# DIGITAL MINDSET ÎN EDUCAȚIE – EDUCAȚIA DE SECURITATE –

*Andreea LOSEKAMM*

*Specialist în management administrativ și reprezentant federal pentru contractare în cadrul FAC-C/Consulatul General al Statelor Unite ale Americii în Frankfurt, Germania/ Departamentul de Stat al SUA*

10.55535/GMR.2023.2.10

*Siguranța și protecția libertăților constituie una dintre provocările cheie cu care se confruntă actualmente sistemul educațional în contextul digitalizării, provocare ce necesită promovarea unei definiții mai elaborate a democrației digitale corelată cu preocupări legate de drepturile omului, inegalitatea dezvoltării prin accesul la educație, responsabilitate și, nu în ultimul rând, construirea de consens în medii cu o mare diversitate. Securitatea, ca valoare fundamentală a societăților democratice, cere așadar o redimensionare în raport cu principiile promovate de instituțiile politice – incluziune, responsabilitate și transparență –, discutabilă pe fundalul polarizării politice și apariției noilor tehnologii digitale. Articolul de față nu pretinde a propune o teorie generală cu privire la modul în care digitalizarea educației și democrația se raportează sau se exclud reciproc. Acesta tratează situații mai mult sau mai puțin contingente și ridică întrebări suplimentare – inclusiv empirice – cu privire la rolul pe care digitalizarea în sistemul educațional îl poate avea pentru starea democrației, indiferent de nivelul de comprehensiune. Intenția este dirijată către modul concret în care digitalizarea poate fi benefică pentru democrație și unde poate fi neadecvată, contribuind la o mai bună înțelegere a provocărilor. Cititorul poate traduce acest lucru în propriul său mediu, legând lectura personală de procese democratice specifice, inclusiv de nivelul și tipul activității digitale.*

*Cuvinte-cheie: sistem educațional, digitalizare, securitate cibernetică, democrație, infrastructuri critice.*





GÂNDIREA MILITARĂ ROMÂNEASCĂ

## DEZVOLTAREA EXPLICATĂ ÎN CODURI NUMERICE BINARE

Lumea digitală este împărțită în structuri clare, sigure și raționale, constând în serii de secvențe de numere – în cele din urmă, coduri numerice binare. Digitalizarea în sine nu înseamnă, practic, altceva decât reprezentarea și stocarea informațiilor, rezultând în exprimarea acțiunilor și valorilor în coduri. Cu toate acestea, impactul transformării digitale nu este simplificat prin aducerea la un numitor comun. Valorile principale ale democrației – libertate, egalitate, demnitate, solidaritate, statul de drept – nu pot fi transpuse în secvențe numerologice. Sub formă de coduri, acestea sunt aplicabile în mod egal atât realității fizice, cât și celei virtuale, iar măsurile care urmează să fie implementate în domeniul securității cibernetice trebuie să respecte în totalitate aceste principii.

Reconfigurarea relației dintre securitate și democrație este apriorică în eforturile naționale pentru a stabiliza criza democratică din sistemul de învățământ invocată de incapacitatea unor guvernări de a oferi un sistem responsabil și adaptiv cu transformarea digitală. Studiul digitalizării sigure și adaptive variază, dar nu depășește conceptul de regionalism sau globalizare, întrucât incluziunea se datorează în esență acestor concepte. În înțelegerea percepțiilor de securitate față de complexitatea procesului de tehnologizare este necesară examinarea acestei reconfigurări fundamentale de-a lungul a două perspective distincte: readaptarea și reproiectarea securității (democratice), cuprinzând modurile diferite și uneori contradictorii în care se schimbă formele democratice de guvernare a securității.

*Studiul digitalizării sigure și adaptive variază, dar nu depășește conceptul de regionalism sau globalizare, întrucât incluziunea se datorează în esență acestor concepte. În înțelegerea percepțiilor de securitate față de complexitatea procesului de tehnologizare este necesară examinarea acestei reconfigurări fundamentale de-a lungul a două perspective distincte: readaptarea și reproiectarea securității (democratice), cuprinzând modurile diferite și uneori contradictorii în care se schimbă formele democratice de guvernare a securității.*

## RAPORTUL EDUCAȚIE – DEMOCRAȚIE – SECURITATE

Subiectul democratizării digitale este unul complex, legat de diferite concepte, precum securitate, participare, adaptare și, nu în ultimul rând, transformare. Pornind de la aceste principii, articolul propune un concept de democrație digitală ca o combinație a dimensiunilor: informație – participare – transformare, dimensiuni preluate din fundamentul educației.

Educația este o nevoie de bază pentru fiecare ființă umană, iar educația digitală este tendința și necesitatea actuală. Deloc imprevizibil, această temă este adesea abordată în conexiune cu prelucrarea de date și implică preocupările legate de confidențialitate, creșterea inegalității, riscul de stigmatizare și discriminare (fie că aceasta este deliberată sau, pur și simplu, o consecință neintenționată). Având în vedere costurile enorme ale creării și întreținerii cursurilor pe platforme online, este surprinzător că securitatea nu este considerată încă o problemă majoră de către autorități, inclusiv profesori și studenți. Spre deosebire de cercetarea tradițională în domeniul securității, care a fost în mare măsură determinată de cerințele militare de a impune secretul, în domeniul e-learning, nu informațiile în sine trebuie protejate împotriva accesului neautorizat, ci modul în care acestea sunt prezentate. În cele mai multe cazuri, cunoștințele conținute în programele de e-learning sunt mai mult sau mai puțin accesibile; prin urmare, nu informația în sine este elementul destabilizator al securității, ci modalitatea folosită pentru a o transmite.

*Spre deosebire de cercetarea tradițională în domeniul securității, care a fost în mare măsură determinată de cerințele militare de a impune secretul, în domeniul e-learning, nu informațiile în sine trebuie protejate împotriva accesului neautorizat, ci modul în care acestea sunt prezentate. În cele mai multe cazuri, cunoștințele conținute în programele de e-learning sunt mai mult sau mai puțin accesibile; prin urmare, nu informația în sine este elementul destabilizator al securității, ci modalitatea folosită pentru a o transmite.*

Într-un mediu de predare securizat, utilizatorii nu trebuie să fie îngrijorați de amenințările specifice platformelor de învățare și de comunicarea electronică în general. O platformă de învățare sigură ar trebui să încorporeze aspecte ale securității astfel încât majoritatea proceselor să fie transparente pentru profesor și elev. Totuși, asigurarea unui sistem complet sigur este un obiectiv prea ambițios, deoarece nimic nu poate fi niciodată complet sigur și – în același timp – rămâne încă utilizabil. Prin urmare, sistemul ar trebui să permită utilizatorului să decidă compromisul dintre utilitate și securitate.

## VULNERABILITĂȚILE SECURITĂȚII INFORMAȚIEI

Pentru dezvoltarea planurilor operaționale, combinația de amenințări, vulnerabilități, precum și efectele acestora trebuie să fie evaluate pentru a identifica tendințe importante și a decide în cazul în care ar trebui să se depună eforturi în vederea eliminării sau a reducerii capacităților amenințărilor, a vulnerabilităților; de asemenea, trebuie să se evalueze, coordoneze și elimine conflictele tuturor operațiunilor spațiului cibernetic (Locke, Gallagher, 2011, p. 1).

Privind sistemul democratic din perspectiva creșterii vulnerabilităților, constatăm că noul model de securitate trebuie să fie – astăzi mai mult ca niciodată – receptiv la provocările globale și capabil să facă față unui mediu politic din ce în ce mai complex și digital. Creșterea populismului, apariția unor mentalități din ce în ce mai radicale, scăderea încrederii în instituțiile politice și așteptările crescute față de participarea politică adaugă provocări suplimentare proceselor și structurilor consacrate ale democrațiilor liberale. Deși transformarea digitală nu va fi singurul răspuns la aceste provocări, ea va fi totuși cheia pentru ca instituțiile democratice și părțile politice interesate să acționeze decisiv într-o lume din ce în ce mai inovativă.

Contextul actual afișează o plenitudine de exemple de rezistență în fața inovației sau de adaptare diferențială a noilor tehnologii (Frey, 2019, p. 59). Personalizarea unui sistem social nu se face de la sine. Participarea trebuie să fie personalizată; fiecare grup necesită o abordare diferită, o limbă diferită și o metodă de lucru diferită (Agenția Uniunii Europene pentru Securitatea Rețelelor și Informațiilor/ENISA, 2015). Oportunitățile pe care le oferă digitalizarea pentru democratizare sunt departe de a fi exploatate pe deplin, întrucât schimbarea tehnologică este o schimbare profundă: proces politic adeseori contestat, al cărui rezultat depinde nu doar de tehnologiile în sine, ci și de modul în care țările reacționează la ele (Schaefer, Coopersmith, 2018).

*Oportunitățile pe care le oferă digitalizarea pentru democratizare sunt departe de a fi exploatate pe deplin, întrucât schimbarea tehnologică este o schimbare profundă: proces politic adeseori contestat, al cărui rezultat depinde nu doar de tehnologiile în sine, ci și de modul în care țările reacționează la ele.*

Din prisma sferei politice, digitalizarea este văzută în principal ca o amenințare la adresa discursului democratic și nu ca o oportunitate. Înșuși Bogdan Aurescu, în calitatea sa de ministru al Afacerilor Externe, afirma, cu ocazia celebrării Zilei Internaționale a Democrației (2021), că amenințările la adresa regimurilor democratice au depășit granițele de natură fizică, răspândindu-se în lumea virtuală (*Bursa*, 2021).

Un stat trebuie să dezvolte o politică cuprinzătoare de securitate a informațiilor, care să conțină toate domeniile și funcțiile critice de securitate cibernetică necesare din cadrul instituțiilor. Accentul documentației politicii trebuie să fie tehnic, fizic și administrativ.

## NOȚIUNI ȘI CONCEPTE ALE SECURITĂȚII INFORMAȚIILOR

Noțiunea de securitate informatică sau cibernetică este definită ca *„starea de normalitate rezultată în urma aplicării unui ansamblu de măsuri proactive și reactive prin care se asigură confidențialitatea, integritatea, disponibilitatea, autenticitatea și nonrepudierea informațiilor în format electronic, a resurselor și serviciilor publice sau private din spațiul cibernetic”* (ENISA, 2022). Securitatea informației este protecția informațiilor împotriva amenințărilor, implementată pentru

a asigura continuitatea fluxului de informație. Cyber Security Challenge Germany/CSCG recomanda Comisiei Europene, în 2015, să-și armonizeze utilizarea termenilor cheie *„securitate cibernetică”, „NIS”* și *„crimă cibernetică”* (ENISA, 2015, p. 8) în întreaga Uniune Europeană, pe baza definițiilor existente. În prezent, comunicările oficiale folosesc toți cei trei termeni fără a face distincție între ei, ceea ce ar putea duce la o interpretare diferită în diferite state membre ale UE (sau limbi). CSCG recomanda, de asemenea, stabilirea și punerea în aplicare a unui model de guvernanță adecvat pentru cele trei domenii, cu accent special pe evitarea *„lucrului în siloz”*[1] pe subiecte care sunt în mod inerent asociate (CNRISC, 2018).

Prin restrângerea contextului general al discuțiilor privind securitatea cibernetică la nivel național, observăm importanța separării conceptuale a direcțiilor principale de acțiune: apărare cibernetică, criminalitate informatică, securitate națională, infrastructuri critice și situații de urgență, diplomație cibernetică internațională și guvernanța internetului. Este nevoie să se stabilească foarte clar rolurile și responsabilitățile fiecărei instituții naționale, în parte.

*Guvernarea securității informațiilor este definită ca „stabilirea și menținerea mediului de control pentru gestionarea riscurilor legate de confidențialitatea, integritatea și disponibilitatea informațiilor întru susținerea proceselor și sistemelor”.*

Potrivit ISO (ISO 38500[2]), guvernanța precizează cadrul de responsabilitate și oferă supraveghere pentru a se asigura că riscurile sunt atenuate în mod adecvat în timp ce conducerea se asigură că sunt implementate controale pentru atenuarea riscurilor. Conducerea recomandă strategii de securitate. Guvernanța asigură că strategiile de securitate sunt aliniate cu obiectivele de afaceri și sunt conforme cu reglementările. Guvernarea securității informațiilor este definită ca *„stabilirea și menținerea mediului de control pentru gestionarea riscurilor legate de confidențialitatea, integritatea și disponibilitatea informațiilor întru susținerea proceselor și sistemelor”* (Moulton, Coles,

[1] *„Lucrul* în *silozuri”* prezintă o situație în care indivizii și echipele lucrează pentru îndeplinirea aceluiași obiectiv, dar nu comunică în mod suficient. Termenul *„silo”*, în sine, se referă la containerele/recipientele utilizate pentru depozitarea cerealelor. Dar are și o semnificație abstractă, în sensul că este folosit ca o metaforă pentru grupuri de oameni care lucrează independent de alte grupuri. Potrivit jurnalistei britanice Gillian Tett, specializată în antropologie, *„silozurile sunt fenomene culturale care apar din sistemele pe care le folosim pentru a clasifica și a organiza lumea”*, https://www.ideagen.com/thought-leadership/blog/working-in-silos, accesat la 21 februarie 2023. (n.red.).

[2] ISO/IEC 38500:2015 – *Information technology. Governance of IT for the organization* – este un standard internațional pentru guvernanța corporativă a tehnologiei informației, publicat în comun de Organizația Internațională de Standardizare (ISO) și Comisia Electrotehnică Internațională (IEC), https://www.iso.org/standard/62816.html, accesat la 29 februarie 2023 (n.red.).





2003, pp. 580-584). Din alt punct de vedere, aceasta este considerată parte a guvernanței care implică implementarea conceptelor și principiilor de guvernanță în ceea ce privește problemele de securitate a informațiilor (Abu-Musa, 2010, pp. 226-276). Guvernanța securității informațiilor, în esență, cuprinde un management bun al riscurilor, controale robuste de raportare, testare, instruire și, nu în ultimul rând, responsabilitate constantă. Oferă direcția strategică pentru activitățile de securitate cibernetică și asigură îndeplinirea obiectivelor de securitate cibernetică stabilite la nivel național.

Un bun proces de guvernare a securității informațiilor poate transforma o instituție și poate aduce unul sau mai multe dintre următoarele beneficii de securitate cibernetică: (1) alocare structurată, concentrată și prioritizată a timpului, resurselor economice și eforturilor; (2) conformitate cu politicile de securitate a informațiilor; (3) previzibilitate mai bună și mai puțină incertitudine; (4) luarea deciziilor care se bazează pe o structură clară; (5) poziție consolidată atunci când se confruntă cu consecințe legale și (6) responsabilitate clară a actorilor implicați și o mai bună protecție a informațiilor.

*Un bun proces de guvernare a securității informațiilor poate transforma o instituție și poate aduce unul sau mai multe dintre următoarele beneficii de securitate cibernetică: alocare structurată, concentrată și prioritizată a timpului, resurselor economice și eforturilor; conformitate cu politicile de securitate a informațiilor; previzibilitate mai bună și mai puțină incertitudine; luarea deciziilor care se bazează pe o structură clară.*

Pentru a ajuta la implementarea unei bune guvernanțe de securitate a informațiilor, este esențial un cadru de bază menit să sprijine și să se asocieze perfect cu obiectivele democrației. Un cadru de securitate cibernetică oferă statelor capacitatea de a se proteja de amenințările cibernetice aflate în evoluție. Obiectivul principal al unui cadru de securitate cibernetică include: (1) armonizarea abordărilor de securitate cibernetică și crearea unui limbaj comun; (2) stabilirea nivelului optim de securitate cibernetică adaptat mediului și nevoilor specifice; (3) alocarea unui buget suficient de securitate cibernetică pentru implementarea cadrului; (4) un schimb eficient de cunoștințe despre riscurile cibernetice.

Conform Institutului Național de Standarde și Tehnologie (NIST), guvernarea securității informațiilor implică stabilirea și menținerea unui cadru care să ofere asigurarea că strategiile de securitate a informațiilor sunt aliniate și sprijină obiectivele de guvernare, sunt în concordanță cu legile și reglementările aplicabile prin respectarea politicilor și a politicilor interne și oferă repartizarea responsabilității, totul într-un efort de a gestiona riscul. Acest cadru cuprinde cinci acțiuni: identifică, protejează, detectează, răspunde, recuperează.

Structura conceptului de securitate simplificată are trei niveluri (Tirziu, 2015, pp. 121-122): (1) Securitatea fizică – aceasta constă în prevenirea, detectarea și limitarea accesului direct asupra informațiilor. În momentul de față, distrugerile de informații cauzate de perturbări ale nivelului de securitate fizică sunt considerate a reprezenta cea mai mare vulnerabilitate. (2) Securitatea logică – reprezentată de totalitatea metodelor ce asigură controlul asupra accesului la resursele și serviciile sistemului și (3) Securitatea juridică, aceasta reprezentând nivelul constituit dintr-o colecție de legi naționale care au rolul de a reglementa actul de violare a primelor două niveluri de securitate menționate mai sus și de a stabili sancțiuni penale pentru aceste acte (Locke, Gallagher, p. 1).

*E-learning este implementarea tehnologiei pentru a sprijini procesul de învățare prin care cunoștințele sau informațiile pot fi accesate folosind tehnologia comunicațiilor. Procesul de învățare poate fi continuu, cu condiția ca disponibilitatea conținutului să existe online.*

## SETAREA TEHNOLOGICĂ ÎN ÎNVĂȚĂMÂNTUL ROMÂNESC

Obiectivele e-learning sunt preocupate de furnizarea de predare hibridă la scară largă, iar principalul scop în strânsă legătură cu securitatea este asigurarea disponibilității și integrității informațiilor. E-learning este implementarea tehnologiei pentru a sprijini procesul de învățare prin care cunoștințele sau informațiile pot fi accesate folosind tehnologia comunicațiilor. Procesul de învățare poate fi continuu, cu condiția ca disponibilitatea conținutului să existe online. Deși consecințele pe termen lung ale evoluțiilor economice, sociale și politice sunt prea puțin previzibile, subiect speculativ, primele efecte ale setării tehnologice asupra peisajului educațional român sunt sesizabile de ceva timp. Societatea, cultura și educația sunt augmentate și afectate în mod egal de digitalizarea în curs, având așadar influență bivalentă asupra dezvoltării de cunoștințe și participării politice și structurilor sociale.

Anul 2020 a marcat începutul pandemiei virusului Sars-COV-2 și a bolii asociate, Covid-19. Concomitent, a fost adusă în prim-plan necesitatea reconfigurării practicilor de abordare în sistemul educațional, prin: lipsa de predictibilitate; o rețea școlară eterogenă, cu un puternic decalaj digital între unitățile de învățământ; competențe digitale insuficient dezvoltate pentru organizarea eficientă a procesului didactic în mediul online; acces redus la tehnologie și conectivitate redusă la internet, precum și posibilitățile reduse ale familiilor în a acorda sprijin beneficiarilor educației, copiii, pentru participare la lecții online (Smart-Edu, 2020). Trecerea abruptă de la tradiționalul interacțiunea







*„față-în-față”* la mediul online a arătat, în scurt timp, că viitorul educației implică tehnologia emergentă și că predarea, învățarea și digitalizarea nu pot fi discutate disparat. În acest context, sistemul de învățământ a trecut și continuă să treacă prin schimbări revoluționare, folosind expresia darwiniană *„nu supraviețuiesc speciile cele mai puternice, nici cele mai inteligente, ci cele mai ușor adaptabile”.*

Cu toate acestea, încă nu a fost dezvoltată o strategie standard de digitalizare. Abordarea fundamentală constă în identificarea soluțiilor de transfer de cunoaștere la nivel global și a metodelor adaptive orientate către incluziune uniformă. Transferul de practici și metode între instituții la orice nivel este considerat o problemă complexă, care necesita angrenarea tuturor resurselor. Înțelegerea acestui transfer oferă un fundament necesar și suficient în gestionarea dezvoltării, deoarece poate susține administrațiile complexe să devină inovatoare și să construiască o serie de capacități dinamice. Transferul altor modele de management al cunoașterii este aprioric așadar pentru abordarea unor teme precum sisteme de anticipație sau de evaluare a riscurilor la adresa securității utilizării tehnologiei folosite cu și pentru elevi.

În raport cu difuziunea culturii de securitate socială, emergența practicilor și modelelor democratizării digitale solicită transparență emergentă și integrabilă etapelor de adaptare instituțională. În continuare, o astfel de soluție presupune atât adaptarea legislației (adaptarea mediului de securitate și informații), cât și o strategie bine definită (adaptarea organizației de securitate și informații).

*Îmbunătățirea produselor software, a disponibilității acestora și a sistemului de învățământ în domeniul introducerii și utilizării tehnologiei informației este o caracteristică dominantă în dezvoltarea managementului (dar și a altor) procese curente.*

## PROVOCĂRI PRINCIPALE, PRIORITĂȚI ȘI DIRECȚII DE ACȚIUNE

**Provocări principale.** Provocările cheie sunt: accesibilitatea, incluziunea, dobândirea competențelor digitale și, nu în ultimul rând, securitatea pentru toți actorii implicați. Cea mai importantă poziție rămâne aceea a ființei umane. Îmbunătățirea produselor software, a disponibilității acestora și a sistemului de învățământ în domeniul introducerii și utilizării tehnologiei informației este, astfel, o caracteristică dominantă în dezvoltarea managementului (dar și a altor) procese curente. Așadar, cum poate sistemul educațional românesc să facă față riscurilor de securitate legate de revoluția digitală fără a pune în pericol valorile democratice fundamentale? Cât de incluziv

este dialogul de securitate și cooperare la nivel guvernamental și instituțional? Și, nu în cele din urmă, care sunt mecanismele prin care se reconstruiește o digitalizare responsabilă?

Cea mai comună soluție în astfel de contexte este dezvoltarea forțată a unor noi perspective. Sursa acestui paradox derivă din conceptul de democrație digitală ca o combinație a dimensiunilor: informație, securitate, participare și transformare. Îndemnarea se face către o imagine a digitalizării ca un proces care depășește procesele analogice anterioare, prezentând căi alternative către implementarea și valorificarea oportunităților democrației digitale responsabile prin readaptarea și reproiectarea mecanismelor. Plecând de la tiparele de interacțiune între instituțiile de învățământ românesc și mediul de invățare la nivel internațional, lucrarea propune ca soluție durabilă la adresa inovației ideea definirii guvernării securității informațiilor.

*Utilizarea tehnologiei în educație nu reprezintă doar o tendință sau o influență asupra proceselor educaționale. În circumstanțele actuale, abordarea reprezintă o necesitate pentru formarea viitorului elevilor și al studenților prin însușirea capabilităților și abilităților specifice.*

Este necesară o nouă perspectivă teoretică, aceasta generând o strategie adaptativă de gestionare a cunoștințelor, fără a exclude riscurile implicate. Adaptarea sistemelor complexe la modelele actuale necesită un plan adaptativ. Metoda va determina care structură din cadrul acestei ecuații este supusă modificării și ce strategii structurale trebuie aplicate pentru ca structura și întregul sistem să se încadreze mai bine în mediul social. Planul urmărește crearea unor astfel de noi direcții, menite să îmbunătățească performanța resurselor participative și eliminarea amenințărilor la adresa democrațiilor analizate.

**Priorități și direcții de acțiune.** Putem afirma că utilizarea tehnologiei în educație nu reprezintă doar o tendință sau o influență asupra proceselor educaționale. În circumstanțele actuale, abordarea reprezintă o necesitate pentru formarea viitorului elevilor și al studenților prin însușirea capabilităților și abilităților specifice. Pentru ca această necesitate să răspundă punctual provocărilor enumerate mai sus, identificarea clară a priorităților este apriorică. Doar astfel, direcțiile de acțiune pot fi ancorate în inițiative, măsuri și programe care susțin rolul tehnologiei digitale în dezvoltarea sistemelor de educație și formare.

SmartEdu pentru Școală Modernă, Accesibilă, bazată pe Resurse și Tehnologii digitale, preluând Strategia privind digitalizarea educației din România, propune următoarele priorități: accesibilitate, conectivitate, comunitate, ecosistem edicațional digital, inovare și sustenabilitate (Sart-Edu, 2020).





O asemenea abordare se cere corelată cu etapa punerii în aplicare a unui plan de acțiune și, cel mai probabil, aceasta coincide cu etapa de pregătire a cadrului normativ și legislativ ce susține digitalizarea responsabilă și sigură în învățământul românesc.



## CONCLUZII

În acest articol, au fost prezentate informații despre tehnologie și securitate în sistemul de educație în termenii unei agende de cercetare. Am evidențiat că securitatea instituției de învățământ necesită o contribuție substanțială la activități de cercetare și dezvoltare. Reconfigurarea interactivă a infrastructurilor tehnice și sociale ale societății contemporane examinate în contextul lor socio-tehnic educațional vine în acord cu dinamica evoluțiilor și tendințelor la nivel global: informația, cea mai importantă resursă.

Comportamentul de securitate este corelat cu utilizarea tehnologiei și cultura securității informațiilor în școli. În mediile educaționale, problema comportamentului de securitate al utilizatorilor este văzută ca un fenomen multidimensional combinat cu utilizarea tehnologiei, învățării, comunicare și predare. Astfel, angajamentele teoretice pentru înțelegerea culturii securității informațiilor ar trebui analizate pe baza practicilor concrete și a interacțiunilor în timpul utilizării e-learning-ului. Conștientizarea securității informației este de o importanță capitală, deoarece ne poate ajuta să identificăm potențialele amenințări înainte ca acestea să apară și, totodată, să aplice măsuri de susținere a digitalizării responsabile și sigure în timp. Raportându-ne la obiectivele României în procesul de dezvoltare a învățământului informațional și de implementare a programelor electronice de educare, se constată că încă sunt necesari pași pentru asigurarea tuturor resurselor și a unui cadru integrat pentru acces la o educație de calitate în era digitală. Elaborarea unui program național în baza reperelor trasate de Strategia privind digitalizarea educației în România menit să asigure elaborarea și punerea în practică a unor proiecte concrete de securitate cibernetică este prioritară.

*Raportându-ne la obiectivele României în procesul de dezvoltare a învățământului informaţional şi de implementare a programelor electronice de educare, se constată că încă sunt necesari pași pentru asigurarea tuturor resurselor și a unui cadru integrat pentru acces la o educație de calitate în era digitală.*

Lipsa unei abordări unitare de inițiative, măsuri și programe aliniate cu contextul actual al problemelor de securitate informațională reprezintă un factor de risc pentru asigurarea confidențialității informației și a securității componentelor sistemului informațional

al instituțiilor. Compromiterea securității informației poate duce la afectarea credibilității instituției publice, poate conduce la fraude sau distrugerea datelor, divulgarea informațiilor confidențiale etc. Fenomenul criminalității cibernetice este, prin natura sa, în dezvoltare rapidă, transnațional și fără granițe. În funcție de tipul de vulnerabilitate, metodele de protecție specifice tehnologiei informatice din ziua de astăzi sunt variate. Soluțiile date de direcțiile de acțiune reprezintă doar startul în realizarea unor standarde și tehnologii de securitate din ce în ce mai elaborate, performante, făcând ca exploatarea vulnerabilităților de natură tehnologică să devină tot mai dificilă.

## BIBLIOGRAFIE:


1. Abu-Musa, A. (2010). *Information Security Governance in Saudi organizations: an Empirical Study*. În *Information Management& Computer Security*, 18(4), pp. 226-276.
2. Aurescu, B. (15 septembrie 2021). *„Amenințările la adresa regimurilor democratice au depășit granițele de natură fizică, răspândindu-se în lumea virtuală”*, în *Bursa*, https://www.bursa.ro/bogdan-aurescu-amenintarile-la-adresa-regimurilor-democratice-au-depasit-granitele-de-natura-fizica-raspandindu-se-in-lumea-virtuala-07992445, accesat la 24 noiembrie 2022.
3. Frey, C.B. (2019). *The Technology Trap: Capital, Labor, and Power in the Age of Automation.* Princeton, NJ&Oxford: Princeton University Press.
4. Locke, G., Gallagher, P.D. (martie 2011). *Information security*. *NIST Special Publication* 800-39, Gaithersburg, MD: Computer Security Division/Information Technology Laboratory/National Institute of Standards and Technology.
5. Moulton, R., Coles, R.S. (2003). *Applying Information Security Governance. Computers&Security*, 22(7), pp. 580-584.
6. Naqvi, W.M., Sahu, A. (2020). *Paradigmatic shift in the education system in a time of COVID 19 Evolution*. În *Journal of Medical and Dental Sciences,* 9 (27): 1974-1976, DOI: 10.14260/jemds/2020/430.
7. Pup, A. (15 martie 2022). *Digitalizarea educației în ultimii doi ani de pandemie. Măsurile pe care autoritățile le-au promis și nu le-au realizat.* În *Libertatea*, https://www.libertatea.ro/stiri/digitalizarea-educatiei-in-ultimii-doi-ani-de-pandemie-masurile-pe-care-autoritatile-le-au-promis-si-nu-le-au-indeplinit-4031891, accesat la 24 noiembrie 2022.
8. Schaefer, D., Coopersmith, J. (2018). *Kranzberg's Fifth and Fourth Laws*. În Technology's Stories, vol. 6, nr. 4. DOI: 10.15763/jou.ts.2018.12.20.02.









9. Tirziu, A.M. (2015). *Protection and security of information at the level of national public authorities from Romania*. *MPRA Paper 77711*. München: University Library of Munich.
10. Banca Centrală Europeană. (2022). *Digitalizarea și evaluarea stategiei*. *BCE,* https://www.ecb.europa.eu/home/search/review/html/digitalisation.ro.html, accesat la 24 noiembrie 2022.
11. Centrul Național de Răspuns la Incidente de Securitate Cibernetică (CNRISC). (2019). *Evoluția amenințărilor în spațiul cibernetic românesc în anul 2018.* Directoratul Național de Securitate Cibernetică, https://dnsc.ro/vezi/document/raport-alerte-2018, accesat la 26 august 2022.
12. Comisia Europeană. (2020). *Noua strategie de securitate cibernetică a UE și noi norme menite să sporească reziliența entităților fizice și digitale critice*. Comisia Europeană, https://ec.europa.eu/commission/presscorner/api/files/document/print/ro/ip_20_2391/IP_20_2391_RO.pdf, accesat la 26 august 2022.
13. *Digitalizarea sistemului educațional – propunere de politici publice* (4 iunie 2019), *Syene*, https://syene.ro/2019/06/04/digitalizarea-sistemului-educational-propunere-de-politici-publice/, accesat la 24 noiembrie 2022.
14. ENISA (2015). *Definition of Cybersecurity – Gaps and overlaps in standardisation*, https://www.enisa.europa.eu/publications/definition-of-cybersecurity, accesat la 24 noiembrie 2022.
15. ENISA. (2022). *Strategia națională de securitate cibernetică a României*. Articol în lucru, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/roncss.pdf, accesat la 24 noiembrie 2022.
16. Ministerul Educației și Cercetării. (2020). *Digitalizarea educației din România 2021-2027. Școală Modernă, Accesibilă, bazată pe Resurse și Tehnologii digitale* – SmartEdu, online, preluând Strategia privind digitalizarea educației din România, document în consultare publică în perioada 18 decembrie 2020 – 15 februarie 2021, https://www.smart.edu.ro, accesat la 24 noiembrie 2022.