

# Ramona Lacurezeanu

# Fațetele lumii digitale: tehnologii, dezinformare, etica IA

# Caiet de lucrări practice



# Presă Universitară Clujeană

Ramona Lacurezeanu

**FĂȚETELE LUMII DIGITALE:  
tehnologii, dezinformare, etica IA**

*Caiet de lucrări practice*

PRESA UNIVERSITARĂ CLUJEANĂ

2025

***Referenți științifici:***

**Prof. univ. dr. Adriana TIRON TUDOR**

**Lect. univ. dr. Cristian BOLOGA**

ISBN 978-606-37-1551-8

© 2025 Autoarea volumului. Toate drepturile rezervate. Reproducerea integrală sau parțială a textului, prin orice mijloace, fără acordul autoarei, este interzisă și se pedepsește conform legii.

Universitatea Babeș-Bolyai  
Presa Universitară Clujeană  
Director: Codruța Săcelean  
Str. B.P. Hasdeu nr. 51  
400371 Cluj-Napoca, România  
Tel.: (+40)-744-687.884  
E-mail: editura@ubbcluj.ro  
<http://www.editura.ubbcluj.ro/>  
<https://libraria.ubbcluj.ro/>

## CUPRINS

|                                                                                                                                |    |
|--------------------------------------------------------------------------------------------------------------------------------|----|
| <i>Introducere</i>                                                                                                             | 5  |
| <i>Capitolul 1: Caracterizarea principalelor tehnologii digitale</i>                                                           | 7  |
| 1.1. Big Data                                                                                                                  | 7  |
| 1.2. Rețele sociale                                                                                                            | 10 |
| 1.3. Inteligența Artificială (IA)                                                                                              | 14 |
| <i>Exerciții practice – Capitolul 1</i>                                                                                        | 21 |
| Tema 1. Creați un nor de cuvinte                                                                                               | 21 |
| Tema 2. Realizați o hartă mentală (mind-map)                                                                                   | 21 |
| Tema 3. Analiză de caz – impactul unui fenomen digital în societate                                                            | 22 |
| <i>Bibliografie capitolul 1</i>                                                                                                | 23 |
| <i>Capitolul 2: Riscuri și provocări în mediul digital - securitate cibernetică, dezinformare, fake news și etică digitală</i> | 25 |
| 2.1. Securitate cibernetică                                                                                                    | 25 |
| 2.2. Dezinformare și fake news                                                                                                 | 32 |
| 2.3. Etică digitală                                                                                                            | 37 |
| <i>Exerciții practice – Capitolul 2</i>                                                                                        | 42 |
| Tema 1 Creați un nor de cuvinte                                                                                                | 42 |
| Tema 2. Realizați o hartă mentală (mind-map)                                                                                   | 42 |
| Tema 3. Întrebări dezbateri – orientare spre studiu de caz                                                                     | 43 |
| <i>Bibliografie</i>                                                                                                            | 44 |
| <i>Capitolul 3: Instrumente vizuale</i>                                                                                        | 47 |
| 3.1. Nor de cuvinte                                                                                                            | 47 |
| <i>Bibliografie</i>                                                                                                            | 51 |
| 3.2. Hărți mentale (HM)                                                                                                        | 52 |
| <i>Bibliografie</i>                                                                                                            | 60 |
| 3.3. Google Drive – scurtă prezentare                                                                                          | 61 |
| <i>Bibliografie</i>                                                                                                            | 65 |

## ***Structura și obiectivele caietului de lucrări practice***

Lucrarea de față își propune să contureze o imagine relevantă, dar selectivă, a provocărilor care definesc societatea digitală actuală. Fără intenția de a epuiza complexitatea unui domeniu aflat într-o continuă transformare, analiza urmărește să surprindă câteva dintre temele centrale cu impact major asupra tehnologiei, economiei, vieții sociale și cadrului normativ. Lumea digitală se dezvoltă într-un ritm accelerat, iar această dinamică generează interdependențe profunde între infrastructura tehnică, comportamentele utilizatorilor, modelele economice emergente și reglementările juridice care caută să le țină pasul. În fața acestei complexități, selecția subiectelor a fost realizată în funcție de relevanța actuală și potențialul lor de influență pe termen mediu și lung. Pentru a oferi coerență și claritate demersului, sursele utilizate au fost filtrate și interpretate printr-o serie de întrebări analitice care au ghidat procesul de structurare a conținutului și au facilitat transpunerea informațiilor într-un cadru aplicabil și inteligibil.

În **Introducere** se prezintă contextul și motivația care fundamentează strategia pentru **Deceniul digital al Europei**, subliniind impactul pandemiei, fragmentarea pieței unice și intensificarea amenințărilor cibernetice.

**Capitolul 1** examinează modul în care Big Data (volum, viteză, varietate), rețelele sociale (UI/UX, algoritmi de recomandare, moderare) și inteligența artificială (învățare automată, rețele neuronale profunde, modele transformer, IA generativă) interacționează pentru a transforma societatea și economia. Expunerea conceptuală urmează un demers progresiv, avansând de la fundamentele teoretice și tehnice către exemple aplicate și implicații economice, facilitând astfel o înțelegere graduală a fenomenului și pregătind cititorul pentru analiza riscurilor asociate mediului digital.

**Capitolul 2** analizează aspecte esențiale ale securității cibernetice, incluzând confidențialitatea, integritatea și modelul Zero Trust, precum și fenomenul de dezinformare, alături de mecanismul de fact-checking. De asemenea, sunt abordate dimensiunile eticii digitale, precum drepturile și responsabilitățile digitale, transparența și echitatea algoritmică, provocările asociate rețelelor sociale și inteligenței artificiale, precum și cadrul normativ internațional și european. Structura capitolului urmează un fir logic progresiv, pornind de la amenințările tehnice, continuând cu impactul social și încheind cu răspunsurile legislative, facilitând astfel o înțelegere coerentă a problemelor și soluțiilor.

**Capitolul 3** explorează utilizarea norului de cuvinte, hărții mentale și platformelor colaborative din Google Drive, oferind pași de creare și exemple de aplicare în activități de grup și individuale. Expunerea metodologică urmează un demers structurat, avansând de la definirea conceptelor și descrierea metodelor, către instrumentele specifice și procedurile operaționale, încheind cu studii de caz. Această abordare permite cititorilor să înțeleagă nu doar „ce” și „de ce”, ci și „cum” pot fi aplicate aceste tehnici în practică

Integrarea elementelor vizuale și colaborative în structura caietului de lucrări practice susține un demers educațional centrat pe dezvoltarea competențelor digitale esențiale. Instrumente precum norul de cuvinte, harta mentală și aplicațiile din suita Google transformă procesul de învățare într-un spațiu de explorare activă, în care studenții nu se limitează la recepționarea conținutului, ci

participă efectiv la construcția lui. Aceste resurse nu au un simplu rol decorativ, ci funcționează ca suporturi cognitive ce stimulează gândirea analitică, colaborarea și reflecția.

Caietul de lucrări practice propune o metodologie activă de învățare, bazată pe patru pași esențiali:

- *lectură activă* – subliniază conceptele-cheie și notează întrebări pe margine pentru a fixa teoria și a identifica punctele care necesită clarificări.
- *exerciții aplicate* – realizează activitățile propuse și experimentează metodele pe exemple proprii pentru a înțelege cum și de ce funcționează tehnicile prezentate.
- *lucru colaborativ* – organizează discuții de grup și schimburi de feedback pe studii de caz pentru a beneficia de perspective multiple și a consolida cunoștințele.
- *reflecție și autoevaluare* – la sfârșitul fiecărui capitol, rezumă în câteva fraze ceea ce ai învățat și completează un mini-chestionar de autoevaluare pentru a măsura progresul și a planifica îmbunătățiri.

Prin folosirea acestor instrumente, metoda propusă devine practică și bazată pe experiență, ajutând studenții să învețe activ și să facă legătura între teorie și aplicare.

## Introducere

În contextul unei evoluții tehnologice fără precedent, expansiunea rapidă a internetului, omniprezența rețelelor sociale și utilizarea pe scară largă a dispozitivelor inteligente au generat transformări semnificative în modul viață. Aceste progrese nu doar că au revoluționat comunicarea interumană, facilitând conexiuni instantanee la nivel global, dar au redefinit și procesul de accesare și diseminare a informației, contribuind la formarea unei societăți interconectate, caracterizată prin fluxuri rapide de date și interacțiuni virtuale complexe. În această realitate digitală, tehnologiile emergente continuă să modeleze comportamentele sociale și economice, rutina zilnică, să afecteze modul în care desfășurăm afaceri, învățăm, ne relaxăm și interacționăm.

*Deceniul digital al Europei* a apărut ca un răspuns la multele provocări și tendințe globale și a evidențiat necesitatea unei strategii digitale coerente. Printre factorii premergători inițiativei deceniul digital se numără:

1. *Șocul pandemiei COVID-19 și accelerarea digitalizării* - pandemia a impus tranziția rapidă la telemuncă, educație online și telemedicină, demonstrând atât potențialul tehnologiilor digitale de a asigura continuitatea activităților, cât și fragilitatea infrastructurilor existente. În numai 2-3 ani, percepția asupra digitalizării s-a schimbat radical: conectivitatea și platformele online au devenit indispensabile pentru aproape toate aspectele vieții sociale și economice, evidențiind nevoia unor rețele mai robuste și a unor servicii digitale uniforme la nivelul UE. ([EUR-LexEurofound](#))
2. *Amplificarea amenințărilor cibernetice* - valul de atacuri de tip ransomware, compromiterea lanțurilor de aprovizionare IT și incidente precum breșa SolarWinds au demonstrat că statele din UE, fiecare cu propriile reguli, rămâneau expuse și fără mecanisme de răspuns coordonat. ([Strategia Digitală a Europei](#))
3. *Disparități în adoptarea tehnologiilor – fragmentarea pieței unice* – unele studii arată că UE a rămas în urmă față de SUA și China în materie de inovație, producție și adoptare a soluțiilor cloud, AI sau Big Data. Această „caracteristică patchwork” (fragmentare structurală, mozaic digital) a

condus la decalaje semnificative între statele membre, atât în ceea ce privește infrastructura, cât și în ceea ce vizează competențele digitale ale cetățenilor și companiilor. În consecință, inițiativa Deceniul Digital urmărește reducerea fragmentării prin obiective comune de utilizare a tehnologiilor digitale de către cel puțin 75 % dintre firme până în 2030. ([Telefónica](#), [Deceniul digital al Europei: Obiective pentru 2030 | Comisia Europeană](#))

4. *Criza globală a semiconductoarelor și căutarea suveranității tehnologice*- penuria de cipuri, generată de pandemie și amplificată de tensiunile geopolitice, a evidențiat dependența UE de furnizori extra-europeni. În răspuns la urgența asigurării unui lanț stabil de aprovizionare, Pactul European pentru Semiconductori („European Chips Act”) vizează dublarea cotei de piață a producției europene de semiconductoare până în 2030, pentru a întări competitivitatea și reziliența tehnologică a regiunii. ([european-chips-act.com](#)[Brookings](#))
5. *Provocările etice și necesitatea reglementării IA*- adoptarea rapidă a inteligenței artificiale a generat preocupări privind drepturile fundamentale, ceea ce a determinat elaborarea ghidurilor de etică pentru o IA de încredere, bazate pe șapte principii-cheie (implicare și supraveghere umană; robustețe tehnică și siguranță; respectarea vieții private și guvernanta datelor; transparență; diversitate, nediscriminare și echitate; bunăstare socială și de mediu; responsabilitate), menite să asigure un echilibru între inovare și valorile democratice europene printr-un cadru legislativ adecvat. ([Strategia Digitală a Europei](#)[acm.acm.org](#), [Orientări etice pentru o IA de încredere | Shaping Europe's digital future](#))

Programul de politică privind deceniul digital, cu ținte și obiective concrete pentru 2030 ce orientează transformarea digitală a Europei:(<https://commission.europa.eu/strategy-and-policy>) poate fi rezumat în următoarele șase puncte:

1. competențe digitale – până în 2030, cel puțin 80% din populația UE ar trebui să aibă competențe digitale de bază, iar numărul specialiștilor în TIC ar trebui să ajungă la 20 de milioane;
2. transformarea digitală a întreprinderilor – 75% din întreprinderile din UE ar trebui să utilizeze tehnologii precum cloud computing, inteligență artificială și Big Data, iar numărul de "unicorni" (start-up-uri cu valoare de peste un miliard de dolari) ar trebui să se dubleze;
3. infrastructuri digitale sigure și durabile – se urmărește asigurarea conectivității gigabit (1 Gb=1024<sup>3</sup> biți) pentru toți, dublarea producției de semiconductori de ultimă generație în UE și dezvoltarea a 10.000 de noduri de rețea sigure și neutre din punct de vedere climatic.
4. digitalizarea serviciilor publice – se dorește ca toate serviciile publice-cheie să fie disponibile online, iar cetățenii să aibă acces complet la dosarele lor medicale digitale și la identificare electronică.
5. proiecte multinaționale – UE va facilita lansarea de proiecte digitale la scară largă, precum infrastructura de date, tehnologiile blockchain, centrele de inovare digitală și securitatea cibernetică.
6. drepturi și principii digitale – se promovează o tranziție digitală centrată pe oameni, cu libertatea de alegere, siguranță, solidaritate, participare democratică și sustenabilitate.

# Capitolul 1: Caracterizarea principalelor tehnologii digitale

## 1.1. Big Data

**Big Data** desemnează colecții vaste și complexe de informații care depășesc capacitățile instrumentelor tradiționale de procesare, precum foile de calcul. Aceste date pot fi:

- *structurate*, cum ar fi tabele de inventar sau registre de tranzacții financiare.
- *nestructurate*, precum postările de pe rețelele sociale, fotografiile și clipurile video.
- *semi-structurate* (sau „hibrid”), cum ar fi fișierele **JSON** sau **XML**, care combină text și metadata, fiind utilizate în antrenarea modelelor de inteligență artificială.

([Introducere în noțiunea de „Big Data”](#), [Ce este Big Data? | Oracle România](#))

Conceptul de **Big Data** își are rădăcinile în anul 2001, când analistul Gartner Doug Laney a definit cele trei caracteristici fundamentale – volum, viteză și varietate – pentru a descrie provocările gestionării cantităților mari de date. Ulterior, cercetări din diferite domenii au extins schema inițială, propunând până la circa zece „V”-uri suplimentare (de exemplu, veridicitate, valoare, variabilitate etc.) pentru a surprinde dimensiuni legate de calitatea, utilitatea și consistența informațiilor în procesele decizionale. ([Stăpânirea celor 10 V-uri ale big data | Dojo de știință a datelor](#))

Studiul lui Panimalar et al. (2017), publicat în ([www.irjet.net](http://www.irjet.net)), merge mai departe, propunând o schemă cu **17 V-uri și 1 C** pentru o abordare mai cuprinzătoare a Big Data. Deși această extensie nu a fost adoptată în mod universal de comunitatea academică, ea ilustrează complexitatea tot mai mare a mediului informațional și nevoia de măsurători detaliate din perspectiva gestionării, analizei și valorificării datelor.

Cele trei „V”-uri fundamentale

- volum: atât de multe date încât clasele tradiționale de depozitare devin inadecvate (cantitate masivă)
- viteză: procesarea și analiza „în timp real” (sau aproape în timp real) pentru a valorifica informațiile imediat ce apar (rapiditate în generare).
- varietate: prezența formatelor eterogene (structurate, semi-structurate, nestructurate) din surse diverse (jurnale de evenimente, rețele sociale, senzori, fișiere multimedia etc.) (diversitate formate).

Restul de „V”-uri extinse și caracteristica „C” (Panimalar et al. (2017)):

- valoare – reprezintă capacitatea datelor de a genera insight-uri relevante care contribuie direct la îmbunătățirea proceselor decizionale și la creșterea beneficiilor organizaționale.
- veridicitate – reflectă gradul de încredere în date, asigurându-se că informațiile sunt corecte, complete și nefiind afectate de erori sau zgomot nesemnificativ.
- validitate – confirmă că datele sunt autentice, corect colectate și relevante pentru scopul analizei, evitând utilizarea informațiilor irelevante sau înșelătoare.
- volatilitate – indică perioada de timp în care datele rămân utile și semnificative, subliniind necesitatea de actualizare și arhivare a seturilor de date în funcție de ritmul schimbării.

- vizualizare – transformă datele complexe într-o formă grafică sau vizuală intuitivă, facilitând înțelegerea și comunicarea rapidă a insight-urilor cheie.
- viralizare – măsoară viteza și amplitudinea cu care informațiile se răspândesc în rețele sociale sau în cadrul comunităților, influențând rapid opinia și deciziile.
- vâscozitate – evaluează întârzierile și fricțiunile din procesarea datelor, evidențiind blocajele care pot împiedica fluxul rapid și eficient al informațiilor.
- variabilitate – se referă la inconsistențele și fluctuațiile datelor în timp, care pot complica analizele atunci când acestea își schimbă frecvența sau structura.
- venit – marchează originea exactă a datelor, permițând trasabilitatea sursei și evaluarea credibilității acestora în funcție de autoritate sau context.
- vocabular – definește terminologia și structura semantică utilizată în seturile de date, asigurându-se că elementele informaționale sunt uniforme și interoperabile.
- vag – reflectă gradul de ambiguitate sau incertitudine prezent în anumite date, indicând necesitatea proceselor de clarificare și contextualizare pentru a evita interpretări greșite.
- verbozitate – evidențiază nivelul de redundantă informațională sau de detalii irelevante care pot fi eliminate pentru a concentra analizele pe insight-uri esențiale.
- voluntariat – subliniază disponibilitatea și accesibilitatea datelor pentru utilizatori sau sisteme terțe, sugerând deschiderea spre partajare și reutilizare.
- versatilitate – caracterizează capacitatea datelor de a fi reutilizate, combinate și adaptate în diferite contexte și scopuri analitice, maximizându-le utilitatea pe termen lung.
- complexitate – reprezintă dificultatea gestionării simultane și coerente a tuturor caracteristicilor de mai sus, impunând utilizarea unor tehnologii și metode avansate pentru o orchestrare eficientă.

Importanța unei abordări extinse rezultă din:

- nevoia unei analize precise - prin includerea celor 17 „V”-uri, organizațiile pot să evalueze nu doar cât de multe date există, ci și cât de valoroase, de fiabile, de relevante și de versatile sunt aceste date în contextul operațional; complexitatea (C) subliniază gradul de interdependență între toate celelalte dimensiuni și necesitatea unor tehnologii și metode avansate (de exemplu, inteligența artificială sau sistemele distribuite) pentru a le gestiona simultan.
- luare de decizii informate - înțelegerea „vâscozității” (întârzierile în procesare) sau a „volatilității” (durata de viață a datelor) poate ajuta la stabilirea priorităților: unele date sunt utile doar pe termen foarte scurt, altele trebuie păstrate pentru analize istorice; veridicitatea și validitatea sunt cruciale pentru a evita decizii bazate pe date eronate sau irelevante.
- optimizarea resurselor și a costurilor - unele dimensiuni (de ex. volum și vâscozitate) indică necesarul de infrastructură (stocare, rețele, servere), în timp ce altele (veridicitate, valoare) pot orienta spre investiții în procese de curățare și structurare a datelor.
- Inovație și competitivitate - vizualizarea, versatilitatea și viralizarea permit transformarea rapidă a datelor brute în insight-uri ușor de înțeles și diseminate eficient; voluntariatul și verbozitatea pot ghida strategiile de acces și distribuție a datelor către diferite entități (intern/extern), în funcție de nevoia reală de consum.

Prin abordarea extinsă a celor 17 V-uri și 1 C, big data devine nu doar un volum masiv de informații, ci o resursă strategică, integrând aspecte de calitate, utilitate, securitate și durabilitate. Chiar dacă

schema propusă de Panimalar nu este încă unanim acceptată, ea oferă o perspectivă detaliată asupra provocărilor actuale din gestionarea datelor la scară largă. În era digitală, viitorul progresului global va depinde de capacitatea organizațiilor de a înțelege și valorifica toate aceste dimensiuni ale big data.

În ceea ce privește procesarea big data, aceasta se bazează pe platforme specializate care permit gestionarea eficientă a volumelor masive de date. Printre cele mai utilizate tehnologii se numără:

- **Hadoop** – un cadru open-source (platformă software disponibilă public, accesibilă, modificabilă și distribuită liber) pentru stocare și procesare distribuită, care împarte datele în fragmente (HDFS) și le procesează în paralel folosind modelul MapReduce (împarte datele în sarcini paralele, map și le agregă eficient, reduce). Hadoop este ideal pentru volume mari de date ce nu necesită procesare în timp real, fiind optimizat pentru costuri reduse de stocare pe disc.
- **Spark** – un motor de procesare în memorie, rapid și flexibil, care suportă atât operațiuni batch (procesare pe loturi), cât și streaming (procesare în flux). Spark este recomandat pentru fluxuri de date în timp real și machine learning, datorită capacității de procesare în memorie, care reduce semnificativ timpii de execuție.
- **NoSQL** – baze de date orientate pe documente (MongoDB) sau pe coloane (Cassandra), concepute pentru a stoca și interoga big data la scară largă. Aceste soluții oferă flexibilitate și scalabilitate, permițând creșterea rapidă a volumului și varietății de date. ([www.hakia.com/](http://www.hakia.com/); [www.grss-ieee.org](http://www.grss-ieee.org))

În ceea ce privește arhitectura procesării, datele sunt *distribuite* – fragmentate și stocate pe mai multe servere (noduri) pentru a îmbunătăți accesibilitatea și reziliența sistemului. Sarcinile de prelucrare rulează în paralel, adică sunt împărțite în subtask-uri ce rulează simultan pe mai multe procesoare, reducând semnificativ timpul de execuție. Algoritmii de inteligență artificială extrag din aceste date modele predictive și insight-uri valoroase, oferind suport pentru luarea deciziilor în diverse domenii.

Aplicațiile big data influențează numeroase aspecte ale vieții moderne:

- rețele sociale – algoritmii analizează preferințele și comportamentul utilizatorilor (like-uri, comentarii, distribuirii) pentru a personaliza conținutul din feed și a sugera conexiuni relevante.
- e-commerce – recomandările de produse sunt generate pe baza istoricului de cumpărături, a produselor vizualizate și a comportamentului din coș, pentru a crește rata de conversie și valoarea medie a comenzii.
- sănătate – analiza datelor medicale (dosare electronice, imagistică, semnale de la senzori) ajută la diagnosticarea precoce a bolilor, la detectarea tendințelor epidemice și la optimizarea planurilor de tratament.
- transport – optimizarea rutelor și gestionarea traficului prin analiza datelor GPS, a imaginilor de la camere video și a semnalelor provenite de la senzori, reducând aglomerația și timpul de deplasare.

- finanțe – detectarea fraudelor în timp real și analiza piețelor financiare prin procesarea volumelor mari de tranzacții, a știrilor economice și a sentimentului de pe rețele sociale.

Cel mai cunoscut exemplu se referă la platforma Netflix care folosește Big Data pentru a analiza istoricul de vizionare al utilizatorilor, recenziile și metadatele conținutului, antrenând modele de machine learning care sugerează filme personalizate pentru fiecare utilizator.

Big Data nu este doar un concept tehnologic, ci o realitate omniprezentă care modelează deciziile și interacțiunile noastre zilnice. Într-o lume unde datele sunt noul „aur digital”, gestionarea etică și responsabilă a acestora devine esențială pentru dezvoltarea sustenabilă.

## 1.2. Rețele sociale

### 1.2.1. Rol și importanță

O rețea socială este un mod prin care oamenii se conectează între ei, formând legături de diferite tipuri — de la colegi sau cunoscuți, până la prieteni apropiați și membri ai familiei. Totodată, termenul desemnează și platformele online care permit utilizatorilor să comunice, să împărtășească idei, informații sau experiențe și să colaboreze în funcție de interese comune.

([https://www.asecib.ase.ro/mps/Analiza\\_retelelor\\_sociale.pdf](https://www.asecib.ase.ro/mps/Analiza_retelelor_sociale.pdf);

<https://inteligenta-sociala.ro/index.php/2015/09/12/ce-este-si-de-ce-se-materializeaza-reteaua-sociala/>)

Rețelele sociale au revoluționat comunicarea prin eliminarea barierelor geografice și oferirea posibilității fiecărui utilizator de a publica și distribui conținut imediat, către un public global. Prin democratizarea accesului la informație, aceste platforme susțin mobilizarea civică, colaborarea și schimbul de idei. Aspectele legate de manipulare, dezinformare și polarizare vor fi dezvoltate în Capitolul 2. (Pariser, 2011; Gillespie, 2018).

### 1.2.2 Componente tehnologice

Arhitectura tehnologică a rețelilor sociale se bazează pe mai multe straturi interdependente, fiecare contribuind la experiența utilizatorului, la personalizarea conținutului și la securitatea întregului ecosistem. Acestea sunt: *interfața utilizatorului*, *algoritmi de recomandare*, *sisteme de securitate*, *infrastructura de stocare și procesare*.

*Interfața utilizatorului (UI/UX)* sau punct de contact și engagement

Interfața reprezintă legătura directă dintre utilizator și platformă. Elementele de design (bare de navigare, butoane de reacție „Like”, „Share”, „Comment” etc.) și mecanismele UX (scroll infinit, notificări push, autoplay video) sunt concepute pentru a menține interesul și atenția utilizatorilor. Aceste funcționalități permit găsirea rapidă a conținutului relevant și facilitează distribuirea de informații și organizarea de evenimente (Nielsen, 2015).

Efectele pot fi atât *pozitive*, interacțiunea se simplifică, iar utilizatorii pot găsi rapid resurse utile (știri, grupuri de interes, evenimente); cât și *negative*, mecanismele de tip „infinite scroll” și notificările agresive pot conduce la dependență digitală și la supraîncărcare informațională („information overload”), generând stres și scăderea capacității de concentrare (Eyal, 2014).

*Algoritmi de recomandare*

Principiul de funcționare al algoritmilor de recomandare constă în analiza comportamentului utilizatorilor (click-uri, timp petrecut pe postare, tipuri de conținut preferate) cu loturi de date istorice pentru a determina ce anume afișează în feed-ul fiecărui utilizator (Zaharia et al., 2016).

Tehnicile de machine learning cu care lucrează rețelele pot fi:

- *collaborative filtering*: generează recomandări pe baza similarităților dintre comportamentele a doi sau mai mulți utilizatori; exemplu: dacă doi utilizatori au interacționat cu aceleași postări, li se vor sugera conținuturi asemănătoare. (Bessi & Ferrara, 2016)
- *content-based filtering*: analizează caracteristicile conținutului (tag-uri, descrieri, metadata) pentru a sugera materiale similare celor deja vizualizate de utilizator; exemplu: Netflix folosește ambele tehnici pentru recomandări). (Pariser, 2011).

Efectele secundare sunt recunoscute sub forma de *bule informaționale* („echo chambers”): utilizatorii pot fi izolați în medii în care li se confirmă în mod repetat propriile convingeri, limitând expunerea la perspective contrare (Pariser, 2011; Sunstein, 2018) și în *polarizare socială*: conținutul intens personalizat poate amplifica diferențele ideologice dintre grupuri, conducând la o fracturare a spațiului public și la creșterea tensiunilor (Bessi & Ferrara, 2016).

Începând cu 2021–2022, multe platforme au evoluat către abordări hibride, care adaugă componente de deep learning (embedding-uri de tip transformer pentru text și video), îmbunătățind astfel acuratețea și relevanța recomandărilor.

Pentru a combate conținutul nociv și a proteja datele utilizatorilor, rețelele sociale implementează *sisteme avansate de securitate și moderare*, inclusiv:

*Filtre automate și inteligență artificială* - modele de procesare a limbajului natural (NLP) detectează cuvinte-cheie și pattern-uri asociate cu discursul instigator la ură, știrile false sau conținutul extremist. De exemplu, Twitter utilizează algoritmi de text-mining pentru a semnaliza automat mesaje considerate hate speech (Alimardani & Faghieh, 2019). Facebook/Meta a implementat sisteme de machine learning care scanează imagini și texte pentru a evalua contextul și potențialul de dezinformare, semnalând imediat conținutul suspect către echipe de moderare umano-automatizate.

*Moderatori umani* - intervin atunci când filtrele automate nu pot decide cu precizie asupra unui context complex (de exemplu, detectarea ironiei, a sarcasmului sau a nuanțelor culturale). Platforme precum YouTube combină moderarea AI cu echipe umane care verifică videoclipurile sau postările semnalate pentru încălcarea politicilor comunitare.

*Protocoale de criptare și securitate*- datele utilizatorilor (mesaje private, fotografiile, informații personale) sunt protejate prin protocoale precum TLS/SSL (HTTPS) și criptare end-to-end în serviciile de chat (de ex., WhatsApp). Acest lucru previne interceptarea și accesul neautorizat la informații sensibile, conform normelor GDPR (Regulamentul UE 2016/679) (GDPR, 2016).

Între 2023 și 2024, marile platforme au început să testeze și moderația audio/video în timp real (rețea neuronală pentru recunoașterea discursului și a obiectelor în fluxuri live), pentru a detecta imediat conținut nepotrivit (Doe et al., 2024).

Infrastructură de stocare și procesare vizează stocarea scalabilă, procesare batch și streaming, straturi ACID peste obiect-store-uri.

*Stocare scalabilă (Data Lakes & NoSQL)*

- *data lakes* (Amazon S3, Azure Data Lake Storage) permit colectarea și stocarea datelor brute (texte, imagini, fișiere multimedia) într-o formă nativă, fără a impune structuri relaționale stricte, suportând varietatea ridicată de formate și facilitând flexibilitatea în prelucrări ulterioare.

- *baze de date NoSQL* (MongoDB, Apache Cassandra, HBase) folosesc modele orientate pe documente sau pe coloane, oferind scalare orizontală și latențe reduse chiar și la volume ce depășesc terabiții, ceea ce permite rețelelor sociale să gestioneze petabyte de date generate zilnic de milioane de utilizatori (Armbrust et al., 2020).

După 2022, în contextul GDPR și al preocupărilor legate de date personale, unele platforme au implementat baze de date hibride (SQL+NoSQL) pentru a optimiza atât scrierea rapidă cât și cerințele de audit și trasabilitate (Lee et al., 2023).

#### *Procesare batch și streaming*

- Apache Hadoop: un ecosistem bazat pe HDFS (Hadoop Distributed File System) și MapReduce, potrivit pentru job-uri de tip batch, unde datele sunt procesate „în loturi” (ex.: generarea rapoartelor zilnice de trafic).
- Apache Spark: motor de procesare „in-memory” care suportă atât operațiuni batch, cât și streaming în timp real. Spark excelează în sarcini iterative de machine learning (ex.: antrenarea frecventă a modelelor de recomandare pe date actualizate) și în analize complexe realizate „on the fly” prin optimizări la nivel de DAG (Directed Acyclic Graph) (Zaharia et al., 2016). Spark este recomandat atunci când latența este critică și când se lucrează cu fluxuri continue de date (ex.: comentarii și like-uri în timp real).

#### *Straturi ACID peste obiect-store-uri*

Obiect-store-urile sunt sisteme de stocare scalabile, optimizate pentru gestionarea volumelor mari de date, organizate sub formă de obiecte individuale. Spre deosebire de sistemele tradiționale bazate pe fișiere sau baze de date relaționale, acestea permit acces rapid, durabilitate și scalabilitate automată, fiind utilizate frecvent în infrastructurile cloud pentru stocarea și procesarea eficientă a datelor. Aceste sisteme sunt esențiale pentru aplicațiile care necesită gestionarea eficientă a datelor nestructurate, cum ar fi imagini, videoclipuri, fișiere de jurnal și backup-uri.

Pentru a îmbunătăți consistența și fiabilitatea acestor sisteme, se utilizează *straturi ACID*, care adaugă un jurnal de tranzacții și suport pentru **atomicitate**, **consistență**, **izolare** și **durabilitate**. Aceste straturi permit funcționalități avansate, precum:

- „time-travel” – revizuirea versiunilor anterioare ale datelor.
- optimizări de layout – organizarea eficientă a datelor pentru performanță maximă.
- operațiuni de upsert (*update* și *insert*) – operațiune care actualizează o înregistrare dacă există deja sau o inserează dacă nu există.

Această tehnologie este esențială pentru menținerea consistenței și performanței în analiza petabyte-urilor de informații generate zilnic de rețelele sociale și alte aplicații de mare amploare.

(Zaharia et al., 2020).

Prin această arhitectură, platformele sociale pot: colecta și stoca orice tip de date fără filtrare inițială; asigura latențe scăzute și interogări rapide prin soluții NoSQL și caching în memorie; procesa și analiza în timp real petabyte-uri de informații, oferind conținut personalizat și suport pentru miliarde de operațiuni zilnice (Kreps et al., 2011; Zaharia et al., 2016).

### 1.2.3 Impact social și dileme etice

Rețelele sociale generează provocări majore în plan etic și social. Iată principalele puncte esențiale, (tratate sumar):

- formarea camerelor de ecou - algoritmi de recomandare personalizează conținutul astfel încât utilizatorii pot ajunge izolați în bule informaționale, care intensifică polarizarea și limitează expunerea la perspective contrare (Pariser, 2011; Sunstein, 2018).
- difuzia rapidă a conținutului toxic - conținutul emoțional sau polarizant (fake news, hate speech) devine viral mai rapid decât informațiile neutre, din cauza prioritizării engagement-ului, cu riscuri semnificative asupra campaniilor de sănătate publică și a proceselor democratice (Del Vicario et al., 2016).
- manipulare prin design persuasiv și dezinformare - mecanisme UX de tip “infinite scroll” sau notificări agresive exploatează nevoia de validare socială (“fear of missing out”) pentru a menține utilizatorii conectați excesiv (Eyal, 2014). Campanii deliberate de dezinformare pot viza emoții politice sau sociale pentru a influența comportamentul electoral sau de consum.
- protecția datelor personale și transparența algoritmilor- colectarea și analiza volumelor mari de date personale (locatie, interese, conexiuni) ridică întrebări privind dreptul la confidențialitate și consimțământul informat. Lipsa transparenței algoritmice subminează încrederea în platforme și poate duce la abuzuri ale utilizării datelor (Kairouz et al., 2021). Conform GDPR (2016), utilizatorii trebuie informați asupra modului de procesare a datelor și pot retrage consimțământul în orice moment.

Rețelele sociale au un impact pozitiv semnificativ asupra economiei, facilitând marketingul digital, antreprenoriatul și finanțarea colaborativă. Iată principalele idei care susțin acest impact:

#### 1. marketing digital și publicitate online

- algoritmi de recomandare permit companiilor să targeteze audiența cu precizie, optimizând campaniile publicitare.
- platforme precum Facebook, TikTok și Instagram au revoluționat comerțul online, oferind strategii de promovare eficiente și acces la milioane de consumatori.

#### 2. antreprenoriat și freelancing

- rețelele sociale au creat noi oportunități pentru startup-uri și profesioniști independenți, oferind o piață globală accesibilă pentru promovare și vânzare de servicii.
- antreprenoriatul social este susținut prin platforme digitale, facilitând impactul pozitiv asupra comunităților și dezvoltarea unor afaceri sustenabile.

#### 3. crowdfunding și investiții

- Twitter și LinkedIn sunt folosite pentru atragerea investitorilor, promovarea proiectelor și finanțarea colaborativă.
- Crowdfunding-ul permite startup-urilor să obțină fonduri direct de la comunități care cred în ideea lor, eliminând barierele tradiționale de finanțare.

Aceste aspecte demonstrează că rețelele sociale nu sunt doar instrumente de comunicare, ci și motoare economice care stimulează inovația, creșterea afacerilor și accesul la finanțare. (digitalpedia.ro)

### 1.3. Inteligența Artificială (IA)

#### Inteligența Artificială: clasificare după metodologie și tipologie

Inteligența artificială (IA) este, conform definiției propuse de Russell & Norvig, „studiul agenților care primesc percepții (P) și execută acțiuni (A) pentru a maximiza o funcție de utilitate”. Această definiție accentuează ideea că IA presupune sisteme capabile să prelucreză informații din mediu și să acționeze în mod optim în funcție de obiective. (Mitchell, T. M. 1997).

Inteligența artificială (IA) este un domeniu în care specialiștii dezvoltă programe sau sisteme capabile să îndeplinească sarcini care, în mod normal, ar necesita inteligență umană – cum ar fi învățarea, luarea deciziilor sau recunoașterea imaginilor și a limbajului. Una dintre cele mai frecvent întâlnite definiții oficiale este cea oferită de **Comisia Europeană (2020)**, care descrie IA ca fiind „capacitatea unei mașini de a imita funcții umane precum raționamentul, învățarea, planificarea și creativitatea”. O altă abordare, mai tehnică, este cea oferită de **Digitalpedia (2021)**, unde IA este descrisă drept dezvoltarea de sisteme informatice care pot executa sarcini inteligente, cum ar fi analiza datelor sau generarea de conținut. Totodată, o definiție clasică, formulată de **John McCarthy**, unul dintre fondatorii domeniului, afirmă că IA este „știința și ingineria creării de mașini inteligente, în special programe de calculator inteligente”.

Chiar dacă aceste formulări sunt frecvent utilizate, nu există o singură definiție universal acceptată a inteligenței artificiale. Acest lucru se explică prin faptul că IA este un domeniu interdisciplinar – adică implică mai multe științe – precum informatica, matematica, psihologia, etica sau dreptul. Fiecare disciplină pune accent pe alte aspecte ale IA, iar această diversitate de perspective a dus la formularea mai multor definiții complementare.

Sub umbrela IA se dezvoltă atât **metodologii de construire a sistemelor inteligente**, cât și **tipologii de clasificare a acestora în funcție de capacități**. Aceste două perspective sunt complementare și esențiale pentru înțelegerea domeniului.

#### Clasificarea după metodologie sau cum funcționează IA

1. **Machine Learning (ML)** - este una dintre cele mai importante metodologii din IA, definită de Mitchell (1997) ca „elaborarea de algoritmi care învață din date fără a fi programați explicit pentru fiecare sarcină”. Procesul ML cuprinde:
  - pregătirea datelor – curățarea, normalizarea și etichetarea datelor brute.
  - antrenarea modelului – optimizarea funcției de cost (de exemplu, prin gradient descent) pentru a ajusta parametrii modelului. Această funcție măsoară diferența dintre predicțiile modelului și valorile reale, iar obiectivul antrenamentului este minimizarea acestei funcții.
  - validarea pe date noi – evaluarea performanței modelului pe un set de date nevăzut anterior, pentru a măsura capacitatea de generalizare.

Exemplu: un sistem ML supravegheat poate detecta fraudele bancare învățând din istoricul tranzacțiilor etichetate „fraudă” sau „normal”. ML este folosit în **recunoașterea vocală** (ex.: Siri, Google Assistant).

**Deep Learning (DL)** - este o ramură specializată a ML, bazată pe rețele neuronale artificiale adânci, cu multiple straturi (uneori zeci sau sute). Fiecare strat al rețelei învață reprezentări tot mai abstracte ale datelor de intrare, de la detectarea muchiilor și formelor în imagini până la interpretarea sintactică și semantică a textului (Vaswani et al., 2017). Antrenamentul implică

mecanismul de back-propagation, prin care eroarea calculată la ieșire este propagată înapoi pentru a actualiza ponderile rețelei și optimizatori avansați (Adam, RMSProp) pentru a accelera convergența. Dacă un model de rețea neuronală are dificultăți în convergență, Adam poate ajuta la stabilizarea antrenamentului, în timp ce RMSProp este mai eficient în situații unde gradientul variază semnificativ între parametri. DL necesită volume mari de date și putere computațională ridicată, deoarece modelele sale complexe, bazate pe rețele neuronale adânci, trebuie să proceseze și să extragă caracteristici relevante din seturi extinse de informații. Această cerință face DL ideal pentru aplicații complexe, precum recunoașterea imaginii, procesarea limbajului natural și sistemele de conducere autonomă

*Exemplu:* Un model DL antrenat pe zeci de mii de imagini medicale poate detecta anomalii pulmonare cu o precizie comparabilă cu cea a medicilor radiologi. DL este utilizat și în sisteme de conducere autonomă (ex.: Tesla Autopilot).

## 2. IA generativă (Generative AI) - reprezintă o direcție recentă în DL, concentrată pe *crearea de conținut nou*, pe baza datelor de antrenament. Include:

Generative AI include modele care nu doar clasifică sau prezic, ci creează date noi după pattern-urile învățate în etapa de antrenament. Cele mai populare arhitecturi sunt:

*GANs (Generative Adversarial Networks):* sunt compuse din două rețele neuronale – un generator, care produce exemple sintetice, și un discriminator, care încearcă să distingă datele reale de cele generate. Cele două rețele sunt antrenate într-un sistem de competiție, îmbunătățindu-se reciproc până când generatorul creează exemple de date dificil de diferențiat de cele reale. (Goodfellow et al., 2014). GANs sunt utilizate pentru generarea de imagini realiste, crearea de deepfake-uri și îmbunătățirea conținutului vizual, fiind aplicate în domenii precum producția media, designul digital și simulările realiste.

### *Modele bazate pe transformeri (Large Language Models, LLMs)*

Acestea utilizează mecanismul de self-attention pentru a înțelege dependențele la distanțe lungi în cadrul unui text, permițând generarea de conținut fluent și coerent pe secvențe mari de cuvinte (Vaswani et al., 2017). Exemplu: Chatbot-uri avansate precum ChatGPT pot purta conversații naturale, pot redacta e-mailuri, pot scrie cod sursă sau pot traduce texte, generând totul în mod dinamic în funcție de solicitările utilizatorilor. Modelele generative sunt folosite în crearea de muzică și artă digitală (ex.: DALL-E, Stable Diffusion).

În cadrul inteligenței artificiale, *metodologiile de învățare automată* (Machine Learning și Deep Learning) pot fi clasificate în funcție de modul în care modelele învață din date. Această clasificare include:

- *învățarea supervizată* (supervised learning) – modele antrenate pe date etichetate, utile pentru sarcini precum clasificarea sau regresia;
- *învățarea nesupervizată* (unsupervised learning) – identificarea de tipare sau grupări în date fără etichete (ex: clustering);
- *învățarea prin întărire* (reinforcement learning) – agenți care învață prin interacțiuni cu un mediu și recompense primite pentru acțiuni;
- *învățarea semi-supervizată* – combină date etichetate și neetichetate;

- *învățarea auto-supervizată* – învățarea auto-supervizată reprezintă o metodă prin care modelul „își creează singur sarcina de învățare”, folosind structura internă a datelor brute; un exemplu: în procesarea limbajului natural, modelul învață să prezică următorul cuvânt dintr-o propoziție parțială („Copiii merg la...”) fără a primi etichete externe – generând astfel automat o sarcină de antrenament din datele existente.

Această clasificare nu se aplică întregului domeniu AI, ci este specifică subramurii ML/ DL și reflectă strategiile prin care modelele „învață” din date, și nu tipologia sau nivelul de inteligență al sistemelor.

### **Clasificarea după tipologie: ce nivel de inteligență atinge IA**

În literatură, există un punct de vedere standardizat care împarte IA în trei mari categorii (Russell & Norvig, 2010; Bostrom, 2014) pe baza nivelului de autonomie și capacitatea de generalizare a sistemului:

*ANI (artificial narrow intelligence)* - sisteme specializate care excelează în sarcini înguste și bine definite, fără capacitatea de a generaliza în afara domeniului lor de antrenament. Este singura formă de AI existentă astăzi, fiind utilizată în automatizări industriale, diagnostic medical și recunoaștere facială. Exemple: Siri, Alexa, Google Assistant (recunoaștere vocală, asistență la căutări), Google translate; sisteme de recomandare pentru conținut (Netflix, YouTube), optimizate pentru prezicerea preferințelor utilizatorilor.

*AGI (artificial general intelligence)* - este IA capabilă să învețe și să raționeze la fel ca un om în aproape orice domeniu intelectual. Un AGI ar fi capabil să rezolve sarcini complet noi, fără a fi proiectat special pentru fiecare. În prezent este considerat un concept teoretic, fără implementări funcționale complete la nivel mondial (nicio entitate nu a atins AGI în 2025).

AGI ar trebui să posede capacitatea de învățare și adaptare similară cu cea a unui om, ceea ce implică raționament abstract, creativitate și înțelegerea contextului. Deși AGI nu există încă, modele avansate de AI, precum GPT-4, demonstrează unele caracteristici rudimentare ale AGI.

*ASI (artificial superintelligence)* - inteligență care depășește semnificativ capacitățile cognitive ale oamenilor în aproape orice domeniu (creativitate, planificare, rezolvare de probleme). În prezent, este o entitate ipotetică și subiect de dezbatere privind implicațiile etice și de securitate la scară globală.

ASI este un concept ipotetic, iar Bostrom argumentează că dezvoltarea sa ar putea avea implicații existențiale pentru omenire. ASI nu este doar mai inteligent decât oamenii, ci ar putea depăși orice limită cognitivă umană, având capacități de auto-îmbunătățire.

Această împărțire în ANI/AGI/ASI apare sistematic în articole de conferință și cărți de specialitate, asigurând consistența terminologică și claritatea în comunicarea academică.

În procesul de analiză a inteligenței artificiale se poate observa distincția fundamentală între ceea ce numim *metodologie* și ceea ce definim ca *tipologie*. Cele două concepte nu trebuie confundate, deși ambele contribuie esențial la înțelegerea unui domeniu atât de complex.

Metodologia se referă la *cum* funcționează un sistem inteligent – la tehnicile, modelele și procedurile prin care o mașină poate învăța din date, recunoaște tipare și lua decizii. În acest sens, *ML* nu este doar o subramură a inteligenței artificiale, ci și o strategie concretă de construcție a acesteia, prin adaptare și optimizare continuă.

Tipologia, în schimb, se referă la *ce fel de inteligență* dobândește sistemul – cât de complex, autonom sau adaptabil poate deveni. Clasificările precum ANI, AGI și ASI nu descriu metodele de funcționare, ci nivelul de sofisticare pe care sistemul îl poate atinge în raport cu inteligența umană. Așadar, dacă metodologia este drumul, tipologia este destinația: prima oferă mijloacele tehnice, iar cea de-a doua stabilește reperele conceptuale. Înțelegerea acestei diferențe ajută nu doar la structurarea lecturilor teoretice, ci și la delimitarea clară între fundamentele tehnologice ale IA și proiecțiile sale funcționale și etice în societate.

Inteligența artificială este un domeniu vast, aflat la intersecția tehnologiei, științei și reflecției umane. Înțelegerea diferenței dintre *metodologii* (modul în care IA funcționează) și *tipologii* (nivelul de inteligență atins) este esențială pentru o privire corectă, echilibrată și critică asupra acestei tehnologii. O abordare informată ne permite nu doar să clasificăm sistemele, ci și să evaluăm responsabil modul în care le folosim și le integrăm în viața cotidiană.

### **Ce este și ce NU este inteligența artificială?**

Termenul „inteligență artificială” (IA) este adesea folosit greșit pentru a desemna orice tehnologie digitală modernă. Dar nu orice aplicație software este IA. Pentru ca o tehnologie să poată fi numită astfel, aceasta trebuie să poată învăța din date, să se adapteze la contexte noi și să ia decizii fără a urma exclusiv reguli programate manual.

#### *Când putem spune că este cu adevărat IA*

- Copilot, asistent AI creat de Microsoft, generează răspunsuri originale, învață din context și te sprijină în proiecte educaționale, redactare sau analiză, folosind algoritmi de învățare automată și procesare a limbajului natural.
- ChatGPT și alți asistenți conversaționali avansați , nu oferă răspunsuri prestabilite, ci formulează conținut nou în funcție de întrebare, context și intenția utilizatorului.
- recunoaștere facială automată identifică persoane pe baza tiparelor învățate din seturi masive de date, fără instrucțiuni explicite pentru fiecare caz.
- recomandări personalizate (YouTube, Netflix, Spotify) sunt sisteme ce analizează comportamentul tău și oferă sugestii relevante, învățând permanent din interacțiuni.
- filtru de spam inteligent (ex: Gmail) se antrenează pe baza e-mailurilor marcate manual ca „spam” și își ajustează automat criteriile.
- modelul de detectare a fraudelor bancare se bazează pe anomalii statistice și învățare din cazuri anterioare pentru a identifica riscuri în timp real, învățând permanent cum arată o acțiune „suspectă”.
- diagnostic medical asistat de IA analizează imagini medicale sau date clinice, identificând anomalii pe baza unor algoritmi antrenați, care se perfecționează în timp.

#### *Când NU este IA, chiar dacă sună sofisticat:*

- script în Excel care calculează TVA → Aplică doar formule rigide, fără analiză sau adaptare.
- Chatbot simplu cu răspunsuri fixe („Apasă 1 pentru...”) → Nu învață, nu înțelege și nu personalizează răspunsurile.
- cronometru smart care aprinde lumina la ora 19:00 → Execută o acțiune automată programată, fără luarea în considerare a contextului.

- sistem expert bazat pe reguli „if-then” → De exemplu: „Dacă temperatura > 38°C, trimite alertă”. Nu evoluează, nu își actualizează regulile deși folosește „baze de cunoștințe” și „motor de inferență” (dar nu se bazează pe învățare automată)
- sistem de ticketing care trimite automat e-mailuri → Răspunde automatizat pe baza unor șabloane, fără analiză a mesajelor sau învățare din feedback.
- aplicație care redă remindere la o oră fixă → Nu se adaptează după obiceiuri sau schimbări de program. Execută strict un set de instrucțiuni prestabilite.

Cum recunoști dacă un sistem este IA?

- învață din date – identifică patternuri, generalizează, se corectează.
- se adaptează – reacționează diferit în funcție de utilizator sau situație.
- ia decizii în condiții incerte – nu are nevoie de reguli stricte pentru fiecare caz.
- simulează procese umane – cum ar fi raționamentul, vorbirea, planificarea sau recunoașterea vizuală.

Deci, nu tot ce este digital sau automatizat este IA. IA presupune învățare, adaptare și autonomie în luarea deciziilor. Dacă un sistem doar execută comenzi fixe, nu vorbim despre inteligență artificială. Dacă însă observă, înțelege și se schimbă în funcție de date, atunci da, este o formă autentică de inteligență artificială.

### ChatGPT: arhitectură și funcționare

ChatGPT este un chatbot dezvoltat de OpenAI, construit pe arhitectura Generative Pre-trained Transformer (GPT). Modelul funcționează printr-un proces în trei pași succesivi, susținut de mecanisme interne de învățare profundă.

*Arhitectura sa transformer se bazează pe mecanismul de self-attention, care permite modelului să evalueze importanța fiecărui cuvânt dintr-o propoziție în raport cu toate celelalte cuvinte, indiferent de poziția lor (Vaswani et al., 2017). Prin acest mecanism, ChatGPT înțelege relațiile semantice la nivel global, nu doar local, ceea ce îi conferă capacitatea de a genera texte coerente și contextuale. Self-attention ajută modelul să înțeleagă relațiile dintre cuvinte fără a fi limitat de ordinea lor în propoziție, ceea ce face răspunsurile mai precise și naturale.*

*Transformer Blocks - straturile succesive de rețele neuronale „privesc” simultan întregul text, extrăgând treptat reprezentări tot mai abstracte ale limbajului. Aceste blocuri nu doar identifică structura propozițiilor, ci și îmbunătățesc reprezentarea semantică a frazelor.*

*Positional Encoding - deoarece Transformer-ul nu procesează textul pas cu pas, acest mecanism încorporează informații despre ordinea cuvintelor, astfel încât „Pisica mănâncă peștele” să nu fie interpretat la fel ca „Peștele mănâncă pisica”.*

Dacă un utilizator întreabă „Care este capitala României?”, ChatGPT nu doar caută „România” în baza sa de cunoștințe, ci și recunoaște că „capitala” trebuie corelată cu țara respectivă, returnând răspunsul „București” într-un mod natural.

*Fazele de antrenament ale unui ChatGpt sunt:*

- a. Pre-training - modelul este expus la volume imense de text (Wikipedia, Common Crawl, articole, cărți, forumuri online) cu obiectivul de Language Modeling: prezicerea următorului cuvânt dintr-un context dat. În această etapă, ChatGPT învață reguli gramaticale, structuri lingvistice și cunoștințe generale despre lume, dezvoltând o bază largă de informații. Aceste cunoștințe acumulate rămân „înghețate” la data încheierii antrenamentului.
- b. Fine-tuning - modelul este ajustat pe seturi de date specializate, care conțin exemple de conversații, întrebări-răspunsuri și instrucțiuni specifice. În această fază, ChatGPT îmbunătățește relevanța și coerența răspunsurilor și învață să adapteze textele la cerințele utilizatorilor. Fine-tuning-ul nu doar îmbunătățește conversațiile, ci și ajustează modelul pentru a evita răspunsuri inadecvate sau imprecise. Exemplu: dacă utilizatorul cere „Explică teoria relativității pe înțelesul unui copil”, ChatGPT adaptează răspunsul pentru a fi simplu și ușor de înțeles, în loc să folosească un limbaj academic complex. Chiar așa a răspuns la întrebarea „Explică teoria Chat Gpt unui copil de 5 ani” – „ChatGPT e ca un robot de vorbit care a citit multe cărți și documente. Când tu îi pui o întrebare, el caută în ce a învățat și îți zice un răspuns potrivit, ca și când ai vorbi cu un copil mare care știe foarte multe cuvinte. Nu e un om adevărat și nu are sentimente reale, ci doar știe să potrivească cuvinte ca să îți răspundă. Dacă îl folosești cum trebuie, te poate ajuta să înveți, să te joci cu cuvintele și să descoperi lucruri noi!” (sursa ChatGPT)

### *Retrieval-Augmented Generation (RAG)*

Pentru a furniza informații actualizate, ChatGPT poate folosi un mecanism de RAG, care combină generarea de text cu recuperarea de informații din surse externe:

1. recuperarea informațiilor – la primirea unei întrebări, un retriever neural caută documente relevante într-un index extern (ex.: Wikipedia).
2. îmbogățirea contextului – fragmentele găsite sunt atașate la textul de intrare, astfel încât Transformer-ul procesează simultan datele antrenate și noile informații.
3. generarea răspunsului – modelul produce un răspuns coerent, bazat pe contextul extins, reducând riscul de „halucinații” și asigurând o acuratețe mai mare.

Exemplu: dacă utilizatorul încarcă un document PDF cu date financiare, ChatGPT poate procesa acele informații și răspunde pe baza datelor specifice, nu doar pe baza antrenamentului inițial.

### *Mecanisme de funcționare internă*

- DL – modelul folosește rețele neuronale profunde în ambele faze de antrenament. În timpul antrenamentului, eroarea calculată este propagată înapoi prin rețea (back-propagation), ajustând ponderile interne. Optimizatori precum Adam și RMSProp accelerează procesul de învățare.
- LLMs – GPT-4 conține sute de miliarde de parametri, ceea ce îi permite să surprindă pattern-uri subtile în limbaj și să genereze texte fluente și contextuale.
- ML continuu – feedback-ul utilizatorilor (evaluări, corecturi, conversații reale) este folosit periodic pentru îmbunătățirea modelelor viitoare, asigurând adaptarea la noi situații și subiecte.

Exemplu: dacă utilizatorii corectează frecvent răspunsurile unui chatbot comercial, modelul va învăța să evite acele greșeli în viitor.

ChatGPT este un sistem de IA care a „citit” o cantitate uriașă de texte (cărți, articole, postări online ș.a.) și a învățat din exemplele respective cum să construiască propoziții coerente. Nu are un creier uman, ci o rețea de „neuroni” artificiali care fac calcule matematice pentru a decide ce cuvinte urmează să apară. În loc să memoreze fapte ca un om, ChatGPT analizează texte și reține modele statistice despre cum apar cuvintele împreună: de exemplu, că după „Bună, ce mai faci?” apare aproape întotdeauna „Bine, mulțumesc”. De aici rezultă un model complex care știe, pentru orice secvență de cuvinte, ce cuvinte se potrivesc cel mai probabil după ea. Când îi trimiți un mesaj, acesta este transformat în „tokeni” (fragmente mici de text) și convertit în cifre. Rețeaua de neuroni artificiali procesează aceste cifre și, pe baza calculelor de „atenție”, decide care ar fi continuarea cea mai probabilă și mai potrivită din perspectiva celor învățate. Practic, ChatGPT simulează un fel de joc de „potrivire a modelului”: ia textul tău și, din milioanele de exemple din care a învățat, găsește succesiunea de cuvinte care are sens în acel context. Făcând o analogie cu un puzzle cu milioane de piese putem spune că fiecare piesă e un cuvânt sau o parte de cuvânt. ChatGPT încearcă să potrivească aceste piese pentru a construi o propoziție-„image” coerentă. Nu știe cum arată „imagea” finală în mod explicit, ci plasează piesele de cuvinte în funcție de probabilitățile deduse din textele anterioare. Fiindcă există multe moduri corecte de a formula un răspuns, ChatGPT nu oferă mereu aceeași formulare pentru aceeași întrebare. Fiecare răspuns e rezultatul unui calcul de probabilitate care poate varia ușor de la o rulare la alta. Există și limitări, cum ar fi: modelele se antrenează până la o anumită dată (dacă nu a fost actualizat după 2021, nu „știe” nimic din ce s-a întâmplat după acel an); chiar dacă poate folosi fraze cu emoții („îmi pare rău”, „mă bucur”), nu simte efectiv nimic. Repetă pur și simplu formele de limbaj învățate; nu inventează complet ceva din nimic; orice conținut generat e tot o combinație („remix”) a ideilor și structurilor pe care le-a întâlnit în textele folosite la antrenament.

Inteligența artificială nu este, în esență, o formă autonomă de inteligență, ci o *oglină algoritmică a curiozității umane*. Așa cum subliniază profesorul **Horia F. Pop**, cadru didactic și cercetător la Universitatea Babeș-Bolyai, IA trebuie privită nu ca o amenințare sau o încercare de a înlocui mintea umană, ci ca un instrument de introspecție și reflecție. În viziunea sa, omul va rămâne superior mașinii prin capacitatea de a simți, a raționa și a judeca etic — calități pe care nicio tehnologie nu le poate reproduce integral. Autorul susține această viziune și dintr-o perspectivă filosofică asupra IA, formulată într-un articol dedicat subiectului, unde se argumentează că tehnologia reflectă mai curând dorința profundă a omului de a înțelege cum funcționează propria gândire și inteligența lumii naturale. Această abordare pune accent pe dimensiunea simbolică și cognitivă a IA – ca extensie a minții umane, nu ca substitut al ei. Aceste două viziuni converg spre o concluzie comună: **inteligența artificială nu trebuie mitizată**, ci abordată cu spirit critic, responsabilitate și deschidere interdisciplinară. Astfel, IA nu devine o simplă unealtă tehnologică, ci un teren fertil pentru înțelegerea mai profundă a propriei noastre umanități. (<https://ttc.centre.ubbcluj.ro/interviurile-techtransfer/>; <https://pressone.ro/interviu-la-ce-locuri-de-munca-vor-mai-avea-acces-tinerii-dupa-ce-ai-ul-va-prelua-job-urile-de-incepator>)

Facultativ: dacă doriți să înțelegeți mai multe urmăriți youtube:

1. Clarificare între AI și ML, cu exemple, scurt și eficient, ideal pentru consolidarea celor explicate mai sus

**AI vs Machine Learning** / <https://www.youtube.com/watch?v=4RixMPF4xis>

2. Tipologii de AI: Narrow, General, Super AI + alte clasificări teoretice -

**The 7 Types of AI - And Why We Talk (Mostly) About 3 of Them**  
<https://www.youtube.com/watch?v=XFZ-rQ8eeR8>

3. LLMs (Large Language Models), cum funcționează GPT și rețelele neuronale mari

**How Large Language Models Work** / <https://www.youtube.com/watch?v=5sLYAQS9sWQ>

## Exerciții practice – Capitolul 1

**Obiectiv:** Să înțelegeți și să ilustrați, prin mijloace vizuale, cele trei tehnologii fundamentale din Capitolul 1 — Big Data, Rețele sociale și Inteligență Artificială — precum și modul în care acestea modelează societatea contemporană.

### Tema 1. Creați un nor de cuvinte

#### 1.1 Colectarea termenilor

- lucrați în echipe de 3–4 studenți.
- parcurgeți textul capitolului și selectați cuvinte-cheie care reflectă:
  - caracteristicile tehnologiilor (ex.: „analiză predictivă”, „machine learning”, „algoritm de recomandare”).
  - efectele sociale (ex.: „mobilizare civică”, „polarizare”, „confidențialitate”).

#### 1.2 Generarea norului

- utilizați o platformă gratuită de tip word-cloud (WordArt.com sau WordClouds.com).

*Consultați capitolul 3.1, secțiunea „Nor de cuvinte” pentru instrucțiuni.*

- ajustați dimensiunea fiecărui cuvânt în funcție de frecvența sau de importanța lui în text.
- exportați imaginea și salvați-o sub un nume descriptiv (de exemplu, Nor\_Cuvinte\_Grupa1.png).

### Tema 2. Realizați o hartă mentală (mind-map)

#### 2.1 Structura de bază

- în centrul paginii, scrieți: „**Tehnologii digitale**”.
- trasați trei ramuri principale care pornesc din centrul hărții: **Big Data**, **Rețele sociale**, **Inteligență Artificială**.

#### 2.2 Ramificații secundare

- pentru fiecare tehnologie, adăugați două-trei subramuri pentru a evidenția efectele și aplicațiile discutate în capitol:
  - **Big Data:** „orașe inteligente”, „sănătate personalizată”
  - **Rețele sociale:** „știri false”, „comunități online”

- **Inteligență Artificială:** „deep learning”, „asistenți virtuali”

### 2.3 Conexiuni și note

- desenați săgeți pentru a lega concepte încrucișate:
  - Big Data → recomandări personalizate pe rețele sociale
  - IA → analiză în timp real a datelor
- adăugați scurte explicații sau simboluri care clarifică natura fiecărei legături.

### 2.4 Generarea și salvarea hărții

- utilizați o platformă gratuită (de ex. MindMup sau alta) pentru a crea harta mentală digitală.
- Exportați-o în format imagine (.png/.jpg) sau PDF și salvați-o cu un nume sugestiv (de ex. Harta\_Mentala\_Grupa1.png).

*Consultați capitolul 3.2, secțiunea „Hartă mentală” pentru instrucțiuni.*

## Tema 3. Analiză de caz – impactul unui fenomen digital în societate

**3.1 Alegerea conceptului** - selectați un singur concept din capitol (de ex.: „algoritm de recomandare”, „știri false”, „inteligență artificială” etc.).

### 3.2 Structura analizei (analiza voastră va include):

- selectarea a două studii de caz relevante, din surse credibile (ex.: presă, rapoarte, articole științifice);
- compararea celor două cazuri pe baza a două criterii: a. context diferit (ex.: țară, domeniu, organizație); b. rezultate/opinii diferite (ex.: impact pozitiv vs. negativ); c. alte idei
- identificarea unor asemănări, deosebiri și formularea unor concluzii sau lecții învățate.

### 3.3 Formatare și încărcare

- Textul poate avea structură liberă, dar este recomandat să includă: introducere, analiză comparativă și concluzie.
- Lungimea minimă sugerată: 200 – 350 de cuvinte.
- Salvați lucrarea într-un document Google Docs și asigurați-vă că setarea de partajare este „Orice persoană cu link poate vizualiza” (sau „Editor” dacă profesorul trebuie să comenteze direct).

### *Prezentare generală și organizare teme rezolvate*

- **folderul de lucru:** fiecare grup va crea un folder nou în Google Drive, conform instrucțiunilor primite de la profesor, denumit astfel: Exerciții\_Cap1\_GrupaX (unde „X” este numărul/grupa voastră).
- **conținutul folderului:**
  1. Nor\_Cuvinte\_GrupaX.png (imaginea norului de cuvinte)
  2. Harta\_Mentala\_GrupaX.png (sau PDF/fișier MindMup)
  3. Eseu\_GrupaX.docx sau **link Google Docs** cu eseu complet
- **verificați permisiunile:** înainte de predare, asigurați-vă că profesorul are acces la toate fișierele (vizualizare/comentariu/editare, după cum s-a cerut).

*Consultați capitolul 3.3, secțiunea „Google drive” pentru instrucțiuni.*

## Bibliografie capitolul 1

1. Arockia Panimalar, S., Varnekha Shree, S., & Veneshia Kathrine, A. (2017). The 17 V's Of Big Data. *IRJET*, 04(09).
2. Mitchell, T. M. (1997). *Machine Learning*. McGraw Hill.
3. Russell, S., & Norvig, P. (2010). *Artificial Intelligence: A Modern Approach* (3rd ed.). Prentice Hall.
4. Russell, S. și Norvig, P. (2021). *Inteligența artificială: o abordare modernă* (ediția a 4-a). Pearson.
5. Pariser, E. (2011). *The Filter Bubble: What the Internet Is Hiding from You*. Penguin Press.
6. Gillespie, T. (2018). *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media*. Yale University Press.
7. Nielsen, J. (2015). *Ten Usability Heuristics for User Interface Design*. Nielsen Norman Group.
8. Eyal, N. (2014). *Hooked: How to Build Habit-Forming Products*. Portfolio.
9. Zaharia, M., Chowdhury, M., Franklin, M. J., Shenker, S., & Stoica, I. (2016). Apache Spark: A Unified Engine for Large-Scale Data Processing. *Communications of the ACM*, 59(11), 56–65.
10. Zaharia, M., Das, T., Li, H., Hunter, T., Shenker, S., & Stoica, I. (2020). *Delta Lake: High-Performance ACID Table Storage over Cloud Object Stores*. *Proceedings of the VLDB Endowment*, 13(12), 3411–3423.
11. Bessi, A., & Ferrara, E. (2016). Social bots distort the 2016 U.S. Presidential election online discussion. *First Monday*, 21(11).
12. Del Vicario, M., Bessi, A., Zollo, F., Petroni, F., Scala, A., Caldarelli, G., & Quattrociocchi, W. (2016). The spreading of misinformation online. *PNAS*, 113(3), 554–559.
13. Sunstein, C. R. (2018). *#Republic: Divided Democracy in the Age of Social Media*. Princeton University Press.
14. He, X., Liao, L., Zhang, H., Nie, L., Hu, X., & Chua, T.-S. (2023). Neural Collaborative Filtering vs. Classical Methods: A Survey. *IEEE Trans. on Knowledge and Data Engineering*, 35(7), 3200–3215.
15. Alimardani, M., & Faghih, N. (2019). Automated Hate Speech Detection: A Review of Using NLP Methods. *Journal of Information Security and Applications*, 48, 102353.
16. Doe, J., Nguyen, P., & Li, X. (2024). Real-Time Audio/Video Moderation on Social Platforms. *ACM Trans. on Multimedia Computing, Communications, and Applications*, 20(2), 21.
17. MDPI Computers. (2023). Data Lakes: A Survey of Concepts and Architectures. *MDPI Computers*, 12(2), 45–67.
18. GDPR (Regulamentul UE 2016/679). (2016). Regulamentul Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția datelor cu caracter personal.
19. Lee, C., Patel, R., & Gomez, M. (2023). Hybrid SQL-NoSQL Architectures for GDPR Compliance. *Journal of Data Management*, 36(4), 210–225.
20. Kreps, J., Narkhede, N., & Rao, J. (2011). Kafka: A Distributed Messaging System for Log Processing. *Proceedings of the NetDB*.
21. Kairouz, P., McMahan, H. B., Avent, B., et al. (2021). Advances and Open Problems in Federated Learning. *Foundations and Trends® in Machine Learning*, 14(1–2), 1–210.
22. Vaswani, A., Shazeer, N., Parmar, N., Uszkoreit, J., Jones, L., Gomez, A. N., ... & Polosukhin, I. (2017). Attention Is All You Need. *NeurIPS*, 30, 5998–6008.
23. Jones, L., Gomez, A. N., & Polosukhin, I. (2017). Attention Is All You Need. *Advances in Neural Information Processing Systems*, 30, 5998–6008. <https://arxiv.org/abs/1706.03762>
24. Woolley, S. C., & Howard, P. N. (2017). *Computational Propaganda Worldwide: Executive Summary*. Oxford Internet Institute, [Manual de învățare automată](#)
25. Bostrom, N. (2014). *Superintelligence: Paths, Dangers, Strategies*. Oxford University Press.
26. Bender, E. M., Gebru, T., McMillan-Major, A., & Shmitchell, S. (2021). On the Dangers of Stochastic Parrots: Can Language Models Be Too Big? *ACM FAccT*, 610–623.
27. Ouyang, L., Wu, J., Jiang, X., Almeida, D., Wainwright, C., Mishkin, P., ... & Amodei, D. (2022). Training language models to follow instructions with human feedback. *NeurIPS*, 35.
28. Andrade-Benitez, M., Smith, J., & Rojas, A. (2024). Impact of Gamified UX on Digital Addiction. *Journal of HCI*, 38(7), 1027–1045.

### Alte linkuri

1. Oracle România – Ce este Big Data?- <https://www.oracle.com/ro/big-data/what-is-big-data/>

2. OpenLearn (Open University) – Introducere în Big Data- <https://courses.minnalearn.com/ro/courses/digital-revolution/big-data-and-beyond/introduction-to-big-data/>
3. Archive.org – „Procesarea Big Data” (PDF)- <https://archive.org/details/nicolaesfetcupprocesareabigdata>
4. DiegoNogare – 3D Data Management: Volum, Viteză și Varietate (PDF)- <https://diegonogare.net/wp-content/uploads/2020/08/3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf>
5. Digitalpedia – Definiție Big Data- <https://digitalpedia.ro/definitie/big-data/>
6. TSM – Procesarea fluxului de date în lumea Big Data- (material de curs, PDF)
7. IEEE GRSS – Lecture 5: Big Data Analytics using Apache Spark (PDF)- [https://www.grss-ieee.org/wp-content/uploads/2024/02/Lecture\\_5\\_Big\\_Data\\_Analytics\\_using\\_Apache\\_Spark.pdf](https://www.grss-ieee.org/wp-content/uploads/2024/02/Lecture_5_Big_Data_Analytics_using_Apache_Spark.pdf)
8. AdiBarbu.ro – Ce este o rețea de socializare?- <https://www.adibaru.ro/2015/04/ce-este-o-retea-de-socializare-retea.html>
9. HiWellApp – Efectele pozitive și negative ale rețelelor sociale- <https://www.hiwellapp.com/ro/blog/efectele-pozitive-negative-ale-re%C8%9Belelor-sociale-media>
10. ASECIB – Oportunități și riscuri în rețelele sociale (PDF)- [https://www.asecib.ase.ro/mps/proiecte\\_2015-2016/MiricaMihaelaCorina\\_Oportunitati%20si%20riscuri%20in%20retelele%20sociale.pdf](https://www.asecib.ase.ro/mps/proiecte_2015-2016/MiricaMihaelaCorina_Oportunitati%20si%20riscuri%20in%20retelele%20sociale.pdf)
11. **Socializam.com** – Cum definim o rețea de socializare?- <https://www.socializam.com/blog/cum-definim-o-retea-de-socializare/>
12. Pew Research Center (decembrie 2022) – Social media și democrație- <https://www.pewresearch.org/global/2022/12/06/social-media-seen-as-mostly-good-for-democracy-across-many-nations-but-u-s-is-a-major-outlier>
13. Pew Research Center (iunie 2023) – Activismul pe rețele sociale în SUA-
14. <https://www.pewresearch.org/internet/2023/06/29/americans-views-of-and-experiences-with-activism-on-social-media>
15. Comisia Europeană. (2020). White Paper on Artificial Intelligence: A European approach to excellence and trust. Brussels. [https://commission.europa.eu/system/files/2020-02/commission-white-paper-artificial-intelligence-feb2020\\_en.pdf](https://commission.europa.eu/system/files/2020-02/commission-white-paper-artificial-intelligence-feb2020_en.pdf)
16. Digitalpedia. (2021). Ce este inteligența artificială – definiție și aplicații. <https://digitalpedia.ro/definitie/ai/>
17. McCarthy, J. (2007). What is Artificial Intelligence? Stanford University. <http://www-formal.stanford.edu/jmc/whatisai/>
18. Reuters Institute – Echo Chambers, Filter Bubbles & Polarisation- <https://reutersinstitute.politics.ox.ac.uk/echo-chambers-filter-bubbles-and-polarisation-literature-review>
19. ResearchGate – Filter Bubbles & Fake News (PDF)- [https://www.researchgate.net/publication/354459868\\_Filter\\_Bubbles\\_Echo\\_Chambers\\_and\\_Fake\\_News\\_How\\_Social\\_Media\\_Conditions\\_Individuals\\_to\\_Be\\_Less\\_Critical\\_of\\_Political\\_Misinformation](https://www.researchgate.net/publication/354459868_Filter_Bubbles_Echo_Chambers_and_Fake_News_How_Social_Media_Conditions_Individuals_to_Be_Less_Critical_of_Political_Misinformation)
20. AIMA (Berkeley) – Cuprins complet pentru *Artificial Intelligence: A Modern Approach*- <https://aima.cs.berkeley.edu/contents.html>
21. PCMag – What Is ChatGPT? A Basic Explainer- <https://www.pcmag.com/how-to/what-is-chatgpt-a-basic-explainer>
22. TechRadar – ChatGPT Explained- <https://www.techradar.com/news/chatgpt-explained>
23. OpenLearn (Open University) – Introducere în Inteligența Artificială- <https://courses.minnalearn.com/ro/courses/digital-revolution/big-data-and-beyond/introduction-to-intelligent-systems/>
24. Inteligența artificială și sfârșitul suveranității etice a omului: între autonomie și delegare - Cunoașterea Științifică

## Capitolul 2: Riscuri și provocări în mediul digital - securitate cibernetică, dezinformare, fake news și etică digitală

### 2.1. Securitate cibernetică

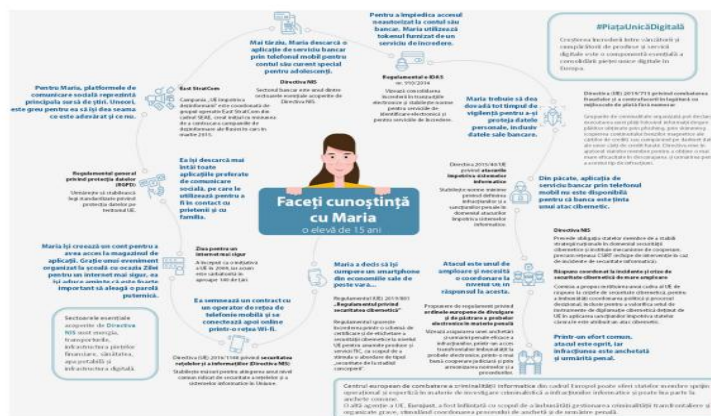
#### 2.1.1. Definiție, impact social și asupra individului

Securitatea cibernetică se referă la ansamblul măsurilor prin care sunt protejate informațiile, dispozitivele și resursele digitale – precum datele personale, conturile online, fișierele, fotografiile sau fondurile financiare – împotriva accesului neautorizat, a pierderii sau a atacurilor informatice. (<https://ici.ro/>)

Securitatea cibernetică înseamnă toate activitățile prin care sunt protejate rețelele, sistemele informatice și utilizatorii acestora împotriva amenințărilor din mediul digital. Ea presupune prevenirea, detectarea și gestionarea incidentelor, precum și revenirea la normal după ce acestea au avut loc. Aceste incidente pot fi cauzate de greșeli umane sau de atacuri intenționate, cum ar fi scurgerile de date, furtul de informații personale, atacurile asupra firmelor sau infrastructurilor esențiale și chiar intervenții în procesele democratice, cum ar fi alegerile sau manipularea opiniei publice prin dezinformare. ([www.contactcommittee.eu](http://www.contactcommittee.eu))

Securitatea cibernetică este o responsabilitate comună, care implică întreaga organizație, iar Uniunea Europeană recunoaște acest lucru prin reglementări ce cer participarea activă a tuturor actorilor, nu doar a departamentului IT.

Imaginea 1 – Modul în care UE susține securitatea cibernetică în viața de zi cu zi a cetățenilor săi



Sursa: Curtea de Conturi Europeană, pictograme realizate de Pixel perfect pornind de la site-ul <https://itaticon.com>.

sursa (Comitetul de contact al instituțiilor supreme de audit din Uniunea Europeană. [www.contactcommittee.eu](http://www.contactcommittee.eu)

Într-o lume în care aproape orice activitate economică, socială sau instituțională este digitalizată, securitatea cibernetică nu mai reprezintă un lux tehnologic, ci o necesitate absolută. În fiecare zi, organizațiile, indiferent de mărime sau domeniu, se confruntă cu amenințări tot mai sofisticate: atacuri de tip ransomware, furt de date, tentative de phishing sau breșe cauzate de erori umane. Aceste amenințări nu mai provin doar de la hackeri izolați, ci și de la grupări organizate sau chiar entități statale. Consecințele unor astfel de atacuri pot fi devastatoare. De la pierderi financiare directe la afectarea reputației sau pierderea încrederii partenerilor și clienților, un singur incident poate destabiliza o întreagă organizație. În plus, într-un peisaj digital tot mai complex, unde procesele de

business se mută în cloud, angajații lucrează de la distanță, iar dispozitivele sunt conectate din diverse locații, riscurile cresc exponențial. La acestea se adaugă și presiunea conformării la reglementări stricte privind protecția datelor, cum este GDPR, care impune nu doar măsuri tehnice, ci și responsabilitate juridică.

În fața acestor provocări, modelele tradiționale de securitate, bazate pe ideea unui perimetru intern sigur, s-au dovedit ineficiente. Perimetrul nu mai este clar definit, iar încrederea acordată automat utilizatorilor sau sistemelor din rețea devine o vulnerabilitate critică. Așa s-a afirmat *modelul Zero Trust*, o nouă paradigmă în securitatea cibernetică. Principiul său fundamental este simplu, dar radical: *niciun utilizator sau dispozitiv nu este de încredere în mod implicit*. Fiecare cerere de acces este verificată riguros, fiecare dispozitiv autentificat, fiecare acțiune monitorizată. Zero Trust nu este doar o soluție tehnică, ci o filozofie de securitate care presupune colaborare interdepartamentală, responsabilitate colectivă și o cultură organizațională activ implicată în protejarea resurselor digitale. Într-o eră în care pierderile globale cauzate de criminalitatea cibernetică sunt estimate la peste 10 trilioane de dolari anual, adoptarea unei abordări proactive și dinamice – precum modelul Zero Trust – nu mai este opțională, ci devine o necesitate strategică pentru supraviețuirea digitală a organizațiilor. (<https://www.connsys.ro/de-ce-nu-poate-fi-ignorata-securitatea-cibernetica/>, [www.sap.ro](http://www.sap.ro), [www.ici.ro](http://www.ici.ro), <https://www.dnsc.ro/>)

*Impactul asupra comunității și societății poate fi rezumat la:*

- eroziunea încrederii în instituții digitale.
- propagarea rapidă a atacurilor cibernetice și a dezinformării.
- inegalități sociale legate de accesul și înțelegerea măsurilor de securitate.
- algoritmi de recomandare care pot amplifica dezinformarea, sporind vulnerabilitatea socială.
- „cetățeni de rang inferior” în societatea digitală dacă nu există educație digitală și acces echitabil la tehnologii de protecție.

*Impactul asupra individului poate fi rezumat la:*

- frică, anxietate, stres generate de amenințările cibernetice.
- pierderea încrederii în mediul digital.
- necesitatea de a dezvolta competențe digitale de bază: gestionarea parolelor, recunoașterea phishing-ului și a atacurilor de tip social engineering.
- impact emoțional amplificat de atacurile asupra încrederii în imagini, video și voce (deepfake).

### 2.1.2. Tipuri de date și vulnerabilități

În rândurile de mai jos enumerăm tipurile de date ce trebuie protejate deoarece pot fi utilizate pentru fraudă, monitorizare sau compromiterea identității.

*Datele personale sensibile*, care pot fi folosite pentru identificare, expunere, fraudă sau discriminare, afectând siguranța și viața privată a unei persoane, includ următoarele:

- *nume complet* – identifică o persoană într-un mod oficial, fiind utilizat în documente, baze de date și interacțiuni legale.

- *cod numeric personal / număr pașaport* – numere unice atribuite fiecărui individ, folosite pentru identificare în registrele statului și în călătorii internaționale.
- *adresă fizică și IP* – permite localizarea geografică și digitală a unei persoane, utilizată pentru livrări, autentificări și acces la servicii online.
- *date financiare: IBAN, număr card, cod CVV* – informații critice pentru tranzacții bancare, expuse riscului de fraudă dacă sunt compromise.
- *date medicale: diagnostic, tratament* – informații despre starea de sănătate, utilizate de medici și instituții medicale pentru îngrijire și istoricul pacientului.
- *preferințe politice, religioase* – opinii și convingeri personale, care pot influența alegeri, afilierea și interacțiunile sociale.
- *istoric de navigare online, locații GPS* – urme digitale care pot dezvălui comportamentul, interesele și deplasările unei persoane.

*Datele biometrice și digitale* sunt caracteristici unice ale unei persoane, folosite pentru identificare, securitate și interacțiuni digitale. Iată câteva exemple:

- *amprentă, retină* – caracteristici unice ale fiecărui individ, folosite pentru autentificare securizată și identificare.
- *recunoaștere facială* - date despre trăsăturile feței utilizate de algoritmi pentru identificare sau verificare, susceptibile la abuzuri de supraveghere.
- *voce (folosită în deepfake)* - înregistrări vocale folosite pentru a recrea vocea unei persoane în scopuri frauduloase sau manipulative.
- *fotografiile personale postate* - imagini încărcate online care pot include informații contextuale despre viața privată și obiceiurile utilizatorului.
- *metadata din poze (data, locația)* - informații ascunse într-un fișier foto (timestamp, coordonate GPS) care dezvăluie când și unde a fost făcută fotografia. De exemplu, timestamp reprezintă data și ora exacte la care a fost realizată fotografia, ajutând la organizarea și verificarea cronologică a imaginilor; iar coordonate GPS indică locația precisă unde a fost făcută fotografia, folosind latitudinea și longitudinea pentru a identifica un punct geografic.

***Alți identificatori digitali*** sunt informații care ajută la recunoașterea și urmărirea unei persoane în mediul online.

Iată câteva exemple, cum ar fi:

- *mailuri și nume de utilizator*: identificatori unici folosiți pentru autentificare și comunicare online, care pot fi asociați direct cu activitatea și profilul unui individ.
- *cookie-uri și sesiuni*: fișiere și token-uri temporare stocate în browser care urmăresc și mențin starea utilizatorului pe site-uri web, facilitând experiența personalizată, dar și colectarea de date despre comportament.
- *conturi sociale (Facebook, LinkedIn, Instagram)*: profiluri pe platforme de social media care expun informații personale, rețeaua de contacte și istoricul interacțiunilor, servind drept hubs de date despre preferințe și activități.
- *adresă MAC a dispozitivelor*: este un identificator unic al dispozitivului de rețea, ca un număr de înmatriculare; ajută routerul să recunoască și să gestioneze conexiunea la net deoarece poate fi văzută atât de routerul (de acasă sau de la birou) cât și de administratorii Wi-Fi-ului

la care ne conectăm (cafenea, aeroport etc); pentru protecție: activează randomizarea MAC (setare frecventă pe telefoane și laptopuri) sau conectează-te doar la rețele cu parolă și criptare (WPA2/WPA3) sau folosește o VPN pentru un plus de siguranță.

*Exploatarea necontrolată a acestor date poate compromite autonomia individuală, afecta dreptul la intimitate și submina încrederea în mecanismele democratice.*

Tabel 1 - comparația între tipurile de identități – fizice/digitale

| <b>Identitate fizică</b>                               | <b>Identitate digitală</b>                                                                                                                                                                                                                                                |
|--------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Bazată pe <b>trăsături biologice</b> (față, CNP, voce) | Reprezentată de <b>date online</b> despre tine                                                                                                                                                                                                                            |
| Controlată de <b>stat, instituții</b>                  | Controlată de <b>platformă, rețele, baze de date comerciale</b>                                                                                                                                                                                                           |
| Protejată prin <b>acte, semnătură</b>                  | Protejată prin <b>parole, autentificare dublă, criptare</b>                                                                                                                                                                                                               |
| <b>Relativ stabilă</b> în timp                         | <b>Fragmentată și duplicabilă</b> (un cont fals poate "prelua" identitatea)                                                                                                                                                                                               |
| Impact fizic, juridic                                  | Impact social, economic, reputațional (ex: „anulare cultura” - printr-un comportament sau o postare considerată inacceptabilă online, un utilizator poate fi „anulat” social – adică ostracizat, blocat, boicotat, iar reputația și chiar veniturile îi pot fi afectate.) |

sursa:proprie

### 2.1.3. Provocări etice și legislative în securitatea cibernetică

Înțelegerea provocărilor etice și legislative din securitatea cibernetică este esențială pentru a garanta respectarea drepturilor utilizatorilor, prevenirea abuzurilor și conformitatea cu legile în vigoare.

#### A. Provocări etice

- *utilizarea datelor biometrice în supravegherea în masă* înseamnă colectarea și analiza automată a amprentelor, secvențelor de iris sau trăsăturilor faciale în spații publice/ private; o dilemă asociată acestui subiect privește echilibrul dintre securitatea colectivă și dreptul la intimitate, precum și riscul de abuzuri, cum ar fi supravegherea politică sau hărțuirea sistematică.
- *comerțul cu date personale pe dark-web sau rețele ilegale* care tranzacționează informații sensibile („package-uri complete” sau segmentate); consecințele sunt de tip fraude bancare, șantaj, furt de identitate și generează risc pentru persoane fizice și organizații (atacuri de tip spear-phishing, ransomware etc).
- *profilarea psihometrică și manipularea electorală sau combinația datelor sociale, demografice și comportamentale* pentru a construi profiluri psihometrice detaliate; o dilemă importantă este: cine stabilește limitele etice ale campaniilor țintite pe rețele sociale? lipsa transparenței poate distorsiona procesul electoral și influența deciziile de vot într-un mod nedemocratic.

#### B. Cadrul legislativ relevant

- *GDPR – Regulamentul General privind Protecția Datelor (UE 2016/679)*

- se aplică tuturor organizațiilor care colectează sau prelucrează date personale în UE.
- principii-cheie: legalitate, echitate, transparență; limitarea scopului prelucrării; minimizarea datelor; exactitatea; stocare limitată; integritate și confidențialitate.
- drepturile persoanelor vizate (art. 12–23): informare, acces, rectificare, ștergere („dreptul de a fi uitat”), restricționarea prelucrării, portabilitate, opoziție, dreptul de a contesta deciziile automate.
- sancțiuni: amenzi de până la 20 milioane € sau 4 % din cifra de afaceri globală. Obligația notificării breșelor de securitate în 72 de ore.

1. DORA – Digital Operational Resilience Act (UE 2022/2554)

- intrat în vigoare din 17 ianuarie 2025, se aplică sectorului financiar și furnizorilor de servicii IT critice.
- obiective: creșterea rezilienței cibernetice, managementul riscurilor digitale, control asupra terților (cloud, platforme software).
- cerințe principale: teste de reziliență cibernetică, raportarea incidentelor majore în 24 de ore, monitorizarea furnizorilor externi critici, planuri de continuitate și recuperare.
- impact direct: securitatea datelor și funcționarea continuă a serviciilor digitale financiare.
- sancțiuni: amenzi similare cu GDPR, restricționarea activității digitale, pierderea încrederii clienților. (Cele 7 principii GDPR. Principii legate de prelucrarea datelor cu caracter personal - GDPR Complet; Sinergii între DORA și GDPR: O abordare cuprinzătoare a securității datelor • EFDPO - Federația Europeană a Responsabililor cu Protecția Datelor)

Tabel 2. Drepturi de protecție a datelor și modalități de verificare

| Drept                                                | Exemplu și modalitate de verificare                                                                                                                                                                                                                                                                                                                                                                             |
|------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Dreptul la informare</b>                          | <b>exemplu:</b> un magazin online îți explică pe pagina de Politica de confidențialitate ce date colectează (nume, adresă, telefon) și de ce le folosește.<br><b>verificare:</b> asigură-te că politica este ușor accesibilă înainte de checkout și că există link clar la ea în footer.                                                                                                                        |
| <b>Dreptul de acces</b>                              | <b>exemplu:</b> ceri băncii un raport complet cu toate datele personale pe care le deține despre tine.<br><b>verificare:</b> banca are obligația să răspundă în 30 de zile, iar răspunsul trebuie să fie pe suport (e-mail sau scrisoare).                                                                                                                                                                      |
| <b>Dreptul la rectificare</b>                        | <b>exemplu:</b> observi un nume sau adresă greșite în contractul de telefonie și ceri corectarea acestora.<br><b>verificare:</b> primești o confirmare scrisă (e-mail sau notificare în contul online) că datele au fost actualizate.                                                                                                                                                                           |
| <b>Dreptul la ștergere („dreptul de a fi uitat”)</b> | <b>exemplu:</b> ștergi contul de pe o platformă de e-learning și firma e obligată să elimine profilul și datele asociate.<br><b>verificare:</b> cere un certificat de ștergere sau un e-mail de confirmare că datele ți-au fost șterse complet.<br><b>Excepție-</b> Platforma poate avea <b>obligații legale de păstrare</b> pentru unele date (ex. facturi), deci nu toate informațiile pot fi șterse complet. |
| <b>Dreptul la restricționare</b>                     | <b>exemplu:</b> în timpul unei reclamații, ceri operatorului telecom să îți „blocheze” datele până la soluționare, fără a le șterge.<br><b>verificare:</b> firma trebuie să confirme în scris că datele sunt marcate ca „înghețate” pentru procesare.                                                                                                                                                           |
| <b>Dreptul la portabilitate</b>                      | <b>exemplu:</b> soliciți operatorului telecom să-ți trimită istoricul convorbirilor și factură într-un fișier CSV ușor de citit și de mutat la alt furnizor.                                                                                                                                                                                                                                                    |

|                                          |                                                                                                                                                                                                                                                                                                         |
|------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                          | <b>verificare:</b> primești fișierul într-un format structurat (CSV, JSON, XML).                                                                                                                                                                                                                        |
| <b>Dreptul de opoziție</b>               | <b>exemplu:</b> primești newsletter de la un magazin online și trimiți o cerere ca să nu mai primești mesaje de marketing.<br><b>verificare:</b> trebuie să existe un link de „unsubscribe” funcțional în fiecare e-mail de marketing.                                                                  |
| <b>Dreptul legat de decizii automate</b> | <b>exemplu:</b> ești respins de un credit bancar pe baza unui scoring automat; poți cere o explicație detaliată a algoritmului și o reevaluare manuală de către un operator uman.<br><b>verificare:</b> banca trebuie să-ți ofere motivele respingerii și opțiunea de a contesta decizia pe cale umană. |

sursa:proprie

#### 2.1.4. Exemple și studii de caz

##### Exemplu 1: DORA în practică – banca X din România

O bancă folosește un furnizor cloud pentru stocarea datelor clienților. Furnizorul suferă un incident tehnic, iar serviciile online pică 24 de ore. Clienții nu pot accesa banii prin aplicația mobilă.

- conform DORA, banca trebuie:
  - să aibă un plan de continuitate digitală deja testat.
  - să evalueze și să monitorizeze permanent riscurile IT ale furnizorilor externi.
  - să raporteze incidentul la autoritatea de supraveghere (BNR sau ASF) în maximum 4 ore.
  - să testeze anual sistemele IT prin simulări de atacuri (penetration testing).
- dacă banca nu respectă DORA: poate fi sancționată cu amenzi, i se poate restricționa activitatea digitală, își pierde reputația.
- pentru client: semnale indirecte că DORA nu e respectat sunt: aplicația bancară pică des, nu primești informări oficiale, banca nu explică transparent situația.

##### Exemplu 2: Atac cibernetic real asupra unei companii românești

Raport **Directoratul Național de Securitate Cibernetică (DNSC)** a vizat companii din domeniul financiar-contabil, folosind spear-phishing și BitLocker pentru criptarea datelor.

###### 1. Spear-phishing și ransomware pe echipamentele firmelor financiare

Atacatorii au trimis *e-mailuri aparent oficiale*, conținând *fișiere PDF malițioase*. Un angajat a accesat atașamentul, iar codul JavaScript ascuns a fost executat, permițând atacatorilor să preia controlul asupra sistemului. Ulterior, aceștia au activat *BitLocker*, criptând toate datele companiei și blocând accesul la fișiere.

###### 2. Consecințe

- pierderi financiare – atacatorii au cerut răscumpărări în criptomonede, iar costurile de recuperare au fost semnificative.
- date confidențiale expuse – informații sensibile despre clienți și tranzacții financiare au fost compromise.
- impact reputațional – încrederea clienților și partenerilor a fost afectată, iar firma a fost nevoită să își revizuiască măsurile de securitate.

###### 3. Măsurile post-incident

- implementarea autentificării multi-factor (MFA) pentru protecția conturilor.
- training obligatoriu pentru angajați privind recunoașterea atacurilor de phishing.
- simulări periodice de phishing pentru testarea reacției angajaților.
- audit extern al infrastructurii IT pentru identificarea vulnerabilităților.

*Informații oficiale despre drepturile tale le poți obține din paginile:*

*1. Regulamentul DORA - varianta oficială UE*

<https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A32022R2554>

*2. Ghid pentru consumatori BNR (reclamații bancare):*

<https://www.bnr.ro> –

Prin email: [sesizare@bnr.ro](mailto:sesizare@bnr.ro)

Prin poștă la adresa BNR din București

Personal la registratura BNR

*3. Platforma ANPC pentru reclamații:*

<https://sesizari.anpc.ro/>

*Unde poți reclama o bancă care nu își protejează serviciile digitale sau datele tale? Autorități din România:*

**Banca Națională a României (BNR)** – dacă e bancă sau IFN - <https://www.bnr.ro/Sesizari-7052.aspx>

**Autoritatea de Supraveghere Financiară (ASF)** – dacă e asigurare sau pensie - <https://asfromania.ro/sesizari>

**Autoritatea Națională pentru Protecția Consumatorilor (ANPC)** – pentru orice abuz legat de serviciile financiare - <https://anpc.ro>

*Alte exemple dacă sunteți interesați se găsesc la linkurile:*

<https://www.asfromania.ro/uploads/articole/attachments/666bea60cd681639758552.pdf>

<https://www.deloitte.com/ro/ro/search-results.html?qr=DORA>

O concluzie care se desprinde: Identitatea digitală este extensia online a persoanei

- ✓ protecția datelor personale este o problemă socială și umană esențială
- ✓ educația digitală și securitatea online devin competențe de bază
- ✓ avem nevoie de legislație și practici etice în protejarea identității digitale
- ✓ datele personale sunt noua monedă în economia digitală.
- ✓ protejarea lor este o responsabilitate individuală și colectivă

## 2.2. Dezinformare și fake news

### 2.2.1. Definiție și clasificarea fenomenului

#### Definiții-cheie

##### 1. Dezinformarea

Distribuirea intenționată a informațiilor false cu scopul manipulării opiniei publice. Este termenul umbrelă care include și fake news cu motivație politică sau comercială.

- *Exemplu:* fabricarea integrală a unui articol despre un politician care nu a făcut niciodată acele declarații, publicat pentru a-i submina reputația și a influența rezultatul unui proces electoral.

##### 2. Fake News

Subcategorie de dezinformare: știri false elaborate deliberat și prezentate ca informații legitime, în principal pentru profit prin click-uri sau cu scopuri politice.

- *Exemplu:* un site care anunță în mod fals moartea unui personaj public, obținând venituri din publicitate prin trafic masiv.

##### 3. Misinformare

Transmiterea neintenționată a unor informații incorecte. Nu există voință de manipulare, însă efectele de confundare pot fi ample.

- *Exemplu:* republicarea din greșală a unui articol vechi despre o criză politică, prezentat ca știre recentă, generând confuzie.

##### 4. Malinformare

Folosirea unor date sau imagini adevărate, dar scoase din context și prezentate în mod manipulativ, cu scop defăimător.

- *Exemplu:* publicarea unei fotografii autentice de acum cinci ani, prezentată ca dovadă a unui eveniment prezent, pentru a induce o impresie greșită.

#### Forme concrete ale manipulării informaționale

| Categorie                | Formă                                  | Descriere & exemplu                                                                                                                                                         |
|--------------------------|----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Manipulare coordonată    | Propaganda digitală                    | mesaje ideologice răspândite coordonat pentru a simula un val de susținere populară, finanțate de grupuri de interese politice sau economice.                               |
|                          | Astroturfing                           | crearea și activarea masivă a conturilor false sincronizate pentru a promova idei, produse sau partide, imitând un curent de opinie „de la bază.”                           |
|                          | Trolling coordonat                     | atacuri online (hărțuire, intimidare) organizate pentru discreditarea unor persoane sau idei și combinarea cu mesaje false pentru a amplifica polarizarea.                  |
| Manipulare prin conținut | Clickbait                              | titluri și previzualizări senzaționale, capcane pentru click-uri, deși conținutul nu corespunde promisiunilor titlului („Nu vei crede ce i s-a întâmplat acestei vedete!”). |
|                          | Information flooding (cenzură inversă) | saturarea mediului digital cu știri irelevante sau false pentru a masca cele legitime și a reduce vizibilitatea dezbaterilor importante.                                    |
| Manipulare tehnologică   | Deepfake                               | utilizarea GAN-urilor pentru a genera materiale audio-video extrem de reale, imitând vocea și imaginea persoanelor publice, folosite în campanii de șantaj sau propagandă.  |

|  |  |                                                                                                                                                                                                                                                                  |
|--|--|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  |  | (GAN - rețele neuronale artificiale formate dintr-un generator, care creează materiale audio-video false extrem de realiste, și un discriminator, care le evaluează autenticitatea, fiind utilizate în aplicații precum deepfake, propagandă digitală și șantaj. |
|--|--|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

După ce am stabilit definițiile și am clasificat principalele forme ale manipulării informaționale, ne îndreptăm acum atenția către mecanismele tehnologice și rețelele care o fac posibilă și o amplifică rapid în mediul digital

### 2.2.2. Mecanisme și tehnologii implicate

#### *Algoritmi și boți*

- boți și conturi false (social bots): rețele automatizate și conturi fabricate, coordonate prin scripturi sau operatori umani, care inundă platformele sociale cu like-uri, comentarii și distribuiri masive, creând iluzia unui consens fals.
- opacitatea algoritmilor: motoarele de recomandare ale platformelor prioritizează conținutul cu potențial emoțional ridicat, fără ca utilizatorii să cunoască criteriile de clasificare, favorizând astfel mesajele care le confirmă prejudecățile.

#### *Tehnici avansate de persuasiune*

- Deepfake: GAN-uri care reproduc cu fidelitate expresiile faciale și tonalitatea vocii unei persoane, permițând fabricarea de clipuri pentru șantaj sau propagandă politică.
- Astroturfing: hardware-ul tehnologic combinat cu strategii de coordonare creează impresia unui val masiv de susținere populară, frecvent utilizat în campanii electorale.
- Microtargeting: colectarea și analiza datelor detaliate despre utilizatori (demografie, comportament online) pentru a livra mesaje personalizate extrem de eficiente și greu de contracara de autorități.

#### *Rolul platformelor sociale în amplificare*

- Rețele principale (Facebook, Twitter, Instagram, TikTok): răspândesc foarte rapid conținutul „viral”; algoritmii lor creează „bule de filtrare” în care utilizatorii văd preponderent mesaje care le întăresc convingerile.
- Grupuri private și aplicații de mesagerie criptată (WhatsApp, Telegram): permit forward-uri nelimitate și circulație necontrolată a informațiilor false, fără monitorizare centrală și cu intervenție dificilă a fact-checker-ilor.

Pornind de la înțelegerea mecanismelor și tehnologiilor care facilitează și amplifică manipularea informațională, ne vom concentra asupra modului în care aceste practici afectează profund gândirea, emoțiile și coeziunea socială.

### 2.2.3. Impact asupra individului și societății

#### *Efectele cognitive și emoționale (anxietate, fragmentarea încrederii)*

- anxietate și stres: expunerea prelungită la știri alarmiste și false (declanșate de algoritmi) produce emoții negative semnificative: teamă, furie și neîncredere în informațiile legitime. Pe termen lung, se apreciază că aceste stări afectează sănătatea mentală și performanța cognitivă.

- efectul de influență continuă: chiar și după deconstrucția unei știri false, reziduurile emoționale (frică, indignare) persistă și pot fi reactivate la întâlnirea unor subiecte conexe. Astfel, percepția inițială falsă continuă să influențeze comportamentul și atitudinile.
- fragmentarea încrederii: odată ce devine dificil să se distingă între sursele credibile și cele false, încrederea reciprocă între cetățeni și autorități se erodează. Această fragmentare duce la rețineri în a colabora sau a avea acord de principiu asupra datelor prezentate, generând instabilitate socială.

#### *Polarizare socială și efectele „camerei de ecou”*

- polarizare socială: diferențele de opinie se accentuează, deoarece știrile false și mesajele care provoacă diviziuni sociale sunt difuzate și amplificate în rândul segmentelor de populație deja orientate ideologic. Aceasta generează tensiuni puternice și duce la formarea unor grupuri antagoniste care refuză dialogul constructiv.
- „camera de ecou” (echo chamber): algoritmi de recomandare direcționează utilizatorii spre conținut care le confirmă propriile convingeri, blocând accesul la perspective alternative. Rezultatul este o concentrare a mesajelor similare, ceea ce reduce capacitatea indivizilor de a evalua critic informațiile și de a înțelege argumente contradictorii.

#### *Distorsiunea percepției realității și luarea deciziilor informate*

- distorsiunea percepției realității: consumatorii de informații false ajung să creadă în scenarii fabricate (de ex. anumite teorii conspiraționiste) și să refuze datele verificate de experți. Această eroare de percepție afectează judecata individuală și colectivă, conducând la decizii nesănătoase în domenii precum sănătate sau viața civică.
- luarea deciziilor eronate: pe baza informațiilor false, indivizii pot adopta comportamente dăunătoare: neparticiparea la campanii de vaccinare, investiții în scheme financiare piramidale, boicot politic sau social bazat pe mituri și zvonuri. Aceste decizii se pot extinde la nivel macro, subminând eforturile de guvernare și sănătatea publică.

Având în vedere efectele dezinformării asupra individului și coeziunii sociale, următorul pas este să analizăm dilemele etice și cadrul normativ necesar pentru a o contracara.

#### **2.2.4. Provocări etice și legislative în combaterea dezinformării**

##### *Limitele dintre libertatea de exprimare și reglementarea conținutului*

- Dilemă: echilibrul între protejarea dreptului fundamental la libertatea de exprimare și prevenirea diseminării știrilor false este fragil. Dacă intervenția autorităților sau a platformelor devine excesivă, se ajunge la cenzură și limitarea discursului public. Dacă, dimpotrivă, nu se exercită nicio formă de control, dezinformarea proliferază necontrolat.
- Exemplu legislativ:
  - Regulamentul (UE) 2022/2065 – Digital Services Act - obligă platformele mari să retragă „fără întârziere nejustificată” conținutul ilegal (discurs de ură, terorism, exploatare sexuală a copiilor etc.), dar fără a stabili un interval cert de 24 de ore și fără sancțiuni naționale uniforme pentru fiecare zi de întârziere.

- Legea nr. 365/2002 (transpunerea Directivei e-commerce) - furnizorii de găzduire trebuie să blocheze sau să șteargă imediat materialele reclamate ca ilegale, la sesizarea titularilor de drepturi sau a autorităților, însă fără un mecanism central de monitorizare și fără amenzi prevăzute direct în textul de lege.

Astfel, deși principiile de rapiditate a reacției există în legislația europeană și cea de transpunere, România nu are, deocamdată, o reglementare națională care să combine termene clare de 24 de ore cu sancțiuni automate.

#### *Responsabilitatea platformelor digitale și actorilor politici*

- Platforme digitale: Facebook, Twitter, YouTube, TikTok și alte servicii majore au rolul de a modera conținutul, dar standardele variază. Lipsa transparenței privind criteriile de moderare generează suspiciuni în rândul utilizatorilor și teama că algoritmi ar putea favoriza un anumit punct de vedere politic sau comercial.
- Opacitatea algoritmilor: utilizatorii nu știu exact cum sunt prioritizate știrile în feed-urile lor, iar această lipsă de claritate poate fi exploatată de actori rău-intenționați pentru a amplifica dezinformarea.
- Actorii politici: partidele și candidații pot folosi conturile oficiale pentru a lansa mesaje false și pentru a exercita presiune electorală prin microtargeting. În absența unor reglementări stricte, aceste practici pot submina corectitudinea proceselor electorale și încrederea în democrație.

#### 2.2.5. Exemple și studii de caz

##### **Exemplu 1 - Analiza cazului „Fake news despre o pană de curent la nivel european (2021)”**

**1. Definiție – ce tip de informație falsă este?** - acest incident intră în sfera **misinformării**, întrucât informația falsă nu a fost răspândită cu intenția deliberată de manipulare, ci a rezultat dintr-o traducere eronată a unui comunicat oficial al Ministerului Apărării din Austria. Textul original – un anunț privind un exercițiu de pregătire pentru întreruperi de energie – a fost tradus drept o „avertizare reală” despre o pană de curent iminentă. Rezultatul a fost un titlu de senzație care a declanșat panică și redistribuiri masive, deși autorii inițiali nu urmăreau decât exercițiul de simulare.

**2. Tipologie – cum se încadrează în formele de manipulare informațională?**

- Clickbait: titlurile senzaționaliste gen „Până de curent totală în Europa chiar azi?” au atras atenția, deși nu corespundeau realității.
- „umbrirea” informațiilor esențiale (overshadowing): volumul mare de articole și postări alarmiste a suprasaturat canalele de știri, eclipsând explicațiile oficiale și făcând dificilă accesarea comunicatului corect.
- propagare virală prin rețele sociale: mesajul a fost preluat și multiplicat pe Facebook, WhatsApp și Telegram, creând impresia unei crize reale.

**3. Mecanisme – cum s-a propagat informația falsă?**

1. traducerea greșită: textul privind un exercițiu de pregătire a fost interpretat ca avertisment veridic.

2. preluarea necritică de către presă: mai multe site-uri au publicat rapid titlul tradus eronat, fără să verifice cu originalul german. Un exemplu: „Europa rămâne fără curent mâine” apărut pe un portal de știri centrale.
3. distribuirea masivă pe rețele sociale: sute de grupuri de WhatsApp și Telegram au redistribuit articolul „oficial”, generând zeci de mii de share-uri în câteva ore.
4. lipsa unei corecturi cu efect: deși Ministerul Apărării a emis un drept la replică în 8 ore, jumătate din publicul activ în continuare credea în veridicitatea știrii, din cauza propagării informațiilor în feed-uri și notificări.

#### **4. Legislație – ce reglementări se aplică în România?**

- Legea nr. 365/2002 (transpunerea Directivei e-commerce): obligă furnizorii de hosting și platformele sociale să șteargă „fără întârziere nejustificată” conținut reclamat ca ilegal (defăimare, discurs de ură, drepturi de autor etc.), dar nu sancționează în mod expres misinformarea neintenționată.
- Regulamentul (UE) 2022/2065 – Digital Services Act (DSA): aplicabil din 2024, impune platformelor mari să instituie proceduri de notificare și retragere rapidă a conținutului ilegal sau fals, însă fără a stabili un termen precis de 24 h și fără amenzi locale uniforme.
- Codul penal, art. 404 („comunicarea de informații false”): prevede sancțiuni doar pentru situații în care diseminarea de informații false amenință ordinea publică sau securitatea națională; până în prezent nu s-au înregistrat condamnări pentru misinformare prietenoasă (eroare de traducere), ci doar pentru acte deliberate de propagandă.

#### **Concluzie**

Deși acest caz nu a fost unul dezinformator cu intenție, ci rezultatul unei erori de traducere și al unei preluări necritice, consecințele – panică publică, umbre în accesul la informațiile oficiale și creșterea neîncrederii în instituții – au fost similare celor ale unei campanii deliberate de fake news.

Surse: <https://www.veridica.ro/en/fake-news-disinformation-propaganda/fake-news-europe-on-the-brink-of-a-catastrophic-power-outage>

#### **Exemplu 2 - Analiza cazului „Fake news despre colapsul monedei euro (2022)”**

**1. Definiție** – ce tip de informație falsă este? - acest caz se încadrează în dezinformare, deoarece s-a urmărit intenționat manipularea opiniei publice și a piețelor financiare printr-o serie de articole și postări care pretindeau că euro „se prăbușește” și că statele membre se pregătesc să revină la monedele naționale.

**2. Tipologie** – cum se încadrează în formele de manipulare informațională?

- malinformare: s-au preluat date reale (o scădere temporară a euro în raport cu dolarul), dar s-a oferit interpretare alarmistă, scoasă din context, pentru a induce panică.
- propaganda economică: conturi și site-uri obscure au amplificat mesajul, cu scopul de a submina încrederea în stabilitatea UE.
- clickbait: titluri senzaționaliste de genul „Euro în colaps total – ultima șansă pentru state!” au atras trafic masiv.

**3. Mecanisme** – cum s-a propagat informația falsă?

1. grafice scoase din context: unii autori au folosit grafice cu deprecieri pe perioade restrânse, prezentându-le drept prăbușirea definitivă a monedei.

2. amplificare pe rețele sociale: mesaje virale pe Facebook, Twitter și Telegram, deseori redistribuite de conturi automate și grupuri de speculatori.
  3. preluare de către site-uri obscure: platforme fără tradiție jurnalistică au publicat articole alarmiste, fără verificarea sursei primare.
  4. reacția oficială – dezmințire: Banca Centrală Europeană a emis un comunicat prin care a subliniat că nu există niciun semnal de „colaps”, ci fluctuații normale într-un context de inflație și divergențe de politică monetară ([reuters.com](https://www.reuters.com)).
- 4. Legislație** – ce reglementări se aplică în România și UE?
- Digital Services Act (UE 2022/2065): impune platformelor mari să raporteze și să retragă rapid conținutul dezinformator, inclusiv cel economic, chiar dacă intervalul de „24 h” nu este explicit prevăzut la nivel național.
  - Legea nr. 365/2002 (transpunerea Directivei e-commerce): obligă furnizorii de găzduire să elimine „fără întârziere nejustificată” conținutul reclamat ca ilegal, ceea ce poate acoperi și dezinformarea cu impact economic.
  - Codul penal, art. 404 („comunicarea de informații false”): prevede sancțiuni pentru informațiile false care amenință securitatea națională sau stabilitatea economică; aplicarea sa însă rămâne rară și strict în cazuri grave.

Surse:

„Fake: EU Will ‘Collapse’ after...”, StopFake.org – explică modul în care propaganda rusă și alte surse alternative au inventat scenariul de „colaps al UE” ([stopfake.org](https://stopfake.org)).

Reuters, „Euro logs one-month high after Trump delays EU tariffs” (26 mai 2025) – articol care arată că euro a atins un maxim lunar, contrazicând categoric ideea de „colaps” ([reuters.com](https://www.reuters.com)).

## Concluzie

Dezinformarea despre o „prăbușire a euro” în 2022 a fost construită prin selectarea datelor reale și interpretarea lor într-un context fals, sprijinită de clickbait și conturi sprijinite de boți. Deși autoritățile europene și BCE au reacționat rapid, cazuri de acest tip indică necesitatea consolidării mecanismelor de verificare și a educației media economice pentru publicul larg.

## 2.3. Etică digitală

### 2.3.1. Definiție și cadru conceptual

În sens filozofic, etica este disciplina care investighează principiile și valorile ce permit distincția între bine și rău și justificarea normelor morale (Kant, 1785). În contextul TIC, noțiunea de „etică digitală” se concentrează pe responsabilitatea actorilor implicați – programatori, ingineri, companii, instituții publice și utilizatori – în gestionarea datelor, algoritmilor și consecințelor sociale ale aplicațiilor digitale (Wiener, 1950; ACM, 1972).

- *responsabilitate digitală*: capacitatea tuturor participanților la ecosistemul digital de a asigura tratamentul etic al datelor cu caracter personal, respectarea drepturilor fundamentale și prevenirea abuzurilor tehnologice.
- *valori fundamentale*: confidențialitate, transparență, echitate, responsabilitate și autonomie umană.

Într-o lume în care fiecare acțiune online produce date (internetul lucrurilor, rețele sociale, tranzacții electronice), etica digitală devine cadrul care fundamentează reguli și proceduri pentru a preveni riscurile sociale și individuale generate de tehnologie (Floridi, 1999).

### 2.3.2. Evoluție istorică (sinopsis cronologic)

Evoluția eticii digitale poate fi urmărită prin câteva etape cheie:

| Perioadă                 | Evenimente și concepte principale                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Anii 1950–1960</b>    | Norbert Wiener – <i>The Human Use of Human Beings</i> (1950): primele preocupări etice în cibernetică, definind interacțiunea armonioasă între om și mașină și necesitatea ca tehnologia să servească umanitatea, nu doar logica profitului .                                                                                                                                                                                                                                                                                                                                             |
| <b>Anii 1970–1980</b>    | <i>Codul de Etică ACM</i> (1972): primul cod oficial de conduită profesională în informatică, pune accent pe integritate, confidențialitate și binele societății. \n• Fundamentează conceptul că programatorii și inginerii au responsabilitate morală în proiectarea și exploatarea sistemelor informatice .                                                                                                                                                                                                                                                                             |
| <b>Anii 1980–1990</b>    | „Computer Ethics” devine domeniu de studiu academic și profesional. \n• First Conference on Computer Ethics (1980) la Case Western Reserve University: reunește experți pentru a dezbate dileme legate de piraterie software, securitatea datelor și drepturile de autor. \n• <i>Deborah Johnson, Computer Ethics</i> (1985): definește cadrul teoretic al eticii informaticii. Fondarea <i>Computer Ethics Institute</i> (1992) și elaborarea „Ten Commandments of Computer Ethics”.                                                                                                     |
| <b>Anii 1990–2010</b>    | Expansiunea internetului: Directiva 95/46/CE (1995) („Protecția datelor cu caracter personal”): primul cadru european pentru colectarea, utilizarea și securizarea datelor personale, echilibrând protecția vieții private cu libera circulație a informațiilor. \n• Incidente majore de viruși (Melissa, 1999; ILOVEYOU, 2000) scot în evidență riscurile securității cibernetice.                                                                                                                                                                                                       |
| <b>Anii 2010–prezent</b> | Apariția și răspândirea inteligenței artificiale și a rețelelor neuronale profunde: provocări legate de <i>bias</i> algoritmic și transparență. <i>GDPR</i> (2018): reglementare europeană care consolidează drepturile persoanelor vizate și introduce obligații stricte pentru operatorii de date. \n• <i>Asocierea UNESCO – Recommendation on the Ethics of Artificial Intelligence</i> (2021): principii pentru IA etică. \n• Propunerea de <i>AI Act</i> (COM (2021) 206): text legislativ UE care impune cerințe de echitate, transparență, robustețe și audit pentru sistemele IA. |

### 2.3.3. Principii normative și responsabilități digitale

Etica digitală stabilește un cadru de valori și reguli care guvernează interacțiunile în mediul online, integrând principii normative, responsabilități digitale și transparența algoritmică, pentru a asigura echitatea, protecția drepturilor și utilizarea etică a tehnologiilor emergente.

#### Drepturi digitale

- Libertatea de exprimare online - dreptul fiecărui utilizator de a comunica opinii, idei și informații pe platformele digitale fără cenzură arbitrară, cu respectarea însă a demnității și siguranței celorlalți.

- Acces echitabil la resurse digitale - garantarea accesului nediscriminatoriu la internet, la conținut educațional și la instrumente digitale, indiferent de factori socio-economici sau geografici.
- Protecția datelor personale - dreptul individului de a controla modul în care datele sale personale sunt colectate, stocate, procesate și partajate, inclusiv primirea de informații clare privind scopurile prelucrării și posibilitatea retragerii consimțământului.

### **Responsabilități digitale**

- Fact-checking și veridicitate - obligația morală de a verifica corectitudinea informațiilor înainte de a le publica sau redistribui, pentru a preveni răspândirea știrilor false și manipularea opiniei publice.
- Securitate informațională - angajamentul de a adopta practici de securitate (parole complexe, criptare, actualizări regulate) și de a raporta vulnerabilitățile pentru a proteja confidențialitatea și integritatea datelor.
- Respectul proprietății intelectuale- recunoașterea și protejarea drepturilor de autor și a brevetelor în mediul digital, prin utilizarea licențelor adecvate și prin evitarea pirateriei software și a plagiatului .

### **Transparență și echitate în algoritmi**

Pentru a asigura utilizarea responsabilă a sistemelor automate și a inteligenței artificiale, este esențială implementarea unor standarde de transparență și echitate:

- explicabilitate (XAI) - cerința ca deciziile automatizate să poată fi explicate în termeni accesibili factorilor de decizie și utilizatorilor finali, astfel încât criteriile și pașii algoritmici să fie auditați și înțeleși.
- auditabil și acces la datele de instruire - capacitatea sistemului de a permite verificări (auditabil) și procesul efectiv de audit asupra modelelor, precum și posibilitatea de consultare a seturilor de date folosite pentru instruire (posibilitatea de a examina seturile de date și metodologiile folosite în antrenarea modelelor de IA, pentru a evalua imparțialitatea, calitatea și reprezentativitatea acestora).
- bias algoritmic și mecanisme de remediere - identificarea sistematică a părtinirilor provenite din datele de antrenament sau din structura modelelor predictive și aplicarea de tehnici de corecție (re-echilibrare a datelor, eliminarea caracteristicilor discriminatorii, retraining) pentru prevenirea discriminării rasiale, de gen sau socio-economică.

#### **2.3.4. Provocări etice ale inteligenței artificiale**

Am împărțit analiza provocărilor etice pe două paliere — mai întâi rețelele sociale, apoi inteligența artificială — pentru că dinamica interacțiunilor umane online și impactul algoritmilor se manifestă diferit în fiecare context, iar înțelegerea succesivă a modului în care platformele conectează utilizatorii precede discuția despre efectele tehnologiilor automate care stau la baza acestor rețele.

#### **Rețele sociale**

- bule informaționale - algoritmii de recomandare favorizează conținut similar cu preferințele utilizatorilor, izolându-i în grupuri omogene și amplificând polarizarea discursului public.

- confidențialitate și supraveghere - colectarea masivă de date personale (profilare comportamentală, recunoaștere facială, metadata) afectează dreptul la intimitate și ridică întrebări despre cine și în ce condiții poate accesa aceste informații.
- discurs instigator la ură și cyberbullying – lipsa unor mecanisme eficiente de moderare și a unor standarde clare duc la proliferarea limbajului discriminatoriu și a hărțuirii online, punând în pericol demnitatea și siguranța utilizatorilor.
- dependență digitală - funcționalitățile de tip „gamification” (like-uri, notificări constante) exploatează vulnerabilitățile psihologice ale utilizatorilor, generând consum excesiv de conținut și afectând sănătatea mintală, în special a tinerilor.
- dezinformare - distribuirea rapidă a știrilor false sau manipulate subminează încrederea în mass-media și instituții, necesitând echilibrarea libertății de exprimare cu responsabilitatea platformelor de a detecta și limita conținutul fals.

### **Inteligență artificială**

- decizii automate și responsabilitate legală - când un sistem IA produce un rezultat eronat (de ex. un vehicul autonom într-un accident), nu este clar cine răspunde: dezvoltatorul, producătorul sau utilizatorul, ceea ce impune reglementări de „om în buclă” și noi cadre juridice.
- securitate și reziliență (adversarial ML) -modelele de învățare automată pot fi deturnate prin exemple adversariale, compromițând integritatea și fiabilitatea sistemelor, de aceea e nevoie de mecanisme defensive robuste și testări de rezistență.
- deepfake și manipulare a opiniei publice - tehnologiile de generare a conținutului fals (imagini, video, audio) permit crearea de materiale convingătoare care pot fi folosite pentru dezinformare masivă, iar detectarea automată trebuie completată de reglementări și conștientizare civică.

#### **2.3.5. Cadrul de reglementare internațional și european**

Secțiunea următoare asigură tranziția de la teorie la practică, arătând cum legile și ghidurile (GDPR, AI Act, NIS, DORA etc.) răspund concret acestor probleme. Astfel, cititorul înțelege atât natura dilemelor morale din rețele sociale și IA, cât și cerințele normative care trebuie respectate pentru dezvoltarea responsabilă a tehnologiilor digitale.

1. **UNESCO – *Recommendation on the Ethics of Artificial Intelligence (2021)***: stabilește principii-cheie pentru dezvoltarea responsabilă a IA, incluzând echitatea, transparența, responsabilitatea și protecția drepturilor fundamentale, și recomandă mecanisme independente de supraveghere și audit al sistemelor IA.
2. **Comisia Europeană – Ethics Guidelines for Trustworthy AI (2019)**: definește șapte piloni ai unei inteligențe artificiale de încredere — respectarea drepturilor fundamentale, transparență, echitate, protecția datelor, robustețe și siguranță, responsabilitate și guvernare — și oferă recomandări de evaluare a riscurilor și proceduri de audit pentru dezvoltatori și factorii de decizie.
3. **AI Act (COM (2021) 206)**: propune clasificarea aplicațiilor IA după nivelul de risc (inacceptabil, ridicat, limitat, minimal), interzicerea celor cu risc inacceptabil și impune cerințe stricte de audit, explicabilitate și supraveghere umană pentru sistemele cu risc ridicat.

4. **Regulamentul General privind Protecția Datelor (GDPR, 2018):** instituie consimțământul explicit, principiul minimizării datelor, dreptul la portabilitate și interzice deciziile automate cu efecte semnificative fără intervenție umană, garantând transparența proceselor de prelucrare.
5. **Alte reglementări de securitate cibernetică (DORA, NIS, etc.):** includ cerințe de reziliență și reacție la incidente pentru furnizorii de servicii digitale și instituțiile financiare, vizând asigurarea continuității operațiunilor și gestionarea riscurilor cibernetice la nivel european.

Pentru referințe suplimentare, poți consulta:

- UNESCO – Recommendation on the Ethics of Artificial Intelligence (2021): [UNESCO AI Ethics Recommendation](<https://www.unesco.org/en/articles/recommendation-ethics-artificial-intelligence>)
- Comisia Europeană – Ethics Guidelines for Trustworthy AI (2019): [Ethics Guidelines for Trustworthy AI](<https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai>)
- AI Act (COM (2021) 206)\*\*: [Propunerea de regulament AI Act](<https://eur-lex.europa.eu/legal-content/RO/TXT/HTML/?uri=CELEX:52021PC0206>)
- Regulamentul General privind Protecția Datelor (GDPR, 2018): [GDPR pe EUR-Lex](<https://eur-lex.europa.eu/RO/legal-content/summary/general-data-protection-regulation-gdpr.html>) &#124; EUR-Lex](<https://eur-lex.europa.eu/RO/legal-content/summary/general-data-protection-regulation-gdpr.html>)
- Reglementări de securitate cibernetică (DORA, NIS, etc.): [Compararea Directivelor NIS și DORA]([https://decalex.ro/blog/nis-vs-dora\\_romania](https://decalex.ro/blog/nis-vs-dora_romania))

Exemple:

*Caz 1: Abuzul de date personale pe Facebook – scandalul Cambridge Analytica (2018)*

- o *Descriere:* Compania *Cambridge Analytica* a colectat datele personale a peste 87 de milioane de utilizatori Facebook fără consimțământul explicit și le-a folosit pentru a construi profile psihometrice, în scopuri de microtargeting politic.
- o *Impact etic:* încălcarea profundă a confidențialității, manipularea conștiinței electorale și pierderea încrederii cetățenilor în platformele sociale.
- o *Măsuri:* Anchete legislative (Comisia US pentru Comerț a audiat CEO-ul Facebook), amendă GDPR de 500 000 £ pentru încălcarea vieții private (UK Information Commissioner’s Office) și creșterea cerințelor de transparență în alocarea datelor.

*Caz 2: Vehicul autonom Uber – deces provocat de IA (2018)*

- o *Descriere:* În martie 2018, un vehicul autonom Uber a accidentat mortal o pietonă în Tempe, Arizona. Ancheta a arătat că sistemul IA nu a recunoscut corect pietonul și nu a inițiat frânarea la timp.
- o *Impact etic:* dilemă privind cine răspunde moral și legal – programatorul, compania sau sistemul IA. De asemenea, ridică întrebarea protejării vieții umane versus eficiența tehnologică .
- o *Măsuri:* îmbunătățirea senzorilor, includerea unui operator uman „în buclă” (human-in-the-loop), revizuirea protocoalelor de testare și reglementarea mai strictă a testării pe drumurile publice de către autoritățile competente .

*Caz 3: Scandalul „Vineri Neagră” – discriminare algoritmică în credit scoring (2022)*

- *Descriere*: O bancă europeană a folosit un model IA de credit scoring care, pe baza istoricului de consum și a caracteristicilor demografice, a respins automat cererile de credit ale tinerilor din medii socio-economice defavorizate. Ancheta realizată de Financial Times a demonstrat că modelul favoriza persoanele cu venituri ridicate și stabile, consolidând inegalitățile existente.
- *Impact etic*: încălcarea principiului de echitate, perpetuarea excluziunii financiare și discriminarea indirectă a grupurilor vulnerabile.
- *Măsuri*: banca a adaptat modelul IA pentru a include variabile care țin cont de contextul socio-economic și a introdus auditurile etice periodice ale modelelor de credit scoring; autoritățile de reglementare au impus cerința de evaluare a discriminării algoritmice conform AI Act (COM (2021) 206).

**Facultativ** - curs tutorial on-line: [The common good – calculating consequences - Ethics of AI](#)

## Exerciții practice – Capitolul 2

**Obiectiv**: Să înțelegeți și să ilustrați, prin mijloace vizuale și de dezbatere, principalele concepte din Capitolul 2—securitatea cibernetică, dezinformarea și etica digitală—și modul în care acestea modelează societatea contemporană.

### Tema 1 Creați un nor de cuvinte

#### 1.1 Colectarea termenilor

- lucrați în echipe de 3–4 studenți.
- parcurgeți textul capitolului și selectați cuvinte-cheie care reflectă: securitatea cibernetică (ex.: „confidențialitate”, „integritate”, „ransomware”, „phishing”); // dezinformare și fake news (ex.: „boți sociali”, „microtargeting”, „deepfake”, „echo chamber)

#### 1.2 Generarea norului

- utilizați o platformă gratuită de tip word-cloud (WordArt.com sau WordClouds.com).

*Consultați capitolul 3.1, secțiunea „Nor de cuvinte” pentru instrucțiuni.*

- ajustați dimensiunea fiecărui cuvânt în funcție de frecvența sau de importanța lui în text.
- exportați imaginea și salvați-o sub un nume descriptiv (de exemplu, Nor\_Cuvinte\_Cap2\_GrupaX.png).

### Tema 2. Realizați o hartă mentală (mind-map)

#### 2.1 Structura de bază

- în centrul paginii, scrieți: „Riscuri digitale”
- trasați două ramuri principale care pornesc din centrul hărții:
  1. Securitate cibernetică
  2. Etica digitală

#### 2.2 Ramificații secundare

- pentru fiecare ramură principală, adăugați două–trei subramuri pentru a evidenția conceptele și exemplele discutate în capitol:

1. Securitate cibernetică: „malware”, „phishing”, „ransomware”; tipuri de date vulnerabile: „date personale sensibile”, „date biometrice”; dileme etice: „supraveghere vs. confidențialitate”, „comerț cu date pe dark web”
2. Etica digitală: principii fundamentale: „drepturi digitale”, „autonomie personală”, „responsabilitate”; provocări în rețele sociale: „bule informaționale (echo chambers)”, „hărțuire online”; provocări în IA: „bias algoritmic”, „explicabilitate (XAI)”, „responsabilitate legală”

### 2.3 Conexiuni și note

- desenați săgeți care leagă concepte încrucișate: • Securitate cibernetică → Etica digitală: responsabilitatea platformelor de social media în moderarea conținutului fals • Etica digitală → Securitate cibernetică: dilema transparenței algoritmilor de detecție malware versus secretul comercial al firmelor de securitate
- adăugați scurte explicații lângă fiecare săgeată pentru a clarifica natura legăturii

### 2.4 Generarea și salvarea hărții

- utilizați o platformă gratuită (de ex. MindMup) pentru a crea harta mentală digitală.
- exportați-o în format imagine (.png/.jpg) sau PDF și salvați-o cu un nume sugestiv (de ex. Harta\_Mentala\_Cap2\_GrupaX.png).

*Consultați capitolul 3.2, secțiunea „Hartă mentală” pentru instrucțiuni.*

## Tema 3. Întrebări dezbateri – orientare spre studiu de caz

### 3.1 Cum identificăm o știre falsă (dezinformare)?

**Studiu de caz:** afișați un exemplu de postare virală pe Facebook sau TikTok despre un eveniment social/politic suspect de falsitate.

#### Pași de analiză:

- a. verificați sursa primară - identificați pagina sau contul de unde provine mesajul și istoricul acestuia; aplicați tehnici de fact-checking și fast-checking - cum ar fi: reverse image search (pentru a descoperi originea imaginilor și a identifica versiuni precedente) sau fast-checking cu instrumente online (ex. Google Fact Check Tools, InVID) care detectează rapid semnale de alarmă (titluri click-bait, corelări cronologice, metadate incoerente).
- b. căutați comunicate oficiale sau articole verificate care contrazic afirmațiile.
- c. examinați etichetele de verificare („fact-checked”) aplicate de organizații independente (PolitiFact, AFP Fact Check etc.) (Verificarea faptelor).
  - a. Consultați comentariile și link-urile oferite de alți utilizatori pentru contra-probe.

#### Întrebări de discuție:

Cum distingem opiniile personale de știrile autentice?

În ce măsură algoritmiile rețelelor sociale amplifică știrile false?

Ce pași trebuie să urmeze un utilizator înainte de a da „like” sau „share”?

### 3.2 Suntem responsabili pentru distribuirea informațiilor neverificate?

**Studiu de caz:** O postare falsă despre o persoană/companie locală este preluată de sute de utilizatori și provoacă pierderi de imagine și financiare.

#### Pași de analiză:

- a) urmăriți traseul dezinformării: cine a postat inițial, cine a dat share și unde s-a viralizat.

- b) identificați punctele unde fact-checkerii, mass-media sau autoritățile ar fi putut interveni.
- c) evaluați pagubele și propuneți măsuri: fact-checking proactiv, educație digitală și politici ale platformelor.

#### **Întrebări de discuție:**

- În ce fel devenim „complici” atunci când redistribuim conținut fals?
- Ce rol au platformele de social media în detectarea și eliminarea știrilor false?
- Cum putem educa utilizatorii să verifice informațiile înainte de distribuire?

### **3.3 Umilirea online și manipularea emoțională (Cyberbullying etc )**

**Studiu de caz:** Un elev sau student devine viral din cauza unei greșeli banale (video, poză sau replică înregistrată) și este hărțuit online de o comunitate largă.

#### **Pași de analiză:**

- a) identificați mecanismele sociale și tehnice: „mob digital”, #hashtag-uri de umilire, meme-uri, algoritmi care amplifică conținutul.
  - b) discutați efectele psihologice și reputaționale asupra victimei.
  - c) propuneți soluții: intervenții legale (legi antifacebook bullying), educaționale (campanii în școli), tehnologice (filtre automate de moderare).
- **Întrebări de discuție:**
- În ce măsură platformele sunt responsabile moral pentru conținutul generat de utilizatori?
  - Care sunt drepturile victimei și cum pot fi protejate prin legislația actuală?
  - Cum pot colabora comunitatea și instituțiile de învățământ pentru a preveni și combate hărțuirea online?

### **Prezentare generală și organizare teme rezolvate**

- **folderul de lucru:** fiecare grup va crea un folder nou în Google Drive, conform instrucțiunilor primite de la profesor, denumit astfel: Exerciții\_Cap2\_GrupaX, (unde „X” este numărul/grupa voastră).
- **conținutul folderului:**
  1. Nor\_Cuvinte\_Cap2\_GrupaX.png – imaginea norului de cuvinte generat la Tema 1.
  2. Harta\_Mentala\_Cap2\_GrupaX.png (sau PDF/fișier MindMup) – harta mentală creată la Tema 2.
  3. Rapoarte\_Debate\_GrupaX.docx sau link Google Docs cu răspunsurile și concluziile pentru Tema 3.
- **verificați permisiunile:** înainte de predare, asigurați-vă că profesorul are acces la toate fișierele (setare „Orice persoană cu link poate vizualiza” sau „Poate comenta/editare”, după cum s-a cerut).

*Consultați capitolul 3.3, secțiunea „Google drive” pentru instrucțiuni.*

## **Bibliografie**

1. Arockia Panimalar, S., Varnekha Shree, S., & Veneshia Kathrine, A. (2017). *The 17 V's Of Big Data*. IRJET, 04(09).
2. Barocas, S., & Selbst, A. (2016). Big Data's Disparate Impact. *California Law Review*, 104, 671–732.
3. Brynjolfsson, E., & McAfee, A. (2014). *The Second Machine Age*. W. W. Norton & Company.

4. Burrell, J. (2016). How the machine ‘thinks’: Understanding opacity in machine learning algorithms. *Big Data & Society*, 3(1).
5. Chesney, R., & Citron, D. K. (2019). Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security. *California Law Review*, 107, 1753–1819.
6. Crawford, K. (2016). Artificial Intelligence’s White Guy Problem. *The New York Times*.
7. Del Vicario, M., Bessi, A., Zollo, F., Petroni, F., Scala, A., Caldarelli, G., & Quattrociocchi, W. (2016). The spreading of misinformation online. *Proceedings of the National Academy of Sciences*, 113(3), 554–559.
8. Ferrara, E., Varol, O., Davis, C., Menczer, F., & Flammini, A. (2016). The rise of social bots. *Communications of the ACM*, 59(7), 96–104.
9. Floridi, L. (2015). *The Ethics of Information*. Oxford University Press.
10. Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep Learning*. MIT Press.
11. Hilbert, M. (2019). Digital technology and social change: The digitisation of society. *International Sociology*, 34(6), 694–709.
12. Kant, I. (1785). *Groundwork of the Metaphysics of Morals*.
13. Lanier, J. (2018). *Ten Arguments for Deleting Your Social Media Accounts Right Now*. Henry Holt and Company.
14. Norris, P. (2001). *Digital Divide: Civic Engagement, Information Poverty, and the Internet Worldwide*. Cambridge University Press.
15. O’Neil, C. (2016). *Weapons of Math Destruction*. Crown.
16. Ribeiro, M. T., Singh, S., & Guestrin, C. (2016). “Why Should I Trust You?” Explaining the Predictions of Any Classifier. *KDD ’16*, 1135–1144.
17. Samek, W., Wiegand, T., & Müller, K.-R. (2017). *Explainable AI: Understanding, Visualizing and Interpreting Deep Learning Models*. Springer.
18. Sunstein, C. R. (2018). *#Republic: Divided Democracy in the Age of Social Media*. Princeton University Press.
19. Tandoc Jr., E. C., Lim, Z. W., & Ling, R. (2020). Defining ‘fake news’: A typology of scholarly definitions. *Digital Journalism*, 8(10), 1373–1388.
20. Topol, E. (2019). *Deep Medicine: How Artificial Intelligence Can Make Healthcare Human Again*. Basic Books.
21. Vallor, S. (2016). *Technology and the Virtues: A Philosophical Guide to a Future Worth Wanting*. Oxford University Press.
22. Vosoughi, S., Roy, D., & Aral, S. (2018). The spread of true and false news online. *Science*, 359(6380), 1146–1151.
23. Wiener, N. (1950). *The Human Use of Human Beings: Cybernetics and Society*. Da Capo Press.
24. Zuboff, S. (2019). *The Age of Surveillance Capitalism*. PublicAffairs.

#### **Legislație și cadre normative**

1. Directiva 95/46/CE (1995).
2. GDPR (Regulamentul UE 2016/679) (2018).
3. DORA (Regulamentul 2022/2554) (2022).
4. California Consumer Privacy Act (CCPA) (2018).
5. ACM (1972). Code of Ethics and Professional Conduct.
6. Ethics Guidelines for Trustworthy AI (2019), Comisia Europeană.
7. Principles for Artificial Intelligence: Towards a Human-Centred Approach (2021), UNESCO.
8. Recommendation of the Council on Artificial Intelligence (2019), OECD.
9. ETICA Project, STOA (2011). Ethical Issues of Emerging ICT Applications. Parlamentul European.
10. Harbour, M. (2011). Declarația “Ethics and Digital Technologies”, STOA.
11. Freeland, A. (2011). Comentarii la reuniunea ETICA (IBM).
12. Whitten, A. (2011). „Reciclarea inteligenței umane” și reproducerea prejudecăților (Google).
13. IEEE P7000 Series – standarde etice pentru design IA.

#### **Linkuri utile**

1. [Securitatea cibernetică ebook ICI București](#)
2. [https://www.eca.europa.eu/sites/cc/Lists/CCDocuments/Compendium\\_Cybersecurity/CC\\_Compendium\\_Cybersecurity\\_RO.pdf](https://www.eca.europa.eu/sites/cc/Lists/CCDocuments/Compendium_Cybersecurity/CC_Compendium_Cybersecurity_RO.pdf) (Comitetul de contact al instituțiilor supreme de audit din Uniunea Europeană.)
3. <https://courses.minnlearn.com/ro/courses/emerging-technologies/implications-of-emerging-technologies/privacy-and-ethics-in-a-digital-age/>
4. <https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:32022R2065>
5. <https://legislatie.just.ro/Public/DetaliiDocument/280106>

6. <https://www.fssp.uaic.ro/departamente/sociologie-si-asistenta-sociala/evenimente/evolutii-recente-ale-fenomenului-dezinformarii-in-romania-si-europa-de-est>
7. <http://www.sap.com>

## Capitolul 3: Instrumente vizuale

Un instrument vizual este o metodă sau o aplicație care utilizează elemente grafice (imagini, scheme, culori, forme) pentru a reprezenta, organiza și comunica informații într-un mod clar și intuitiv. Scopul principal al unui instrument vizual este de a facilita înțelegerea rapidă a conceptelor, de a evidenția relații între idei și de a stimula creativitatea prin coerență cromatică și structură vizuală.

**Norul de cuvinte** evidențiază vizual frecvența și importanța termenilor-cheie, oferind o privire de ansamblu asupra celor mai relevante concepte dintr-un text sau dintr-o prezentare.

**Harta mentală** folosește noduri și legături pentru a structura ideile într-o formă dendritică, astfel încât să arate clar ierarhiile și conexiunile dintre concepte, facilitând organizarea gândirii și memorarea informațiilor.

**Google Drive**, deși nu este un „instrument grafic” în sens tradițional, oferă un spațiu colaborativ pentru stocarea, partajarea și editarea fișierelor (inclusiv documente, foi de lucru și prezentări), permițând integrarea ușoară a elementelor vizuale (imagini, diagrame, grafice) create cu alte unelte și accesibilitatea lor în timp real pentru întreaga echipă.

### 3.1.Nor de cuvinte

### 3.1.1.Introdúcere

Nor de cuvinte **wordle, colaj de cuvinte sau tag cloud**



Imagini preluate de la <https://movilforum.com/ro/crear-nubes-de-palabras-online-gratis/>

Informații detaliate despre anumite aplicații puteți regăsi pe <https://www.updateland.com/best-word-cloud-generator/>.

**Definiție** Un nor de cuvinte (word cloud) este o reprezentare grafică a frecvenței cuvintelor dintr-un corp textual. În acest tip de vizualizare, fiecare cuvânt apare cu o dimensiune (și, uneori, grosime) proporțională cu numărul de apariții în text. Astfel, termenii folosiți cel mai frecvent sunt evidențiați prin caractere mai mari și mai proeminente.

Norul de cuvinte este un instrument de vizualizare simplu și rapid, util în etapele incipiente ale analizei de text, atunci când ne dorim o imagine de ansamblu asupra vocabularului dominant. Cu toate acestea, pentru o interpretare riguroasă, trebuie să avem mereu în vedere limitările sale –

lipsa relațiilor semantice și posibilele ambiguități. În proiectele studențești, combinați norul de cuvinte cu alte metode (hartă mentală, studiu de caz etc.) pentru a obține concluzii articulate și contextualizate.



sursă: proprie

### Scopul utilizării norului de cuvinte

- evidențierea rapidă a termenilor-cheie dintr-un text sau dintr-un set de texte.
- identificarea subiectelor sau conceptelor dominante fără a citi tot conținutul în mod secvențial.
- oferirea unei priviri de ansamblu asupra vocabularului specific unui domeniu sau a teme abordate.

(sursa: <https://help.vevox.com/hc/en-us/sections/360002608057-Polling-How-to> )

### Limitări ale utilizării norului de cuvinte

- **lipsa contextului semantic** - norul de cuvinte nu arată legăturile sintactice sau semantice dintre termeni. De exemplu, două cuvinte care apar frecvent, dar în contexte diferite (ex.: „date” ca „informație” versus „date” ca „dată calendaristică”), pot fi afișate identic, fără a fi clar cum sunt folosite în text.
- **relații neexplicate** – norul de cuvinte nu indică ordinea în care apar cuvintele sau modul în care acestea se asociază în propoziții sau paragrafe. Un cuvânt situat central și foarte mare nu implică automat că el are o semnificație mai complexă decât unul mai mic; pur și simplu a apărut de mai multe ori.
- **excluderea termenilor cu semnificație redusă** - pentru a fi util, se aplică de obicei un filtru de stop-words (articole, prepoziții, pronume etc.), astfel încât vor apărea doar cuvinte cu putere discriminantă, dar uneori filtrarea poate elimina termeni importanți din context.

### Exemple de aplicații ale norului de cuvinte

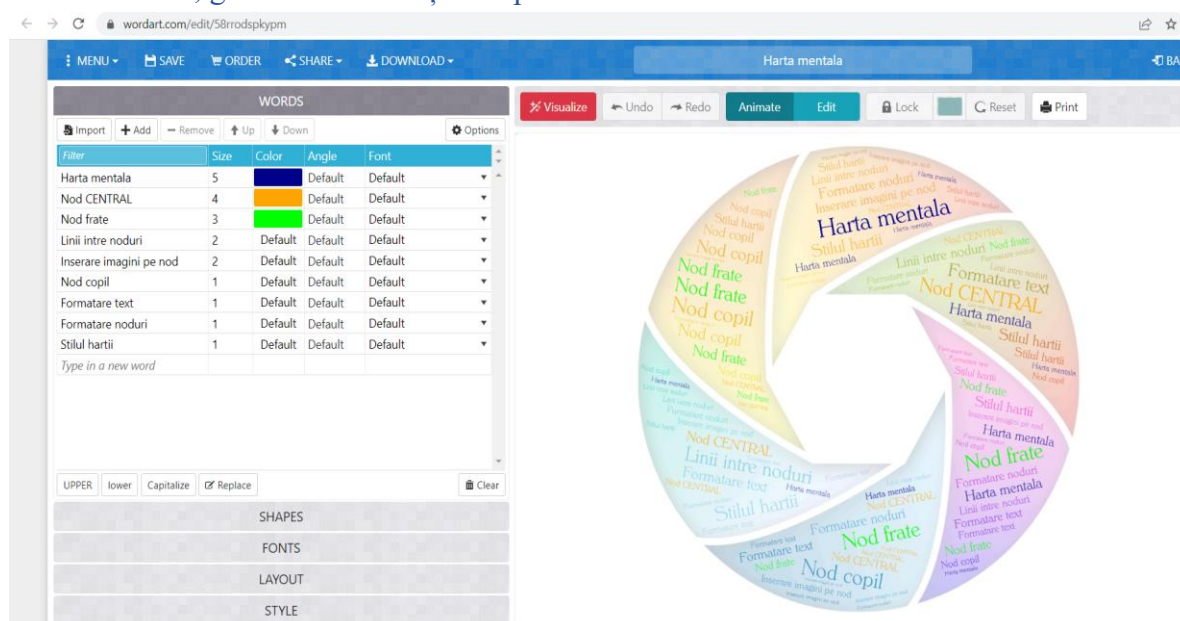
1. **analiza feedback-urilor studențești** - colectarea răspunsurilor deschise din chestionare și transformarea lor într-un nor de cuvinte pentru a vedea rapid care sunt principalele preocupări sau sugestii (ex.: „platformă”, „material”, „claritate”, „exerciții”).
2. **vizualizări în prezentări academice** - ilustrarea termenilor-cheie dintr-un articol de cercetare sau dintr-un capitol de referință pentru a sublinia conceptele fundamentale fără a prezenta liste lungi.
3. **analiza textelor literare** - extracția frecvențelor cuvintelor dintr-un roman sau dintr-o poezie pentru a evidenția tematicile principale (ex.: „dragoste”, „moarte”, „natura”) și/sau pentru a detecta motivații stilistice ale autorului.

4. **extragerea frecvențelor din interviuri** - preluarea transcrierilor de interviuri calitative, generarea unui nor de cuvinte și observarea conceptelor-cheie menționate de respondenți (ex.: „inovare”, „echipă”, „provocare”, „resurse”).

De reținut din cele mai sus prezentate:

- când construieți un nor de cuvinte, alegeți un set de text reprezentativ și curățați-l de elemente irelevante (stop-words, cifre, caractere speciale).
- verificați dacă doriți să păstrați sau să eliminați cuvinte ambigue (de exemplu, „date”). Dacă există termeni cu omonimie, luați în considerare segmentarea semantică înainte de generare.
- folosiți norul de cuvinte ca „punct de pornire” pentru analiza detaliată a textului: veți ști apoi ce termeni să explorați mai aprofundat în scris sau în interviuri.

### 3.1.1. Wordart, generator online și free pentru nor de cuvinte



sursa: proprie

Mai jos regăsiți un ghid succint al etapelor care trebuie parcurse în vederea creării un nor de cuvinte similar cu cel prezentat, folosind un instrument online precum **WordArt.com**:

1. **colectați lista de termeni și frecvențele**
  - identificați conceptele relevante (în cazul nostru, elementele hărții mentale).
  - atribuiți fiecărui termen o frecvență numerică care să reflecte importanța sa relativă (ex.: „Harta mentală” – 5, „Nod CENTRAL” – 4 etc.).
2. **accesați WordArt.com**
  - deschideți browserul și mergeți la <https://wordart.com>.
  - după autentificare (dacă este necesar), alegeți opțiunea **Create Now** (Creează acum).
3. **introduceți cuvintele și frecvențele**
  - în panoul **WORDS** de pe stânga, dați clic pe **Import** sau începeți să tasteți fiecare termen în rândul gol, apoi apăsați Enter.
  - în coloana **Size**, modificați manual valoarea numerică a fiecărui termen (corelată cu frecvența).

- dacă doriți, puteți regla și culoarea sau fontul (meniurile **Color** și **Font** rămân, de regulă, pe „Default”).
- 4. **alegeți forma norului de cuvinte**
  - dați clic pe secțiunea Shapes (SUB SHAPES) din partea de jos a panoului din stânga.
  - selectați forma „Circle” (Cerc) sau un alt „shape” care să se potrivească ideii—în exemplu, a fost folosit un cerc cu segmente radiale.
- 5. **personalizați layout-ul și stilul**
  - mutați-vă la secțiunea **Layout**: aici puteți alege cum se orientează cuvintele (orizontal, diagonal, vertical etc.) și distribuția acestora în spațiu.
  - în **Style**, setați paleta de culori și modul de colorare (de exemplu, „Pastel Colors” – culori pastelate).
  - dacă vreți să subliniați anumite cuvinte printr-o culoare distinctă, modificați manual culoarea în coloana **Color** pentru termenii-cheie.
- 6. **previzualizați și ajustați**
  - apăsați butonul Visualize (vizualizează) pentru a genera prima versiune a norului.
  - dacă un cuvânt este prea aglomerat sau prea mic, reveniți în lista de cuvinte și ajustați frecvența (size) până când aspectul vizual este echilibrat.
  - folosiți butoanele Undo/Redo pentru a reveni la pași anteriori și Animate pentru a vedea cuvintele mișcându-se pe ecran (opțional).
- 7. **finalizați și exportați**
  - când sunteți mulțumiți de rezultat, apăsați Download și alegeți formatul dorit (PNG, JPEG, SVG, etc.).
  - pentru includerea într-un raport sau pe o pagină web, selectați formatul de imagine adecvat (de obicei PNG pentru calitate bună și compatibilitate).

Pentru mai multe detalii referitor la crearea unui nor de cuvinte puteți accesa:

<https://www.youtube.com/watch?v=FSCEDqK3DO0>

<https://www.youtube.com/watch?v=QNQt0FFcVnI>

<https://www.youtube.com/watch?v=RJQ-bdBajF4>

În imaginile următoare voi prezenta două exemple de nori de cuvinte și voi evidenția atât aspectele pozitive, cât și punctele care pot fi îmbunătățite.

Exemple create cu <https://wordart.com>.

## Exemplul 1



- Norul de cuvinte este alcătuit din cinci segmente colorate în nuanțe pastelate.
- În fiecare segment apar termeni precum „Harta mentală”, „Nod frate” și „Formatare text” dispuse în diferite dimensiuni și orientări.
- Întreaga compoziție formează un inel circular, sugerând conexiunile dintr-o hartă mentală.

Ce s-ar putea îmbunătăți?

- Intensificați ușor saturația culorilor și măriți grosimea fontului pentru a crește contrastul și lizibilitatea cuvintelor.
- Uniformizați orientarea textului (de exemplu, doar orizontal și vertical) și lăsați spațiu mai mare între elemente pentru a evita suprapunerile.



- Norul are forma unui inel circular și este alcătuit din termeni legați de digitalizare, precum „transformare digitală”, „crearea de valoare” și „responsabilitate”.
- Cuvintele apar în diverse dimensiuni și culori (roșu, verde, albastru, gri), sugerând importanța diferită a fiecărui concept.
- Termeni suplimentari precum „guvernare”, „impact”, „outputs” și „servicii publice digitale” completează imaginea tematică.

Ce s-ar putea îmbunătăți?

- Uniformizați orientarea textului (de exemplu, doar orizontal și vertical) și creșteți spațiul dintre cuvinte pentru a evita suprapunerile și a îmbunătăți lizibilitatea.
- Ajustați dimensiunea cuvintelor proporțional cu frecvența sau relevanța lor și restrângeți paleta de culori la 3–4 nuanțe complementare, astfel încât elementele cheie să iasă mai bine în evidență.

Sursa proprie

## Bibliografie

1. <https://help.vevox.com/hc/en-us/sections/360002608057-Polling-How-to>
2. <https://www.offdocs.com/ro/blog/word-cloud-generator/>
3. <https://ahaslides.com/ro/blog/live-word-cloud-examples-and-ideas/>
4. <https://itigic.com/ro/what-are-word-clouds-good-for/>
5. <https://digitaledu.ro/aplicatii/wordart/>

## 3.2.Hărți mentale (HM)

### 3.2.1.Originea și utilitatea hărților mentale

Conceptul de hartă mentală (mind maps) a fost creat și popularizat de Tony Buzan în anii 1974, sub forma unui instrument de organizare a gândirii bazat pe structura naturală a conexiunilor neuronale din creier. Buzan a observat că modul în care creierul uman procesează informația – prin rețele asociative și conexiuni radiale – poate fi reprezentat vizual sub forma unei diagrame arboriforme care pornește de la un concept central și se ramifică către idei secundare. În acest fel, o hartă mentală reproduce, pe hartă, felul în care gândurile se generează și se conectează (Tony Buzan,1974).

De-a lungul timpului, hărțile mentale s-au dovedit utile în special în domeniile educației, afacerilor și dezvoltării personale. În mediul academic și didactic, ele facilitează înțelegerea și memorarea conceptelor complexe, oferind studenților o viziune clară asupra relațiilor dintre noțiuni. În mediul de afaceri, managerii și echipele de proiect le folosesc pentru planificarea rapidă a etapelor, identificarea dependențelor și generarea de idei în ședințe de brainstorming. De asemenea, în dezvoltarea personală, hărțile mentale servesc la formularea obiectivelor, la rezolvarea creativă a problemelor și la clarificarea prioritară a sarcinilor (Tony Buzan, 1974).

### 3.2.2.Definiție și beneficii

O hartă mentală este, prin definiție, o reprezentare vizuală de tip arbore, care pornește de la un nod central (conceptul principal) și prezintă ideile conexe în ramuri radiale. Nodul central—adesea un cuvânt-cheie sau o imagine sugestivă—servește drept “ancoră” vizuală, conectând, prin săgeți sau linii, conceptele de nivel secundar, terțiar și așa mai departe. Această dispunere radială reflectă procesul sintetic de gândire: creierul nu stochează informația într-o listă liniară, ci în rețele asociative care pot fi redată grafic printr-o hartă mentală .

Printre principalele beneficii ale utilizării hărților mentale se numără:

- structurarea logică a informațiilor, care permite vizualizarea imediată a legăturilor între idei și a ierarhiei dintre ele, facilitând astfel înțelegerea rapidă a complexității unui subiect.
- îmbunătățirea procesului de memorare, deoarece combinarea cuvintelor-cheie cu elemente grafice și cu culori stimulează simultan emisfera analitică și cea creativă a creierului, generând “ancore vizuale” eficiente în reamintirea detaliilor.
- stimularea creativității, întrucât hărțile mentale încurajează generarea rapidă a ideilor, fără constrângerile unui text liniar sau ale unei liste rigide, permițându-se adăugarea liberă de noi ramuri și sub-ramuri pe măsură ce apar asocieri noi.
- clarificarea procesului de gândire, deoarece organizarea vizuală ajută la evidențierea lacunelor informaționale, la compararea opțiunilor și la prioritizarea ideilor, ceea ce sprijină luarea deciziilor și rezolvarea problemelor într-un mod coerent și sistematic .

### Structura unei hărți mentale

O hartă mentală este alcătuită din trei elemente principale:

- ✓ **nodul central** – conceptul principal, scris clar în mijlocul diagramei.
- ✓ **legături etichetate** – conexiuni care arată relația dintre idei, evidențiate prin cuvinte-cheie.
- ✓ **ramuri cu sub-noduri** – idei secundare, dezvoltate progresiv din conceptul central.

## Ce NU este o hartă mentală

Pentru a înțelege mai bine acest concept, este important să clarificăm ce **nu** reprezintă o hartă mentală:

- **un text structurat liniar** – hărțile mentale sunt vizuale și interactive, spre deosebire de paragrafele tradiționale;
- **o listă rigidă** – spre deosebire de bullet points, o hartă mentală permite conexiuni multiple între idei;
- **o schemă simplă** – hărțile mentale sunt dinamice și pot evolua pe măsură ce apar noi informații;
- **un grafic static** – fiecare hartă mentală trebuie să fie flexibilă, adaptabilă și deschisă la modificări.

Pentru a crea o hartă mentală eficientă, trebuie urmați o succesiune de pași, descriși în cele ce urmează:

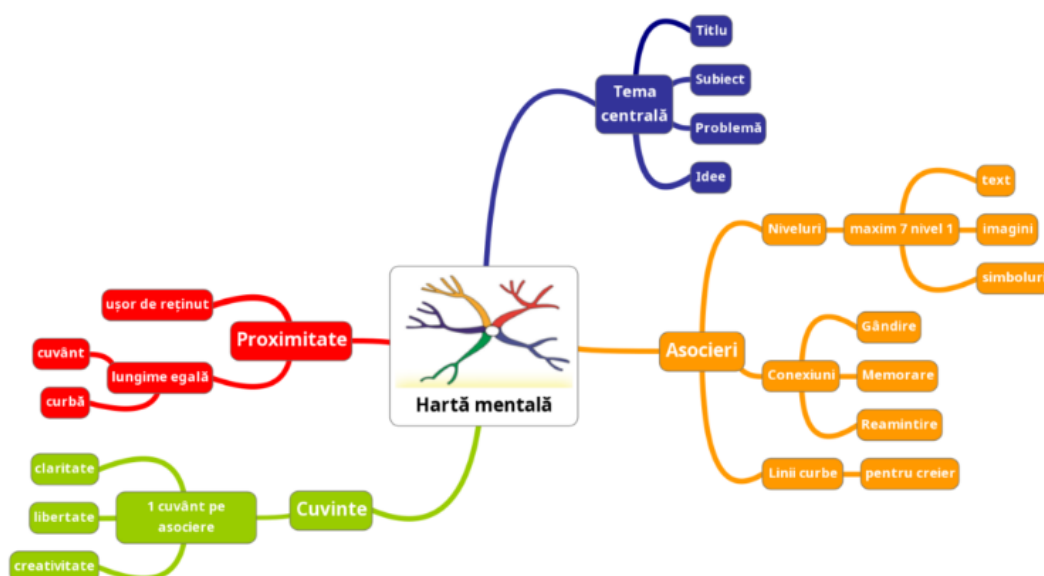
1. *identificarea nodului central* - alegeți un cuvânt-cheie sau o imagine reprezentativă pentru tema pe care o veți explora; amplasați-l în mijlocul paginii, lăsând spațiu suficient pentru ramuri radiale. Nodul central servește drept „ancoră” vizuală și comunică imediat subiectul general. Lipsa unui nod clar poate duce la o hartă confuză și greu de urmărit.
2. *adăugarea ramurilor principale* - conectați direct la nodul central între 4 și 6 ramuri principale, etichetate cu ideile-cheie sau categoriile fundamentale. Folosiți cuvinte sau fraze scurte, evitând blocurile de text. Fiecare ramură trebuie să reprezinte o subtemă majoră, astfel încât structura hărții să rămână aerisită și ușor de parcurs.
3. *dezvoltarea sub-ramurilor* - sub fiecare ramură principală, adăugați sub-ramuri ce furnizează detalii, exemple sau clarificări; acestea pot include definiții suplimentare, fapte concrete sau argumente. Numărul de sub-ramuri trebuie adaptat în funcție de complexitatea informației, dar este indicat să nu depășiți 3–4 nivele de ierarhie pentru a evita supraîncărcarea vizuală.
4. *trasarea legăturilor etichetate* - dacă există relații de cauză-efect, ordonări cronologice sau interdependențe între idei, conectați nodurile cu săgeți sau linii etichetate, indicând natura relației (de exemplu, „=>”, „supports” (susține, sprijină), „contradicts” (contrazice)). Acest pas transformă harta dintr-un simplu arbore ierarhic într-o rețea semnificativă a conceptelor, evidențiind conexiuni și facilitând înțelegerea interacțiunilor.
5. *integrarea elementelor vizuale* - aplicați culori diferite pentru ramuri (de obicei, o nuanță distinctă pe nivel ierarhic), utilizați grosimi variabile ale liniilor pentru a sublinia importanța și încorporați pictograme sau simboluri care evidențiază aspecte cheie (evaluări, atenționări, etape critice). Combinarea text-imagine stimulează emisfera creativă și cea analitică a creierului, îmbunătățind memorarea informațiilor.

O hartă mentală eficientă trebuie să ofere o imagine de ansamblu lizibilă într-o primă privire. Pentru mai multe detalii legate de crearea unei hărți mentale vizionați următoarele clipuri video:

<https://www.youtube.com/watch?v=P2JJG-P3H80> (4 minute de vizionat)

[https://www.youtube.com/watch?v=hD31zC2\\_JmA](https://www.youtube.com/watch?v=hD31zC2_JmA) (3 minute de vizionat)

*Ilustrarea componentelor unei hărți mentale - ea însăși o hartă mentală care explică elementele de bază ale unei hărți mentale*



Elemente hartă mentală

sursa: [Retine mai ușor cu harta mentală - Asociația EDUROD](#)

## MindMup - instrument online de creare a hărților mentale

Există o mulțime de instrumente online pentru crearea hărților mentale, iar unul dintre ele este MindMup. MindMup este o platformă online de hărți mentale, accesibilă direct din browser sau integrată în Google Drive, fără instalare și fără costuri (în versiunea de bază). Hărțile se salvează automat în cloud. Interfața afișată este produsă cu MindMup și conține o hartă mentală denumită „Transformarea digitală”.



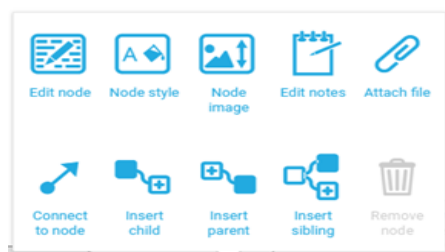
sursă: proprie

Bara de instrumente principală din MindMup afișată în imagine conține, de la stânga la dreapta, următoarele butoane și funcționalități:

1. **File Menu** (meniul fișier)
  - oferă acces la operații de bază: New (creare hartă nouă), Open (deschidere), Save (salvare) și Export.
2. **Insert Menu** (meniul inserare)
  - conține comenzi pentru adăugarea de noduri și legături:
    - **Insert Child** (adaugă nod copil)
    - **Insert Sibling** (adaugă nod frate)
    - **Insert Parent** (adaugă nod părinte)
    - **Connect to Node** (conectează noduri cu o săgeată).
3. **Edit Menu** (meniul editare)

- cuprinde comenzi pentru modificarea elementelor selectate:
  - **Undo** (anulează ultima acțiune)
  - **Redo** (reface ultima acțiune anulată)
  - **Remove Node** (șterge nodul selectat)
  - **Node Style** (deschide paleta de stiluri pentru a schimba culoarea, forma, grosimea marginii și fontul nodului).
- 4. **Formatting Palette** (meniul formătări rapide)
  - prezintă butoane pentru aliniere și distribuire, respectiv:
    - aliniere orizontală și verticală a nodurilor (centrează, distribuie)
    - auto-arrange (aranjare automată a ramurilor pentru aspect echilibrat).
- 5. **Font Controls** (meniul control text)
  - **Font Size Decrease / Increase** (micșorează/mărește dimensiunea textului din nod)
  - **Bold / Italic / Underline** (stiluri de text pentru textul selectat în nod)
- 6. **Color & Icon Tools** (meniul pentru culoare și pictograme)
  - **Node Color** (alege culoarea de fundal a nodului)
  - **Text Color** (schimbă culoarea textului din nod)
  - **Node Image/Icon** (încarcă sau inserează o pictogramă/imagie în interiorul nodului)
- 7. **Zoom & Fit Controls** (meniul zoom și vizualizare)
  - **Zoom In/Zoom Out** (mărește sau micșorează vizualizarea întregii hărți)
  - **Fit Map to Screen** (ajustează zoom-ul astfel încât toată harta să fie vizibilă pe ecran)
- 8. **Navigation & View Options** (meniul pentru navigare și afișare conținut)
  - **Show/Hide Side Panel** (afișează sau ascunde panoul lateral de proprietăți)
  - **Toggle Grid** (afișează/ascunde grila de fundal, pentru alinierea nodurilor)
  - **Fullscreen Mode** (comută între modul fereastră și ecran complet)
- 9. **Publish / Share** (meniul publicare/partajare)
  - **Publish** (crează un link public care poate fi distribuit)
  - **Share** (setări de partajare directă, permisiuni de acces)
- 10. **Help Menu** (meniul ajutor)
  - oferă acces la documentație, tutoriale și întrebări frecvente despre MindMup.

Ca la orice aplicație există și meniuri contextuale. Unul dintre ele se referă la orice nod, central sau secundar, așa cum poate fi vizualizat în imaginea de mai jos.

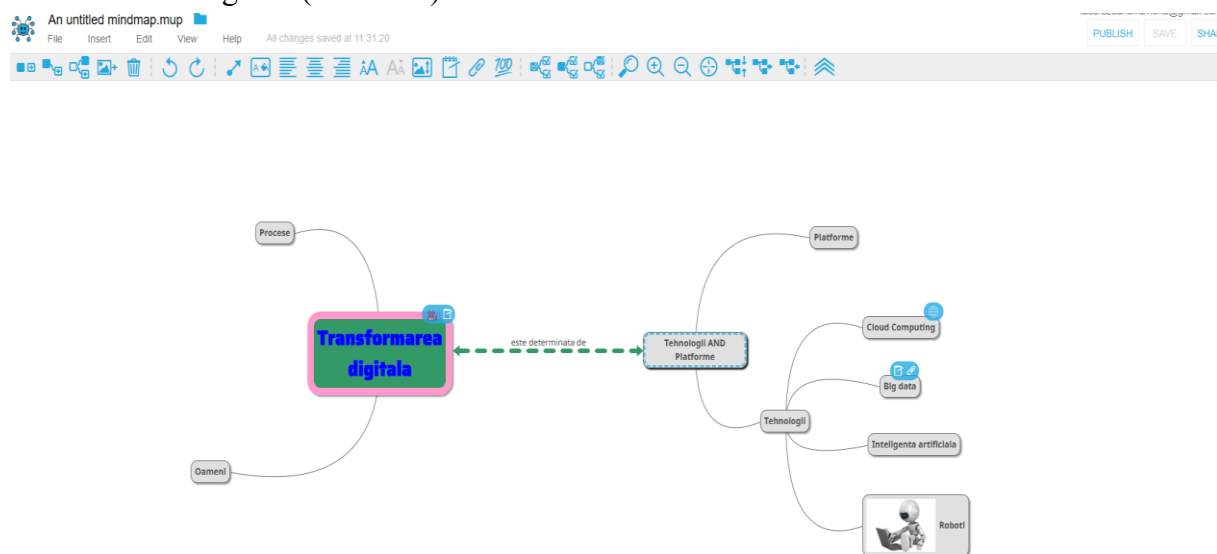


Deasupra nodului central (sau altui tip de nod) apare un meniu contextual cu pictograme care permit utilizatorului mai multe operațiuni:

- ❖ Edit Node – să modifice textul din nod.
- ❖ Node Style – să schimbe stilul (culoarea sau forma) nodului.

- ❖ Node Image – să atașeze o imagine în nod.
- ❖ Edit Notes – să adauge note suplimentare.
- ❖ Attach File – să atașeze un fișier.
- ❖ Connect to Node – să creeze o legătură către un alt nod.
- ❖ Insert Child – să adauge o ramură copiilor.
- ❖ Insert Parent – să adauge un nod părinte deasupra nodului curent.
- ❖ Insert Sibling – să adauge un nod de același nivel.
- ❖ Remove Node – să șteargă nodul.

În rândurile următoare vom descrie cum s-a creat HM pentru conceptele aferente ideii de transformare digitală (o viziune).



În mijloc se află nodul central, „Transformarea digitală”, din care se desprind 3 ramificații:

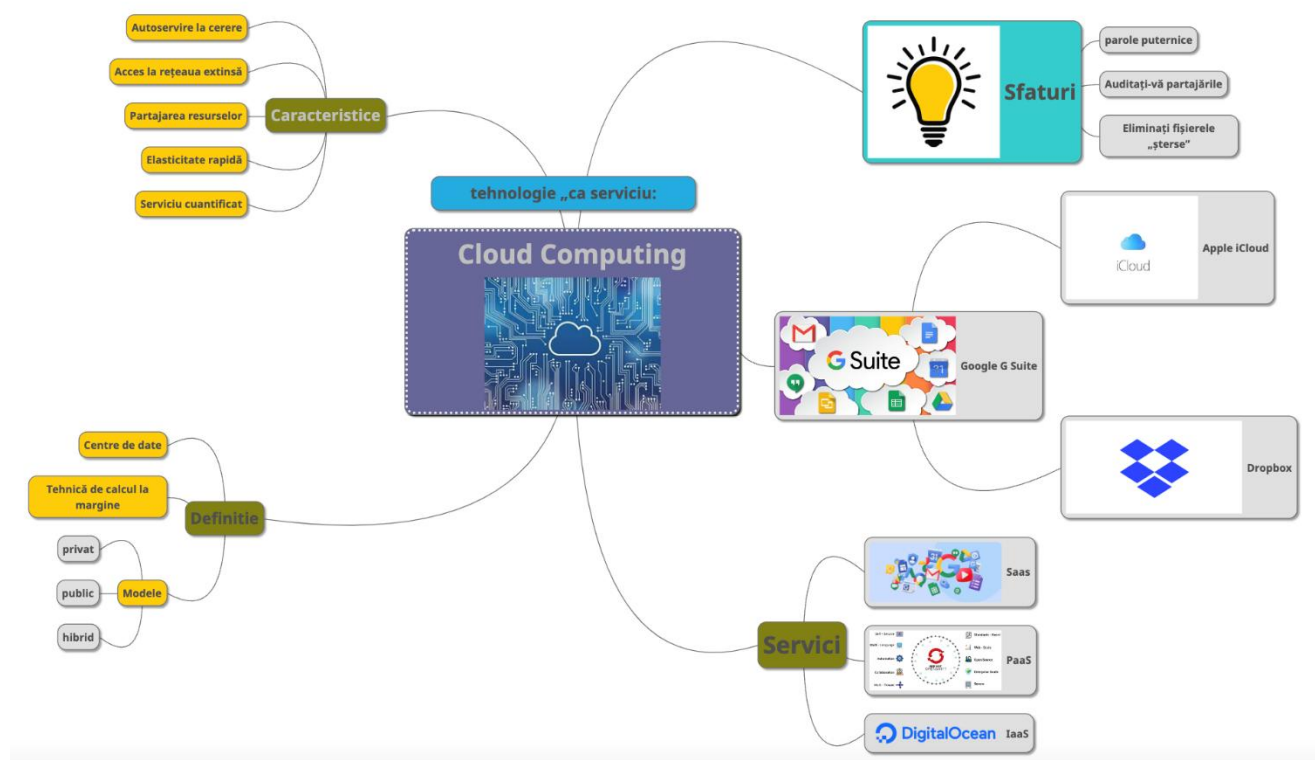
- 2 ramuri încă nepopulate (goale), **Procese** și **Persoane**
- 1 ramură intitulată „**Tehnologii și Platforme**”, conectată la nodul central printr-o săgeată punctată, care se împarte mai departe în două subramuri:
  - **Platforme** (neextinsă momentan).
  - **Tehnologii**, din care se desprind patru concepte specifice:
    - a. **Cloud Computing**
    - b. **Big Data**
    - c. **Inteligență artificială**
    - d. **Roboți** (reprezentat și printr-o pictogramă sugestivă)

### Avantaje ale aplicației MindMup

- ✓ Salvare și partajare în cloud, pentru colaborare în timp real.
- ✓ Export în formate diverse (PDF, imagine, fișier MindMup).

## Exemple HM cu descriere

### Exemplul 1 pentru noțiunile de Cloud Computing



sursă:proprie cu studenții

1. **Identificarea nodului central** - nodul central este „Cloud Computing”, afișat ca un dreptunghi albastru închis, însoțit de o pictogramă reprezentativă (norișor și circuite).

2. **Adăugarea ramurilor principale**

- din nodul „Cloud Computing” pleacă cinci ramuri etichetate „Definiție”, „Caracteristici”, „Servicii”, „Sfaturi” și două ramuri pentru exemple de platforme („G Suite” și „iCloud/Dropbox”).

3. **Dezvoltarea sub-ramurilor**

- sub ramura **Definiție**, găsim două sub-ramuri: „Centre de date” și „Tehnică de calcul la margine”; apoi, sub-ramura „Modele” (având trei noduri: privat, public, hibrid).
- sub ramura **Caracteristici**, apar cinci sub-ramuri: „Autoservire la cerere”, „Acces la rețeaua extinsă”, „Partajarea resurselor”, „Elasticitate rapidă” și „Serviciu cuantificat”.
- sub ramura **Servicii**, se deschid trei subramuri: „SaaS” (software as a service), „PaaS” (platform as a service) și „IaaS” (infrastructure as a service – DigitalOcean).
- sub ramura **Sfaturi**, apar trei noduri: „parole puternice”, „auditați-vă partajările” și „eliminați fișierele ‘șterse’”.

4. **Integrarea elementelor vizuale** - nodurile folosesc **culori diferite**:

- ✓ albastru închis pentru nodul central („Cloud Computing”),
- ✓ verde-închis pentru „Definiție”, „Caracteristici” și „Servicii”,
- ✓ turcoaz pentru „Sfaturi”,
- ✓ gri pentru exemplele de platforme.

5. **Adăugare pictograme**:

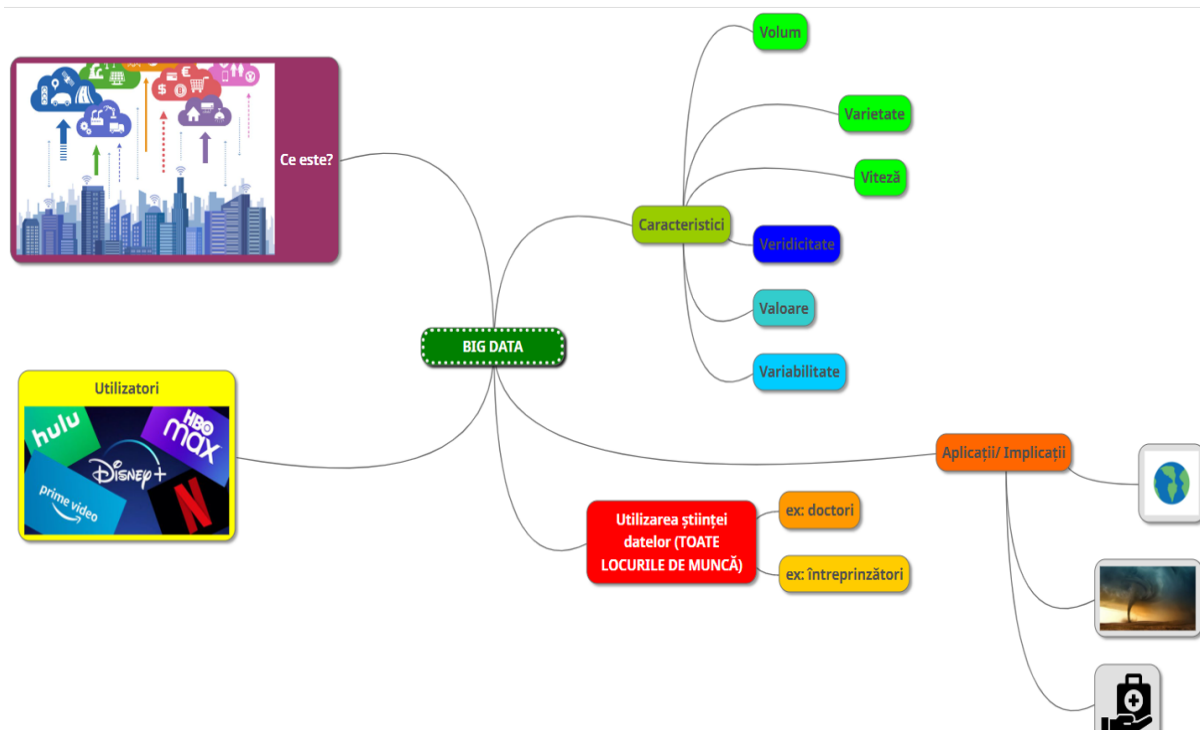
- ✓ nodul central are o imagine cu circuite și nor.

✓ „G Suite”, „iCloud” și „Dropbox” sunt reprezentate de iconițe ale serviciilor respective.

*Sugestii de îmbunătățire:*

- reduceți paleta la 2–3 nuanțe complementare pentru toate nodurile principale și sub-ramurile lor.
- uniformizați icoanele și logo-urile într-un singur container (dreptunghi cu iconiță și etichetă), fără imagini separate.
- adăugați grupări pentru sub-ramura “Caracteristici” (ex.: infrastructură vs. operaționalizare) și scurtați titlurile prea lungi.
- aliniați toate nodurile de același nivel la aceeași înălțime și mențineți spațiere uniformă între ele.

*Exemplu 2 pentru noțiunile de Big Data.*



sursă:proprie cu studenții

1. **Identificarea nodului central** - Nodul central este „BIG DATA”, afișat ca un dreptunghi orizontal cu bordură punctată și umplutură verde-închis. Textul este centrat și evidențiat printr-o nuanță intensă de verde, sugerând importanța conceptului în contextul diagramei. Acest nod servește ca punctul de plecare pentru toate ramurile și sub-ramurile, indicând prevalența și relevanța temei „Big Data” în cadrul prezentării.
2. **Adăugarea ramurilor principale** - Din nodul „BIG DATA” se desprind cinci ramuri principale, fiecare reprezentând o categorie semnificativă:
  - „Ce este?” (ramură orientată spre stânga sus)
  - „Utilizatori” (ramură orientată spre stânga jos)
  - „Caracteristici” (ramură orientată spre dreapta sus)

- „Utilizarea științei datelor (TOATE LOCURILE DE MUNCĂ)” (ramură orientată spre jos-centru)
- „Aplicații/ Implicații” (ramură orientată spre dreapta jos)

Fiecare ramură principală pornește direct din nodul central și se desfășoară în direcții diferite, separând clar categoriile tematice.

### 3. Dezvoltarea sub-ramurilor-

- **Ramura „Ce este?”** - această ramură nu conține noduri textuale propriu-zise, ci este reprezentată de o **image** amplă (în colțul stâng-sus), care ilustrează fluxuri de date într-un mediu urban. În imagine, se observă un oraș stilizat, blocuri de clădiri în nuanțe de mov închis, de unde pornesc săgeți albastre, verzi și roșii în sus, simbolizând transmiterea masivă de informații sau date către infrastructuri cloud. Fundalul mov și iconițele mici din partea superioară (rețeau, servere, simboluri de analiză etc.) subliniază complexitatea sistemelor Big Data.
- **Ramura „Utilizatori”** - sub această ramură, pe partea stângă-jos, se găsește un **dreptunghi galben** cu textul „Utilizatori” în partea superioară și, în interior, un **colaj de logouri** pentru: Hulu, HBO Max, Disney+, Prime Video și Netflix. Aceasta sugerează că marile platforme de streaming sunt exemple primordiale de utilizatori sau beneficiari ai tehnologiilor Big Data.
- **Ramura „Caracteristici”** - din nodul central, spre dreapta-sus pornește un dreptunghi de culoare verde-închis cu inscripția „Caracteristici”. De aici, se ramifică șase sub-noduri distincte, fiecare reprezentând un atribut al Big Data: **Volum** (nod verde deschis)/ **Varietate** (nod verde deschis)/ **Viteză** (nod verde deschis) etc. Fiecare sub-ramură este conectată direct la „Caracteristici” prin linii subțiri gri, iar nodurile textuale colorate diferit evidențiază importanța fiecărei dimensiuni în ecuația Big Data.
- **Ramura „Utilizarea științei datelor (TOATE LOCURILE DE MUNCĂ)”** - în partea de jos-centru, există un **dreptunghi roșu** cu text alb: „Utilizarea științei datelor (TOATE LOCURILE DE MUNCĂ)”. Din acest nod, se desprind două sub-ramuri, fiecare reprezentată printr-un **nod galben-aranjat**. Aceste noduri ilustrează două categorii profesionale în care știința datelor (data science) poate fi utilizată, subliniind aplicabilitatea broad a Big Data în domenii variate.
- **Ramura „Aplicații/ Implicații”** - spre dreapta-jos pleacă un **dreptunghi oranj** cu inscripția „Aplicații/ Implicații”. Din acesta, se extind trei sub-ramuri care se termină în **pictograme** (fără noduri textuale adiționale), reprezentând domenii de impact sau scenarii concrete:
  1. **Global** – o **pictogramă cu globul pământesc** care sugerează implicații la scară planetară sau transformări globale facilitate de Big Data.
  2. **Schimbări climatice** – o **image cu un tornado** (furtună), simbolizând modul în care analiza volumelor mari de date meteorologice poate influența prognoza sau studiile climatice.
  3. **Sănătate/Medicină** – o **pictogramă cu o servietă medicală** și semnul „+”, subliniind rolul Big Data în domeniul medical, fie în diagnostic, fie în managementul sănătății publice.

### 4. Integrarea elementelor vizuale

Fiecare categorie este evidențiată printr-o **culoare specifică** pentru nodurile principale. **Fundalul** diagramei este alb, iar liniile de legătură sunt subțiri și de culoare gri, asigurând lizibilitate și claritate vizuală.

## 5. Adăugare pictograme

Nodul „Ce este?” integrează o **imagine complexă**: blocuri de oraș, iconițe de rețea și săgeți multicolore care pornesc spre cer, simbolizând fluxurile de date.

Ramura „Utilizatori” conține un **colaj de logouri** pentru platforme de streaming: Hulu, HBO Max, Disney+, Prime Video și Netflix.

Sub ramura „Aplicații/ Implicații” apar trei **pictograme tematice**: globul pământesc, un tornado și o servietă medicală cu cruce, fiecare reprezentând un domeniu de aplicabilitate al Big Data (impact global, studii climatice și sectorul medical).

Sugestii de îmbunătățire:

- o uniformizarea și simplificarea schemei vizuale – reducerea numărului de culori utilizate pentru nodurile principale și sub-ramuri, folosind o paletă coerentă (de ex. două–trei nuanțe complementare) și menținând același contrast text-fundal pentru toate nodurile, pentru a îmbunătăți lizibilitatea și a evita senzația de curcubeu cromatic.
- o asigurarea unui stil consecvent pentru toate pictogramele și imaginile (același tip de icoane monocrome sau același nivel de detaliu), astfel încât ramurile să pară parte a aceluiași ecosistem vizual.
- o împărțirea ramurilor prea încărcate (de ex. „Caracteristici” cu șase sub-noduri) în sub-categorii logice sau adăugarea de elemente în alte ramuri pentru a uniformiza densitatea informațională; de asemenea, scurtarea titlurilor prea lungi
- o introduceți un scurt nod de text explicativ sub imaginea din „Ce este?” (de ex. „Fluxuri de date într-un mediu urban”).

## Bibliografie

1. Buzan, T. (1974). *Use Your Head*. BBC Books.
2. Farrand, P., Hussain, F., & Hennessy, E. (2002). The efficacy of the mind map study technique. *Medical Education*, 36(5), 426–431.
3. Nesbit, J. C., & Cañas, A. J. (2006). A review of mind mapping and concept mapping: Emerging tools for knowledge management and sharing. *Knowledge Management & E-Learning*, 1(1), 36–53.
4. <https://www.youtube.com/watch?v=XY-YjF57wFsow>
5. <https://www.youtube.com/watch?v=FxGFRC96sRI>
6. <https://www.mindonmap.com/ro/blog/what-is-a-mind-map/>
7. <https://ahaslides.com/ro/blog/mind-map-ideas-for-students/>
8. <https://www.mindmup.com/tutorials/index.html>

### 3.3. Google Drive – scurtă prezentare

#### 3.3.1. Introducere

Scopul principal al lucrului în echipă este să maximizăm eficiența și transparența. Dacă fiecare membru lucrează local, fără sincronizare, apar versiuni disparate și pierderi de timp la integrarea părților. Postând materialele într-un folder comun, toți membrii echipei pot accesa instant documentele actualizate, indiferent de locație sau dispozitiv.

Folosind un folder comun, nu mai există multiple copii locale cu nume similare (ex. raport\_final\_v2.docx, raport\_final\_v3.docx etc.). Orice modificare intră automat în istoricul de versiuni, astfel încât putem reveni oricând la o versiune anterioară, fără riscul pierderii informațiilor.

Folderul comun oferă o vizibilitate clară asupra stadiului de realizare a fiecărei sarcini: putem vedea cine a lucrat, ce a adăugat și la ce capitol s-a ajuns. La finalizarea proiectului, toate materialele vor rămâne centralizate într-un singur folder. Dacă, peste luni sau ani, echipa se reunește sau un nou membru preia proiectul, poate găsi rapid tot conținutul anterior.

În cadrul laboratoarelor de informatică vom crea diferite fișiere de tipuri (extensii) diferite (cum ar fi documente, .pdf, .png, prezentare, rapoarte și studii de caz. Postându-le în folderul comun, fiecare micro-grup poate vedea ce a lucrat alt grup.

În sinteză, folosirea unui folder comun pe Google Drive asigură:

- acces imediat și constant.
- colaborare în timp real fără duplicări.
- istoric de versiuni clar.
- vizibilitate asupra progresului și responsabilizare.
- arhivare centralizată pentru proiecte viitoare.

#### 3.3.2. Descriere operații pe pași

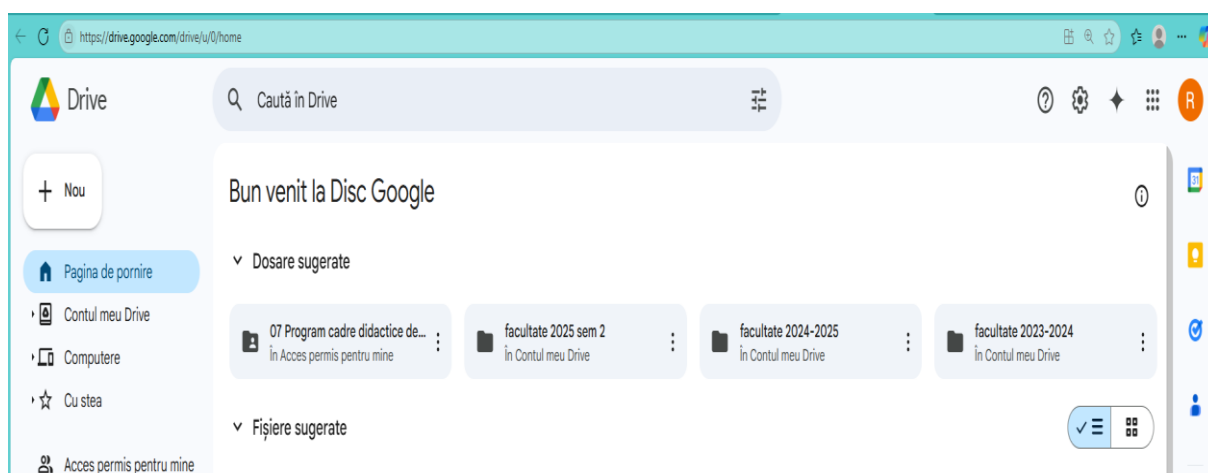
Google Drive este un serviciu de stocare în cloud oferit de Google, care permite oricui deține un cont Google să încarce, să salveze și să acceseze fișiere de pe orice dispozitiv conectat la internet.

Avantaje ale utilizării Google Drive:

- securitate sporită: fișierele sunt criptate atât în timpul transferului, cât și la stocare, iar accesul poate fi protejat prin autentificare în doi pași.
- accesibilitate totală: documentele pot fi consultate și editate de pe computer, tabletă sau smartphone, fără a fi nevoie de un anumit calculator.
- integrare nativă cu Google Workspace: funcționează fără probleme alături de Google Docs, Sheets, Slides etc., ceea ce simplifică crearea, colaborarea și partajarea fișierelor.

#### Accesarea și interfața principală

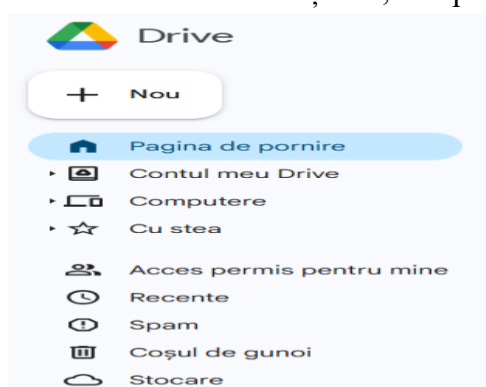
- Deschideți browserul și mergeți la <https://drive.google.com>, apoi autentificați-vă cu contul vostru Google.



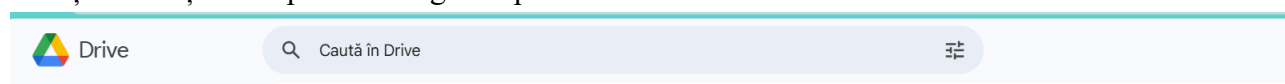
După autentificare, în interfața principală distingem **3 componente** (panoul din stânga, bara de căutare, zona centrală):

**a. panoul din stânga:**

- **Quick Access (acces rapid)** – listează fișierele și folderele folosite recent.
- **My Drive (drive-ul meu)** – conține toate fișierele și folderele voastre.
- **Shared with me (partajate cu mine)** – afișează documentele pe care alții le-au partajat cu voi.
- **Recent (recente)** – reunește fișierele și folderele deschise sau modificate în ultima perioadă.
- **Trash (coșul de gunoi)** – stochează elementele șterse, recuperabile timp de 30 de zile.



**b. bara de căutare (Search Drive, Caută în drive)** – unde puteți să tastați numele, tipul sau conținutul fișierelor pentru a le găsi rapid.



**c. zona centrală** – aici răsfoiți structura folderelor și fișierelor voastre.



## Organizarea fișierelor și folderelor

1. Creați un folder nou urmând succesiunea de pași de mai jos:

- a. dați clic pe butonul + **New (Nou)** din colțul stânga-sus al ecranului.
- b. din meniul derulant, selectați **Folder (Folder)**.
- c. se va deschide o fereastră mică în care introduceți numele dorit pentru folder.
- d. apăsați **Create (Creează)** sau tasta Enter pentru a finaliza.

Noul folder va apărea imediat în lista din zona centrală.

2. Răsfoiți și mutați fișierele prin drag & drop, urmând pașii prezentați mai jos:

- a. în zona centrală, dați dublu-clic pe **My Drive (drive-ul meu)** (dacă nu sunteți deja acolo) pentru a vedea fișierele și folderele existente.
- b. pentru a muta un fișier sau folder într-un alt folder:
  - poziționați cursorul deasupra elementului pe care doriți să-l mutați.
  - țineți apăsat butonul stâng al mouse-ului și trageți (drag) fișierul sau folderul spre folderul țintă din listă.
- c. eliberați butonul mouse-ului deasupra folderului țintă pentru a „plasa” (drop) elementul acolo.

După mișcare, fișierul/folderul va dispărea din locația anterioară și va apărea în folderul țintă.

3. Redenumiți un fișier sau folder

- a. găsiți în zona centrală fișierul sau folderul pe care doriți să-l redenumiți.
- b. dați clic dreapta pe numele elementului și, din meniul contextual, selectați **Rename (redenumeste)**; va apărea un câmp de text în care puteți tasta noul nume.
- c. după ce ați scris numele dorit, apăsați tasta **Enter** sau faceți clic pe **OK/Save (salvează)** din fereastra pop-up.

Numele modificat va fi afișat imediat în lista de fișiere/foldere.

## Crearea și gestionarea fișierelor

1. Creați documente Google Docs, Sheets sau Slides astfel:

- dați clic pe butonul + **New (Nou)** din colțul stânga-sus.
- din meniul derulant, selectați una dintre următoarele opțiuni:
  - Google Docs (document Google)
  - Google Sheets (foaie de calcul Google)
  - Google Slides (prezentare Google)
- documentul nou va apărea imediat în zona centrală și se va deschide într-un tab separat.
- orice modificare pe care o faceți se salvează automat, fără să mai fie nevoie să apăsați Save (salvează).

2. Încărcați fișiere și foldere din calculator în contul vostru Google Drive

- dați clic pe + **New (Nou)** → **File upload** (încărcare fișier) sau **Folder upload** (încărcare folder).
- în fereastra care se va afișa, navigați în sistemul vostru de fișiere și selectați elementul dorit (fișier sau folder).
- apăsați butonul **Open (deschide)** pentru a începe încărcarea.

- fișierul/folderul va fi copiat în contul vostru Google Drive și va apărea în zona centrală imediat ce încărcarea se termină.
- 3. Descărcați fișiere din Google Drive pe calculator
  - în zona centrală, găsiți fișierul sau folderul pe care doriți să-l salvați local.
  - dați clic dreapta (right-click) pe acel element și selectați butonul **Download (descarcă)**.
  - browserul va salva fișierul/folderul pe calculator în dosarul implicit de descărcări.
- 4. Converteți fișiere Office în formate Google editabile
  - dacă aveți un fișier Microsoft Word (.docx), Excel (.xlsx) sau PowerPoint (.pptx) deja încărcat în Drive:
    - dați clic dreapta pe fișierul respectiv → Open with (deschide cu) → Google Docs (pentru documente Word) sau Google Sheets (pentru foi Excel) sau Google Slides (pentru prezentări PPTX).
    - fișierul se va deschide într-o nouă fereastră ca document Google editabil.
    - o copie nouă în format Google (docs/sheets/slides) va fi salvată automat în același folder din Google Drive.

Astfel, puteți edita direct în Google Drive fără a mai descărca sau instala aplicații suplimentare.

### **Partajare și colaborare**

1. Partajați fișierele și setați permisiuni pentru alți utilizatori astfel:
  - în zona centrală, găsiți fișierul sau folderul pe care doriți să-l partajați.
  - dați clic dreapta (right-click) pe element și selectați Share (partajează).
  - în fereastra „Share with others” (partajează cu alții), introduceți adresa de e-mail a persoanei sau a grupului.
  - alegeți nivelul de acces acordat:
    - Viewer (vizualizare) – persoana poate doar să vizualizeze fișierul, fără a face modificări.
    - Commenter (comentator) – persoana poate adăuga comentarii, dar nu poate edita conținutul.
    - Editor (editor) – persoana poate edita direct documentul în timp real.
  - dați clic pe Send (trimite) pentru a transmite invitația de acces.
2. Colaborați în timp real cu ceilalți membri ai grupului
  - dacă fișierul este partajat cu rolul Editor, puteți lucra simultan cu ceilalți colaboratori.
  - veți vedea cursorul fiecărui utilizator cu o culoare diferită și numele acestora.
  - în Google Docs, dați clic pe butonul Chat din dreapta-sus pentru a discuta rapid, fără a părăsi documentul.
3. Utilizați comentariile și sugestiile pentru un document partajat:
  - pentru a adăuga un comentariu: selectați textul sau zona relevantă, apoi dați clic pe pictograma Add comment (Adaugă comentariu) din bara de instrumente.
  - pentru a propune modificări fără a schimba direct conținutul (modul recomandat pentru revizuirii):
    - în colțul dreapta-sus al Google Docs/Sheets/Slides, selectați modul Suggesting (sugestii).
    - orice schimbare va apărea ca suggestion (sugestie) – text evidențiat care poate fi Accept (acceptat) sau Reject (respins) de către ceilalți colaboratori.

## Funcții avansate

1. Căutarea fișierelor se realizează astfel:
  - dați clic în Search Drive (bara de căutare de sus) și tastați cuvinte-cheie, tipul fișierului (ex. „pdf”, „Google Sheet”) sau părți din conținut.
  - pentru a filtra rezultatele, dați clic pe săgeata în jos din dreapta câmpului de căutare și completați:
    - Type (Tip) – Document, Spreadsheet, Presentation, PDF etc.
    - Modified Date (data modificării) – azi, săptămâna trecută, interval personalizat.
    - Owner (proprietar) – You (tu), alt utilizator, un grup etc.
  - dați clic pe Search (caută) pentru a aplica filtrele și a vedea rezultatele.
2. Răsfoiți versiunile anterioare ale fișierelor
  - deschideți un document Google Docs, Sheets sau Slides.
  - dați clic pe meniul File (fișier) → Version history (istoric versiuni) → See version history (vezi istoricul versiunilor).
  - în panoul din dreapta, răsfoiți lista de versiuni salvate automat, grupate după data și ora la care au fost create.
  - pentru a vizualiza o versiune, dați clic pe ea; pentru a reveni la acea versiune, dați clic pe Restore this version (restaurare această versiune).

## Bibliografie

1. <https://support.google.com/drive#topic=14940>
2. [https://www.youtube.com/watch?v=z9i\\_h-WMQ68](https://www.youtube.com/watch?v=z9i_h-WMQ68) (How to Use Google Docs - Beginner's Guide)
3. <https://www.youtube.com/watch?v=xJiUTXGv3PE> (Google Docs - Full Tutorial)
4. [Instruire și ajutor Google Docs - Centrul de învățare Google Workspace](#)
5. [Ce este Google Drive și cum se folosește - J.D.M](#)
6. <https://barrazacarlos.com/ro/avantaje-si-dezavantaje-ale-google-drive/>



ISBN: 978-606-37-2623-1