategică*: utilizarea eficientă a datelor crește eficiența organizațională prin alocarea resurselor acolo unde sunt necesare. Analiza datelor contribuie la identificarea problemelor atât a celor generalizate cât și a celor izolate, permițând direcționarea precisă a resurselor în abordarea acestora.
 9. *Identificarea punctelor forte*: datele permit replicarea măsurilor de succes în cadrul organizației. Analiza datelor ajută la identificarea programelor, serviciilor și persoanelor cu performanțe ridicate, facilitând dezvoltarea strategiilor pentru îmbunătățirea celor mai slab performante.
 10. *Monitorizarea progresului*: datele de calitate permit stabilirea unor valori de referință, standarde și obiective de performanță ce pot fi comparate cu surse externe în vederea îmbunătățirii performanței.
 11. *Maximizarea eficienței financiare*: trecerea de la finanțarea bazată pe servicii la cea susținută de rezultate necesită folosirea practicilor bazate pe dovezi. În acest context, introducerea unor sisteme eficiente de colectare și analiză a datelor poate contribui la distribuirea optimă a resurselor.

Informațiile nu reprezintă o resursă importantă doar pentru mediul de afaceri, ci oferă beneficii și sectorului public. Capacitatea de a justifica deciziile pe baze empirice nu oferă doar un avantaj competitiv în afaceri, ci ajută la îmbunătățirea calității vieții într-un context extins. De exemplu, la nivelul societății, datele sunt folosite pentru a înțelege provocări majore, precum schimbările climatice, sărăcia și inegalitatea. Informațiile oferite de date pot ghida deciziile referitoare la politicile publice de impact. Un exemplu în acest sens este dat de examinarea datelor privind performanța elevilor în vederea identificării domeniilor în care aceștia au nevoie de mai mult sprijin și care pot conduce la adaptarea diverselor strategii educaționale sau alt tip de intervenție țintită.

O gestionare eficientă a datelor generează multiple beneficii, contribuind la îmbunătățirea procesului decizional, optimizarea operațiunilor și stimularea inovației. Printre avantajele unei administrări adecvate a datelor se numără creșterea transparenței și a responsabilității organizaționale, îmbunătățirea securității și protecției informațiilor sensibile, facilitarea interoperabilității între diferite sisteme și actori implicați, precum și sprijinirea proceselor de personalizare a serviciilor și produselor. De asemenea, o gestionare riguroasă a datelor permite alinierea mai eficientă la cerințele de conformitate și reglementare, oferind în același timp un

avantaj competitiv prin exploatarea inteligentă a informațiilor disponibile. Pentru a înțelege mai bine impactul unei astfel de administrări, putem analiza mai detaliat principalele beneficii:

Luarea deciziilor bazate pe date: guvernanța datelor asigură acuratețea, actualizarea și fiabilitatea informațiilor utilizate în organizație, contribuind astfel la luarea deciziilor informate și la optimizarea strategiilor manageriale.

Conformitate legală și protecția împotriva riscurilor: într-o eră în care confidențialitatea datelor este strict reglementată, guvernanța datelor ajută organizațiile să evite sancțiunile legale și reputaționale. Implementarea unor politici clare de protecție și gestionare a datelor ajută la respectarea legislației și la reducerea riscurilor asociate cu breșele de securitate.

Îmbunătățirea eficienței operaționale: o guvernanță bună a datelor reduce redundanța și ineficiența în colectarea și utilizarea datelor. Prin centralizarea și standardizarea proceselor, organizațiile pot obține o viziune mai coerentă asupra activelor lor de date, și pot reduce costurile asociate gestionării datelor. Protecția împotriva fraudelor și utilizării abuzive: prin implementarea unor măsuri stricte de securitate, guvernanța datelor contribuie la prevenirea riscurilor asociate fraudelor și utilizării neautorizate a informațiilor, asigurând un mediu de lucru mai sigur pentru organizații.

Încredere și transparență: organizațiile au obligația de a administra datele în mod responsabil. O guvernanță eficientă a datelor asigură transparență și claritate în privința proceselor de utilizare și protecție a informațiilor.

Provocări în gestionarea și utilizarea eficientă a datelor

În era digitală, gestionarea eficientă a datelor joacă un rol central în procesul decizional și în planificarea strategică. Creșterea exponențială a volumului și diversității surselor de date generează provocări legate de calitate, integrare, securitate și guvernanță, ceea ce impune adoptarea unor practici riguroase de management. Colectarea, stocarea și interpretarea corectă a datelor nu doar îmbunătățește eficiența operațională, ci și oferă un avantaj competitiv. Totuși, sincronizarea surselor și garantarea accesibilității necesită măsuri suplimentare pentru protejarea confidențialității și securității informațiilor. Pentru a valorifica datele în mod optim, organizațiile trebuie să se adapteze unui mediu dinamic, marcat de schimbări tehnologice, cerințe de reglementare și provocări etice. Gestionarea eficientă a acestor aspecte contribuie la transformarea datelor într-un activ strategic, aliniat obiectivelor organizaționale pe termen lung.

Gestionarea și utilizarea eficientă a datelor implică o serie de provocări complexe în diverse domenii, fiecare având particularitățile sale. Iată o analiză

detaliată a principalelor probleme cu care se confruntă organizațiile și profesioniștii în acest context:

Calitatea datelor (Data Quality)

Reprezintă unul dintre cei mai importanți factori în procesul de organizare eficientă a datelor în cadrul organizațiilor, ce include aspecte precum acuratețea, completitudinea și consecvența. Acuratețea datelor asigură o reprezentare fidelă a realității, completitudinea previne apariția lacunelor în seturile de date, iar consecvența garantează uniformitatea și compatibilitatea informațiilor între diferite sisteme. O calitate deficitară a datelor poate genera disfuncționalități operaționale, analize inexacte și decizii eronate, având un impact negativ asupra strategiilor organizaționale și experienței utilizatorilor. Pentru a minimiza aceste riscuri, este necesară implementarea unui cadru solid de guvernanță a datelor, bazat pe politici, standarde și proceduri clare. Validarea și întreținerea periodică a datelor, utilizarea instrumentelor automate ETL (Extract, Transform, Load) și integrarea surselor disparate, contribuie la reducerea erorilor și îmbunătățirea calității informațiilor. În plus, deficitul de specialiști în domeniu subliniază importanța investițiilor în formarea și retenția personalului calificat. O soluție eficientă o reprezintă colaborarea cu furnizori de tehnologie care oferă instruire avansată, asigurând menținerea unor standarde ridicate în gestionarea și protecția datelor.

Integrarea datelor (Data Integration)

Un proces complex de unificare a informațiilor din surse diverse, interne și externe, stocate în formate și sisteme variate, asigură coerența, consistența și accesibilitatea datelor într-o formă unificată, facilitând astfel analiza, raportarea și luarea deciziilor informate. Unul dintre obstacolele majore în implementarea acestui proces este reprezentat de fragmentarea datelor în depozite izolate, care limitează interoperabilitatea și îngreunează eforturile de consolidare și unificare a informațiilor. Prin urmare, o integrare eficientă impune o analiză detaliată a structurilor și semanticii fiecărei surse de date, alături de elaborarea unui cadru de mapare care să alinieze și să convertească informațiile într-un format unificat, asigurând astfel coerența și compatibilitatea între sistemele utilizate. Utilizarea instrumentelor ETL poate automatiza aceste procese, reducând implicarea umană și asigurând consistența între seturile de date. De asemenea, utilizarea API-urilor oferite de sursele de date poate facilita o recuperare directă și standardizată a informațiilor, simplificând astfel procesul de integrare. Această abordare minimizează riscul inexactităților în rapoarte și analize, crescând fiabilitatea generală a informațiilor derivate din datele integrate.

Securitatea și confidențialitatea datelor (Data security and privacy)

Securitatea datelor include protejarea informațiilor sensibile împotriva accesului neautorizat și a încălcării regulilor de securitate, asigurând totodată conformitatea

cu reglementări precum GDPR și HIPAA. În contextul actual, dominat de utilizarea extinsă a tehnologiilor bazate pe date, protejarea confidențialității și securității informațiilor a devenit o prioritate absolută atât pentru organizații, cât și pentru indivizi, aceștia fiind extrem de conștienți de riscurile asociate cu breșele de securitate, accesul neautorizat și utilizarea necorespunzătoare a datelor sensibile. Pentru a reduce aceste riscuri, sunt necesare măsuri de securitate avansate, cum ar fi aplicarea tehnicilor de criptare de ultimă generație pentru transmiterea și stocarea sigură a datelor, utilizarea autentificării multifactoriale pentru controlul accesului și efectuarea de actualizări periodice ale sistemelor de securitate pentru a remedia vulnerabilitățile existente. Un alt factor important îl reprezintă educarea angajaților cu privire la practicile corecte de manipulare a datelor și menținerea unei strategii clare pentru gestionarea incidentelor de securitate. Investițiile în software-uri avansate de gestionare a datelor și în instrumente de guvernanță a datelor pot contribui la securizarea acestora prin monitorizarea conformității și asigurarea integrității informațiilor.

Guvernanța datelor (Data governance)

Implică instituirea unor politici și standarde riguroase pentru practicile de gestionare a datelor, alături de clarificarea responsabilităților în ceea ce privește acuratețea, accesibilitatea și securitatea informațiilor. Acest cadru asigură conformitatea organizațiilor cu cerințele de reglementare și standardele industriei în ceea ce privește manipularea, stocarea și confidențialitatea datelor. Lipsa unei guvernări eficiente a datelor generează provocări majore, putând conduce la încălcări ale reglementărilor, cu consecințe precum amenzi și repercusiuni legale. De asemenea, fără o gestionare adecvată, organizațiile riscă să nu valorifice pe deplin potențialul activelor lor de date, pierzând astfel informații importante și oportunități de inovare, ceea ce poate limita creșterea și reduce avantajul competitiv. Pentru a consolida cadrul de guvernanță a datelor, organizațiile au obligația să desemneze roluri clare, să stabilească standarde stricte de date, să implementeze politici cuprinzătoare, să documenteze cu precizie sursele de date și să gestioneze cu rigurozitate calitatea acestora. În plus, este necesară asigurarea conformității și a securității, alături de furnizarea unei instruirii continue pentru angajați. Aceste măsuri permit menținerea integrității datelor, facilitarea unor decizii informate și gestionarea eficientă a resurselor informaționale. Instituirea unui cadru formal de guvernanță a datelor, cu roluri și responsabilități bine definite, și utilizarea sistemelor automate pentru monitorizarea și raportarea conformității, pot simplifica procesul de aliniere la reglementările în schimbare, asigurând astfel o conformitate constantă și o reziliență organizațională sporită.

Volumul și scalabilitatea datelor (Volume and Scalability)

Pe măsură ce volumele de date continuă să crească, multe organizații se confruntă cu dificultăți în scalarea sistemelor de gestionare a datelor. Prin urmare,

sunt necesare soluții pentru gestionarea optimă a volumelor mari de date și pentru asigurarea scalabilității sistemelor, astfel încât expansiunea datelor să nu compromită performanța. Problemele legate de scalabilitate apar adesea în contextul în care strategiile tradiționale de gestionare a datelor se confruntă cu limitări legate de infrastructură și cu dificultăți în adaptarea la noile tehnologii. Pentru a gestiona eficient volumul mare de date, organizațiile pot adopta soluții cloud scalabile, automatizare și inteligență artificială pentru optimizare, precum și o guvernanță flexibilă a datelor. Virtualizarea permite acces la date într-un mod unificat, fără relocare fizică, dar una dintre principalele provocări rămâne stocarea eficientă a informațiilor. Organizațiile mari pot deține propriile depozite de date dar managementul acestora rămâne o provocare majoră. De exemplu, extragerea unui raport la începutul lunii, în care datele sunt dispersate, poate duce la inexactități semnificative. Pentru a aborda eficient aceste probleme, utilizarea fluxurilor de date în timp real permite colectarea imediată a datelor, în loc de o actualizare zilnică. Această abordare automatizată și standardizată este adoptată de majoritatea sistemelor avansate de management al datelor.

Accesul la date (Data Access)

Reprezintă capacitatea de a asigura accesul la informații pentru persoanele autorizate, exact atunci și unde sunt necesare, facilitând utilizarea lor eficientă în cadrul organizației. Acest lucru implică două dimensiuni principale: utilizabilitatea și interoperabilitatea. Utilizabilitatea se axează pe asigurarea că datele sunt accesibile celor care au nevoie de ele, evitând aplicarea unor reguli uniforme care pot împiedica accesul eficient. Interoperabilitatea se referă la integrarea și funcționarea armonioasă a diferitelor sisteme și instrumente pentru a asigura un flux de lucru coerent. Provocările legate de accesibilitatea datelor sunt accentuate de preocupările legate de securitatea cibernetică, reglementările guvernamentale și cerințele de guvernanță a datelor, care pot restricționa accesul la date esențiale și pot reduce valoarea acestora. Un studiu realizat de BusinessWire¹⁰ a constatat că 60% dintre liderii de date din SUA și Europa nu au reușit să utilizeze mai mult de 40% din datele disponibile din cauza preocupărilor legate de confidențialitate. Același studiu a evidențiat că 67% dintre respondenți consideră că mandatele de guvernanță restricționează accesul la date utile, iar 61,2% susțin că protecția datelor reduce valoarea acestora. Problemele legate de procesele complexe și ad-hoc de accesare a datelor contribuie și ele la dificultăți semnificative în utilizarea datelor. Costurile de oportunitate asociate cu subutilizarea datelor pot fi considerabile, afectând competitivitatea și eficiența organizațiilor. Conform unui alt

¹⁰ BusinessWire (2022), *New Survey from Privitar and Bloor Research Reveals a Majority of Data Leaders Unable to Use More than 40% of Their Data Due to Security and Privacy Concerns*. Disponibil la: <https://www.businesswire.com/news/home/20221206006030/en/New-Survey-from-Privitar-and-Bloor-Research-Reveals-a-Majority-of-Data-Leaders-Unable-to-Use-More-than-40-of-Their-Data-Due-to-Security-and-Privacy-Concerns> [Accesat: 23 Iul. 2024].

studiu¹¹, în medie, 30% din timpul total al întreprinderilor este consumat de sarcini care nu adaugă valoare din cauza problemelor legate de calitatea și accesibilitatea datelor. De asemenea, cercetările NewVantage Partners au relevat că, în ciuda investițiilor de peste 50 milioane de dolari, doar o minoritate dintre companiile de top utilizează datele pentru a stimula inovația și a concura pe baza analizei acestora¹². Pentru a îmbunătăți accesibilitatea datelor, organizațiile trebuie să elimine obstacolele care limitează accesul la datele stocate și să susțină angajații în procesul de luare a deciziilor bazate pe date. Investiția în soluții bazate pe cloud și în strategii de integrare a datelor, împreună cu sprijinul oferit angajaților în interpretarea și utilizarea datelor, reprezintă soluții ce vin în sprijinul maximizării valorii și a impactului datelor disponibile.

Analiza datelor (Data Analytics)

Reprezintă un proces ce implică interpretarea precisă a informațiilor în vederea obținerii unor perspective acționabile, precum și utilizarea de unelte și competențe adecvate pentru a analiza și vizualiza datele în mod eficient. Când analiza depășește competențele individuale, dificultățile în înțelegerea convențiilor de denumire sau a structurilor complexe ale datelor pot reduce eficiența procesului de analiză. Astfel, dacă conversia datelor necesită un efort disproporționat, analiza devine inefficientă, diminuând valoarea potențială a informațiilor disponibile. Deși datele pot fi de înaltă calitate, ele pot avea o valoare limitată în starea lor brută. În acest caz, rolul principal revine tehnologiilor care facilitează procesul de analiză și extragere de informații din volume mari de date. Prin urmare, organizațiile trebuie să investească în platforme avansate care procesează datele brute în mod eficient și extrag perspective valoroase, sprijinind astfel dezvoltarea strategică și inovarea în cadrul organizației.

Considerații etice (Ethical Considerations)

Considerațiile etice în gestionarea și utilizarea datelor au impact atât asupra integrității datelor, cât și asupra încrederii părților interesate. O provocare majoră este reprezentată de menținerea confidențialității, ce impune obținerea consimțământului informat înainte de colectarea și utilizarea datelor. Măsuri de protecție, precum criptarea și anonimizarea, sunt utilizate pentru prevenirea accesului neautorizat și respectarea cerințelor legale. Alte măsuri importante vizează prevenirea furnizării unor date manipulatorii și asigurarea corectitudinii acestora pentru a garanta echitatea deciziilor. În plus, transparența în gestionarea datelor, definirea clară a responsabilităților, respectarea drepturilor de proprietate asupra datelor, prevenirea

¹¹ McKinsey (2020), *Designing data governance that delivers value*, Disponibil la: <https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/designing-data-governance-that-delivers-value> [Accesat: 23 Iul. 2024].

¹² BusinessWire (2021), *Big-Data-and-AI-Executive-Survey*, Disponibil la: <https://www.businesswire.com/news/home/20210104005022/en/NewVantage-Partners-Releases-2021-Big-Data-and-AI-Executive-Survey> [Accesat: 24 Iul. 2024].

utilizării necorespunzătoare și luarea în considerare a implicațiilor sociale și culturale contribuie la menținerea conformității etice. Abordând aceste aspecte în mod integrat, organizațiile pot promova o cultură de responsabilitate și utilizare etică a datelor.

Context tehnologic și organizațional

În anii 1960 și 1970, tehnologia informatică era încă într-un stadiu incipient de dezvoltare. Majoritatea organizațiilor foloseau sisteme informatice centralizate, cunoscute sub numele de mainframe, care erau extrem de costisitoare și complexe. Aceste sisteme erau utilizate în principal pentru gestionarea tranzacțiilor operaționale, precum și pentru procese financiare și contabile. De asemenea, la acea vreme, datele erau stocate pe suporturi fizice, cum ar fi banda magnetică și discurile mari, ceea ce limita capacitatea de stocare și prelucrare rapidă a informațiilor.

În această etapă inițială, accentul era pus pe eficiența operațională și pe accesul rapid la datele necesare pentru desfășurarea activităților de bază ale organizațiilor, cum ar fi procesarea comenzilor, stocurile și evidențele financiare. În general, datele erau privite ca un mijloc de susținere a funcțiilor administrative și operaționale, nu ca un activ strategic. Această mentalitate era reflectată și în modul în care erau organizate departamentele IT – specialiștii se concentrau în principal pe dezvoltarea și întreținerea sistemelor de calcul, mai degrabă decât pe gestionarea datelor în sine.

De asemenea, în această perioadă nu existau cadre formale de guvernanță a datelor. Organizațiile nu aveau politici structurate privind colectarea, stocarea sau protejarea datelor. În schimb, accentul era pus pe securitatea fizică a sistemelor informatice, deoarece multe dintre aceste sisteme erau accesibile doar prin terminale locale, cu acces limitat. Politicile de acces și de securitate a datelor erau rudimentare, iar rolurile precum cel de administrator de baze de date (DBA) erau încă în curs de definire.

În anii 1970, au început să apară primele sisteme de gestionare a bazelor de date (SGBD), cum ar fi IBM IMS (Information Management System), lansat în 1966, și mai târziu, bazele de date relaționale propuse de Edgar F. Codd în 1970. Aceste tehnologii au schimbat în profunzime modul în care organizațiile gestionau și accesau datele. Sistemele de baze de date relaționale permiteau stocarea și organizarea datelor într-un mod mult mai flexibil, bazat pe tabele și relații între acestea, spre deosebire de sistemele anterioare, care stocau datele într-o formă liniară, pe bandă magnetică. Această schimbare tehnologică a deschis noi oportunități pentru gestionarea datelor și a dat naștere la primele concepte de administrare formală a datelor. Odată cu introducerea bazelor de date relaționale și creșterea complexității informațiilor pe care organizațiile le stocau și gestionau, a apărut și necesitatea unor roluri specializate pentru a coordona și administra aceste date. Totuși, în această perioadă, guvernanța datelor în

sensul modern – adică gestionarea calității, securității, integrității și accesului la date – era încă un concept vag. Analiștii se ocupau mai ales de gestionarea tehnică a bazelor de date, precum backup-ul și restaurarea datelor, iar organizațiile se concentrau pe eficiența operațională și optimizarea performanțelor sistemelor de gestionare a datelor.

La sfârșitul anilor 1970 și începutul anilor 1980, odată cu creșterea volumului și diversității datelor gestionate de organizații, a devenit evident că era nevoie de mai mult control și standardizare în gestionarea acestor date. Aceasta a fost prima etapă în care organizațiile au început să gândească în termeni de guvernanță formală a datelor, deși la un nivel încă rudimentar. În această etapă timpurie, focusul principal a fost pe integritatea datelor și pe standardizarea proceselor de gestionare a datelor. Organizațiile au început să își dezvolte proceduri de control pentru a se asigura că datele sunt introduse în sistem în mod corect și consecvent. De asemenea, au apărut primele inițiative de a crea standarde de date în cadrul organizațiilor, astfel încât informațiile să fie gestionate într-un mod mai coerent și să fie ușor accesibile pentru diferite departamente. Tot în această perioadă a început să apară nevoia de calitate a datelor. Întrucât organizațiile au început să folosească datele nu doar pentru operațiuni curente, ci și pentru analize și decizii strategice, a devenit clar că datele de proastă calitate ar putea afecta serios performanțele și luarea deciziilor. Primele sisteme de raportare și analiză de afaceri au apărut în această perioadă, și au pus bazele dezvoltării ulterioare a instrumentelor moderne de business intelligence (BI).

Cu toate acestea, un aspect care lipsea în această etapă era securitatea și confidențialitatea datelor. Deși organizațiile au început să pună accent pe accesul controlat la sisteme și pe păstrarea integrității datelor, conceptul de protejare a datelor confidențiale și de respectare a confidențialității utilizatorilor se afla încă într-o fază incipientă. Reglementările ce urmează să fie adoptate în deceniile următoare (cum ar fi GDPR) au făcut parte dintr-o evoluție mai târzie a guvernanței datelor, pe măsură ce volumul de date personale a crescut și a devenit clar că acestea necesită protecție specială.

Principalele abordări în guvernanța datelor

Dezvoltarea guvernanței datelor a trecut prin două etape majore. Prima etapă s-a realizat în Statele Unite ale Americii în anii 1970¹³ și a stabilit principiile privind practicile echitabile în informații (Fair Information Practices Principles - FIPPs). Acestea reglementau transparența, calitatea datelor, notificarea, accesul, dreptul de corecție și protecția securității datelor. O versiune simplificată a acestor principii a fost introdusă de Comisia Federală pentru Comerț în 2000, pe măsură ce afacerile

¹³ Justice U. S. D. of (1970), *Records, Computers, and the Rights of Citizens*, Disponibil la: <https://www.justice.gov/opcl/docs/rec-com-rights.pdf> [Accesat: 24 Iul. 2024].

online s-au extins, necesitând notificarea și consimțământul utilizatorilor înainte de utilizarea serviciilor. Pe măsură ce volumul datelor a crescut, preocupările privind colectarea lor au dus la reglementări precum Actul privind confidențialitatea consumatorilor din California (CCPA) din 2018. Acesta garantează drepturi sporite, inclusiv accesul și ștergerea datelor personale, informarea despre utilizarea lor, și opțiunea de a renunța la vânzarea datelor¹⁴.

A doua etapă a avut loc în Europa, unde Directiva UE privind protecția datelor din 1995 și ulterior GDPR în 2018 au stabilit șapte principii de bază: corectitudine, limitarea scopului, minimizarea datelor, acuratețea, limitarea stocării, integritatea și confidențialitatea, și responsabilitatea¹⁵. GDPR, devenită standard global, necesită consimțământul pentru prelucrarea datelor personale, dar aplicarea practică a acestor reguli, inclusiv utilizarea standardelor deschise și cerințele detaliate de consimțământ, rămâne o provocare, mai ales pentru companiile de tehnologie¹⁶.

Definiția și rolul guvernanței datelor

Guvernanța datelor nu se limitează doar la controlul și protecția acestora; include și activarea și valorificarea informațiilor obținute de la un număr mare de persoane, adesea prin intermediul Internetului (crowdsourcing). Într-un mediu de afaceri dinamic și competitiv, guvernanța eficientă a datelor nu doar că asigură conformitatea cu reglementările și protejează informațiile sensibile, dar permite și identificarea oportunităților strategice, optimizarea operațiunilor și luarea deciziilor bazate pe analize precise. Pe măsură ce organizațiile au acum posibilitatea de a colecta volume mari de date interne și externe, este necesar să adopte o abordare disciplinată pentru a maximiza valoarea acestor date, a gestiona riscurile asociate și a reduce costurile de administrare.

Guvernanța datelor cuprinde un ansamblu de procese, roluri, politici, standarde și valori menite să asigure utilizarea optimă a informațiilor, facilitând astfel îndeplinirea obiectivelor organizației. Aceasta stabilește cadrul de procese și responsabilități necesar pentru garantarea calității și securității datelor utilizate în cadrul afacerii. Guvernanța datelor definește cine are autoritatea să ia decizii privind datele, în ce condiții și prin ce metode, asigurând astfel o gestionare clară și eficientă a acestora.

Pentru a înțelege nu doar definițiile, ci și semnificația guvernanței datelor, este necesar să analizăm structura și elementele fundamentale care compun arhitectura sa.

¹⁴ State of California (2024), *California Consumer Privacy Act (CCPA)*, [Accesat: 3 Aug. 2024].

¹⁵ Union E. (2018), *General Data Protection Regulation (GDPR)*, Disponibil la: <https://www.consilium.europa.eu/en/policies/data-protection/data-protection-regulation/> [Accesat: 30 Oct. 2024].

¹⁶ International Settlements B. for (2022), *The design of a data governance system*, Disponibil la: <https://www.bis.org/publ/bppdf/bispap124.htm> [Accesat: 4 Aug. 2024].

1. *Roluri și responsabilități*: stabilirea clară a rolurilor și responsabilităților persoanelor care gestionează și utilizează datele, asigurând o distribuție adecvată a sarcinilor.
2. *Tehnologii și instrumente*: cumulum de tehnologii, instrumente și sisteme necesare pentru a susține capacitățile în diverse domenii, cum ar fi managementul, asigurarea calității, securitatea, integrarea, descoperirea, accesibilitatea și disponibilitatea datelor.
3. *Procese și controale*: dezvoltarea și aplicarea de procese și controale riguroase pentru a menține consistența, integritatea, utilizabilitatea și confidențialitatea datelor. Aceste măsuri asigură că datele rămân fiabile și utile pe tot parcursul ciclului lor de viață.
4. *Politici, proceduri și standarde*: crearea și implementarea de politici, proceduri și standarde care să sprijine conformitatea cu reglementările legale și etice, oferind în același timp claritate asupra responsabilităților tuturor părților implicate în gestionarea datelor.
5. *Calitatea datelor*: asigurarea unei calități înalte a datelor, inclusiv gestionarea metadatelor și securitatea informațiilor, pentru a garanta fiabilitatea și acuratețea datelor utilizate în procesele de afaceri și deciziile strategice.

Există numeroase definiții ale guvernanței datelor, însă toate converg asupra unui principiu fundamental: aceasta se concentrează pe organizarea oamenilor, proceselor și tehnologiei pentru a facilita gestionarea eficientă a datelor. O definiție frecvent întâlnită descrie guvernanța datelor ca fiind procesul de exercitare și aplicare a autorității asupra gestionării datelor și a activelor asociate acestora. Guvernanța datelor trebuie să fie în conformitate cu politicile de guvernanță corporativă și integrată în cadrul general de guvernanță IT al organizației (Abraham et al., 2019).

În funcție de obiectivele specifice, definițiile guvernanței datelor se axează pe valori specifice pentru fiecare grup în parte. De exemplu, MDM Institute¹⁷ definește guvernanța datelor, punând accent pe aspectele fundamentale ale oamenilor, proceselor și tehnologiei, ca fiind „organizarea formală a resurselor umane, proceselor și tehnologiilor pentru a permite unei organizații să valorifice datele ca un activ strategic al întreprinderii”.

Pentru Forrester, guvernanța datelor pune accent pe responsabilitatea fiduciară și planificarea organizațională, aceasta ca fiind: „un program strategic de afaceri care identifică și prioritizează beneficiile financiare aduse de date organizațiilor, în timp ce reduce riscurile asociate cu practici de gestionare și calitate a datelor deficiente.

¹⁷ MDM Institute (2015), *What is Data Governance?*. Disponibil la: <http://www.tcdii.com/whatIsDataGovernance.html> [Accesat: 5 Aug. 2024].

Acest program se axează pe proprietate, responsabilitate, procese, planificare și managementul performanței în contextul datelor¹⁸.

Cu accent pe responsabilitățile managerilor de nivel mediu și pe regulile de angajament, Data Governance Institute definește guvernanța datelor ca: „un sistem de drepturi decizionale și responsabilități pentru procesele legate de informații, executat conform unor modele agreeate care descriu cine poate întreprinde ce acțiuni, cu ce informații, când, în ce circumstanțe și prin ce metode”¹⁹.

NASCIO definește guvernanța datelor ca fiind: „disciplina de operare pentru gestionarea datelor și a informațiilor ca un activ cheie al întreprinderii. Această disciplină operațională include organizarea, procesele și instrumentele de stabilire și exercitare a drepturilor de decizie privind evaluarea și gestionarea datelor. Aspectele cheie ale guvernanței datelor includ autoritatea de luare a deciziilor, monitorizarea conformității, politici și standarde, inventare de date, managementul ciclului de viață complet, managementul conținutului, managementul înregistrărilor, conservarea, calitatea datelor, clasificarea datelor, securitatea și accesul la date, gestionarea riscului de date și evaluarea datelor”²⁰.

Alte abordări privind guvernanța datelor sunt prezentate în continuare:

- Guvernanța datelor (DG) se referă la gestionarea generală a disponibilității, utilizabilității, integrității și securității datelor folosite într-o întreprindere²¹.
- Guvernanța datelor este practica de organizare și implementare a politicilor, procedurilor și standardelor pentru utilizarea eficientă a activelor informaționale structurate/nestructurate ale unei organizații²².
- Guvernanța datelor este procesul de luare a deciziilor care prioritizează investițiile, alocă resurse și măsoară rezultatele pentru a se asigura că datele sunt gestionate și implementate pentru a sprijini nevoile afacerii²³.

¹⁸ Goetz M. (2015), *Data Governance and Data Management Are Not Interchangeable*, Disponibil la: https://www.forrester.com/blogs/15-09-11-data_governance_and_data_management_are_not_interchangeable/ [Accesat: 5 Aug. 2024].

¹⁹ Data Governance Institute (2020), *Defining Data Governance*, Disponibil la: <https://data.governance.com/defining-data-governance/> [Accesat: 9 Aug. 2025].

²⁰ Nascio (2008), *Data Governance – Managing Information As an Enterprise Asset Part 1*, Disponibil la: <https://www.nascio.org/Portals/0/Publications/Documents/NASCIO-DataGovernance-Part1.pdf>. [Accesat: 5 Aug. 2024].

²¹ Stedman C. (2024), *What is data governance and why does it matter?*, Disponibil la: <https://www.techtarget.com/searchdatamanagement/definition/data-governance> [Accesat: 7 Aug. 2024].

²² EIM Institute (2024), *Data Governance Maturity – An Overview*, Disponibil la: <https://www.eiminstitute.org/resource-portals/data-governance-stewardship/data-governance-maturity-an-overview/> [Accesat: 7 Aug. 2024].

²³ DBHIDS (2018), *Data governance framework strategic plan*, Disponibil la: <https://dbhids.org/wp-content/uploads/2019/02/DBHIDS-DG-Framework-Strategic-Plan-v2.03.pdf> [Accesat: 10 Aug. 2024].

Rolul și responsabilitățile în guvernanța datelor

Organizațiile publice sau private care colectează și agregă date de la utilizatori au multiple responsabilități, printre care se numără asigurarea calității și integrității datelor, respectarea reglementărilor privind confidențialitatea și securitatea informațiilor, precum și furnizarea de analize precise și relevante pentru luarea deciziilor informate. Cu toate acestea, acest tip de organizații nu dețin în proprietate datele colectate. Legislații precum Regulamentul general privind protecția datelor (GDPR) al Uniunii Europene (UE) încearcă să răspundă provocărilor și ambiguității din acest domeniu prin clarificarea dreptului de proprietate asupra datelor.

Conform GDPR, persoana pe care datele o reprezintă este și proprietara acestora. Organizația care colectează datele trebuie să acționeze ca administrator al acestor date dar, în realitate, nu exercită nicio proprietate asupra informațiilor personale²⁴.

Universitatea din Queensland²⁵ propune următorul model de roluri și responsabilități, descris în tabelul 5.1:

Tabel 5.1. Roluri și responsabilități conform modelului furnizat de Universitatea din Queensland

Roluri	Responsabilități
Administrator (custode) informații	Are autoritate la nivel de organizație și răspundere conform legislației pentru colectarea și gestionarea informațiilor
Coordonator (lider) informații	Oferă îndrumări strategice cu privire la cerințele de informații în cadrul unui sau mai multor domenii de informații
Administrator al domeniului de informații	Definește și implementează măsuri de prevenire pentru a asigura protecția informațiilor în domeniul specific de informații
Steward informații	Responsabil pentru calitatea, integritatea și utilizarea activelor informaționale
Creator de informații	Preia sau crează informațiile așa cum sunt definite de Administratorul Domeniului de Informații
Consumator de informații	selectează cele mai bune surse de informații pentru a satisface cerințele lor de utilizare

Rolurile și responsabilitățile descrise mai sus sunt denumite „drepturi de decizie”. Drepturile de decizie în cadrul UQ sunt un factor cheie pentru guvernanța datelor ce oferă sprijin în luarea eficientă a deciziilor cu privire la gestionarea datelor și informațiilor pe parcursul ciclului lor de viață.

²⁴ Queensland U. of (2024), *Data Governance Essentials Handbook*, Disponibil la: <https://data.uq.edu.au/files/6833/Data%20Governance%20Essentials%20handbook%20August%20%2021.pdf> [Accesat: 10 Aug. 2024].

²⁵ Ibid.

Ca și în cazul precedent, în contextul afacerilor, guvernanța datelor implică colaborarea mai multor persoane cu roluri distincte. Acest proces include directori de afaceri, specialiști în managementul datelor, personal IT și utilizatori finali care au cunoștințe despre domeniile de date specifice din sistemele organizației. Principalii actori care contribuie la gestionarea eficientă a datelor și au atribuții clar definite în cadrul acestui proces sunt evidențiați în tabelul 5.2.

Tabel 5.2. Roluri și responsabilități în domeniul afacerilor (adaptat după Stedman, 2024)

Roluri	Responsabilități
Director de date (Chief Data Officer – CDO)	Este responsabil pentru utilizarea eficientă a datelor ca activ strategic, respectând reglementările și bunele practici. Principalele responsabilități includ: elaborarea și implementarea strategiei de date aliniate obiectivelor organizației, aplicarea politicilor privind calitatea, confidențialitatea și securitatea datelor, asigurarea acurateței și fiabilității acestora, respectarea reglementărilor (ex. GDPR, CCPA), supravegherea arhitecturii și integrării datelor, definirea rolurilor și responsabilităților, facilitarea colaborării între echipe, susținerea analizelor de date și promovarea unei culturi organizaționale bazate pe date.
Manager pentru guvernanța datelor	Este responsabil pentru implementarea politicilor și practicilor de guvernanță a datelor, asigurând procese eficiente, sigure și conforme cu reglementările. Atribuțiile includ: dezvoltarea și aplicarea politicilor privind calitatea, securitatea și utilizarea datelor, stabilirea standardelor pentru menținerea integrității datelor, garantarea conformității, gestionarea rolurilor de administrare a datelor, supravegherea arhitecturii și integrării acestora, instruirea angajaților, monitorizarea eficacității practicilor, facilitarea colaborării interdepartamentale și îmbunătățirea continuă a strategiilor de guvernanță.
Comitetul/consiliul de guvernanță a datelor	De obicei, echipa de guvernanță nu ia decizii privind politicile sau standardele. Aceasta este responsabilitatea comitetului sau a consiliului de guvernanță a datelor, care este alcătuit în principal din directori de afaceri și alți proprietari de date. Comitetul aprobă politica fundamentală de guvernanță a datelor, împreună cu politicile și regulile asociate cu accesul și utilizarea datelor, plus procedurile de implementare a acestora. De asemenea, rezolvă disputele, cum ar fi dezacordurile dintre diferite entități cu privire la definițiile și formatele datelor.
Stewardul de date	Responsabilitățile acestui rol includ supravegherea seturilor de date pentru a le menține în ordine, asigurarea că politicile și regulile aprobate de comitetul de guvernanță a datelor sunt implementate și că utilizatorii finali le respectă.
Arhitecții de date, modelatorii de date, analiștii și inginerii de calitate a datelor	Contribuie la gestionarea eficientă a datelor și la asigurarea utilizării corecte a acestora. Rolul acestora în cadrul organizației poate varia de la proiectarea și dezvoltarea infrastructurii de date a organizației; crearea și întreținerea modelelor de date detaliate; furnizarea de rapoarte și analize până la identificarea și rezolvarea problemelor legate de calitatea datelor, crearea de politici și proceduri pentru gestionarea calității și colaborarea cu alte echipe pentru a asigura integritatea și fiabilitatea datelor în întreaga organizație.

Introducere în conceptul de Data Governance Framework (DGF)

Plecând de la definițiile prezentate anterior, putem spune despre conceptul de guvernanță a datelor că acesta se referă la modul în care este asigurată gestionarea, securitatea și utilizarea corespunzătoare a datelor în cadrul unei organizații, sau la modul în care o organizație își folosește oamenii, procesele și tehnologia pentru a-și gestiona datele interne. Prin guvernanța datelor se urmărește maximizarea activului de date (Carretero et al., 2017) dar și gestionarea riscului asociat managementului acestora (Data Administration Management Association, 2010). Principala componentă ce oferă consistență oricărui program eficient de guvernanță a datelor este reprezentată de cadrul de guvernanță a datelor sau Data Governance Framework (DGF).

Un cadru de guvernanță a datelor (DGF) sau de gestionare a datelor reprezintă o abordare metodică ce subliniază modul în care datele sunt gestionate, securizate și utilizate într-o organizație. Acesta stabilește politicile, standardele, rolurile și responsabilitățile necesare pentru a garanta calitatea, securitatea, conformitatea și uniformitatea datelor în întreaga organizație. Pentru o mai bună înțelegere vom utiliza o definiție larg răspândită în literatura de specialitate care este oferită de Data Governance Institute²⁶ și anume ”cadrul de guvernanță a datelor este o structură logică utilizată pentru clasificarea, organizarea și comunicarea activităților complexe implicate în deciziile cu privire la datele organizației”. Cadrul acționează ca un ghid pentru implementarea inițiativelor de guvernanță a datelor, oferind o structură cuprinzătoare care leagă tehnicile de gestionare a datelor cu obiectivele de afaceri și cerințele de reglementare ale organizației.

În continuare, vom realiza o analiză detaliată a principalelor beneficii și provocări asociate implementării unui cadru de guvernanță a datelor. Această trecere în revistă va sublinia atât avantajele pe care un astfel de cadru le aduce în contextul managementului eficient al datelor, cât și dificultățile majore pe care organizațiile le pot întâmpina în procesul de implementare.

Un cadru solid de guvernanță a datelor permite unei organizații să își gestioneze datele ca un activ strategic.

Implementarea unui cadru de guvernanță a datelor (DGF) într-o organizație generează o serie de beneficii, cele mai importante vizând o mai bună aliniere cu obiectivele de afaceri, îmbunătățirea conformității cu reglementările legale, menținerea unor definiții uniforme ale datelor, rezolvarea provocărilor legate de analiză și raportarea datelor și reducerea cheltuielilor. De asemenea, un DGF bine implementat permite identificarea și atenuarea riscurilor asociate cu securitatea, integritatea și confidențialitatea datelor, oferind totodată procese standardizate pentru gestionarea datelor, eliminarea redundanțelor și utilizarea eficientă a resurselor de date în cadrul organizației. Beneficiile implementării unui cadru de guvernanță a datelor sunt detaliate în tabelul 5.3.

²⁶ Data Governance Institute (2024), *DGI Data Governance Framework*, Disponibil la: <https://datagovernance.com/the-dgi-data-governance-framework/> [Accesat: 14 Aug. 2024].

Tabel 5.3. Beneficiile implementării unui cadru de guvernanță a datelor

Beneficii	Descriere	Perspectivă
Îmbunătățește conformitatea cu reglementările	Un DGF ajută organizațiile să-și alinieze practicile de gestionare a datelor cu cerințele de reglementare prin definirea modului în care datele ar trebui să fie colectate, stocate, procesate și partajate, asigurând responsabilitatea și transparența	Cercetările indică faptul că breșele de securitate în ceea ce privește managementul datelor și nerespectarea reglementărilor privind confidențialitatea datelor pot provoca daune grave reputației unei organizații și pot conduce la amenzi în valoare de milioane de dolari (Cavoukian, 2012).
Îmbunătățirea calității datelor	DGF se asigură că datele sunt exacte, consecvente și fiabile în întreaga organizație. Prin stabilirea de politici și proceduri standardizate pentru introducerea, procesarea și stocarea datelor, problemele de calitate a datelor, cum ar fi dublările, inconsecvențele și erorile sunt minimizate. Acest lucru îmbunătățește calitatea și acuratețea analizei și raportării datelor. Datele inexacte pot conduce la decizii greșite, ineficiență în afaceri și pierderi financiare.	Studiile arată că o calitate slabă a datelor poate costa organizațiile până la 15-25% din veniturile lor, subliniind importanța guvernării datelor în asigurarea datelor de înaltă calitate (Redman, 2016).
Îmbunătățirea securității datelor	Prin implementarea unor controale stricte de acces, politici de criptare și mecanisme de protecție a datelor, organizațiile pot reduce riscurile unor breșe de securitate, scurgeri și acces neautorizat la date. Măsurile de securitate integrate în cadrul de guvernanță asigură că informațiile sensibile și de identificare personală sunt protejate, astfel fiind reduce riscurile unor amenințări cibernetice.	Conform unui raport furnizat de IBM ²⁷ , costul mediu al unei breșe de securitate în ceea ce privește managementul datelor este de 4,24 milioane USD, subliniind importanța critică a guvernanței datelor în prevenirea și atenuarea încălcării reglementărilor în vigoare.
Luarea deciziilor bazate pe Informații	Un cadru de guvernanță a datelor asigură acces la date de înaltă calitate, exacte și în timp util, permițând o mai bună luare a deciziilor. Organizațiile pot folosi informațiile pentru a identifica tendințele pieței, comportamentele clienților și eficiența operațională. Această utilizare strategică a datelor sprijină deciziile de afaceri, oportune stimulând creșterea și inovația.	Conform unui raport McKinsey, organizațiile care iau decizii bazate pe date au șanse de 23 de ori mai mari să își crească baza de clienți, șanse mai mari de a-i păstra, și de 19 ori mai multe șanse de a fi profitabile decât cele care nu se bazează pe decizii bazate pe date ²⁸ .

²⁷ IBM (2022), Data breach costs reach a record high, Disponibil la: <https://www.ibm.com/r eports/data-breach-action-guide>.

²⁸ Henke N. et al. (2016), The age of analytics: Competing in a data-driven world, Disponibil la: <https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-age-of-analytics-competing-in-a-data-driven-world>.

Îmbunătățirea eficienței operaționale	Un DGF ajută la eficientizarea proceselor de gestionare a datelor prin reducerea redundanței și îmbunătățirea accesibilității datelor. Procedurile și rolurile standardizate reduc confuzia, dublarea eforturilor și erorile, ceea ce duce la o eficiență operațională sporită. Mai mult, guvernanța datelor îmbunătățește colaborarea între departamente, oferind o înțelegere clară a proprietății și responsabilităților datelor.	Cercetările ne arată că organizațiile care investesc în cadre de guvernanță a datelor raportează o creștere cu 15% a eficienței operaționale datorită reducerii depozitelor de date izolate și a îmbunătățirii accesibilității datelor (Davenport et al., 2007)
Creșterea gradului de accesibilitate și utilizabilitate al datelor	Implementarea unui cadru de guvernanță a datelor permite democratizarea accesului la date, acestea fiind accesibile întregului personal autorizat, indiferent de expertiza tehnică a acestuia. Elimină depozitele de date izolate și promovează o cultură a partajării datelor în cadrul organizației. Acest acces dă putere angajaților din toate departamentele să utilizeze informații bazate pe date în munca lor, stimulând inovația, creativitatea și colaborarea.	S-a demonstrat că democratizarea accesului la date sporește agilitatea și receptivitatea organizațională, permițând personalului non-tehnic să extragă informații utile și să contribuie la inovarea bazată pe date (Bughin et al., 2018).
Reducerea costurilor	De ce este importantă guvernanța datelor? Reducerea costurilor Îmbunătățind calitatea datelor, reducând redundanțele și asigurând procese mai eficiente de gestionare a datelor, organizațiile pot evita costurile asociate cu calitatea slabă a datelor, cum ar fi risipa de resurse, ineficiența operațională și luarea incorectă a deciziilor. În plus, guvernanța eficientă a datelor poate reduce riscul amenzilor și sancțiunilor legale asociate cu încălcările reglementărilor. Optimizarea utilizării datelor reduce, de asemenea, nevoia de stocare și procesare în exces a acestora, ceea ce duce la economii de costuri în infrastructura IT.	Organizațiile care implementează DGF pot reduce costurile operaționale cu 20-30% prin practici îmbunătățite de gestionare a datelor, redundanță redusă și procese simplificate (Ladley, 2020). În plus, evitarea costurilor legate de încălcarea reglementărilor în vigoare privind datele (în medie 4,24 milioane USD per incident), subliniază și mai mult beneficiile financiare ale guvernării solide a datelor ²⁹

Un cadru de guvernanță a datelor urmărește stabilirea unei abordări structurate pentru gestionarea activelor de date și asigurarea integrității, securității și accesibilității acestora. Totuși, procesul de implementare a unui astfel de cadru se confruntă cu o serie de provocări, care pot influența în mod substanțial succesul acestuia. De cele mai multe ori aceste provocări apar din interacțiunea dintre cultura organizațională, infrastructura tehnologică, conformitatea cu reglementările și alinierea părților interesate. Înțelegerea acestor provocări diminuează riscurile

²⁹ IBM (2022), *Data breach costs reach a record high*, Disponibil la: <https://www.ibm.com/r eports/data-breach-action-guide>.

asociate cu gestionarea improprie a datelor și crește potențialul de valorificare a acestora în cadrul organizațiilor. În tabelul 5.4 sunt prezentate principalele provocări ce apar în implementarea unui DGF.

Tabel 5.4. Provocările implementării unui cadru de guvernanță a datelor

Provocări	Descriere	Perspective
Confuzie privind proprietatea datelor	Rolurile și responsabilitățile pentru date nu sunt stabilite în mod eficient, proprietatea asupra datelor nu este clar stabilită în cadrul organizației, ceea ce conduce la conflicte și ambiguitate în asumarea responsabilității asupra seturilor de date, pentru calitatea, securitatea și conformitatea acestora. Acest lucru poate îngreuna gestionarea și utilizarea datelor în mod responsabil.	Organizațiile cu structuri ambigue de proprietate asupra datelor sunt mai susceptibile de a întâmpina probleme legate de inconsecvența datelor, redundanță și responsabilitate (Wende, 2017).
Definirea inconsecventă a datelor	Definițiile inconsecvente ale datelor apar atunci când diferite părți ale unei organizații folosesc termeni, valori sau standarde diferite pentru a descrie aceleași elemente de date, ceea ce poate conduce la neînțelegeri, comunicare greșită și erori în interpretare, analiză și raportare. Aceste inconsistențe în definirea datelor pot introduce redundanțe și pot crea dificultăți în cazul integrării în sisteme neomogene.	Rezolvarea acestor inconsecvențe reprezintă adesea unul dintre aspectele mari consumatoare de timp, necesitând un efort semnificativ de standardizare și armonizare a definițiilor datelor în cadrul organizației (Wende, 2017). O abordare inconsecventă în definirea datelor poate conduce la o creștere de peste 50% a timpului dedicat activităților de reconciliere a datelor în cadrul unei organizații, cu consecințe negative asupra eficienței (Otto, 2015).
Calitatea slabă a datelor	Problemele legate de calitatea datelor au cauze multiple, de cele mai multe ori acestea provenind din utilizarea unor sisteme vechi, din erori la introducerea datelor, lipsa standardizării și utilizarea unor metode disparate de management. Calitatea slabă a datelor se poate manifesta prin informații incomplete învechite, inexacte sau duplicate, diminuând eficacitatea inițiativelor de guvernanță a datelor. În plus, problemele legate de calitatea datelor sunt adesea abordate într-un mod reactiv și manual, fără a aborda în mod adecvat cauzele fundamentale, care pot duce la reapariția acestor probleme.	În multe organizații, peste 80% din timpul dedicat analizei datelor este consumat de activitățile de curățare și pregătire a acestora. În plus, calitatea slabă a datelor costă organizațiile în jur de 12,9 milioane USD anual, din cauza ineficienței, oportunităților ratate și reluării proceselor ³⁰ .

³⁰ Gartner (2021), *12 Actions to Improve Your Data Quality*, Disponibil la: <https://www.gartner.com/smarterwithgartner/how-to-improve-your-data-quality> [Accesat: 24 Apr. 2025].

Absența liniei de urmărire a datelor	Lipsa provenienței datelor poate duce la dificultăți în monitorizarea corectă a originii și fluxului datelor și auditarea utilizării acestora, afectând astfel capacitatea organizației de a asigura conformitatea cu reglementările și de a menține integritatea datelor	Organizațiile care nu dispun de un sistem eficient de proveniență a datelor se confruntă cu un risc crescut de erori și inexactități, afectând performanța operațională și conformitatea legală (Ponnusamy et al., 2023; Peuralinna, 2024)
Menținerea echilibrului între accesul la date și normele de securitate	Una din principalele obiective ale unui cadru de guvernanță a datelor se referă la menținerea unui echilibru între accesibilitate și democratizarea accesului la date și protejarea informațiilor sensibile. Politicile stricte pot împiedica accesul și în consecință inovarea bazată pe date, în timp ce politicile permissive pot lăsa organizația vulnerabilă la riscurile de securitate.	Organizațiile care nu reușesc să creeze un echilibru între accesul la date și securitate se confruntă adesea fie cu blocaje în utilizarea datelor, fie cu o vulnerabilitate crescută la atacurile cibernetice (Brouwers, 2016; Sharma, 2024; Tehrani, 2024)
Rezistența la schimbare	Introducerea noilor politici de guvernanță a datelor poate întâmpina opoziția angajaților, principala temere fiind legată de limitarea autonomiei sau încetinirea proceselor cauzate de o supraveghere sporită. Depășirea acestei inerții culturale necesită aplicarea unor strategii eficiente de management al schimbării și comunicare.	Un studiu publicat în recent indică faptul că aproximativ 70% dintre inițiativele de guvernanță a datelor eșuează din cauza rezistenței culturale, întrucât angajații întâmpină dificultăți în adaptarea la noile roluri, responsabilități și procese (Weber et al., 2009).
Dinamica mediului de reglementare	Mediul de reglementare referitor la confidențialitatea și protecția datelor este în continuă schimbare, ceea ce constituie o provocare semnificativă pentru organizații în menținerea conformității. Legislațiile recente, precum GDPR sau reglementările specifice anumitor industrii, impun adesea organizațiilor să-și actualizeze sau să-și ajusteze periodic practicile de guvernanță a datelor. Adaptarea constantă la aceste modificări poate consuma resurse considerabile și poate complica structura de guvernanță.	În urma unor cercetări recente rezultă faptul că organizațiile au petrecut în medie 12-18 luni pregătindu-se pentru conformitatea cu reglementările în vigoare privind datele, ceea ce subliniază timpul și efortul semnificativ necesar adaptării la noile cadre de reglementare (Spalević et al., 2022).

Guvernanța datelor în Metavers: de la principii clasice la spații virtuale interconectate

În capitolele anterioare am văzut cum Metaversul combină fluxuri de date 3D persistente, interacțiuni sincrone multi-utilizator, economii digitale (NFT-uri, monede, asset-uri) și componente descentralizate (ledger-e, DIDs/VCS), rezultând un regim de date mai dens și mai sensibil în unele cazuri. Amintim aici posibilitatea

de a colecta date ce pot identifica sau profila utilizatorii chiar fără a colecta „nume și prenume”. Vorbim aici despre telemetrie spațială, biometrie comportamentală, mapări ale spațiului și expresii faciale/oculare etc. Un studiu realizat de USENIX Security pe un eșantion de 55.541 utilizatori VR ne arată cum pot fi identificați aceștia cu o acuratețe de 94% în doar 100 de secunde de monitorizare a mișcărilor capului și a mâinilor în raport cu obiecte virtuale (Nair et al., 2023). Plecând de la aceste premise, la nivel de guvernanță a datelor principiile clasice (roluri, politici, stewardship, calitate, risk & compliance) rămân valabile, dar extinse cu o clasificare pentru „biometrie comportamentală XR”, control ciclul de viață pentru asset-uri 3D și trasabilitate on/off-chain (Data Administration Management Association, 2010; ISO et al., 2017).

Utilizatorii au posibilitatea în Metavers de a folosi identități interoperabile între diverse lumi. Standardele W3C pentru Decentralized Identifiers (DID) (W3C, 2022) și Verifiable Credentials (VC 2.0) (W3C, 2025) oferă un cadru neutru de platformă destinat gestionării identităților digitale. Aceste standarde permit identificarea principalelor atribute specifice unui utilizator (de exemplu, vârstă, drepturi de acces sau statut) prin mecanisme de divulgare minimă a informațiilor, precum și prin procese de delegare și revocare controlată. Acest model poate asigura portabilitatea identității, precum și implementarea unui regim de consimțământ granular specific mediilor virtuale multiple și interconectate, cum este Metaversul. W3C a publicat DID v1.0 (stabil), iar VC Data Model v2.0 este recomandare W3C din 15 mai 2025; v1.1 pentru DID este în lucru.

La nivel de asset-uri, guvernanța datelor acoperă atât metdatele în sine (on și off-chain) cât și obiectele ca atare. Aceste date nu au o protecție infailibilă și pot fi compromise/furate cu repercursiuni economice și la nivel de încredere dintre cele mai grave. Un caz relevant îl reprezintă atacul major petrecut în martie 2022 asupra sidechain-ului Ronin (folosit de Axie Infinity) rezultând pierderi de ordinul milioanei de dolari în criptomonede, incident care a evidențiat vulnerabilități structurale în custodia cheilor private, mecanismele de validare a tranzacțiilor și monitorizarea rețelei. Acest eveniment a demonstrat în mod concret că lipsa unor mecanisme robuste de guvernanță a datelor și infrastructurilor asociate poate submina încrederea utilizatorilor și stabilitatea ecosistemelor digitale bazate pe blockchain (Halborn, 2022; Reuters, 2022). Guvernanța activelor digitale în Metavers presupune implementarea unor controale tehnice și organizaționale avansate menite să reducă riscurile asociate proceselor de custodie, transfer și interoperabilitate. În primul rând, se impune separarea clară a responsabilităților privind custodia cheilor criptografice și utilizarea unor mecanisme puternice de protecție și gestionare a acestora. Două astfel de mecanisme pot fi Hardware Security Modules (HSM) sau Multi-Party Computation (MPC). HSM-urile reprezintă dispozitive hardware specializate, concepute pentru generarea, stocarea și utilizarea cheilor într-un mediu securizat și rezistent la manipulare, în timp ce MPC se bazează pe împărțirea unei

chei private în mai multe părți distribuite, astfel încât operațiile criptografice să poată fi realizate colaborativ fără ca cheia completă să fie expusă într-un singur punct. În al doilea rând, infrastructura tranzacțională trebuie susținută de jurnalizare inviolabilă și trasabilă, completată cu sisteme de detecție a anomaliilor și cu un playbook de răspuns la incidente (set documentat de proceduri operaționale standard - Standard Operating Procedures – SOPs) care să includă atât notificarea imediată a utilizatorilor, cât și protocoale clare de recuperare și compensare (Reuters, 2022). În al treilea rând, adoptarea unor standarde de interoperabilitate poate evita fragmentarea și riscul creării unor ecosisteme digitale închise. Pentru active digitale, formatele deschise avem glTF sau USD ce facilitează portabilitatea obiectelor 3D între diferite lumi virtuale, în timp ce, pentru identitate digitală, Decentralized Identifiers (DID) și Verifiable Credentials (VC 2.0) oferă un cadru interoperabil de atestare și verificare. Aceste inițiative sunt deja promovate de Metaverse Standards Forum, care funcționează ca un consorțiu de armonizare a standardelor tehnice (W3C, 2022; Metaverse Standards Forum, 2025; W3C, 2025)

Rapoarte precum (OCDE, 2024) propun realizarea unei convergențe între politicile de AI și confidențialitate, prin aplicarea principiilor de protecție a datelor pe întregul ciclu de viață al unui sistem AI: de la colectarea și preprocesarea datelor, la antrenarea și rularea modelelor, și până la stocarea și reutilizarea ulterioară. În contextul Metaversului, acest cadru este relevant deoarece datele generate de dispozitive XR (de exemplu, mișcări, gesturi sau expresii faciale) pot fi folosite pentru a antrena modele predictive privind comportamentul sau emoțiile utilizatorilor, ceea ce ridică probleme privind nivelul de transparență, minimizare și control asupra datelor personale.

În concluzie, este greșit să privim astăzi guvernanța datelor în Metavers exclusiv prin prisma principiilor tradiționale (DAMA-DMBOK, ISO/IEC 38505, COBIT etc.) fără o extindere și adaptare la noile realități tehnologice. Dacă în lumea clasică guvernanța datelor operează în principal prin structuri centralizate, baze de date instituționale și procese formale de conformitate, în Metavers aceasta trebuie să răspundă unor contexte distribuite și descentralizate, unde identitatea, activele și interacțiunile utilizatorilor se desfășoară în timp real și dincolo de granițele unei singure platforme. Persistența mediilor 3D, caracterul continuu al interacțiunilor multi-utilizator și dezvoltarea unor economii digitale complexe transformă datele într-o resursă critică, și indispensabilă atât pentru funcționarea sistemelor, cât și pentru protecția utilizatorilor. În această paradigmă, dimensiunile de securitate, confidențialitate, trasabilitate și interoperabilitate devin elemente structurale ce permit integrarea unor mecanisme specifice mediilor virtuale persistente, precum protecția datelor biometrice comportamentale, gestionarea identităților descentralizate și asigurarea portabilității activelor digitale. Prin consolidarea acestor repere, guvernanța datelor poate sprijini dezvoltarea unui Metavers sigur, transparent și sustenabil.

6. Modele și exemple de cadre de guvernare a datelor

Prezentare generală a principalelor cadre de guvernare a datelor

Alegerea unui model de guvernare potrivit reprezintă primul pas în proiectarea unui cadru de guvernare, în special în guvernarea datelor. Un model de guvernare de nivel superior acționează ca un plan ce direcționează luarea deciziilor, formarea politicilor și implementarea standardelor în întreaga organizație. Modelul de guvernare ales de o organizație influențează modul în care sunt atribuite sarcinile, gestionate informațiile, respectate politicile interne și reglementările externe. Astfel, modelul influențează maniera în care deciziile sunt vehiculate în cadrul organizației, determinând aspecte care variază de la alinierea strategică la nivel macro până la implementarea operațională cotidiană.

Înainte de implementarea cadrului de guvernare a datelor, o organizație trebuie să identifice acel model aliniat atât obiectivelor sale strategice cât și culturii și circumstanțelor sale operaționale. În același timp, trebuie să identifice tipurile de decizii ce vor trebui adoptate la nivel de conducere. Aceste alegeri pot include diferite responsabilități ce variază de la decizii strategice, cum ar fi elaborarea politicilor de confidențialitate și a cadrului de conformitate, până la decizii tactice, precum stabilirea controlului accesului la date sau gestionarea standardelor de calitate a datelor. Această abordare nu doar că optimizează procesele de guvernare, ci și garantează alinierea fiecărei decizii la obiectivele strategice ale organizației, consolidând astfel coerența și eficacitatea implementării politicilor de guvernare a datelor.

Un alt factor important în stabilirea modelului de guvernare a datelor se referă la transmiterea deciziilor de guvernare la nivel de organizație. În acest sens trebuie avut în vedere modul în care deciziile sunt propagate în cadrul organizației și în ce fel diferitele părți interesate interacționează în cadrul de guvernare. În linii mari, organizațiile pot alege între mai multe modele de guvernare, fiecare cu caracteristici distincte: de sus în jos (top-down), de jos în sus (bottom-up), din centru spre periferie (center-out), structuri izolate (Silo-in) și hibrid.

Guvernare și fluxuri decizionale de tip top-down (de sus în jos)

Dacă deciziile liderilor au impact asupra întregii organizații sau doar asupra unor segmente, acestea trebuie să fie comunicate în mod eficient către grupurile de guvernare. Acest proces este similar cu transmiterea deciziilor executive prin organigrama organizațională, utilizând canale de management adecvate, unde fiecare subnivel adaugă detalii specifice și relevante pentru implementarea corespunzătoare a deciziilor.

Modelele de guvernanță și decizie de tip top-down se bazează pe modele de autoritate. Odată luate, deciziile nu sunt de obicei deschise dezbaterii, iar conformitatea nu este opțională. Pentru creșterea eficienței acestui model într-un cadru de guvernanță a datelor, este necesară o legătură clară între Consiliul de guvernanță a datelor de la nivel executiv și celelalte structuri implicate.

Acest model, precum și toate celelalte modele de guvernanță, sunt influențate semnificativ de conceptul cunoscut sub denumirea de „Tone from the Top” (Tonul de la vârful). Această noțiune se referă la impactul pe care comportamentul și declarațiile liderilor îl au asupra percepției și conformării la politicile din cadrul organizației¹. Dacă există o politică oficială, dar leadershipul manifestă o atitudine sau un comportament ce desconsideră acest criteriu, managementul de nivel mediu și personalul operațional sunt mult mai puțin predispuși să acorde importanță respectării acelei politici. Prin urmare,

„Tonul de la vârful” poate determina tendința în asigurarea unei implementări consistente și a respectării politicilor organizaționale.

Guvernanță și fluxuri decizionale de tip bottom-up (de jos în sus)

În contrast cu modelul top-down, unele decizii legate de date pot fi asumate de personalul operațional ca parte a muncii lor zilnice, iar rezultatele ”să urce” ierarhic în organizație. Un exemplu în acest sens poate fi procesul de standardizare a denumirii datelor, acolo unde o echipă dedicată propune o serie de standarde ce sunt adoptate ulterior de întreaga organizație. Pentru ca acest model să fie eficient, indivizii cu responsabilități de gestionare a datelor trebuie să știe cine este punctul lor de contact în cadrul ierarhiei de responsabilitate și/sau al Biroului de Guvernanță a Datelor. Sugestiile, problemele și cerințele trebuie să poată „urca” până la niveluri superioare.

Guvernanță și fluxuri decizionale de tip center-out (din centru spre periferie)

În anumite contexte, prezența experților care să ofere îndrumări precise asupra acțiunilor necesare nu poate fi înlocuită de alte soluții. Biroul de Guvernanță a Datelor (sau CIO-ul sau alt lider) poate solicita experților să specifice modele de date, să interpreteze cerințele de conformitate, să proiecteze controale sau să stabilească protocoale. Deciziile center-out sunt luate de echipa sau persoana responsabilă cu guvernanța datelor care stabilește standarde de date, ce sunt ulterior adoptate de întreaga organizație. Conducerea poate emite în cele din urmă un mandat (să ia o decizie de tip top-down), dar înainte de aceasta, grupul desemnat evaluează opțiunile și impactul lor asupra părților interesate.

Pentru ca modelele de guvernanță și fluxurile decizionale „center-out” să fie eficiente, nu este suficient să se bazeze exclusiv pe autoritatea sursei. Este necesar

¹ Domnisoru S. et al. (2017) Interacțiuni între cultura organizațională și controlul intern. *Audit Financiar*. 15(148), 628.

să se implementeze multiple strategii de persuasiune pentru a convinge părțile interesate să adere la deciziile furnizate de centru. În acest context, se recomandă luarea în considerare a următoarelor aspecte:

- Solicitarea conducerii să stabilească un „Tone from the Top” puternic în ceea ce privește conformitatea;
- Utilizarea mai multor canale de comunicare pentru a transmite mesaje clare despre importanța deciziei și necesitatea conformității;
- Educarea părților interesate cu privire la motivele pentru care a fost luată decizia și ce alternative au fost luate în considerare;
- Stabilirea unui proces clar de excepții, a unui traseu de escaladare a problemelor și a unui proces de rezolvare a problemelor;
- Guvernanță și fluxuri decizionale de tip silo-in (structuri/grupuri izolate)

Fluxul decizional silo-in aduce împreună reprezentanți din mai multe grupuri de experți pentru a conveni colectiv asupra unei căi de acțiune. Consiliile de guvernanță și stewardship (responsabil în gestionarea datelor) sunt exemple ale acestui model. În vederea realizării unui echilibru optim între cerințele specifice ale fiecărui grup de experți și obiectivele generale ale organizației, se organizează frecvent întâlniri între aceste grupuri. Aceste întâlniri au ca scop elaborarea de politici, stabilirea standardelor pentru întreaga organizație și luarea deciziilor privind soluționarea problemelor asociate cu gestionarea datelor. Astfel de interacțiuni facilitează alinierea și integrarea nevoilor diverse ale părților interesate, rezultând un cadru de guvernanță a datelor coeziv și eficient.

În procesul decizional de tip silo-in, consiliul de guvernanță este așteptat să furnizeze perspective variate și cuprinzătoare. Membrii consiliului sunt obligați să analizeze efectele potențiale asupra diferitelor grupuri de părți interesate din întreaga organizație, având în vedere impactul deciziilor asupra diverselor segmente și funcții ale acesteia. Această abordare holistică conduce către o guvernanță eficientă, minimizând riscurile legate de izolarea informațiilor și a deciziilor.

Modelele de flux decizional silo-in pot fi foarte eficiente în luarea „deciziilor care rămân”. Ele elimină argumentul că părțile interesate au fost excluse dintr-un proces decizional și, prin urmare, nu ar trebui să fie obligate să se conformeze deciziei. Participanții devin implicați în proces și sunt mai predispuși să promoveze conformitatea. Pentru ca acest model să funcționeze, grupul de experți trebuie să primească autoritatea deplină pentru a lua decizii în numele întreprinderii. Reprezentanții trebuie să fie autorizați să acționeze în numele grupurilor lor și trebuie să fie respectați de cei pe care îi reprezintă, astfel încât deciziile lor să fie acceptate.

Modele hibride

Unele decizii trebuie luate la mai multe niveluri. Un grup de experți poate elabora o recomandare, iar apoi un grup de nivel superior va lua decizia finală. Atunci când sunt implicate considerații politice sau cu impact bugetar, poate fi necesar un model hibrid de flux decizional: o recomandare center-out sau silo-in va fi urmată de o decizie de tip top-down.

În prezent, s-au dezvoltat și testat în mod extensiv diverse cadre și metodologii pentru guvernanța datelor în diferite sectoare industriale, furnizând soluții structurate și validate pentru gestionarea eficientă a activelor informaționale. Aceste cadre includ o serie de recomandări și bune practici ce asigură calitatea, integritatea și conformitatea datelor. De asemenea, oferă o soluție matură de gestionare a diverselor probleme complexe legate de managementul datelor, contribuind astfel la o mai bună gestionare a informațiilor ce susțin atât obiectivele strategice ale organizațiilor, cât și cerințele legale actuale. Principalele exemple de cadre de guvernanță a datelor consacrate, validate și implementate pe scară largă, care au demonstrat eficacitate în practică, sunt: DGI; DAMA DMBOK; McKinsey; Eckerson; PwC; Deloitte; COBIT (Control Objectives for Information and Related Technologies); ISO/IEC 38500; EDM Council's DCAM (Data Management Capability Assessment Model); GDPR (EU General Data Protection Regulation); The CMMI (Capability Maturity Model Integration) Data Management Maturity (DMM) Model; The NIST (National Institute of Standards and Technology) Privacy Framework; CDMC (Cloud Data Management Capabilities) Framework.

Analiză detaliată a principalelor cadre de guvernanță a datelor

Cadrul de guvernanță a datelor propus de DGI

Dezvoltat de Data Governance Institute, DGI Framework este unul dintre cele mai utilizate cadre de guvernanță a datelor, oferind o structură logică pentru gestionarea deciziilor privind datele într-o organizație. Acest cadru se axează pe alinierea strategiilor de gestionare a datelor la obiectivele organizaționale². Componentele cheie ale acestui cadru includ principii pentru gestionarea calității datelor, securitate, acces și conformitate. Totodată, DGI oferă orientări clare privind rolurile și responsabilitățile în gestionarea datelor, stabilind proprietățile datelor și proceduri pentru asigurarea calității.

² Data Governance Institute (2024), *DGI Data Governance Framework*, Disponibil la: <https://datagovernance.com/the-dgi-data-governance-framework/> [Accesat: 14 Aug. 2024].

În continuare vor fi analizate componentele de bază ale sistemului:

- Obiectivele, metricii și finanțarea vizează clarificarea modului în care programul de guvernanță a datelor ar putea contribui la creșterea veniturilor, optimizarea costurilor și asigurarea rezilienței afacerii în fața riscurilor sau a perturbărilor.
- Controalele sunt utilizate pentru gestionarea riscurilor și pot fi preventive sau corective. Acestea pot fi aplicate la diverse niveluri ale cadrului, pentru a susține obiectivele programului de guvernanță a datelor.
- Biroul de Guvernanță a Datelor (DGO) are rolul de a supraveghea întregul program de guvernanță, de a colabora și de a coordona cu ceilalți factori interesați, de a alinia politicile și standardele referitoare la date și de a menține înregistrări detaliate despre program.

DGI este un cadru flexibil și ușor de adaptat, axat pe obiective de afaceri și politici clare, facilitând alinierea dintre date și cerințele de afaceri. Totuși, acest cadru poate necesita resurse semnificative de implementare, în special în organizațiile mari, unde este nevoie de o adaptare detaliată pentru a integra toate structurile organizaționale.

DAMA DMBOK (Data Management Body of Knowledge)

DAMA DMBOK este un cadru de gestionare a datelor recunoscut la nivel global, oferind un corpus de cunoștințe în guvernanța datelor și managementul acestora. Structura DAMA DMBOK include aspecte legate de arhitectura datelor, calitatea datelor, securitate și confidențialitate, precum și managementul metadatelor și al resurselor.

Viziunea asupra managementului datelor este reprezentată de un cerc cu guvernanța datelor în centru (ca un ax), înconjurată de nouă arii de cunoaștere. Guvernanța datelor este considerată planificarea la nivel înalt necesară pentru un management eficient al datelor. Fiecare arie de cunoaștere explorează o direcție a guvernanței datelor. De exemplu:

- Managementul arhitecturii datelor reprezintă structura generală a datelor și modul în care acestea se conectează cu fiecare aplicație din ecosistemul de date;
- Dezvoltarea datelor se concentrează pe modelarea datelor, analiza cerințelor, proiectarea, implementarea și mentenanța elementelor de stocare a datelor, cum ar fi bazele de date;

- Managementul metadatelor implică colectarea, clasificarea, integrarea și menținerea metadatelor de înaltă calitate.

Cadrul definește, de asemenea, elemente de mediu care oferă structură fiecărei arii de cunoaștere. Acestea definesc procesele fundamentale, rolurile, tehnologiile și livrabilele care ghidează planificarea și execuția fiecărei arii.

Ca avantaj principal, acest cadru oferă o privire holistică asupra guvernancei și managementului datelor, fiind ideal pentru organizațiile ce doresc o gestionare structurată și completă a datelor (Dama International, 2017).

Totuși, în anumite condiții, DAMA DMBOK este un cadru complex și tehnic, ceea ce îl poate face dificil de implementat fără resurse și expertiză semnificativă în managementul datelor.

Modelul McKinsey de guvernancea a datelor

Modelul McKinsey își propune să îmbunătățească valoarea datelor prin utilizarea eficientă a acestora și alinierea managementului datelor la obiectivele strategice ale organizației. Componentele cheie includ patru piloni esențiali: managementul calității datelor, definirea și controlul accesului, securitatea datelor și conformitatea cu reglementările³.

McKinsey consideră că regândirea întregului design organizațional este punctul de plecare pentru asigurarea succesului în guvernancea datelor. Șablonul pentru cadrul de guvernancea a datelor include trei componente esențiale:

- Un birou de management al datelor (DMO) care definește politicile și standardele, instruește și ghidează liderii de date și asigură integrarea guvernancei datelor cu fiecare altă funcție din cadrul organizației;
- Roluri bazate pe domeniu care gestionează execuția zilnică a programului de guvernancea a datelor;
- Un consiliu al datelor care conduce direcția strategică generală a programului de guvernancea a datelor. Acesta reunește biroul DMO și liderii de domeniu pentru a revizui progresul, a autoriza finanțarea și a soluționa problemele și blocajele în vederea unei guvernance eficiente.

Punctele forte vizează faptul că modelul este structurat astfel încât să fie eficient pentru implementări rapide, fiind ușor adaptabil la cerințele de afaceri. Limitările decurg din accentul pus pe obiectivele strategice, fapt care poate să nu ofere o structură detaliată pentru toate funcțiile de gestionare a datelor.

³ McKinsey & Company (2018), *Analytics comes of age*, [Accesat: 30 Oct. 2024].

Modelul Eckersons pentru guvernanța datelor

Dezvoltat de Eckerson Group, acest model este cunoscut pentru abordarea sa flexibilă, bazată pe obiective, concentrându-se pe simplificarea proceselor de guvernanță a datelor. Per ansamblu, modelul se concentrează pe patru domenii-cheie: politică și conformitate, calitatea datelor, accesul la date și integrarea datelor (Eckerson, 2010).

Grupul Eckerson propune un cadru de guvernanță a datelor structurat pe șase niveluri și 39 de componente. Iată câteva dintre aceste niveluri:

- Obiectivele și standardele abordează motivele și modalitățile de implementare a unui program de guvernanță a datelor;
- Procesele asigură că inițiativele de guvernanță a datelor își ating obiectivele finale. Acestea pot include de la asigurarea calității și acurateții datelor până la catalogarea metadatelor;
- Cultura promovează un mediu de colaborare, democratizarea datelor și transparență, fără conflicte.

Elementul distinctiv al acestui cadru este că plasează oamenii în centrul guvernanței datelor, definind roluri precum proprietari de date, administratori, curatori și părți interesate, pentru a clarifica rolurile și responsabilitățile lor în accesarea, utilizarea și modificarea datelor.

Principalul avantaj al acestui model este faptul că simplifică procesul de guvernanță și se concentrează pe probleme esențiale precum calitatea și conformitatea, ceea ce îl face potrivit pentru organizațiile care doresc o guvernanță a datelor ușor de implementat. Totuși, este posibil ca acest cadru să nu fie suficient de robust pentru organizațiile cu structuri complexe și cerințe detaliate de gestionare a datelor.

Cadrul de guvernanță a datelor propus de PwC

PricewaterhouseCoopers (PwC) a dezvoltat un cadru de guvernanță a datelor la nivel de întreprindere care combină managementul datelor cu alinierea strategică și conformitatea. Componentele cheie ale PwC Framework includ strategii pentru alinierea datelor la obiectivele de afaceri, standardizarea datelor și asigurarea conformității și securității datelor⁴.

Cadrul de guvernanță a datelor pentru întreprinderi PwC pornește de la modelele convenționale precum DAMA DMBOK pentru a integra datele de nouă generație.

PwC include cinci componente în standardele sale cadru de guvernare a datelor.

⁴ PricewaterhouseCoopers (2024), *Data and analytics*, Disponibil la: <https://www.pwc.com/gr/en/advisory/data-and-analytics.html> [Accesat: 30 Oct. 2024].

Începe cu o strategie de guvernare a datelor, urmată de un nivel de management care cuprinde toate aspectele unui ecosistem de date. Stratul de management al ciclului de viață acoperă toate politicile necesare pentru a asigura un flux eficient de date pe parcursul ciclului său de viață. Nivelul de administrare se concentrează pe impunerea guvernării, iar facilitatorii guvernării țin cont de oamenii, procesele și tehnologiile implicate în asigurarea unei guvernări eficiente.

Ca punct forte, acest cadru de guvernanță este ușor de aplicat de către organizațiile mari cu o structură bine definită și orientată spre conformitate. Totuși, în anumite condiții, poate necesita resurse semnificative și expertiză pentru implementarea completă.

Modelul Deloitte de guvernanță a datelor

Modelul Deloitte se concentrează pe riscurile și beneficiile datelor pentru a asigura o guvernanță robustă și aliniată la cerințele legale. Principalele componente ale acestui cadru includ gestionarea calității datelor, protecția datelor, conformitatea și analiza riscurilor.

Potrivit modelului Deloitte, guvernarea datelor se referă la „maximizarea valorii datelor pentru eficiența operațională, luarea deciziilor și cerințele de reglementare precum și reducerea la minimum a riscurilor asociate cu un management defectuos al datelor”⁵.

Principalele elemente ale acestui cadru de guvernare a datelor sunt:

- Politici și principii care ghidează guvernarea și gestionarea datelor;
- Organizații care stabilesc roluri și responsabilități de guvernare a datelor;
- Procese care descriu modul în care datele sunt create, modificate și întreținute;
- Instrumente și tehnologie care stabilesc implementarea instrumentelor, modelării și arhitecturii de date;
- Controalele de guvernare definesc valorile pentru a măsura eficacitatea guvernării datelor.

Modelul Deloitte oferă o abordare structurată, orientată pe reducerea riscurilor și pe respectarea conformității legale. Cu toate acestea, acest cadru poate fi mai potrivit pentru organizațiile mari, care au nevoie de un management detaliat al riscurilor în gestionarea datelor.

⁵ Deloitte (2022), *Data Governance - Deloitte Point of View (PoV)*, Disponibil la: <https://www.serverdirect.nl/assets/pdfs/deloitte-uk-data-governance-point-of-view.pdf> [Accesat: 30 Oct. 2024].

COBIT (Control Objectives for Information and Related Technologies)

Dezvoltat de ISACA (Information Systems Audit and Control Association), COBIT este un cadru de management IT ce include principii și politici pentru guvernanța datelor și securitatea informației. Structura COBIT include obiective clare pentru securitatea datelor, gestionarea riscurilor, monitorizarea performanței și conformitatea (Lainhart et al., 2019).

COBIT include următoarele componente cheie relevante pentru guvernanța datelor:

- Alinierea cu obiectivele de afaceri: COBIT subliniază importanța alinierii inițiativelor de guvernanță a datelor cu obiectivele și scopurile de afaceri pentru a maximiza beneficiile investițiilor în IT și a spori succesul organizațional;
- Managementul riscurilor: Cadrul oferă o foaie de parcurs strategică pentru analiza, evaluarea și atenuarea riscurilor în activitățile de guvernanță a datelor. Susține o gestionare proactivă a riscurilor, sugerând că organizațiile își pot proteja activele de date esențiale prin anticiparea și prevenirea potențialelor amenințări;
- Măsurarea performanței: COBIT include metrici și indicatori care pot fi utilizați pentru măsurarea performanței proceselor de guvernanță a datelor. Prin aderarea la aceste metrici, organizațiile își pot urmări performanța în ceea ce privește guvernanța datelor și pot identifica modalități de îmbunătățire a succesului;
- Conformitatea cu cerințele legale și de reglementare: Dincolo de implementarea legilor și reglementărilor legale, COBIT ajută organizațiile să rămână conforme. Organizațiile care respectă practicile și regulile agreeate evită penalitățile.

COBIT este un cadru foarte robust, potrivit pentru organizațiile care doresc să integreze guvernanța IT cu managementul datelor. Totodată, acest model este complex și poate necesita expertiză IT avansată, astfel că implementarea sa poate fi dificilă pentru organizațiile mici

Standardul internațional ISO/IEC 38500

ISO/IEC 38500 este un standard internațional ce oferă linii directoare pentru guvernanța corporativă IT, incluzând gestionarea și securitatea datelor. Principiile

sale includ responsabilitate, strategie, achiziție, performanță, conformitate și comportament uman.

ISO/IEC 38500:2015 oferă principii directe destinate forurilor de conducere ale organizațiilor (ce pot include proprietari, directori, parteneri, manageri executivi sau persoane în funcții similare) pentru o utilizare eficientă, eficace și acceptabilă a tehnologiei informației (IT) în cadrul organizațiilor lor (Standardization, 2015).

Standardul ISO/IEC 38500:2015 se aplică guvernantei privind tehnologia informației în organizație, inclusiv proceselor de management și deciziilor legate de utilizarea actuală și viitoare a tehnologiei informației. Aceste procese pot fi gestionate de specialiști IT din cadrul organizației, de furnizori externi de servicii sau de unități de afaceri din interiorul organizației (Standardization, 2015).

Totodată, standardul este aplicabil tuturor tipurilor de organizații, inclusiv companiilor private și publice, entităților guvernamentale și organizațiilor non-profit. Este aplicabil organizațiilor de orice dimensiune, de la cele mai mici la cele mai mari, indiferent de nivelul de utilizare a tehnologiei informației. Scopul ISO/IEC 38500:2015 este de a promova o utilizare eficientă, eficace și acceptabilă a IT în toate organizațiile, prin:

- asigurarea părților interesate că, dacă principiile și practicile propuse de standard sunt urmate, acestea pot avea încredere în guvernanța IT a organizației;
- informarea și ghidarea organelor de conducere în guvernarea utilizării IT în organizația lor;
- stabilirea unui vocabular pentru guvernanța IT (ISO/IEC, 2015).

Puncte forte: Este un standard recunoscut la nivel internațional, potrivit pentru organizațiile care doresc să implementeze practici de guvernanță a datelor bazate pe standarde internaționale.

Limitări: Necesită un nivel ridicat de aliniere cu structura organizațională, ceea ce poate îngreuna aplicabilitatea în organizațiile dinamice sau mai mici.

Modelul DCAM (Data Management Capability Assessment Model) propus de EDM Council

DCAM este un model de evaluare a capacității de management al datelor, conceput de EDM Council pentru a măsura și îmbunătăți practicile de gestionare a datelor. Data Management Capability Assessment Model (DCAM) definește modul în care se stabilește strategia de date, se fundamentează cazul de afaceri, se implementează modelul operațional și se sprijină colaborarea organizațională

necesară pentru a guverna unul dintre cele mai importante active ale unei firme - datele sale⁶.

Cele opt componente esențiale organizează cele 38 de capacități și 136 de sub-capacități ale modelului. Cea mai recentă versiune, DCAM v2.2, include o a opta componentă pentru Managementul Analitic, formalizând modul în care activitățile de analiză din cadrul unei organizații sunt structurate, executate și gestionate pentru a asigura alinierea acestora cu activitățile de management al datelor⁷.

Avantajul principal al DCAM este că permite organizațiilor să-și evalueze maturitatea în guvernanța datelor și să identifice oportunități de îmbunătățire.

Totodată, acest model necesită resurse pentru implementarea evaluărilor și ajustarea proceselor de guvernanță.

Modelul CMMI (Capability Maturity Model Integration) pentru guvernanța datelor

CMMI (Capability Maturity Model Integration) este un model de soluții bazat pe rezultate, conceput pentru a oferi organizațiilor rezultate mai rapide, mai bune și mai economice. Reprezintă un standard recunoscut la nivel global pentru îmbunătățirea capacității și performanței organizaționale, oferind un parcurs prioritar pentru dezvoltarea și implementarea unor noi capacități ce produc rezultate măsurabile și constante⁸.

Recunoscut drept un standard global pentru îmbunătățirea performanței, CMMI a fost inițial creat pentru Departamentul Apărării al Statelor Unite ale Americii pentru a evalua calitatea și capacitatea contractorilor săi de software. De atunci, modelul CMMI s-a extins dincolo de ingineria software pentru a sprijini orice organizație din orice industrie să construiască, să îmbunătățească și să măsoare capacitățile sale și să crească performanța.

Modelul CMMI este un set de bune practici evolutive la nivel global care permit organizațiilor să dezvolte și să compare capacitățile esențiale necesare pentru a răspunde celor mai frecvente provocări de afaceri. Modelul este proiectat să fie ușor de înțeles, accesibil, flexibil și să se integreze cu alte metodologii, cum ar fi Agile, SAFe și DevSecOps.

Evaluarea CMMI ajută la identificarea punctelor forte și a punctelor slabe ale proceselor unei organizații și examinează cât de bine se aliază acestea cu bunele practici ale modelului CMMI. Evaluarea oferă un focus clar, consecvent și aplicabil

⁶ EDM Council (2022), *DCAM: Data Management Capability Assessment Model 2.2*, Disponibil la: <https://edmcouncil.org/frameworks/dcam/> [Accesat: 30 Oct. 2024].

⁷ Ibid.

⁸ ISACA (2023), *Capability Maturity Model Integration (CMMI) Model*, Disponibil la: <https://www.isaca.org/enterprise/cmmi-performance-solutions> [Accesat: 30 Oct. 2024].

asupra îmbunătățirilor de performanță care vor avea cel mai mare impact asupra afacerii și vor sprijini dezvoltarea și îmbunătățirea capacităților organizațiilor la nivel global⁹.

Ca punct forte, acest model ajută organizațiile să-și stabilească o cale de dezvoltare graduală în guvernanța datelor. Totodată este un model foarte structurat, iar implementarea completă poate fi solicitantă din punct de vedere al timpului.

Cadrul NIST (National Institute of Standards and Technology) pentru confidențialitatea datelor

Dezvoltat de National Institute of Standards and Technology, NIST Privacy Framework este un cadru pentru protejarea confidențialității în utilizarea datelor. Componentele cheie includ funcții de identificare, guvernanță, control și comunicare a riscurilor de confidențialitate.

NIST Privacy Framework reprezintă un set de ghiduri concepute pentru a ajuta organizațiile să gestioneze riscurile de confidențialitate asociate cu colectarea, utilizarea, stocarea și partajarea informațiilor personale. Cadrul oferă o abordare flexibilă și scalabilă, care permite organizațiilor să adapteze programele lor de management al confidențialității la nevoile, profilurile de risc și obiectivele lor de afaceri specifice. Cadrul se bazează pe principii fundamentale de confidențialitate, aliniat la principii, legi și reglementări larg acceptate în domeniul confidențialității. NIST Privacy Framework sprijină organizațiile în construirea și menținerea unei posturi puternice de protecție a confidențialității.

Structura NIST Privacy Framework se bazează pe trei componente principale: Nucleu, Profile și Niveluri de implementare.

- Componenta Nucleu definește activitățile esențiale de confidențialitate, cum ar fi procesarea datelor, de-identificarea și securitatea, ghidând modul în care organizațiile își pot alinia obiectivele de confidențialitate cu misiunea generală.
- Componenta Profile ajută organizațiile să-și prioritizeze obiectivele de confidențialitate, să identifice lacunele și să dezvolte strategii pentru îmbunătățire continuă.
- Nivelurile de implementare permit organizațiilor să evalueze capacitățile de management al riscurilor de confidențialitate și să stabilească obiective pentru avansarea practicilor lor de confidențialitate.

Datorită flexibilității sale, cadrul poate fi adaptat la organizații de dimensiuni și industrii variate, făcându-l un instrument valoros pentru orice întreprindere care

⁹ Ibid.

dorește să-și îmbunătățească practicile de confidențialitate. În cele din urmă, NIST Privacy Framework permite organizațiilor să protejeze mai eficient datele sensibile, promovând o cultură a confidențialității și responsabilității (NIST, 2020).

NIST este un cadru flexibil și poate fi utilizat ca referință pentru alte reglementări de confidențialitate la nivel internațional. Totuși, aplicabilitatea sa poate fi limitată în afara SUA, deoarece se concentrează pe reglementările specifice din această regiune.

Cadrul CDMC (Cloud Data Management Capabilities)

Cloud Data Management Capabilities (CDMC) este un cadru de gestionare a datelor pentru platformele de tip cloud, conceput pentru a asigura guvernanța, securitatea și confidențialitatea datelor în mediile cloud. Componentele cheie includ strategii de guvernanță pentru integrarea securității, confidențialității și conformității în ecosistemele de tip cloud.

CDMC a fost dezvoltat de Grupul de Lucru CDMC al Consiliului EDM, cu participarea a peste 300 de profesioniști din peste 100 de firme, inclusiv principalii furnizori globali de servicii cloud – AWS, Google Cloud, IBM și Microsoft – precum și firme financiare de top, companii de consultanță, firme de tehnologie și numeroase alte corporații.

Pentru a sprijini companiile în migrarea către cloud și pentru a obține o vizibilitate mai mare asupra datelor din cloud, Cadrul CDMC este structurat în 6 componente, 14 capacități și 37 de sub-capacități care oferă orientări detaliate pentru protejarea datelor sensibile într-un mediu cloud sau cloud hibrid¹⁰.

CDMC este ideal pentru organizațiile care utilizează intens tehnologiile cloud și care doresc să integreze gestionarea datelor cu soluții de securitate avansate. Totuși, acest model poate fi mai puțin relevant pentru organizațiile ce nu utilizează platformele de tip cloud într-o măsură considerabilă.

Analiză comparativă a modelelor de guvernanță a datelor

Modelele de guvernanță a datelor analizate în această lucrare — DAMA-DMBOK, COBIT, ISO/IEC 38500, McKinsey și PwC — oferă perspective distincte asupra gestionării și valorificării datelor într-un cadru organizațional. În cele ce urmează, în Tabelul 6.1 prezentăm o analiză comparativă care evidențiază punctele forte și limitele fiecărui cadru, având în vedere aplicabilitatea lor în ecosisteme digitale emergente, cum este Metaversul. Modelul DAMA-DMBOK este considerat

¹⁰ Council E. (2021), Cloud Data Management Capabilities (CDMC) Framework, Disponibil la: <https://edmcouncil.org/frameworks/cdmc/> [Accesat: 30 Oct. 2024].

standardul de facto în managementul datelor, oferind un cadru robust și detaliat, ideal pentru organizațiile care urmăresc o guvernanță formalizată și cuprinzătoare. Avantajul său principal constă în structurarea clară a celor 11 domenii funcționale, de la arhitectura datelor și calitatea acestora, până la integrare și securitate. Totuși, tocmai această detaliere îl face relativ greu de implementat în contexte emergente și dinamice precum Metaversul, unde rapiditatea deciziei și adaptabilitatea contează mai mult decât rigoarea procesuală. Prin urmare, DAMA-DMBOK este potrivit ca bază teoretică sau cadru de referință pentru construirea unei politici coerente de guvernanță a datelor, dar trebuie combinat cu instrumente mai flexibile pentru implementarea practică.

Tabel 6.1. Principii grupate pe diferite aspecte ale ciclului de viață al guvernanței datelor

Model	Avantaje principale	Limite majore	Aplicabilitate în Metavers
DAMA-DMB	OCCadru cuprinzător, standardizat, acoperă toate domeniile de guvernanță a datelor.	Complexitate ridicată; dificil de adaptat rapid la contexte emergente.	Bun pentru structurarea inițială a guvernanței datelor.
COBIT 2019	Orientat spre guvernanță IT; suport pentru alinierea la obiective strategice.	Mai puțin focalizat pe specificul datelor și pe dinamica datelor nestructurate.	Util în proiecte de infrastructură digitală complexă.
ISO/IEC 38500	Recunoscut internațional; accent pe responsabilități la nivel de conducere.	Mai abstract, necesită completări din alte cadre pentru implementare practică.	Bază solidă pentru conformitate și audit.
Modelul McKinsey	Orientare strategică; pune accent pe valoarea de business a datelor.	Mai puțin formalizat; lipsa unei metodologii pas cu pas.	Eficient în proiecte agile și inovative.
Modelul PwC	Practic și flexibil; accent pe riscuri și oportunități de afaceri.	Nu este un standard formal; poate varia în funcție de consultant sau industrie.	Potrivit pentru evaluări rapide și inițiative pilot.

Pe de altă parte, COBIT 2019 este un model centrat pe guvernanța și managementul IT, oferind un limbaj comun și o structură bine definită pentru responsabilizarea actorilor implicați în procesele digitale. Este valoros în special pentru organizațiile cu infrastructuri IT complexe, deoarece include controale de audit, mecanisme de măsurare a performanței și linii directe pentru alinierea obiectivelor IT cu cele de afaceri. Cu toate acestea, COBIT este relativ generalist când vine vorba de guvernanța specifică a datelor, neabordând în profunzime aspecte precum viața ciclică a datelor, clasificarea acestora sau strategiile de monetizare. În Metavers, COBIT poate fi util ca fundament de control și conformitate, dar necesită suplimentare cu cadre orientate mai direct spre valoarea și comportamentul datelor.

ISO/IEC 38500 este un standard internațional pentru guvernanța IT care pune accent pe responsabilitate, strategie și performanță, adresându-se în special conducerii executive a organizațiilor. Punctul său forte este furnizarea unui cadru etic și strategic care ajută factorii decizionali să asigure utilizarea responsabilă a tehnologiei informației. Însă, standardul nu oferă instrumente concrete de implementare și nici nu abordează specific domeniul datelor într-o manieră operațională. În contextul Metaversului, ISO/IEC 38500 poate juca un rol important în setarea direcțiilor de guvernanță, asigurând un climat de încredere și responsabilizare, dar pentru o abordare eficientă a datelor este necesară completarea lui cu modele tehnice și procedurale mai detaliate.

Modelul de guvernanță a datelor dezvoltat de McKinsey este un cadru consultativ, valoros mai ales prin accentul pe rezultate concrete și valoare de business. Acesta promovează o abordare pragmatică, în care datele sunt tratate ca un activ strategic ce trebuie guvernat în funcție de impactul asupra obiectivelor organizației. Având o structură flexibilă și adaptabilă, este ideal pentru organizațiile care doresc să implementeze rapid politici de guvernanță într-un mediu aflat în schimbare, cum este Metaversul. Totuși, lipsa unei metodologii standardizate sau a unor instrumente formale poate limita aplicabilitatea sa în organizațiile care necesită conformitate strictă. Modelul McKinsey este foarte eficient pentru prototipuri, experimente și pentru susținerea inovației continue în guvernanța datelor.

Modelul PwC aduce o perspectivă orientată către risc și oportunitate în guvernanța datelor, fiind foarte apreciat în contexte de audit, conformitate sau transformare digitală accelerată. Acesta este construit pe logica evaluării continue și adaptării în funcție de maturitatea digitală a organizației, permițând astfel intervenții rapide, focalizate pe rezultate. Flexibilitatea modelului este un avantaj major în medii dinamice precum Metaversul, dar și o potențială vulnerabilitate în lipsa unei abordări standardizate, deoarece implementarea poate varia semnificativ în funcție de consultanți sau industrie. Cu toate acestea, PwC oferă un cadru excelent pentru evaluări de tip „quick wins”, precum și pentru integrarea rapidă a guvernanței datelor în strategiile organizaționale.

Ca observații generale, putem afirma că modelele standardizate (DAMA-DMBOK, ISO/IEC 38500) oferă robustețe și rigoare, dar pot fi mai greu de adaptat la viteza cu care evoluează tehnologiile emergente precum Metaversul. Modelele consultative (PwC, McKinsey) sunt mai flexibile și pot răspunde rapid la schimbări, dar lipsesc uneori instrumentele de validare formală. Modelul COBIT oferă un echilibru între guvernanța IT și alinierea strategică, dar este mai puțin centrat pe valorificarea datelor în sine, aspect esențial în ecosistemele Metavers.

Limitele și eșecurile guvernării datelor: lecții din sectorul public românesc

În contextul actual tehnologic și social, suntem obișnuiți să asociem deseori guvernarea datelor cu progresul organizațional și modernizarea instituțiilor publice, totuși realitatea ne arată în multe cazuri o implementare incompletă sau inefficientă. În România, sectorul public se confruntă cu întârzieri structurale, fragmentare instituțională și dificultăți în aplicarea principiilor de transparență și interoperabilitate. Inițiative precum programele de date deschise sau adoptarea principiilor FAIR au rămas în multe cazuri la nivel de intenții declarative, fără a fi transformate în practici instituționalizate și mecanisme de guvernare sustenabile. Un exemplu relevant îl constituie situația portalului data.gov.ro, principalul instrument național pentru publicarea datelor deschise. Din punct de vedere statistic, se observă o evoluție constantă în publicarea seturilor de date. De exemplu, în anul 2021, în cadrul angajamentului RO0065 din Open Government Partnership (Open Government Partnership, 2021), obiectivul era publicarea a minimum

535 seturi de date. În prezent (septembrie 2025), platforma data.gov.ro indică 4.803 seturi de date provenind de la 174 de instituții publice, ceea ce confirmă o tendință pozitivă în direcția deschiderii sectorului public. Dar, conform unor evaluări independente și reacții la nivel de societate civilă, persista anumite probleme privind interoperabilitatea și actualizarea datelor. Multe dintre seturile publicate sunt incomplete, dificil de reutilizat sau nu respectă principiile FAIR (Findable, Accessible, Interoperable, Reusable), ceea ce limitează valoarea lor practică pentru cetățeni, mediul academic și mediul privat. În aceste condiții, portalul riscă să fie perceput mai degrabă ca o realizare formală de conformitate cu angajamente internaționale, decât ca un mecanism funcțional de guvernare a datelor și de sprijin pentru politici publice bazate pe dovezi (World Wide Web Foundation, 2017; European Commission, 2022b).

Unul dintre cele mai importante efecte ale absenței unei guvernări eficiente a datelor se observă în domeniul colectării veniturilor fiscale. Conform rapoartelor OCDE, România continuă să înregistreze o eficiență scăzută în acest proces, în principal din cauza fragmentării infrastructurilor de date și a dificultăților de interoperabilitate între instituțiile responsabile. Iar lipsa unor mecanisme solide de integrare și analiză a datelor fiscale limitează capacitatea statului de a formula politici publice coerente și a câștiga încrederea contribuabililor (OCDE, 2022). Un alt exemplu negativ și din păcate, persistent privind guvernarea datelor, îl reprezintă incapacitatea instituțiilor publice de a corela și integra registrele electronice. De exemplu, registrele de stare civilă, evidența populației și bazele de date fiscale funcționează în paralel, cu standarde tehnice diferite și fără protocoale uniforme

de interoperabilitate. Raportul Digital Economy and Society Index (DESI) arată că România rămâne pe ultimele locuri în Uniunea Europeană la indicatorii privind serviciile digitale publice (European Commission, 2022a).

Un alt punct critic al guvernanței datelor îl constituie utilizarea inefficientă a acestora în fundamentarea politicilor publice. Datele colectate de instituții nu sunt valorificate în mod sistematic pentru formularea unor politici coerente în diverse domenii de la sănătate până la infrastructură. Spre exemplu, în domeniul sănătății, pandemia de COVID-19 a relevat întârzieri și inconsistențe în raportarea datelor epidemiologice, ceea ce a limitat reacțiile instituționale și a afectat transparența față de public (Andrei, 2022). Situații similare se regăsesc în educație sau infrastructură, unde datele există, dar sunt slab utilizate în procesul decizional.

Aceste exemple arată destul de limpede cum deficiențele structurale în colectarea și corelarea informațiilor afectează eficiența administrației publice și legitimitatea proceselor decizionale. Ca și concluzie, în România, guvernanța datelor se confruntă cu un decalaj structural între aspirațiile declarate și capacitatea instituțională efectivă, un decalaj ce trebuie redus prin politici consecvente, standardizare și o cultură organizațională orientată către valoarea datelor.

7. Componentele de bază ale unui cadru de guvernanta a datelor în Metavers

Principii de guvernanta a datelor în Metavers

Una dintre din principalele teorii din domeniul managementului strategic precum RBV (Viziunea Bazată pe Resurse - Resource-Based View) subliniază importanța resurselor interne ale unei organizații ca factor principal pentru obținerea unui avantaj competitiv sustenabil (Madhani, 2010). Una dintre principalele resurse este formată din date ce reprezintă un pilon strategic pentru avantajul și eficiența operațională a unei organizații. Această perspectivă este aliniată cu necesitatea unei structuri de guvernanta formalizate ce include roluri, politici de guvernanta a calității, securității și confidențialității datelor, contribuind astfel la gestionarea eficientă a disponibilității, utilizabilității, integrității și securității datelor în cadrul organizației.

Liniile directe sau principiile care stau la baza unui cadru de guvernanta a datelor reflectă valorile, scopurile și obiectivele organizației privind managementul și guvernanta datelor. Din perspectivă academică, principiile guvernantei datelor se bazează pe diverse teorii și exemple din domeniul sistemelor informaționale, comportamentului organizațional și managementului riscurilor. Adoptarea unor instrumente și tehnologii precum sistemele de management al metadatelor și a calității datelor, susține operaționalizarea acestor principii. Un raport publicat recent în care sunt analizate mai multe cadre de guvernanta (Marcucci et al., 2023), evidențiază 14 principii de bază aplicate gestionării datelor, acestea fiind: confidențialitate și securitate, responsabilitate, transparență, scop definit și legitim, corectitudine, protecția confidențialității, proporționalitate, confidențialitatea datelor, accesibilitate, protecție împotriva vătămării și nediscriminării, consimțământ informat, legalitate, cen-trat pe oameni, participare. Aceste principii formează baza pentru dezvoltarea unei strategii solide de guvernanta a datelor și contribuie la asigurarea unei gestionări eficiente și conforme a informațiilor într-o organizație. Mai mult, autorii au identificat și grupat aceste principii în funcție de diferitele aspecte ale ciclului de viață al guvernantei datelor, precum: procese, decizii și manipularea datelor, așa cum rezultă din Tabelul 7.1.

Tabel 7.1. Principii grupate pe diferite aspecte ale ciclului de viață al guvernantei datelor

Procese	Decizii	Manipularea datelor
Transparență	Transparență	Confidențialitate și securitate
Responsabilitate	Proporționalitate	Proporționalitate
Centrare pe oameni	Scop legitim	Date și informații accesibile
Corectitudine	Responsabilitate	Respectarea legii
Participare	Corectitudine	Consimțământ informat
Respectarea legii	Protecție împotriva vătămării și nediscriminării	Calitatea datelor

Dar care sunt principiile unui cadru de guvernanță pentru Metavers? Câțiva autori au încercat să răspundă la această întrebare ținând cont de particularitățile acestui concept. Principala caracteristică se referă la faptul că în Metavers, spațiul fizic și spațiul virtual interacționează simultan în timp real. Spațiile și evenimentele din lumea fizică sunt preluate sub formă de semnale prin utilizarea unui număr mare de senzori și dispozitive mobile, ulterior materializate într-o lume virtuală. În mod corespunzător, anumite acțiuni sau evenimente din domeniul virtual pot afecta lumea fizică (de exemplu, tranzacțiile financiare sau de bunuri, promovarea produselor, etc.). Astfel, pe de o parte, spațiul fizic este virtual îmbunătățit cu informații, iar pe de altă parte, spațiul virtual este reîmprospătat continuu cu intrări în timp real, din lumea reală. Într-un astfel de context, o cantitate mare de date și informații traversează Metaversul, între spațiile real și virtual pentru a avea cele două lumi sincronizate (Zhang et al., 2024). Acest context generează provocări semnificative, cum ar fi necesitatea de a procesa fluxuri de date eterogene pentru a integra evenimentele din lumea reală în cea virtuală și a disemina informații relevante din spațiul virtual către utilizatorii din lumea fizică. În plus, sunt indispensabile tehnologii avansate care să faciliteze gestionarea fără întreruperi a informațiilor între mediile fizice și digitale, incluzând interfețe inteligente, realități augmentate, gestionarea eficientă a stocării și diseminarea datelor la scară largă.

Coexistența spațiilor fizice și digitale oferă oportunități pentru aplicații noi. Unele dintre acestea sunt caracterizate prin fluxuri mari de date: exerciții militare, comerț și tranzacții financiare, jocuri și rețele sociale, asistență medicală inteligentă, educație inteligentă, oraș inteligent și administrație. Aceste aplicații sunt susținute de tehnologii emergente care alimentează construcția Metaversului. De exemplu: 1) tehnologia AI care facilitează generarea de conținut divers și interacțiune personalizată în Metavers; 2) tehnologia Blockchain care oferă baza economică în Metaversului; 3) Tehnologie interactivă imersivă (AR/VR/MR/XR) care oferă Metaversului o experiență senzorială superioară.

Acest potențial considerabil de inovare al Metaversului în multiple domenii implică și alte provocări, în principal legate de guvernanță, confidențialitate și considerente etice. Printre aceste provocări se numără aspecte precum conformitatea cu reglementările legale și fiscale, riscul de spălare a banilor, escrocheriile, fraudă, pirateria, rasismul și discriminarea (Dwivedi et al., 2022). Studii recente despre Metavers au arătat că securitatea datelor și implicit siguranța utilizatorilor în Metavers reprezintă unele dintre principalele provocări care trebuie rezolvate (Dwivedi et al., 2022; Fernandez et al., 2022). Conform lui Fernandez și Hiu, datele colectate de pe dispozitivele de realitate extinsă (XR) și căștile montate pe cap (HMD) sau comportamentul și comunicarea avatarurilor în lumea virtuală conțin informații sensibile despre utilizatori, care trebuie protejate împotriva infractorilor cibernetici.

Pe lângă securitatea datelor, colectarea datelor și preocupările legate de confidențialitate în Metavers reprezintă una dintre marile provocări. La nivel global, 41% dintre utilizatori își manifestă preocuparea cu privire la aspectele legate de confidențialitate și protecția datelor în Metavers¹. Capacitatea Metaversului de a colecta date privind comportamentul, expresiile și interacțiunile utilizatorilor ridică preocupări de confidențialitate comparabile cu cele din lumea reală. Există riscul ca utilizatorii să nu înțeleagă pe deplin amploarea procesului de colectare a datelor sau modul în care aceste date sunt utilizate. În acest sens, transparența în practicile de colectare a datelor, obținerea consimțământului informat și capacitatea utilizatorilor de a-și controla datele reprezintă principii de care va trebui să ținem seama într-un cadru de guvernanță a datelor în Metavers.

O provocare importantă în Metavers se referă la stabilirea (determinarea) proprietății datelor. De exemplu, avatarurile și interacțiunile utilizatorilor generează date, dar cui aparțin datele respective? Din acest punct de vedere, este utilă o definiție corespunzătoare a drepturilor de proprietate și înzestrarea utilizatorilor cu drepturi specifice de gestionare și ștergere a datelor personale. Pe măsură ce Metaversul devine mai integrat cu lumea fizică, legile existente privind protecția datelor ar putea avea nevoie de adaptare pentru a acoperi în mod adecvat mediile virtuale. Din acest motiv devine obligatorie actualizarea legislației și a reglementărilor în vigoare pentru a lua în considerare aspectele unice ale Metaversului, menținând totodată intacte și protejate drepturile utilizatorilor. Găsirea unui echilibru între reglementare și încurajarea creativității reprezintă o provocare pe care legiuitorii trebuie să o abordeze.

Plecând de la cele arătate anterior, putem afirma că pentru Metavers, guvernarea datelor trebuie să ghideze gestionarea colaborativă, responsabilă și transparentă a datelor, respectând principiile etice și reglementările în vigoare. Cadrul de guvernare a datelor pentru Metavers poate fi ancorat în următoarele principii descrise în Tabelul 7.2.

Tabel 7.2. Principii de guvernanță a datelor în Metavers

Principiu	Scop	Aplicare
Confidențialitate și protecția datelor cu caracter personal	Protejarea confidențialității utilizatorilor asigurând transparența, consensualitatea și caracterul minim invaziv al proceselor de colectare, procesare și partajare a datelor în Metavers.	Utilizatorii au posibilitatea de a-și gestiona propriile date, sistemul limitând colectarea acestora la strictul necesar pentru asigurarea funcționalității.
Securitate	Implementarea unor măsuri de securitate robuste în infrastructura Metavers ce contribuie la protejarea împotriva breșelor de securitate, hacking-ului și accesului neautorizat la date.	Criptare, autentificare multi-factor și monitorizare continuă pentru a proteja datele în toate etapele, de la creare la stocare și transmitere.

¹ Clement J. (2022), *Metaverse*, Statista, Disponibil la: <https://www.statista.com/topics/8652/%20525%20Metaverse/>.

Transparență și responsabilitate	Asigurarea transparenței în colectarea, utilizarea și partajarea datelor în Metavers. Toate activitățile de manipulare a datelor sunt transparente, iar părțile interesate sunt responsabile pentru acțiunile lor.	Furnizează informații clare utilizatorilor despre politicile și practicile privind datele. Necesită prezența unor organisme independente de supraveghere pentru a monitoriza și a aplica politicile de guvernare a datelor.
Trasabilitate	Garantarea urmăririi tuturor datelor din Metavers până la sursa lor și fiecare interacțiune sau transformare care implică datele este înregistrată și auditabilă.	Implementarea unor sisteme și instrumente care înregistrează metadatele, urmăresc descendența datelor și mențin jurnalele complete ale tuturor tranzacțiilor și activităților de procesare a datelor.
Proprietate și control asupra datelor	Stabilirea autorității, controlului și responsabilității asupra anumitor active de date.	Selectarea unor persoane sau entități specifice cu responsabilități clare și autoritate asupra datelor. Se permite utilizatorilor să dețină, gestioneze și să transfere datele pe diferite platforme și medii din Metavers.
Interoperabilitate	Promovarea interoperabilității datelor și a activelor digitale pe diferite platforme și servicii din Metavers, asigurând experiențe fără întreruperi.	Dezvoltarea și adoptarea de standarde și protocoale comune pentru formatele de date, API-uri și transfer de active, ce permit interacțiunea pe multiple platforme.
Accesibilitate, diversitate și incluziune	Facilitarea participării complete și echitabile a persoanelor din diverse medii și cu diferite abilități în experiențele din Metavers. De asemenea, trebuie să reprezinte diversitatea din lumea reală.	Abordarea diverselor nevoi ale utilizatorilor, inclusiv aspectele legate de diversitatea lingvistică, accesibilitatea pentru persoanele cu dizabilități și diferențele socio-economice.
Încredere și reputație	Implementarea unor mecanisme prin care se garantează faptul că datele rezultate în urma interacțiunilor și tranzacțiilor sunt exacte, valide, de încredere, oportune și relevante.	Protejarea sistemelor de manipulare și abuz.
Utilizarea etică a datelor	Evitarea practicilor care ar putea dăuna indivizilor sau comunităților, cum ar fi discriminarea, manipularea sau exploatarea.	Implementarea la nivel de algoritmi, AI și alte tehnologii bazate pe date și care interacționează cu utilizatorii în Metavers a unor norme și orientări etice.

Conformitate cu reglementările în vigoare	Garantarea respectării legilor, reglementărilor și standardelor relevante în domeniul gestionării datelor, confidențialității și securității.	Identificarea legilor și standardelor aplicabile privind protecția datelor. Integrarea cerințelor de reglementare în politicile și procedurile de guvernanță a datelor. Ajustarea politicilor și practicilor după necesitate.
Adaptabilitate	Adaptarea la natura evolutivă a Metaversului, permițând îmbunătățirea continuă și receptivitatea la noile provocări.	Actualizarea regulată a politicilor și a cadrului de guvernare a datelor, încorporând tehnologii emergente și cele mai bune practici.
Sustenabilitate	Minimizarea impactului asupra mediului datorat practicilor de gestionare a datelor în cadrul Metaversului.	Încurajarea utilizării centrelor de date eficiente din punct de vedere energetic și urmărirea amprentei de carbon digitală în cadrul platformelor Metavers.

Pilonii care susțin cadrul de guvernanță a datelor în Metavers

Următoarele elemente structurale ale unui cadru de guvernare a datelor sunt Pilonii. Aceștia oferă un cadru pentru operaționalizarea principiilor de guvernare a datelor. Literatura de specialitate oferă multiple perspective care variază în ceea ce privește numărul de piloni ce susțin guvernanța datelor și importanța acestora în cadrul operațiunilor moderne de afaceri.

Cigniti (2024) propune patru piloni principali ce stau la baza unui cadru de guvernare a datelor și a strategiilor de management²: Guvernanța datelor; Managementul datelor; Calitatea datelor; Securitate și conformitate. Freeson (2023) propune șapte piloni³ din care șase pot fi asociați cu un cadru de guvernanță a datelor și anume: Managementul calității datelor; Confidențialitatea și securitatea datelor; Gestionarea și supravegherea datelor; Gestionarea metadatelor; Managementul ciclului de viață al datelor; Conformitatea și reglementarea datelor. Pe blogul lor, cei de la DataGalaxy propun o soluție mai elaborată formată din 8 piloni⁴. Această soluție o vom prezenta în continuare detaliat.

² Cigniti (2024), *4 Key Pillars of Data Governance Framework and Management Strategies*, Disponibil la: <https://www.cigniti.com/blog/four-pillars-information-assets-management-data-insights/> [Accesat: 20 Aug. 2024].

³ Freeson O. (2023), *Understanding the Pillars of Data Governance: A Comprehensive Overview*, Disponibil la: <https://www.linkedin.com/pulse/understanding-pillars-data-governance-comprehensive-o-pmp-csm->

⁴ DataGalaxy (2023), *8 pillars of a successful data governance framework*, Disponibil la: <https://www.datagalaxy.com/en/blog/8-pillars-of-data-governance-frameworks/> [Accesat: 20 Aug. 2024].

Strategia și obiectivele de guvernare a datelor

Primul pilon este format dintr-o strategie clară de guvernare a datelor și obiective bine definite. Strategia de guvernare a datelor oferă o foaie de parcurs pentru implementarea practicilor de guvernare a datelor și asigură alinierea la obiectivele organizației. Organizațiile trebuie să-și stabilească viziunea de guvernare a datelor, să o alinieze cu strategia lor generală de afaceri și să definească obiective specifice care urmează a fi atinse prin strategia de guvernare a datelor. În acest pilon sunt evidențiate rezultatele urmărite, cum ar fi îmbunătățirea calității datelor, îmbunătățirea conformității și facilitarea luării deciziilor bazate pe date.

Roluri și responsabilități de guvernare a datelor

Al doilea pilon se concentrează pe definirea unor roluri și responsabilități clare de guvernare a datelor. Acest pas este important pentru identificarea persoanelor care vor fi responsabile de activitățile de guvernare a datelor, cum ar fi administratorii de date, proprietarii de date și comitetele de guvernare a datelor. Aceste roluri ar trebui să aibă responsabilități, autoritate și responsabilitate clar definite pentru deciziile și acțiunile legate de date. Prin atribuirea unor roluri și responsabilități specifice, organizațiile se asigură că practicile de guvernare a datelor sunt implementate, monitorizate și menținute în mod eficient. Delimitarea clară a rolurilor ajută la promovarea unei culturi a responsabilității datelor și a proprietății în cadrul organizației.

Politici și proceduri de guvernare a datelor

Politicile și procedurile de guvernare a datelor formează un alt pilon important al unui cadru de guvernare a datelor. Aceste politici definesc regulile, standardele și liniile directe pentru gestionarea datelor în cadrul organizației. Politicile pot include clasificarea datelor, cerințele privind calitatea, confidențialitatea, securitatea și păstrarea datelor. Procedurile subliniază procesele pas cu pas pentru implementarea practicilor de guvernare a datelor, cum ar fi profilarea, curățarea și controlul accesului la date. Politici și proceduri bine definite asigură coerența, claritate și aderarea la practicile de guvernare a datelor în întreaga organizație.

Managementul calității datelor

Acest pilon cuprinde o serie de procese și controale menite să garanteze acuratețea, completitudinea, coerența și actualitatea datelor. Aceste inițiative includ profilarea datelor pentru a analiza caracteristicile datelor, curățarea datelor pentru a rectifica erorile și consecvențele, validarea datelor pentru a asigura respectarea standardelor de calitate predefinite și monitorizarea datelor pentru a evalua continuu integritatea datelor.

Gestionarea metadatelor servește ca un alt pilon al unui cadru de guvernare a datelor. Metadatele oferă informații contextuale despre datele organizației, cum ar fi definițiile datelor, descendența datelor, relațiile de date și transformările datelor. Gestionarea eficientă a metadatelor asigură că utilizatorii pot descoperi, înțelege și utiliza cu ușurință elementele de date. Permite practici de guvernare a datelor, cum ar fi urmărirea liniei de date, analiza impactului și descoperirea datelor. Prin implementarea

unor practici robuste de gestionare a metadatelor, organizațiile pot maximiza valoarea activelor lor de date și pot facilita procesele de guvernanță a datelor.

Securitatea datelor și confidențialitatea

Organizațiile trebuie să acorde prioritate protecției informațiilor sensibile, să prevină accesul neautorizat și să asigure conformitatea cu reglementările privind protecția datelor. Sunt necesare măsuri adecvate de securitate a datelor, cum ar fi controale de acces, criptare și mecanisme de autentificare pentru a proteja activele de date de amenințări. Pe lângă securitatea datelor, este necesară și asigurarea confidențialității acestora. Organizațiile trebuie să stabilească politici și proceduri pentru a gestiona datele personale și sensibile în conformitate cu legile și reglementările aplicabile privind confidențialitatea. Acest lucru presupune obținerea consimțământului adecvat, implementarea tehnicilor de anonimizare a datelor și stabilirea de practici de păstrare și eliminare a datelor.

Comunicare și instruire privind guvernanța datelor

Comunicarea clară și continuă privind inițiativele de guvernanță a datelor asigură pentru toate părțile interesate înțelegerea importanței, beneficiilor, procedurilor și a așteptărilor strategiei. Acest pilon include comunicarea către personalul relevant din cadrul organizației a politicilor, procedurilor și modificărilor aduse strategiei de guvernanță a datelor. De asemenea, sunt necesare programe de instruire cuprinzătoare pentru a educa angajații despre principiile de guvernanță a datelor, cele mai bune practici, precum și despre rolurile și responsabilitățile acestora.

Măsurarea și monitorizarea guvernării datelor

Stabilirea indicatorilor cheie de performanță (KPI) și a unor metrici permite organizațiilor să evalueze eficacitatea și impactul inițiativelor lor de guvernanță a datelor. KPI-urile pot include scoruri de calitate a datelor, niveluri de conformitate, jurnalele de acces la date și sondaje privind satisfacția utilizatorilor. Monitorizarea regulată a acestor valori ajută la identificarea zonelor de îmbunătățire și la urmărirea progresului pentru atingerea obiectivelor de guvernanță a datelor.

Maturitatea guvernancei datelor și îmbunătățirea continuă

Acest pilon subliniază importanța evoluției și maturizării cadrului de guvernanță a datelor în timp. Guvernanța datelor nu este o implementare unică, ci un parcurs continuu de îmbunătățire și rafinare. Organizațiile ar trebui să își evalueze în mod regulat nivelul de maturitate al guvernancei datelor, să identifice lacune și să dezvolte o foaie de parcurs pentru îmbunătățirea continuă. Acest lucru implică o cunoaștere a celor mai bune practici din industrie, o adaptare la progresele tehnologice și alinierea practicilor de guvernanță a datelor cu nevoile în schimbare ale afacerii. Prin îmbunătățirea continuă, organizațiile pot crește eficiența, agilitatea și valoarea cadrului lor de guvernanță a datelor și pot asigura succesul pe termen lung.

Prin încorporarea acestor opt piloni într-un cadru cuprinzător de guvernanță a datelor, organizațiile pot stabili o bază solidă pentru gestionarea eficientă,

conformitate și luarea deciziilor bazate pe date. Fiecare pilon joacă un rol important în asigurarea succesului și sustenabilității inițiativelor de guvernanță a datelor, permițând organizațiilor să exploateze întregul potențial al activelor lor de date și să se îndrepte către excelența în afaceri.

Pentru Metavers, implementarea unui cadru solid de guvernanță a datelor implică alinierea cu un set de cerințe specifice, rezultat al specificității spațiilor virtuale și a tehnologiilor utilizate:

- Alinierea cu dinamica Metaversului: pilonii vor fi astfel definiți încât să abordeze provocările unice ale Metaversului, cum ar fi structura sa descentralizată, conținut generat de utilizator și interacțiunile multiplatformă. Fiecare pilon are rolul de a menține un mediu virtual sigur, interoperabil și guvernat etic.
- Asigurarea încrederii și siguranței: pilonii propuși trebuie să construiască și să susțină încrederea utilizatorilor, concentrându-se pe confidențialitate, securitate și utilizare etică.
- Sprijinirea inovației și scalabilității: pilonii trebuie să fie adaptabili și să susțină inovația și scalabilitatea necesare într-un peisaj digital în evoluție rapidă.
- Conformitate cu reglementările: Acești piloni trebuie să asigure alinierea practicilor de guvernare a datelor cu diverse cerințe legale.
- Consolidarea autonomiei utilizatorilor: accentul trebuie pus pe consolidarea autonomiei și suveranitatea datelor, promovând o abordare mai centrată pe utilizator a guvernanței datelor, care se aliază cu așteptările moderne privind drepturile digitale.

Având în vedere aceste cerințe și raportându-ne la principiile de guvernanță a datelor în Metavers expuse în capitolul anterior, propunem cinci domenii specifice sau piloni (vezi figura 7.1), care susțin strategia generală de guvernanță a datelor în Metavers.

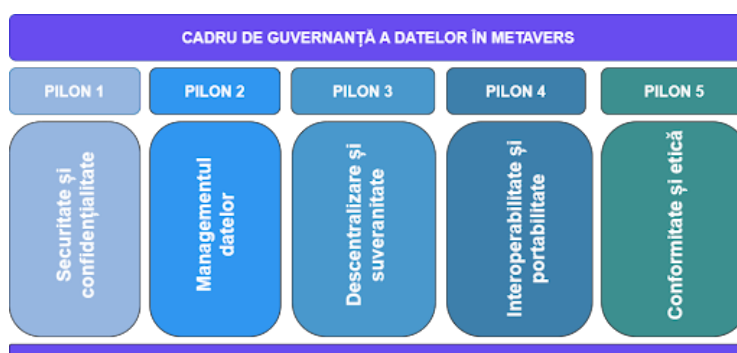


Figura 7.1. Piloni ai unui cadru de guvernare a datelor de succes în Metavers

Securitate și confidențialitate

În Metavers, cerințele de securitate la nivelul datelor și nu numai sunt determinate în principal de caracteristicile sale imersive și descentralizate, având drept scop să protejeze utilizatorii și sistemele împotriva breșelor, manipulării și fraudei. Securitatea la nivel de Metavers vizează în principal protejarea integrității lumii virtuale și a utilizatorilor prin măsuri precum autentificarea, criptarea datelor și controlul accesului, asigurând accesul exclusiv al utilizatorilor autorizați. De asemenea, prioritizează protecția datelor personale împotriva partajării sau utilizării neautorizate.

Accesul la Metavers prin intermediul avatarului și al dispozitivelor avansate implică riscuri de integritate a datelor personale ale utilizatorilor și provocări etice privind confidențialitatea, în special pentru categorii vulnerabile, precum copiii. Lipsa de securizare adecvată a conturilor și a platformelor aferente amplifică riscurile de securitate legate de identitate. Persoane rău intenționate pot recurge la phishing sau piratarea dispozitivelor pentru a fura sau replica identitatea avatarului, comițând fraude de identitate prin preluarea conturilor. Astfel, nu doar activele virtuale și datele personale, inclusiv cele de sănătate, sunt vulnerabile, ci și conexiunile sociale ale utilizatorului, mai ales dacă se utilizează dispozitive portabile sau VR avansat pentru autentificare biometrică. În timp ce parolele pot fi resetate, datele biometrice, odată compromise, nu pot fi schimbate, expunând utilizatorii la atacuri repetate. Identitățile furate pot fi utilizate pentru uzurparea conturilor, crearea de replici de avatar și comiterea de fraude sau atacuri de phishing.

Prin urmare, este necesară adoptarea unui set de măsuri de securitate specifice Metaversului având în vedere complexitatea și diversitatea amenințărilor cibernetice din acest mediu emergent. Aceste considerente includ implementarea unor metode robuste de autentificare și criptare pentru protejarea identității utilizatorilor, precum și dezvoltarea unor politici stricte de control al accesului, menite să prevină accesul neautorizat la conturi și date sensibile. Pot fi utilizate în acest sens metode de criptare avansată precum protocoalele SSL/TLS, pentru securizarea transferului de date între utilizatori, servere și aplicații Metavers, în special în cazul interacțiunilor în timp real ce implică date sensibile precum identitatea, tranzacțiile financiare și comunicațiile. În plus, este important să se asigure securitatea infrastructurii digitale și a dispozitivelor utilizate pentru accesarea Metaversului, inclusiv dispozitivele portabile și tehnologiile VR avansate, care pot colecta date biometrice extrem de sensibile.

Pe lângă măsurile tehnice, aspectele etice și legale ce țin de confidențialitate, protecția datelor reprezintă o alta obligativitate mai ales pentru protejarea grupurilor vulnerabile, cum ar fi minorii. Un cadru de reglementare adecvat și transparența în utilizarea datelor colectate pot garanta protecția drepturilor utilizatorilor în acest spațiu virtual complex. În mod similar, dezvoltarea unor mecanisme eficiente de detectare și răspuns la atacuri cibernetice în timp real contribuie la prevenirea și minimizarea impactul incidentelor de securitate. În continuare vom trece pe scurt în revistă principalele măsuri ce pot fi luate pentru îmbunătățirea cadrului de securitate al datelor în Metavers:

1. *Criptare*, atât a datelor aflate în tranzit prin metode avansate de tip SSL/TLS, cât și a tuturor datelor stocate, inclusiv activele, avatarele, tranzacțiile și conținutul generat de utilizatori.
2. *Controlul accesului și autentificare*: prin implementarea autentificării multi factor (MFA), mai ales mai ales când utilizatorii interacționează cu Metaversul prin rețele descentralizate sau dispozitive inteligente (căști VR, dispozitive mobile, dispozitive purtabile). De asemenea, controlul accesului bazat pe roluri (Role-based Access Control - RBAC) reprezintă o altă modalitate de securizare la nivel de acces în spațiul Metavers prin care sunt definite roluri și niveluri de acces pentru diferiți utilizatori și sisteme din Metavers, mai ales în cazul celor care pot accesa date sensibile și pot efectua operațiuni critice. Alte metode se referă la verificarea identității securizate pentru a preveni fraudă sau uzurparea identității în lumea virtuală.
3. *Monitorizare în timp real și detectarea amenințărilor prin*: 1) implementarea de sisteme de detectare a intruziunilor (IDS) ce pot monitoriza activitățile suspecte sau încercările de acces neautorizat în timp real, furnizând răspunsuri imediate la potențialele amenințări; 2) utilizarea analizei comportamentale în vederea detectării anomaliilor, precum accesul neautorizat la cont sau transferurile neobișnuite de active, care pot indica o încălcare sau o activitate rău intenționată și 3) detectarea descentralizată a amenințărilor în sistemele descentralizate sau bazate pe blockchain, cu privire la potențialele vulnerabilități sau atacuri în timp real.
4. *Menținerea integrității datelor* prin utilizarea blockchain și a tehnologiilor de regiștrii distribuți; utilizarea unor structuri criptografice ce pot verifica integritatea seturilor mari de date, orice modificare sau corupere a datelor putând fi detectată instantaneu; menținerea unor jurnale de audit cuprinzătoare ale accesului la date, tranzacțiilor și modificărilor.
5. *Descentralizarea managementului datelor* prin stocarea distribuită a datelor pe mai multe noduri, ceea ce reduce riscul unui singur punct de eșec. Tehnologii precum InterPlanetary File System (IPFS) sau soluțiile descentralizate de stocare în cloud asigură că datele rămân accesibile și securizate chiar dacă o parte a rețelei este compromisă; utilizarea protocoalelor „zero-knowledge proof” pentru a verifica anumite atribute (de exemplu, identitatea sau proprietatea) fără a dezvălui datele confidențiale, sporind atât securitatea, cât și confidențialitatea.
6. *Contracte inteligente (Smart contracts)* pentru automatizarea unor aspecte ale guvernanței datelor în Metavers (cum ar fi transferurile de active sau permisiunile de acces).

7. *Răspuns la încălcarea datelor și planificare pentru situații de urgență* prin existența unui plan de răspuns la incidentele și încălcările de securitate, inclusiv măsuri pentru detectarea incidentelor, investigare și recuperare; redundanța datelor și implementarea unor sisteme de backup securizate ce pot restaura datele rapid. Copiile de rezervă ar trebui, de asemenea, să fie criptate pentru a evita accesul neautorizat.
8. *Moderarea conținutului*: asigurarea faptului că conținutul generat de utilizatori este adecvat și nu încalcă regulile sau legile comunității.
9. *Respectarea legilor și reglementărilor*: Asigurarea că lumea virtuală respectă legile și reglementările relevante, în special în ceea ce privește protecția datelor și confidențialitatea utilizatorilor, combaterea spălării banilor și cunoașterea reglementărilor în vigoare.
10. *Monitorizare și testare continuă*: monitorizarea regulată a măsurilor de securitate aplicate și testarea acestora pentru a se asigura că funcționează conform prevederilor.
11. *Respectarea standardelor de securitate* prin alinierea practicilor de securitate a datelor în Metavers cu standardele globale de securitate, cum ar fi ISO/IEC 2700, GDPR pentru a asigura un management complet al securității informațiilor.

Gestionarea confidențialității și a consimțământului

Una dintre principalele provocări privind confidențialitatea în Metavers se referă la colectarea și utilizarea datelor utilizatorilor, existând preocupări privind conformitatea cu reglementările de protecție a datelor în vigoare. Metaversul necesită obținerea unor informații extinse despre utilizatori, inclusiv date personale, istoricul de navigare și locația, pentru a funcționa eficient. Aceste activități ridică îngrijorări legate de publicitatea țintită și de vânzarea datelor către terțe părți. Studiile au identificat diverse metrici derivate din caracteristicile morfologice ale unei persoane precum înălțimea, lungimea brațelor, culoarea părului etc, care pot fi utilizate pentru a deduce genul, vârsta, etnia, statutul socio-economic și chiar dizabilitățile utilizatorilor. Analiza acestor metrici poate avea implicații serioase în cadrul reglementărilor privind protecția datelor în Metavers, subliniind necesitatea unor măsuri adecvate pentru protecția acestora.

În Metavers, protecția datelor utilizatorilor reprezintă o preocupare majoră, având în vedere riscurile ridicate de exploatare de către actori malițioși. Vulnerabilitățile dispozitivelor AR/VR pot fi exploatare în vederea obținerii accesului neautorizat la datele sensibile ale utilizatorilor, iar atacurile de phishing pot induce utilizatorii în eroare să își dezvăluie informațiile personale. O altă strategie folosită de atacatori este crearea de aplicații false sau software care pot fura datele

utilizatorilor sau instala malware pe dispozitivele lor. Tactici de inginerie socială pot fi, de asemenea, utilizate pentru a înșela utilizatorii să ofere acces la dispozitivele sau informațiile lor personale.

Utilizatorii pot lua măsuri pentru a-și proteja confidențialitatea în Metavers, cum ar fi limitarea informațiilor personale partajate și utilizarea pseudonimelor sau avatarilor pentru a-și masca identitatea. De asemenea, pot adopta tehnologii de îmbunătățire a confidențialității, precum criptarea sau rețelele virtuale private (VPN), care anonimizează datele utilizatorilor, făcând astfel dificilă identificarea de către terți. În continuare urmează să fie detaliate câteva dintre principalele considerații referitoare la confidențialitate și gestionarea consimțământului în Metavers:

- a. Mecanisme de consimțământ pentru utilizatori: Utilizatorii trebuie să fie informați în mod clar și concis despre modul în care datele lor vor fi colectate, procesate, partajate și stocate. Această informație ar trebui să fie prezentată într-un format transparent și ușor de înțeles, mai ales în mediile de realitate virtuală, unde metodele tradiționale (de exemplu, acorduri lungi) pot fi ineficiente. Utilizatorii ar trebui să aibă posibilitatea de a oferi consimțământ granular pentru tipuri specifice de colectare și utilizare a datelor; de exemplu, pot consimți să împărtășească datele de bază ale avatarului, dar să refuze urmărirea comportamentului sau a informațiilor biometrice de la dispozitivele VR. De asemenea, având în vedere natura interactivă și în continuă evoluție a Metaversului, utilizatorii ar trebui să poată modifica preferințele de consimțământ în timp real, permițându-le ajustarea permisiunilor în funcție de noi experiențe sau interacțiuni.
- b. Minimizarea datelor și limitarea scopului implică colectarea doar a informațiilor necesare pentru furnizarea serviciilor și utilizarea acestora exclusiv în scopurile pentru care au fost colectate, evitând astfel utilizarea neautorizată sau abuzivă a datelor personale sensibile.
- c. Transparența în colectarea datelor impune ca platformele să dezvăluie clar informațiile colectate, inclusiv acțiunile din joc, achizițiile și datele biometrice, prezentând aceste informații într-un mod accesibil utilizatorilor și informându-i despre urmărirea interacțiunilor și comportamentului, oferindu-le opțiunea de a renunța, acolo unde este posibil.
- d. Anonimizarea și pseudonimizarea datelor cu caracter personal prin care utilizatorii trebuie să aibă posibilitatea de a interacționa în Metavers fără a-și dezvălui identitățile reale, prin utilizarea pseudonimelor sau avatarilor anonime, iar platformele trebuie să garanteze că datele pseudonime nu sunt ușor re-identificabile, considerându-se anonimitatea totală în cazurile în care nu este necesară asocierea activităților utilizatorului cu date personale.

- e. Controlul și portabilitatea datelor utilizatorului: în Metavers, utilizatorii trebuie să aibă un control clar asupra proprietății datelor personale, inclusiv a celor generate prin interacțiuni și active create, precum și capacitatea de a-și transfera datele (de exemplu, avatare, active digitale, conexiuni sociale) între diferite platforme sau de a le retrage complet.
- f. Protecția datelor biometrice și a celor provenite de la senzori: dispozitivele de realitate virtuală (VR) și augmentată (AR) colectează frecvent date biometrice sensibile, precum mișcarea ochilor, ritmul cardiac și gesturile, care necesită protecții speciale, iar consimțământul explicit și specific trebuie obținut pentru colectarea și utilizarea acestor date, împreună cu măsuri stricte pentru a preveni profilarea neautorizată bazată pe aceste informații sensibile.
- g. Ștergerea datelor și „Dreptul de a fi uitat” prin care platformele trebuie să stabilească politici clare de retenție a datelor personale, stipulând durata de păstrare și condițiile de ștergere, oferind utilizatorilor dreptul de a solicita ștergerea datelor lor în orice moment, în conformitate cu dreptul de a fi uitat, iar procesul de ștergere trebuie să fie realizat în mod sigur și ireversibil, în special în cazul platformelor descentralizate.
- h. Respectarea reglementărilor globale de confidențialitate prin care platformele care operează în Metavers trebuie să respecte reglementările globale privind confidențialitatea, precum Regulamentul General privind Protecția Datelor (GDPR), care impune cerințe stricte pentru obținerea consimțământului, garantarea drepturilor utilizatorilor asupra datelor și protejarea informațiilor personale, precum și legislații locale precum Legea privind Confidențialitatea Consumatorilor din California (CCPA), care conferă utilizatorilor dreptul de a fi informați despre datele colectate și de a refuza înstrăinarea acestora.
- i. Confidențialitate prin design și confidențialitate implicită: considerațiile de confidențialitate trebuie să fie integrate în arhitectura Metaversului încă de la început, stabilind confidențiatea ca setare implicită pentru toți utilizatorii, care trebuie să opteze activ pentru partajarea datelor, iar platformele trebuie să prioritizeze setările de confidențialitate ușor de utilizat, permițând utilizatorilor să controleze cine are acces la datele lor, modul în care sunt partajate și ce informații sunt vizibile pentru ceilalți.
- j. Protecția confidențialității copiilor: în cazul în care copiii utilizează Metaversul, ar trebui să se respecte legislații precum Legea privind Protecția Confidențialității Copiilor pe Internet (COPPA), care impune consimțământul parental pentru colectarea datelor de la minori, iar platformele trebuie să implementeze mecanisme de verificare a vârstei pentru a preveni expunerea minorilor la conținut inadecvat sau la practici de date neconforme cu reglementările.

- k. Realizarea de audituri de confidențialitate: platformele trebuie să efectueze sistematic operațiuni de audit a confidențialității pentru a asigura conformitatea cu propriile politici de confidențialitate și cu reglementările globale, iar rapoartele de transparență ar trebui să fie publicate pentru a detalia modul în care sunt utilizate datele, frecvența partajării acestora cu terțe părți și solicitările guvernamentale pentru informațiile utilizatorilor.

Gestionarea confidențialității și consimțământului în Metavers trebuie să fie transparentă, centrată pe utilizator și conformă cu reglementările. Oferind control clar asupra datelor, consimțământ granular și respectarea normelor globale, mediile virtuale au șansa să devină spații de încredere pentru utilizatori.

Managementul datelor

Ciclul de viață al datelor

Datele urmează un ciclu de viață complex, de la generare până la arhivare sau eliminare, iar guvernanța datelor stabilește un cadru riguros pentru gestionarea acestora pe tot parcursul acestui proces. Aceasta presupune implementarea unor politici clare de colectare, proceduri de arhivare eficiente și protocoale stricte de ștergere, asigurând nu doar o gestionare eficientă a datelor, ci și conformitatea cu cerințele legale și de reglementare, contribuind astfel la optimizarea resurselor și reducerea riscurilor asociate. Managementul ciclului de viață al datelor implică definirea proceselor pentru colectarea, stocarea, păstrarea și eliminarea datelor. Organizațiile trebuie să stabilească linii directe cu privire la cât timp trebuie păstrate diferite tipuri de date pe baza cerințelor legale, a nevoilor de afaceri și a modelelor de utilizare a datelor. De exemplu, o companie de telecomunicații poate păstra înregistrările cu detaliile apelurilor pentru o anumită perioadă pentru a respecta obligațiile de reglementare, în timp ce fișierele jurnal necritice pot fi șterse după o perioadă mai scurtă.

La nivel de Metavers principiile rămân aceleași, dar gestionarea datelor de-a lungul întregului ciclu de viață capătă totuși un alt sens, deoarece volume mari de date personale, tranzacționale și comportamentale sunt generate continuu. Din acest motiv sunt necesare măsuri complexe pentru manipularea adecvată în fiecare etapă a ciclului de viață a datelor pentru menținerea securității, integrității și confidențialității acestora, inclusiv a conformității cu reglementările. Principalele cerințe întâlnite la nivelul de management al ciclului de viață al datelor (Data Lifecycle Management - DLM) în contextul Metaversului pot fi încadrate în următoarele categorii:

- a. Crearea și colectarea datelor: în Metavers, generarea datelor prin interacțiunile utilizatorilor, crearea de conținut și colectarea datelor biometrice sau comportamentale necesită transparență și consimțământ explicit, iar platformele trebuie să respecte principiul minimizării datelor, colectând

doar informațiile necesare pentru scopuri specifice, conform reglementărilor precum GDPR.

- b. Păstrarea și clasificarea datelor: după colectare, datele trebuie stocate în mod securizat, fie în medii cloud centralizate, sisteme descentralizate (precum blockchain), sau abordări hibride, iar clasificarea acestora în funcție de tipul lor (e.g., date cu caracter personal, tranzacționale, comportamentale) impune măsuri suplimentare de securitate, cum ar fi criptarea și accesul restricționat, în timp ce redundanța stocării asigură protecția împotriva pierderilor accidentale sau atacurilor cibernetice.
- c. Utilizarea datelor: datele generate prin activitățile utilizatorilor în Metavers sunt utilizate pentru a îmbunătăți experiențele virtuale, a alimenta interacțiuni bazate pe inteligență artificială sau a facilita relaționarea socială, însă utilizarea acestora trebuie să respecte consimțământul utilizatorului, iar accesul terților la date trebuie reglementat prin acorduri clare și controlabile de către utilizatori.
- d. Partajarea datelor și portabilitatea: asigurarea portabilității și interoperabilității datelor în Metavers permite utilizatorilor să transfere ușor și în siguranță datele personale, activele digitale și informațiile de identitate între diverse platforme. Acest lucru necesită adoptarea de formate standardizate și API-uri securizate care să faciliteze partajarea autorizată a datelor.
- e. Controlul accesului bazat pe roluri: asigura că doar utilizatorii, serviciile sau sistemele autorizate pot accesa date sensibile, precum informațiile personale sau financiare, iar platformele din Metavers trebuie să ofere utilizatorilor controale intuitive de confidențialitate pentru gestionarea preferințelor de partajare și acces la date.
- f. Politici de păstrare a datelor: trebuie să stabilească clar durata stocării pentru diferite tipuri de date, asigurând conformitatea cu reglementările, iar arhivarea automată și securizată a datelor neutilizate trebuie implementată pentru o păstrare eficientă și accesibilă atunci când este necesar.
- g. Protecția și securitatea datelor: trebuie să includă metode de criptare puternice a datelor atât în tranzit, cât și în repaus, monitorizarea continuă a accesului pentru detectarea tentativelor neautorizate și planuri solide de răspuns la incidente, care să gestioneze eficient breșele de securitate și să prevină incidentele viitoare.

Gestionarea eficientă a ciclului de viață al datelor în Metavers necesită o planificare riguroasă la fiecare etapă, de la colectare și stocare până la ștergere, asigurând manipularea corectă a datelor, aplicarea criptării și controlul accesului, respectând în același timp reglementările globale de confidențialitate, ceea ce consolidează încrederea utilizatorilor și minimizează riscurile de breșe de securitate.

Managementul calității datelor

Managementul calității datelor reprezintă un pilon fundamental într-un cadru robust de guvernare a datelor, cuprinzând o serie de procese și controale destinate să asigure acuratețea, completitudinea, coerența și actualitatea informațiilor. Aceste inițiative includ profilarea datelor, care analizează caracteristicile acestora; curățarea, care rectifică erorile și inconsecvențele; validarea, care verifică conformitatea cu standardele de calitate predefinite; și monitorizarea, care evaluează continuu integritatea datelor.

Gestionarea metadatelor constituie un alt pilon al unei guvernări eficiente a datelor, oferind informații contextuale despre elementele de date ale organizației, inclusiv definiții, descendență, relații și transformări. O gestionare eficientă a metadatelor facilitează descoperirea, înțelegerea și utilizarea datelor, sprijinind practici precum urmărirea liniei de date, analiza impactului și descoperirea informațiilor. Prin implementarea unor practici solide de gestionare a metadatelor, organizațiile pot maximiza valoarea activelor lor de date și pot îmbunătăți procesele de guvernare a datelor.

În continuare, vor fi explorate principalele caracteristici sau cerințe necesare implementării managementului calității datelor în Metavers, evidențiind provocările și oportunitățile care apar în eforturile de a crea o experiență virtuală coerentă și centrată pe utilizator.

- a. Evaluare multidimensională a calității datelor: calitatea datelor poate fi evaluată pe mai multe dimensiuni, precum: 1) acuratețe: datele trebuie să reprezinte cu exactitate entitățile și evenimentele din lumea reală pe care le descriu. Datele inexacte pot duce la neînțelegeri, tranzacții eronate sau experiențe slabe ale utilizatorului; 2) completitudine: seturile de date ar trebui să includă toate informațiile necesare pentru ca utilizatorii și sistemele să funcționeze eficient. Datele lipsă pot împiedica interacțiunile și pot reduce calitatea generală a experienței Metaversului; 3) consecvență: datele trebuie să fie consecvente pe diferite platforme și sisteme din Metavers. 4) promptitudine: datele ar trebui să fie actuale și disponibile utilizatorului atunci când este necesar. Datele învechite pot avea un impact negativ asupra experiențelor utilizatorilor și luării deciziilor; 5) relevanță: datele ar trebui să fie relevante pentru contextul în care sunt utilizate. Datele irelevante pot aglomera interfețele cu utilizatorul și pot reduce implicarea.
- b. Validarea și verificarea datelor reprezintă procese ce includ implementarea unor instrumente automate care asigură acuratețea și conformitatea cu standardele de calitate stabilite, precum și mecanisme prin care utilizatorii pot verifica corectitudinea propriilor date, profiluri, tranzacții și active digitale.

- c. Monitorizare continuă și îmbunătățire implică realizarea de audituri regulate pentru evaluarea calității datelor în diverse sisteme și aplicații, precum și stabilirea unor mecanisme de feedback prin care utilizatorii pot raporta problemele legate de calitatea datelor, contribuind astfel la îmbunătățirea continuă a acestora.
- d. Interoperabilitate și standardizare asigurată prin dezvoltarea unor standarde comune de date în cadrul platformelor Metaversului. Astfel, poate fi asigurată consistența și calitatea datelor, inclusiv prin definirea formatelor, protocoalelor și terminologiei.
- e. Educație și conștientizare prin inițiative de alfabetizare digitală ce contribuie la creșterea implicării active a utilizatorilor în gestionarea calității propriilor date. De asemenea, platformele ar trebui să comunice clar metricile de calitate a datelor pentru a-i ajuta să înțeleagă fiabilitatea și validitatea informațiilor întâlnite.
- f. Soluții tehnologice: utilizarea instrumentelor de curățare a datelor poate ajuta la identificarea și corectarea inexactităților, duplicatelor și inconsecvențelor în seturile de date, iar aplicarea inteligenței artificiale și a învățării automate permite automatizarea evaluărilor calității datelor, detectarea tiparelor și identificarea problemelor de calitate în timp real, îmbunătățind astfel guvernanța datelor.
- g. Metrici de calitate a datelor și KPI: Definirea indicatorilor cheie de performanță (KPIs) pentru evaluarea calității datelor, cum ar fi ratele de eroare sau scorurile de completitudine, și raportarea periodică a acestor metrici permit factorilor de decizie să evalueze starea calității datelor și să ia măsuri pentru îmbunătățire.

Prin utilizarea soluțiilor tehnologice avansate și promovarea implicării utilizatorilor, platformele Metaversului pot îmbunătăți calitatea datelor și susține luarea deciziilor informate, contribuind astfel la optimizarea experienței utilizatorilor.

Descentralizare și suveranitate

Managementul distribuit al datelor

Descentralizarea și managementul distribuit al datelor sunt elemente fundamentale în construcția unui Metavers deschis și centrat pe utilizator. Distribuind datele în mai multe noduri, valorificând tehnologia blockchain și oferind utilizatorilor control asupra datelor lor, Metaversul poate oferi confidențialitate, securitate și experiențe utilizator îmbunătățite. Dar, introduce și provocări care necesită soluții inovatoare pentru a asigura integritatea datelor, scalabilitatea și interoperabilitatea perfectă pe diverse platforme.

Conceptul de descentralizare implică distribuirea controlului și proprietății între participanți, în loc de a fi concentrat într-o singură autoritate, ceea ce influențează procesul decizional, stabilirea regulilor și menținerea structurii mediului virtual. Sistemele descentralizate ale unei platforme Metavers utilizează adesea tehnologia blockchain pentru a stabili proprietatea asupra activelor virtuale, cum ar fi imobile digitale, avataruri sau monede virtuale, asigurându-se astfel prin chei criptografice controlul utilizatorilor asupra activelor lor digitale. Descentralizarea facilitează interoperabilitatea între diferitele lumi virtuale și platforme din Metavers, permițând utilizatorilor să transfere fără întreruperi active sau personaje între medii virtuale, promovând astfel o experiență coezivă și conectată care susține interacțiunea socială și participarea la procesele de guvernare care afectează întregul ecosistem Metavers.

Descentralizarea în contextul spațiului virtual, în special în Metavers, se referă la distribuirea controlului, autorității și procesului decizional între o rețea de participanți, în loc de a fi concentrate într-o entitate centrală, și implică utilizarea tehnologiilor distribuite, precum blockchain, pentru a asigura că nicio parte nu deține control total asupra mediului virtual. În guvernarea descentralizată a Metaversului, proprietatea activelor virtuale este facilitată prin tehnologia blockchain, adesea utilizând token-uri non-fungibile (NFT-uri), permițând participanților să controleze direct bunurile digitale, cum ar fi imobilele virtuale sau obiectele din joc, iar modelele descentralizate de guvernare permit utilizatorilor să participe la procesele de decizie prin organizații autonome descentralizate (DAO-uri). Luarea deciziilor este adesea împărțită între utilizatori și părțile interesate, permițând un model de guvernare mai democratic și mai participativ. Mecanismele de guvernare pot include organizații autonome descentralizate (DAO) în care părțile interesate votează asupra politicilor, caracteristicilor sau deciziilor financiare.

Chiar dacă descentralizarea vine cu unele compromisuri, aceasta oferă o mulțime de beneficii, permițând utilizatorilor să depășească unele probleme complexe ale lumii fizice. Dintre toate beneficiile pe care guvernarea descentralizată a Metaversului le oferă, următoarele sunt cele mai semnificative:

Împuternicirea utilizatorului: participanții la Metavers au un control sporit asupra activelor lor digitale, ceea ce încurajează participarea activă și investițiile în lumile virtuale.

Interoperabilitate: descentralizarea facilitează interoperabilitatea între diferite lumi și platforme virtuale. Utilizatorii pot transfera fără probleme active sau personaje dintr-o lume virtuală descentralizată în alta, promovând o versiune descentralizată din ce în ce mai complexă a spațiului virtual.

Rezistența la cenzură: descentralizarea reduce riscul de cenzură, deoarece nu există o singură entitate, cum ar fi un guvern, care să poată impune restricții asupra conținutului generat de utilizatori. Acest lucru promovează libertatea de exprimare și

creativitatea în spațiul digital și reprezintă o schimbare semnificativă în dezvoltarea unei societăți echitabile.

Proprietatea și suveranitatea datelor

Una dintre principalele promisiuni pe care a fost edificat conceptul de Web 3.0 se referă la restabilirea suveranității asupra datelor, depășind limitările impuse de către marile companii de tehnologie care continuă să se concentreze pe istoricul căutărilor și datelor de tip cookie în elaborarea profilului comportamental al utilizatorilor. În acest context, suveranitatea datelor se poate referi la „conceptul conform căruia datele colectate, stocate și procesate de o organizație sunt supuse legilor naționale și celor mai bune practici generale acolo unde sunt localizate fizic”.

Metavers-urile viitoare vor acumula cantități masive de date biometrice, în creștere exponențială, datorită utilizării căștilor VR și a ochelarilor de realitate augmentată dotate cu inteligență artificială, capabile să monitorizeze mișcările ochilor, să cartografieze mediul înconjurător și să înregistreze date precum ritmul cardiac și reacțiile pielii. Având acces la aceste informații, marile corporații tehnologice pot ști nu doar cum acționăm ci și cum reacționăm, putând construi profiluri extrem de cuprinzătoare și precise ale fiecărui utilizator. În plus există riscul exploatării în continuare a breșelor de securitate prin care au fost furate cantități importante de date personale. Un raport în acest sens este furnizat de Chainalysis State Of Web3 (Chainalysis, 2022). De asemenea, raportul evidențiază modul în care acei utilizatori care s-au confruntat cu încălcări ale normelor privind securitatea datelor prezintă un risc mai mare să devină victime ale infractorilor cibernetici.

În plus, marketingul și publicitatea în timp real în Metavers vor evolua semnificativ, depășind formele tradiționale de publicitate. În prezent, utilizatorii sunt expuși la anunțuri generice în urma căutărilor efectuate pe platforme precum Amazon sau Google, dar în Metavers, publicitatea va fi interactivă și personalizată, fiind facilitată de agenți controlați de inteligența artificială. Acești agenți, având forma unor avatare, vor fi capabili să se adapteze emoțiilor utilizatorilor în timp real, folosind algoritmi avansați pentru a influența comportamentele de cumpărare și a maximiza eficiența campaniilor publicitare. În mod special, adolescenții și copiii vor fi mai vulnerabili la aceste tehnici de marketing avansate, având în vedere că aceștia sunt adesea adoptatori timpurii ai noilor tehnologii. Această predispoziție îi face să fie expuși în mod special la influențele comerciale, dată fiind capacitatea lor limitată de a evalua critic mesajele publicitare și impactul acestora asupra comportamentului lor de consum.

În lumea fizică, uzurparea identității unei persoane este o provocare considerabilă; în contrast, platformele de socializare au simplificat acest proces prin proliferarea conturilor false și a roboților automatizați, cum ar fi cele întâlnite pe

Twitter (X). Metaversul are potențialul de a agrava aceste probleme, complicând astfel capacitatea utilizatorilor de a verifica autenticitatea identității cu care interacționează, fie că este vorba de indivizi sau de entități comerciale. Nu atât tehnologia în sine cât utilizarea ei necorespunzătoare poate genera îngrijorare, de aceea se dovedește necesară dezvoltarea unui cadru de identitate robust în Metavers, care să permită utilizatorilor un control adecvat asupra partajării datelor lor. Importanța suveranității datelor nu poate fi subestimată, iar considerentele de securitate ar trebui să fie integrate în arhitectura Metaversului încă de la început.

Să ne imaginăm un scenariu în care utilizatorii ar putea să își transporte datele de pe platforme de socializare, precum Instagram, oriunde s-ar deplasa. Aceste date ar include acreditările de conectare, cookie-urile și istoricul de navigare. La întoarcerea pe platformă, utilizatorii ar putea să se autentifice prin intermediul unui portofel digital, demonstrându-și identitatea, iar fluxul de știri ar fi personalizat în întregime pentru a reflecta preferințele anterioare. Această abordare ar permite o experiență de utilizare mult mai fluidă și adaptată nevoilor individuale. Pentru realizarea acestui scenariu a apărut conceptul de ”identități digitale auto-suverane (Self-Sovereign Identities)”. Este un concept în care utilizatorii găzduiesc date pe propria lor stocare (IPFS, Filecoin etc.) fără a se baza pe o terță parte. Aceste identități autonome sunt verificate de identificatori publici ai rețelelor descentralizate și nu se bazează pe un depozit central. Pe scurt înseamnă că un utilizator are control complet și autonomie asupra datelor sale de identitate și asupra modului în care acestea sunt utilizate. Pentru a verifica identitatea unei persoane care utilizează o identitate digitală, se recurge la Identificatori Decentralizați (Decentralized Identifiers - DIDs) și acreditive verificabile (verifiable credentials - VCs), standarde fundamentale definite de Consorțiul World Wide Web (W3C) pentru dezvoltarea unei structuri de Identitate Decentralizată; un DID este un identificator unic global, generat și înregistrat prin tehnologii de registre distribuite (DLT), asociat cu acreditive verificabile care atestă caracteristici specifice ale proprietarului, stocate într-un portofel digital fără a necesita intermediari. Astfel, utilizatorii nu trebuie să se reidentifice pentru fiecare acțiune, având capacitatea de a-și accesa identitatea digitală simplu prin extragerea portofelului, ceea ce facilitează interacțiunile și procesele online fără a necesita repetarea autentificării, sporind astfel eficiența și confortul utilizatorului în mediul digital.

Interoperabilitate și portabilitate

Interoperabilitatea datelor în Metavers se referă la capacitatea sistemelor, platformelor sau aplicațiilor de a comunica și de a utiliza datele eficient, asigurându-se că formatele și protocoalele sunt compatibile, în timp ce portabilitatea datelor permite utilizatorilor să transfere ușor bunurile digitale și informațiile personale

între platforme, fără pierderea dreptului de proprietate asupra acestora sau a funcționalității lor.

Importanța interoperabilității și portabilității constă în împuternicirea utilizatorilor prin controlul identităților și bunurilor digitale, asigurând o experiență utilizator fără întreruperi și stimulând inovația și colaborarea între dezvoltatori în cadrul ecosistemului Metavers. Standardele deschise și cadrele de interoperabilitate facilitează comunicarea și schimbul de date între diverse sisteme, aplicații și platforme. Aceste standarde asigură că diferitele tehnologii utilizate în Metavers pot colabora eficient, eliminând restricțiile proprietare care pot împiedica integrarea. Inițiativele precum cele ale W3C, cum ar fi Web3, își propun să stabilească protocoale și orientări comune pentru aplicațiile descentralizate (dApps) în Metavers, promovând astfel un mediu în care dezvoltatorii pot crea soluții interoperabile și portabile. Prin implementarea acestor standarde, utilizatorii pot beneficia de o experiență fluidă, având posibilitatea de a-și transfera fără dificultate activele digitale și identitățile între diferite medii virtuale, contribuind astfel la un ecosistem mai dinamic și mai integrat.

La acest nivel provocările se referă la fragmentarea standardelor de date, cauzată de lipsa unor formate și protocoale universale acceptate, ceea ce împiedică schimbul eficient de informații între platforme diferite. Complexitatea tehnică este, de asemenea, un obstacol major, deoarece implementarea soluțiilor de interoperabilitate necesită o colaborare strânsă între dezvoltatori, platforme și alți actori implicați pentru a asigura compatibilitatea sistemelor. În plus, transferul de date între platforme ridică probleme serioase de securitate și confidențialitate, iar protejarea datelor utilizatorilor și asigurarea securității acestora pe parcursul transferului este crucială pentru menținerea încrederii în sistemele interoperabile.

Pentru a menține un grad înalt de interoperabilitate și portabilitate a datelor în Metavers este necesară îndeplinirea unui set de cerințe fundamentale pentru construirea unui spațiu deschis, interconectat, care acordă prioritate libertății și controlului utilizatorului. Principalele cerințe pot fi încadrate astfel:

- a. Standardizarea formatelor de date sunt necesare pentru a asigura interoperabilitatea, deoarece permit platformelor din Metavers să utilizeze structuri comune de date și metadate, facilitând schimbul și interpretarea uniformă a informațiilor între diverse sisteme.
- b. Utilizarea de protocoale interoperabile și API-uri standardizate pentru a permite schimbul de date și interacțiunea sigură între platformele din Metavers, facilitând comunicarea în timp real și transferul fluent al avatarurilor și bunurilor virtuale între diverse medii virtuale fără conversii suplimentare de date.

- c. Identitate descentralizată (DID) și identitate auto-suverană (SSI) permit utilizatorilor să dețină și să gestioneze independent identitatea lor digitală, facilitând verificarea interoperabilă a identității și controlul asupra datelor personale în diverse platforme din Metavers.
- d. Portabilitatea activelor digitale oferă utilizatorilor posibilitatea de a transfera și utiliza în mod eficient activele între platforme diverse, prin adoptarea unor formate interoperabile. Aceasta asigură nu doar continuitatea experienței utilizatorului, ci și menținerea controlului și integrității activelor digitale (e.g., avatare, NFT-uri), eliminând dependența de o platformă specifică și promovând un mediu virtual deschis și conectat.
- e. Adoptarea standardelor deschise: platformele din Metavers trebuie să adopte standarde deschise pentru schimbul de date și interoperabilitate, precum cele dezvoltate de W3C sau inițiative precum Metavers Standards Forum, care se concentrează pe crearea unor linii directoare universale pentru ecosistemul Metaversului. Framework-urile de interoperabilitate definesc modul în care diferitele platforme pot integra sisteme, protocoale și formate de date compatibile, facilitând astfel unificarea Metaversului și asigurând o funcționalitate fluidă și coerentă între platforme.
- f. Securitatea datelor și respectarea preferințelor de confidențialitate asigură protecția informațiilor sensibile și partajarea acestora doar pe baza consimțământului utilizatorilor. Prin adoptarea de formate de date standardizate, protocoale securizate, sisteme de identitate descentralizate și modele de guvernare interoperabile, Metaversul poate oferi utilizatorilor posibilitatea de a se deplasa fluid între platforme/spații virtuale, de a menține controlul asupra propriilor active și de a se implica în diverse experiențe virtuale.
- g. Sisteme de plăți interoperabile ce necesită adoptarea unor mecanisme unificate care să permită transferul facil al criptomonedelor, token-urilor sau monedelor virtuale între platforme, asigurând astfel compatibilitatea și funcționarea fără întreruperi a economiilor virtuale.

Conformitate și etică

Conformitatea cu reglementările

Guvernanța datelor asigură că organizațiile respectă reglementările legale și specifice industriei. Conformitatea implică stabilirea de procese care monitorizează utilizarea datelor, urmăresc modificările și aplică politicile legate de date. Prin alinierea practicilor de date cu reglementările, organizațiile atenuează riscurile și potențialele răspunderi legale.

Mediile virtuale trebuie să fie guvernate de reglementări precum GDPR, CCPA și alte legi regionale care protejează datele personale, asigurându-se că practicile lor de gestionare a datelor respectă aceste norme. De asemenea, se impune implementarea unor sisteme de auditare și raportare, care să permită monitorizarea și evaluarea constantă a modului în care datele sunt gestionate. Aceste sisteme vor oferi transparență și vor asigura că orice practici neconforme sau riscuri de securitate sunt identificate și remediate prompt, consolidând încrederea utilizatorilor.

Pe lângă acestea, pot fi stabilite mecanisme eficiente de soluționare a disputelor pentru a aborda conflictele legate de proprietatea datelor, încălcările de securitate sau utilizările abuzive. Principalele aspecte ce țin de conformitate cu reglementările în vigoare pot fi descrise astfel:

- a. Confidențialitatea și protecția datelor implică necesitatea respectării reglementărilor globale privind protecția datelor, precum GDPR și CCPA, astfel încât utilizatorii să își poată exercita drepturile de acces, rectificare și ștergere a datelor, chiar dacă se află imersați într-un mediu virtual cu jurisdicție ambiguă.
- b. Moderarea conținutului și asumarea răspunderii presupune necesitatea reglementării conținutului generat de utilizatori, moderarea eficientă a conținutului dăunător sau ilegal în conformitate cu legi precum Digital Services Act, asigurând totodată mecanisme de raportare și soluționare a activităților ilicite.
- c. Reglementări financiare și de combatere a spălării banilor (AML) prin implementarea unor mecanisme de prevenire a activităților financiare ilicite, alinierea cu legislația fiscală și facilitarea raportării conformității fiscale pentru activele și veniturile virtuale.
- d. Protejarea proprietății intelectuale (IP) presupune necesitatea protejării drepturilor creatorilor și prevenirea falsificării în Metavers, gestionarea diferențelor între jurisdicțiile internaționale în materie de IP necesitând noi cadre sau acorduri.
- e. Protecția consumatorilor cu aplicabilitate inclusiv asupra tranzacțiilor virtuale din Metavers, asigurându-se astfel protecția utilizatorilor împotriva practicilor frauduloase, publicității înșelătoare și prețurilor neloiale, precum și stabilind responsabilitatea pentru bunurile virtuale defectuoase sau prezentate greșit.
- f. Conformitate cu legile muncii și ocupării forței de muncă: dacă Metaversul devine un spațiu pentru munca virtuală și activități economice, platformele vor trebui să asigure conformitatea cu legile muncii, drepturile muncii și protecția lucrătorilor. Aceasta ar putea include asigurarea unor salarii echitabile, evitarea practicilor de exploatare a muncii în spații virtuale și asigurarea drepturilor lucrătorilor, chiar dacă aceștia operează într-o economie virtuală.

- g. Protecția copiilor și furnizarea de conținut adecvat vârstei: având în vedere accesibilitatea Metaversului pentru publicul mai tânăr, platformele trebuie să respecte reglementări precum Children's Online Privacy Protection Act (COPPA) din S.U.A., asigurându-se că datele copiilor sunt protejate și că este furnizat conținut adecvat vârstei. De asemenea, trebuie implementate mecanisme de verificare a vârstei, obținerea consimțământului părinților și mecanismele de control pentru a asigura conformitatea cu legile care protejează minorii împotriva conținutului neadecvat sau exploatării.
- h. Reglementări de mediu: practicile de sustenabilitate în Metavers implică conformarea cu reglementările emergente privind sustenabilitatea mediului, inclusiv adoptarea tehnologiilor eficiente din punct de vedere energetic și raportarea emisiilor de carbon, ceea ce poate necesita integrarea tehnologiilor verzi și utilizarea algoritmilor de consens eficienți energetic, precum Proof of Stake.
- i. Etică și responsabilitate socială: platformele din Metavers trebuie să adopte cadre etice care să asigure standarde de corectitudine, transparență și nediscriminare, mai ales în utilizarea inteligenței artificiale (AI) pentru luarea deciziilor și personalizarea experiențelor utilizatorilor.

În concluzie, pilonii unui cadru de guvernare a datelor asigură în mod colectiv că datele sunt exacte, sigure și gestionate etic. Prin prioritizarea acestor elemente fundamentale, organizațiile pot spori încrederea utilizatorilor, pot promova practici responsabile de date și pot sprijini creșterea durabilă a Metaversului, în timp ce protejează drepturile utilizatorilor și promovează un mediu virtual corect, transparent și incluziv.

Împreună, pilonii descriși mai sus formează un cadru holistic de guvernanță a datelor, esențial pentru navigarea în complexitatea Metaversului; pe măsură ce potențialul vast al datelor este valorificat în acest mediu imersiv, va exista un angajament puternic față de principiile de guvernanță, ceea ce va contribui la sporirea încrederii utilizatorilor, promovarea practicilor responsabile de gestionare a datelor și susținerea creșterii sustenabile a Metaversului. Implementarea de succes a unui Cadru de Guvernanță a Datelor nu doar că asigură conformitatea și securitatea, dar permite organizațiilor să valorifice pe deplin datele lor, stimulând inovația și îmbunătățind angajamentul utilizatorilor, astfel că, pe măsură ce avansăm în această nouă frontieră a interacțiunii digitale, adoptarea acestor piloni va permite construirea unui Metavers echitabil, de încredere și benefic pentru toți participanții.

Utilizarea etică a datelor

Având în vedere cantitatea enormă de date personale, comportamentale și financiare care sunt generate și procesate în interiorul spațiilor virtuale, adoptarea unor linii directoare privind utilizarea etică a datelor în Metavers contribuie în

mod substanțial la protejarea utilizatorilor, asigurarea transparenței și încurajarea gestionării responsabile a datelor în Metavers. La acest nivel principalele cerințe pot fi rezumate astfel:

- a. Asigurarea confidențialității și protecția datelor utilizatorilor reprezintă o cerință prioritară la nivel de Metavers, ce permite utilizatorului să exercite un control sporit asupra informațiilor partajate, cum sunt folosite și cu cine, în timp ce colectarea datelor ar trebui să fie minimizată pentru a evita utilizările nejustificate.
- b. Asigurarea consimțământului informat se bazează pe politici de transparență a datelor, care garantează o informare detaliată a utilizatorilor cu privire la modalitățile de colectare, utilizare și partajare a datelor, oferindu-le în același timp posibilitatea de a-și revoca sau modifica consimțământul în orice moment.
- c. Supraveghere și urmărire comportamentală trebuie să se bazeze pe monitorizarea etică a datelor în Metavers și evitarea exploatării acestora în scopuri manipulative sau de supraveghere excesivă, protejând autonomia și confidențialitatea utilizatorilor, iar publicitatea personalizată trebuie să fie limitată pentru a preveni exploatarea vulnerabilităților psihologice și comportamentelor nocive.
- d. Asigurarea proprietății și controlului asupra datelor presupune atingerea unui grad înalt de suveranitate al utilizatorilor asupra propriilor date prin garantarea dreptului acestora de a-și accesa, modifica, transfera sau șterge datele, inclusiv activele digitale create.
- e. Asigurarea securității și integrității datelor prin criptare, autentificare sigură și control al accesului. Necesitatea protejării integrității datelor împotriva manipularii pentru a preveni fraudele sau furtul de identitate în Metavers.
- f. Utilizarea corectă a datelor și evitarea exploatării acestora constituie o altă cerință importantă în contextul exploatării etice a datelor în Metavers. Practicile curente de utilizare a datelor trebuie să contribuie la prevenirea discriminării și exploatării utilizatorilor, asigurând totodată că algoritmi și sistemele de inteligență artificială sunt concepute într-o manieră transparentă, care să promoveze echitatea, evitând impunerea unor modele de afaceri ce pot profita de grupurile vulnerabile, garantând astfel un mediu digital responsabil și echitabil pentru toți participanții.
- g. Transformarea etică a IA și transparența algoritmilor necesită integrarea valorilor etice în fiecare etapă a dezvoltării, de la concepție la evaluare. Utilizarea responsabilă a datelor implică clarificarea funcționării sistemelor, a deciziilor luate și a impactului asupra utilizatorilor, oferind informații accesibile și responsabilitate, mai ales când există consecințe asupra bunăstării utilizatorilor.

- h. În cazul specific al protecției datelor privind minorii și persoanele vulnerabile mecanismele de consimțământ trebuie să fie clare și adaptate nivelului de înțelegere al utilizatorilor, iar platformele trebuie să implementeze măsuri suplimentare de securitate. Respectarea reglementărilor globale, precum COPPA/GDPR, alături de protejarea confidențialității și implicarea activă a părinților sau tutorilor, contribuie la realizarea unui mediu digital sigur și respectuos față de drepturile utilizatorilor.
- i. Bunăstare digitală și sănătate mintală: utilizarea datelor în Metavers trebuie să țină cont de impactul asupra bunăstării mentale și emoționale a utilizatorilor, evitând crearea unor medii care să favorizeze dependența sau comportamentele dăunătoare; platformele nu ar trebui să folosească datele comportamentale pentru a manipula utilizatorii în a petrece timp excesiv în Metavers, ignorând responsabilitățile lor în lumea reală.

Prioritizând liniile directoare etice privind consimțământul, proprietatea datelor și echitatea, platformele pot construi o relație de încredere și proteja drepturile utilizatorilor, dezvoltând un Metavers care promovează bunăstarea digitală și evită exploatarea.

Componentele de bază ale unui cadru de guvernanță a datelor în Metavers

Un cadru de guvernanță a datelor în Metavers reprezintă un set de principii, politici și proceduri menite să ghideze colectarea, stocarea, utilizarea și partajarea datelor într-un mod responsabil. Componentele acestui cadru nu sunt doar măsuri tehnice, ci și elemente strategice care asigură transparența, securitatea și respectarea drepturilor utilizatorilor. Prin definirea clară a responsabilităților și prin stabilirea unor standarde etice, un astfel de cadru promovează încrederea utilizatorilor care este strâns legată de succesul pe termen lung al Metaversului.

Componentele de bază ale unui cadru de guvernanță a datelor oferă o abordare structurată pentru gestionarea și supravegherea activelor de date ale unei organizații. Aceste componente conlucrează pentru garantarea preciziei, securității și utilizării eficiente a datelor, asigurând, în același timp, alinierea acestora cu obiectivele organizaționale și cerințele de conformitate.

Deși pilonii ce susțin cadrul de guvernanță a datelor în Metavers stabilesc fundația tehnică și de reglementare, componentele abordează provocările etice, sociale și de securitate într-un mod holistic, adaptat contextului complex al Metaversului. Fiecare dintre aceste componente joacă un rol important în crearea unui mediu de încredere, în care utilizatorii se simt în siguranță să interacționeze și să participe.

Principalele componente ale unui cadru de guvernanță a datelor în Metavers sunt prezentate în figura 7.2.

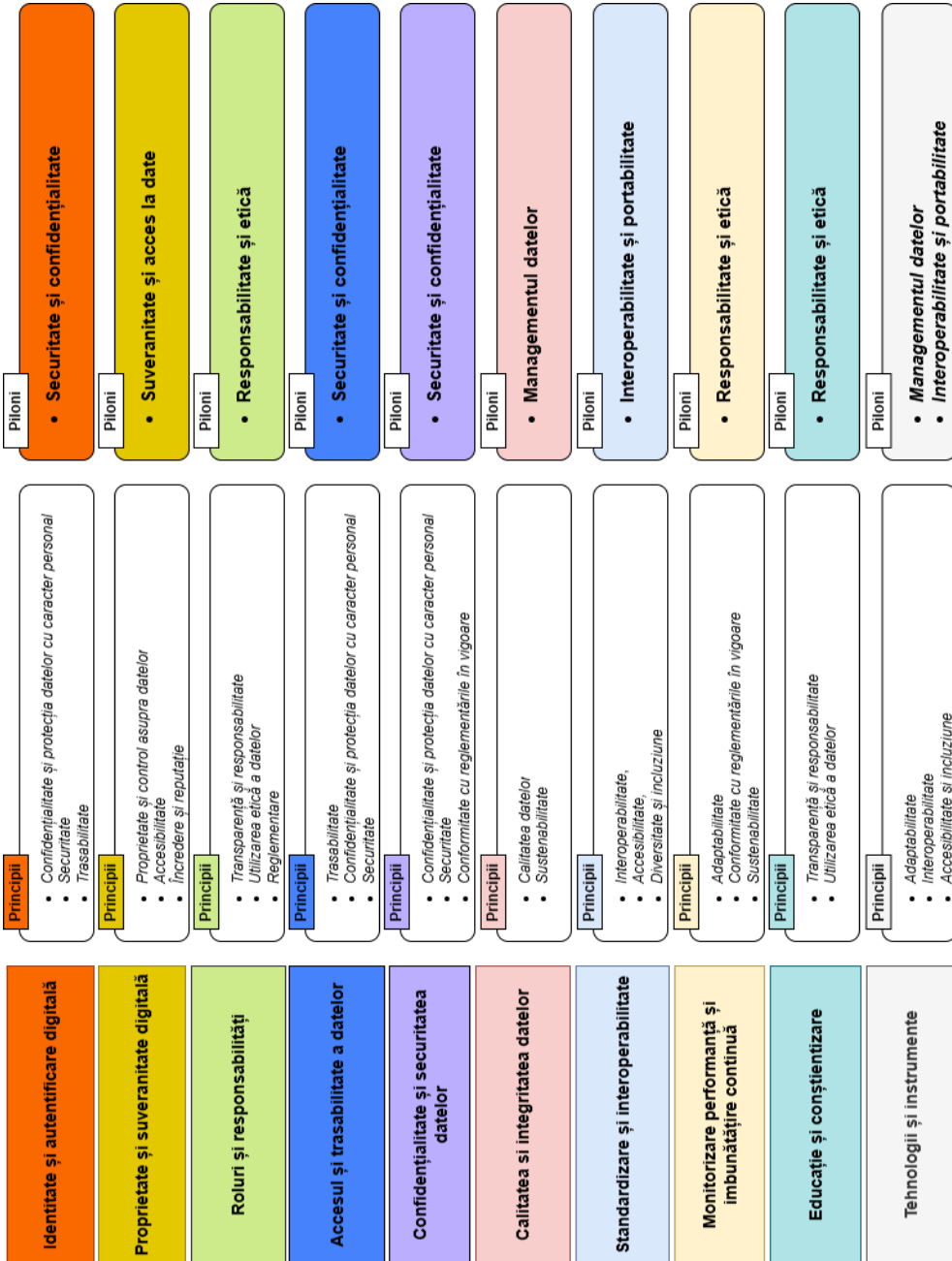


Figura 7.2. Principalele componente ale unui cadru de guvernare a datelor în Metavers

Identitate și autentificare digitală

Descriere: componenta de „Identitate și autentificare digitală” sprijină gestionarea identităților virtuale ale utilizatorilor în Metavers, asigurând autentificarea securizată și conectarea între diversele platforme și lumi virtuale. Această componentă vizează nu doar siguranța datelor de identitate, ci și o experiență de utilizare fluidă, protejând identitățile de accesul neautorizat și utilizarea abuzivă. Permite utilizatorilor să acceseze diverse medii Metavers prin utilizarea unei identități unice, controlată în mod descentralizat, fără a compromite siguranța datelor personale. Astfel, tranzițiile între platforme devin mult mai fluide prin eliminarea obligativității de a crea conturi separate, ceea ce reduce și riscul asociat cu gestionarea mai multor parole și date de acces. Astfel, utilizatorii își pot menține controlul asupra propriilor date de identificare, chiar și atunci când navighează prin diverse aplicații sau lumi virtuale în cadrul Metavers.

Include: componenta care integrează elemente cheie ce permit gestionarea eficientă și sigură a identităților utilizatorilor.

- *Portofele de identitate digitală (wallets):* acționează ca hub-uri unificate de identificare ce oferă utilizatorilor o identitate consistentă și interoperabilă pe toate platformele din Metavers. Aceste portofele conțin informații de identificare, accesibile doar de către utilizator, cum ar fi certificările de autentificare, acreditările și alte date personale necesare pentru accesul în spațiul virtual.
- *Autentificarea bazată pe blockchain sau alte tehnologii descentralizate* utilizează o rețea distribuită pentru criptarea și stocarea datelor de identitate în registre securizate. Această metodă conferă utilizatorilor un control sporit asupra propriilor date de identitate, împiedicând accesul neautorizat și modificările neautorizate. În plus, utilizatorii își pot revoca sau ajusta autorizațiile în mod direct, ceea ce le oferă o autonomie mai mare în gestionarea datelor personale.
- *Protocol de interoperabilitate a identității:* definește standarde și mecanisme prin care diverse platforme și aplicații pot recunoaște și valida identitatea digitală a utilizatorilor în mod constant și sigur. Aceste protocoale permit utilizatorilor să acceseze multiple aplicații și lumi virtuale, păstrând o identitate unică și securizată, fără a fi nevoie să se autentifice de fiecare dată.
- *Identitate descentralizată (DID):* DID permite ca datele de identitate să fie stocate pe blockchain, fără a fi gestionate de o singură entitate. Astfel, utilizatorii păstrează controlul asupra datelor lor, reducând riscul de compromitere.

Piloni: Securitate și confidențialitate.

Principii: Confidențialitate și protecția datelor cu caracter personal; Securitate; Trasabilitate.

Proprietate și suveranitate digitală

Descriere: această componentă contribuie la creșterea gradului de conștientizare asupra controlului și drepturilor utilizatorilor asupra datelor și activelor lor digitale, fără riscul unor constrângeri din partea unor intermediari centralizați. Într-un ecosistem descentralizat, această componentă permite utilizatorilor să-și gestioneze și să-și protejeze proprietatea asupra datelor și bunurilor virtuale, fie că este vorba de informații personale, achiziții digitale sau conținut creat în Metavers. Proprietatea și suveranitatea digitală oferă utilizatorilor controlul exclusiv de a decide cum, când și cu cine își partajează datele, facilitând un cadru bazat pe transparență, autonomie și încredere în spațiile virtuale.

Rol: componenta ”proprietate și suveranitate digitală” promovează o utilizare etică și transparentă a datelor, garantând că numai proprietarii de drept au capacitatea de a transfera, modifica sau utiliza aceste date. În plus, această componentă sprijină dezvoltarea unui sistem de încredere în care identitățile, resursele și activitățile virtuale sunt protejate de manipulări și abuzuri, respectând principiile suveranității datelor. De asemenea, acest rol contribuie la consolidarea unei economii digitale sustenabile, în care utilizatorii sunt recompensați în mod corect pentru contribuțiile și investițiile lor în lumea virtuală.

Include:

- *Drepturi de acces și control al datelor:* Reprezintă capacitatea utilizatorilor de a controla cine și în ce condiții poate accesa datele personale ale utilizatorilor. Practic, utilizatorii ar trebui să aibă dreptul să stabilească permisiunile de acces, să revoce accesul la datele lor atunci când doresc și să aibă vizibilitate asupra modului în care datele lor sunt utilizate de platforme sau de alte terțe părți.
- *Management al consimțământului:* Presupune obținerea consimțământului explicit de la utilizatori înainte ca datele lor să fie colectate, stocate, sau partajate. Consimțământul trebuie să fie informat, oferind utilizatorilor detalii clare despre scopul colectării datelor și despre cum vor fi folosite sau partajate. Acest proces oferă utilizatorilor controlul asupra modului în care informațiile lor sunt gestionate, permițându-le să fie mai conștienți și să decidă pe baza unei înțelegeri complete a implicațiilor.
- *Protecția proprietății digitale:* Utilizatorii au dreptul să își păstreze controlul asupra bunurilor digitale create și deținute, să stabilească

cine le poate utiliza și să primească compensații în cazul în care aceste bunuri sunt valorificate de alte părți. Tehnologiile blockchain sunt adesea folosite pentru a sprijini această protecție, asigurând un registru transparent și imuabil al proprietăților digitale și al tranzacțiilor.

Piloni: Suveranitate și acces la date.

Principii: Proprietate și control asupra datelor, Accesibilitate, Încredere și reputație.

Roluri și Responsabilități

Descriere: stabilește structura organizațională și rolurile-cheie în gestionarea datelor și activelor în Metavers. Aceasta include atribuirea responsabilităților în guvernanța datelor, asigurând că toți actorii implicați au o înțelegere clară a rolurilor lor și a măsurilor necesare pentru protecția datelor.

Rol: oferă o claritate operațională cu scopul de a evita conflictele de responsabilitate, asigurând în același timp conformitatea și securitatea datelor. Oferă o distribuție eficientă a rolurilor și a responsabilităților, permite gestionarea transparentă și eficientă a datelor, încurajează responsabilitatea fiecărui actor pentru protecția și utilizarea etică a datelor.

Include:

- *Structuri de guvernanță:* acestea sunt structurile organizatorice și de decizie care coordonează și supraveghează guvernanța datelor. În Metavers, structurile de guvernanță trebuie să includă nu doar lideri și echipe interne de guvernanță a datelor, ci și colaborări cu părțile interesate externe (de exemplu, alți actori din ecosistemul digital) pentru a menține standardele de siguranță, transparență și echitate în interacțiunile și tranzacțiile care au loc.
- *Proceduri de conformitate:* sunt seturi de reguli și mecanisme de verificare menite să asigure respectarea reglementărilor și politicilor stabilite pentru protecția datelor și a drepturilor utilizatorilor. În contextul Metavers, conformitatea cu reglementările nu înseamnă doar respectarea normelor de protecție a datelor (cum ar fi GDPR sau CCPA), ci și adaptarea la cerințele unui mediu digital descentralizat. Aceste proceduri presupun monitorizare constantă, raportarea și implementarea unor măsuri corective pentru a remedia rapid orice abateri de la standardele de conformitate.
- *Responsabilități în gestionarea și monitorizarea datelor:* se referă la sarcinile și obligațiile atribuite diferitelor părți care gestionează și monitorizează datele în Metavers. Aceasta include asigurarea securității

și confidențialității datelor utilizatorilor, auditul și evaluarea regulată a conformității, precum și intervențiile rapide în caz de breșe de securitate sau încălcări ale reglementărilor.

Piloni: Responsabilitate și etică.

Principii: Transparență și responsabilitate, Utilizarea etică a datelor, Reglementare

Accesul și trasabilitatea datelor

Descriere: presupune monitorizarea detaliată a activităților asupra datelor pentru a detecta orice abateri sau încercări de acces neautorizat, precum și gestionarea permisiunilor de acces.

Rol: permite gestionarea accesului și monitorizarea utilizării datelor, garantând că doar utilizatorii autorizați pot accesa informațiile și că activitățile efectuate asupra datelor pot fi urmărite în mod transparent. În Metavers, unde datele sunt distribuite între multiple platforme, trasabilitatea asigură vizibilitate și responsabilitate.

Include:

- *Mecanisme de audit:* implică procese de revizuire periodică și de evaluare a conformității cu politicile de securitate și guvernanța a datelor. Aceste mecanisme verifică dacă regulile și procedurile de utilizare și protecție a datelor sunt respectate în toate platformele din Metavers.
- *Jurnale de acces:* sunt înregistrări detaliate ale tuturor accesărilor și modificărilor făcute asupra datelor, oferind un istoric complet al acțiunilor utilizatorilor. Aceste jurnale conțin informații despre cine a accesat datele, când, de unde, și ce tip de operațiuni au fost realizate. Aceste jurnale au rolul de a permite operatorilor de platformă să monitorizeze activitățile și să identifice orice încercare de acces neautorizat sau abuz.
- *Politici de control al accesului:* stabilesc reguli clare despre cine poate accesa și utiliza datele și în ce scop. Aceste politici definesc niveluri de acces distincte, protejând astfel informațiile sensibile și reducând riscul accesului neautorizat.
- *Monitorizarea în timp real a utilizării datelor:* presupune supravegherea continuă a activităților de utilizare a datelor pentru a detecta și a răspunde imediat la orice activitate suspectă sau neregulă. Aceasta poate include identificarea accesărilor neobișnuite, a fluxurilor neautorizate de date și a acțiunilor neconforme cu politicile de securitate.

Piloni: Managementul datelor.

Principii: Trasabilitate, Securitate, Confidențialitate și protecția datelor.

Confidențialitatea și securitatea datelor

Descriere: protejează datele utilizatorilor de accesul neautorizat și menține confidențialitatea acestora conform reglementărilor și normelor de securitate.

Rol: contribuie la prevenirea scurgerilor de date și protejează informațiile sensibile de accesul neautorizat.

Include: criptare, firewall-uri, politici de confidențialitate, evaluări periodice de securitate.

Piloni: Securitate și confidențialitate.

Principii: Confidențialitate și protecția datelor cu caracter personal, Securitate, Conformitate cu reglementările.

Calitatea și integritatea datelor

Descriere: această componentă se concentrează pe protejarea informațiilor personale prin mecanisme de criptare, autentificare multi-factor și tehnologii de securitate avansate, precum blockchain. Proceduri stricte de securitate, împreună cu politici de confidențialitate, oferă un control clar asupra cine și în ce scop poate accesa datele personale.

Rol: protejează datele sensibile ale utilizatorilor, asigurând confidențialitatea și integritatea acestora. Un grad înalt de securitate poate preveni accesul neautorizat, breșele de securitate și pierderea de date, menținând încrederea utilizatorilor în platforme.

Include: Validarea datelor, proceduri de curățare și corectare a datelor, procese de verificare a integrității.

Piloni: Managementul datelor

Principii: Calitatea datelor, Sustenabilitate.

Standardizare și interoperabilitate

Descriere: asigură implementarea unor standarde comune și a unor protocoale interoperabile care permit platformelor să funcționeze eficient împreună în Metavers. Standardizarea asigură un limbaj comun între diverse platforme și dispozitive, facilitând astfel integrarea, portabilitatea și accesul facil al utilizatorilor în toate spațiile Metaversului.

Rol: permite realizarea unui ecosistem coerent, care permite utilizatorilor să migreze între diferite lumi virtuale fără obstacole tehnice. Creează o experiență uniformă și accesibilă pentru utilizatori, reducând fragmentarea tehnologică și sprijinind inovația, contribuind la dezvoltarea unui Metavers integrat și colaborativ.

Include:

- API-uri: permit conectarea diverselor platforme, servicii și experiențe digitale, facilitând astfel integrarea datelor și interacțiunea între ecosisteme diferite.

- Formate de date standardizate: convențiile comune privind structura și prezentarea datelor, permițând compatibilitatea între sisteme și platforme. Acestea asigură că datele pot fi înțelese și utilizate în mod corespunzător, indiferent de tehnologia sau platforma pe care sunt transferate. Permit ca elementele precum avatarurile, obiectele virtuale și achizițiile digitale să fie utilizabile între diverse platforme.
- Protocoale de interoperabilitate: permit utilizatorilor să-și transfere identitatea, activele și istoricul între lumi virtuale diferite. De exemplu, protocoalele pot permite unui avatar creat pe o platformă să fie utilizat și recunoscut pe altă platformă, păstrând toate caracteristicile și datele aferente. Un alt exemplu ar fi portabilitatea bunurilor digitale (NFT-uri) între marketplace-uri și spații virtuale diferite.

Piloni: Interoperabilitate și portabilitate.

Principii: Interoperabilitate, Accesibilitate, Diversitate și incluziune.

Monitorizarea performanței și îmbunătățirea continuă

Descriere: evaluează și monitorizează constant performanța guvernanței datelor pentru a implementa îmbunătățiri continue. Oferă mecanisme prin care performanța datelor și sistemelor din Metavers este măsurată și evaluată continuu. Aceasta permite detectarea și remedierea rapidă a oricăror breșe de securitate sau erori de sistem, precum și îmbunătățirea constantă a proceselor.

Rol: asigură adaptarea la noi cerințe și menținerea unui standard ridicat în gestionarea datelor.

Include:

- Indicatori de performanță (KPI-uri): sunt măsuri cantitative și calitative ce pot măsura, de exemplu, nivelul de satisfacție al utilizatorilor, timpul de încărcare a obiectelor 3D, stabilitatea conexiunilor între lumi virtuale, sau chiar conformitatea cu reglementările de protecție a datelor.
- Rapoarte periodice: joacă un rol important în informarea echipelor interne, a partenerilor și a utilizatorilor cu privire la funcționarea platformelor, dar și în luarea de decizii strategice. În Metavers, acestea permit urmărirea tendințelor de utilizare, impactul schimbărilor de design, dar și pentru a demonstra conformitatea cu reglementările de guvernanță a datelor.
- Mecanisme de audit: asigură conformitatea și transparența, protejând astfel utilizatorii și menținând încrederea acestora. Ele oferă o bază pentru a aborda deficiențele identificate și a optimiza procesele de guvernanță a datelor, asigurând o funcționare eficientă și securizată a platformei Metavers.

Piloni: Responsabilitate și etică.

Principii: Adaptabilitate, Conformitate cu reglementările, Sustenabilitate.

Educație și conștientizare digitală

Descriere: în Metavers, unde utilizatorii interacționează constant cu noi tehnologii și unde datele personale sunt intens utilizate, educația și conștientizarea pot preveni comportamentele riscante. Această componentă poate include sesiuni de instruire, resurse educative și campanii de conștientizare privind riscurile de securitate și drepturile utilizatorilor asupra datelor lor. Educarea utilizatorilor contribuie semnificativ la reducerea expunerii la atacuri și la crearea unui mediu de utilizare sigur și etic.

Rol: instruirea utilizatorilor și a administratorilor de platforme privind practicile de securitate și guvernanță a datelor. Aceasta contribuie la crearea unei culturi a responsabilității și la prevenirea riscurilor printr-o mai bună înțelegere a regulilor de utilizare a datelor.

Include: Programe de instruire, resurse de informare, ghiduri de bune practici.

Piloni: Responsabilitate și etică

Principii: Utilizarea etică a datelor, Transparență și responsabilitate.

Tehnologii și instrumente

Descriere: această componentă acționează ca un motor al guvernanței eficiente, oferind soluții automate și integrative pentru a asigura aplicarea regulilor, respectarea drepturilor utilizatorilor și îmbunătățirea calității interacțiunilor digitale.

Rol: această componentă se referă la utilizarea de tehnologii și instrumente avansate pentru a sprijini și a eficientiza implementarea strategiilor de guvernanță a datelor. Rolul său este de a oferi suport tehnologic pentru a asigura conformitatea și performanța sistemelor de guvernanță.

Include:

- Tehnologii blockchain: Permite autentificarea descentralizată, gestionarea suveranității digitale și securitatea datelor, garantând încredere și trasabilitate.
- Tehnologii XR (VR, AR, MR): Facilitează interacțiunea imersivă și realistă în Metavers, oferind experiențe augmentate și virtuale de înaltă calitate.
- Instrumente de analiză a datelor: Software și platforme pentru colectarea, procesarea și interpretarea datelor în timp real, optimizând deciziile și experiențele utilizatorilor.

- Inteligență Artificială (AI) și Machine Learning (ML): Permite personalizarea experiențelor utilizatorilor, detectarea anomaliilor în comportamentul datelor și optimizarea proceselor de gestionare a datelor.
- Tehnologii de interoperabilitate și standardizare: API-uri, formate de date standardizate și protocoale de interoperabilitate care facilitează transferul și partajarea datelor între platformele din Metavers.
- Mecanisme de protecție și autentificare (ex. 2FA, biometrie): Asigură acces securizat și protecția identităților utilizatorilor împotriva accesului neautorizat.

Piloni: Managementul datelor, Interoperabilitate și portabilitate.

Principii: Adaptabilitate, Interoperabilitate, Accesibilitate și incluziune.

În această secțiune au fost prezentate cititorilor principalele provocări și oportunități asociate guvernanței datelor în Metavers, având ca punct de plecare reglementările internaționale și implicațiile acestora asupra utilizatorilor și entităților economice care operează în acest spațiu digital emergent. Studiul subliniază că, în ciuda existenței unor reglementări robuste precum Regulamentul General privind Protecția Datelor (GDPR) al Uniunii Europene, Data Governance Act, EU AI Act și alte cadre legislative aplicabile în multiple jurisdicții, natura descentralizată și transnațională a Metaversului generează un vid normativ cu posibile consecințe negative asupra celor implicați. Din acest motiv, implementarea eficientă a unui cadru de guvernanță a datelor în Metavers este adesea obstrucționată de fragmentarea reglementărilor la nivel global. În timp ce Uniunea Europeană promovează un model bazat pe transparență, protecția datelor și drepturile utilizatorilor, alte jurisdicții, precum Statele Unite și China, adoptă abordări diferite, mai orientate fie spre inovație tehnologică liberă, fie spre suveranitate digitală strict reglementată. Această divergență în abordare face dificilă aplicabilitatea unor norme unitare, ridicând probleme legate de portabilitatea datelor, interoperabilitatea și suveranitatea digitală.

Pe lângă disparitățile legislative, conceptul de proprietate și control asupra datelor personale în Metavers rămâne insuficient clarificat. Într-un spațiu virtual descentralizat, unde blockchain-ul și contractele inteligente joacă un rol din ce în ce mai important, se impune o reevaluare a conceptelor tradiționale de suveranitate a datelor și drepturi digitale. Abordările curente din cadrul GDPR privind dreptul de a fi uitat, dreptul la portabilitatea datelor sau consimțământul informat se dovedesc greu de aplicat într-un mediu bazat pe identități digitale persistente, proprietate descentralizată a activelor digitale și interacțiuni inter-platformă.

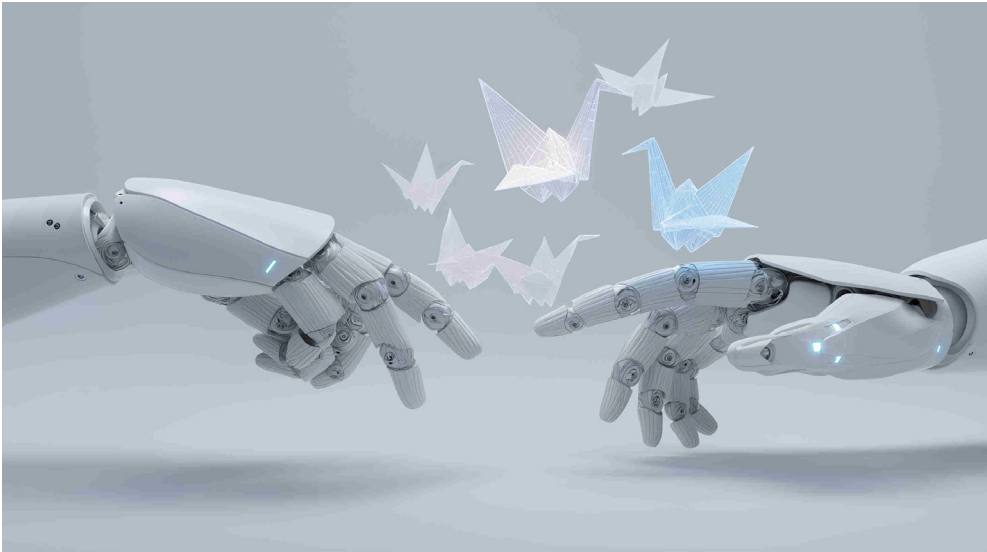
Pe măsură ce Metaversul devine tot mai interconectat cu economia globală, cu industriile emergente și cu societatea digitală, apare necesitatea unei armonizări internaționale a standardelor de guvernanță a datelor. Inițiativele OECD, ITU și

AI Governance Frameworks propun crearea unor standarde transnaționale pentru protecția datelor și utilizarea etică a tehnologiilor emergente, însă aplicabilitatea acestora depinde de nivelul de cooperare dintre actorii statali și non-statali. Un alt aspect critic identificat în această analiză este nevoia de adaptabilitate a reglementărilor la dinamica tehnologică. Spre deosebire de industriile tradiționale, unde legislația poate fi aplicată pe termen lung, Metaversul și ecosistemele sale conexe evoluează rapid, necesitând un cadru normativ flexibil, bazat pe reglementare algoritmică, mecanisme de conformitate automate și inteligență artificială explicabilă (XAI - Explainable AI). În acest context, contractele inteligente, blockchain-ul reglementat și self-sovereign identity (SSI) ar putea reprezenta pilonii unei noi arhitecturi de guvernanță digitală.

Pe lângă provocările juridice, studiul evidențiază impactul etic al Metaversului asupra confidențialității, securității datelor și drepturilor fundamentale ale utilizatorilor. Utilizarea extinsă a biometriei comportamentale, recunoașterii faciale și interacțiunilor bazate pe realitate augmentată și inteligență artificială ridică întrebări esențiale privind bias-ul algoritmic, discriminarea digitală și vulnerabilitățile cibernetice. În acest sens, necesitatea unor mecanisme solide de audit AI, coduri etice clare și supraveghere democratică a platformelor virtuale devine tot mai evidentă.

În concluzie, putem spune că guvernanța datelor în Metavers reprezintă atât o provocare legislativă, cât și o oportunitate pentru inovare normativă. În absența unui cadru juridic unificat, interoperabil și flexibil, Metaversul riscă să devină un spațiu al incertitudinii legale, unde utilizatorii sunt expuși riscurilor privind securitatea datelor, supravegherea digitală și discriminarea algoritmică. Totodată, analiza scoate în evidență nevoia unei abordări proactive și colaborative, în care reglementările internaționale, standardele tehnologice și principiile etice să fie integrate într-o strategie coerentă de guvernanță digitală. Astfel, pentru a construi un Metavers sigur, echitabil și sustenabil, viitoarele cercetări ar trebui să se concentreze asupra dezvoltării unui cadru global de reglementare a datelor, bazat pe standarde deschise și interoperabile, unde inteligența artificială poate fi utilizată pentru reglementare și conformitate automată în ecosistemele digitale descentralizate. O altă direcție viitoare de cercetare trebuie să țină cont de impactul social și economic al datelor în Metavers, inclusiv asupra incluziunii digitale și echității algoritmice, dar și de explorarea modelelor de proprietate și control asupra datelor în rețelele descentralizate.

Partea IV.
Perspective finale



8. Arhitectura încrederii într-un viitor imersiv

În paginile pe care le-am elaborat la începutul acestei cărți, am pornit de la o întrebare fundamentală și pragmatică: *dincolo de entuziasmul tehnologic, ar putea fi Metaversul o soluție reală pentru provocările tot mai presante cu care se confruntă societatea modernă?*

Astfel, am navigat prin complexitatea urbanizării accelerate, a imperativului de a atinge neutralitatea climatică și a nevoii de a gestiona resurse finite, argumentând că lumile virtuale imersive nu reprezintă o evadare din realitate, ci un instrument extraordinar pentru a o înțelege, modela și îmbunătăți.

Am încercat să arătăm cum conceptul de geamă digital al unui oraș, alimentat cu date în timp real de la senzori IoT și imagini satelitare, poate deveni un laborator virtual pentru planificatori și administratori publici. În acest spațiu lipsit de riscuri fizice, putem simula impactul unor noi infrastructuri de transport, putem optimiza consumul energetic al clădirilor și putem testa strategii de management al crizelor, de la inundații la valuri de căldură.

Am explorat, de asemenea, potențialul inovator al agriculturii urbane, arătând cum tehnologiile de realitate extinsă pot facilita proiectarea și gestionarea fermelor verticale sau a grădinilor pe acoperiș, contribuind la securitatea alimentară și la crearea unor ecosisteme urbane mai reziliente și sustenabile.

Însă, pe parcursul acestei explorări a posibilităților, un adevăr fundamental a devenit incontestabil: întregul edificiu al Metaversului ca soluție pentru orașe inteligente este construit pe o fundație invizibilă, dar esențială – datele.

Fără date de calitate, securizate și interoperabile, gemenii digitali rămân simple modele 3D statice, iar simulările devin exerciții de imaginație lipsite de acuratețe. Aici, viziunea pragmatică pe care am conturat-o se intersectează inevitabil cu tema centrală a întregii cărți: guvernanta datelor.

Din perspectiva noastră, guvernanta datelor nu este un concept birocratic sau o constrângere legală, ci o cerință funcțională absolută. Este mecanismul care asigură încrederea cetățenilor în a participa la aceste noi platforme civice. Este setul de standarde care garantează că datele despre trafic pot comunica fluent cu cele despre calitatea aerului pentru a crea politici publice coerente. Este scutul de securitate care protejează infrastructura critică a unui oraș inteligent de atacuri cibernetice cu consecințe devastatoare.

Cartea, în ansamblul ei, a aprofundat această necesitate, transformând-o dintr-o condiție implicită într-un cadru de acțiune explicit. Capitolele ulterioare au disecat complexitatea modelelor de guvernanta existente, și, mai important, au propus o arhitectură de guvernanta adaptată specificului Metaversului.

Principiile și pilonii detaliați în capitolul 7 – de la securitate și confidențialitate, la descentralizare, suveranitate și interoperabilitate – reprezintă planul tehnic și etic necesar pentru a transforma viziunile din primul capitol în realitate. Acestea oferă răspunsuri la întrebări critice privind proprietatea datelor, consimțământul și utilizarea etică, fără de care proiectele de anvergură în orașe inteligente nu pot fi implementate în mod responsabil.

Problema fundamentală constă în faptul că guvernanța tradițională a datelor este inadecvată pentru Metavers. Caracteristicile unice ale Metaversului—cum ar fi fuziunea în timp real a lumii fizice cu cea virtuală, descentralizarea, volumele masive de date eterogene (inclusiv biometrice) și interacțiunile multi-platformă—crează un „vid normativ” și provocări complexe de securitate, etică și reglementare.

Aplicarea unor reguli unitare este dificilă din cauza abordărilor legislative diferite la nivel global (de exemplu, modelul UE bazat pe drepturi vs. modelele din SUA sau China, mai orientate spre inovație sau control statal). Concepte din reglementări actuale, precum GDPR, sunt greu de aplicat direct într-un mediu descentralizat bazat pe blockchain.

Astfel, cea mai importantă contribuție a lucrării este propunerea unui cadru de guvernanță a datelor holistic și structurat pe mai multe niveluri, special conceput pentru Metavers.

În acest sens, am sintetizat complexitatea Metaversului în cinci domenii strategice sau „piloni” care trebuie să susțină orice strategie de guvernanță a datelor. Aceștia sunt:

- *Securitate și confidențialitate:* Protejarea datelor și identităților împotriva fraudelor și accesului neautorizat.
- *Managementul datelor:* Gestionarea întregului ciclu de viață al datelor, de la creare la ștergere, asigurându-le calitatea și integritatea.
- *Descentralizare și suveranitate:* Promovarea controlului distribuit și a proprietății utilizatorului asupra datelor, utilizând tehnologii precum blockchain.
- *Interoperabilitate și portabilitate:* Asigurarea că utilizatorii își pot muta activele și identitatea între diferite platforme fără a fi blocați într-un singur ecosistem.
- *Conformitate și etică:* Alinierea cu reglementările legale și respectarea unor principii etice pentru a preveni discriminarea, manipularea și alte daune.

Pentru a face pilonii aplicabili în practică, aceștia au fost descompuși în 10 componente operaționale, fiecare cu un rol și funcții clare:

1. *Identitate și autentificare digitală*: Această componentă gestionează identitățile virtuale ale utilizatorilor, asigurând o autentificare sigură și unitară pe diverse platforme. Scopul este de a permite utilizatorilor să folosească o singură identitate controlată de ei, eliminând necesitatea conturilor separate și reducând riscurile de securitate. Include elemente precum portofele de identitate digitală și autentificare bazată pe blockchain.
2. *Proprietate și suveranitate digitală*: Componenta se concentrează pe garantarea drepturilor și controlului utilizatorilor asupra datelor și activelor lor digitale. Permite utilizatorilor să decidă cum, când și cu cine își partajează informațiile, promovând autonomia și încrederea într-un mediu descentralizat. Include managementul consimțământului și mecanisme pentru protecția proprietății digitale, cum ar fi NFT-urile.
3. *Roluri și responsabilități*: Stabilește o structură organizațională clară, atribuind responsabilități specifice pentru gestionarea și protecția datelor. Scopul este de a asigura claritate operațională și responsabilitate, astfel încât toți actorii implicați să înțeleagă rolurile lor în menținerea securității și conformității.
4. *Accesul și trasabilitatea datelor*: Asigură monitorizarea detaliată a tuturor activităților legate de date și gestionează permisiunile de acces. Rolul său este de a garanta că doar utilizatorii autorizați pot accesa informații și că orice acțiune poate fi urmărită în mod transparent pentru a detecta abuzuri. Include mecanisme de audit, jurnale de acces și politici de control.
5. *Confidențialitatea și securitatea datelor*: Această componentă se axează pe protejarea datelor sensibile ale utilizatorilor împotriva accesului neautorizat și a scurgerilor de informații. Include măsuri tehnice precum criptarea, firewall-urile, politici clare de confidențialitate și evaluări periodice de securitate.
6. *Calitatea și integritatea datelor*: Asigură că datele din Metavers sunt exacte, complete, corecte și de încredere. Calitatea slabă a datelor poate duce la experiențe eronate și la neîncredere din partea utilizatorilor. Componenta include procese de validare, curățare și verificare a integrității datelor.
7. *Standardizare și interoperabilitate*: Implementează standarde și protocoale comune care permit diferitelor platforme din Metavers să comunice și să funcționeze eficient împreună. Scopul este de a crea un ecosistem digital coerent și deschis, unde utilizatorii își pot transfera identitatea și activele între lumi virtuale fără obstacole tehnice.
8. *Monitorizare performanță și îmbunătățire continuă*: Evaluează constant eficiența cadrului de guvernare pentru a implementa îmbunătățiri. Prin indicatori de performanță (KPI-uri), rapoarte și audituri, această componentă asigură adaptarea la noi provocări și menținerea unui standard ridicat în gestionarea datelor.

9. *Educație și conștientizare digitală*: Se referă la instruirea utilizatorilor și a administratorilor privind practicile de securitate, riscurile și drepturile lor asupra datelor. O mai bună înțelegere contribuie la crearea unei culturi a responsabilității și la prevenirea comportamentelor riscante.
10. *Tehnologii și instrumente*: Reprezintă motorul tehnologic care sprijină și eficientizează implementarea guvernanței. Include utilizarea de tehnologii avansate precum blockchain pentru trasabilitate, inteligență artificială (AI) pentru detectarea anomaliilor, XR (VR, AR, MR) pentru interacțiune și API-uri pentru interoperabilitate.

Contribuția esențială nu este doar listarea acestor elemente, ci integrarea lor într-un cadru coerent și ierarhic, în care fiecare componentă este legată de unul sau mai mulți piloni și este susținută de principii de guvernanță specifice (ex. transparență, adaptabilitate, securitate).

Acest model conectează conceptele abstracte (principii) cu cele strategice (piloni) și cele practice (componente), oferind o foaie de parcurs completă pentru organizațiile care activează în Metavers.

În final, concluzia noastră, este una de optimism temperat de pragmatism. Potențialul Metaversului de a ne ajuta să construim orașe mai eficiente, mai verzi și mai echitabile este imens. Avem la dispoziție tehnologii capabile să ne ofere o înțelegere fără precedent a sistemelor urbane complexe. Însă, pentru a valorifica acest potențial, trebuie să construim cu aceeași rigoare și inovație și cadrul de reguli care guvernează datele. Așa cum am argumentat, guvernanța datelor este puntea dintre inovație și rezultate concrete. Această carte nu oferă doar o privire asupra destinației – orașul inteligent și sustenabil – ci, mai ales, trasează harta drumului, un drum pavat cu o guvernanță a datelor solidă, transparentă și demnă de încrederea publică.

Atunci când am analizat utilizarea Metaversului în administrația publică, am mutat focalizarea de la infrastructura tehnică a orașelor la infrastructura socială și civică a guvernării. Am argumentat că introducerea Metaversului în sfera publică reprezintă mai mult decât o simplă actualizare tehnologică; ea promite să reconfigureze fundamental însăși natura relației dintre stat și cetățean.

Am propus distincția conceptuală esențială între e-guvernarea tranzacțională, bazată pe formulare online, și o viitoare meta-guvernanță, un model experiențial, spațial și imersiv, bazat pe co-creare.

Am explorat potențialul extraordinar al acestei noi paradigme: primării virtuale care sporesc accesibilitatea serviciilor pentru persoanele cu mobilitate redusă sau din zone izolate; procese de bugetare participativă în care cetățenii pot „păși” într-un model 3D al cartierului lor pentru a vizualiza și dezbate impactul proiectelor propuse; sesiuni de formare imersive pentru funcționari publici și echipe de intervenție în situații de urgență, care pot exersa scenarii complexe într-

un mediu sigur. Acestea nu sunt doar optimizări, ci transformări care pot duce la o democratizare sporită și la o implicare civică mai profundă. În același timp, analiza noastră, fundamentată pe studiile de caz ale unor pionieri precum Seul și Dubai, dar mai ales pe cercetarea calitativă pe care am realizat-o printr-un focus grup cu experți din administrația publică din România, a scos la iveală o realitate mult mai nuanțată și plină de provocări.

Pe de o parte, am văzut cum strategiile naționale pot varia fundamental, de la modelul Seul, axat pe servicii pentru cetățeni, la cel din Dubai, orientat spre crearea unui hub economic. Această dihotomie demonstrează că nu există o singură cale de urmat, ci decizii strategice profunde care trebuie luate.

Pe de altă parte, și poate cel mai important, focus grupul a relevat preocupările legitime și scepticismul celor care se află în prima linie a serviciului public. Experții au ridicat semne de întrebare critice privind securitatea datelor, protejarea categoriilor vulnerabile, riscurile de manipulare și dezinformare și, nu în ultimul rând, aplicabilitatea cadrului legal actual, precum GDPR, într-un mediu atât de complex.

O voce a surprins perfect sentimentul general: „*Prima dată să discutăm măcar despre o strategie de data governance și mai vedem apoi*”.

Această afirmație surprinde esența cercetării noastre. Cartea de față, în integralitatea sa, este exact răspunsul la această cerință. În timp ce am identificat dilemele și am articulat întrebările din perspectiva practicianului din administrația publică, capitolele următoare au construit, pas cu pas, răspunsurile. Analiza detaliată a cadrelor de reglementare, precum EU Data Act și AI Act, și propunerea unui model de guvernare pentru Metavers cu piloni clari privind responsabilitatea, etica și conformitatea, oferă exact acea strategie pe care experții o consideră un punct de plecare obligatoriu.

Prin urmare, concluzia noastră este că tranziția către meta-guvernare este un proces cu un potențial imens, dar și cu riscuri pe măsură. Nu putem permite ca tehnologia să dicteze ritmul și condițiile acestei transformări. Trebuie să fie un proces deliberat, incluziv și guvernat de principii clare, co-create prin dialog între factorii de decizie, experți tehnici și societatea civilă. Așa cum interacțiunile din focus grup au arătat, încrederea este capitalul cel mai de preț în relația dintre administrație și cetățeni, iar această încredere poate fi erodată iremediabil de o implementare pripită sau neglijență a noilor tehnologii.

Această carte nu este doar un manifest tehnologic, ci ne amintește că, înainte de a construi primăria virtuale spectaculoase, trebuie să construim fundația solidă a încrederii, iar această fundație, așa cum exprimă întreaga lucrare, este o guvernare a datelor etică și pusă în slujba cetățeanului.

Bibliografie

Abraham R., Schneider J. & Vom Brocke J. (2019) Data governance: A conceptual framework, structured review, and research agenda. *International Journal of Information Management*. 49, 424-438.

Akour I. A. et al. (2022) A conceptual framework for determining metaverse adoption in higher institutions of gulf area: An empirical study using hybrid SEM-ANN approach. *Computers and Education: Artificial Intelligence*. 3, 100052.

Andrei D.-M. (2022) Excess Mortality Associated with the Covid-19 Pandemic in Romania. *Ovidius University Annals, Economic Sciences Series*. 0(1), 2-11.

Aspen Institute (2024), *Metaverse Potential for Romania*, rap. teh.

Baker A. (2018), 'I Knew We Were in Trouble.' *What It's Like to Live Through Cape Town's Massive Water Crisis*, Disponibil la: <https://time.com/cape-town-south-africa-water-crisis/> [Accesat: 19 Aug. 2025].

Ball M. (2022), *The metaverse: and how it will revolutionize everything*, Liveright Publishing.

Baloup J. et al. (2021), *White Paper on the Data Governance Act*.

Barcelona Energia (2025), *Strategy for energy transition | Urban Planning, Ecological Transition, Urban Services and Housing*, Disponibil la: <https://ajuntament.barcelona.cat/ecologiaurbana/en/what-we-do-and-why/energy-and-climate-change/strategy-energy-transition> [Accesat: 19 Aug. 2025].

Barnes A. (2023), *Metaverse in Gaming: Revolution in Gaming industry With Next-Generation Experience*, Disponibil la: <https://www.datasciencecentral.com/metaverse-in-gaming-revolution-in-gaming-industry-with-next-generation-experience/> [Accesat: 19 Aug. 2025].

Berndtsson M. et al. (2018), Becoming a data-driven organisation, în *European Conference on Information System (ECIS)*.

Bian Y., Leng J. & Zhao J. L. (2022), Demystifying Metaverse as a New Paradigm of Enterprise Digitization, în *Big Data – BigData 2021*, ed. de J. Wei & L.-J. Zhang, vol. 12988, Series Title: Lecture Notes in Computer Science, Cham: Springer International Publishing, 109-119.

Bibri S. E., Allam Z. & Krogstie J. (2022) The Metaverse as a virtual form of data-driven smart urbanism: platformization and its underlying processes, institutional dimensions, and disruptive impacts. *Computational Urban Science*. 2(1), 24.

Bosworth A., Clegg N. et al. (2021) Building the metaverse responsibly. *Meta*. 27.

Bourbonnais Cecile A. F. (2020), *Time of Use Rates: An International Perspective*, Disponibil la: <https://energyregulationquarterly.ca/articles/time-of-use-rates-an-international-perspectives> [Accesat: 19 Aug. 2025].

Brecht M. (2025), *How 15-Minute City Paris Became the Role Model for Urban Transformation* | *MOTION Magazine* | *Electric Mobility Lifestyle*, Disponibil la: <https://www.motion-mag.com/articles/how-15-minute-city-paris-became-the-role-model-for-urban-transformation> [Accesat: 19 Aug. 2025].

Brooklyn Grange (2024), *Brooklyn Grange* | *Green Roof System & Eco-Friendly Landscaping In Brooklyn*, Disponibil la: <https://www.brooklyngrangefarm.com> [Accesat: 19 Aug. 2025].

Brouwers S. J. (2016), *Balancing Data Security and Accessibility in Higher Education*, Capstone report, University of Oregon, Disponibil la: <https://scholarsbank.uoregon.edu/xmlui/bitstream/handle/1794/21962/Brouwers2016.pdf?sequence=1&isAllowed=y>

Bughin J. et al. (2018), *Notes from the AI frontier: modeling the impact of AI on the world economy*, rap. teh., McKinsey Global Institute, Disponibil la: <https://www.mckinsey.com/~/media/McKinsey/Featured%20Insights/Artificial%20Intelligence/Notes%20from%20the%20frontier%20Modeling%20the%20impact%20of%20AI%20on%20the%20world%20economy/MGI-Notes-from-the-AI-frontier-Modeling-the-impact-of-AI-on-the-world-economy-September-2018.ashx>

BusinessWire (2021), *Big-Data-and-AI-Executive-Survey*, Disponibil la: <https://www.businesswire.com/news/home/20210104005022/en/NewVantage-Partners-Releases-2021-Big-Data-and-AI-Executive-Survey> [Accesat: 24 Iul. 2024].

BusinessWire (2022), *New Survey from Privitar and Bloor Research Reveals a Majority of Data Leaders Unable to Use More than 40% of Their Data Due to Security and Privacy Concerns*. Disponibil la: <https://www.businesswire.com/news/home/20221206006030/en/New-Survey-from-Privitar-and-Bloor-Research-Reveals-a-Majority-of-Data-Leaders-Unable-to-Use-More-than-40-of-Their-Data-Due-to-Security-and-Privacy-Concerns> [Accesat: 23 Iul. 2024].

C40 Cities (2025), *C40 Cities - A global network of mayors taking urgent climate action*, Disponibil la: <https://www.c40.org/> [Accesat: 19 Aug. 2025].

C40 Cities Climate Leadership Group (2025), *C40 Knowledge Hub*, Disponibil la: https://www.c40knowledgehub.org/s/?language=en_US [Accesat: 19 Aug. 2025].

Carretero A. G. et al. (2017) MAMD 2.0: Environment for data quality processes implantation based on ISO 8000-6X and ISO/IEC 33000. *Computer Standards & Interfaces*. 54, 139-151.

Casalegno F. (2024), *The EU AI Act — A Complete Guide to Laws and Regulations on AI*, Disponibil la: <https://medium.com/@francesco.casalegno/the-eu-ai-act-a-complete-guide-to-laws-and-regulations-on-ai-61f630fcc1be> [Accesat: 19 Aug. 2025].

Cavoukian A. (2012), *Privacy Protection Measures and Technologies in Business Organizations: Aspects and Standards*, IGI Global.

Chainalysis (2022), *Chainalysis State Of Web3 report for 2022*, rap. teh., Disponibil la: https://www.linkedin.com/redir/redirect?url=https%3A%2F%2Fgo%2Echainalysis%2Ecom%2Frs%2F503-FAP-074%2Fimages%2Fstate-of-web3%2Epdf&urlhash=lgw_&trk=article-ssr-frontend-pulse_little-text-block

- Chen Z. et al. (2023), *Open Metaverse: Issues, Evolution, and Future*.
- Cheng R. et al. (2022) Will Metaverse Be NextG Internet? Vision, Hype, and Reality. *IEEE Network*. 36(5), 197-204.
- Cheng X. et al. (2022) Exploring the metaverse in the digital economy: an overview and research framework. *Journal of Electronic Business & Digital Economics*. 1(1/2), 206-224.
- Cheremnykh P. (2024) Gaming the Metaverse: user experience analysis and insights from Fortnite.
- Chidera Victoria Ibeh et al. (2024) Business analytics and decision science: A review of techniques in strategic business decision making. *World Journal of Advanced Research and Reviews*. 21(2), 1761-1769.
- Choi H.-s. & Kim S.-h. (2017) A content service deployment plan for metaverse museum exhibitions—Centering on the combination of beacons and HMDs. *International Journal of Information Management*. 37(1), 1519-1527.
- Cigniti (2024), *4 Key Pillars of Data Governance Framework and Management Strategies*, Disponibil la: <https://www.cigniti.com/blog/four-pillars-information-assets-management-data-insights/> [Accesat: 20 Aug. 2024].
- City of Vancouver (2012), *Greenest City 2020 Action Plan - the City's Sustainability Plan*, Disponibil la: <https://vancouver.ca/files/cov/greenest-city-action-plan.pdf> [Accesat: 19 Aug. 2025].
- Clement J. (2022), *Metaverse, Statista*, Disponibil la: <https://www.statista.com/topics/8652/%20525%20Metaverse/>
- Collins C. (2008) Looking to the Future: Higher Education in the Metaverse. *Educational Review*. 43, 50-52.
- Commission E. (2020), *A European strategy for data, Brussels*, Disponibil la: <https://digital-strategy.ec.europa.eu/en/policies/strategy-data> [Accesat: 22 Iul. 2024].
- Council E. (2021), *Cloud Data Management Capabilities (CDMC) Framework*, Disponibil la: <https://edmcouncil.org/frameworks/cdmc/> [Accesat: 30 Oct. 2024].
- CQL (2018), *12 Reasons Why Data Is Important*, Disponibil la: <https://www.c-q-l.org/resources/guides/12-reasons-why-data-is-important/> [Accesat: 24 Iul. 2024].
- Cyber Risk GmbH (2024), *Data Governance Act (DGA) | Updates, Compliance, Training*, Disponibil la: <https://www.european-data-governance-act.com/> [Accesat: 19 Aug. 2025].
- Dama International (2017), *DAMA-DMBOK: Data Management Body of Knowledge: 2nd Edition Second Edition*, Technics Publications.

Data Administration Management Association (2010), *The DAMA guide to the data management body of knowledge: DAMA-DMBOK guide*, ed. de M. Mosley et al., First edition, Bradley Beach, NJ: Technics Publications, LLC. Data Governance Institute (2020), *Defining Data Governance*, Disponibil la: <https://datagovernance.com/defining-data-governance/> [Accesat: 9 Aug. 2025].

Data Governance Institute (2024), *DGI Data Governance Framework*, Disponibil la: <https://datagovernance.com/the-dgi-data-governance-framework/> [Accesat: 14 Aug. 2024].

DataGalaxy (2023), *8 pillars of a successful data governance framework*, Disponibil la: <https://www.datagalaxy.com/en/blog/8-pillars-of-data-governance-frameworks/> [Accesat: 20 Aug. 2024].

Davenport T. H. & Harris J. G. (2007), *Competing on analytics: the new science of winning*, OCLC: ocm74649067, Boston, Mass: Harvard Business School Press.

DBHIDS (2018), *Data governance framework strategic plan*, Disponibil la: <https://dbhids.org/wp-content/uploads/2019/02/DBHIDS-DG-Framework-Strategic-Plan-v2.03.pdf> [Accesat: 10 Aug. 2024].

Deloitte (2018), *The Analytics Advantage*, Disponibil la: <https://www2.deloitte.com/ro/ro/pages/deloitte-analytics/articles/the-analytics-advantage.html> [Accesat: 24 Iul. 2024].

Deloitte (2022), *Data Governance - Deloitte Point of View (PoV)*, Disponibil la: <https://www.serverdirect.nl/assets/pdfs/deloitte-uk-data-governance-point-of-view.pdf> [Accesat: 30 Oct. 2024].

Detroit Future City (2024), *Detroit Future City: Think Tank, Policy Advocate, Innovation Engine*, Disponibil la: <https://detroitfuturecity.com/> [Accesat: 19 Aug. 2025].

DG CONNECT (2024), *Data Governance Act explained | Shaping Europe's digital future*, Disponibil la: <https://digital-strategy.ec.europa.eu/en/policies/data-governance-act-explained> [Accesat: 18 Iul. 2024].

Dionisio J. D. N., Iii W. G. B. & Gilbert R. (2013) 3D Virtual worlds and the metaverse: Current status and future possibilities. *ACM Computing Surveys*. 45(3), 1-38.

Domnisoru S., Ogarca R. & Dragomir I. (2017) Interacțiuni între cultura organizațională și controlul intern. *Audit Financiar*. 15(148), 628.

Dong-hwan K. (2023), *Seoul gov't launches world's 1st public services platform in metaverse - The Korea Times*, Disponibil la: <https://www.koreatimes.co.kr/business/tech-science/20230117/seoul-govt-launches-worlds-1st-public-services-platform-in-metaverse> [Accesat: 19 Aug. 2025].

Dwivedi Y. K. et al. (2022) Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. *International Journal of Information Management*. 66, 102542.

Eckerson W. (2010), *Performance Dashboards: Measuring, Monitoring, and Managing Your Business*, 2nd edition, Wiley.

EDM Council (2022), *DCAM: Data Management Capability Assessment Model 2.2*, Disponibil la: <https://edmcouncil.org/frameworks/dcam/> [Accesat: 30 Oct. 2024].

EIMInstitute (2024), *Data Governance Maturity – An Overview*, Disponibil la: <https://www.eiminstitute.org/resource-portals/data-governance-stewardship/data-governance-maturity-an-overview/> [Accesat: 7 Aug. 2024].

Environment Bureau (2015), *Energy Saving Plan for Hong Kong Built Environment*, Disponibil la: <https://www.eeb.gov.hk/sites/default/files/pdf/EnergySavingPlanEn.pdf> [Accesat: 19 Aug. 2025].

European Bank for Reconstruction and Development (2024), *Incentives to use public and active transport: Freiburg, Germany – EBRD*, Disponibil la: <https://www.ebrdgreencities.com/policy-tool/incentives-to-use-public-and-active-transport-freiburg-germany-2/> [Accesat: 19 Aug. 2025].

European Commission (2022a), *Digital Economy and Society Index (DESI) 2022*, rap. teh., European Commission, Disponibil la: <https://digital-strategy.ec.europa.eu/en/library/digital-economy-and-society-index-desi-2022>

European Commission (2022b), *Open Data Maturity Report 2022*, rap. teh., Publications Office of the European Union, Disponibil la: <https://data.europa.eu/en/publications/open-data-maturity>

Far S. B. et al. (2022) A Review of Non-fungible Tokens Applications in the Real-world and Metaverse. *Procedia Computer Science*. 214, 755-762.

Farm.One (2025), *Indoor Farm*, Disponibil la: <https://www.farm.one/> [Accesat: 19 Aug. 2025].

Fernandez C. B. & Hui P. (2022), Life, the Metaverse and Everything: An Overview of Privacy, Ethics, and Governance in Metaverse, in *2022 IEEE 42nd International Conference on Distributed Computing Systems Workshops (ICDCSW)*, Bologna, Italy: IEEE, 272-277.

Forbes (2022), *The Age Of Analytics And The Importance Of Data Quality*, Disponibil la: <https://www.forbes.com/sites/forbesagencycouncil/2019/10/01/the-age-of-analytics-and-the-importance-of-data-quality/#7e16ab8d5c3c> [Accesat: 22 Iul. 2024].

Freeson O. (2023), *Understanding the Pillars of Data Governance: A Comprehensive Overview*, Disponibil la: <https://www.linkedin.com/pulse/understanding-pillars-data-governance-comprehensive-o-pmp-csm->

Gadekallu T. R. et al. (2023) Blockchain for the metaverse: A review. *Future Generation Computer Systems*. 143, 401-419.

Gartner (2021), *12 Actions to Improve Your Data Quality*, Disponibil la: <https://www.gartner.com/smarterwithgartner/how-to-improve-your-data-quality> [Accesat: 24 Apr. 2025].

Goetz M. (2015), *Data Governance and Data Management Are Not Interchangeable*, Disponibil la: https://www.forrester.com/blogs/15-09-11-data_governance_and_data_management_are_not_interchangeable/ [Accesat: 5 Aug. 2024].

Green City Times (2017), *What are Transit Options in Vancouver?*, Disponibil la: <https://www.greencitytimes.com/vancouver-alternative-transit/> [Accesat: 19 Aug. 2025].

Güven İ. & Ballı O. (2024), Empowering Metaverse through artificial intelligence, în.

Halborn (2022), *Explained: The Ronin Hack (March 2022)*, Disponibil la: <https://www.halborn.com/blog/post/explained-the-ronin-hack-march-2022>

Hallett S., Hoagland L. & Toner E. (2016), Urban Agriculture: Environmental, Economic, and Social Perspectives, în *Horticultural Reviews*, ed. de J. Janick, Hoboken, NJ, USA: John Wiley & Sons, Inc., 65-120.

Hamburg Invest (2025), *Transport and mobility in Hamburg | Hamburg Business*, Disponibil la: <https://hamburg-business.com/en/future-hamburg/mobility-traffic/> [Accesat: 19 Aug. 2025].

Hansson F. (2024) Linked geodata: CityGML represented as a virtual knowledge graph. *Student thesis series INES*.

Henke N. et al. (2016), *The age of analytics: Competing in a data-driven world*, Disponibil la: <https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-age-of-analytics-competing-in-a-data-driven-world>

Huang Y., Li Y. J. & Cai Z. (2023) Security and Privacy in Metaverse: A Comprehensive Survey. *Big Data Mining and Analytics*. 6(2), 234-247.

Huggett J. (2020) Virtually Real or Really Virtual: Towards a Heritage Metaverse. *Studies in Digital Heritage*. 4(1), 1-15.

Hughes I. (2012) Virtual worlds, augmented reality, blended reality. *Computer Networks*. 56(18), 3879-3885.

Hussain A. (2023), *Court case held in the metaverse*, Disponibil la: <https://www.legalcheek.com/2023/02/court-case-held-in-the-metaverse/> [Accesat: 19 Aug. 2025].

Hutagalung S. S. & Sulistio E. B. (2024) Transforming Public Service Delivery in Indonesia: Exploring the Potential and Challenges of the Metaverse. *Jurnal Borneo Administrator*. 20(3), 273-288.

IBM (2022), *Data breach costs reach a record high*, Disponibil la: <https://www.ibm.com/reports/data-breach-action-guide>.

IEEE SA (2024), *The IEEE Global Initiative 2.0 on Ethics of Autonomous and Intelligent Systems*, Disponibil la: <https://standards.ieee.org/industry-connections/activities/ieee-global-initiative/> [Accesat: 19 Aug. 2025].

IIBA (2022), *The Critical Role of Data*, Disponibil la: <https://www.iiba.org/business-analysis-blogs/the-critical-role-of-data/> [Accesat: 22 Iul. 2024].

International Settlements B. for (2022), *The design of a data governance system*, Disponibil la: <https://www.bis.org/publ/bppdf/bispap124.htm> [Accesat: 4 Aug. 2024].

Intersoft Consulting (2024), *Art. 5 GDPR – Principles relating to processing of personal data*, Disponibil la: <https://gdpr-info.eu/art-5-gdpr/> [Accesat: 1 Oct. 2024].

IPCC (2018), *Global Warming of 1.5 °C*, Disponibil la: <https://www.ipcc.ch/sr15/> [Accesat: 19 Aug. 2025].

ISACA (2023), *Capability Maturity Model Integration (CMMI) Model*, Disponibil la: <https://www.isaca.org/enterprise/cmmi-performance-solutions> [Accesat: 30 Oct. 2024].

ISO & International Electrotechnical Commission (2017), *ISO/IEC 38505-1:2017 Information technology — Governance of IT — Governance of data — Part 1: Application of ISO/IEC 38500 to the governance of data*, Disponibil la: <https://www.iso.org/standard/56639.html>

ITU (2025a), *About ITU*, Disponibil la: <https://www.itu.int:443/en/about/Pages/default.aspx> [Accesat: 19 Aug. 2025].

ITU (2025b), *AI-powered virtual worlds and Metaverse*, Disponibil la: <https://www.itu.int/metaverse/> [Accesat: 19 Aug. 2025].

ITU (2025c), *FG-MV Outcomes – Metaverse*, Disponibil la: <https://www.itu.int/metaverse/fg-mv-outcomes/> [Accesat: 19 Aug. 2025].

Janssen M. et al. (2020) Data governance: Organizing data for trustworthy Artificial Intelligence. *Government Information Quarterly*. 37(3), 101493.

Jaynes C. et al. (2003), The Metaverse: a networked collection of inexpensive, self-configuring, immersive environments, in *Proceedings of the workshop on Virtual environments 2003*, Zurich Switzerland: ACM, 115-124.

Jhan A. S. (2024), *Unexplored Use Cases of Blockchain in Education*, Disponibil la: <https://medium.com/@arslanshahjhan214/unexplored-use-cases-of-blockchain-in-education-c5c002cd6e60> [Accesat: 19 Aug. 2025].

Jurcys P. (2022), *Prifina Comments to the Proposed EU Data Act: What Will Data Access, Interoperability, and Data...* Disponibil la: <https://medium.com/prifina/prifina-comments-to-the-proposed-eu-data-act-what-will-data-access-interoperability-and-data-5900e2bb4ed1> [Accesat: 19 Aug. 2025].

Justice U. S. D. of (1970), *Records, Computers, and the Rights of Citizens*, Disponibil la: <https://www.justice.gov/opcl/docs/rec-com-rights.pdf> [Accesat: 24 Iul. 2024].

Kalyvaki M. (2023) Navigating the Metaverse Business and Legal Challenges: Intellectual Property, Privacy, and Jurisdiction. *Journal of Metaverse*. 3(1), 87-92.

Kavipriya (2023), *Seoul unveils smart intersection testbed to enhance urban mobility – Telematics Wire*, Disponibil la: <https://telematicswire.net/seoul-unveils-smart-intersection-testbed-to-enhance-urban-mobility/> [Accesat: 19 Aug. 2025].

Kelly A. (2024), *Future Of Metaverse In Gaming Industry*, Section: Game Development, Disponibil la: <https://euphoriaxr.com/metaverse-in-gaming-i ndustry-the-future-of-gaming/> [Accesat: 19 Aug. 2025].

Kim J. (2021) Advertising in the Metaverse: Research Agenda. *Journal of In-teractive Advertising*. 21(3), 141-144.

Ko E. & Jang J. (2014), The Virtual Device Managing Module of the Metaverse Assisted Living Support System, in *Proceedings of the International Conference on Modeling, Simulation and Visualization Methods (MSV)*, The Steering Committee of The World Congress in Computer Science, 1.

Kostenko O. et al. (2022) Genesis of Legal Regulation Web and the Model of the Electronic Jurisdiction of the Metaverse. *Bratislava Law Review*. 6(2), 21-36.

Kshetri N., Dwivedi Y. K. & Janssen M. (2024) Metaverse for advancing government: Prospects, challenges and a research agenda. *Government Information Quarterly*. 41(2), 101931.

Kulkarni A. (2019), 28. *Payments in — Education Sector*, Disponibil la: <https://medium.com/authncapture/28-industry-education-3aee3b973342> [Accesat: 19 Aug. 2025].

Ladley J. (2020), *Data governance: how to design, deploy, and sustain an effective data governance program*, Second edition, London San Diego, CA Cambridge, MA Oxford: Academic Press.

Laeq K. (2022) Metaverse: why, how and what. *How and what*.

Lainhart J. W., Conboy M. & Saull R. (2019) COBIT 2019 Framework Introduction and methodology. Schaumburg. *ISACA*.

Lee L.-H. et al. (2021), *All One Needs to Know about Metaverse: A Complete Survey on Technological Singularity, Virtual Ecosystem, and Research Agenda*, arXiv:2110.05352 [cs], Disponibil la: <http://arxiv.org/abs/2110.05352> [Accesat: 28 Ian. 2025].

Li H., Yu L. & He W. (2019) The Impact of GDPR on Global Technology Development. *Journal of Global Information Technology Management*. 22(1), 1-6.

Lnenicka M. et al. (2024) Government in the metaverse: Requirements and suitability for providing digital public services. *Technological Forecasting and Social Change*. 203, 123346.

Madhani P. M. (2010) Resource Based View (RBV) of Competitive Advantage: An Overview. *Resource based view: concepts and practices.*, 3-22.

Marcucci S. et al. (2023), *Mapping and Comparing Data Governance Frameworks: A benchmarking exercise to inform global data governance deliberations*, arXiv:2302.13731 [cs], Disponibil la: <http://arxiv.org/abs/2302.13731> [Accesat: 2 Sept. 2024].

Marr B. (2019), *How Can Small Businesses Use Big Data?*, Disponibil la: <https://bernardmarr.com/how-can-small-businesses-use-big-data-here-are-6-practical-examples/> [Accesat: 22 Iul. 2024].

McKinsey (2020), *Designing data governance that delivers value*, Disponibil la: <https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/designing-data-governance-that-delivers-value> [Accesat: 23 Iul. 2024].

McKinsey & Company (2018), *Analytics comes of age*, [Accesat: 30 Oct. 2024]. McKinsey Global Institute (2020), *Data Strategy Session*, Disponibil la: <https://www.dataideology.com/data/data-driven-organizations-are-23-times-more-likely-to-acquire-customers-six-times-as-likely-to-retain-customers-and-19-times-as-likely-to-be-profitable-as-a-result/> [Accesat: 24 Iul. 2024].

MDM Institute (2015), *What is Data Governance?*. Disponibil la: <http://www.tcdii.com/whatsDataGovernance.html> [Accesat: 5 Aug. 2024].

Medium (2023), *The Importance of Data Strategy in Today's Business Landscape*, Disponibil la: <https://medium.com/@data.pilot/the-importance-of-data-strategy-in-todays-business-landscape-deb4140365bb> [Accesat: 22 Iul. 2024].

Metaverse Standards Forum (2025), *About the Metaverse Standards Forum*, Disponibil la: <https://metaverse-standards.org/>

Michael Greenwood (2024), *Digital Wallets Market Report: Growth, Trends 2024-2029*, Disponibil la: <https://www.juniperresearch.com/research/fintech-payments/core-payments/digital-wallet-research-report/> [Accesat: 19 Aug. 2025].

Minecraft (2020), *New Study: Understanding the Impact of Minecraft in the Math Classroom*, Disponibil la: <https://education.minecraft.net/en-us/blog/new-study-understanding-the-impact-of-minecraft-in-the-math-classroom> [Accesat: 19 Aug. 2025].

Modulos (2025), *A Guide to AI Governance*, Disponibil la: <https://www.modulos.ai/guide-to-ai-governance/> [Accesat: 19 Aug. 2025].

Morgado L. (2009) Interconnecting virtual worlds. *Journal For Virtual Worlds Research*. 1(3).

Murphy K. R. (2022), *Data, Methods and Theory in the Organizational Sciences: A New Synthesis*, 1-a ed., New York: Routledge.

Mystakidis S. (2022) Metaverse. *Encyclopedia Journal*. 1(2), 486-497.

Nam D. et al. (2019) Performance Comparison of 3D File Formats on a Mobile Web Browser. *International Journal of Internet, Broadcasting and Communication*. 11(2), 31-42.

Nascio (2008), *Data Governance – Managing Information As an Enterprise Asset Part 1*, Disponibil la: <https://www.nascio.org/Portals/0/Publications/Documents/NASCIO-DataGovernance-Part1.pdf> [Accesat: 5 Aug. 2024].

NayaOne (2024), *The EU AI Act and Its Impact on Businesses*, Disponibil la: <https://medium.com/@NayaOne/the-eu-ai-act-and-its-impact-on-businesses-f2d4eb2f66df> [Accesat: 19 Aug. 2025].

Nevelsteen K. J. L. (2018) Virtual World, Defined from a Technological Perspective, and Applied to Video Games, Mixed Reality and the Metaverse. *Computer Animation and Virtual Worlds*. 29(1), e1752.

Nguyen B.-H. T. et al. (2024) Are we ready for education in Metaverse? PLS-SEM analysis. *Edelweiss Applied Science and Technology*. 8(2), 73-83.

NIST (2020) NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management. *National Institute of Standards and Technology*.

Nitu A. (2024), *Metaversul : Provocări și Oportunități pentru Protecția și Aplicarea Drepturilor de Proprietate Intelectuală*, Disponibil la: <https://infocons.ro/metaversul-provocari-si-oportunitati-pentru-protectia-si-aplicarea-drepturilor-de-proprietate-intelectuala/> [Accesat: 19 Aug. 2025].

OCDE (2022), *OECD Economic Surveys: Romania 2022*, rap. teh., OECD Publishing, Disponibil la: https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/01/oecd-economic-surveys-romania-2022_2b8e8be0/e2174606-en.pdf [Accesat: 9 Mar. 2025].

OCDE (2024), *AI, Data Governance and Privacy: Synergies and Areas of International Co-operation*, rap. teh. OECD Artificial Intelligence Papers, No. 222, OECD, Disponibil la: https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/06/ai-data-governance-and-privacy_2ac13a42/2476b1a4-en.pdf

Odunayo Josephine Akindote et al. (2023) A Review of Data-Driven Business Optimization Strategies in the U.S. Economy. *International Journal of Management & Entrepreneurship Research*. 5(12), 1124-1138.

OECD (2022), *Going Digital Guide to Data Governance Policy Making*, OECD. OECD (2025a), *The Organisation for Economic Cooperation and Development*, Disponibil la: <https://www.oecd.org/en.html> [Accesat: 19 Aug. 2025].

OECD (2025b), *AI Principles Overview*, Disponibil la: <https://oecd.ai/en/principles> [Accesat: 19 Aug. 2025].

Ooi B. C. et al. (2022), *The Metaverse Data Deluge: What Can We Do About It?*, Version Number: 2, Disponibil la: <https://arxiv.org/abs/2206.10326> [Accesat: 7 Aug. 2024].

Open Government Partnership (2021), *Romania Commitment RO0065: Open Data Portal*, Disponibil la: <https://www.opengovpartnership.org/members/romania/commitments/RO0065/>

Orsini F. et al. (2013) Urban agriculture in the developing world: a review.

Agronomy for Sustainable Development. 33(4), 695-720.

- Ortiz L. (2022) Risks of the Metaverse: A VRChat Study Case. *The Journal of Intelligence, Conflict, and Warfare*. 5(2), 53-128.
- Oslo City Council (2024), *Climate Budget 2024*, Disponibil la: <https://www.klimaoslo.no/wp-content/uploads/sites/2/2024/08/Climate-budget-2024.pdf> [Accesat: 19 Aug. 2025].
- Otto B. (2015) Quality and Value of the Data Resource in Large Enterprises. *Information Systems Management*. 32(3), 234-251.
- Owens D. et al. (2011) An empirical investigation of virtual world projects and metaverse technology capabilities. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems*. 42(1), 74-101.
- Papagiannidis S. & Bourlakis M. (2010) Staging the New Retail Drama: at a Metaverse near you! *Journal For Virtual Worlds Research*. 2(5).
- Park J. et al. (2023) Digital twins and land management in South Korea. *Land Use Policy*. 124, 106442.
- Park S.-M. & Kim Y.-G. (2022) A Metaverse: Taxonomy, Components, Applications, and Open Challenges. *IEEE Access*. 10, 4209-4251.
- Peuralinna J. (2024), „Data Lineage in the financial sector”, Teză de dizert., Aalto University, Disponibil la: <https://aaltodoc.aalto.fi/server/api/core/bitstreams/02d288f3-70a7-46a1-ac4b-6de62554b2d0/content> [Accesat: 10 Aug. 2024].
- Pew Research Center (2022), *The Metaverse in 2040*, Disponibil la: <https://www.pewresearch.org/internet/2022/06/30/the-metaverse-in-2040/> [Accesat: 28 Ian. 2025].
- Pino De Francesco MSc (2024), *EU Data Act: how it impacts Solution and Software Architecture?*, Disponibil la: <https://medium.com/law-and-software-architecture/eu-data-act-how-it-impacts-solution-and-software-architecture-125a210d4fd8> [Accesat: 19 Aug. 2025].
- Ponnusamy S. & Gupta P. (2023) Connecting the Dots: How Data Lineage Helps in Effective Data Governance. *International Journal of Computer Science and Engineering*. 10(10), 6-10.
- PricewaterhouseCoopers (2024), *Data and analytics*, Disponibil la: <https://www.pwc.com/gr/en/advisory/data-and-analytics.html> [Accesat: 30 Oct. 2024].
- Prisco G. (2009) A virtual world space agency. *Futures*. 41(8), 569-571.
- Proniewska K. et al. (2021) Immersive technologies as a solution for general data protection regulation in Europe and impact on the COVID-19 pandemic. *Cardiology Journal*. 28(1), 23-33.
- Queensland U. of (2024), *Data Governance Essentials Handbook*, Disponibil la: <https://data.uq.edu.au/files/6833/Data%20Governance%20Essentials%20handbook%20August%202021.pdf> [Accesat: 10 Aug. 2024].

Redman T. C. (2016), *Getting in front on data: who does what*, First edition, OCLC: 956481486, Basking Ridge, NJ: Technics Publications.

Reuters (2022) Blockchain project Ronin hit by \$615 million crypto heist. *Reuters*.

Rymaszewski M., ed. (2007), *Second life: the official guide*, San Francisco, Calif:Sybex.

Schenker J. L. (2022), *What Business Needs To Know About The EU Data Act*, Disponibil la: https://medium.com/@jennifer_45057/what-business-needs-to-know-about-the-eu-data-act-ad6d961830ad [Accesat: 19 Aug. 2025].

Schroeder R., Huxor A. & Smith A. (2001) Activeworlds: geography and social interaction in virtual reality. *Futures*. 33(7), 569-587.

SFA (2024), *Singapore Food Agency*, Disponibil la: <https://www.sfa.gov.sg/> [Accesat: 19 Aug. 2025].

Shahadat M. M. H. et al. (2023) Digital Technologies for Firms' Competitive Advantage and Improved Supply Chain Performance. *Journal of Risk and Financial Management*. 16(2), 94.

Sharma G. (2024) Balancing Privacy and Innovation: Assessing Data Protection Laws in the Modern Era. *Supremo Amicus*. 35.

Sim J. K. et al. (2024) Designing an Educational Metaverse: A Case Study of NTUUniverse. *Applied Sciences*. 14(6), 2559.

Singapore's National Water Agency (2024), *NEWater*, Disponibil la: <https://www.pub.gov.sg/Public/WaterLoop/OurWaterStory/NEWater> [Accesat: 19 Aug. 2025].

Sky Urban Solutions (2014), *Sky Greens*, Disponibil la: <https://www.skygreens.com/> [Accesat: 19 Aug. 2025].

Snowflake (2024), *AI Governance, Threat Intelligence and Anomaly Detection*, Disponibil la: <https://www.snowflake.com/content/snowflake-site/global/en/fundamentals/ai-governance-threat-intelligence-and-ml-anomaly-detection> [Accesat: 19 Aug. 2025].

Spalević Ž. & Vićentijević K. (2022) GDPR and challenges of personal data protection. *The European Journal of Applied Economics*. 19(1), 55-65.

Specht K. et al. (2014) Urban agriculture of the future: an overview of sustainability aspects of food production in and on buildings. *Agriculture and Human Values*. 31(1), 33-51.

Standardization I. O. for (2015) ISO/IEC 38500: 2015 Information Technology: Governance of IT for the Organization. *International Organization for Standardization*.

State of California (2024), *California Consumer Privacy Act (CCPA)*, [Accesat: 3 Aug. 2024].

Stedman C. (2024), *What is data governance and why does it matter?*, Disponibil la: <https://www.techtarget.com/searchdatamanagement/definition/data-governance> [Accesat: 7 Aug. 2024].

Stefanic D. (2025), *Unlocking the Power of Data in Metaverse Experiences*, Disponibil la: <https://hyperspace.mv/data-in-metaverse/> [Accesat: 19 Aug. 2025].

Sun J. et al. (2022), *Big Data Meets Metaverse: A Survey*, arXiv:2210.16282[cs], Disponibil la: <http://arxiv.org/abs/2210.16282> [Accesat: 7 Aug. 2024]. Svalna (2024), *Calculate your climate impact*, Disponibil la: <https://svalna.se/web/en> [Accesat: 19 Aug. 2025].

Tamer T. (2024), *Real Examples and Use Cases of Metaverse in Tourism*, Disponibil la: <https://capsulesight.com/metaverse/real-examples-and-use-cases-of-metaverse-in-tourism/> [Accesat: 18 Aug. 2025].

TDRA (2023), *Dubai Metaverse Strategy | The Official Portal of the UAE Government*, Disponibil la: <https://u.ac/en/about-the-uae/strategies-initiatives-and-awards/strategies-plans-and-visions/government-services-and-digital-transformation/dubai-metaverse-strategy> [Accesat: 19 Aug. 2025].

Technical and Environmental Administration, City of Copenhagen (2025), *The CPH 2025 Climate Plan | Urban Development*, Disponibil la: <https://urbandevlopmentcph.kk.dk/climate> [Accesat: 19 Aug. 2025].

Tehrani C. (2024), *How Data Management Frameworks Can Enhance Data Security*, Disponibil la: <https://concentric.ai/how-data-management-frameworks-can-enhance-data-security/> [Accesat: 10 Aug. 2024].

Tiliute D. (2020) Two Years of GDPR in Romania. *The USV Annals of Economics and Public Administration*. 20(1 (31)), 198-208.

Truyo (2024), *The Importance of Data: The Top Benefits of Collecting Customer Data*, Disponibil la: <https://truyo.com/blog/the-importance-of-data-the-top-benefits-of-collecting-customer-data/> [Accesat: 22 Iul. 2024].

Union E. (2018), *General Data Protection Regulation (GDPR)*, Disponibil la: <https://www.consilium.europa.eu/en/policies/data-protection/data-protection-regulation/> [Accesat: 30 Oct. 2024].

United Nations (2024), *Net Zero Coalition*, Publisher: United Nations, Disponibil la: <https://www.un.org/en/climatechange/net-zero-coalition> [Accesat: 19 Aug. 2025].

UrbanizeHub (2023), *Orașul Basel vrea ca locuințele să fie protejate de acoperișuri verzi*, Disponibil la: <https://urbanizehub.ro/orasul-basel-vrea-ca-locuintele-sa-fie-protejate-de-acoperisuri-verzi/> [Accesat: 19 Aug. 2025].

Veit D. et al. (2014) Business Models: An Information Systems Research Agenda. *Business & Information Systems Engineering*. 6(1), 45-53.

Vidal-Tomás D. (2022) The new crypto niche: NFTs, play-to-earn, and metaverse tokens. *Finance Research Letters*. 47, 102742.

VMZ Berlin (2025), *Traffic Planning and Consulting – VMZ Berlin*, Disponibil la: <https://www.vmzberlin.com/kompetenzbereiche/verkehrsplanung/> [Accesat: 19 Aug. 2025].

W3C (2022), *Decentralized Identifiers (DIDs) v1.0*, W3C Recommendation, W3C, Disponibil la: <https://www.w3.org/TR/did-core/>

W3C (2025), *Verifiable Credentials Data Model v2.0*, W3C Recommendation, W3C, Disponibil la: <https://www.w3.org/TR/vc-data-model-2.0/>

Weber K., Otto B. & Österle H. (2009) One Size Does Not Fit All—A Contingency Approach to Data Governance. *Journal of Data and Information Quality*. 1(1), 1-27.

Weingarden G. & Matthias Artzt (2022), *Metaverse and privacy | IAPP*, Disponibil la: <https://iapp.org/news/a/metaverse-and-privacy-2> [Accesat: 19 Aug. 2025].

Wende K. (2017), A Model for Data Governance – Organising Accountabilities for Data Quality Management, în *ACIS 2007 Proceedings*.

World Wide Web Foundation (2017), *Open Data Barometer – Global Report, 4th Edition*, rap. teh., World Wide Web Foundation, Disponibil la: <https://opendatabarometer.org/4thedition/>

Xynogalas V. & Leiser (Mark) M. R. (2024) The Metaverse: searching for compliance with the General Data Protection Regulation. *International Data Privacy Law*. 14(2), 89-105.

Yfantis V. & Ntalianis K. (2022), Exploring the potential adoption of metaverse in government, în *Data Intelligence and Cognitive Informatics: Proceedings of ICDICI 2022*, Springer, 815-824.

Yoon K. et al. (2015), *MPEG-V: Bridging the virtual and real world*, Academic Press.

Zackery A. et al. (2016) Toward a simulated replica of futures: Classification and possible trajectories of simulation in futures studies. *Futures*. 81, 40-53. Zamfir M. & Crăciun A.-C. (2023) Who is Threatening My Avatar in Metaverse? *Romanian Cyber Security Journal*. 5(2), 75-86.

Zamfir M.-C., Giura I.-E. & Crăciun A. C. (2024) Betting on Metaverse for a more modern and efficient public administration. *Romanian Journal of Information Technology and Automatic Control*. 34(3), 117-130.

Zhang B. et al. (2024) Managing Metaverse Data Tsunami: Actionable Insights. *IEEE Transactions on Knowledge and Data Engineering*., 1-20.

Despre autori



Alexandru STANCIU este cercetător științific II la ICI București în cadrul Departamentului de Securitate Cibernetică și Protecția Infrastructurilor Critice. Alexandru Stanciu a participat în diverse proiecte de cercetare, iar traiectoria sa profesională evidențiază o evoluție a intereselor sale de cercetare, reflectând dinamica domeniului IT&C. Inițial, activitatea sa a fost concentrată pe dezvoltarea și operarea infrastructurilor de calcul de mari dimensiuni, având un rol important în coordonarea implementării și operării infrastructurii naționale de calcul distribuit de tip Grid. Contribuțiile sale din această perioadă includ proiectarea și implementarea de platforme pentru calcul distribuit, dezvoltarea infrastructurii Grid ca suport pentru servicii de e-Science, crearea de medii pentru orchestrarea și planificarea serviciilor Grid, dezvoltarea de structuri de suport pentru Organizații Virtuale pe multiple infrastructuri Grid și implementarea de aplicații Grid pentru modelare, simulare și optimizare. Interesele sale curente se concentrează pe Inteligența Artificială și învățarea automată aplicată, cu precădere în domeniile vederii artificiale și procesării limbajului natural. Totodată, Alexandru are un interes activ în explorarea tehnologiilor imersive (XR) și a Metavers-ului, abordând atât potențialul lor aplicativ, cât și provocările inerente.



Carmen Elena CÎRNU este Director Științific și Vicepreședinte al Consiliului Științific al Institutului Național de Cercetare-Dezvoltare în Informatică – ICI București. Este Cercetător Științific gradul I, cu o prezență marcantă în domeniul securității cibernetice, al educației virtuale, al guvernancei digitale și al diplomației cibernetice. Are o vastă experiență în coordonarea proiectelor naționale și internaționale și a contribuit la definirea unor direcții strategice esențiale pentru transformarea digitală a instituțiilor publice și pentru consolidarea securității cibernetice în Europa Centrală și de Est. Absolventă a Facultății de Filosofie a Universității din București, unde și-a obținut doctoratul în 2011 cu o teză transdisciplinară, Carmen Cîrnu și-a construit

un profil profesional complex, care combină gândirea critică, etica digitală și inovația tehnologică. Este fondatoarea Centrului de Diplomatie Cibernetică și inițiatoarea primei reviste internaționale dedicate acestui domeniu emergent – International Journal of Cyber Diplomacy. De altfel, contribuția sa în domeniul diplomatiei cibernetice este recunoscută la nivel european, prin cursuri integrate în cadrul European Security and Defence College și prin implicarea directă în formarea de experți prin exerciții internaționale organizate de Uniunea Internațională a Telecomunicațiilor (ITU). Activitatea sa recentă reflectă o direcție clară spre integrarea tehnologiilor avansate în infrastructura digitală publică. A fondat ecosistemul ICI InnoLabs, ce cuprinde laboratoare multidisciplinare în inteligență artificială, blockchain, realitate virtuală și metavers, contribuind activ la modernizarea infrastructurii de cercetare din România. Este membru în structuri internaționale, fiind Vice-Chair al International Council for IT in Government Administration (ICA), reprezentantă a României în cadrul European Blockchain Partnership, membră în comitetul Ad-Hoc privind AI al Consiliului Europei, și colaboratoare apropiată a inițiativelor EuroDefense. De asemenea, este Fellow al Aspen Japan Institute și a fost cercetător invitat la Keio University din Japonia, în cadrul Global Security Research Institute. Este o promotoare activă a leadershipului feminin în tehnologie, fiind inclusă în lista Global 200 Women Power Leaders 2025, precum și în topurile „Top 100 Femei de Succes din România” și „Women Who Change Romania”. A fondat platforma ShesLeading, dedicată mentoratului și susținerii femeilor în știință și tehnologie, și coordonează activ inițiative Women4Cyber România.



Ionuț PETRE este cercetător științific gradul II și coordonator al Departamentului Transformare Digitală și Guvernanță din cadrul Institutului Național de Cercetare-Dezvoltare în Informatică – ICI București, unde activează de peste 20 de ani în domenii precum tehnologii emergente, infrastructuri digitale, orașe inteligente și guvernanța datelor. Absolvent al Facultății de Electronică, Telecomunicații și Tehnologia Informației din cadrul Universității Politehnica din București, și doctor în Management al Universității „Lucian Blaga” din Sibiu, a încercat să ofere în carieră și o perspectivă interdisciplinară asupra relației dintre tehnologie și politici

publice digitale. În activitatea sa de cercetare și coordonare, s-a implicat în numeroase proiecte naționale și internaționale, lucrând la dezvoltarea de sisteme distribuite intensive ca date, aplicații de Smart City, data analytics, aplicații ale inteligenței artificiale, tehnologii imersive, vizând un impact pozitiv pe care tehnologia îl poate avea asupra societății. Este coordonator al proiectului „Cercetări avansate în Metavers și tehnologii emergente pentru transformarea digitală a societății”, precum și coordonator al XR Innolab (xr.ici.ro) – laborator dedicat cercetării aplicate în realitate virtuală, augmentată și mixtă. În plan internațional, este preocupat activ de definirea standardelor și bunelor practici în domeniul Metaversului, fiind membru al ITU Focus Group on Metaverse (FG-MV), grup constituit sub egida Uniunii Internaționale a Telecomunicațiilor. În activitatea sa, a menținut o abordare echilibrată între inovație tehnologică, etică digitală și responsabilitate instituțională – teme care stau și la baza acestei cărți.



Ion Alexandru MARINESCU este cercetător științific gradul III (din 2015) al Departamentului Transformare și Guvernanță Digitală din cadrul Institutului Național de Cercetare-Dezvoltare în Informatică – ICI București. A absolvit Facultatea de Inginerie Mecanică și Mecatronică cu specializarea „Robotică și Automatizare“ la Universitatea Politehnica din București (2007), precum și cursurile de Master în Inginerie Mecanică din cadrul aceleiași universități la Facultatea de Inginerie Mecanică și Mecatronică (2009). În prezent, este interesat de cercetarea în domeniul tehnologiilor informației și comunicațiilor, cu un accent deosebit pe dezvoltarea și integrarea soluțiilor software inovatoare. Printre domeniile sale de interes se numără inteligența artificială, dezvoltarea de aplicații web și mobile, securitatea cibernetică și utilizarea tehnologiilor emergente în educație și sănătate. De asemenea, este implicat în studii privind Metaversul și impactul acestuia asupra transformării digitale a societății. În alte proiecte de cercetare, Alexandru a contribuit la dezvoltarea și implementarea unor soluții software pentru monitorizare, analiză și optimizare în diverse domenii, inclusiv sănătate, securitate cibernetică și infrastructură urbană inteligentă. În acest rol, el a fost implicat în proiectarea și realizarea unor platforme integrate, capabile să gestioneze volume mari de date

și să faciliteze interoperabilitatea între sisteme. De asemenea, a lucrat la asigurarea conformității cu standardele de securitate și protecția datelor, contribuind la dezvoltarea unor arhitecturi scalabile și eficiente pentru implementarea tehnologiilor emergente. Nu în ultimul rând, Alexandru a investigat utilizarea tehnologiilor emergente, precum Metaversul și inteligența artificială, în domeniul educației și al orașelor inteligente. Aceasta a implicat analiza potențialului acestor tehnologii pentru îmbunătățirea proceselor de învățare, dar și explorarea modurilor în care acestea pot facilita tranziția către orașe neutre climatic. Studiul său a contribuit la dezvoltarea unor modele conceptuale, deschizând noi perspective pentru integrarea tehnologiilor digitale în guvernanță, infrastructură urbană și transformarea digitală a societății.



Monica BARBU este cercetător științific gradul III și Șef al Serviciului „Reziliență, Interoperabilitate și Standardizare” din cadrul Institutului Național de Cercetare-Dezvoltare în Informatică – ICI București. A absolvit Facultatea de Administrație și Management Public din cadrul Academiei de Studii Economice din București și este deținătoarea a două diplome de master: în Managementul Informațiilor și Documentelor, obținută la Facultatea de Litere, Universitatea din București, respectiv în Relații Internaționale și Integrare Europeană, acordată de Școala Națională de Științe Politice și Administrative din București, Departamentul pentru Relații Internaționale. Titlul de doctor în Management i-a fost conferit de Facultatea de Studii Economice a Universității „Lucian Blaga” din Sibiu. Activitatea sa de cercetare se concentrează asupra unor direcții de actualitate și relevanță strategică, precum interoperabilitatea sistemelor informatice, serviciile publice electronice, guvernarea electronică (e-Guvernare), precum și învățarea asistată de tehnologie (e-Learning). În plus, manifestă un interes deosebit pentru Metavers și tehnologiile emergente asociate, fiind implicată în cadrul proiectului de cercetare „Cercetări avansate în Metavers și tehnologii emergente pentru transformarea digitală a societății”, ce vizează investigarea potențialului acestor tehnologii în contextul tranziției digitale.



Mădălina-Cornelia ZAMFIR este absolventă a Facultății de Automatică și Calculatoare din cadrul Universității Naționale de Știință și Tehnologie Politehnica din București și ocupă funcția de Cercetător Științific gradul III la Institutul Național de Cercetare-Dezvoltare în Informatică (ICI București). Subiectele sale de interes în activitatea de cercetare acoperă bazele de date relaționale și non relaționale, procesele de afaceri BPMN, Sistemele de Management al Conținutului Web WCMS, infrastructurile de tip Cloud, suportul IoT pentru soluțiile de tip Big Data, Big Data Analytics, Geospatial Analytics, Metavers și Mădălina a fost implicată în numeroase proiecte de cercetare și dezvoltare, naționale și internaționale, atât ca membru în echipa proiectului cât și ca responsabil de proiect, în cadrul cărora a contribuit la dezvoltarea de idei inovatoare. Activitatea sa științifică cuprinde publicații în reviste și conferințe de impact, numeroase perfecționări și participări la forumuri științifice majore și evenimente de diseminare, care au contribuit la consolidarea aptitudinilor necesare în zona de cercetare-dezvoltare.



Ionuț-Emanuel GIURA este în prezent Asistent Cercetător la Institutul Național de Cercetare-Dezvoltare în Informatică (ICI București), unde contribuie la dezvoltarea unor aplicații software folosind tehnologii de ultimă generație. De asemenea, a publicat articole științifice despre Metavers, explorând în profunzime această tehnologie inovatoare și contribuind la înțelegerea sa în cadrul comunității academice. Ionuț a absolvit Universitatea „Lucian Blaga” din Sibiu în 2021, obținând licența în Ingineria Calculatoarelor. Este un dezvoltator software pasionat, mereu dornic să învețe noi tehnologii pentru a-și îmbunătăți abilitățile și pentru a se menține la curent cu cele mai recente tendințe din industrie. În prezent, Ionuț își concentrează atenția asupra tehnologiei React pentru dezvoltarea front-end și explorează Node.js și Django pentru back-end. De asemenea, este familiarizat cu baze de date precum MySQL, PostgreSQL și MongoDB.



Cu o experiență de peste 25 de ani în domeniul academic și de cercetare, **dr. Ella Magdalena CIUPERCĂ** a dezvoltat o pasiune pentru explorarea intersecțiilor disciplinare, îmbinând interesele pentru domeniul social cu cel al securității și al tehnologiei informațiilor și comunicării. Pe parcursul activității sale de predare în învățământul superior și de cercetare în cadrul Academiei Naționale de Informații Mihai Viteazul și ulterior în Institutul Național de Cercetare și Dezvoltare în Informatică - ICI București, a fost interesată de subiecte inovatoare precum schimbarea socială, studiul minorităților active, influența socială, egalitatea de gen și incluziunea, erorile cognitive, infrastructurile critice și analiza datelor și metodologia cercetării științifice. A participat în diferite organisme de reglementare în învățământul superior (CNATDCU, ARACIS), a coordonat lucrări de licență, master și doctorat și a fost responsabilă pentru organizarea unor evenimente prestigioase precum conferințe științifice de specialitate (ICVL, CNIV, RCIC) sau workshopuri dedicate unor subiecte inovative (e.g. securitatea cibernetică în domeniul SCADA, Romanian Stanford Datathon for Women in Data Science, Realitatea virtuală în România). Experiența sa vastă în managementul educațional și de cercetare, împreună cu abilitățile dovedite de relaționare în echipă, i-au permis obținerea excelenței în inovare într-un mediu interdisciplinar în continuă schimbare.



Dragoș-Daniel IORDACHE este cercetător științific gradul II în cadrul departamentului „Sisteme și aplicații pentru societate” al Institutului Național de Cercetare-Dezvoltare în Informatică – ICI București. Cu un doctorat în Științele Educației obținut în 2012, parcursul său profesional reflectă o preocupare constantă pentru inovația în educație prin integrarea tehnologiilor emergente. Activitatea sa de cercetare s-a concentrat pe explorarea și dezvoltarea mediilor virtuale de învățare, realității augmentate (AR), realității virtuale (VR) și extinse (XR), precum și a aplicațiilor educaționale în Metaverse. Este implicat activ în proiecte naționale și internaționale care vizează testarea cu utilizatori și evaluarea euristică a platformelor interactive, cu un accent deosebit pe eficiența pedagogică și experiența utilizatorului în contexte educaționale digitale. Expertiza sa interdisciplinară se regăsește la intersecția dintre tehnologie, psihologie și științele educației, cu un interes special pentru modul în care realitatea virtuală și Metaversul pot transforma fundamental procesele de predare și învățare.



Guvernanța datelor se află la intersecția unor forțe puternice și adesea contradictorii, formând un _nexus_ complex care modelează societatea digitală. Acesta se articulează în jurul a trei axe fundamentale, fiecare prezentând propriile provocări și necesități de echilibru.

Pe de o parte, suveranitatea națională impune statelor dreptul de a-și reglementa și proteja datele cetățenilor și ale instituțiilor, considerându-le o resursă strategică.

Pe de altă parte, fluxul global de date este vital pentru economia digitală, iar companiile multinaționale și platformele online globale depind de capacitatea de a transfera date peste granițe, pentru a oferi servicii integrate și a rămâne competitive.

Și nu în ultimul rând, inovația tehnologică, motorul progresului în numeroase domenii precum Metaversul, care se bazează pe accesul la volume masive de date.

Fiecare nou set de date colectat și fiecare nouă tehnologie implementată creează noi vulnerabilități și riscuri de securitate, de la breșe de date la utilizarea abuzivă a informațiilor. Prin urmare, este esențial ca dezvoltarea tehnologică să fie însoțită de principii de "privacy by design" și de o cultură a securității cibernetice, asigurând că progresul nu se realizează cu prețul siguranței și intimității noastre.

ISBN 978-606-95858-2-5



9 786069 585825