

# MANUAL DE EDUCAȚIE (ALFABETIZARE) ÎN DOMENIUL INTERNETULUI

” Sprijinirea utilizatorilor  
în mediul online

Construind o Europă  
cu și pentru copii  
[www.coe.int/children](http://www.coe.int/children)





# **MANUAL DE EDUCAȚIE (ALFABETIZARE) ÎN DOMENIUL INTERNETULUI**

Sprijinirea utilizatorilor  
în mediul online

Consiliul European

Ediția engleză:

*Internet Literacy Handbook*

Opiniile exprimate în prezenta lucrare reprezintă responsabilitatea autorului (autorilor) și nu reflectă, în mod necesar, politica oficială a Consiliului European.

Toate drepturile rezervate. Nicio parte a prezentei publicații nu poate fi tradusă, reprodusă sau transmisă, sub nicio formă sau prin niciun fel de mijloace, electronice (CD-ROM, Internet etc.) sau mecanice, inclusiv fotocopiere, înregistrare sau orice sistem de stocare sau recuperare de informații, fără permisiunea prealabilă în scris a Direcției de Comunicare (F-67075 Strasbourg Cedex sau [publishing@coe.int](mailto:publishing@coe.int)).

Copertă, așezare în pagină și grafică: Iddifix

Editura Consiliului European  
F-67075 Strasbourg Cedex  
<http://book.coe.int>

Autori: Janice Richardson, Elizabeth Milovidov  
și Martin Schmalzried

Manual de Educație (alfabetizare) în domeniul  
internetului

Text creat de, și folosit cu permisiunea Consiliului European. Această traducere neoficială este publicată în acord cu Consiliul European, dar cu responsabilitatea unică a traducătorului.

© Consiliul European, martie 2020

Machetat în cadrul proiectului "Protecția copiilor împotriva exploatării sexuale și abuzului sexual în Republica Moldova"

# Cuprins

---

<b>CUVÂNT ÎNAINTE</b>	<b>7</b>
<b>INTRODUCERE</b>	<b>9</b>
<b>1. INTERNETUL – ORICÂND, ORIUNDE</b>	
Fișa 1 – Conectarea	13
Fișa 2 – Prezența în mediul online și pe „nor” (cloud)	19
Fișa 3 – Web 2.0, Web 3.0 și alte versiuni	25
Fișa 4 – Blogurile și vlogurile	31
Fișa 5 – Internetul în mișcare	37
<b>2. INTERNETUL – CONECTAREA IDEILOR ȘI A OAMENILOR</b>	
Fișa 6 – Emailul și comunicarea	45
Fișa 7 – Rețelele de discuții și mesagerie	51
Fișa 8 – Socializarea online și distribuirea pe rețelele sociale	57
Fișa 9 – Viața privată și setările de confidențialitate	63
<b>3. INTERNETUL – PARTICIPAREA LA SOCIETATEA CUNOAȘTERII</b>	
Fișa 10 – Căutarea informațiilor	73
Fișa 11 – Găsirea informațiilor de calitate pe web	79
Fișa 12 – Învățământul la distanță și cursurile online deschise cu participare nelimitată (CODPN-urile)	85
Fișa 13 – Cumpărăturile în mediul online	91
<b>4. INTERNETUL – PENTRU TOATĂ LUMEA</b>	
Fișa 14 – Videoclipurile, muzica și imaginile pe Internet	97
Fișa 15 – Creativitatea	103
Fișa 16 – Jocurile	107
Fișa 17 – Cetățenia digitală	111
Fișa 18 – Parentajul digital: pozitiv și proactiv	119
<b>5. INTERNETUL – RĂSPUNS LA PROVOCĂRI</b>	
Fișa 19 – Criminalitatea informatică: mesajele comerciale nesolicitate (spam), codurile ostile (malware), fraudă și securitatea	127
Fișa 20 – Etichetarea și filtrarea	133
Fișa 21 – Hărțuirea în mediul online: bullying-ul, stalking-ul și trolling-ul	139
Fișa 22 – Obținerea de asistență	145
<b>6. INTERNETUL – O PRIVIRE ÎN VIITOR</b>	
Fișa 23 – Internetul obiectelor	151
Fișa 24 – Inteligența artificială, automatizarea și tehnologiile perturbatoare	157
Fișa 25 – Realitatea virtuală și realitatea augmentată	163
Fișa 26 – Sunteți produsul? Examinarea volumelor mari de date (big data), extragerea de date și viața privată	169

## Mulțumiri

**Janice Richardson** este consultant în domeniul drepturilor copiilor în mediul online de câteva decenii și a condus echipa editorială pentru acest manual. Fiind, până în anul 2014, coordonatoare a rețelei *Insafe* a Comisiei Europene care cuprinde 30 de țări și, mai recent, a rețelei *ENABLE* împotriva bullying-ului, Janice este, de asemenea, membră a Comitetului Consultativ al Facebook pentru Siguranță.

**Elizabeth Milovidov**, dr. în drept, este consultantă în domeniul siguranței în mediul online, având o experiență de peste 20 de ani în calitate de avocată, profesor de drept și susținătoare a drepturilor copilului. Misiunea acesteia este de a informa și abilita părinții și copiii în privința aspectelor legate de Internet, tehnologii și rețelele sociale. E. Milovidov este, de asemenea, fondatoarea *DigitalParentingCoach.com*.

**Martin Schmalzried** este Ofițer Senior de Politici pentru COFUE (Confederația Organizațiilor Familiale din UE) și este specializat în noile tehnologii și un Internet mai sigur. Acesta este președinte al proiectului *SIP BENCH III* (evaluarea instrumentelor de control parental) și a fost implicat în numeroase proiecte și inițiative ale UE din acest domeniu

# Cuvânt înainte

---

■ Cât de important este să deții competențe de utilizare a Internetului? Răspunsul scurt la această întrebare este destul de clar: foarte important. Numărul utilizatorilor de Internet se apropie rapid de 3,5 miliarde, dintre care aproximativ 20% sunt în regiunea europeană. Și în timp ce Internetul oferă un flux de informații care sunt aflate și partajate, navigarea în siguranță prin complexul univers online, poate fi o sarcină dificilă. Prin urmare, este necesar să existe un set de cunoștințe de bază.

■ Acest manual oferă acel set de cunoștințe care sunt redade printr-un limbaj simplu și accesibil. Prezenta publicație nu este completamente nouă, ci reprezintă o serie de sfaturi utile, care evoluează în permanență, cu privire la modul de abordare a fluxului informațional în continuă creștere. Versiunea online a manualului este în egală măsură redată clar, datorită și graficii captivante, astfel încât secțiunile să poată fi prezentate grupurilor din sălile de clasă sau din centrele comunitare. În acest fel, acesta poate fi utilizat ca un instrument de instruire pentru toate grupurile de vârstă.

■ Elucidând o multitudine de complexități, manualul oferă perspective asupra considerentelor etice și a riscurilor asociate schimbului de informații: în cazul în care dorim să utilizăm Internetul pentru a ne potoli setea de cunoaștere și a ne împărtăși gândurile și opiniile, atunci trebuie să o facem în mod responsabil. Principiile de bază privind drepturile omului se aplică în aceeași măsură în lumea digitală, ca și în cea offline. Acestea sunt aplicabile, de exemplu, în raport cu respectarea libertății de exprimare și a vieții private a celorlalți în mediul online, precum și respectarea vieții noastre private de către ceilalți. Cum ne asigurăm că datele noastre personale sunt în siguranță? Ce facem în cazul în care întâlnim conținuturi ilegale sau suntem ținta bullying-ului sau a discursului care instigă la ură? Aceste subiecte și multe, multe altele sunt prezentate sub formă de recomandări și sfaturi practice pentru un public deschis. Manualul invită cititorii să aibă o gândire critică față de ceea ce văd și citesc în mediul online și să facă alegeri informate și sigure.

■ Când ne aflăm în mediul online pentru a împărtăși idei, în același timp ne orientăm spre cunoașterea și înțelegerea lucrurilor noi; putem contesta înțelepciunea convențională și putem crea rețele pentru o schimbare pozitivă. Acest fapt este evident, în special în cazul generațiilor mai tinere, cărora Internetul le oferă oportunități nesfârșite de a explora, învăța, socializa și crea, fapt care, la rândul său, contribuie în mod direct la dezvoltarea personală a acestora. Internetul a devenit principala lor sursă de libertate și informare pe măsură ce cresc și le oferă mijloacele necesare pentru a-și exercita drepturile și libertățile în mediul online. Deși Internetul ascunde potențiale capcane, pot fi luate măsuri de precauție și poate fi oferită o asistență considerabilă. Pentru a nu descuraja utilizatorii (mai ales, pe cei tineri), Internetul nu trebuie prezentat ca un loc întunecat, plin de pericole și avertizări. Tocmai scopul de a oferi suport în ceea ce privește utilizarea informată, creativă, în siguranță și fără teamă a Internetului, face din prezentul manual un instrument unic și valoros. Dacă, prin intermediul manualului, copiii pot să îmbrățișeze multitudinea de posibilități pe care le oferă Internetul, în același timp, consolidând reziliența lor digitală, fiind conștienți de propriile capacități și responsabilități, atunci manualul și-a atins scopul.

■ Pentru Consiliul Europei, este un prilej de mândrie faptul că a putut urmări evoluția manualului și își exprimă recunoașterea nenumăratelor persoane implicate de-a lungul anilor în lansarea inițială, precum și revizuirea și editarea ulterioară a acestuia. Actualmente, acest instrument reprezintă o sursă și mai amplă de informații de calitate pentru ca copiii, părinții, cadrele didactice și factorii de decizie din cele 47 de state membre să beneficieze din plin de pe urma utilizării Internetului și să pregătească generațiile viitoare pentru a folosi Internetul în siguranță și cu încredere.



**Snežana Samardžić-Marković**  
Director General pentru Democrație



**Christos Giakoumopoulos**  
Director General pentru Drepturile Omului  
și Statul de Drept



# Introducere

---

” Educația este o punte între mizerie și speranță. Aceasta este un bastion împotriva sărăciei și o piatră de temelie a dezvoltării, ... o platformă pentru democratizare și un mijloc de promovare a identității culturale și naționale. ... În cele din urmă, educația este drumul către progresul uman și mijloacele prin care fiecare bărbat, femeie și copil își poate realiza întregul potențial.

*Kofi Annan, fost Secretar General al Organizației Națiunilor Unite,  
ianuarie 1997-decembrie 2006*

**A**ceasta este a doua ediție a *Manualului de educare (alfabetizare) în domeniul Internetului*, care a fost publicat inițial în 2003. Prima ediție a fost revizuită la intervale de trei ani, în 2006 și 2009, în efortul de a ține pasul cu ritmul fascinant al evoluției din domeniul tehnologiilor online. Deși această ediție implică o structură similară, conținutul a fost complet actualizat și au fost adăugate noi Fișe de informare, cu accent special pe tehnologiile de mâine.

■ Manualul este destinat publicului larg, inclusiv familiilor, educatorilor și factorilor de decizie politică; cu toate acestea, acesta oferă și legături către informații și resurse mai detaliate pentru cei care doresc să se aprofundeze mai departe în subiectele abordate. În același timp, acesta urmărește să ghideze adolescenții și tinerii cu vârsta de 20 de ani, care se numără printre cei mai pasionați utilizatori ai tehnologiilor și sunt formatorii și creatorii noilor tendințe.

■ Mai presus de toate, *Manualul de educare (alfabetizare) în domeniul Internetului* are rolul de a oferi informații și de a promova reflecția asupra unora dintre problemele etice, sociologice și culturale mai complexe care sunt intrinsec legate de activitățile digitale și mass-media, care ocupă un rol atât de important în viața majorității oamenilor din multe părți ale lumii. Consiliul Europei, care publică prezentul manual, depune eforturi din 1949 pentru a promova, proteja și dezvolta drepturile omului, democrația și statul de drept în cele 47 de state membre ale sale.

■ Pe măsură ce, în ultima jumătate de secol, tehnologiile au afectat rapid cele mai multe sfere ale vieții unei multitudini de oameni, acestea au avut impact și asupra drepturilor omului, responsabilităților și libertăților și, în același timp, au lărgit considerabil conceptul de alfabetizare, care constituie un aspect esențial al acestora. *Manualul de educare (alfabetizare) în domeniul Internetului* face parte din paleta largă de instrumente ale Consiliului Europei care vizează abordarea numeroaselor provocări și exploatarea numeroaselor oportunități care au apărut grație Internetului. Unele dintre aceste instrumente sunt menționate în manual.

■ Competențele de utilizare implică stăpânirea instrumentelor contemporane de comunicare ca mijloc de exprimare și înțelegere – cunoscute anterior în limba engleză ca cei 3 R (lectura, scrierea și aritmetica). Dar când utilizăm instrumente și platforme digitale pentru a ne exprima, influența, viteza lor, dar și instantaneitatea diseminării transformă competențele de utilizare într-un concept eterogen, cu care mulți dintre noi continuăm să ne confruntăm. Fotografii, videoclipurile, mesajele cu număr limitat de caractere, emoticoanele și podcasturile au devenit limbaje independente, prin instrumente precum Instagram, Snapchat, Vine și Periscope, iar interacțiunea și comunicarea reală sunt adesea un proces fără chip, mediat electronic. Acest lucru este valabil în special pentru tinerii care trimit texte, tweet-uri, joacă jocuri electronice și fac schimb de imagini zi și noapte în mediul online, care are tangențe și se contopește cu ceea ce adulții încă mai numesc „lumea reală”.

■ Convențiile sociale și culturale sunt transformate, de vreme ce utilizatorii media se „împrietenesc” și „rup prietenia” cu persoane din cealaltă parte a lumii, pe care, probabil, nu le vor întâlni niciodată. Relațiile se creează din ce în ce mai mult în mediul online, pe măsură ce partenerii de afaceri se întâlnesc și creează companii prin intermediul Internetului și acesta devine tot mai des locul în care oamenii își întâlnesc pentru prima dată partenerii de viață. Aceste schimbări profunde au plasat responsabilitatea și răspunderea în centrul setului de competențe de utilizare de bază, necesitând o înțelegere profundă a propriilor noastre drepturi fundamentale ale omului și respectarea drepturilor altora, dacă dorim să evităm capcanele și să contribuim pozitiv la societatea actuală.

■ *Manualul de educare (alfabetizare) în domeniul Internetului* este prezentat ca un compendiu de Fișe de informare și apare într-un format similar cu cel al primei ediții. Totuși, Fișele de informare au fost acum organizate în șase secțiuni tematice, permițând utilizatorilor să descarce și să imprime mai ușor secțiune după secțiune sau acele secțiuni pe care le doresc. Fiecare secțiune oferă o prezentare generală a propriului conținut sub formă de liste de verificare. Acest lucru este mai cuprinzător comparativ cu un index simplu și facilitează consultarea Fișelor de informare oferind un reper succint pentru cele mai importante puncte abordate. Toate secțiunile vizează abordarea aspectelor principale ale Internetului, de la informații esențiale despre modul în care funcționează acesta și unde sunt stocate datele noastre, la găsirea de informații de calitate și conectarea cu oameni și cunoștințe, la obținerea de asistență și anticiparea direcției spre care ne pot duce tehnologiile online în viitor. Secțiunile constituie un set de instrumente menite să ajute utilizatorii să navigheze prin rețeaua de posibilități pe care le oferă Internetul și, în acest proces, să găsească modalități prin care mai degrabă pot contribui la modelarea lumii online, decât să fie modelați de aceasta.

■ Ținând cont de mediul electronic în care sunt prezentate, Fișele de informare sunt foarte succinte, ușor de citit și facilitează identificarea rapidă a ideilor, alertelor, dar și a linkurilor utile. Fiecare începe cu o privire de ansamblu de ultimă oră asupra subiectului în cauză, înainte de a investiga puțin mai complet și cu puțin mai multă precizie modul în care poate fi folosit instrumentul, platforma sau serviciul educațional pentru a aduce un plus de valoare și oportunități. Apoi, utilizatorii sunt invitați să reflecte și să analizeze unele aspecte etice, dar, după cum s-a menționat anterior, tehnologiile sunt în perpetuă mișcare și, prin urmare, apar mereu noi considerații etice. Secțiunea „Instrucțiuni” din majoritatea Fișelor de informare este un ghid practic al cărui scop este să furnizeze pas cu pas informații despre cum stau lucrurile în realitate sau cum pot fi făcute să funcționeze, astfel încât utilizatorii să poată profita la maxim de tehnologii.

■ Secțiunile finale ale fiecărei Fișe de informare oferă idei pentru utilizarea în clasă, exemple de bune practici și informații suplimentare care pot varia de la link-uri către articole și ghiduri până la alte aplicații ale instrumentului sau serviciului respectiv. Aceste pagini pot fi văzute ca un repozitoriu al celor mai bune practici care au fost colectate de la instituții, organizații și persoane care lucrează în întreaga lume în domeniul social, educațional, cultural și protecției copilului și sunt gestionate de un șir de specialiști, în special pentru utilizatorii manualului. Au fost depuse eforturi pentru a se asigura că toate recomandările propuse sunt actualizate, relevante și fiabile pentru a fi utilizate de către toate grupele de vârstă, cu excepția cazului în care se prevede altfel. Însă, utilizatorii sunt cu siguranță conștienți de faptul că, în lumea de astăzi, aflată într-o evoluție rapidă, mii de URL-uri (adrese pentru localizarea resurselor, altfel cunoscute sub numele de „link” sau „link web”) sunt zilnic create și șterse. Prin urmare, niciun manual ce se referă la tehnologiile online nu ar putea garanta că toate informațiile vor rămâne valabile și că toate URL-urile pe care le conține vor continua să existe.

■ *Manualul de educare (alfabetizare) în domeniul Internetului* ar trebui văzut mai degrabă ca un instantaneu sau o „captare” la un anumit moment dat. Acesta va trebui să fie completat cu noi informații, idei și orientări, dacă se dorește ca acesta să rămână cu adevărat relevant pentru publicul vizat. Cititorii sunt invitați să contribuie la acest proces evolutiv trimițând ideile, resursele și exemplele de bune practici la adresa Diviziunii Protecția Copiilor din cadrul Consiliului European, [children@coe.int](mailto:children@coe.int).

# 1. Internetul: oricând, oriunde

---

” „Cu toții suntem acum conectați prin Internet, ca neuronii dintr-un creier uriaș.”

*Stephen Hawking, fizician teoretic*

## LISTA DE VERIFICARE PENTRU FIȘA 1 – CONECTAREA

---

V-ați asigurat că conexiunea dumneavoastră la Internet este securizată prin configurarea unui antivirus, a unui firewall și prin setarea unei parole pentru routerul dumneavoastră Wi-Fi?

Ați stabilit o politică de utilizare acceptabilă (numită uneori o politică de utilizare responsabilă) pentru oricine care utilizează/acesează Internetul prin intermediul rețelei și a dispozitivelor dumneavoastră?

Ați creat conturi de „clienți” pe dispozitivele utilizate de copiii dumneavoastră?

## LISTA DE VERIFICARE PENTRU FIȘA 2 – PREZENȚA ONLINE ȘI PE „NOR” (CLOUD)

---

Ați inclus date de contact pe site-ul dumneavoastră web sau blogul dumneavoastră?

Ați luat măsuri pentru a vă proteja viața privată în mediul online?

Ați verificat dacă conținutul pe care îl utilizați pentru site-ul dumneavoastră web/blogul dumneavoastră este în conformitate cu legislația cu privire la drepturile de autor?

## LISTA DE VERIFICARE PENTRU FIȘA 3 – INTERNET 2.0, INTERNET 3.0 ȘI ALTE VERSIUNI

---

Solicitați în mod sistematic permisiunea de la persoanele care apar în fotografiile și videoclipurile pe care le postați în mediul online?

Recomandările utilizatorilor pe site-urile de călătorii și produse pot fi utile, dar sunteți sigur că acestea sunt reale?

Conținutul generat de utilizatori promovează creativitatea și libertatea de exprimare, dar, dacă se dorește ca Internetul să devină un loc mai bun atunci responsabilitatea revine utilizatorilor.

## LISTA DE VERIFICARE PENTRU FIȘA 4 – BLOGURI ȘI VLOGURI

---

Protejați-vă confidențialitatea utilizând un pseudonim și nu divulgați anumite detalii personale.

Protejați-vă blogul sau vlogul de hackeri prin luarea unor măsuri de siguranță adecvate și salvând periodic conținuturile.

Luați în calcul obiectivul și publicul blogului dumneavoastră atunci când postați un conținut.

## LISTA DE VERIFICARE PENTRU FIȘA 5 – INTERNETUL ÎN MIȘCARE

---

De la ce vârstă pot copiii să înceapă să utilizeze în siguranță dispozitivele mobile și care sunt cele mai potrivite pentru copiii foarte mici?

Aveți o înțelegere suficientă a geolocației și Bluetooth-ului pentru a utiliza dispozitivele mobile în mod confortabil și în siguranță?

Învățarea mobilă și portofelele mobile sunt domenii în care utilizarea dispozitivelor mobile schimbă modul în care învățăm, lucrăm și cumpărăm. Ce știți despre aceste evoluții recente?



## Fișa 1

# Conectarea



Internetul este o rețea mondială de calculatoare conectate împreună prin servere care funcționează ca noduri de conexiune<sup>1</sup>. În iunie 2016, în lume existau aproximativ 3,5 miliarde de utilizatori de Internet, din care 614 milioane locuiau în Europa<sup>2</sup>.

— Cum funcționează Internetul și de ce este important să cunoaștem procesul? Cel mai probabil, deja utilizați Internetul zilnic, chiar mai frecvent decât ați folosi bicicleta sau mașina. Deși nu aveți nevoie să cunoașteți toate detaliile tehnice despre modul în care funcționează Internetul, ar trebui să aveți cel puțin o înțelegere de bază a funcționării acestuia, la fel cum știți să schimbați roata la bicicletă sau să verificați nivelul uleiului la mașină.

— Acasă, sunteți cel mai probabil conectat la Internet utilizând un router, acea cutie misterioasă care se conectează fie la linia dumneavoastră telefonică, fie la cablul dumneavoastră TV. Toate dispozitivele dumneavoastră, indiferent dacă este vorba de telefonul inteligent sau calculatoare, sunt conectate la routerul respectiv, fie printr-un cablu Ethernet, fie prin Wi-Fi.

1. [http://en.wikipedia.org/wiki/Node\\_%28networking%29](http://en.wikipedia.org/wiki/Node_%28networking%29)

2. [www.Internetworldstats.com/stats.htm](http://www.Internetworldstats.com/stats.htm)

— Acum, imaginați-vă că routerul dumneavoastră a fost conectat cu un cablu la routerul vecinilor dumneavoastră, iar routerul vecinului dumneavoastră – la casa vecină etc. Aceasta este exact ceea ce reprezintă Internetul la o scară mai mică. Internetul este, pur și simplu, un număr foarte mare de routere conectate unele cu altele, care vă permit să redirecționați și să transmiteți informații (date care conțin emailuri, imagini, videoclipuri etc.) de la un punct (de exemplu, calculatorul dumneavoastră de acasă) la altul (telefonul inteligent al prietenului care este în vacanță la celălalt capăt al lumii).

— Pe cât de uimitor sună acest lucru, există cabluri subacvatice uriașe care se întind pe sub ocean de-a lungul tuturor continentelor, ajungând direct într-un punct de convergență a cablurilor, care se conectează la infrastructura terestră (de obicei, liniile telefonice).

— Așadar, imaginați-vă, ori de câte ori trimiteți o imagine de la calculatorul dumneavoastră la un prieten, iată ce se întâmplă: fotografia dumneavoastră este tocată în bucăți minuscule de date numite „pachete”, care sunt etichetate la fel ca un plic la poștă (destinație, origine și informațiile cu privire la modul de reintroducere a respectivei bucăți de date pentru a recompune imaginea dumneavoastră). În locul informațiilor privind numele străzii și numărul casei, pachetele de date conțin adresa IP<sup>3</sup> de unde au fost trimise și adresa IP a locului în care ar trebui să ajungă. Acestea trec apoi prin linia dumneavoastră telefonică la facilitățile prestatorului dumneavoastră de servicii Internet care sunt conectate la structura de bază a Internetului (ce constă în numărul mare de routere interconectate, despre care am vorbit). Pachetele sunt redirecționate de aceste routere de mai multe ori până când ajung la destinație (aceasta se numește număr de hopuri). Dar care este cu adevărat destinația imaginii dumneavoastră? Dacă trimiteți, de exemplu, o imagine prin email, destinația nu este calculatorul prietenului dumneavoastră, ci centrele de date ale clientului de email pe care îl folosește prietenul dumneavoastră.

— Centrele de date sunt depozite uriașe pline de routere și hard disk-uri. Imaginea dumneavoastră va fi stocată pe mai multe hard disk-uri (pentru a proteja datele în cazul unor defecțiuni ale hard disk-ului). Dacă prietenul dumneavoastră utilizează Gmail, de exemplu, imaginea pe care ați trimis-o prietenului dumneavoastră poate fi stocată fizic într-unul dintre centrele de date Google din Statele Unite, Irlanda, Belgia, Olanda și multe alte țări<sup>4</sup>. Iar prietenul dumneavoastră, când dorește să se uite la aceasta, trimite o solicitare de la calculatorul său, care este redirecționată prin structura de bază a Internetului, până la acel centru de date, care trimite apoi datele cu imaginea dumneavoastră la ecranul computerului său.



## GUVERNANȚA INTERNETULUI

— Dar cum a fost înființat Internetul în primul rând? Cine este responsabil de menținerea infrastructurilor actuale și crearea de noi infrastructuri? Cine decide cu privire la standarde precum adresele IP?

— În timp ce ideea de hyperlink-uri și pagini web interconectate a venit de la Tim Berners-Lee și Robert Cailliau, care lucrau la CERN în Elveția, prima rețea interconectată numită ARPANET a fost înființată în SUA, între universități<sup>5</sup>.

— Prin urmare, primul organ care a fost responsabil de alocarea „adreselor” unice, care a permis, în esență, conectarea unei persoane la rețea, a fost înființat în SUA: Autoritatea de Atribuire a Numerelor pe Internet (*Internet Assigned Numbers Authority – IANA*).

— Pe măsură ce Internetul s-a extins, la fel a crescut și nevoia de a coordona mai bine dezvoltarea, întreținerea, stabilitatea și securitatea Internetului. Departamentul de Comerț al Statelor Unite a promovat o reformă a IANA, care a devenit în 1998 ICANN<sup>6</sup> (Corporația Internet pentru Nume și Numere Alocate). ICANN a fost înființată în mod oficial ca o corporație non-profit „pentru scopuri caritabile și publice”, cu o puternică abordare „de jos în sus” a guvernării, care constă în coordonarea a mii de părți interesate la nivel mondial, inclusiv a actorilor din sectorul privat, a societății civile și a guvernelor. Cu toate acestea, Corporația s-a confruntat cu multe critici și solicitări de reforme

3. [https://en.wikipedia.org/wiki/IP\\_address](https://en.wikipedia.org/wiki/IP_address)

4. <http://www.google.com/about/datacenters/inside/locations/index.html>

5. [https://en.wikipedia.org/wiki/World\\_Wide\\_Web](https://en.wikipedia.org/wiki/World_Wide_Web)

6. <https://www.icann.org/>

din partea țărilor lumii din cauza legăturilor sale cu Guvernul Statelor Unite și a riscului de supraprezentare a intereselor SUA.

— Ca răspuns, ICANN s-a deschis unei mari varietăți de actori, inclusiv 111 state și un număr de observatori, cum ar fi organizațiile-cheie de telecomunicații și Consiliul Europei. Dar, ICANN a fost criticată în continuare pentru lipsa contribuției sale democratice și lipsa consultării mai largi a părților interesate, ceea ce a determinat crearea în 2006 a Forumului pentru Guvernarea Internetului (Internet Governance Forum – IGF) de către Organizația Națiunilor Unite.

— IGF se reunește anual și oferă oportunitatea pentru o gamă largă de părți interesate, inclusiv pentru tineri, de a-și împărtăși opiniile cu privire la viitorul Internetului.



## BENEFICIILE EDUCAȚIONALE

- Internetul oferă acces la o multitudine de idei, resurse, oportunități de învățare, informații și servicii noi.
- Internetul facilitează schimbul de experiență și de comunicare între utilizatorii aflați dincolo de frontierele internaționale, prin diverse modalități: forumuri, email-uri, rețele sociale, conversații, conferințe video etc. Prin urmare, oferă elevilor/studentilor posibilitatea de a participa la proiecte și de a lucra cu alți elevi/studenti fără ca ei să investească în călătorii costisitoare.
- Internetul face ca instrumentele de cercetare să fie accesibile chiar și celor care nu merg în mod regulat la bibliotecile tradiționale.
- Cu dispozitive și programe suplimentare, Internetul poate deschide noi oportunități pentru persoanele cu nevoi speciale.
- Învățarea despre modul în care este guvernat Internetul, permite tuturor cetățenilor să se implice în deciziile-cheie care le vor modela viitorul.



## CONSIDERAȚII DE ORDIN ETIC ȘI RISCURI

- Fiți conștienți de faptul că Internetul oferă adesea un fals sentiment de anonimitate. Având în vedere modul în care funcționează Internetul, ori de câte ori îl accesați, întotdeauna lăsați o urmă (adresa dumneavoastră IP).
- La fel ca în lumea offline, aici sunt comise fraude, apar informații false și materiale nepotrivite pentru copii.
- În timp ce Internetul oferă o serie de noi posibilități, soluțiile tehnice nu sunt întotdeauna mai bune decât cele tradiționale. De exemplu, emailul a revoluționat comunicarea însă, deși videoconferințele pot da sentimentul că „aproape ești acolo”, aceasta nu va înlocui niciodată comunicarea față în față.
- Guvernarea Internetului poate avea un impact extraordinar asupra experienței dumneavoastră online, reieșind din astfel de principii precum anonimatul sau neutralitatea rețelei în echilibru. Se duce o bătălie constantă între cei care promovează principiul unui Internet liber și deschis și cei care doresc să îl controleze. Unele companii încearcă să redirectioneze traficul către propriile site-uri web, aplicații sau servicii prin furnizarea unor planuri „gratuite” de Internet mobil, limitate la respectivele site-uri web, aplicații sau servicii și prin tarifarea vizitării altora<sup>7</sup>. De exemplu, Facebook a creat portalul „Internet.org”, care este pagina de pornire implicită pentru toți utilizatorii care se conectează prin intermediul serviciului său de Internet în diferite părți ale lumii, în special în țările în curs de dezvoltare<sup>8</sup>.
- Fiți conștienți de faptul că orice distribuți în mediul online poate fi memorat în cache, stocat sau copiat.

7. <https://en.wikipedia.org/wiki/Zero-rating>

8. <https://en.wikipedia.org/wiki/Internet.org>



## INSTRUCȚIUNI

- Practic, toate dispozitivele pe care le cumpărați în prezent sunt capabile să se conecteze la Internet, fie prin Wi-Fi sau acces la Internet mobil (de exemplu, telefoanele inteligente și tabletele se pot conecta prin Wi-Fi sau Internet mobil) sau printr-un cablu Ethernet (majoritatea calculatoarelor sunt echipate cu un port Ethernet).
- Pentru a vă conecta la Internet, aveți două opțiuni principale:
  - ▶ Contactați un PSI (prestator de servicii Internet), de obicei, o companie de telefonie sau de cablu, care vă va furniza un nume de utilizator și o parolă și, uneori, un modem/router pentru a vă conecta la Internet, fie prin linia telefonică, fie prin cablul dumneavoastră de televiziune.
  - ▶ Obțineți un plan de „Internet mobil” de la operatorul dumneavoastră de telefonie mobilă. Rețineți că restricțiile privind volumul de date pe care îl puteți descărca/încărca sunt în continuare destul de mari în ceea ce privește Internetul mobil, deși acestea vor fi treptat reduse, pe măsură ce tot mai mulți operatori introduc standarde de telecomunicații mobile 4G sau 5G (cu o creștere mare a vitezei).
- Există, de asemenea, tot mai multe puncte de acces (hotspot-uri) Wi-Fi „deschise,” pe care le puteți utiliza pentru a vă conecta gratuit la Internet. Le puteți găsi într-o varietate de locuri publice, cum ar fi bibliotecile publice, dar și în baruri, restaurante și mall-uri. De cele mai multe ori, înainte de a vă conecta, vi se va cere să faceți una sau mai multe dintre următoarele acțiuni: să acceptați termenii de utilizare, să creați un cont utilizând adresa dumneavoastră de email (rețineți faptul că emailul dumneavoastră poate fi apoi utilizat pentru a vă trimite anunțuri publicitare, așadar, asigurați-vă că ați creat o adresă de email special pentru aceste situații) sau introduceți o parolă pentru a vă conecta la Internet. De exemplu, în baruri, restaurante sau hoteluri, Wi-Fi-ul „deschis” este adesea accesibil numai clienților, astfel încât trebuie să solicitați parola unui membru al personalului. Nu distribuiți niciodată date sensibile sau nu efectuați operațiuni sensibile, cum ar fi serviciile bancare mobile, prin puncte de acces Wi-Fi publice.
- Majoritatea PSI vă vor furniza un router preconfigurat pe care va trebui doar să îl conectați la telefonul/cablul dumneavoastră pentru a fi conectat. Uneori, va trebui să cumpărați un router și să îl configurați dumneavoastră. Asigurați-vă că verificați cu PSI-ul dumneavoastră dacă routerul pe care îl aveți sau pe care intenționați să îl achiziționați este compatibil cu abonamentul dumneavoastră de Internet!

## IDEI PENTRU LUCRUL ÎN CLASĂ



### Pentru Windows 7 și alte versiuni



1. Apăsați pe butonul „Start” din Windows.
2. Tastați „cmd” în bara de „căutare” și apăsați pe pictograma programului care apare în meniul de pornire.

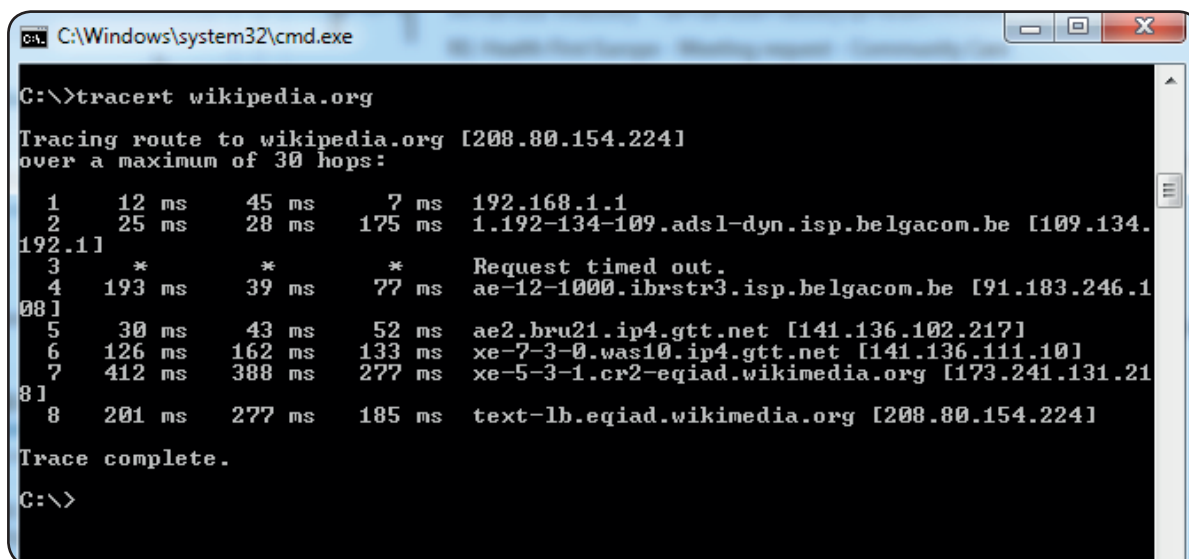
```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\>
```

3. Introduceți „tracert wikipedia.org” și apăsați „enter”.



4. Veți putea vedea „**hopurile**” care există între calculatorul dumneavoastră și site-ul web pe care încercați să îl accesați și cât timp va dura fiecare „hop”. În acest exemplu, vedem că pentru a accesa Wikipedia, navigăm mai întâi prin routerele PSI-ului nostru „local” (în acest caz Belgacom din Belgia), apoi mergem prin Oceanul Atlantic spre un router din Washington (abreviat „was”), pentru a ajunge, în cele din urmă, la locul în care este găzduită Wikipedia. Elevii sunt, desigur, încurajați să încerce acest lucru cu alte site-uri web. Observați cât timp a durat fiecare pas în milisecunde.



```
C:\Windows\system32\cmd.exe
C:\>tracert wikipedia.org
Tracing route to wikipedia.org [208.80.154.224]
over a maximum of 30 hops:
  0  12 ms  45 ms  7 ms  192.168.1.1
  1  25 ms  28 ms  175 ms  1.192-134-109.adsl-dyn.isp.belgacom.be [109.134.192.11]
  2  *      *      *      Request timed out.
  3  193 ms  39 ms  77 ms  ae-12-1000.ibrstr3.isp.belgacom.be [91.183.246.108]
  4  30 ms  43 ms  52 ms  ae2.bru21.ip4.gtt.net [141.136.102.217]
  5  126 ms  162 ms  133 ms  xe-7-3-0.was10.ip4.gtt.net [141.136.111.10]
  6  412 ms  388 ms  277 ms  xe-5-3-1.cr2-eqiad.wikimedia.org [173.241.131.218]
  7  201 ms  277 ms  185 ms  text-lb.eqiad.wikimedia.org [208.80.154.224]
Trace complete.
C:\>
```



### Pentru Mac OS X și alte versiuni

1. Lansați utilitarul rețelei în Mac OS X (puteți face acest lucru accesând Spotlight și introducând „**utilitar rețea**” și apăsând pe partea de sus a paginii).
2. Apăsați pe „**Traceroute**”.
3. Introduceți numele domeniului pentru care doriți să efectuați o urmărire a traseului, cum ar fi „**Wikipedia.org**” și apăsați pe „**Urmărire**”.
4. Veți putea vedea „**hopurile**” care există între calculatorul dumneavoastră și site-ul web pe care încercați să îl accesați și cât timp va dura fiecare „hop”.

### Material opțional pentru cadrele didactice

- Pentru mai multe informații, vizionați videoclipul Naked Science Scrapbook „Cum funcționează Internetul?”<sup>9</sup>.
- Inițiați o discuție în clasă cu privire la modul în care tehnologiile online pot aduce beneficii persoanelor cu nevoi speciale și aruncați o privire asupra planului de acțiune al Consiliului Europei pentru a impulsiona noi idei<sup>10</sup>.



### PRACTICI BUNE

- Alegeți o conexiune adecvată pentru utilizarea Internetului. Dacă utilizați în mod regulat servicii care necesită un Internet foarte rapid, cum ar fi transmisiuni video de înaltă definiție, asigurați-vă că aveți o conexiune mai rapidă la Internet (cel puțin 20 megabiți pe secundă, echivalentul ADSL2+). Mai ales, căutați o conexiune la Internet fără limitări ale volumului de date descărcate. Dacă aveți nevoie de Internet doar pentru a citi știrile și a trimite emailuri, atunci practic orice abonament de bază de Internet va fi suficient pentru dumneavoastră<sup>11</sup>.

9. <https://www.youtube.com/watch?v=oj7A2YDgIWE>

10. [https://www.coe.int/t/dg4/majorhazards/activites/2013/DIDRR/Action\\_Plan\\_CoE\\_Easy\\_to\\_Read\\_13nov08\\_EN.pdf](https://www.coe.int/t/dg4/majorhazards/activites/2013/DIDRR/Action_Plan_CoE_Easy_to_Read_13nov08_EN.pdf)

11. [www.cnet.com/internet-speed-test](http://www.cnet.com/internet-speed-test)

- Închideți întotdeauna dispozitivele (calculatoarele) sau dezactivați conexiunea Wi-Fi pe telefonul inteligent/tableta dumneavoastră atunci când mergeți la culcare. Lăsarea dispozitivelor conectate poate crește riscul de securitate pentru datele dumneavoastră și poate prezenta, de asemenea, riscuri pentru sănătate (a se vedea Fișa 19 cu privire la securitate).
- Asigurați-vă că știți cum să accesați pagina de configurare a routerului dumneavoastră. Cel mai des, o puteți accesa dacă introduceți una dintre următoarele adrese IP în browserul dumneavoastră: 192.168.1.0 sau 192.168.1.1. De ce este important acest lucru? Majoritatea paginilor de configurare Wi-Fi au conturi de administrator „implicite,” cu nume de utilizator și parole foarte simple (de exemplu, nume de utilizator „admin” și parolă „admin”). Este foarte important să vă asigurați accesul la pagina de configurare a routerului dumneavoastră, deoarece acesta poate fi utilizat cu ușurință pentru a vă schimba setările sau pentru a obține accesul la rețeaua calculatorului dumneavoastră de acasă.
- Stați alături de copiii dumneavoastră ori de câte ori puteți atunci când aceștia navighează pe Internet, pentru a stimula discuțiile despre experiențele lor în mediul online și pentru a consolida încrederea; luați-o ca pe o provocare de a învăța împreună.
- Manifestați un interes activ față de guvernarea Internetului și asigurați-vă că vocea dumneavoastră este auzită în cadrul dezbaterilor publice în legătură cu principiile fundamentale, cum ar fi anonimatul, securitatea sau neutralitatea rețelei.
- Elaborați o politică de utilizare acceptabilă (PUA)<sup>12</sup> sau o politică de utilizare responsabilă (PUR) în cazul în care alte persoane urmează să utilizeze computerul sau rețeaua de care sunteți responsabil.



## INFORMAȚII SUPLIMENTARE

- Lista este un catalog mondial al PSI-urilor. <<http://www.thelist.com>>.
- Site-uri web educaționale, cum ar fi European Schoolnet la <<http://www.eun.org>>, Global SchoolNet la <<http://www.globalschoolnet.org/GSH/>> și Education World la <<http://www.educationworld.com/>> oferă resurse și proiecte de colaborare.
- Sfaturi privind scrierea unei PUA pot fi găsite prin intermediul Education World, un portal online pentru cadrele didactice și profesioniștii din domeniul educației: <[http://www.educationworld.com/a\\_curr/curr093.shtml](http://www.educationworld.com/a_curr/curr093.shtml)>.
- Portalul Insafe oferă resurse și sfaturi cu privire la conectarea și navigarea în condiții de siguranță: <<https://www.betterinternetforkids.eu/>>.
- Site-ul web oficial al Forumului de Guvernare a Internetului permite desfășurarea unor discuții cu privire la problemele de politică publică referitoare la Internet: <<http://www.intgovforum.org/cms/>>.
- Următoarea pagină Wikipedia conține diverse informații despre neutralitatea rețelei: <[https://en.wikipedia.org/wiki/Net\\_neutrality](https://en.wikipedia.org/wiki/Net_neutrality)>.
- Informațiile despre ICANN pot fi găsite pe site-ul web oficial al acesteia: <<https://www.icann.org/>>.

12. [http://en.wikipedia.org/wiki/Acceptable\\_use\\_policy](http://en.wikipedia.org/wiki/Acceptable_use_policy)

## Fișa 2

# Prezența în mediul online și pe „nor” (cloud)



**A**veți ceva ce doriți să împărtășiți cu lumea și aveți nevoie de un loc unde să-l partajați în mediul online?

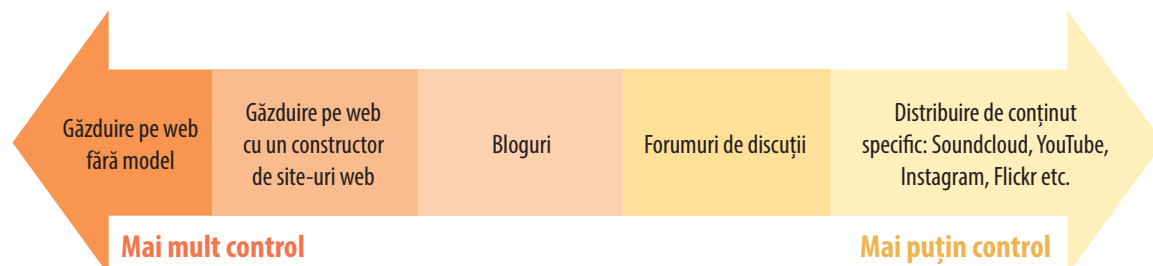
— În timp ce site-urile web au constituit una dintre primele modalități de distribuire în mediul online, în ultimul deceniu au apărut tot mai multe alternative acestora. La începuturile Internetului, crearea unui site web nu era o glumă: era destul de costisitor și necesita anumite abilități de codificare. Cu toate acestea, în zilele noastre, nici măcar nu trebuie să fiți specialist IT pentru a crea și concepe propriul site web. Dar, înainte de a face acest lucru, întotdeauna reflectați, pentru a lua în considerare toate opțiunile.

— În concluzie, trebuie să înțelegeți ce doriți să distribuiți și cum doriți să distribuiți.

— Doriți să distribuiți conținuturi foarte specifice (imagini, video, texte etc.) sau doriți să distribuiți o gamă largă de conținut? Doriți să aveți control deplin asupra întregului proces de creativitate sau preferați să lucrați în baza unui model prestabilit pe care îl puteți modifica într-o oarecare măsură?

Care ar fi scopul distribuirii conținutului și de ce aveți nevoie de acesta? Cine este publicul – întreaga lume, sectorul, orașul natal sau doar elevii și părinții? Ce sumă sunteți dispus să plătiți pentru a distribui conținutul în mediul online?

— Diagrama de mai jos ilustrează o listă neexhaustivă a modurilor în care puteți distribui conținut, organizat de-a lungul unui continuum care pornește de la control /personalizare totală, ajungând la un control/personalizare mai redusă.



— Dacă doriți să beneficiați de o libertate totală în ceea ce privește atât conținutul, cât și designul, atunci ar trebui să optați pentru găzduirea pe web fără model. Dar rețineți că acest lucru are un cost și, în majoritatea cazurilor, va trebui să achiziționați un nume de domeniu (de exemplu, <www.mywebsite.com>). Dacă nu doriți să învățați cum să codificați, dar totuși doriți să distribuiți o mare varietate de conținuturi și să aveți o flexibilitate mare în ceea ce privește designul, puteți opta pentru găzduirea pe web cu un constructor de site-uri web sau pentru un blog (care, uneori, va avea și mai puțină flexibilitate în ceea ce privește conceptul). Forumurile de discuții sunt deja destul de specifice: de exemplu, puteți crea forumuri de discuții sau un panou electronic de mesaje pentru școala dumneavoastră. Și, în cele din urmă, dacă doriți doar să distribuiți fotografii, videoclipuri sau muzică, puteți alege să configurați un cont pe un serviciu specializat în găzduirea respectivului tip de conținut. Conținutul dumneavoastră, oricare ar fi acesta, va ajunge în cele din urmă, undeva pe serverul serviciului de găzduire pe care îl veți alege: acesta va fi în „cloud (nor)”.

— De asemenea, nu uitați că, deși multe dintre aceste servicii sunt gratuite, acest lucru înseamnă adesea că publicul dumneavoastră ar putea fi expus unei publicități mai mult sau mai puțin intruzive (o publicitate care îngreunează foarte mult experiența utilizatorului, cum ar fi numeroase pop-up-uri, suprapuneri de site-uri web, un număr excesiv de afișe publicitare etc.).



## VALOAREA EDUCAȚIONALĂ, DE CE ESTE RELEVANT, IMPORTANT?

— Construirea unei prezențe online și distribuirea conținutului în mediul on-line are o valoare educațională excelentă și contribuie la dobândirea unui număr de competențe.

- **Content management/organisation: Gestionarea/organizarea conținutului:** dacă decideți să construiți un site web sau să creați o galerie foto, conținutul dumneavoastră trebuie organizat într-un mod simplu, pentru ca utilizatorii să găsească ceea ce caută.
- **Conceptul:** identitatea dumneavoastră în mediul online va fi adesea legată de un logo, de o imagine, de culorile alese de dumneavoastră, de aspectul site-ului dumneavoastră web, toate acestea făcând parte din munca de proiectare.
- **Competențe digitale:** în mod evident, dezvoltarea unei prezențe în mediul online va consolida anumite competențe digitale, cum ar fi codificarea (de exemplu, HTML, PHP, HTML5, Javascript) în cazul în care optați pentru construirea unui site web. Dar chiar și cu alte opțiuni, va trebui să învățați despre motoarele de căutare și vizibilitatea conținutului dumneavoastră, formatele fișierelor etc.
- **Abilități de comunicare/scriere:** cu excepția cazului în care intenționați să distribuiți conținut fără comentarii, va trebui să vă perfecționați abilitățile de comunicare/scriere pentru a capta atenția și interesul utilizatorilor dumneavoastră.
- **Competențe de marketing:** ținând cont de numărul impunător de persoane prezente în mediul online, este ușor să treci neobservat. Pentru a vă construi o reputație și a crește vizibilitatea

dumneavoastră în mediul online, va trebui să cunoașteți modul în care puteți să vă vindeți și să promovați ceea ce ați creat sau ați distribuit.

- **Munca în echipă:** în plus, în cazul în care prezența dumneavoastră în mediul online este un proiect comun cu prietenii/colegii de școală/clasă, atunci acest lucru va consolida și competențele privind lucrul în echipă. Gestionarea unui site web nu este o sarcină ușoară și această muncă este adesea organizată și împărțită între mai multe persoane: administrator, designer web, redactor conținut etc.
- **Alte avantaje:** prin crearea unui site web pe un anumit subiect, de exemplu un site web despre matematică pentru un proiect școlar, în mod inevitabil, vă aprofundați și mai mult înțelegerea și cunoștințele cu privire la subiectul respectiv.



## CONSIDERAȚII DE ORDIN ETIC ȘI RISCURI

— În cazul în care doriți să distribuiți conținut personal sau să creați un site web personal, veți fi singurul responsabil pentru ceea ce postați. Dumneavoastră (și părinții dumneavoastră, dacă sunteți minor) v-ați putea afla în dificultate din varii motive.



### Motive juridice

— Limitele „libertății de exprimare”: acest drept nu este absolut și există anumite limite ale exercitării sale. Limitele libertății de exprimare trebuie să fie expres prevăzute în lege, să fie necesare într-o societate democratică (proporționat) și să urmărească un scop legitim (articolul 10.2 din Convenția Europeană a Drepturilor Omului prevede: „măsuri necesare pentru securitatea națională, integritatea teritorială sau siguranța publică, apărarea ordinii și prevenirea infracțiunilor, protecția sănătății, a moralei, a reputației sau a drepturilor altora, pentru a împiedica divulgarea informațiilor confidențiale sau pentru a garanta autoritatea și imparțialitatea puterii judecătorești”). Aceste limite pot varia de la un stat la altul, dar există câteva considerații largi de care trebuie să țineți cont:

- ▶ defăimarea<sup>1</sup>;
- ▶ discursurile care instigă la ură<sup>2</sup>;
- ▶ distribuirea datelor personale ale terților persoane<sup>3</sup>;
- ▶ stocarea datelor – dacă optați pentru utilizarea serviciilor cloud, aflați în prealabil unde vor fi stocate datele dumneavoastră; este dreptul și responsabilitatea dumneavoastră de a deține controlul asupra utilizării și accesibilității acestora<sup>4</sup>;
- ▶ încurajarea activităților teroriste:
  - <<https://goo.gl/cv9XDR>>;
  - <<https://goo.gl/Tq3UDp>>;
- ▶ proprietatea intelectuală: dumneavoastră distribuiți conținut care nu vă aparține? Dacă răspundeți afirmativ, atunci asigurați-vă că ați verificat dacă vi se permite să îl distribuiți sau nu. Conținuturile comerciale sunt protejate prin legea cu privire la dreptul de autor și aveți nevoie de o autorizație specifică de la deținătorul de drepturi de autor pentru a le folosi. Unii artiști sau creatori publică conținutul în baza unei anumite „licențe”, cunoscută și sub denumirea de „Creative Commons”. În temeiul unei astfel de licențe, este posibil să puteți utiliza conținutul, fără a menționa autorul, precum și să îl utilizați în scopuri comerciale. În ceea ce privește materialul protejat prin drepturi de autor, dacă doriți să îl utilizați, aveți nevoie de o autorizație corespunzătoare din partea organizației/persoanei care deține drepturile (compania de discuri, studioul de film etc.).

— Oricare dintre acțiunile de mai sus ar putea să vă creeze probleme de ordin juridic.

1. <https://en.wikipedia.org/wiki/Defamation>

2. [https://en.wikipedia.org/wiki/Hate\\_speech](https://en.wikipedia.org/wiki/Hate_speech).

3. [http://www.echr.coe.int/Documents/Handbook\\_data\\_protection\\_ENG.pdf](http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf)

4. [http://ec.europa.eu/justice/data-protection/reform/index\\_en.htm](http://ec.europa.eu/justice/data-protection/reform/index_en.htm)



## Motive personale

- Distribuirea exagerată: rețineți că orice distribuiți va fi, cel mai probabil, accesibil oricui în întreaga lume. Distribuirea fotografiilor dumneavoastră din vacanța privată, de exemplu, care conțin informații despre locație (GPS), ar putea permite persoanelor străine să vă urmărească sau hoților să știe exact când sunteți „în afara orașului” și să vă atace locuința. Fiți mai strategici când e vorba de ceea ce alegeți să distribuiți.
- Reputația în mediul online: deși aveți iluzia că puteți rămâne anonim în mediul online, există multe modalități prin care oamenii vă pot afla adevărata identitate. Reprezentanții organelor de drept dețin mijloacele necesare pentru a identifica utilizatorii de Internet în baza unor anumite condiții (în majoritatea cazurilor, în baza unui mandat judecătoresc). Atunci când distribuiți ceva online, trebuie să fiți conștient că acel lucru va avea impact asupra reputației dumneavoastră și în mediul online, și în offline.
- Dacă distribuiți conținut ofensator sau stupidități în mediul online, aceasta vă poate afecta viața socială și profesională în prezent și în perspectivă. De exemplu, dacă doriți să vă spuneți păsul, discutați cu prieteni de încredere/membrii familiei, lăsați-vă emoțiile în pernă, dar nu trimiteți un tweet întregii lumi, deoarece acesta se va întoarce împotriva dumneavoastră și o să regretați toată viața. Consultați site-ul „Web We Want” (*Web-ul pe care ni-l dorim*)<sup>5</sup> pentru a afla mai multe detalii despre cum puteți să vă protejați reputația online.

— Dacă doriți să distribuiți și alte forme de conținut (de exemplu, ceva creat de școala dumneavoastră) sau să creați un site oficial în numele școlii dumneavoastră, trebuie luate în calcul și alte aspecte:

- Politica școlară privind siguranța pe Internet și buna utilizare a acestuia trebuie să fie clar definită înainte de crearea site-ului oficial sau participarea elevilor la concursurile de creare a site-urilor web.
- Formatul și modul de utilizare a fotografiilor trebuie să reflecte politica școlară privind siguranța pe Internet.
- Din cauza preocupărilor privind siguranța și confidențialitatea, multe școli nu afișează numele sau menționează doar prenumele celor din fotografiile pe care le publică. Acesta este un lucru care trebuie luat în considerare la crearea site-ului web: care este protocolul dumneavoastră de siguranță în această privință?
- Este o idee bună să examinați toate hiperlegăturile externe către alte site-uri web pentru a asigura integritatea informațiilor și faptul că site-ul sau site-urile web reflectă, în mod adecvat, poziția școlii privind siguranța pe Internet.
- Dacă sunteți profesor, școala dumneavoastră va trebui să decidă dacă accesul dumneavoastră la Internet va fi filtrat (exceptând cazul în care este necesar din punct de vedere juridic) sau învățați elevii dumneavoastră să fie mai descurcăriți în utilizarea Internetului. Multe școli consideră că o combinație a celor două tehnici este mai eficientă. De asemenea, atunci când elevii au sarcina de a crea un site web, nu uitați că acesta poate fi vizitat de utilizatori din întreaga lume. Tratați aceste site-uri web ca pe un fel de instrument de relații publice pentru școala dumneavoastră. Prin urmare, ar fi înțelept pentru dumneavoastră, în calitate de profesor, să supravegheați munca elevilor și să îi îndrumați în timpul procesului creativ.
- Cadrele didactice și, în unele cazuri, părinții, sunt, în cele din urmă, responsabili de tot ceea ce elaborează elevii. Prin urmare, cadrele didactice trebuie să aibă puterea de a refuza paginile web sau de a le elimina de pe site-ul web al școlii sau al proiectului. Pentru a supraveghea corespunzător munca elevilor, cadrele didactice trebuie să aibă întotdeauna acces la parole<sup>6</sup>, site-uri web<sup>7</sup> și așa mai departe.

5. <http://www.webwewant.eu>

6. <http://en.wikipedia.org/wiki/Password>

7. <http://en.wikipedia.org/wiki/Website>



## INSTRUCȚIUNI

- Cu excepția cazului în care doriți să plătiți pentru un serviciu profesionist de găzduire web și să aveți propriul nume de domeniu, nu este prea complicat să începeți să distribuiți conținutul în mediul online.
- Majoritatea serviciilor pe care le veți utiliza, fie că este vorba despre constructorii de site-uri web, bloguri sau vloguri (a se vedea Fișa 4) au tutoriale incluse pentru a vă ajuta să începeți.
- Cu toate acestea, în cazul în care doriți să creați un site web de la zero, trebuie să aveți anumite competențe. Din fericire, în prezent, există milioane de modalități de a învăța codajul pentru a crea un site web, dintre care, Codecademy<sup>8</sup> și W3schools<sup>9</sup> sunt printre cele mai populare. Dar nu vă limitați doar la acestea. Faceți-vă timp pentru a realiza cercetări în mediul online ca să găsiți și alte materiale în limba dumneavoastră sau potrivite nevoilor dumneavoastră.
- Dacă doriți să apelați la servicii profesionale de găzduire web, va trebui să prezentați, pe lângă adresa dumneavoastră de email, informații suplimentare cum ar fi numele dumneavoastră real, adresa, numărul de telefon și, în special, unele informații privind modalitățile de plată, ca de exemplu, datele privind cardul de credit. De aceea, copiii și tinerii trebuie întotdeauna să solicite, în prealabil, îndrumare și sprijin din partea unui adult (profesor, părinte)



## IDEI PENTRU LUCRUL ÎN CLASĂ

### Construirea prezenței în mediul online a școlii dumneavoastră

— Atunci când este utilizat corect, site-ul web, blogul, vlogul școlii sau alte mijloace similare pot servi drept un instrument eficient pentru a reuni numeroase și variate fațete ale unei comunități. Acesta poate promova un sentiment de coeziune și constituie un valoros instrument de comunicare, ce facilitează accesul tuturor părților la informații. Iată câteva sugestii utile pentru conținutul site-ului web.

- Cadrele didactice ar putea publica planurile lecțiilor sau prezentări generale despre ceea ce au făcut elevii într-o anumită perioadă.
- Administratorii ar putea posta agende sau anunțuri.
- Este posibil ca copiii și tinerii să dorească să publice desene, picturi, poezii, povestiri, rapoarte sau alte lucrări.
- Părinții pot folosi site-ul pentru a anunța despre activitățile comune părinți-cadre didactice, ca de exemplu, festivaluri sau alte întâlniri.
- Comunitatea, în general, poate să îl folosească ca forum pentru anunțuri despre echipele de fotbal (meciuri), călătorii (excursii), activitatea poliției, lucrările de construcții de drumuri și așa mai departe.

— O varietate largă de conținuturi pot îmbogăți un site web, un blog sau un vlog, dar o bază largă de contribuitori poate îngreuna întreținerea rețelei Web. Este important să se aleagă o echipă mică de persoane care să fie responsabilă de colectarea și editarea conținutului. Această sarcină ar putea fi realizată cel mai bine de un profesor sau de un administrator, sau de o altă persoană aleasă în calitate de coordonator al tehnologiei informației și comunicațiilor (TIC).



## BUNE PRACTICI

- Monitorizați toate conturile. Creați fișiere în adresa de email pe care o utilizați pentru a vă abona la aceste servicii și categorisiți emailurile pentru a găsi întotdeauna informațiile importante despre conturile dumneavoastră, cum ar fi numele dumneavoastră de utilizator.

8. [www.codecademy.com](http://www.codecademy.com)  
9. [www.w3schools.com/](http://www.w3schools.com/)

- Utilizați întotdeauna adresa dumneavoastră de email, nu contul dumneavoastră de pe rețelele sociale, atunci când vă înregistrați la servicii online importante cum ar fi conturile site-urilor web, blogurile, vlogurile sau altele similare. Oricât de convenabil vi s-ar părea să vă înregistrați la servicii utilizând conturile de pe Facebook, Google+ sau alte conturi de pe rețele sociale, nu uitați că astfel, acceptați ca aceste servicii să acceseze o mare parte din informațiile dumneavoastră. De asemenea, deși unele rețele sociale lasă impresia că vor exista pentru totdeauna, în cazul în care serviciile acestora ar înceta într-o bună zi, este posibil să nu vă mai puteți conecta la contul dumneavoastră (de exemplu, atunci când publicul nu utilizează suficient un instrument, instrumentul respectiv poate deveni desuet).
- Partajarea conținutului în mediul online prin intermediul unui site web, blog sau vlog este o ocazie excelentă de a vă împărtăși opiniile, dar este recomandabil să vă protejați viața privată utilizând un pseudonim și să nu divulgați anumite detalii personale.
- Începeți cu pași mici, găsiți timp să învățați și să experimentați înainte de a publica conținutul dumneavoastră online sau de a-l prezenta în sala de clasă. V-ar putea fi de ajutor vizitarea altor site-uri web, bloguri sau vloguri pentru idei și inspirație.
- Întotdeauna specificați informații cheie de contact, cum ar fi adresa și numărul de telefon al școlii pe site-ul web, blogul sau vlogul școlii.
- Asigurați-vă că conținutul dumneavoastră web este prietenos utilizatorului și ajustat la dispozitive. În prezent, din ce în ce mai mulți oameni accesează conținuturile web de pe telefoanele lor mobile, iar acest lucru necesită deseori un format și un design distinct. A realiza un conținut web care este accesibil utilizatorilor cu dizabilități este, de asemenea, o bună practică. Analizați câteva dintre resursele de pe acest site web: <http://www.w3.org/WAI/gettingstarted/Overview.html>.
- Ori de câte ori este posibil, asigurați-vă că conținutul dumneavoastră web este multilingv, astfel încât persoanele care nu sunt vorbitoare de limbă română să poată, de asemenea, beneficia de conținutul dumneavoastră.



## INFORMAȚII SUPLIMENTARE

- Acest articol privind tendințele digitale oferă mai multe informații cu privire la constructorii de site-uri web: <http://web.archive.org/web/20160622040107/http://www.digitaltrends.com/computing/best-website-build-websites-free/>.
- Un articol din Wikipedia vă oferă mai multe informații cu privire la gestionarea reputației în mediul online: [https://en.wikipedia.org/wiki/Online\\_presence\\_management](https://en.wikipedia.org/wiki/Online_presence_management).
- Fișele de informare ale Comisiei Europene referitoare la noul Regulament General privind Protecția Datelor (General Data Protection Regulation – GDPR) includ „dreptul de a fi uitat”: [http://ec.europa.eu/justice/data-protection/document/factsheets\\_2016/factsheet\\_dp\\_reform\\_citizens\\_rights\\_2016\\_en.pdf](http://ec.europa.eu/justice/data-protection/document/factsheets_2016/factsheet_dp_reform_citizens_rights_2016_en.pdf).
- Articolele relevante din Convenția ONU cu privire la drepturile copilului:
 

Articolul 13 – Copiii au dreptul de a obține și difuza informații, cu excepția cazului când acest fapt ar leza drepturile altora.

Articolul 16 – Copiii au dreptul la viață personală. Copilul are dreptul la protecția legii contra unor atacuri asupra vieții lor personale, reputației, familiei și domiciliului.

Articolul 29 – Educația trebuie să dezvolte personalitatea și talentele copilului la nivelul potențialului maxim. Aceasta trebuie să încurajeze respectul copiilor față de părinți, față de propria lor cultură, precum și față de alte culturi.

Articolul 31 – Toți copiii au dreptul la odihnă și joacă și să participe la o gamă largă de activități.



## Web 2.0, Web 3.0 și alte versiuni



**W**eb 2.0 ne permite nu doar să descărcăm și să consumăm, ci să încărcăm și să creăm. Termenul „Web 2.0” se referă la ceea ce este perceput drept „a doua generație” de servicii bazate pe web care pun accent pe conținutul generat de utilizatori, utilitate și interoperabilitate. Exemplele tipice sunt site-urile rețelelor sociale (a se vedea Fișa 8), wiki-urile, instrumentele de comunicare și folksonomiile, toate facilitând colaborarea și schimbul online de informații între utilizatori. Web 2.0 cuprinde mai degrabă modificări cumulative, decât referiri la actualizări tehnice specifice, bazându-se pe facilitățile interactive ale „Web 1.0” pentru a oferi o computerizare de tip „rețea ca platformă”, care permite utilizatorilor să ruleze în întregime aplicațiile software printr-un browser.

— Utilizatorii pot deține datele de pe un site Web 2.0 și exercită controlul asupra datelor respective printr-o „arhitectură participativă,” care încurajează utilizatorii să adauge valoare aplicației pe măsură ce o utilizează. Acest lucru oferă avantaje uriașe față de site-urile tradiționale, care limitează vizitatorii la vizualizare și al căror conținut poate fi modificat doar de proprietarul site-ului. Site-urile Web 2.0 au adesea o interfață ușor de utilizat, bazată pe medii îmbinate sau „rich”, adică tehnologii avansate, cum ar fi transmisiunile video în direct, applet-uri (programe) descărcate care interacționează instantaneu cu utilizatorul și conținut care se schimbă atunci când cursorul este plasat pe acesta.

## WEB 3.0 ALTE VERSIUNI

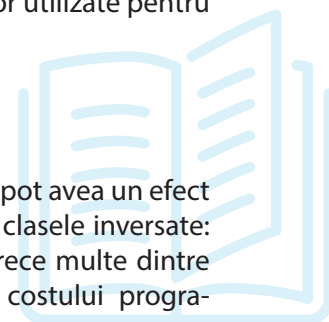
Web 3.0 (uneori puteți vedea și Web 4.0, 5.0 etc.) este un termen intens discutat. În timp ce unii îl descriu ca fiind evoluția și extinderea Web 2.0, alți specialiști îl definesc ca pe un fel de „intelență conectivă”, care unește date, concepte, aplicații și oameni și, în opinia multora, va începe, în cele din urmă, să genereze date pe cont propriu. Unii preferă termenul de „Web Semantic”, în timp ce alți experți definesc Web-ul Semantic ca fiind doar una dintre tehnologiile și tendințele convergente, care vor defini următoarea mare evoluție a Web.

Există și alte tipuri de rețele. Darknetul este o rețea care există ca o suprapunere peste ceea ce numim World Wide Web și poate fi accesat numai cu un program, configurații sau autorizări specifice, de obicei utilizând protocoale de comunicații și porturi speciale. Rețelele de la prieten la prieten (F2F – numai conexiuni directe între persoanele care se cunosc) și de la egal la egal (între persoane cu drepturi egale de utilizator) sunt utilizate, de obicei, pentru partajarea de fișiere. Rețelele precum Tor funcționează printr-o serie de conexiuni anonime și pot fi, prin urmare, mai ușor utilizate pentru activități ilegale.



## IMPLICAȚII PENTRU ȘCOLI

Instrumentele Web 2.0 facilitează creativitatea, colaborarea și comunicarea și pot avea un efect profund asupra învățării. Acestea au promovat noi modele pedagogice, cum ar fi clasele inversate: elevii realizează acasă<sup>1</sup> mai multe activități care, de regulă, au loc în clasă. Deoarece multe dintre instrumentele Web 2.0 sunt programe gratuite, acestea au contribuit la reducerea costului programelor și au încurajat dezvoltarea de noi modele de licențiere pentru școli.



Există multe distincții între Web 1.0, 2.0 și 3.0, după cum se arată în tabelul de mai jos.

Web 1.0	Web 2.0	Web 3.0
Bazat pe aplicație	Bazat pe Web	Aplicații cu mai multe dispozitive/ dinamice
Izolată	În colaborare	Distribuie conținut personalizat
Licențiat sau achiziționat	Gratuit	Platforme multi-licență convergente
Creator unic	Creație în colaborare	Creatorii și dispozitivele interacționează
Cod de proprietate	Sursă deschisă	Construit în colaborare, executabil
Conținut protejat prin drepturi de autor	Conținut partajat	Conținut generat de utilizator și de dispozitiv

Patru dintre cele mai frecvent utilizate tehnologii Web 2.0 sunt rețelele sociale (a se vedea Fișa 8), mesageria, crearea și vizionarea de videoclipuri și filme (prin podcast, MP4 etc.) și wiki-urile, deși există și alte tehnologii.

**Podcasting**<sup>2</sup> – a apărut odată cu lansarea iPod-ului (playerul multimedia portabil Apple lansat în 2001) și e format din cuvintele „iPod” și „broadcast”. Aceasta a fost o modalitate de a partaja fișierele audio pe Internet pentru a fi reproduse pe dispozitive mobile sau computere și a fost cunoscut și sub numele de MP3 (fișier digital MPEG cu o componentă audio). În prezent, majoritatea dispozitivelor mobile au facilități de înregistrare video, iar MP3 a fost depășit de MP4, un format multimedia care stochează atât audio, cât și video. Podcast-urile și videoclipurile MP4 facilitează munca profesorilor și a elevilor de a aduce lumea exterioară în sala de clasă și de a împărtăși evenimente și experiențe.

**Distribuirea de videoclipuri** a devenit extrem de populară de la lansarea YouTube în 2005 și este acum posibilă și prin numeroasele platforme sociale de comunicare. Teachertube<sup>3</sup> este un site

1. [https://en.wikipedia.org/wiki/Flipped\\_classroom](https://en.wikipedia.org/wiki/Flipped_classroom)

2. <http://computer.howstuffworks.com/internet/basics/podcasting.htm>

3. [www.teachertube.com](http://www.teachertube.com)

dedicat cadrelor didactice pentru a fi utilizat în scop educațional, bazat pe YouTube<sup>4</sup>, care poate fi, de asemenea, utilizat de școli și organizații pentru a-și crea propriile canale de partajare video. Site-urile de partajare video<sup>5</sup> au, de obicei, opțiuni de căutare și permit utilizatorilor să posteze, să comenteze, să eticheteze și să vizioneze videoclipuri. Există multe comunități pentru crearea și distribuirea de videoclipuri asociate unui interes comun. Mai recent, au apărut site-uri care permit utilizatorilor să posteze videoclipurile online și să adauge sunet, subtitrări și așa mai departe. Un astfel de exemplu este Jumpcut<sup>6</sup>.

— **Wiki-urile** sunt pagini web care permit cititorilor să interacționeze și să colaboreze cu alte persoane, deoarece astfel de pagini pot fi editate sau completate de oricine. Un wiki este un minunat instrument Web 2.0 pentru scrierea prin colaborare de lucrări în cadrul școlii. De exemplu, Google docs<sup>7</sup> permite utilizatorilor să lucreze în colaborare pe texte, prezentări Power Point și tabele. Un alt exemplu de un wiki bine-cunoscut este Wikipedia, o enciclopedie dezvoltată prin colaborare, care include acum mai multe articole actualizate decât Encyclopaedia Britannica.

— **Social bookmarking** (înscrisura în directoare sociale) permite utilizatorilor să partajeze pe Internet preferințele sau marcajele (bookmarks) generate de utilizator. În mod tradițional, utilizatorii aveau o listă de site-uri web preferate, ca parte a propriului lor browser de Internet. Acum, social bookmarking permite ca aceste liste să fie ușor partajate, astfel încât oricine să le poată utiliza. Conținutul poate fi clasificat utilizând etichete (tag-uri) pentru a facilita căutarea și utilizarea acestuia. Site-ul web și aplicația Delicious<sup>8</sup> constituie un exemplu de social bookmarking și arată utilizatorilor câte alte persoane au salvat un anumit site.

— **Distribuirea de fotografii** este un instrument popular, care permite utilizatorilor să partajeze fotografii cu familia și prietenii. Un astfel de exemplu este Flickr<sup>9</sup>, care permite utilizatorilor să posteze fotografii și apoi să invite alte persoane să le vizualizeze fie una câte una, fie ca o succesiune de imagini. Fiecărei fotografii i se pot adăuga note și etichete și toate persoanele pot lăsa, de asemenea, comentarii.

— **Programul de editare și retușare a fotografiilor** este acum disponibil online și permite utilizatorilor să își îmbunătățească fotografiile. Exemple ale acestei aplicații din ce în ce mai populare sunt:

- Picasa (Google) <<http://picasa.google.com>>
- iPhoto (Apple) <[www.apple.com/iphoto](http://www.apple.com/iphoto)>
- Photo Story (Microsoft) <<http://microsoft-photo-story.en.softonic.com>>.



## CONSIDERAȚII DE ORDIN ETIC ȘI RISCURI

- Instrumentele Web permit oricărei persoane să încarce sau să editeze materiale pe Internet, dar este posibil ca conținutul să nu fie întotdeauna corect sau exact din punct de vedere factual. Acest lucru evidențiază importanța oferirii unor oportunități ample elevilor, în vederea dobândirii competențelor mediatice necesare pentru a evalua corectitudinea și atitudinea site-urilor și a conținutului.
- Cadrele didactice nu ar trebui să meargă pe linia simplistă, conform căreia orice conținut fals este în mod necesar rău – acesta poate fi o extensie a unui simulacru în mediul online și ar putea avea și o valoare educațională (de exemplu, profiluri false ale unor personaje celebre din istorie pe rețelele de socializare).
- Instrumentele și aplicațiile Web oferă oportunități nelimitate utilizatorilor de a publica informații despre ei înșiși și despre alții. Cu toate acestea, ei trebuie să rămână vigilenți la riscurile dezvăluirii propriei persoane și la pierderea vieții private. Regula principală este de a nu publica nimic ce nu este destinat lumii întregi (a se vedea Fișa 8 cu privire la rețelele sociale).

4. <https://support.google.com/youtube/search?q=teachers+channel>

5. <http://computer.howstuffworks.com/internet/basics/video-sharing.htm>

6. [www.jumpcut.com](http://www.jumpcut.com)

7. <https://www.google.com/docs/about/>

8. <https://del.icio.us>

9. [www.flickr.com/](http://www.flickr.com/)

- Este nevoie de timp și efort pentru a integra tehnologiile în procesul de învățare, dar, înainte de a începe acest proces, asigurați-vă că utilizarea instrumentelor Web 2.0 și Web 3.0 va avea un impact semnificativ asupra elevilor dumneavoastră.
- Nu toate instrumentele Web 2.0 sunt egale sau au aceeași filozofie, sau model de afaceri. În timp ce un site ca Wikipedia are o abordare necomercială, independentă, bazată pe voluntariat și colaborare, multe rețele sociale, precum Facebook, au un scop comercial.
- Conținutul pe care îl introduceți în Wikipedia va fi folosit în beneficiul comunității, în timp ce conținutul pe care îl introduceți pe Facebook va fi folosit, printre altele, pentru a vă prezenta publicitate personalizată.
- Evaluarea produselor și a serviciilor a devenit un lucru popular datorită capacităților Web 2.0/3.0. Cu toate acestea, opinia critică este mai necesară decât oricând deoarece, chiar și pe cele mai populare site-uri de acest tip, ratingurile nu sunt întotdeauna fiabile – recomandările plătite sunt din ce în ce mai frecvente.



## IDEI PENTRU LUCRUL ÎN CLASĂ

- **Utilizarea Internetului:** pentru 86% dintre utilizatorii de Internet, socializarea este cea mai populară activitate în mediul online, fiind urmată de căutarea de informații (aproximativ 50%) și de activitățile legate de carieră și comerț (aproximativ 25%)<sup>10</sup>. Discutați cu elevii/copiii dumneavoastră despre statisticile de utilizare a Internetului. Cum se compară utilizarea de către aceștia a Internetului cu cea a altor tineri din țara lor și din alte țări din întreaga lume, dar și cu utilizarea de acum un deceniu? Ce consecințe ar implica acest fapt?
- **Video:** elevii își pot crea propriile videoclipuri pentru a-și distribui pe larg părerile și opiniile cu privire la un anumit subiect. Rugați elevii să lucreze în echipe, să pregătească un scenariu și să utilizeze telefonul mobil pentru a crea videoclipul. Acest lucru le va oferi ocazia de a discuta subiecte precum drepturile de autor (a se vedea Fișa 14), obținerea acordului persoanei filmate/fotografiate (sau permisiunii părinților acestora, în cazul minorilor) înainte de a încărca imagini pe Internet și așa mai departe. Aceștia pot să distribuie videoclipul prin intermediul site-ului web al clasei sau al școlii sau să utilizeze un canal dedicat pe YouTube<sup>11</sup> pentru a se adresa milioanei de utilizatori de Internet. În prezent, unele școli dispun de înregistrări video ale lecțiilor, pentru a le permite elevilor care au absentat să recupereze lecțiile pe care le-au pierdut.
- **Wiki-urile:** identificați wiki-urile care sunt cel mai bine adaptate mediului dumneavoastră educațional (a se vedea informații suplimentare), apoi propuneți elevilor dumneavoastră să realizeze o lucrare prin colaborare. Veți putea să monitorizați, în mod activ, activitatea fiecărui elev și să păstrați o evidență a tuturor schimbărilor efectuate. Wiki-urile oferă oportunități ideale pentru ca elevii să se implice în adevărate proiecte de colaborare dintre diferite școli și țări.
- **Social bookmarking:** stabiliți un proiect de cercetare specific și împărțiți sarcinile fiecărui elev sau grupurilor de elevi. Puteți utiliza un motor de căutare pentru a găsi un instrument de social bookmarking care să se potrivească nevoilor dumneavoastră. Fiecare grup poate folosi social bookmarking-ul pentru a compila un set detaliat de link-uri utile. Unul dintre avantajele este faptul că elevii nu trebuie să acceseze același computer de fiecare dată când vor să continue lucrul, deoarece adresele lor preferate sunt disponibile pe orice calculator, în orice moment.

10. <http://www.pewglobal.org/2015/03/19/2-online-activities-in-emerging-and-developing-nations/>.

11. [www.youtube.com](http://www.youtube.com)

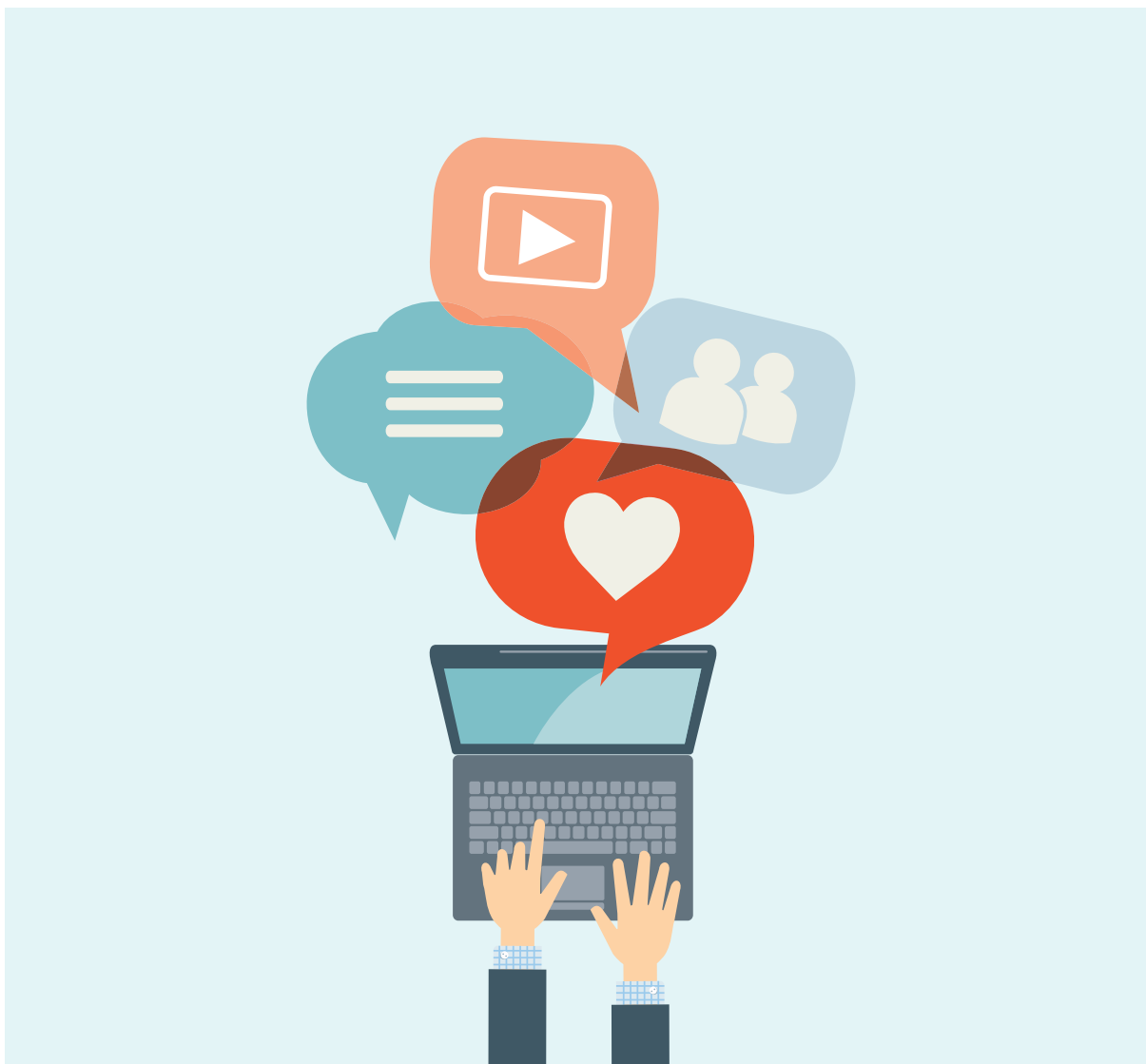


## INFORMAȚII SUPLIMENTARE

- Aceste două wiki-uri pot fi folosite în mediul educațional: <http://mediawiki.com> și <http://www.pbworks.com>.
- Cadrele didactice din câteva sute de mii de școli din Europa lucrează în prezent în colaborare într-un mediu de învățare sigur, cu clase din alte țări, prin intermediul rețelei de eTwinning a Comisiei Europene: [www.etwinning.net/en/pub/index.htm](http://www.etwinning.net/en/pub/index.htm).
- Informațiile privind utilizarea în siguranță a instrumentelor Web 2.0 la domiciliu și la școală pot fi găsite la [www.betterinternetforkids.eu/](http://www.betterinternetforkids.eu/).
- Deși YouTube Kids oferă mai puține funcții decât YouTube.com pentru vizionarea și distribuirea de videoclipuri, acesta funcționează într-un mediu sigur, adaptat în mod special pentru copiii de vârste mici și oferă îndrumări pentru părinți, cadre didactice și îngrijitori: <https://kids.youtube.com/>.
- Informațiile despre instrumentele Web 2.0 destinate utilizării în clasă și descărcările gratuite pot fi găsite la <http://web.archive.org/web/20160413121845/http://www.solutionwatch.com/512/back-to-school-with-the-class-of-web-20-part-1/>.
- Aplicațiile Web 2.0 utile pentru clasele primare pot fi găsite la adresa <http://web.archive.org/web/20150914224206/http://langwitches.org/blog/2007/12/22/best-web-20-applications-for-elementary-school/>.



## Blogurile și vlogurile



Jurnalul online a evoluat în blogul modern de astăzi, încă de la începutul anilor 1990. Cuvântul „blog”<sup>1</sup> este prescurtarea termenului „weblog” și se referă la un jurnal online creat și publicat de grupuri și persoane fizice. Termenul „weblog” a fost adăugat în dicționarul Oxford în 2003. Deși unii politicieni și celebriități s-au apucat de blogging, blogurile continuă să fie cel mai des asociate cu simplitii utilizatori, care își expun opiniile și vorbesc despre viața lor de zi cu zi.

— Blogurile și vlogurile (bloguri video) au devenit, de asemenea, platforme pentru schimbarea socială, în care bloggerii și vloggerii evidențiază provocări din viețile lor, informând publicul despre astfel de probleme precum parentajul sau viața cu autism, sau creșterea gradului de conștientizare politică cu privire la diverse probleme.

— Din cauza popularității blogurilor, au fost create multe site-uri web care oferă programe pentru a ajuta la crearea și publicarea materialelor. Fiecare idee dintr-un blog poate fi comentată, fapt ce oferă oportunități de discuție și poate ajuta la generarea de noi idei.

— Blogurile sunt găzduite de servicii dedicate de găzduire a blogurilor sau de servicii obișnuite de găzduire pe web și, în prezent, comisioanele serviciilor de găzduire sunt considerate a fi rezonabile.

1. <https://en.wikipedia.org/wiki/Blog>



## Blogurile mobile

— Blogurile mobile, cunoscute ca mobloguri, sunt o metodă de publicare pe un site web sau pe un blog utilizând un telefon mobil sau un dispozitiv portabil. Bloggingul mobil<sup>2</sup> a apărut datorită dezvoltării caracteristicilor funcționale ale emailului pe telefoanele mobile (a se vedea Fișa 5 cu privire la tehnologiile mobile).



## Vlogurile

— Un blog video sau un jurnal video este același ca și un blog, așa cum e descris mai sus, dar postările sunt în format video. Vlogurile au fost inițial populare pe YouTube, iar acum puteți găsi vloguri pe Vine, Instagram, Facebook și chiar pe Pinterest.



## Feed-uri RSS

— RSS<sup>3</sup> sau „Rich Site Summary” este acum folosit pentru a sindicaliza blogurile. Cei care doresc să își publice conținutul pe alte site-uri web pot să-l pună la dispoziție utilizând un limbaj XML<sup>4</sup> sau un limbaj de marcare XML pentru sindicalizarea web.

— XML este un tip de cod similar cu HTML și este, de asemenea, cunoscut sub numele de „feed”. Practic, acesta le permite cititorilor să se „aboneze” la conținut și să primească actualizări de bloguri, fără ca ei să viziteze blogul pentru a le obține.



## Importanța educațională a blogurilor și a vlogurilor

- ▶ Blogurile și vlogurile permit creatorilor să își vocifereze opiniile. Bloggerii și vloggerii pot să împărtășească interesele, să facă schimb de gânduri și să informeze publicul despre problemele la care rezonază. Aceștia au posibilitatea să documenteze viața, să partajeze aventuri și să ofere puncte de vedere vizuale pe o platformă care este ușor accesibilă tuturor.
- ▶ Bloggerii și vloggerii pot fi simultan și bloggeri mobili, deoarece își folosesc telefoanele inteligente pentru a scrie, publica și încărca conținut.
- ▶ Deoarece telefoanele inteligente sunt disponibile pe scară largă, un public mai variat și, adesea, mai tânăr poate să realizeze bloguri și vloguri, fără a avea nevoie de echipamente informaționale scumpe.
- ▶ De asemenea, blogurile și vlogurile sunt folosite și de jurnaliști, cercetători și activiști ca un mijloc și o sursă importantă de informare și exprimare.
- ▶ De asemenea, s-au dezvoltat și blogurile și vlogurile care abordează tematici precum dizabilitatea și nevoile speciale, pentru a crește gradul de conștientizare și a iniția discuții.



## Blogurile în mediul educațional

— Blogurile oferă elevilor posibilitatea de a prelua controlul asupra studiilor și de a crea un forum public în care să își publice gândurile și sentimentele. Acesta poate fi utilizat ca un instrument didactic creativ pentru discuții și colaborare. De exemplu, elevii care studiau disciplina literatura modernă, au folosit blogul pentru a studia romanul *Viața secretă a albinelor*. Autorul a scris o introducere pentru cursul dat, iar elevii și părinții acestora au fost invitați să scrie despre impresiile lor, despre însărcinările legate de lectură, care erau fixate pentru fiecare zi. Autorul a comentat apoi pe marginea acestora (a se vedea <<http://techtraining.dpsk12.org/ilt/Bees/SLOBees.pdf>>).

— Experții observă un proces în trei etape implicat în blogging: definirea publicului, a scopului și a domeniului de aplicare. Acest lucru este descris pe site-ul <<https://macln.wordpress.com/2011/01/12/three-step-process-for-blogging/>>. Bloggerii trebuie să descopere, să filtreze și să posteze materiale în mod continuu. Căutând materialul pe baza căruia trebuie realizate comentarii, elevul devine din ce în ce mai familiarizat cu diferite teorii și idei și dezvoltă competențele necesare pentru a analiza în mod critic conținutul și pentru a discerne conținutul adevărat.

2. [https://en.wikipedia.org/wiki/Mobile\\_blogging](https://en.wikipedia.org/wiki/Mobile_blogging)

3. <https://en.wikipedia.org/wiki/RSS>



— Această tehnologie poate fi folosită ca factor motivațional în educație. Elevii sunt interesați de bloguri datorită creativității acestora și a posibilității de auto-exprimare. Acesta poate fi folosit ca un mijloc pentru predarea unei mari varietăți de subiecte.

— Blogurile oferă fiecărui elev din clasă șansa de a participa la o discuție care expune copiii și tinerii la diferite perspective.



## CONSIDERAȚII DE ORDIN ETIC ȘI RISCURI

- Reamintiți elevilor că nu trebuie să divulge informații personale în spațiile publice pe Internet, la fel cum nu le-ar dezvălui într-un forum offline. Aceasta reprezintă o problemă mai ales pentru bloguri, care adesea, sunt personale prin însăși natura lor.
- Nici blogurile anonime nu sunt întotdeauna complet anonime și ștergerea unui blog nu înseamnă că întregul său conținut nu va putea fi vizualizat.
- Gândiți-vă la securitatea dumneavoastră în mediul offline și puneți-vă întrebarea: cât de ușor i-ar fi cuiva să mă găsească în baza informațiilor pe care le-am furnizat?
- Gândiți-vă la mesajul și la personalitatea pe care le veți demonstra în calitate de blogger sau vlogger. Ar putea fi acestea ofensatoare pentru unele persoane? Ar putea fi acestea ofensatoare pentru școala dumneavoastră sau viitorul angajator?
- Blogurile și vlogurile pot fi, de asemenea, utilizate pentru a difuza mesaje pline de ură și discriminatorii sau pentru a promova conținut extremist, radical sau jenant.



## INSTRUCȚIUNI

— Dacă aveți competențe tehnice, puteți crea un blog de la zero. Majoritatea oamenilor folosesc site-uri care oferă instrumente pentru crearea și publicarea conținutului ca blog. Bloguri Școlare la adresa <<http://www.schoolblogs.net/wpress/>>, Blogger (a se vedea mai jos) și Wordpress sunt gazde populare, care oferă servicii gratuite. Acestea oferă instrucțiuni simple, pas cu pas, care vă ajută să creați un cont, să vă denumiți blogul și să alegeți un model.

— Odată ce blogul dumneavoastră este pus în funcțiune, elaborați și editați intrările de pe o pagină web centrală. Interfața pentru programul popular este formatul WYSIWYG5 și este extrem de ușor de utilizat. Vizitatorii blogului dumneavoastră pot comenta conținutul dând clic pe un link de comentarii de la sfârșitul fiecărei intrări.

— Puteți alege să vă moderați comentariile înainte ca acestea să fie afișate pe pagina dumneavoastră web.

— Puteți să adăugați hyperlink-uri și imagini la comentariile dumneavoastră. Butoanele pentru aceste funcții sunt incluse pe bara de instrumente deasupra casetei de text în care introduceți conținutul.



## IDEI PENTRU LUCRUL ÎN CLASĂ

- Rugați elevii să se împartă în echipe a câte doi, în care vor aborda un subiect. Un elev este bloggerul, iar celălalt elev este intervievatorul. Bloggerul jurnalist realizează un interviu și apoi scrie un blog pe care interlocutorul îl aprobă.
- Cercetați blogurile și vlogurile de top dedicate dizabilităților, nevoilor speciale, schimbărilor sociale sau gradului de conștientizare socială. Rugați elevii să discute modul în care pot contribui prin comentarii sau prin trimiterea unui articol de blog.
- Rugați elevii să analizeze care este cea mai bună metodă de a transmite un mesaj: blogul, vlogul, tweet-urile, videoclipurile virale sau videoclipurile Periscope. Lista nu este exhaustivă.

Dacă elevii aleg Twitter, Vine, Periscope sau altă aplicație, atenționați-i să includă link-uri către blogul lor.

- Rugați elevii să enumere 5-10 subiecte de interes. Apoi efectuați niște cercetări pentru a afla dacă există bloguri pe subiectul preferat al acestora.
- Identificați pe unii dintre cei mai buni bloggeri elevi și tineri. Ce subiecte abordează aceștia: mediul, politica, moda, muzica, tehnologia?



## BUNE PRACTICI

- Un blog este o ocazie excelentă de a vă exprima opiniile, dar este bine să vă protejați viața privată utilizând un pseudonim și nedivulgând anumite detalii personale. Copiii și tinerii trebuie să fie atenți în mod special în ceea ce privește dezvăluirea de informații personale într-un blog.
- Respectați legile privind drepturile de autor și nu utilizați modelul de blog sau fotografiile altor persoane pe blogul dumneavoastră fără permisiunea acestora. Există multe site-uri care vă permit să le utilizați gratuit fotografiile, cu sau fără atribuire.
- Începeți propriul blog pentru a vă familiariza cu această practică înainte de a o prezenta în sala de clasă. Puteți să vizitați și alte bloguri pentru idei și inspirație. Site-ul web Bloguri Școlare (*School Blogs*)<sup>4</sup> are peste 4 mii de membri și oferă utilizatorilor posibilitatea de a-și lansa propriul blog școlar.
- Petreceți timp explicând elevilor dumneavoastră conceptul de blogging. Spuneți-le care este scopul și dați exemple de bloguri bune și mai puțin bune. Apoi, oferiți elevilor un set de reguli stricte, care ar putea include volumul și frecvența postărilor, subiectele, numărul de hyperlink-uri/fotografii și așa mai departe. Cereți elevilor să întrețină un blog, să discute despre experiențele lor și să comenteze blogurile altor persoane.



## INFORMAȚII SUPLIMENTARE

- Blogger este un site care oferă instrumente pentru blogging și acum pentru blogging mobil: [www.blogger.com/start](http://www.blogger.com/start).
- Sfaturi juridice și etice pentru bloggeri pot fi găsite la: <http://weblogs.about.com/od/bloggingethics/tp/Blogging-Best-Practices.htm>.
- Fundația Frontiere Electronice (Electronic Frontiers Foundation – EFF) oferă un ghid juridic pentru bloggeri: <http://www.eff.org/bloggers/lg/>.
- Weblogg-ed – acest site urmărește tendințele actuale de blogging în domeniul educației: [www.weblogg-ed.com/](http://www.weblogg-ed.com/).
- „Blogging și RSS – „ce este?” și „inițierea” în noile instrumente web eficiente pentru cadrele didactice”: <http://web.archive.org/web/20160413030845/http://www.infotoday.com/MMSchools/jan04/richardson.shtml>.
- „Bloggerul educat: folosirea blogurilor pentru a promova educația în clasă”: <http://firstmonday.org/ojs/index.php/fm/article/view/1156/1076>.
- Instrumentele pentru sprijinirea competențelor de scriere ale copiilor de la grădiniță până în clasa a XII-a pot fi găsite la adresa [www.readwritethink.org/student\\_mat/index.asp](http://www.readwritethink.org/student_mat/index.asp).
- Resursele de blogging pentru formatori sunt disponibile la adresa <http://www.socialstudiescentral.com/>.

4. <http://www.schoolblogs.net/>

- Darren Rowse a fost unul dintre primii bloggeri care și-a câștigat existența în întregime din bloguri. Acesta oferă sfaturi și resurse pe site-ul său web: [www.probblogger.net/](http://www.probblogger.net/).
- Site-urile cu fotografii gratuite care pot fi utilizate pe bloguri: [www.pixabay.com](http://www.pixabay.com), [www.flickr.com/creativecommons/](http://www.flickr.com/creativecommons/) și [www.freedigitalphotos.net](http://www.freedigitalphotos.net).
- „Să învățăm împreună să fim în siguranță” este un set de instrumente elaborate pentru școli de către Departamentul Copii, Școli și Familii din Marea Britanie, ce oferă resurse pentru cadrele didactice în materie de extremism și radicalizare: [www.preventforschools.org/download/file/mmu-learning-together-to-be-safe.pdf](http://www.preventforschools.org/download/file/mmu-learning-together-to-be-safe.pdf).
- Articole relevante ale Consiliului Europei, inclusiv Convenția Europeană a Drepturilor Omului: [www.echr.coe.int/Documents/Convention\\_ENG.pdf](http://www.echr.coe.int/Documents/Convention_ENG.pdf):  
 Articolul 8 – Dreptul la respectarea vieții private și de familie.  
 Articolul 10 – Libertatea de exprimare.  
 Articole relevante din Convenția ONU cu privire la drepturile copilului:  
 Articolul 13 – Copiii au dreptul de a obține și difuza informații, cu excepția cazului când acest fapt ar leza drepturile altora.  
 Articolul 16 – Copiii au dreptul la viață personală. Copilul are dreptul la protecția legii contra unor atacuri asupra vieții lor personale, reputației, familiei și domiciliului.  
 Articolul 29 – Educația trebuie să dezvolte personalitatea și talentele copilului la nivelul potențialului maxim. Aceasta trebuie să încurajeze respectul copiilor față de părinți, față de propria lor cultură, precum și față de alte culturi.



## Internetul în mișcare



**U**tilizarea Internetului mobil – utilizarea Internetului pe un calculator portabil sau un dispozitiv portabil prin conexiunea mobilă sau fără fir – este în creștere, deoarece oamenii profită de noi modalități de conectare atunci când sunt departe de casă sau de lucru.

— În 2012, 36% dintre persoanele cu vârste cuprinse între 16 și 74 de ani din cele 28 de state membre ale UE au folosit un dispozitiv mobil pentru a se conecta la Internet. Doi ani mai târziu, numărul crescuse la 51%. Studiile<sup>1</sup> arată că cele mai frecvente dispozitive mobile pentru conectarea la Internet au fost telefonul mobil sau inteligent, laptopul, notebookul, netbookul sau tableta.

— Puține persoane au achiziționat telefoane mobile atunci când acestea au devenit disponibile pentru prima dată în 1983. În 1995, existau cinci abonamente mobile la 100 de locuitori din Uniunea Europeană. Potrivit Eurostat, în 2003 cifra era de 80 de telefoane mobile la 100 de locuitori în cele 25 de state care făceau parte din UE după extindere.

— Zece ani mai târziu, numărul de abonamente pentru telefoanele inteligente a constituit aproximativ 400 de milioane, reprezentând aproape 40% din numărul total de telefoane mobile. Ericsson

1. [http://web.archive.org/web/20160413105315/http://ec.europa.eu/eurostat/statistics-explained/index.php/Information\\_society\\_statistics\\_-\\_households\\_and\\_individuals](http://web.archive.org/web/20160413105315/http://ec.europa.eu/eurostat/statistics-explained/index.php/Information_society_statistics_-_households_and_individuals)

prognozează că până la sfârșitul anului 2020, numărul de telefoane inteligente în Europa va ajunge la 800 de milioane<sup>2</sup>.

— Limita dintre tehnologia mobilă și calculatoarele personale s-a estompat, având în vedere faptul că majoritatea telefoanelor mobile sunt dotate cu funcție de navigare pe Internet și email, iar tot mai multe calculatoare sunt wireless.



## TEHNOLOGIA MOBILĂ

— Tehnologia mobilă este tehnologia utilizată pentru comunicațiile celulare, iar unii susțin că tehnologia mobilă reprezintă viitorul informaticii<sup>3</sup>.

### Mesajele SMS

— Serviciile de mesaje scurte (SMS) reprezintă funcția serviciului de mesagerie text a sistemelor de telefonie, a Webului sau a comunicațiilor mobile<sup>4</sup>.

### Mesajele MMS

— Serviciile de mesaje multimedia (MMS) este o funcție care permite utilizatorilor să trimită mesaje care includ conținut multimedia de pe și pe telefoanele mobile<sup>5</sup>.

### Învățarea mobilă (M-learning)

— Învățarea mobilă se referă la învățarea cu ajutorul tehnologiilor mobile, cum ar fi telefoanele mobile, calculatoarele portabile și asistenții digitali personali (ADP)<sup>6</sup>.

### Geolocalizarea

— Geolocalizarea este capacitatea de a identifica locația geografică a unui obiect real, cum ar fi un telefon mobil sau un terminal de calculator conectat la Internet.

— Utilizatorii de tehnologii mobile trebuie să înțeleagă funcția de geolocalizare de pe dispozitivele lor și să poată configura setările de confidențialitate standard pe dispozitivele mobile (pentru mai multe informații cu privire la setările de confidențialitate, a se vedea Fișa 9).

### Aplicații

— O aplicație sau o aplicație mobilă este un program de calculator destinat în mod specific să funcționeze pe dispozitive mobile, cum ar fi telefoanele, tabletele, ceasurile inteligente și, în unele cazuri, îmbrăcămintea și accesoriile<sup>7</sup>. Pentru mai multe informații despre haine și accesorii inteligente, a se vedea Fișa 23.

— Volumul de aplicații a crescut direct proporțional cu numărul de utilizatori de telefoane mobile și se estimează că industria aplicațiilor generează venituri de peste 10 miliarde de euro pe an în cadrul Uniunii Europene<sup>8</sup>.

— Există o mare varietate de aplicații disponibile care sunt fie gratuite, fie plătite. Se recomandă citirea recenziilor pentru aplicații înainte de descărcare sau achiziționare, deoarece aplicațiile gratuite pot ajunge să fie costisitoare din cauza achizițiilor in-app (a se vedea Fișa cu privire la cumpărăturile online).

### Mobicash

— Odată cu creșterea numărului de utilizatori de telefoane mobile, instituțiile financiare au introdus o singură platformă financiară mobilă fără numerar, care oferă servicii de procesare a tranzacțiilor și de plăți mobile.

2. <http://web.archive.org/web/20150324081657/http://www.ericsson.com/res/docs/2014/emr-november2014-regional-appendices-europe.pdf>

3. [https://en.wikipedia.org/wiki/Mobile\\_technology](https://en.wikipedia.org/wiki/Mobile_technology)

4. [https://en.wikipedia.org/wiki/Short\\_Message\\_Service](https://en.wikipedia.org/wiki/Short_Message_Service)

5. [https://en.wikipedia.org/wiki/Multimedia\\_Messaging\\_Service](https://en.wikipedia.org/wiki/Multimedia_Messaging_Service)

6. <https://en.wikipedia.org/wiki/M-learning>

7. [https://en.wikipedia.org/wiki/Mobile\\_app](https://en.wikipedia.org/wiki/Mobile_app)

8. <http://web.archive.org/web/20160617033122/http://www.visionmobile.com/product/the-european-app-economy/>

— De exemplu, serviciile financiare mobile de la furnizorul Orange, Orange Money, sunt disponibile în 13 țări: Botswana, Camerun, Coasta de Fildeș, Egipt (sub denumirea de Mobicash), Guinea, Iordania, Kenya, Madagascar, Mali, Mauritius, Niger, Senegal și Uganda<sup>9</sup>.

— Marea Britanie raportează că până în anul 2021, consumatorii britanici ar putea cheltui aproximativ 30,5 miliarde de dolari pentru achizițiile realizate de pe telefoanele mobile<sup>10</sup>.



## IMPORTANȚA ÎNȚELEGERII PROBLEMELOR

- Există îngrijorări legate de faptul că copiii primesc telefoane mobile sau tablete prea devreme, deoarece nu au fost încă efectuate studii pe termen lung pentru a investiga ce probleme de dezvoltare pot apărea din cauza accesului timpuriu la telefoanele mobile sau tablete.
- Alte îngrijorări țin de implicarea copiilor în cumpărăturile online și în comerțul electronic, fără înțelegerea implicațiilor.
- Cercetările efectuate nu sunt concludente în ceea ce privește pericolele pe termen lung ale expunerii la radiații, indiferent cât de mică ar fi doza.
- Deși utilizarea calculatorului este adesea încă reglementată în casă, mulți părinți consideră că utilizarea telefonului mobil este „privată”. Încurajați de această libertate recent dobândită, copiii se pot confrunta cu probleme financiare, cheltuind bani pe campanii de promovare a unor premii „cadou” sau a unor accesorii cum ar fi tonurile de apel.
- Telefoanele mobile pot fi utilizate ca dispozitive de urmărire prin facilitățile de geolocalizare pe care le încorporează. Siguranța versus libertatea încă rămâne a fi subiect de discuții.
- Tehnologia Bluetooth<sup>11</sup> ridică probleme de securitate, cum ar fi pirateria (hacking-ul) și trimiterea sau primirea de mesaje nesolicitate.
- Blogurile mobile (moblogurile)<sup>12</sup> sunt bloguri pe telefoane mobile (jurnale web). Acestea facilitează postarea de către tineri a informațiilor și a fotografiilor, însă, pot compromite siguranța acestora și a altora.
- Bullyingul mobil (intimidare, agresare) devine din ce în ce mai îngrijorător și nu se limitează numai la telefoanele inteligente și tablete. Actualmente, există ceasuri inteligente cu aplicații pre-instalate ale rețelelor sociale.
- Camera foto a telefonului mobil și accesul ușor la Internet de pe telefon pot reprezenta o amenințare la adresa vieții private: există o tendință îngrijorătoare în rândul tinerilor de a face „fotografii compromițătoare” (de exemplu, fotografii cu tineri din vestiarul sălii de sport sau în situații jenante, fotografii cu cadrele didactice din sală) și chiar de a le altera înainte ca acestea să fie încărcate pe Web.
- Costurile telefonului mobil: adesea, copiii nu sunt conștienți de costurile ridicate ale anumitor servicii, cum ar fi votul electronic, serviciile SMS premium nedorite și achizițiile în cadrul aplicațiilor.
- Deoarece telefoanele mobile distrag atenția, acestea pot reprezenta un risc pentru șoferi, dar și pentru pietoni, după cum s-a observat recent. Sunt numeroase persoane care trimit mesaje text în timp ce merg pe jos, încât există aplicații disponibile pe Apple<sup>13</sup> sau Android<sup>14</sup>, care permit vizualizarea terenului în timp ce persoana trimite mesaje text, cu capul aplecat.
- Virușii<sup>15</sup> au infectat telefoanele mobile de prin 2004, încă de când acestea au devenit articole de uz cotidian. F-Secure estimează că există sute de viruși mobili și că aceștia continuă să crească în permanență ca număr și tip. Vedeți cele mai recente amenințări în secțiunea „Descrierea amenințărilor”<sup>16</sup>.

9. <https://goo.gl/4LQveU>

10. <https://goo.gl/8a7Dx7>

11. <https://en.wikipedia.org/wiki/Bluetooth>

12. [https://en.wikipedia.org/wiki/Mobile\\_blogging](https://en.wikipedia.org/wiki/Mobile_blogging)

13. <https://itunes.apple.com/en/app/type-n-walk/id331043123?mt=8>

14. <https://play.google.com/store/apps/details?id=com.biztech.typewhilewalk&hl=en>

15. [http://en.wikipedia.org/wiki/Computer\\_virus](http://en.wikipedia.org/wiki/Computer_virus); [https://en.wikipedia.org/wiki/Mobile\\_virus\\_and\\_worms](https://en.wikipedia.org/wiki/Mobile_virus_and_worms); [http://en.wikipedia.org/wiki/Computer\\_worm](http://en.wikipedia.org/wiki/Computer_worm)

16. [https://www.f-secure.com/en/web/labs\\_global/threat-descriptions](https://www.f-secure.com/en/web/labs_global/threat-descriptions)



## CONSIDERAȚII DE ORDIN ETIC ȘI RISCURI

- Internetul „de oriunde” prezintă mai multe riscuri, deoarece mulți nu se gândesc nici măcar pe o clipă să seteze corespunzător parametrii de confidențialitate. Facilitatea de utilizare și disponibilitatea mai multor dispozitive per utilizator face ca intruziunile să fie mai probabile.
- Mulți utilizatori profită de conectivitatea wireless gratuită, disponibilă în cafenele, restaurante și alte locuri publice și furnizează informații personale și financiare în aceste spații.
- Fiind disponibil oricând, oriunde, Internetul înseamnă, de asemenea, că nu există o perioadă de reflecție pentru a lua decizii despre ceea ce se încarcă sau se postează în mediul online, despre cumpărături și alte activități în mediul online. De exemplu, multe aplicații permit transmiterea în direct a evenimentelor în desfășurare, astfel încât copilul dumneavoastră poate să transmită o scenă jenantă sau violentă care are loc în fața ochilor săi, fără a putea să reflecteze dacă este o idee bună sau nu să înregistreze sau să publice un astfel de conținut.
- Din cauza ușurinței cu care chiar și copiii foarte mici pot face achiziții prin intermediul dispozitivelor mobile, specialiștii avertizează asupra unei tendințe emergente a ceea ce ei numesc „virtualizarea” banilor. Este vorba de situații în care copiii nu înțeleg valoarea reală a banilor.



## INSTRUCȚIUNI

- Telefoanele mobile sunt populare și este ușor și relativ ieftin să îl procuri. Odată ce ai cumpărat un telefon, poți alege să plătești prin opțiunea PrePay pentru anumite suplimentări de minute sau poți să vă abonați la un anumit operator și să plătești o taxă lunară pentru servicii.
- Dispozitivele mobile, cum ar fi telefoanele inteligente, tabletele, cititoarele de cărți electronice (eReader) și jocurile de mână, necesită doar o conexiune Wi-Fi pentru a oferi acces la lumea online.



## IDEI PENTRU LUCRUL ÎN CLASĂ

- Deoarece telefoanele mobile sunt atât de populare în rândul tinerilor, cadrele didactice îi pot motiva pe elevi prin încorporarea utilizării mesajelor SMS etc. în activitățile din clasă. Portabilitatea dispozitivelor este benefică pentru cadrele didactice care se află în mișcare și pentru elevii care lucrează în grupuri sau fac muncă în teren. S-a observat că utilizarea dispozitivelor mobile în procesul de învățare atât în școală, cât și în afara școlii, încurajează elevii să își asume responsabilitatea pentru munca lor. Probabilitatea ca aceștia să își piardă caietele cu notițe și temele pentru acasă este mai mică.

- În timpul vizitelor în teren, cereți elevilor să înregistreze impresiile pe un dispozitiv mobil, utilizând fotografii și videoclipuri pentru a realiza pe deplin sarcinile primite.
- Solicitați elevilor să utilizeze diverse aplicații pentru a-și detalia temele, de exemplu Vine pentru videoclipuri scurte, Periscope pentru raportarea la fața locului sau Twitter și Facebook pentru activitățile academice curente.
- Solicitați elevilor să identifice riscurile și provocările legate de utilizarea telefoanelor inteligente și a dispozitivelor mobile în sala de clasă. Sunt aceștia de părere că este posibil ca o oră de clasă să se bazeze 100% pe tehnologie? De ce? De ce nu?



## BUNE PRACTICI

- Utilizați un telefon mobil cu radiații scăzute<sup>17</sup> și anume, cu o valoare RAS la nivelul urechii de cel mult 0,56 W/kg și o valoare a RAS la nivelul corpului mai mică de 0,57 W/kg și căști – cele mai bune sunt echipate cu un filtru de frecvență.

17. <http://www.phonerated.com/top-rated-best-overall-low-sar-phones-global>



- Încurajați tinerii să reducă timpul de utilizare a telefoanelor mobile și tabletelor. Nu interziceți însă utilizarea. Utilizarea telefonului mobil și a diverselor servicii de mesagerie sunt un fenomen larg răspândit în rândul adolescenților și, în multe cercuri, aceasta este esențială pentru relaționarea cu colegii.
- Dezactivați conexiunea Bluetooth dacă nu o utilizați, pentru a evita riscurile în materie de securitate.
- Ca și în cazul emailului, acceptați date numai din partea surselor de încredere. Atenție la mesajele SMS spam: trimiteți numărul telefonului dumneavoastră mobil numai persoanelor pe care le cunoașteți bine.
- Înainte de a publica fotografii, asigurați-vă că acestea nu vor încălca drepturile legale ale altor persoane.
- Discutați cu copiii dumneavoastră despre schimbul de conținut dăunător și subliniați faptul că acesta ar putea fi contrar legislației naționale cu privire la protecția copiilor.
- Fiți atenți atunci când utilizați telefonul și tableta. Persoanele care vă înconjoară ar putea să nu fie tocmai dornice să vă asculte conversația.
- Dacă vă deranjează apelurile sau mesajele SMS nedorite, contactați operatorul dumneavoastră de telefonie mobilă sau linia dumneavoastră de asistență națională Insafe<sup>18</sup>.
- Multe telefoane mobile au o opțiune de filtrare: utilizați o listă neagră pentru a bloca numerele nedorite sau o listă albă pentru a accepta numai numerele selecționate (de exemplu, numai numerele din agenda telefonică). Puteți, de asemenea, să descărcați de pe Internet filtre de control parental (programe gratuite) sau să achiziționați unul de la operatorul dumneavoastră de telefonie mobilă.
- Rețineți faptul că telefoanele mobile nu sunt singurele dispozitive care pot fi utilizate pentru a comunica: tabletele și ceasurile inteligente au, de asemenea, funcții de mesagerie și voce.
- Pentru copiii mai mici sau adolescenți, care nu sunt deocamdată capabili să își gestioneze finanțele în mod responsabil, alegeți un plan „preplătit” în locul unui abonament lunar, pentru a evita surprizele neplăcute. Discutați despre cheltuielile lor și asigurați-vă că înțeleg valoarea reală a banilor.
- Nu uitați să configurați telefonul inteligent al copilului dumneavoastră la achiziționare. Cele mai multe dispozitive sunt dotate cu funcții complete (cameră foto, GPS, comunicare la distanță mică (NFC), Bluetooth etc.) și sunt implicit configurate pentru adulți. Nu ezitați să căutați ghiduri online despre configurarea telefonului inteligent al copilului dumneavoastră. Unii dintre pașii recomandați sunt: creați contul copilului protejat cu o parolă, dezactivați achizițiile incorporate în aplicații (achiziții in-apps) , dezactivați instalarea de aplicații noi (pentru copiii foarte mici), dezactivați geolocalizarea și utilizarea GPS și instalați programul de control parental.
- Fiți conștient de faptul că odată ce ați introdus o parolă pentru a efectua o achiziție pe un dispozitiv mobil, parola poate rămâne activă încă 15 minute, permițând efectuarea din neatenție a unei alte achiziții<sup>19</sup>.

18. [http://www.saferinternet.org/ww/en/pub/insafe/focus/national\\_helplines.htm](http://www.saferinternet.org/ww/en/pub/insafe/focus/national_helplines.htm)

19. <http://www.creditcards.com/credit-card-news/whos-responsible-kids-unauthorized-charges-1279.php>



## INFORMAȚII SUPLIMENTARE

- A GSMA report can help understand the mobile economy: [http://web.archive.org/web/20160411155639/http://www.gsmamobileeconomy.com/GSMA\\_Global\\_Mobile\\_Economy\\_Report\\_2015.pdf](http://web.archive.org/web/20160411155639/http://www.gsmamobileeconomy.com/GSMA_Global_Mobile_Economy_Report_2015.pdf).
- Un raport GSMA pentru o mai bună înțelegere a economiei mobilului: [http://web.archive.org/web/20160411155639/http://www.gsmamobileeconomy.com/GSMA\\_Global\\_Mobile\\_Economy\\_Report\\_2015.pdf](http://web.archive.org/web/20160411155639/http://www.gsmamobileeconomy.com/GSMA_Global_Mobile_Economy_Report_2015.pdf).
- Peisajul social, digital și mobil al Europei în 2014 prezentat într-o serie de infografice : <http://web.archive.org/web/20151211195326/http://wearesocial.net/blog/2014/02/social-digital-mobile-Europa-2014/>.
- S212 este un site independent din Regatul Unit pentru revizuirea telefoanelor mobile și a altor dispozitive: <http://www.s21.com/mobile-phones.htm>.
- UNESCO a publicat un raport privind viitorul învățării mobile și implicațiile acestuia pentru factorii de decizie și planificatori de politici: <http://unesdoc.unesco.org/images/0021/002196/219637E.pdf>.
- „Copiii și telefoanele mobile, agenda de acțiune” este o publicație online a Childnet International: [http://www.childnet.com/ufiles/CMPA\\_A4.pdf](http://www.childnet.com/ufiles/CMPA_A4.pdf).
- Consiliul Britanic pentru Clasificarea Filmelor a preluat de la Organul Independent de Clasificare Mobilă (OICM) rolul de stabilire a cadrului independent care stă la baza codului de practică al operatorilor de telefonie mobilă: <http://www.bbfc.co.uk/what-classification/mobile-content>.
- Aflați mai multe despre protejarea Bluetooth și modul în care funcționează: <http://web.archive.org/web/20160407133222/http://electronics.howstuffworks.com/bluetooth4.htm>.
- Operatorul de telefonie mobilă Vodafone a elaborat un ghid pentru părinți: <https://www.vodafone.com/content/parents/howto-guides.html>.

## 2. Internetul: Conectarea ideilor și a oamenilor

---

” „În cele din urmă totul se conectează – oamenii, ideile, obiectele. Calitatea conexiunilor reprezintă cheia calității propriu-zise.”

*Charles Eames, designer de la începutul secolului XX*

### LISTA DE VERIFICARE PENTRU FIȘA 6 – EMAILUL ȘI COMUNICAREA

---

Ați creat mai multe conturi de email și ați stabilit parole diferite pentru fiecare?

Parola este suficient de „puternică” (mai mult de 8 caractere, cu o combinație de litere, cifre și simboluri)?

Etichetați clar emailurile, cu cuvinte cheie relevante în câmpul „subiect”?

Ați activat securitatea pe bază de doi factori pentru conturile dumneavoastră de email (întrebare de securitate suplimentară și/sau numărul dumneavoastră de telefon mobil)?

### LISTA DE VERIFICARE PENTRU FIȘA 7 – REȚELELE DE DISCUȚII ȘI MESAGERIE

---

Ați inclus detalii de contact pe site-ul sau blogul dumneavoastră?

Ați luat măsuri pentru a vă proteja confidențialitatea în mediul online?

Ați verificat dacă conținutul pe care îl utilizați pentru site-ul/blogul dumneavoastră este în conformitate cu legea cu privire la drepturile de autor?

### LISTA DE VERIFICARE PENTRU FIȘA 8 – REȚELELE SOCIALE ȘI DISTRIBUIREA PE REȚELELE SOCIALE

---

Reputația este un lucru de care beneficiem o singură dată: întotdeauna reflectați „înainte de a posta”?

Când ați efectuat ultima actualizare a setărilor dumneavoastră de confidențialitate pe site-urile pe care le utilizați?

Democrația depinde de participarea cât mai multor cetățeni la dezbaterile publice: ați încercat să vă faceți vocea auzită prin intermediul site-urilor de socializare relevante?

### LISTA DE VERIFICARE PENTRU FIȘA 9 – VIAȚA PRIVATĂ ȘI SETĂRILE DE CONFIDENȚIALITATE

---

Este necesar să încărcați respectiva fotografie etichetată pe un site de socializare?

Ați citit acordul prevăzut de aplicația mobilă: ați înțeles ceea ce e al dumneavoastră și ceea ce „a lor” atunci când distribuiți ceva?

Atunci când instalați o aplicație, sunteți sigur că cunoașteți cu exactitate la ce informații private acesta va avea acces? Este necesar un astfel de acces pentru ca aplicația să funcționeze?

Înțelegeți ceea ce implică Regulamentul General privind Protecția Datelor al UE pentru dumneavoastră?



## Emailul și comunicarea



**E**mailul<sup>1</sup>, prescurtare pentru poșta electronică, este sistemul de trimitere de mesaje între calculatoarele conectate într-o rețea, precum Internetul. Termenul se referă și la mesajul propriu-zis. Emailul se transferă, de obicei, cu succes în câteva secunde, iar destinatarul poate accesa și răspunde oricând este în mod convenabil. Un sistem flexibil și eficient, emailul, a schimbat drastic modul în care lucrăm și comunicăm. Zilnic sunt trimise miliarde de mesaje.

— Adresa de email se compune din două părți: un nume local și de domeniu, separate de semnul „@”. Denumirea locală va indica deseori – dar nu întotdeauna – numele unui utilizator. Domeniul poate indica organizația, compania sau prestatorul de servicii Internet al utilizatorului. Numele de domenii pot indica, de asemenea, tipul de organizație și/sau țara. De exemplu, name@ox.ac.uk ar fi o persoană care lucrează sau studiază la Universitatea din Oxford.

— Deși au apărut multe alte modalități de comunicare, conturile de email reprezintă încă nucleul experienței online a unui utilizator, deoarece este adesea singura modalitate de a crea conturi pentru a participa în mediul online. Deși actualmente există alte mijloace de comunicare preferate emailurilor (rețele sociale, mesageria instant etc.), emailurile au devenit un element-cheie al identității online a utilizatorilor, servind adesea ca nume de autentificare („login”) pentru a se conecta la toate serviciile din mediul online pe care le utilizează.

1. <https://en.wikipedia.org/wiki/Email>



## IMPORTANȚA ÎN EDUCAȚIE

— Deoarece adresele de email sunt solicitate atât de des în mediul online, învățarea gestionării, în mod corespunzător, a unui cont de email are și o deosebită valoare educațională, la fel ca învățarea de a sorta scrisorile obișnuite, prin separarea conținutului personal și a conținutului administrativ important, pentru a le găsi cu ușurință.

— Emailul este, de asemenea, un instrument valoros în cadrul proiectelor interculturale dintre clasele de copii și tineri din diferite țări. Copiii și tinerii îl pot folosi pentru a-și dezvolta abilitățile lingvistice și pentru a partaja informații cu privire la propriile culturi.

— Unii dintre copiii și tinerii mai rezervați se pot exprima mai bine prin intermediul emailului decât ar face-o în cazul unei discuții față în față în sala de clasă.



## CONSIDERAȚII DE ORDIN ETIC ȘI RISCURI

- Deoarece emailul dumneavoastră este „poarta” către toate conturile dumneavoastră din mediul online, consecințele, în cazul în care o persoană vă sparge contul de email, pot fi foarte grave.
- Majoritatea clienților de poștă electronică (programe de calculator utilizate pentru a accesa și a gestiona emailul unui utilizator),<sup>2</sup> pe care le puteți găsi online, sunt gratuite, însă multe dintre acestea folosesc algoritmi pentru a scana conținutul emailurilor dumneavoastră și pentru a afișa publicitate țintită pe pagina de email.
- Exprimarea emoțiilor prin intermediul emailului este dificilă. De aceea, trebuie să scrieți întotdeauna mesajele cu atenție pentru a vă asigura că acestea nu sunt înțelese greșit. „Emoticoanele”<sup>3</sup>, mici pictograme expresive, cum ar fi fețele zâmbitoare, vă pot ajuta să vă exprimați intențiile, în special ironia sau umorul. Cu toate acestea, utilizați-le cu atenție, pentru a nu distrage atenția de la mesajul dumneavoastră.
- O mare parte a mesajelor primite prin email constituie mesaje comerciale nesolicitate și, de obicei, nedorite (spam)<sup>4</sup> (a se vedea Fișa 19 cu privire la mesajele spam, programele malware (virusii cibernetici), fraudă și securitatea). Din fericire, filtrele de spam devin din ce în ce mai performante în privința diferențierii mesajelor comerciale nesolicitate de emailurile obișnuite.
- Asigurați-vă că nu contribuiți chiar dumneavoastră la „spamming” prin redirectionarea abuzivă a emailurilor pe care le considerați „amuzante” sau „interesante” către toate contactele dumneavoastră. Dacă faceți acest lucru prea des, filtrele de spam vă pot identifica adresa de email ca indicator pentru spam și o pot introduce pe lista neagră, punându-vă în imposibilitatea de a mai contacta pe cineva.
- Unele „redirecționări” sunt false sau frauduloase. Un exemplu îl constituie emailurile care pretind, în mod fals, că o companie sau o organizație promite să plătească o sumă mică de bani pentru o cauză umanitară (adesea citând o cauză precum un copil bolnav care necesită o intervenție chirurgicală) de fiecare dată când emailul este redirecționat.
- Este ușor să ascunzi un nume pentru a induce în eroare. Acest lucru se poate face prin simpla schimbare a numelui în setări sau crearea unei adrese de email, cum ar fi elvispresley@hotmail.com. Chiar dacă recunoașteți adresa de email ca aparținând uneia dintre persoanele dumneavoastră de contact, verificați și câmpul „subiect,” deoarece este posibil ca dispozitivul proprietarului să fi devenit un „calculator zombie”<sup>5</sup> atacat de un hacker sau afectat de un virus.
- Este posibil ca un link să pară că vă direcționează spre un anumit site web, când, de fapt, acesta duce la un altul. Acest lucru este întâlnit în special în cazul escrocheriilor de tip „phishing” (înșelăciune)<sup>6</sup>.

2. [https://en.wikipedia.org/wiki/Email\\_client](https://en.wikipedia.org/wiki/Email_client)

3. [https://en.wikipedia.org/wiki/Emoticon#Basic\\_examples](https://en.wikipedia.org/wiki/Emoticon#Basic_examples)

4. [https://en.wikipedia.org/wiki/Email\\_spam](https://en.wikipedia.org/wiki/Email_spam)

5. [https://en.wikipedia.org/wiki/Zombie\\_\(computer\\_science\)](https://en.wikipedia.org/wiki/Zombie_(computer_science))

6. <https://en.wikipedia.org/wiki/Phishing>



## BUNE PRACTICI

- Creați mai multe conturi de email pentru diferite scopuri (pentru înregistrarea pe site-uri de socializare, achiziționarea de produse online etc.). Păstrați un cont cât mai privat posibil, nepublicându-l pe Internet și utilizându-l exclusiv pentru serviciile importante pe care dumneavoastră și prietenii dumneavoastră le folosiți. Utilizați unul diferit pentru a vă înscrie la servicii pe care probabil o să le utilizați o singură dată sau servicii pe care le utilizați rar.
- Scrieți mesaje email scurte și la subiect. Încercați să evitați textele lungi. Verificați ortografia.
- Asigurați-vă că includeți cuvinte relevante în câmpul pentru titlu. Acest lucru îl ajută pe destinatar să vă identifice mesajul ca fiind autentic și să găsească ulterior emailul dumneavoastră.
- Creați parole puternice pentru conturile dumneavoastră de email (mai mult de 8 caractere, combinând litere, cifre și simboluri) și pentru fiecare cont, folosiți diferite parole.
- Fiți atenți la volumul mesajelor email pe care le trimiteți și comunicați inteligent și strategic cu ceilalți. Dacă trebuie să aveți o discuție de grup cu un număr mare de persoane, poate este mai util să organizați o teleconferință sau o conversație pe un forum privat, decât să trimiteți un număr uriaș de emailuri.
- Evitați să vă verificați emailurile la fiecare 10 minute. Mulți oameni își întrerup constant activitățile pentru a verifica emailul.
- Ca regulă generală, nu includeți niciodată informații sensibile într-un email, cum ar fi datele bancare. Există situații rare în care va trebui să trimiteți astfel de informații, de exemplu, pentru a face o rezervare de hotel. Dacă aveți dubii, acționați cu atenție, verificați reputația online a serviciului pe care doriți să îl utilizați, verificați procedura de anulare a cardului dumneavoastră sau a tranzacției, utilizați servicii de plată mai sigure, cum ar fi PayPal și evitați serviciile mai puțin sigure, precum serviciile directe de transfer de bani (de exemplu, Western Union). Cu toate acestea, nu trimiteți niciodată prin email detalii cum ar fi numele dumneavoastră de utilizator și parola conturilor dumneavoastră online. Serviciile online nu vă vor cere niciodată acest lucru, așadar, dacă primiți un email care solicită astfel de detalii, aceasta este cu siguranță o tentativă de phishing.
- Strategii din ce în ce mai sofisticate de phishing constau în emailuri de notificare „false”, care emulează perfect mesajele pe care le primiți din partea serviciilor pe care le utilizați (site-uri de socializare) și care vă direcționează la un site web fals, ce vă solicită numele de utilizator și parola pentru a vă conecta. Asigurați-vă că verificați întotdeauna adresa de email a expeditorului și adresa site-ului web dacă aveți suspiciuni.
- Afișați un scepticism ferm față de emailurile pe care le primiți. Nu deschideți emailurile dacă nu aveți încredere în sursă.
- Fiți foarte atenți în cazul anexelor. Dacă nu așteptați să primiți o anexă din partea expeditorului sau nu aveți încredere în aceasta din orice alt motiv, ștergeți-o fără a o deschide. Chiar și anexele de la expeditori cunoscuți și de încredere trebuie mai întâi salvate, apoi scanate, înainte de a fi deschise.
- Utilizați toate funcțiile de securitate propuse de clientul dumneavoastră de poștă electronică. De obicei, clienții de poștă electronică vă permit să introduceți o adresă de email secundară în cazul în care contul de email este piratat și, tot mai des, clienții de poștă electronică propun să introduceți numărul de telefon mobil pentru verificări suplimentare de securitate în circumstanțe excepționale. Dacă contul dumneavoastră este compromis, configurați-vă corect setările de securitate, astfel încât să vă fie mult mai ușor să îl recuperați.
- Pentru sfaturi suplimentare referitoare la email, consultați Fișa 19 cu privire la mesajele spam, programele malware (virusii cibernetici), fraudă și securitatea.



## INSTRUCȚIUNI

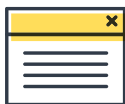
- Pentru a consulta mesajele dumneavoastră de email, puteți utiliza fie aplicația „oficială” a serviciului de email pe telefonul dumneavoastră inteligent, pe tabletă sau chiar pe calculatorul dumneavoastră care operează cu Windows 8 sau o versiune ulterioară (cum ar fi aplicația Gmail, aplicația Outlook sau aplicația Yahoo!); puteți accesa site-ul web al serviciului de email (utilizând serviciul de „webmail”) sau puteți utiliza un client de poștă electronică care este o aplicație externă ce vă descărcă mesajele de email din serviciul dumneavoastră de email și vă permite să le gestionați/organizați. Avantajul utilizării unui client de poștă electronică este acela că îl puteți configura pentru a descărca emailuri din mai multe servicii diferite de email, astfel încât să vă puteți consulta toate emailurile din diferitele adrese de email într-un singur loc. Cei mai populari clienți de poștă electronică sunt Thunderbird și Outlook. Clienții de poștă electronică sunt utilizați în majoritatea cazurilor pentru un email profesional.
- Pentru informații cu privire la configurarea unui filtru de spam, consultați Fișa 19 cu privire la mesajele spam, programele malware (virusii cibernetici), fraudă și securitatea.



## IDEI PENTRU LUCRUL ÎN CLASĂ

- În cazul elevilor mai mari, care au o adresă de email, rugați-i să se conecteze la serviciul lor de email și să ajusteze setările de securitate pentru a-și asigura contul de email, adăugând o întrebare suplimentară de securitate, un al doilea email sau un număr de telefon mobil.
- Iată procedurile de urmat pentru a vă asigura contul de email pe Gmail, Yahoo! și Outlook.
  - ▶ <<https://support.google.com/accounts/answer/46526?hl=en>>
  - ▶ <<http://windows.microsoft.com/en-us/windows/outlook-security>>
  - ▶ <<https://help.yahoo.com/kb/SLN8292.html>>
- Există mulți furnizori de email pe piață, pe lângă cei trei „giganți” menționați. De ce insistăm pe cei trei? Deoarece, cel puțin în cazul Gmail și Outlook/Hotmail, aceștia sunt conectați la multe alte servicii. De exemplu, un cont „Google” este aproape o necesitate atunci când dețineți un telefon inteligent cu Android, iar un cont Outlook este adesea conectat la sistemul dumneavoastră de operare Windows. Aceasta înseamnă că, indiferent de preferințele dumneavoastră, s-ar putea să fiți „obligat” să creați un cont de email la unul dintre serviciile menționate anterior. Dar, desigur, aveți libertatea de a utiliza clienți de poștă electronică cu standarde de confidențialitate mai stricte, cum ar fi Web.de sau Protonmail.com. Chiar și prestatorul dumneavoastră de servicii Internet oferă, de obicei, un serviciu de email. Puteți să căutați și alte alternative online.
- Grupați elevii în echipe a câte trei sau mai mulți și rugați-i să creeze parole solide pentru un cont de email imaginar. Explicați-le foarte clar că nu trebuie să își divulge parola reală! După un schimb de idei (brainstorming) de 10 minute, solicitați fiecărei echipe să își prezinte parola propusă și să explice de ce consideră că aceasta este una sigură. Ajutați-i să identifice caracteristicile unei parole puternice (mai mult de 8 caractere, combinând litere, cifre și caractere simbol) și capcanele obișnuite ale parolelor slabe (pot fi găsite într-un dicționar, sunt asociate utilizatorului într-un anumit fel – numele câinelui, numele de familie etc.).





## INFORMAȚII SUPLIMENTARE

- Exemple bine-cunoscute de clienți de poștă electronică sunt Microsoft Outlook <<https://products.office.com/en-us/outlook/email-and-calendar-software-microsoft-outlook>> sau Mozilla Thunderbird <<http://www.mozilla.org/projects/thunderbird/>>.
- Truth or Fiction este un site web pentru utilizatorii de Internet pentru a verifica veridicitatea celor mai des expediate emailuri <<http://www.truthorfiction.com/>>. Un alt site similar este <<http://m.snopes.com/whats-new/>>.
- Trei dintre cele mai populare site-uri de webmail sunt Outlook <<https://office.live.com/start/Outlook.aspx>>, Yahoo! <<https://mail.yahoo.com>> și Google Gmail <<http://www.gmail.com>>. Puteți căuta furnizori alternativi de email, în special în țara dumneavoastră.

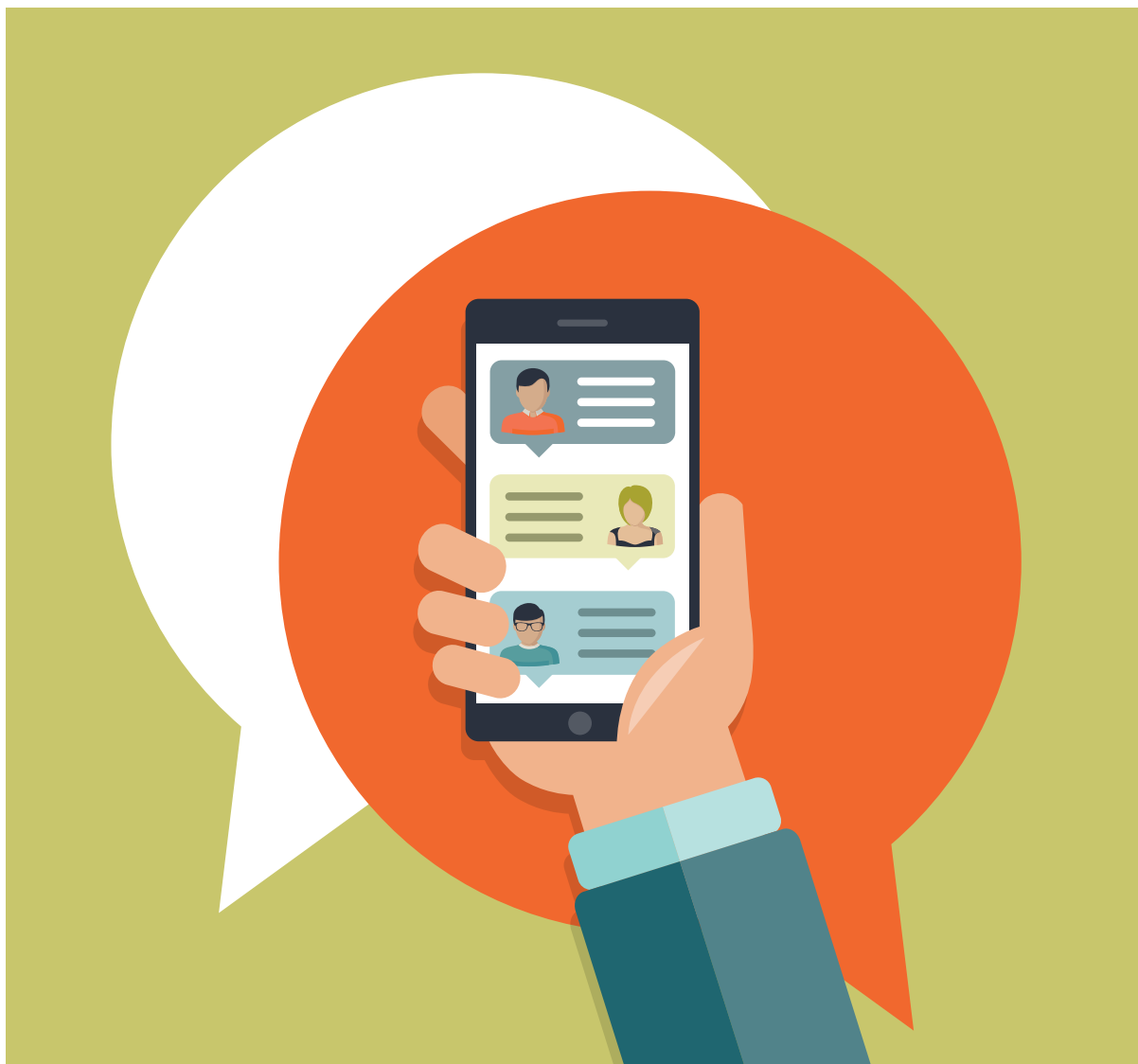
- Articole relevante din Convenția ONU cu privire la drepturile copilului:

**Articolul 13** – Copiii au dreptul de a obține și difuza informații, cu excepția cazului când acest fapt ar leza drepturile altora.

**Articolul 16** – Copiii au dreptul la viață personală. Copilul are dreptul la protecția legii contra unor atacuri asupra vieții lor personale, reputației, familiei și domiciliului



## Rețelele de discuții și mesagerie



— „Chat” (discuție) este un termen generic, ce se referă la comunicarea interactivă care se desfășoară pe un canal conceput pentru discuții. Utilizatorii pot conversa cu grupuri de persoane în camerele de chat (chatroom)<sup>1</sup> sau pot organiza conversații private cu prietenii selectați utilizând serviciile de mesagerie instantanee<sup>2</sup>.

— Chatul este un mijloc informal de comunicare, similar conversațiilor față în față și are loc între două sau mai multe persoane. Discuțiile chat se realizează, de obicei, prin tastare, dar pot include și transmisiuni video sau audio<sup>3</sup> cu utilizarea căștilor sau a camerelor web. Această formă de comunicare este instantanee și, prin urmare, diferită de email, care nu presupune prezența destinatarului în același timp cu expeditorul.

### Chatting-ul vs. mesageria instantanee

— Termenii sunt sinonimi; totuși, un utilizator poate discuta prin chat în timp ce utilizează serviciile de mesagerie instantanee, dar trimiterea unui mesaj instant (MI) nu este considerată un chat.

1. [https://simple.wikipedia.org/wiki/Chat\\_room](https://simple.wikipedia.org/wiki/Chat_room)  
2. [https://en.wikipedia.org/wiki/Instant\\_messaging](https://en.wikipedia.org/wiki/Instant_messaging)  
3. [https://en.wikipedia.org/wiki/Streaming\\_media](https://en.wikipedia.org/wiki/Streaming_media)

Discuțiile chat erau destul de populare, dar se pare că acestea își pierd poziția în favoarea mesageriei instantanee și a altor tipuri de rețele de mesagerie. Multe companii nu sunt de acord cu MI la locul de muncă, deoarece dacă angajații sunt întreruși în mod constant de mesaje în timpul îndeplinirii sarcinilor, productivitatea lor scade.

### Care sunt celelalte tipuri de rețele de mesagerie?

— Aplicațiile de mesagerie, cum ar fi WhatsApp, Kik, Viber, Telegram sau iMessage, sunt din ce în ce mai utilizate de posesorii de telefoane inteligente. Aplicațiile cu funcție de autodistrugere, cum ar fi Snapchat și Wickr, sunt de asemenea populare printre posesorii de telefoane inteligente. De fapt, aceste tipuri de rețele de mesagerie sunt gratuite și se pare că oferă mai multă „confidențialitate” decât tipurile de mesagerie care sunt disponibile pe platformele mai mari, cum ar fi Facebook, Twitter sau LinkedIn.

— Disponibilitatea rapidă a acestor aplicații de mesagerie pe telefoanele inteligente înseamnă adesea că utilizatorii filmează, comentează, fac fotografii și le trimit înainte de a se gândi la consecințe. De aceea, acestea au fost citate, din păcate, ca având un rol important în ceea ce privește intensificarea hărțuirii și a intimidării în mediul online.

— Evoluția mesageriei instantanee și a altor tipuri de rețele de mesagerie va continua, fără îndoială, pe măsură ce telefoanele inteligente pătrund pe piețe noi. Facebook a achiziționat compania WhatsApp, compania japoneză Rakuten a achiziționat Viber, iar alți actori au investit bani în multe dintre celelalte aplicații de mesagerie. Mesajul este foarte clar: rețelele de mesagerie vor mai rămâne ceva timp în preajmă.

### Importanța înțelegerii chat-ului și a mesageriei instantanee

— Chat-ul și mesageria instantanee sunt distracții populare și transformă modul în care tinerii comunică între ei. Chatting-ul și mesageria instantanee sunt folosite în mod util, deoarece elevii fac schimb de idei și discută despre teme și alte proiecte academice, dar din nefericire, acestea sunt utilizate și pentru a intimida și a hărțui alte persoane în mediul online (a se vedea Fișa 21 cu privire la bullying și hărțuire).

— Cadrele didactice subestimează adesea importanța chatului pentru tineri și pot pierde ocazia de a valorifica această forță și de a o aplica ca instrument educațional. Unele idei de utilizare includ:

- sesiuni de schimb de idei (brainstorming) și discuții în timp real bazate pe probleme
- jocuri de rol și simulări
- schimbul de opinii și dezbateri și discuții în grupuri mici
- îndrumare și orientare
- cercetare în grup
- crearea unei comunități online



### CONSIDERAȚII DE ORDIN ETIC ȘI RISCURI

- Atunci când chatul se bazează pe text, semnalele sociale, gesturile și comunicarea non-verbală nu pot fi transmise prin taste, iar neînțelegerile pot apărea cu ușurință în mediul online. Persoanele trebuie să fie la fel de agreabile, politicoase și bine manierate ca și în situațiile din viața reală și să își facă obiceiul de a folosi o bună netichetă<sup>4</sup>. Umorele și emoțiile pot fi, de asemenea, prezentate prin utilizarea emoticoanelor<sup>5</sup>, mici simboluri care arată ca niște fețe scrise lateral. Majoritatea tinerilor utilizează abrevieri sau acronime; cele mai frecvente au fost incluse într-un dicționar și pot fi accesate aici: <<http://www.netlin-go.com/acronyms.php>>.
- Atunci când discutați cu necunoscuți pe Internet, este, de asemenea, important să rețineți faptul că oamenii nu sunt întotdeauna ceea ce pretind a fi. Chaturile pentru grupuri închise<sup>6</sup>,

4. [https://en.wikipedia.org/wiki/Etiquette\\_in\\_technology#Netiquette](https://en.wikipedia.org/wiki/Etiquette_in_technology#Netiquette)

5. <https://en.wikipedia.org/wiki/Emoticon>

6. [https://en.wikipedia.org/wiki/Collaborative\\_software](https://en.wikipedia.org/wiki/Collaborative_software)

care oferă posibilități de conferință pentru utilizarea în școli sau sălile de clasă, sunt mai sigure de utilizat, deoarece accesul este limitat la un grup definit de utilizatori.

- Timpul petrecut în discuții chat sau expedierea de mesaje instant a crescut în mod considerabil, adolescenții trimițând zilnic sute de mesaje sub diferite forme (texte, mesaje instant, chat-uri, emailuri etc.). În timp ce ergonomia tastaturii calculatoarelor și mouse-urile calculatoarelor s-au îmbunătățit în mod considerabil, adolescenții care petrec mult timp în fața tastierei, se confruntă cu noi sindroame, cum ar fi tendinita. Telefoanele inteligente sunt dispozitive relativ recente, iar trimiterea de mesaje sau tastarea de emailuri lungi poate avea ca rezultat suprautilizarea degetelor mari. Prin urmare, limitarea discuțiilor chat și a mesajelor text nu reprezintă doar o chestiune de echilibru în viața de zi cu zi, ci și o problemă de sănătate.
- Deși multe aplicații IM par să fie „gratuite”, rețineți întotdeauna că o companie trebuie să își acopere, într-un fel sau altul, costurile de operare. Multe aplicații optează pentru strategia „construiește și vinde”, atrăgând utilizatorii cu o aplicație „gratuită”, după care vând baza de utilizatori către o altă companie imediat ce aceasta este suficient de mare. Acesta a fost cazul și cazul Whatsapp, care a fost cumpărat de Facebook. Alte aplicații, cum ar fi Snapchat, își construiesc mai întâi baza de utilizatori și apoi încep să introducă publicitate. Fiți întotdeauna conștienți de modelul de business al serviciului de mesagerie pe care îl utilizați și alegeți cu înțelepciune, luând în considerare compromisurile (viață privată mai puțin protejată, control asupra datelor, expunerea la publicitate, taxă anuală/lunară etc.).
- Oamenii fac adesea schimb de fișiere prin intermediul mesageriei și prin chat și este important să rețineți faptul că fișierele pot conține programe malware. Asigurați-vă că toate fișierele sunt scanate de viruși înainte de a fi distribuite și, după recepționare, înainte de a le deschide (a se vedea Fișa 19 cu privire la securitate).
- A existat multă publicitate negativă cu privire la riscurile cu care tinerii se pot confrunta atunci când folosesc camerele de discuții. Din cauza mai multor cauze penale intens mediatizate, părinții și cadrele didactice sunt adesea îngrijorați că copiii ar putea să intre în contact cu pedofili în camerele de discuții, în special prin intermediul jocurilor online (a se vedea Fișa 16 cu privire la jocuri). Deși aceste pericole există, este important să păstrăm o perspectivă echilibrată în ceea ce privește aceste temeri. Marea majoritate a utilizatorilor camerelor de discuții sunt persoanele care afirmă cine sunt în realitate, iar cea mai mare parte a comunicărilor prin chat este absolut inocentă. Decât să inducă frici sau să interzică utilizarea chatului, adulții ar trebui să responsabilizeze tinerii, învățându-i cum să rămână în siguranță. Iată câteva reguli de bază pe care copiii și tinerii trebuie să le urmeze:
  - ▶ Alegeți o cameră de discuții potrivită pentru grupul dumneavoastră de vârstă și cu un moderator live și raportați orice incident negativ moderatorului.
  - ▶ Utilizați un nume de utilizator neutru din punctul de vedere al genului și nu oferiți niciodată informațiile dumneavoastră personale sau nu postați fotografii cu dumneavoastră (a se vedea Fișa 9 cu privire la viața privată).
  - ▶ Dacă într-adevăr vă veți întâlni cu un prieten din camera de discuții, discutați acest lucru mai întâi cu părinții dumneavoastră și luați cu dumneavoastră un adult de încredere. La prima întrevvedere reală cu o persoană pe care ați cunoscut-o în mediul online, întotdeauna optați pentru un loc public, cum ar fi scuarul din oraș.
  - ▶ Comunicați adulților dacă anumite lucruri cu care v-ați confruntat într-o sesiune de discuții vă fac să vă simțiți incomod. Dacă întâmpinați orice fel de probleme într-o cameră de discuții sau oriunde altundeva pe Internet, puteți discuta întotdeauna acest lucru cu consultanți cu experiență, la linia națională de asistență<sup>7</sup>.
  - ▶ Dacă doriți să discutați cu persoane pe care le cunoașteți, optați pentru mesageria instantanee (de exemplu, MSN, Skype) în locul camerei de discuții, pentru a putea controla lista de contacte.

7. [www.betterinternetforkids.eu/web/portal/practice/helplines](http://www.betterinternetforkids.eu/web/portal/practice/helplines)



## INSTRUCȚIUNI

- Există multe tipuri de programe gratuite de discuții disponibile pe Internet. Puteți găsi o gamă largă introducând cuvântul „discuții” în orice motor de căutare<sup>8</sup>. Multe programe de discuții bazate pe web, cum ar fi Yahoo Chat<sup>9</sup>, ICQ<sup>10</sup> și AOL Chat<sup>11</sup> oferă o mare varietate de camere de discuții cu grupuri de discuții în timp real. De obicei, utilizatorii trebuie să descarce mai întâi o mică aplicație pentru a valida chatul și să se înregistreze la moderator, dar apoi pot să se autentifice și să participe liber la conversație.
- Aplicațiile de mesagerie instantanee<sup>12</sup>, care permit conversații private cu utilizatori selectați, depășesc acum în popularitate camerele de discuții. Aceste capacități pot fi găsite căutând „mesagerie instantanee” în orice motor de căutare. Utilizatorii descarcă o aplicație pentru a activa mesageria instantanee și apoi compilează o listă de persoane cu care doresc să discute. Deoarece comunicarea se desfășoară în cadrul unui grup restricționat de utilizatori, mesageria instantanee este adesea considerată „mai sigură” decât schimbul de păreri din camerele de discuții.

### Cum se utilizează o cameră de discuții?

- Deschideți programul de discuții pe care ați ales să îl utilizați.
- Dacă este necesar, furnizați un nume de utilizator și o parolă.
- Alegeți o cameră de discuții potrivită, moderată de persoane. De obicei, există camere pentru diferite scopuri și subiecte, de exemplu, grupuri de interese legate de automobile, grupuri de studiu privind o anumită temă, discuții pentru cadrele didactice și așa mai departe.
- După autentificare, veți vedea conversația participanților derulând pe afișajul text principal.
- Introduceți mesajul dumneavoastră și apăsați „enter” sau dați clic pe „trimite” pentru a-l posta, astfel încât participanții să îl poată vedea.
- Dacă doriți să trimiteți un mesaj unei anumite persoane, selectați o persoană din lista participanților din fereastră.
- Multe camere de discuții pot fi, de asemenea, utilizate pentru schimb de fișiere de la egal la egal (*peer-to-peer*)<sup>13</sup>. Camerele de discuții permit schimbul de fișiere care sunt prea mari pentru a fi trimise prin email<sup>14</sup>.
- Verificați-vă întotdeauna setările astfel încât să nu adăugați, accidental, utilizatori nedorți în camera dumneavoastră de discuții.

### Cum se utilizează mesageria instantanee?

- Deschideți aplicația dumneavoastră de mesagerie instantanee<sup>15</sup>.
- Verificați-vă lista de contacte pentru a afla cine este online și disponibil pentru discuții.
- Puteți adăuga persoane de contact noi introducând adresa de email a acestora și invitându-le să se alăture grupului dumneavoastră de contacte. Aceștia vor primi o invitație prin email și, dacă sunt de acord, vor fi înregistrați în lista dumneavoastră. Acest lucru vă va permite să discutați cu ei în timp real atunci când sunteți online în același timp.
- Dați clic pe ID-ul persoanei selectate pentru a trimite un mesaj și a deschide un dialog pentru comunicare.
- Introduceți mesajul dumneavoastră și apăsați „enter” sau dați clic pe „trimite” pentru a-l posta, astfel încât participanții să îl poată vedea.
- Cel mai bine este să nu participați la conversații cu utilizatori necunoscuți sau să răspundeți la emailul sau MI al persoanelor pe care nu le cunoașteți.
- Verificați-vă întotdeauna setările pentru a nu adăuga, în mod accidental, utilizatorii nedorți la MI al dumneavoastră.

8. [https://en.wikipedia.org/wiki/Web\\_search\\_engine](https://en.wikipedia.org/wiki/Web_search_engine)

9. <http://chat.yahoo.com>

10. <http://www.icq.com/>

11. <http://lifestream.aol.com>

12. [https://en.wikipedia.org/wiki/Instant\\_messaging](https://en.wikipedia.org/wiki/Instant_messaging)

13. <https://en.wikipedia.org/wiki/Peer-to-peer>

14. <https://en.wikipedia.org/wiki/Email>

15. [https://en.wikipedia.org/wiki/Instant\\_messaging](https://en.wikipedia.org/wiki/Instant_messaging)



## IDEI PENTRU LUCRUL ÎN CLASĂ

- Alegeți un subiect și rugați elevii să adreseze întrebări unii altora și să facă schimb de informații într-un cadru de discuții.
- Decideți asupra unui subiect de studiu. Adunați niște materiale de ghidare pentru a ajuta elevii să realizeze activități de pregătire pentru lecție. Solicitați elevilor să lucreze la sarcinile stabilite în perechi sau în grupuri mici. Această fază de lucru trebuie organizată în conformitate cu modelul unui grup de studiu (discuțiile merg cel mai bine în cazul interacțiunilor din cadrul grupurilor mici, de 2-6 elevi).
- La sfârșitul proiectului, elevii pregătesc prezentări potrivite pentru o sesiune de discuții. Discuția începe cu prezentările grupurilor mici pe diferite subiecte de studiu. Elevii fac concluzii privitor la ceea ce au învățat pe parcursul cursului.
- Deoarece sesiunile de discuții modelează conversațiile din viața reală, acestea oferă elevilor oportunități de interacțiune autentică și, prin urmare, sunt utile în studierea limbilor străine. Profesorul poate încuraja elevii să participe la discuție, sfătuindu-i să posteze mesaje scurte. Interacțiunea poate fi îmbunătățită prin crearea de roluri pentru elevi: unul poate fi un inovator, altul un critic. Ceilalți elevi pot urmări discuțiile și, ulterior, pot oferi feedback.
- Environment Online (ENO)<sup>16</sup> este un proiect internațional de educație ecologică bazat pe web. La începutul cursului, elevii își iau subiectele de pe paginile web ale proiectului. Elevii colectează date științifice și empirice despre mediu, evaluează diferite fenomene sau realizează fotografii.
- În timpul fiecărei sesiuni tematice, lecțiile virtuale capătă forma unei discuții interactive și sincrone în timp real<sup>17</sup>, a unor chestionare electronice și forumuri<sup>18</sup>. Înainte și după activitățile desfășurate în timpul lecției, elevii fac schimb de idei, își monitorizează sarcinile prin chat și reflectează asupra celor studiate.



## BUNE PRACTICI

— Limbajul folosit în chatting este segmentat, asociativ și colocvial; un participant la discuție trebuie să fie nu numai rapid, dar și suficient de flexibil pentru a trece de la un subiect la altul și chiar de la o discuție la alta. Rolul profesorului este esențial în promovarea și asigurarea calității conținutului și a participării echilibrate a tuturor celor care contribuie la chat. Cu cât vârsta elevilor este mai mică, cu atât este mai important ca discuțiile să fie găzduite și moderate de către profesor.

- Urmăriți activ discuția pe parcursul întregii sesiuni de chatting.
- Conveniți anticipat asupra programului ședinței: toate persoanele trebuie să fie prezente în același timp.
- Respectați regulile netichetei: fiți politicoși, amabili și respectuoși, de parcă ați fi față în față.
- Nu uitați că un mesaj scris nehibzuit poate răni, chiar dacă nu aceasta a fost intenția dumneavoastră.
- Mesajul scurt funcționează cel mai bine. Nu monopolizați o sesiune de discuții în timp real, lipind bucăți de text pre-scris, pe care ceilalți sunt obligați să le citească și la care trebuie să reacționeze.
- Stilul de discuții este apropiat de stilul fluxului conștiinței. Citiți cu atenție mesajele altora pentru a înțelege ce vor să comunice. Aceasta poate implica și cititul printre rânduri.
- Nici când nu distribuiți numele de utilizator și parola. Păstrați confidențialitatea informațiilor personale în timpul discuțiilor chat sau a transmiterii mesajelor instant. Întotdeauna se pot realiza capturi de ecran ce conțin informațiile (sau comentariile) dumneavoastră, care pot fi apoi distribuite altor persoane.

16. <http://www.enoprogramme.org>

17. <http://www.netlingo.com/word/real-time-chat.php>

18. [https://en.wikipedia.org/wiki/Internet\\_forum](https://en.wikipedia.org/wiki/Internet_forum)



## INFORMAȚII SUPLIMENTARE

- Unele idei pentru cadrele didactice școlare se găsesc la adresa: [http://www.educationworld.com/a\\_tech/chat-room-get-new-life-in-classrooms.shtml](http://www.educationworld.com/a_tech/chat-room-get-new-life-in-classrooms.shtml).
- tChat este o cameră de discuții în limba franceză: <http://www.tchat-orange.fr/index.php>.
- Informații cu privire la „Discuțiile din camere ca instrument social” se găsesc la adresa: <http://www.openp2p.com/lpt/a/3071>.
- Pentru o listă cu emoticoanele de bază, a se vedea Wikipedia: [https://en.wikipedia.org/wiki/Emoticon#Basic\\_examples](https://en.wikipedia.org/wiki/Emoticon#Basic_examples).
- Centrul de Cercetare Pew a studiat mesageria mobilă și rețelele sociale: <http://web.archive.org/web/20160703022409/http://www.pewinternet.org/2015/08/19/mobile-messaging-and-social-media-2015/>.
- „Ce este snapchat și de ce copiii îl adoră și părinții se tem de el?": <http://web.archive.org/web/20160619055301/http://www.forbes.com/sites/larrymagid/2013/05/01/what-is-snapchat-and-why-do-kids-love-it-and-parents-fear-it/#65fc2b447875>.
- În Danemarca, Cyberhus utilizează „discuțiile de grup” ca pe o platformă valoroasă pentru a contribui la sporirea bunăstării adolescenților vulnerabili și pentru a încuraja creșterea participării acestora în societate: <http://cfdp.dk/2015-cyberhus-chat-counselling-last-year/>.



## Fișa 8

# Socializarea online și distribuirea pe rețelele sociale



**U**n serviciu de rețea socială sau un site de socializare (SNS)<sup>1</sup> este o platformă utilizată pentru a crea rețele sociale în rândul persoanelor care împărtășesc interese sau activități similare. Acest sistem bazat pe web oferă utilizatorilor o multitudine de modalități de interacțiune, cum ar fi chatul, mesageria, emailul, videoul, chatul vocal, partajarea de fișiere, bloggingul, grupurile de discuții și așa mai departe.

— Rețelele sociale se bazează pe profiluri personale care conțin date personale importante, interese, o rețea de prieteni și altele aspecte similare. Site-urile de socializare reunesc comunități de persoane care împărtășesc interese și activități sau care sunt interesate să exploreze interesele și activitățile altora. Acestea oferă diferite tipuri de programe<sup>2</sup> pentru ca utilizatorii să realizeze acest scop.

— Site-urile de socializare permit persoanelor să se conecteze (de obicei, prin pagini pe care fiecare membru al rețelei se prezintă) și să ofere sisteme de recomandare bazate pe încredere pentru a conecta utilizatorii. Unele site-uri conțin directoare de categorii specifice de utilizatori (cum ar fi foști colegi de clasă).

1. [https://en.wikipedia.org/wiki/Social\\_networking\\_service](https://en.wikipedia.org/wiki/Social_networking_service)

2. [https://en.wikipedia.org/wiki/Social\\_software](https://en.wikipedia.org/wiki/Social_software)

■ Partajarea socială permite utilizatorilor să distribuie conținutul de pe un site web pe un site sau pe o aplicație de socializare.<sup>3</sup>

■ Site-urile și aplicațiile globale populare de socializare includ: Twitter, Facebook, LinkedIn, Google+, Snapchat, Tumblr, Pinterest, Vine și Whatsapp.

■ Site-urile și aplicațiile europene includ: Badoo, Bebo, Vkontakte sau VK (Rusia), Delphi, Draugiem.lv (Letonia), iWiW (Ungaria), Nasza-Klasa (Polonia), Soup (Austria), Glocals în Elveția, Skyrock, The Sphere, StudiVZ (Germania), Tagged, Tuenti (în principal în Spania) și multe altele.

■ Rețelele sociale sunt la fel de importante pentru schimburile privind drepturile omului și libertățile fundamentale și pot oferi informații relevante publicului larg.

■ Majoritatea rețelelor sociale sunt organizate în jurul experiențelor de viață, dar există și alte comunități:

- comunități de tranzacții, care facilitează cumpărarea și vânzarea, închirierea de proprietăți sau camere etc.;
- comunitățile de interes care sunt, în mod obișnuit, centrate pe un anumit subiect, cum ar fi filmele, sănătatea etc.;
- comunitățile de fantasy, care sunt bazate pe lumi imaginare și joc, cum ar fi „World of Warcraft” și „Second life”;
- comunitățile de apărare a drepturilor omului și/sau de activism centrate pe problemele care afectează utilizatorii;
- comunitățile de sprijin și consiliere cu privire la dizabilități, nevoi speciale sau alte provocări.

■ Cele mai multe rețele sociale oferă, de asemenea, funcții simple pentru gestionarea confidențialității datelor personale (a se vedea Fișa 9 cu privire la setările de confidențialitate). Aceste instrumente permit utilizatorilor să restricționeze accesul la anumite părți ale profilului lor doar pentru prieteni sau numai pentru membrii cu anumite autorizări. De asemenea, acestea permit membrilor să restricționeze accesul prin căutări aleatorii și disponibilitatea conținutului acestora de a fi etichetat de către alți membri.



## IMPORTANȚA ÎN EDUCAȚIE

- Rețelele sociale și partajarea socială sunt metode ieftine și rapide de partajare de conținut, de la informații personale la informații de marketing.
- Socializarea pe rețelele sociale permite persoanelor să păstreze contactul și să restabilească legătura cu familia și prietenii care trăiesc la distanță sau cu care au pierdut contactul.
- Site-urile de socializare permit, de asemenea, organizarea de evenimente. Unele evenimente pot fi obișnuite, așa precum un spectacol de bijuterii sau o petrecere pentru copii, în timp ce altele pot fi ofensatoare, cum ar fi o petrecere rave sau o demonstrație pentru o cauză rasistă/xenofobă/homofobă sau de altă natură extremă și denigratoare.
- Multe industrii recunosc importanța rețelelor sociale în promovarea mărcilor (branding) și urmăresc să obțină recomandări (și eventuale vânzări) prin intermediul rețelelor sociale.
- Din cauza ușurinței partajării pe rețelele sociale prin intermediul site-urilor web și al aplicațiilor de pe telefoanele inteligente, mulți tineri distribuie orice și totul fără prea multă analiză.
- Socializarea responsabilă pe rețelele sociale este crucială, deoarece potențialii angajatori, liceele/colegiile sau universitățile, sau chiar familia și prietenii, pot avea acces la aceste informații.
- Socializarea responsabilă pe rețelele sociale poate fi văzută ca o modalitate ieftină de auto-promovare (de exemplu, un tânăr care inițiază o campanie pentru un serviciu comunitar), de creare a unui conținut viral pentru binele comun sau chiar de a fi recunoscut (când o persoană tânără publică informații despre un premiu sau certificat obținut recent).
- Site-urile de socializare pot fi utilizate pentru a promova informații care sunt false sau bazate pe prejudecăți, iată de ce utilizatorii trebuie să fie precauți în alegerea „prietenilor” și să verifice dacă un anumit conținut este de încredere.

3. [www.oxforddictionaries.com/definition/english/social-sharing](http://www.oxforddictionaries.com/definition/english/social-sharing)



## CONSIDERAȚII DE ORDIN ETIC ȘI RISCURI

— De multe ori, oamenii vorbesc despre pierderea inhibițiilor personale atunci când folosesc site-urile de socializare. Aceștia se simt împuterniciți și uneori invincibili, făcând comentarii și spunând altora lucruri pe care nu le-ar spune, în mod normal, într-o conversație față în față. Acest lucru este în continuare exacerbat de faptul că este foarte ușor să hiperbolizăm emoțiile în lumea virtuală sau să spunem lucruri pe care nu le-am exprima dacă am comunica față în față cu cineva.

— Site-urile de socializare permit utilizatorilor să facă comentarii pe profilurile altor persoane. Este necesar să se acorde atenție tipului și naturii acestor comentarii.

— După cum menționează Get Safe Online din Regatul Unit<sup>4</sup>, unele riscuri asociate utilizării site-urilor de socializare includ:

- divulgarea informațiilor personale fie de dumneavoastră, fie de către prieteni/persoane de contact;
- bullying-ul;
- hărțuirea/urmărirea online;
- accesul la conținut nepotrivit vârstei;
- ademenirea online și abuzul asupra copiilor;
- confruntarea cu comentarii de natură violentă, sexuală, extremistă sau rasistă, sau activități ofensatoare și atitudini pline de ură;
- persoane care încearcă să vă hărțuiască sau să vă convingă să vă schimbați convingerile sau ideile fundamentale ori să adoptați o poziție extremistă;
- urmărirea penală sau incriminarea postării unor comentarii ofensive sau necorespunzătoare;
- emailurile de phishing, aparent trimise din partea unor site-uri de socializare, dar care vă încurajează, de fapt, să vizitați site-uri web frauduloase sau nepotrivite;
- postările prietenilor, ale altor persoane și ale companiilor care vă încurajează să vă conectați la site-uri web frauduloase sau nepotrivite;
- persoane care vă piratează sau vă fură contul sau pagina;
- viruși sau programe spion (spyware) conținute în anexe sau fotografii;
- dumneavoastră sau un membru al familiei care postează că nu sunteți acasă sau plecați în vacanță și, prin urmare, anunțați că casa dumneavoastră este goală, lăsând calea deschisă hoților; dacă faceți acest lucru și ulterior solicitați o creanță de asigurare pentru un furt comis în timp ce erați plecat de acasă, compania dumneavoastră de asigurări ar putea să o respingă din acest motiv<sup>5</sup>.

— Dar există și alte riscuri, cum ar fi:

- expunerea la conținut comercial și exploatarea datelor dumneavoastră private în scopuri comerciale;
- prejudicierea permanentă a reputației dumneavoastră în mediul online, fapt ce poate implica dificultăți în găsirea unui loc de muncă sau diferite alte tipuri de discriminare, cum ar fi excluderea financiară (incapacitatea de a obține un împrumut sau o asigurare etc.);
- expunerea la un conținut părtinitor, în conformitate cu convingerile/cunoștințele/opiniile dumneavoastră, care pot limita creșterea și evoluția personală;
- expunerea la presiuni sociale extreme de a arăta perfect, a avea o viață interesantă și fericită și de a posta în mod continuu lucruri impresionante/grozave.

— Ca și în cazul tuturor tehnologiilor online, soluția nu este de a interzice tinerilor să utilizeze rețelele sociale. Tinerii trebuie să fie responsabilizați să aibă un comportament sigur, bazat pe discernământ atunci când sunt în mediul online și încurajați să respecte rigorile legate de vârstă, să nu divulge informațiile personale și să fie responsabili când publică un anumit conținut.

4. <https://www.getsafeonline.org/social-networking/social-networking-sites/>

5. [www.getsafeonline.org/social-networking/social-networking-sites/](http://www.getsafeonline.org/social-networking/social-networking-sites/)

— Adulții responsabili ar trebui mai degrabă să se informeze despre pericolele și bunele practici cu privire la utilizarea în condiții de siguranță a site-urilor de socializare, decât să încerce a împiedica utilizarea acestora. Toate aceste lucruri se fac, firește, în mediul offline – și atunci, de ce nu și în mediul online?

— Tinerii trebuie încurajați să vorbească despre experiențele lor în mediul online cu adulți de încredere, cum ar fi părinții și cadrele didactice. Ca și în cazul tuturor aspectelor privind siguranța Internetului, implicarea activă a părinților și a cadrelor didactice în viața online a tinerilor va avea un impact pozitiv palpabil asupra comportamentului acestora în mediul online.

— Acest lucru are un efect benefic și asupra adulților, deoarece aceștia învață despre laturile pozitive ale site-urilor de socializare.



## IDEI PENTRU LUCRUL ÎN CLASĂ

- Rugați elevii să se gândească la informațiile pe care le consideră acceptabile a fi publicate într-un profil din mediul online. După elaborarea unei liste, cereți-le să creeze un profil pe hârtie. Ar fi ei de-acord ca acest profil să fie trimis acasă, tuturor părinților care au elevi în școală? În majoritatea cazurilor, elevii nu ar vrea ca acest lucru să se întâmple, dar ar trebui să li se reamintească faptul că oricine poate să le vizualizeze profilul pe un site de socializare, cu excepția cazului când acesta este setat ca profil privat. Realizarea acestei legături între lumea reală și lumea virtuală este importantă, deoarece ajută copiii și tinerii să înțeleagă implicațiile postării în mediul online.
- Accesați în clasă două sau trei site-uri de socializare și solicitați elevilor să evidențieze orice comportament riscant pe care îl observă. Discutați care sunt riscurile ce amenință utilizatorii. Acum rugați elevii dumneavoastră să revizuiască propriile activități din mediul online, în lumina elementelor pe care tocmai le-au identificat.
- Divizați elevii pe grupuri pentru ca ei să creeze propriile liste de verificare cu aspectele care trebuie urmărite atunci când publică materiale în mediul online pe un site de socializare. Comparați listele și combinați-le pentru a crea o singură listă de verificare pentru toată clasa, pe care elevii să o poată imprima și lua acasă, pentru a o lipi pe peretele de lângă calculatorul lor.
- Solicitați elevilor să aducă fotografii digitale pe care ar dori să le încarce pe un site de socializare. Lucrând în grupuri mici, analizați împreună fiecare fotografie pentru a vedea ce informații private sunt dezvăluite. Acordați fiecărei fotografii un „rating de siguranță” pe o scară de la 1 la 5, atribuind 5 oricărei fotografii care protejează perfect confidențialitatea utilizatorului.
- Pentru mai multe sugestii despre utilizarea acestor tehnologii de socializare în clasă, consultați secțiunea Web 2.0, 3.0 și alte versiuni (Fișa 3).
- Pregătiți material ajustat pentru copiii sau elevii dumneavoastră pentru a iniția o discuție cu privire la ceea ce constituie un conținut extremist și la modul în care acesta poate avea impact asupra comportamentului. Lucrați cu ei pentru a descoperi idei despre cum să contracareze extremismul. Planul de acțiune al Consiliului Europei privind lupta împotriva extremismului violent și a radicalizării va fi util pentru a informa elevii și a declanșa idei noi<sup>6</sup>.
- Consultați Regulamentul General privind Protecția Datelor cu elevii dumneavoastră și discutați de ce Uniunea Europeană ar putea dori să impună o anumită limită de vârstă sub care nu va fi permis accesul copiilor la rețelele de socializare.<sup>7</sup> Ce limită de vârstă ar trebui să fie stabilită?

6. [https://search.coe.int/cm/Pages/result\\_details.aspx?ObjectID=09000016805c3576](https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805c3576)

7. [http://ec.europa.eu/justice/data-protection/document/factsheets\\_2016/factsheet\\_dp\\_reform\\_citizens\\_rights\\_2016\\_en.pdf](http://ec.europa.eu/justice/data-protection/document/factsheets_2016/factsheet_dp_reform_citizens_rights_2016_en.pdf)



## BUNE PRACTICI

- Oricine poate accesa informațiile personale pe care le postați – regula este de a presupune că totul este public, cu excepția cazului în care vă asigurați că nu este așa. În consecință, nu trebuie să spuneți pe un site de socializare nimic din ceea ce nu ați fi dispus să divulgați offline, în public. Opțiunea de a seta profilul pe privat nu înseamnă întotdeauna că numai prietenii pot vedea profilul. În unele cazuri, tot ceea ce se postează pe un profil poate, totuși, fi văzut de toată lumea, dar numai „prietenii” pot posta comentarii sau să trimită MI (mesaje instantanee). De asemenea, trebuie să fiți conștienți de faptul că, dacă vă alăturați grupurilor sau rețelelor mari (de exemplu, rețele naționale sau municipale), riscați să vă pomeniți cu un număr mare de persoane care au acces la profilul dumneavoastră.
- Aveți încredere în instinctul dumneavoastră – dacă ceva nu arată bine sau dacă simțiți că ceva nu este corect, probabil, intuiția nu vă înșală! Dacă găsiți ceva în mediu online care nu vă place sau care vă face să vă simțiți incomod, deconectați calculatorul și discutați cu un prieten de încredere despre acest lucru.
- Aveți grijă la informațiile personale. Problema este că, de îndată ce o persoană postează informații personale pe Internet, aceasta nu mai controlează cine le va vedea și cum acestea vor fi folosite. Fotografii pot fi cu ușurință copiate și distribuite altor mii de persoane prin apăsarea unui singur buton. Din cauza naturii digitale a fotografiilor, acestea pot fi chiar modificate sau falsificate. De asemenea, există programe noi de căutare ce pot identifica persoanele din fotografii, chiar dacă imaginea nu este însoțită de nume. Cu toții trebuie să învățăm să postăm numai fotografii care ne-ar place să fie văzute de toată lumea, inclusiv de părinți și cadre didactice.
- Nu toate persoanele aflate în mediul online sunt ceea ce pretind a fi în realitate. Faptul că anumite site-uri afirmă că au conectat elevii din cadrul aceleiași școli nu înseamnă nimic. Informațiile furnizate de utilizatori atunci când se înregistrează nu sunt verificate. Oricine poate crea un profil de utilizator pretinzând că este altcineva. În plus, oricine se poate alătura oricâtor comunități școlare dorește, indiferent de vârsta reală sau pretinsă.
- Fiți echilibrat – dacă rețelele sociale au devenit o obsesie și nu puteți trăi fără a vă verifica/actualiza profilul, fără a posta imagini și număra like-urile, atunci poate că ar trebui să luați „o pauză de la rețelele de socializare” sau, cel puțin, să controlați timpul petrecut pe site-urile de socializare.
- Examinați materialele de îndrumare oferite de majoritatea prestatorilor de servicii de rețele sociale despre site-urile lor, pentru utilizarea lor în condiții de siguranță.
- Analizați cu atenție materialele pe care le postați în mediul online – rețineți faptul că odată ce ați postat ceva, este posibil să nu mai reușiți niciodată să ștergeți complet postarea de pe Internet.
- Fiți deosebit de atenți atunci când postați imagini. Chiar dacă nu vă puneți numele pe o imagine, puteți fi identificat în baza fotografiei și ea poate rămâne disponibilă în cache-urile web mult timp după ce ați retras-o.
- Protejați-vă informațiile personale, în special informațiile care vă pot identifica sau localiza.
- Nu postați niciodată ceva ce ar putea fi ofensator, defăimător sau degradant pentru ceilalți.
- Rețineți faptul că puteți seta un profil public sau privat. Examinați cu atenție care este setarea cea mai potrivită pentru utilizare.
- Utilizați caracteristicile de confidențialitate oferite de site-urile de socializare. Gândiți-vă bine înainte de a vă face profilul public.

- Rețineți faptul că, dacă optați pentru un profil public, acesta poate fi văzut de oricine. Chiar dacă nu este public, acesta poate fi văzut de toți cei din rețelele în care sunteți membru. Este o idee bună să vă verificați setările în mod periodic, deoarece site-urile de socializare își pot schimba politicile.
- În cazul în care vă confrunțați cu probleme cum ar fi campaniile de ură, intimidare sau mesajele țintite cu conținut rasist, xenofob, homofob sau de altă natură extremă, solicitați întotdeauna ajutor din partea unei persoane în care aveți încredere, chiar dacă gândiți că probabil nu va înțelege sau nu va aproba.
- Nu divulgați niciodată detaliile de contact în profilul dumneavoastră.
- Rețineți faptul că conținutul pe care îl postați în mediul online poate fi utilizat pentru mai multe scopuri, inclusiv publicitate personalizată și chiar în scopuri de angajare sau politice.
- Verificați setările atunci când accesați site-uri de socializare de pe diferite dispozitive, deoarece acestea pot solicita permisiunea de a vă accesa informațiile de pe telefonul dumneavoastră inteligent, tabletă sau calculator.



## INFORMAȚII SUPLIMENTARE

- Pentru mai multe informații privind rețelele sociale, a se vedea „Cele mai importante 21 de site-uri și aplicații de socializare din lume în 2015”:  
<<http://web.archive.org/web/20160423200413/http://www.socialmediatoday.com/social-networks/2015-04-13/worlds-21-most-important-social-media-sites-and-apps-2015>>.
- Pentru sfaturi cu privire la „Socializarea în siguranță pe rețelele sociale”, a se vedea:  
<[http://web.archive.org/web/20120602054510/http://www.getsafeonline.org/nqcontent.cfm?a\\_id=1459](http://web.archive.org/web/20120602054510/http://www.getsafeonline.org/nqcontent.cfm?a_id=1459)>.
- Informații privind o varietate de subiecte legate de utilizarea site-urilor socializare și sfaturi privind garantarea siguranței pot fi găsite la: <[www.privacyrights.org/social-networking-privacy](http://www.privacyrights.org/social-networking-privacy)>.
- Raportul Rețelei de Cercetare a Științelor Sociale privind utilizarea rețelelor sociale de către adolescenți este disponibil la adresa: <[http://web.archive.org/web/20160703112245/http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1925128](http://web.archive.org/web/20160703112245/http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1925128)>.
- Centrul de Cercetare PEW a publicat un studiu privind adolescenții, tehnologia și prietenia pe: <<http://web.archive.org/web/20160710143035/http://www.pewinternet.org/2015/08/06/teens-technology-and-friendships/>>.
- Documente relevante ale Consiliului Europei: Recomandarea CM/Rec(2012)4 a Comitetului de Miniștri către statele membre privind protecția drepturilor omului în contextul rețelelor de socializare: <<https://wcd.coe.int/ViewDoc.jsp?id=1929453>>.

## Fișa 9

# Viața privată și setările de confidențialitate



**P**rotecția vieții private se referă la gradul de control pe care îl are o persoană în ceea ce privește accesul și utilizarea informațiilor sale personale. Majoritatea utilizatorilor de email și de Internet presupun că informațiile personale nu vor fi utilizate fără permisiune și că schimburile de informații sunt private și sigure. Însă realitatea este foarte diferită.

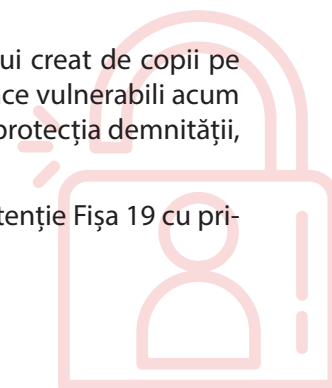
— De fiecare dată când accesați un site web, postați conținut pe rețelele sociale sau trimiteți un email, lăsați informații despre dumneavoastră, care ar putea include adresa fizică și adresa calculatorului dumneavoastră, numerele de telefon și ale cardurilor de credit, datele modelului de consumator și multe altele.

— De asemenea, trebuie să rețineți faptul că, odată ce datele dumneavoastră ajung pe Internet, este posibil să întâmpinați dificultăți în a vă menține controlul asupra acestora și pot exista consecințe pe termen lung.

— Deoarece comerțul electronic – inclusiv cumpărăturile și publicitatea în mediul online – devine o modalitate frecvent acceptată de a face afaceri, trebuie acordată o atenție specială protecției datelor sensibile, comunicărilor și preferințelor.

— Nu trebuie să existe nicio evidență durabilă sau permanentă a conținutului creat de copii pe Internet dacă acesta le afectează demnitatea, securitatea și viața privată sau îi face vulnerabili acum sau într-o etapă ulterioară a vieții lor (Declarația Comitetului de Miniștri privind protecția demnității, securității și vieții private a copiilor pe Internet, adoptată la 20 februarie 2008)<sup>1</sup>.

— Confidențialitatea este strâns legată de securitate; asigurați-vă că citiți cu atenție Fișa 19 cu privire la securitate.



## CONFIDENȚIALITATEA PE INTERNET

- Confidențialitatea pe Internet (sau online) este un termen larg, care se referă la o varietate de factori, tehnici și tehnologii utilizate pentru a proteja datele, comunicațiile și preferințele confidențiale și private<sup>2</sup>.
- Confidențialitatea pe Internet reprezintă o preocupare de fiecare dată când un utilizator accesează mediul online prin intermediul unui calculator, tablete, telefon inteligent, console de jocuri sau altui dispozitiv echipat cu Wi-Fi.
- Confidențialitatea pe Internet nu se referă numai la modul în care vă păstrați datele private în mediul online, ci și la accesibilitatea pe care spărgătorii de coduri (hackeri) o au de a vă sustrage informațiile.
- Regulamentul General privind Protecția Datelor oferă utilizatorilor mai mult control asupra propriilor date și le oferă mai multă intimitate în mediul online. Considerentele cheie ale RGPD includ:
  - ▶ o nouă definiție a consimțământului utilizatorului – consimțământul nu mai poate fi considerat ca fiind acordat în mod liber în cazul în care utilizatorii trebuie să accepte prelucrarea mai multor date decât este strict necesar pentru furnizarea serviciului respectiv;
  - ▶ o mai mare transparență în ceea ce privește informarea utilizatorilor cu privire la modul în care datele lor sunt procesate prin utilizarea de pictograme/iconițe și printr-un „limbaj simplu” – aceasta va permite utilizatorilor să compare mai bine serviciile și să le aleagă pe acelea care respectă mai mult confidențialitatea;
  - ▶ dreptul utilizatorilor la portabilitatea datelor, ceea ce înseamnă că aceștia își vor putea recupera datele într-un format utilizabil de la serviciile pe care le utilizează – această prevedere consolidează controlul utilizatorului asupra propriilor date și principiul proprietății datelor;
  - ▶ protecție sporită pentru copii – orice copil cu vârsta cuprinsă între 13 ani (minim) și 16 ani (maxim) va beneficia de protecție suplimentară, cum ar fi necesitatea autorizării parentale pentru prelucrarea datelor și protecția împotriva prelucrării datelor în scopuri publicitare;
  - ▶ taxe mai mari (până la 4% din cifra de afaceri a unei companii) în cazul încălcării acestor reguli.

### Setările de confidențialitate

— Setările de confidențialitate sunt comenzile care permit utilizatorilor să limiteze accesul la informațiile lor și la volumul de informații care pot fi văzute de alții.

— Setările de confidențialitate pentru majoritatea rețelelor sociale sunt inițial setate la o poziție prestabilită; de obicei, le puteți personaliza în funcție de necesitățile dumneavoastră și ar trebui să le verificați de fiecare dată când platforma socială vă informează că a implementat actualizări.

— Setările de confidențialitate trebuie verificate în mod regulat și pe toate dispozitivele echipate cu Wi-Fi. Nu uitați să verificați și setările de geolocalizare, deoarece coordonatele locației dumneavoastră/dispozitivului dumneavoastră sunt aspecte importante ale confidențialității dumneavoastră (a se vedea Fișa 5 cu privire la tehnologia mobilă).

1. <https://wcd.coe.int/ViewDoc.jsp?Ref=Decl%2820.02.2008%29&Language=lanEnglish&Ver=0001&Site=COE&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75>

2. <http://web.archive.org/web/20160703014430/https://www.techopedia.com/definition/24954/internet-privacy>



## Geolocalizarea

■ Geolocalizarea<sup>3</sup> constituie identificarea locației unui obiect, cum ar fi radarul, telefonul mobil sau calculatorul conectat la Internet.

■ Geolocalizarea este procesul de identificare a locației unui obiect. Aplicațiile de geolocalizare raportează locația dumneavoastră utilizatorilor și acestea pot, de asemenea, să identifice distanța față de locații din lumea reală în raport cu locația dumneavoastră. Aplicațiile de geolocalizare au deschis noi modele de afaceri pentru servicii și produse.

■ Geolocalizarea poate fi o amenințare la adresa confidențialității dumneavoastră, deoarece aceasta indică locul în care vă aflați, iar localizarea geografică a unui copil poate reprezenta o amenințare pentru siguranța copilului respectiv.

## Cookie-urile

■ Un cookie<sup>4</sup> este un fișier text lăsat pe calculatorul dumneavoastră atunci când vizitați un site web. Acesta nu vă poate afecta calculatorul, ci vă va oferi acces la informații privind comportamentul și interesele dumneavoastră. Acest lucru poate crea o atmosferă mai personală de navigare. De exemplu, atunci când vă înregistrați pe un site web, acesta ar putea să vă „întâmpine”, afișând numele dumneavoastră la revenire.

■ Este important să decideți cât de confidențial doriți să vă păstrați comportamentul în mediul online. Deoarece cookie-urile pot fi utilizate pentru a urmări modelele de utilizare și informațiile de contact, acestea oferă posibilitatea afectării confidențialității dumneavoastră. Acestea facilitează, de asemenea, targetarea comportamentală din partea agențiilor de publicitate<sup>5</sup>.

■ Puteți utiliza programe anti-spionaj<sup>6</sup> pentru a controla datele pe care le transmite sistemul dumneavoastră și pentru a curăța cookie-urile nedorite.

■ Astăzi, toate site-urile web deținute în UE sau destinate cetățenilor UE trebuie să respecte Legea Cookie-urilor (Directiva 2009/136/CE a UE). Aceasta oferă persoanelor fizice dreptul de a refuza utilizarea cookie-urilor care le reduc confidențialitatea în mediul online.

## Protecția datelor

■ Protecția datelor cu caracter personal este reglementată de Convenția Consiliului Europei pentru protecția persoanelor cu privire la prelucrarea automată a datelor cu caracter personal.

■ Aveți dreptul să știți ce date deține despre dumneavoastră o anumită companie. De asemenea, trebuie să aveți posibilitatea de a le modifica dacă ele nu sunt exacte și să vă dați consimțământul cu privire la modul în care sunt utilizate aceste date.

■ Cele mai bune linii directoare cu privire la protejarea datelor dumneavoastră se găsesc în Regulamentul General privind Protecția Datelor<sup>7</sup>.

■ Citiți cu atenție declarația de declinare a responsabilității pe toate site-urile și aplicațiile unde vi se solicită furnizarea de informații private<sup>8</sup>. Acesta este un acord juridic între dumneavoastră și operatorul de date,<sup>9</sup> care trebuie să includă detalii cu privire la locul și durata stocării datelor dumneavoastră, precum și modul în care puteți să le ștergeți.

■ Asigurați-vă că calculatorul și programele dumneavoastră de email sunt protejate prin parolă<sup>10</sup>. Atunci când achiziționați un dispozitiv sau un program nou sau vă înregistrați la un prestator de servicii Internet, probabil, implicit obțineți și numele de utilizator și parola<sup>11</sup>. Asigurați-vă că modificați rapid aceste setări implicite cu o parolă și un ID mai sigure.

3. <https://en.wikipedia.org/wiki/Geolocation>

4. [https://en.wikipedia.org/wiki/HTTP\\_cookie](https://en.wikipedia.org/wiki/HTTP_cookie)

5. [https://en.wikipedia.org/wiki/Behavioral\\_targeting](https://en.wikipedia.org/wiki/Behavioral_targeting)

6. <https://en.wikipedia.org/wiki/Spyware>

7. [http://ec.europa.eu/justice/data-protection/reform/index\\_en.htm](http://ec.europa.eu/justice/data-protection/reform/index_en.htm)

8. <https://en.wikipedia.org/wiki/Disclaimer>

9. <https://goo.gl/XEkvjh>

10. <https://en.wikipedia.org/wiki/Password>

11. <http://www.netlingo.com/right.cfm?term=default>

■ Cel mai bine este să criptați<sup>12</sup> toate informațiile sensibile care sunt transmise prin Internet. Din fericire, acest lucru este un standard pentru majoritatea tranzacțiilor de comerț electronic,<sup>13</sup> dar, cu toate acestea, trebuie să vă asigurați în continuare că o pagină este sigură înainte de a transmite informații despre cardul de credit sau contul bancar.

■ Calculatorul dumneavoastră și părțile sale componente pot fi securizate utilizând parole. Creați parole pentru dosarele care conțin documente valoroase, cum ar fi proiecte, cercetări, modele originale confidențiale și așa mai departe.

### Dreptul de a fi uitat

■ Dreptul de a fi uitat este un element important în orice discuție despre confidențialitate, deoarece acest drept le permite persoanelor să își „reia controlul” asupra vieții private.

■ În Uniunea Europeană, o persoană poate solicita ștergerea anumitor rezultate din indexul motorului de căutare ca acestea să nu mai apară atunci când cineva îi caută numele. Dar există limite și această măsură va trebui întotdeauna să fie echilibrată în raport cu drepturile fundamentale ale altor persoane, precum libertatea de exprimare. În orice caz, informațiile vor rămâne, totuși, accesibile pe site-ul web pe care se află; însă acest lucru va face și mai dificilă găsirea.

■ Pentru ca o persoană să își exercite dreptul de a fi uitat și a solicita eliminarea dintr-un motor de căutare, aceasta trebuie să completeze un formular de pe site-ul web al motorului de căutare<sup>14</sup>.

■ Dar, rețineți, este mai bine să nu postați deloc informații private pentru că odată ce acestea ajung pe Internet, este aproape imposibil să le ștergeți complet.

### Importanța de a vorbi despre confidențialitate în clasă sau acasă

■ Aspectele tehnice și sociale ale confidențialității și riscurile auto-divulgării oferă teme de învățare valoroase. Aspectele tehnice pot fi discutate în cadrul disciplinei Informatica, dar trebuie, de asemenea, să facă parte și din curriculumul la disciplina Deprinderi de viață.

■ Un element important al educației privind viața privată este conceptul de „realizare a profilului” și a conectării elementelor disparate de informații referitoare la o persoană pentru a deduce o imagine mai detaliată. Implicația educațională importantă este că mult mai multe informații pot fi găsite despre noi prin corelația dintre acestea. De exemplu, un profil „anonim” pe o rețea socială (ascuns în spatele unui pseudonim) poate fi identificat cu numele dumneavoastră real prin corelarea fotografiilor de pe profilul anonim și cele de pe un profil complet, dar de pe un alt site.

■ Ideea că confidențialitatea este încălcată numai prin divulgarea informațiilor personale clasice trebuie examinată cu atenție. Noile tehnici de marketing, care fac distincția între oameni pe baza trăsăturilor lor comportamentale (și anume, țintirea comportamentală), pot fi, de asemenea, considerate invazive în ceea ce privește viața privată.

■ Viața privată este din ce în ce mai subminată de rapiditatea și ușurința cu care copiii și tinerii pot publica și/sau transmite imagini digitale pe Internet prin aplicații web și prin camerele foto și serviciul MMS de pe telefoanele mobile. O regulă simplă: niciodată nu publicați ceva ce nu doriți să fie văzut de cadrele didactice sau părinții dumneavoastră.

■ Toată lumea trebuie să aibă abilitățile necesare pentru a naviga în condiții de siguranță pe Internet și anume, să cunoască cum să se protejeze, cum să comunice eficient și cum să demonstreze responsabilitate față de ceilalți.

■ Din această temă reiese o legătură firească cu dimensiunea cetățenească a oricărui curriculum. Problemele referitoare la confidențialitatea în mediul online reflectă cu acuratețe problemele sociale predominante în majoritatea culturilor din ziua de azi. Examinarea motivațiilor hackerilor<sup>15</sup>, a spărgătorilor și a activiștilor care pledează pentru confidențialitate oferă multiple posibilități de a discuta valoarea principiilor democratice.

12. <http://en.wikipedia.org/wiki/Encryption>

13. <http://en.wikipedia.org/wiki/Ecommerce>

14. [https://en.wikipedia.org/wiki/Right\\_to\\_be\\_forgotten](https://en.wikipedia.org/wiki/Right_to_be_forgotten)

15. <http://en.wikipedia.org/wiki/Hacker>



## CONSIDERAȚII DE ORDIN ETIC ȘI RISCURI

- Confidențialitatea în mediul online este unul dintre cele mai complexe subiecte etice și juridice privind Internetul.
- Toată lumea are dreptul la protecția vieții private și trebuie să fie protejată de intențiile răuvoitoare.
- Riscurile privind confidențialitatea pe Internet includ phishing-ul (piratare pe Internet cu scop de a fura date securizate de utilizator), pharming-ul (piratare pe Internet cu scopul de a redirecționa un vizitator al unui site web legitim, către o altă adresă IP), programele spion (spyware – aplicație offline care obține date fără consimțământul utilizatorului) și coduri ostile (malware – aplicație utilizată pentru a submina utilizatorii online și offline prin intermediul troienilor, a virusilor și a programelor spion)<sup>16</sup>.
- Sexting-ul sau trimiterea de fotografii nud pe telefonul cuiva, trimiterea de conținut, imagini (de multe ori selfie-uri), videoclipuri sugestive și explicite, prin intermediul telefonului, calculatorului, camerei web sau a altui dispozitiv sau scrierea de mesaje seducătoare în mediul online are consecințe grave nu numai din punct de vedere juridic, dar și din punctul de vedere al riscurilor reputaționale pentru persoana implicată, deoarece mesajele, imaginile sau videoclipurile pot fi postate pe site-urile rețelelor sociale sau utilizate pe site-urile web și în videoclipurile pornografice.
- Suntem responsabili pentru toate deciziile pe care le luăm cu privire la drepturile noastre și ale altora, așa precum drepturile de autor<sup>17</sup> și proprietate intelectuală<sup>18</sup>.
- Libertatea de exprimare este un drept; totuși, în practică, aceasta este o zonă gri, fără răspunsuri simple. Ce este acceptabil și ce nu este? Cum se poate impune respectarea regulilor fără a aduce atingere drepturilor vorbitorului?



## INSTRUCȚIUNI

- Utilizarea setărilor de confidențialitate pentru toate echipamentele dumneavoastră cu acces la Internet prin Wi-Fi este una dintre cele mai bune modalități de a vă proteja viața privată.
- În funcție de browserul dumneavoastră, faceți o căutare rapidă în setările de confidențialitate pentru a vedea cum puteți:
  - să blocați anunțurile și trasabilitatea
  - să blocați cookie-urile terților
  - să blocați site-urile web ca să nu vă acceseze locația.
- Nu uitați să setați parametrii de confidențialitate pe telefoanele inteligente, tablete și consolele de jocuri. Cele mai recente camere foto au setări de localizare pe care de asemenea trebuie să le verificați.



## IDEI PENTRU LUCRUL ÎN CLASĂ

- Solicitați elevilor să caute pe Google propriile nume. Asigurați-vă că efectuați căutarea și la imagini și videoclipuri. Lăsați-i să creeze o alertă Google pentru propriile nume, astfel, ei vor cunoaște când numele lor este postat online.
- Elaborați un cadru de cunoștințe de bază cu privire la viața privată împreună cu clasa dumneavoastră. Definiți atât conceptele tehnice, cât și cele sociale și identificați prejudecățile și miturile pentru a le discuta. Astfel de întrebări simple precum „Ce înseamnă viața privată?” și „Este necesar a fi respectată viața privată?” ar trebui să genereze dezbatere intense.

16. <http://web.archive.org/web/20160703014430/https://www.techopedia.com/definition/24954/internet-privacy>

17. <http://en.wikipedia.org/wiki/Copyright>

18. [http://en.wikipedia.org/wiki/Intellectual\\_property](http://en.wikipedia.org/wiki/Intellectual_property)

- Căutați site-uri referitoare la confidențialitatea pe Internet și utilizați programe traceroute<sup>19</sup> pentru a localiza adresele fizice ale acestor site-uri, pentru a demonstra diferitele probleme geofizice care reglementează legalitatea pe Internet. Explorați alte aspecte (culturale, politice și istorice) care decurg din rezultatele traserii. De exemplu, alegeți un site de re-expediere a emailurilor (remailer site)<sup>20</sup> sau un serviciu proxy anonim, urmăriți un traseu, apoi căutați motivele pentru care serviciile sunt localizate în țările respective.
- Jocul de rol „Joacă-Decide” privind protecția datelor și viața privată<sup>21</sup> oferă o modalitate distractivă de a explora implicațiile legii cu privire la viața privată, a drepturilor de autor și a libertății de exprimare și informare în diferite state sau pentru diferite grupuri de vârstă și culturale.
- Învățați elevii cum să creeze parole securizate<sup>22</sup>.
- Explorați și comparați profilurile utilizatorilor de pe unele dintre cele mai populare site-uri de socializare împreună cu elevii dumneavoastră (consultați Fișa 8 cu privire la socializarea online). Ce informații private divulgă utilizatorii din neatenție? Întocmiți o listă de verificare pentru crearea unui profil de utilizator sigur.



## BUNE PRACTICI

- Două reguli de aur:
  - ▶ nu partajați informațiile dumneavoastră personale cu nicio persoană pe care nu o cunoașteți și în care nu aveți încredere;
  - ▶ nu utilizați informațiile personale sau fotografiile unor alte persoane fără consimțământul acestora.
- Faceți copii de rezervă<sup>23</sup> ale sistemului dumneavoastră și asigurați-vă că aveți o politică a copiilor de rezervă.
- Actualizați măsurile de securitate ale sistemului dumneavoastră și căutați informații despre instrumente suplimentare la <http://www.epic.org/privacy/tools.html> care vor completa preferințele dumneavoastră în mediul online.
- Programele anti-virus<sup>24</sup> și sistemul firewall<sup>25</sup> sunt o necesitate absolută. S-ar putea să doriți, de asemenea, să luați în considerare și alte instrumente, cum ar fi blocajele ferestrelor (pop-up blockers)<sup>26</sup> și programele antispyonaj (anti-spyware)<sup>27</sup>. Asigurați-vă că efectuați o verificare periodică a sistemului dumneavoastră.
- Utilizați „parole puternice”<sup>28</sup> pentru a vă proteja calculatorul, emailul și conexiunea la Internet. Parolele puternice constau din litere, cifre și caractere speciale.
- Înainte de a divulga date personale, verificați simbolul lacătului blocat care este afișat în bara de instrumente. Acesta denotă că tranzacția dumneavoastră are loc printr-o conexiune securizată. Înainte de a efectua tranzacții în mediul online, verificați ca adresa URL să includă HTTPS; în acest caz, S semnifică „sigur” în Protocolul de Transfer Hipertext (HTTP) și autentifică site-ul web și serverul web asociat, care protejează împotriva atacurilor terților.
- Evitați cumpărăturile online pe site-uri web nesigure și evitați expunerea datelor cu caracter personal pe site-uri cu niveluri de securitate mai reduse.
- Asigurați-vă că vă verificați drepturile; este posibil să fiți mai protejat decât credeți. Utilizatorii constituie întotdeauna veriga cea mai slabă în ceea ce privește viața privată și protecția datelor.

19. <http://en.wikipedia.org/wiki/Traceroute>

20. <http://en.wikipedia.org/wiki/Remailer>

21. <http://paneuyouth.eu/files/2013/06/PD-kit-privacy-and-data-protection.pdf>

22. [http://en.wikipedia.org/wiki/Password#Factors\\_in\\_the\\_security\\_of\\_an\\_individual\\_password](http://en.wikipedia.org/wiki/Password#Factors_in_the_security_of_an_individual_password)

23. [http://en.wikipedia.org/wiki/Back\\_up](http://en.wikipedia.org/wiki/Back_up)

24. <http://en.wikipedia.org/wiki/Antivirus>

25. [http://en.wikipedia.org/wiki/Firewall\\_%28networking%29](http://en.wikipedia.org/wiki/Firewall_%28networking%29)

26. [http://en.wikipedia.org/wiki/Pop\\_up#Add-on\\_programs\\_that\\_block\\_pop-up\\_ads](http://en.wikipedia.org/wiki/Pop_up#Add-on_programs_that_block_pop-up_ads)

27. <http://en.wikipedia.org/wiki/Spyware>

28. [http://en.wikipedia.org/wiki/Password#Factors\\_in\\_the\\_security\\_of\\_an\\_individual\\_password](http://en.wikipedia.org/wiki/Password#Factors_in_the_security_of_an_individual_password)



## INFORMAȚII SUPLIMENTARE

- Pentru a citi mai multe despre Legea Cookie-urilor și Directiva UE, a se vedea: [<http://www.cookie-law.org/the-cookie-law/>](http://www.cookie-law.org/the-cookie-law/).
- Există o Fișă a Comisiei Europene privind dreptul de a fi uitat: [http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet\\_data\\_protection\\_en.pdf](http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf).
- De asemenea, există o Fișă a Comisiei Europene privind protecția datelor: [http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet\\_data\\_protection\\_eurobarometer\\_240615\\_en.pdf](http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_eurobarometer_240615_en.pdf) și alte informații referitoare la reforme conexe [http://ec.europa.eu/justice/data-protection/reform/index\\_en.htm](http://ec.europa.eu/justice/data-protection/reform/index_en.htm).
- Centrul de informare privind confidențialitatea electronică (Electronic Privacy Information Center – EPIC) menține o listă de instrumente și articole privind protecția vieții private: <http://www.epic.org/privacy/tools.html>.
- Aflați ce spune calculatorul dumneavoastră oricărei persoane aflate pe net care are curiozitatea să caute, utilizând BrowserSpy: <http://gemal.dk/browserspy/>.
- Îngrijorat de libertățile dumneavoastră civile? Aceste discuții cu privire la respectul pentru viața privată ar putea să extindă cursul dumneavoastră despre cetățenie pentru ceva timp: Fundația Frontiera Electronică (Electronic Frontier) la <http://www EFF.org/>, Epic.org la <http://www.epic.org>, Privacy International la <http://www.privacyinternational.org/> și Privacy.net la <http://www.privacy.net/>.
- TuCows la <http://www.tucows.com/> este un site care oferă acces la peste 40 000 de programe partajate (shareware) și gratuite (freeware). Acesta promite descărcări rapide, locale și sigure, fără viruși și fără programe spion.
- Zone Alarm la <http://www.zonelabs.com/store/content/home.jsp> este unul dintre cele mai cunoscute sisteme firewall. Acesta vă permite să setați controale de acces pentru diferite programe care trimit informații prin Internet.
- CryptoHeaven este un pachet de criptare care oferă securizarea poștei, partajării fișierelor și a discuțiilor chat, prin criptare simetrică și asimetrică: <http://www.cryptoheaven.com/>.
- Centrul de asistență al Facebook oferă informații despre setările de confidențialitate: <https://www.facebook.com/help/193677450678703>.
- Statisticile privind modul în care copiii și tinerii înțeleg respectul la viața privată în mediul online și setările de confidențialitate, pot fi găsite la: <http://web.archive.org/web/20160703155259/https://www.techopedia.com/2/30101/internet/online-privacy/dm-millennials-understand-online-privacy>.
- Pentru statisticile despre tineretul din Europa de astăzi, a se vedea: [http://web.archive.org/web/20160604111543/http://ec.europa.eu/eurostat/statistics-explained/index.php/Being\\_young\\_in\\_Europe\\_today\\_-\\_digital\\_world](http://web.archive.org/web/20160604111543/http://ec.europa.eu/eurostat/statistics-explained/index.php/Being_young_in_Europe_today_-_digital_world).
- Pentru informații despre drepturile digitale europene, a se vedea: <http://www.edri.org>.

- Documente relevante ale Consiliului Europei:
  - ▶ Convenția pentru protecția persoanelor cu privire la prelucrarea automată a datelor cu caracter personal (ETS Nr. 108): <http://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37>.
  - ▶ Declarația Comitetului de Miniștri privind protecția demnității, securității și vieții private a copiilor pe Internet: <https://wcd.coe.int/ViewDoc.jsp?id=1252427>.
  - ▶ Pagina dată a Consiliului Europei conține informații despre activitatea Consiliului Europei în domeniul vieții private și protecției datelor: <http://www.coe.int/en/web/internet-users-rights/privacy-and-data-protection>, precum și informații despre drepturile și responsabilitățile dumneavoastră în mediul online.

## 3. Internetul – Participarea la societatea cunoașterii

---

” „Cunoașterea înseamnă putere. Informația este eliberatoare. Educația este premisa progresului, în fiecare societate, în fiecare familie.”

*Kofi Annan, , fost Secretar General al Organizației Națiunilor Unite, ianuarie 1997-decembrie 2006*

### LISTA DE VERIFICARE PENTRU FIȘA 10 – CĂUTAREA INFORMAȚIILOR

---

Citiți declarația de declinare a responsabilității atunci când consultați un site web?

Cum puteți fi siguri că informațiile pe care le găsiți sunt faptice și obiective?

Consultați mai multe site-uri web pentru a verifica faptele?

### LISTA DE VERIFICARE PENTRU FIȘA 11 – GĂSIREA INFORMAȚIILOR DE CALITATE PE WEB

---

Înainte de a descărca fișierele, verificați dacă programul antivirus este activ?

Dacă obișnuiți să citiți știrile de pe Internet, căutați mai multe surse privind aceeași știre?

Periodic, curățați cookie-urile pentru a evita să vi se realizeze „profilul” de către motoarele de căutare.

### LISTA DE VERIFICARE PENTRU FIȘA 12 – ÎNVĂȚĂMÂNTUL LA DISTANȚĂ ȘI CURSURILE ONLINE DESCHISE CU PARTICIPARE NELIMITATĂ (CODPN-URILE)

---

Alegeți o metodă de învățare la distanță potrivită pentru dumneavoastră: determinați ce tip de învățare (sincron, asincron, program deschis, învățare la distanță mixtă) vă va ajuta cel mai bine să vă atingeți obiectivele.

Înainte de a selecta un curs de învățare la distanță, cercetați recenziile – atât de la elevi/studenti, cât și de la profesori.

Luați măsuri de precauție adecvate pentru a vă asigura că echipamentul și programul calculatorului dumneavoastră sunt protejate de hackeri, viruși și alte amenințări.

### LISTA DE VERIFICARE PENTRU FIȘA 13 – CUMPĂRĂTURILE ÎN MEDIUL ONLINE

---

Nu efectuați achiziții în mediul online prin conexiuni nesigure pe Internet.

Trebuie să înțelegeți și apoi să aprobați informațiile cheie furnizate cu privire la produs sau serviciu.

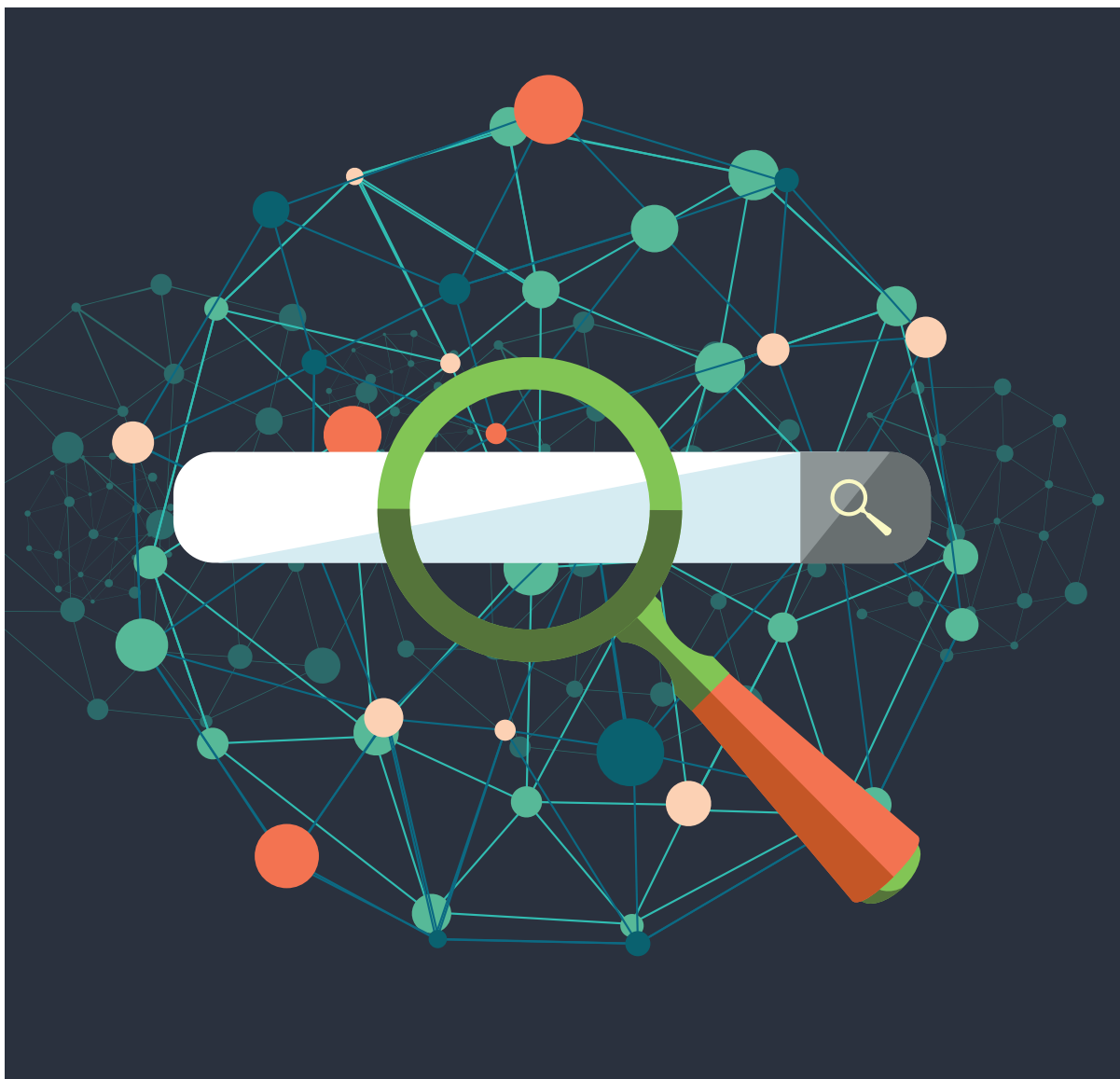
Dezactivați achizițiile in-app pe telefonul dumneavoastră inteligent sau pe tabletă.

Nu vă bazați pe toate recomandările pentru utilizatori pe care le vedeți, deoarece crearea recomandărilor pentru „utilizator” poate fi, de asemenea, o afacere profitabilă.





## Căutarea informațiilor



La începuturile Internetului, nu existau motoare de căutare. Încercați să vă imaginați o lume fără motoare de căutare. Oamenii trebuiau să găsească site-uri web tipărite pe hârtie sau în reviste și să introducă adresa în propriile browsere. Din fericire, respectivul site web avea link-uri către un alt site web și făcând clic de la un link la altul, utilizatorii puteau „explora” World Wide Web-ul. Treptat, au fost create portaluri sau directoare<sup>1</sup> de Internet, care se asemănau oarecum cu o carte de telefoane: o vastă listă de site-uri web sortate pe categorii. Unele dintre aceste directoare sau portaluri încă mai există, cum ar fi Yahoo! și MSN.

Alte forme de portaluri includ:

- portaluri cu conținut „oficial”, cum ar fi site-ul web al Națiunilor Unite sau cel al Consiliului Europei;
- portaluri specializate în conținut sau servicii specifice cum ar fi Booking.com pentru hoteluri sau Amazon.com pentru cumpărături;
- portaluri care se bazează pe conținut generat de utilizatori și care sunt foarte diverse – rețelele sociale precum Facebook pot fi, de asemenea, considerate o formă de portal.

1. [https://en.wikipedia.org/wiki/Web\\_portal](https://en.wikipedia.org/wiki/Web_portal)

■ Ulterior au fost create motoarele de căutare și acestea au revoluționat modul în care oamenii au căutat conținut pe Internet. Dar cum funcționează motoarele de căutare? În prezent, motoarele de căutare se bazează pe tehnologia de extragere a datelor (web crawler)<sup>2</sup> și pe algoritmi foarte sofisticăți care analizează conținutul, clasifică conținutul în indexuri<sup>3</sup> și decid ce site-uri web să extragă din aceste indexuri, în funcție de cuvintele-cheie pe care le folosiți în căutarea dumneavoastră.

■ Modul în care algoritmul este setat este extrem de important, deoarece majoritatea oamenilor se opresc la primele pagini ale rezultatelor căutării. În prezent, Google este cel mai des utilizat motor de căutare și a devenit popular datorită algoritmului său care a utilizat o metodă originală de clasificare a importanței unui site reieșind din numărului de backlink-uri (backlinks)<sup>4</sup> pe care le are. În principiu, acest lucru înseamnă, câte site-uri web externe includ link-uri către site-ul dumneavoastră web. De exemplu, dacă site-ul web wikipedia.org este menționat pe un număr mare de alte site-uri web, atunci acesta obține o clasificare mai bună.

■ Dar algoritmi sunt optimizați în mod constant pentru a avea o acuratețe sporită. De exemplu, Google intenționează să adauge un element care să calculeze „gradul de încredere” al site-urilor web bazându-se pe corespondențele dintre conținut și faptele stocate în baza de date a Google denumită Knowledge Vault. Mai mult, algoritmi pot fi, de asemenea, modificați în scopuri comerciale, după cum vom vedea mai târziu.

■ Consultați explicația animată a Google privind modul în care funcționează motorul său de căutare: <<https://www.google.com/insidesearch/howsearchworks/thestory/>>.



## VALOAREA EDUCAȚIONALĂ, DE CE ESTE RELEVANT, IMPORTANT?

■ Învățarea modului de a utiliza corect un motor de căutare este, fără îndoială, cea mai importantă competență care ar trebui dezvoltată, nu numai pentru a naviga, în mod responsabil, pe Internet, ci și pentru a dobândi competențe transversale, cum ar fi gândirea critică (căutând și comparând surse divergente online). Odată ce ați înțeles cum să utilizați un motor de căutare, acesta vă poate ajuta să găsiți informații de calitate pentru a dezvolta alte mii de competențe sau pentru dobândi și mai multe cunoștințe despre o gamă infinită de subiecte, inclusiv – conduita responsabilă pe Internet!

■ De exemplu, vă puteți consolida competențele digitale, căutând soluții la problemele pe care le aveți cu dispozitivele dumneavoastră sau pur și simplu satisfăcându-vă curiozitatea cu privire la modul în care acestea funcționează. Datorită utilizării unui motor de căutare, veți putea găsi acest manual ce se referă la competențele de utilizare a Internetului pe care îl citiți.



## CONSIDERAȚII DE ORDIN ETIC ȘI RISCURI

- Unele portaluri pot impune calitatea de membru sau înregistrarea, care poate fi un serviciu plătit. Înainte de a vă înregistra (chiar și pentru servicii „gratuite”), asigurați-vă că înțelegeți termenii și condițiile serviciului și că ați examinat și ați înțeles politica de confidențialitate a site-ului web (a se vedea <<http://www.netlingo.com/right.cfm?term=privacy%20policy>>).
- Site-urile web utilizează o varietate de mijloace, inclusiv plata, pentru a-și îmbunătăți clasamentul în rezultatele motorului de căutare. Unele motoare de căutare, cum ar fi Google, identifică în mod clar care rezultate sunt anunțuri sponsorizate. Mulți alții însă, nu fac această distincție.
- Algoritmi propriu-ziși nu sunt niciodată neutri și fac subiect al diverselor controverse și critici<sup>5</sup>. De exemplu, este cunoscut faptul că Google și-a crescut vizibilitatea propriilor servicii, cum ar fi Google Shopping, Google+ sau YouTube, în detrimentul concurenților săi (Amazon, Facebook, Dailymotion etc.). Motoarele de căutare pot fi, de asemenea, manipulate din motive politice. Ca regulă generală, să nu credeți niciodată că, doar pentru că un rezultat

2. [https://en.wikipedia.org/wiki/Web\\_crawler](https://en.wikipedia.org/wiki/Web_crawler)

3. [https://en.wikipedia.org/wiki/Web\\_indexing](https://en.wikipedia.org/wiki/Web_indexing)

4. <https://en.wikipedia.org/wiki/Backlink>

5. [https://en.wikipedia.org/wiki/Criticism\\_of\\_Google](https://en.wikipedia.org/wiki/Criticism_of_Google)

al căutării este poziționat mai sus, acesta este reprezentativ pentru „adevăr” sau că site-urile web poziționate mai jos sunt „neimportante” sau „irelevante”.

- De aceea este esențial să avem mai multe portaluri (gateway-uri) și motoare de căutare capabile să caute pe web pentru a obține rezultate mai diversificate și pentru a menține o concurență sănătoasă, care poate contribui la o mai bună acuratețe și neutralitate a căutării. În calitate de utilizator, jucați un rol important în modelarea mediului online: nu uitați să utilizați alte motoare de căutare, cum ar fi Yahoo!, Bing, Qwant, IXquick sau DuckDuckGo. Prin utilizarea motoarelor de căutare mai puțin cunoscute, veți contribui la existența acestora și, astfel, la asigurarea diversității<sup>6</sup>.
- Rețineți faptul că locația dumneavoastră geografică<sup>7</sup> și cookie-urile din căutările dumneavoastră anterioare vă vor influența rezultatele căutării. Cu toate că este imposibil de evitat ca datele dumneavoastră de localizare geografică să fie preluate de motorul de căutare<sup>8</sup>, ștergerea periodică a cookie-urilor (a se vedea Fișa 9 cu privire la viața privată și protecția vieții private) și – într-o măsură mai mică – a istoricului dumneavoastră de navigare, vor reduce publicitatea direcționată pe care o primiți în legătură cu cele mai recente căutări (de exemplu, destinația de călătorie). De asemenea, vă va ajuta să vă asigurați că sunteți bine informat cu privire la problemele sociale și politice importante, fără a vă limita la perspectiva percepută de dumneavoastră<sup>9</sup>. De asemenea, puteți să dezactivați toate cookie-urile, analizând setările în interiorul browserului dumneavoastră de Internet; cu toate acestea, aveți grijă, fiindcă este posibil ca anumite site-uri web să nu funcționeze corect.
- În final, rețineți faptul că rezultatele pe care le obțineți în căutările dumneavoastră vor depinde foarte mult de ceea ce căutați. De exemplu, în cazul în care căutați conținut foarte violent, probabil asta veți găsi, dar este posibil să vă alegeți cu mult mai multe decât v-ați fi dorit. Dezvoltarea rezilienței la conținuturile șocante sau deranjante este un proces continuu, așadar, nu vă grăbiți și adoptați o abordare progresivă.



## INSTRUCȚIUNI

Deoarece motoarele de căutare sunt cele mai importante gateway-uri în accesarea informațiilor, este esențial să înțelegem cum funcționează în profunzime. Limitarea doar la rezultatele căutării primei pagini vă poate oferi o viziune extrem de trunchiată asupra a ceea ce este important și ce nu este. Cele mai importante funcții de căutare avansate pe care trebuie să le rețineți sunt:

- Ghilimelele: aceasta este probabil una dintre cele mai utile și cele mai cunoscute funcții de căutare avansată. Dacă doriți să vă asigurați că un motor de căutare caută o expresie exactă, utilizați ghilimele pentru a o încadra. Acest lucru poate fi util dacă doriți să găsiți o sintagmă sau expresie exactă.
- Semnul minus „-”: acesta se folosește atunci când căutați ceva, dar excludeți un anumit termen. De exemplu, dacă căutați cuvântul „amurg”, primele rezultate vor fi toate despre seria de filme. Dar dacă căutați „amurg - vampir”, veți obține definiția cuvântului „amurg”. Semnul minus este, prin urmare, foarte util atunci când un cuvânt este prea des asociat cu altceva și doriți să vă asigurați că acel lucru nu se intercalează în căutarea dumneavoastră.
- Opțiunile de interogare: puteți adăuga o anumită opțiune la căutarea dumneavoastră, utilizând anumite cuvinte-cheie. De exemplu, dacă tastați „a defini: pasăre”, va fi căutată definiția „păsării” și nu cuvântul, în general. Dacă tastați „site: wikipedia.org apple”, Google va căuta doar pe site-ul web „Wikipedia”. Acest lucru este foarte util atunci când căutați prin portaluri, după cum vom vedea mai jos. Există mult mai multe opțiuni de interogare, așadar, consultați-le accesând link-ul de mai jos.
- Căutări specializate: majoritatea motoarelor de căutare, inclusiv IXquick, Qwant, DuckDuckGo, Google, Yahoo! și Bing au opțiuni de căutare specializate, cum ar fi căutarea de conținut multimedia

6. [https://en.wikipedia.org/wiki/Web\\_search\\_engine](https://en.wikipedia.org/wiki/Web_search_engine)

7. <http://www.advancedwebranking.com/blog/geo-location/>

8. <http://www.allaboutcookies.org/cookies/cookie-profiling.html>

9. <http://www.pcadvisor.co.uk/how-to/internet/how-delete-cookies-web-browsing-history-3218163/>

(imagini, videoclipuri etc.), lucrări academice, cărți, hărți și așa mai departe. Familiarizați-vă cu aceste posibilități de căutare specializate, deoarece acestea includ propriile lor opțiuni avansate. De exemplu, puteți filtra imaginile în funcție de dimensiune, culoare, tip de fișier și chiar drepturi de autor și licență.

- Instrumentele de căutare: „instrumentele de căutare” disponibile imediat sub bara de căutare după efectuarea unei căutări sunt, de asemenea, extrem de utile. Puteți filtra rezultatele în funcție de țară și în funcție de timp. Acest lucru este foarte practic dacă căutați, de exemplu, știri, deoarece puteți limita căutarea la cele mai recente știri sau la știrile publicate exact cu un an în urmă.
- Căutarea avansată: opțiunea de „căutare avansată” poate fi găsită făcând clic pe butonul „opțiuni” în partea dreaptă sus. Căutarea avansată vă oferă toate funcțiile de căutare de mai sus într-un mod ușor de utilizat, astfel încât, dacă nu vă simțiți confortabil folosind operatorii sau termenii opțiunii specifice de interogare, utilizați „căutare avansată”<sup>10</sup>.



## IDEI PENTRU LUCRUL ÎN CLASĂ

- Stabiliți o țintă de căutare pentru orice subiect: creați echipe care să utilizeze portaluri/motoare de căutare diferite, precum și o echipă care să utilizeze unele dintre tehnicile de căutare descrise mai sus, pentru a căuta informații. Permiteți echipelor să compare rezultatele, ușurința accesului și calitatea informațiilor.
- Stabiliți un subiect de cercetare, de exemplu, imaginea copilului în arta sec. al XVIII-lea sau dinamica ecosistemului unei anumite specii care trăiește în oceane. Furnizați clasei dumneavoastră URL-uri de portal<sup>11</sup> care vor duce la link-uri ce oferă suport planului lecției. Întrucât vor exista probabil prea multe link-uri care să fie urmărite de fiecare persoană, creați echipe pentru a împărți link-urile și pentru a cuprinde cât mai mult posibil dintr-un subiect, permițând fiecărei echipe să își prezinte constatările. Rezultatele pe echipe pot fi diferite, ce va permite o abordare restrictivă față de perfecționarea în continuare a învățării elevilor.
- Prevenirea sau vindecarea: solicitați elevilor să caute propriul nume pe un motor de căutare și să vadă cât de multe informații nedorite găsesc despre ei înșiși. Cum pot ei evita accesarea unor astfel de informații de către ceilalți și cum pot reglementările privind protecția datelor să îi ajute să șteargă conținuturile nedorite?



## BUNE PRACTICI

- Păstrați o doză sănătoasă de scepticism față de materialul pe care îl găsiți. Internetul reprezintă un spațiu liber pentru ca oamenii să poată partaja opinii și să exprime idei. Asigurați-vă că evaluați cu un ochi critic și căutați opiniile și informațiile divergente pentru a evita propagarea miturilor sau a fi înșelat de afirmații false.
- Evitați plagiatul, nu utilizați eseuri sau lucrări gata realizate. În măsura în care este posibil, acordați credit autorului și faceți referire la sursa materialului pe care îl citați sau utilizați. Acest lucru este important deoarece:
  - ▶ acordă autorului și sursei creditul datorat;
  - ▶ vă protejează de acuzațiile de plagiat;
  - ▶ îi ajută pe alții să își formeze propria judecată despre credibilitatea materialului;
  - ▶ fiți conștient de problemele privind drepturile de autor dacă folosiți materiale pe care le găsiți pe Internet (a se vedea mai jos secțiunea „Instrucțiuni” și Fișa 14 cu privire la muzică și imagini).

10. [https://www.google.com/advanced\\_search?hl=en](https://www.google.com/advanced_search?hl=en); [https://en.wikipedia.org/wiki/Google\\_Search#Search\\_options](https://en.wikipedia.org/wiki/Google_Search#Search_options)

11. <http://en.wikipedia.org/wiki/URL>

- Acordați-vă timp pentru a vă gestiona/șterge cookie-urile și istoricul navigării dumneavoastră. Puteți dezactiva în întregime cookie-urile pentru o confidențialitate sporită, dar rețineți faptul că în lipsa acestora, unele site-uri web ar putea să nu funcționeze corect.
- Încercați întotdeauna mai mulți termeni și tehnici avansate de căutare și diferite motoare de căutare pentru a profita la maxim de căutarea dumneavoastră și pentru a găsi o diversitate de surse.
- Marcați site-urile sau portaluri utile, astfel încât să nu mai fie nevoie să le căutați din nou.
- Uneori, veți căuta anumite informații de pe un anumit portal, cum ar fi un document oficial al administrației publice, definiția unui cuvânt, compararea prețurilor la hoteluri sau a tarifelor pentru transportul aerian sau prețul unui produs pe care doriți să-l procurați. Pentru toate aceste interogări, puteți utiliza o combinație de motoare de căutare și portaluri bine cunoscute, cum ar fi Booking.com, Wikipedia sau Amazon. Multe portaluri au propriile lor motoare de căutare interne, însă puteți utiliza și un motor extern de căutare și restrânge căutarea doar pe portalul respectiv. De exemplu, căutați „Hotel Brussels site: booking.com”. Combinând ambele opțiuni este o practică bună pentru a găsi ceea ce căutați.
- Dacă găsiți materiale utile, imprimați-le, faceți o captură de ecran sau salvați-le. Este posibil să nu le mai găsiți din nou sau acestea ar putea fi scoase offline fără să fi fost atenționați.
- Dacă nu puteți găsi răspunsurile prin intermediul unui motor de căutare, postați o interogare într-un forum de mesaje, forum de discuții sau pe o rețea socială relevantă.
- Nu uitați să contribuiți la crearea de conținut în mediul online. Toate răspunsurile pe care le căutați atunci când utilizați un motor de căutare au fost scrise și create de cineva. Partajarea propriilor cunoștințe și competențe ar putea într-o bună zi ajuta o altă persoană (a se vedea Fișa 15 cu privire la creativitate).



## INFORMAȚII SUPLIMENTARE

- Wikipedia este o enciclopedie cu conținut gratuit, scrisă de utilizatori din întreaga lume în colaborare: <<http://www.wikipedia.org/>>.
- Portalul Europeana găzduiește un volum vast de conținut digitalizat, reprezentând patrimoniul cultural al Europei: <<http://www.europeana.eu/portal/>>.
- Aceste motoare de căutare europene au standarde înalte pentru protecția vieții private: <<https://www.qwant.com/>> și <<https://ixquick.com/>>.
- Există, de asemenea, un motor de căutare din SUA cu standarde înalte pentru protecția vieții private: <<https://duckduckgo.com/>>.
- Următorul site vă explică cum să folosiți motorul de căutare Google: <<https://support.google.com/websearch/answer/134479?hl=en>>.
- Pentru sfaturi despre utilizarea Bing pe Microsoft în Windows 8, a se vedea: <<http://onlinehelp.microsoft.com/en-us/bing/jj684589.aspx>>.
- Cum funcționează motoarele de căutare? A se vedea: <<http://web.archive.org/web/20160509142554/http://www.bbc.co.uk/guides/ztbjq6f>>.
- Articole relevante din Convenția ONU cu privire la drepturile copilului:
 

**Articolul 13** – Copiii au dreptul de a obține și difuza informații, cu excepția cazului când acest fapt ar leza drepturile altora.

**Articolul 16** – Copiii au dreptul la viață personală. Copilul are dreptul la protecția legii contra unor atacuri asupra vieții lor personale, reputației, familiei și domiciliului.

**Articolul 17** – Copiii au dreptul la informații de încredere din partea mass-media. Televiziunea, radioul și ziarele trebuie să ofere informații pe înțelesul copiilor și care nu dăunează bunăstării acestora.

- Documente relevante ale Consiliului Europei:
  - ▶ Recomandarea CM/Rec(2012)3 a Comitetului de Miniștri către statele membre asupra protecției drepturilor omului cu privire la folosirea motoarelor de căutare: <https://wcd.coe.int/ViewDoc.jsp?id=1929429&Site=CM&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383>.
  - ▶ Recomandarea CM/Rec(2008)6 a Comitetului de Miniștri către statele membre privind măsurile pentru promovarea respectării libertății de exprimare și de informare referitor la filtrele pe Internet: <https://wcd.coe.int/ViewDoc.jsp?Ref=CM/Rec%282008%296&Language=lanEnglish&Ver=original&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75>.

## Găsirea informațiilor de calitate pe web



deea originală care a stat la baza creării Internetului<sup>1</sup> a fost dezvoltarea unei biblioteci electronice pentru accesul și distribuirea ușoară a informațiilor<sup>2</sup>. În multe privințe, acest obiectiv a fost realizat: astăzi Internetul funcționează ca o bibliotecă enormă în care sunt prezente majoritatea bibliotecilor publice și private din întreaga lume. Acestea oferă informații despre servicii, programe și activități și oferă acces la cărțile fizice listate în cataloage și care pot fi comandate prin Internet. Bibliotecile digitale oferă acces la cărți și colecții online, de obicei digitizate ca html script<sup>3</sup> care le conferă aspectul unei pagini web<sup>4</sup>, a unor documente Word sau PDF<sup>5</sup> sau unui text neformatat (ASCII)<sup>6</sup>. Unele biblioteci și muzee importante vă permit să navigați prin versiunile digitalizate ale cărților rare și ale colecțiilor de artefacte<sup>7</sup>.

1. [http://www.livinginternet.com/i/ii\\_summary.htm](http://www.livinginternet.com/i/ii_summary.htm)

2. [http://www.livinginternet.com/i/ii\\_summary.htm](http://www.livinginternet.com/i/ii_summary.htm)

3. <https://en.wikipedia.org/wiki/HTML>

4. <http://en.wikipedia.org/wiki/Html>

5. <http://www.census.gov/main/www/pdf.html>

6. <http://en.wikipedia.org/wiki/ASCII>

7. <http://www.bl.uk/manuscripts/Default.aspx>

De asemenea, Internetul depășește cadrul bibliotecilor în oferirea de informații și poate furniza informații actualizate și de încredere potrivit intereselor dumneavoastră: problemele actuale, tehnologii, hobby-uri, divertisment, artă, sport și multe altele. Aceste informații sunt disponibile într-o gamă largă de surse, inclusiv canalele de știri de 24 de ore<sup>8</sup>, ziare<sup>9</sup>, jurnale<sup>10</sup> și agregatoare de știri, cunoscute sub numele de fluxuri de știri sau fluxuri RSS (*rich site summary*, a se vedea <[www.whatisrss.com](http://www.whatisrss.com)>) și acestea pot fi accesate prin intermediul numeroaselor site-uri web și platforme sociale. Utilizatorii se abonează la acestea pentru a primi, periodic, cele mai recente conținuturi web agregate de la ziarele, blogurile, podcast-urile și blogurile video (vlogurile) din mediul online, într-un singur loc, pentru o vizualizare ușoară.

În prezent, mulți europeni urmăresc știrile naționale și internaționale prin intermediul Internetului și îl folosesc pentru a găsi informații despre sănătate. Aflarea știrilor prin intermediul platformelor sociale este, de asemenea, o tendință în creștere. Forumurile și grupurile de discuții constituie platforme eficiente pentru discuții și reprezintă un mijloc de a identifica perspective multiple asupra problemelor de actualitate, contribuind, de asemenea, la fortificarea competențelor de dezbateri ale elevilor. Există sute de mii de astfel de forumuri în întreaga lume, iar grupurile mai active primesc zilnic sute de mesaje noi. Mesajele sunt împărțite în teme de discuții, care înregistrează și afișează numele expeditorului și ora la care a fost trimis mesajul. Actualmente, majoritatea serverelor și a browserelor vă pot îndruma către forumuri care ar prezenta interes pentru elevii dumneavoastră<sup>11</sup>.

Twitter este un alt mijloc de a obține actualizări ale informațiilor de pe Internet. Puteți utiliza propria adresă Twitter pentru a urmări posturile de știri, jurnaliștii și experții din domeniile care vă interesează sau puteți să vă înscrieți pe o listă de Twitter pentru a putea urmări în mod anonim<sup>12</sup>. Alertele Google pot fi utilizate, în mod similar, pentru a urmări știri pe teme specifice, dar dacă termenii cheie nu sunt definiți atent și clar, este posibil să primiți prea multe alerte pentru ca acestea să mai fie utile. Platformele sociale adaugă, în mod progresiv, noi funcții pentru a vă ține la curent și cu știrile la nivel global.



## IMPORTANȚA ÎN EDUCAȚIE

- Competențele de cercetare necesare pentru a naviga prin bibliotecile tradiționale, cât și cele online, sunt similare. Este esențial ca copiii să fie ghidați de părinții și cadrele lor didactice pentru a învăța și a exersa aceste competențe încă de la primii lor pași pe Internet.
- Există mii de biblioteci pe web specifice unei anumite categorii, ce pot fi găsite la adresa <<http://vlib.org/>> și <<http://www.sldirectory.com/libsf/resf/libplans.html>> care se referă la ariile și tematicile curriculare. „În esență, webquest-urile (activitate centrată pe căutarea informațiilor pe web de către elevi) sunt mini-proiecte în care un procent mare al informației și materialului este furnizat de Internet. Webquest-urile pot fi inițiate de cadrele didactice sau de elevi, în funcție de activitatea de învățare stabilită de profesor.”<sup>13</sup> Modelul prezentat la adresa <<http://webquest.org/>> poate fi foarte util atunci când se creează activități pentru ca participanții din clasă care vor folosi biblioteci online, în timp ce dezvoltă o serie de competențe fundamentale, precum cercetarea, arhivarea, citirea și scrierea, analiza și evaluarea.
- Grupurile de discuții și forumurile de discuții reprezintă o resursă utilă pentru dezvoltarea gândirii critice și a abilităților de dezbateri, cu condiția ca tinerii să fie încurajați să își verifice faptele prin consultarea unei varietăți mari de surse. Acestea pot, de asemenea, oferi o platformă pentru partajarea de informații și pentru a învăța din experiența altora.

8. [http://wwitv.com/news\\_tv\\_live/](http://wwitv.com/news_tv_live/)

9. <http://www.onlinenewspapers.com>

10. <http://www.e-journals.org>

11. <http://www.newsforum.com>

12. <https://en.wikipedia.org/wiki/Twitter>

13. <https://www.teachingenglish.org.uk/article/webquests>





## CONSIDERAȚII DE ORDIN ETIC ȘI RISCURI

- Cookie-urile (fișierele mici lăsate pe dispozitivul dumneavoastră online pentru a stoca informații despre dumneavoastră și preferințele dumneavoastră) vă pot îmbunătăți experiența de navigare, prin memorarea preferințelor sau prin evitarea înregistrării dumneavoastră de fiecare dată când vizitați anumite site-uri. Cu toate acestea, prin utilizarea cookie-urilor, motoarele de căutare vă vor direcționa numai către site-uri asemănătoare și ar putea să vă îngusteze treptat perspectiva asupra știrilor și a problemelor de actualitate.
- Internetul a democratizat jurnalismul, oferind oamenilor de toate vârstele posibilitatea de a contribui activ la conținut. Prin urmare, oferta de informații pe Internet devine nelimitată, subliniind mai mult ca niciodată importanța deosebirii dintre conținutul de calitate și cel care nu este de încredere, precum și dintre informație și info-reclamă, cu alte cuvinte, publicitatea care arată ca o informație obiectivă.
- Foarte puține grupuri sau forumuri de discuții sunt pe deplin moderate, prin urmare, utilizatorii nu sunt monitorizați constant. În rezultat, acestea pot fi exploatare pentru activități ilegale, cum ar fi distribuirea de materiale protejate prin drepturi de autor, propaganda rasistă, materialele extremiste sau privind exploatarea sexuală a copiilor. Utilizarea unor astfel de platforme necesită un anumit sentiment de responsabilitate și conștientizare a convențiilor sociale acceptabile, deoarece presupusa anonimitate pe care o pot oferi poate conduce la o conduită antisocială, cum ar fi postarea de mesaje răutăcioase și ostile (*flaming*) sau bullying-ul<sup>14</sup>. Elevii ar trebui, de asemenea, să fie îndrumați să reflecteze asupra aspectelor ce țin de viața privată atunci când utilizează astfel de forumuri<sup>15</sup>.
- Majoritatea bibliotecilor vor oferi acces conform anumitor reguli. Potrivit regulilor<sup>16</sup> utilizatorul va trebui să respecte criteriile de protejare a drepturilor de autor ale materialului. Rețineți faptul că, cu excepția cazului în care materialele aparțin domeniului public, nu aveți dreptul să le redistribuiți sau să le publicați fără permisiunea editorului. Drepturile de autor sunt, de asemenea, o responsabilitate personală. Plagiatul reprezintă utilizarea muncii altcuiva fără a credita sursa. Asigurați-vă că ați acordat credit surselor dumneavoastră și insuflați acest obicei elevilor dumneavoastră.



## INSTRUCȚIUNI

- Usenet<sup>17</sup> este un sistem de discuții distribuit la nivel mondial, care constă dintr-un set de „grupuri de știri” / newsgroup-uri care sunt clasificate ierarhic în funcție de subiect. Accesul la aceste grupuri este definit de prestatorul dumneavoastră de servicii internet (PSI) sau de serverul<sup>18</sup> școlii, universității sau afacerii dumneavoastră. Accesul la anumite platforme este gratuit, în timp ce serviciile „premium” funcționează pe bază de abonament.
- Există multe instrumente pentru configurarea unei știri sau a unui flux RSS. Videoclipul „Get organized: streamline your newsfeeds”<sup>19</sup> oferă o descriere pas cu pas a modului în care puteți utiliza instrumentele care se potrivesc cel mai bine necesităților dumneavoastră.
- Pentru a configura alertele Google, trebuie mai întâi să creați un cont Google. Puteți introduce apoi o listă de cuvinte, puteți seta câțiva alți parametri și alerta Google vă va informa prin email sau feed atunci când acești termeni apar în mediul online. Veți primi o listă de adrese URL care prezintă actualizări ale termenului dumneavoastră sau puteți adăuga alerta într-un cititor de fluxuri RSS la alegere.

14. <http://en.wikipedia.org/wiki/Flaming>

15. <http://www.webwewant.eu/information>

16. [http://web.archive.org/web/20160102210205/http://www.gallowglass.org/jadwiga/SCA/libraries.html#Copyright\\_\\_Plagiarism](http://web.archive.org/web/20160102210205/http://www.gallowglass.org/jadwiga/SCA/libraries.html#Copyright__Plagiarism)

17. <http://en.wikipedia.org/wiki/Usenet>

18. [https://en.wikipedia.org/wiki/Server\\_\(computing\)](https://en.wikipedia.org/wiki/Server_(computing))

19. <http://web.archive.org/web/20151231202307/http://www.pcmag.com/article2/0,2817,2458165,00.asp>

- Alegeți o temă curentă pe care o studiați, identificați o bibliotecă de o anumită categorie la <<http://vlib.org/>>. Puteți lansa un webquest în jurul resurselor din această bibliotecă sau utilizați un webquest disponibil la adresa <<http://webquest.org/>> și <<http://www.spiritsd.ca/teacherresources/default.asp>>. Puteți găsi și alte webquest-uri utilizând un motor de căutare<sup>20</sup>. Îmbogățiți-vă serviciul webquest prin setarea unei alerte Google sau aderând la o listă de Twitter<sup>21</sup> și comparând calitatea informațiilor pe care le primiți de la fiecare dintre aceste instrumente.
- Adulții, copiii și tinerii pot găsi site-uri web de știri și activități de calitate pe site-ul multilingv al Federației Internaționale a Asociațiilor și Instituțiilor de Biblioteci (*International Federation of Library Associations and Institutions – IFLA*)<sup>22</sup> din Scoția. Acesta oferă o gamă largă de subiecte de la artă și istorie la știință și matematică. Altele sunt disponibile pe „site-uri web grozave pentru copii” (*Great websites for kids*)<sup>23</sup>, dezvoltat de un departament al Asociației Americane de Biblioteci. Mai multe informații despre bibliotecă și serviciile de informare pot fi găsite și pe site-ul IFLA, care este considerat a fi vocea globală a profesiei de bibliotecar și celei de specialist în informații.



## BUNE PRACTICI

- Înainte de a încuraja elevii să utilizeze bibliotecile online, asigurați-vă că revizuiți competențele de documentare și strategiile de cercetare<sup>24</sup>. De asemenea, asigurați-vă că au o înțelegere profundă a protecției dreptului de autor.
- Asigurați-vă că există un filtru antivirus pe toate dispozitivele utilizate pentru descărcarea fișierelor. Înainte de a descărca fișierele<sup>25</sup> pe serverul școlii, verificați cu administratorul rețelei școlii dumneavoastră dacă există o protecție adecvată și un spațiu suficient pentru stocarea fișierelor și arhivarea<sup>26</sup> corespunzătoare a acestora.
- Când setați sarcini de găsim a informațiilor pentru clasa dumneavoastră, este mai bine să oferiți propria listă de URL-uri<sup>27</sup> care să fie utilizate. În acest fel, puteți fi siguri că adresele funcționează și că conținutul este potrivit.
- Multe dintre fișierele pe care le veți descărca vor fi în format Adobe PDF pentru a proteja drepturile de autor. Asigurați-vă că ați descărcat și instalat o versiune recentă a Acrobat Reader pentru ca elevii să poată deschide aceste fișiere. Acest lucru se poate face de pe site-ul Adobe Systems<sup>28</sup>.
- Principiile de bază privind siguranța pe care le aplicați atunci când utilizați Internetul trebuie aplicate și atunci când se utilizează bibliotecile online. Verificați declarațiile de confidențialitate, condițiile de utilizare și scanați fișierele de viruși.
- Când vă alăturați pentru prima dată unui grup de discuții, asigurați-vă că ați verificat întrebările frecvente - FAQ<sup>29</sup> pentru a cunoaște regulile de utilizare. Acest lucru vă va oferi o idee despre neticheta grupului de discuții. Diferite grupuri de discuții au reguli diferite.
- Scrieți mesaje concise, dar asigurați-vă că prezentați toate informațiile relevante. De exemplu, dacă căutați un răspuns la o problemă tehnică, oferiți detalii precise cu privire la echipamentul și programul pe care îl utilizați.

20. [http://en.wikipedia.org/wiki/Search\\_engine](http://en.wikipedia.org/wiki/Search_engine)

21. <https://media.twitter.com/best-practice/create-and-use-twitter-lists>

22. <http://www.ifla.org/activities-and-groups>

23. <http://gws.ala.org>

24. <https://www.pinterest.com/explore/library-skills/>

25. <http://www.walthowe.com/glossary/d.html#download>

26. [http://en.wikipedia.org/wiki/Archiving#Computing\\_sense](http://en.wikipedia.org/wiki/Archiving#Computing_sense)

27. <http://en.wikipedia.org/wiki/URL>

28. <http://www.adobe.com/products/acrobat/readstep2.html>

29. <http://en.wikipedia.org/wiki/Faq>



## INFORMAȚII SUPLIMENTARE

- Grupurile de discuții de pe Google la <http://groups.google.com/> prezintă o listă completă de grupuri de discuții și o arhivă de peste 1 miliard de postări.
- David Lawrence și Russ Allbery oferă sfaturi privind crearea unui grup de discuții Big 8: <http://web.archive.org/web/20140330141231/http://www.faqs.org/faqs/usenet/creating-newsgroups/part1/>.
- Wikipedia are un articol despre grupurile de discuții: <http://en.wikipedia.org/wiki/Newsgroups>.
- Biblioteca Britanică oferă colecții digitalizate: <http://www.bl.uk/manuscripts/Default.aspx>.
- Fundația World e-book oferă mii de texte: <http://www.netlibrary.net/>.
- Library Spot oferă un centru de resurse gratuite al bibliotecilor virtuale: <http://www.libraryspot.com/>.
- „Teacher tap” are o listă de peste o 1000 de webquest-uri și resurse conexe: <http://eduscapes.com/tap/topic4.htm>.
- În publicația pentru adolescenți „The Web We Want” (*Web-ul pe care ni-l dorim*), capitolul „Informația nu este cunoaștere” <http://www.webwewant.eu/web/guest/information> descrie activități interactive pentru adolescenți care pot îmbunătăți gândirea critică și competențele jurnalistice ale acestora.



Fișa 12

## Învățământul la distanță și cursurile online deschise cu participare nelimitată (CODPN-urile)



Învățământul la distanță este un sistem de învățământ formalizat, în care elevii și cadrele didactice nu sunt fizic prezenți împreună într-o clasă. Procesul educațional se desfășoară prin mijloace electronice; deoarece tehnologia a avansat, la fel a evoluat și învățământul la distanță. Acum avem clase virtuale în care elevii și cadrele didactice fac schimb de conținut prin email, mesagerie instantanee, videoconferințe, camere de discuții, buletine de știri și altele.

Indiferent de tehnologia utilizată, învățământul la distanță rămâne o metodă dovedită, care deschide oportunități de învățare pe tot parcursul vieții pentru oamenii din toate țările și de toate vârstele, permițând acestora să obțină diplome, certificate și titluri academice de la aproape orice universitate online din lume. Elevii pot, de asemenea, discuta cu alți elevi sau profesori care se află la sute sau chiar mii de kilometri distanță, fapt ce îmbogățește, cu siguranță, învățarea.

■ Învățământul la distanță a început la mijlocul anilor 1800 cu generații de adulți aflați în căutarea unei educații avansate de acasă, din armată sau de la locul de muncă. Cursurile se făceau prin corespondență, cu materiale trimise de la expeditor la destinatar, prin sistemul poștal tradițional. Actualmente, învățământul la distanță a evoluat, profitând de tehnologia actuală. Aceasta se dezvoltă grație Internetului, iar studenții pot studia pentru obținerea diplomelor universitare fără a călca vreodată într-o sală de curs tradițională.

■ Învățământul la distanță există în prezent în diferite forme, variind de la definiția clasică de mai sus, până la cursurile online deschise cu participare nelimitată (CODPN), de la cursurile de formare și webinarele de la egal la egal de pe YouTube la vizitele virtuale în teren de pe Periscope. Deși tehnologia a progresat rapid, elementele fundamentale ale învățării la distanță rămân aceleași: asigurarea educației.



## TIPURI DE ÎNVĂȚĂMÂNT LA DISTANȚĂ

### CODPN-urile

- CODPN-urile au fost introduse pentru prima dată în 2008, cu scopul de a furniza conținut prin Internet pentru orice persoană care își dorește să urmeze un curs fără limită de participare. Forumurile comunitare interactive au fost create pentru a permite schimburi între elevi/studenți și cadrele didactice.
- Până în 2012, CODPN-urile erau sponsorizate de instituții de învățământ formal, iar universități precum Universitatea Stanford, Universitatea Princeton, Universitatea din Michigan și Universitatea din Pennsylvania erau alinate la Coursera, o companie de tehnologii educaționale cu scop lucrativ.
- Alte programe CODPN de succes includ Udacity, un alt partener al Universității Stanford și edX, un furnizor CODPN fondat de Institutul de Tehnologie din Massachusetts și Universitatea Harvard.
- CODPN-urile se bazează pe un model profesor-student, în timp ce YouTube a creat un alt model de învățare la distanță: de la egal la egal.

### Formarea de la egal la egal

- Formarea de la egal la egal poate fi descrisă ca sesiuni în care oamenii învață de la colegi care vin dintr-un mediu similar. Un exemplu ar putea fi copiii care învață alți copii, avocații care formează alți avocați etc.
- Acest modul de co-învățare este ușor de găsit pe YouTube, unde „profesorii” YouTube cu milioane de abonați oferă tutoriale pentru software, tutoriale pentru design de site-uri web, tutoriale pentru machiaj, scriere și pentru alte mii de lucruri.

### Seminare online (webinare)

- Și webinarele sau seminarele online, se găsesc peste tot pe Internet. Îndrumătorii, educatorii, experții și oricine profesează pentru a împărtăși cunoștințe, poate oferi un seminar online.
- Formatele seminarelor online pot include prezentări, prelegeri, prezentări PowerPoint, videoclipuri, materiale de lucru și multe altele.
- Seminarele online pot include, de asemenea, materiale care pot fi descărcate pentru a fi studiate ulterior.

### Periscope

- Periscope este o aplicație care oferă posibilitatea de a face transmisiuni și permite oamenilor să vadă ceea ce vede un utilizator, în timp real. Aplicația a avut un succes neegalat în primul său an, iar formatorii continuă să identifice și alte modalități de utilizare a acesteia.
- Unii formatori consideră că vizitele virtuale în teren, orele deschise sau primirea în timp real a întrebărilor de la vizualizatori (elevi) ar putea fi utile; totuși, acesta este un instrument de învățare la distanță care va trebui de urmărit pe viitor.

■ Progresele în domeniul învățământului la distanță au revoluționat mediile de învățare, de la învățământul primar la învățământul terțiar. De exemplu:

- Cursurile pot fi transmise prin streaming media<sup>1</sup> sau ca materiale tipărite salvate în fișiere stocate pe serverul formatorului<sup>2</sup>.
- Elevii comunică cu profesorul și între ei prin intermediul forumurilor de mesaje<sup>3</sup>, emailurilor<sup>4</sup> și discuțiilor online<sup>5</sup>.
- Resursele educaționale deschise (open educational resources – OER) sunt documente și mijloace media (de obicei, având licență deschisă) care sunt utile pentru predare, învățare și evaluare, precum și pentru cercetare. OER-urile reprezintă încă un mijloc ce permite cadrelor didactice să utilizeze și să facă schimb de conținut cu alte școli și formatorii de pe toate continentele. OER-urile sunt uneori create de experți care nu sunt cadre didactice și vizează teme specifice. Ele pot fi partajate și selectate cu ușurință prin intermediul unui repozițoriu, ca de exemplu OER Commons<sup>6</sup>.
- Instrumentele menționate anterior au dat naștere așa-numitei „clase inversate”, o strategie de instruire și un tip de învățământ mixt, care inversează tiparul educațional tradițional prin oferirea de conținut instructiv, adesea în mediul online, în afara sălii de clasă și realizarea unor activități, inclusiv a celor care ar fi putut fi, în mod tradițional, considerate teme pentru acasă, în sala de clasă. Pentru mai multe informații suplimentare despre instrumente, accesați Edutopia<sup>7</sup>.
- Elevii pot încărca tema pentru acasă într-un dropbox, care este, de obicei, un serviciu gratuit, în care utilizatorii înregistrați pot păstra fișierele în siguranță, le pot sincroniza și le pot partaja ușor cu oricine aleg. Chiar și testele și examenele pot fi automatizate și luate online.
- Cu CODPN-urile și învățământul la distanță, materialele de curs sunt întotdeauna disponibile și pot fi ușor de actualizat. Mai mult, aceste noi formate de medii de învățare oferă o flexibilitate de neegalat, fapt ce permite oamenilor să lucreze după propriul lor ritm.



## IMPORTANȚA ÎNVĂȚĂMÂNTULUI LA DISTANȚĂ

- Internetul este perfect pentru crearea unui mediu virtual de învățare. Studenții pot, de exemplu, să rămână în orașul lor natal, în timp ce studiază la o universitate virtuală din străinătate sau își partajează timpul de învățare între diferite locuri, de exemplu între o companie și o școală de studii comerciale.
- Asigurarea accesului studenților la întreaga bază de material didactic le oferă posibilitatea de a deveni mai autonomi și de a înțelege mai bine ce și de ce învață.
- Studenții au mai multă responsabilitate față de propria activitatea de învățare, iar rolul profesorului este transformat în rolul unui îndrumător.
- Cursurile nu se limitează la orele de program ale școlilor sau universităților „obișnuite”, astfel încât toată lumea să poată beneficia de mai multe oportunități de a învăța pe tot parcursul vieții.
- Învățarea la distanță schimbă conduita profesorului și a elevului. Elevii/studenții de succes devin mai perseverenți și organizați, iar cadrul didactic trebuie să se familiarizeze mai mult cu tehnologia.



## CONSIDERAȚII DE ORDIN ETIC ȘI RISCURI

### Acreditarea

- Capacitatea de a face distincția între programele acreditate și cele neacreditate este utilă în determinarea legitimității furnizorului de curs.

1. [http://en.wikipedia.org/wiki/Streaming\\_media](http://en.wikipedia.org/wiki/Streaming_media)

2. [http://en.wikipedia.org/wiki/Web\\_server](http://en.wikipedia.org/wiki/Web_server)

3. [https://en.wikipedia.org/wiki/Internet\\_forum](https://en.wikipedia.org/wiki/Internet_forum)

4. <https://en.wikipedia.org/wiki/Email>

5. [https://en.wikipedia.org/wiki/Online\\_chat](https://en.wikipedia.org/wiki/Online_chat)

6. <https://www.oercommons.org>

7. <http://www.edutopia.org/blog/flipped-learning-lets-talk-tech-jon-bergmann>

- Mărcile de acreditare pentru învățământul la distanță<sup>8</sup> apar în multe domenii și reprezintă un pas important în egalarea oportunităților de învățare.
- În cazul în care programele nu au o acreditare reală, dar sunt în parteneriat cu universități bine-cunoscute și consacrate, acestea dețin adesea o formă de validare a calificărilor.

### Cadrele didactice și competențele

- Învățământul la distanță nu schimbă cerința fundamentală de a avea cadre didactice competente. De fapt, mai mult ca niciodată, acesta subliniază necesitatea ca profesorii să aibă mai multe oportunități de formare pentru a ține pasul cu noile tendințe în materie de educație.
- Valoarea învățării față în față nu poate fi negată, dar beneficiile tehnologiei și educației sunt, de asemenea, demne de remarcat.
- Deoarece oricine poate să își lanseze propriul seminar online sau curs online de la egal la egal și chiar să se numească „expert”, gândirea critică este la fel de importantă aici pentru utilizatori, cum este și în cazul altor forme de conținut web.



## INSTRUCȚIUNI

— Ar trebui să fiți conștienți de faptul că dumneavoastră, ca utilizator, sunteți responsabili pentru luarea unor măsuri de precauție atunci când alegeți o universitate sau alt program de învățare la distanță. Iată câteva aspecte de urmărit:

- Rețineți faptul că pe piață există instituții de învățământ la distanță dubioase, alături de cele care sunt recunoscute. Asigurați-vă că ați analizat cu temeinicie un program sau o organizație înainte de a vă înscrie;
- Problemele de securitate sunt întotdeauna importante, ca și în cazul oricărui schimb de informații prin Internet. Virușii (a se vedea Fișa 19 cu privire la securitate) și spărgătorii de coduri<sup>9</sup> pot provoca un dezastru într-un sistem de învățământ la distanță, așadar asigurați-vă că consultați Fișele 9 cu privire la viața privată și 19 cu privire la securitate, pentru a vedea ce măsuri de precauție ar trebui să luați;
- Dreptul de autor<sup>10</sup> este, de obicei, protejat de legislația țării de origine a elevului. Cu toate acestea, atunci când urmați programe de învățare la distanță în alte țări, asigurați-vă că verificați dacă sursele de învățare sunt acoperite de drepturile de autor internaționale.



## IDEI PENTRU LUCRUL ÎN CLASĂ

- Divizați studenții în grupuri a câte doi, un grup fiind „cadru didactic”, iar celălalt fiind „elevul”. Rugați-i să cerceteze un subiect din curs și să explice de ce un tip de învățământ la distanță ar fi mai bun decât altul pentru abordarea sau studiarea subiectului dat.
- Odată ce elevii sunt de acord cu metoda de învățare la distanță și cu un subiect din curs, rugați grupul „cadru didactic” să cerceteze aspectele care ar face acest curs ideal și invitați grupul „elev” să facă același lucru. Faceți o analiză comparativă și contrastivă a nevoilor cadrelor didactice și ale elevilor.
- Alegeți o metodă de învățare la distanță și cercetați sau verificați tipul de certificare disponibil. Este aceasta o instituție respectabilă? Ce indicatori stau la baza renumelui unei instituții? Instituția oferă certificate sau badge-uri (micro-certIFICATE de participare)?

8. <https://wiki.mozilla.org/Badges>

9. [https://en.wikipedia.org/wiki/Hacker\\_\(computer\\_security\)](https://en.wikipedia.org/wiki/Hacker_(computer_security))

10. <http://en.wikipedia.org/wiki/Copyright>

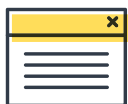


- Discutați despre diferența dintre învățarea cu utilizarea aplicațiilor și învățarea în cadrul cursurilor. Cum ar putea acestea oferi noi oportunități de învățare pentru persoanele cu dizabilități?
- Invitați elevii să își creeze propriul curs de scurtă durată pe un subiect din domeniul preferat și să încurajeze alți elevi să urmeze cursul. Reieșind din această experiență, solicitați clasei să elaboreze o listă de criterii care fac mai eficientă învățarea online.



## BUNE PRACTICI

- Internetul schimbă modul în care învățăm și este foarte important ca elevii să aibă acces la toate informațiile și instrumentele disponibile pentru a-i ajuta să învețe.
- „Diviziunea digitală”<sup>11</sup> este considerată o problemă principală în creșterea economică și socială a multor națiuni, iar utilizarea învățământului la distanță poate reduce acest decalaj. Cu toate acestea, opiniile opuse arată că, dacă există o diviziune digitală și oamenii nu pot accesa Internetul (și învățământul la distanță), decalajul va spori.
- Învățământul la distanță poate îmbunătăți învățarea elevilor/studentilor într-un mod măsurabil. Acesta oferă cursuri de formare pe Internet cu experiență practică pentru elevi/studenti, familiile acestora și cadrele didactice.
- Învățământul la distanță oferă elevilor/studentilor posibilitatea de a-și construi noi competențe și calificări și de a se implica în noi direcții.
- Învățământul la distanță poate oferi, de asemenea, acces elevilor/studentilor cu dizabilități care nu ar fi putut să frecventeze anterior un curs. Elevii/studentii pot să participe la un curs online și să facă schimburi cu alți elevi/studenti și cu cadrul didactic.



## INFORMAȚII SUPLIMENTARE

- Portalul pentru învățământul la distanță oferă informații cu privire la programele și instituțiile de învățământ la distanță din întreaga lume: <http://www.distancelearningportal.com/>.
- Consiliul Internațional pentru învățământul deschis și la distanță oferă informații și resurse despre instituțiile internaționale: <http://www.icde.org/>.
- European Schoolnet, un consorțiu de miniștri ai educației la nivel european, oferă un repozițoriu de OER pentru cadrele didactice: <http://lreforschools.eun.org/web/guest>. De asemenea, acesta oferă resurse educaționale pentru persoanele cu nevoi speciale: <http://lreforschools.eun.org/web/guest/sennet>.

11. [https://en.wikipedia.org/wiki/Digital\\_divide](https://en.wikipedia.org/wiki/Digital_divide)



## Cumpărăturile în mediul online



Comerțul electronic poate fi definit drept colectarea de servicii, programe și proceduri care permit vânzarea de produse în mediul online. Aproape orice se poate achiziționa online: de la cărți până la vacanțe și de la îmbrăcăminte până la electronică. În afară de bunurile materiale, puteți plăti, de asemenea, pentru servicii, cum ar fi accesul la conținutul online.

Comerțul electronic a adus fără îndoială beneficii pozitive deoarece cumpărăturile devin mai ușor de realizat și mai convenabile; cu toate acestea, tranzacțiile de comerț electronic prezintă și anumite riscuri. Și, odată cu creșterea industriei, vor spori și beneficiile, și riscurile.

O tendință recentă arată că tot mai mulți copii efectuează achiziții în mediul online (adesea, prin intermediul cardului de credit al unui părinte) înainte de a atinge vârsta de 18 ani sau chiar înainte de a avea un loc de muncă cu fracțiune de normă, în anii de facultate, de exemplu. Acest aspect a suscit îngrijorări privind „virtualizarea” banilor de către copii, care sunt incapabili să înțeleagă valoarea acestora, fapt ce ar putea avea un impact economic major asupra viitorului lor.



## ACHIZIȚII ÎN CADRUL APLICAȚIILOR

- Achizițiile încorporate în aplicații se referă la capacitatea unui telefon inteligent sau a unui dispozitiv mobil de a facilita vânzarea de produse sau servicii în cadrul unei anumite aplicații<sup>1</sup>.
- În timp ce achizițiile in-apps aduc profit companiilor, acestea pot constitui o problemă pentru cei care nu înțeleg cum funcționează achizițiile încorporate în aplicații.
- Achizițiile in-apps au reprezentat o problemă deosebită pentru consumatorii copii și tineri, care nu sunt eligibili să efectueze achiziții, însă pot face acest lucru cu doar câteva clicuri.



## DREPTURILE CONSUMATORILOR

- În cazul în care achiziționați un produs sau un serviciu în mediul online, beneficiați de reguli de protecție a consumatorului, inclusiv: livrarea în termenul convenit, posibilitatea de a returna bunurile nedorite și de a plăti numai pentru produsele pe care le acceptați, în mod expres, să le achiziționați. De exemplu, în UE aveți dreptul de a returna bunurile nedorite în termen de 14 zile de la primirea acestora.
- În cazul în care achiziționați online un produs sau un serviciu, înainte de a efectua achiziția, vânzătorul trebuie să vă furnizeze anumite informații cheie despre produs sau serviciu, care sunt clare, corecte și ușor de înțeles.
- Pentru o listă a informațiilor cheie, consultați site-urile web ale Uniunii Europene, menționate mai jos.



## IMPORTANȚA ÎNȚELEGERII PROBLEMELOR

- Copiii și tinerii trebuie să fie consumatori bine informați: aceștia trebuie să știe dacă au voie sau nu să efectueze achiziții online, care sunt termenii și condițiile de achiziție și cum să își revendice drepturile în cazul unei probleme. Pe măsură ce achizițiile în mediul online sunt tot mai importante, este vital ca copiii și tinerii să înțeleagă cum să devină consumatori responsabili, capabili să profite de beneficii și să evite riscurile asociate achizițiilor online.
- Cumpărătorii neinformați, în special tinerii și persoanele în vârstă, pot fi vulnerabili la înșelăciunile online și la fraudele legate de achizițiile online.
- În general, în cazul comerțului electronic, cumpărătorii și vânzătorii nu se cunosc reciproc, iar această anonimitate poate desensibiliza oamenii în a face distincția dintre bine și rău.



## CONSIDERAȚII DE ORDIN ETIC ȘI RISCURI

- Protejați-vă datele cardului de credit, numerele de telefon și alte informații de identificare personală. Spărgătorii de coduri pot obține informații despre cardurile de credit prin accesarea computerului dumneavoastră sau prin spargerea site-urilor web nesecurizate, care dețin informațiile dumneavoastră. Fiți precauți în cazul site-urilor web care vă solicită salvarea informațiilor despre cardul dumneavoastră de credit, deoarece aceste informații pot fi furate.
- Evitați plata produselor utilizând o conexiune Wi-Fi publică. Având în vedere ubicuitatea punctelor de acces Wi-Fi din cafenele, hoteluri, aeroporturi și chiar parcuri publice, spărgătorii de coduri pot accesa punctele de acces Wi-Fi și vă pot fura informațiile personale.
- Infracții obțin, de asemenea, informațiile cu privire la cărțile de credit sau bancare păcălind persoanele, astfel încât acestea le oferă de bună voie. Phishing-ul<sup>2</sup> se încadrează în această categorie. Aceste atacuri vizează adesea utilizatorii site-urilor de cumpărături sau de plăți online, care le solicită să „reconfirme” detaliile.

1. <http://www.techopedia.com/definition/27510/in-app-purchasing>  
2. <http://en.wikipedia.org/wiki/Phishing>

- Deoarece cumpărăturile în mediul online implică adesea plățile efectuate prin cardul de credit, consumatorii trebuie să își gestioneze cu atenție finanțele pentru a evita cheltuielile în exces. Verificați, în mod periodic, extrasul cardului dumneavoastră de credit pentru a vă asigura că nu ați efectuat o achiziție nedorită și că nu există achiziții neautorizate.
- Feriți-vă de lucrurile care par „prea bune pentru a fi adevărate”. Accesați site-ul vânzătorului cu amănuntul pentru a confirma dacă oferta este valabilă.
- Metodele de plată prin Internet s-au diversificat: PayPal, Bitcoins, transfer bancar, plăți mobile și altele, dar rețineți că nicio metodă de plată nu este pe deplin sigură, prin urmare, fiți întotdeauna precaut atunci când faceți orice fel de plăți online.



## INSTRUCȚIUNI

— Pentru a face achiziții online în siguranță, consumatorii trebuie să nu uite că achizițiile în mediul online necesită precauții suplimentare.

- Faceți achiziții numai de la furnizori cu renume. Acest lucru poate deveni dificil, pe măsură ce tot mai mulți vânzători intră pe piață, dar... informați-vă.
- Asigurați-vă că parametrii calculatorului, tabletei sau ai telefonului dumneavoastră inteligent sunt setați la optim.
- Verificați ca zona de plată a comenzii să fie criptată. Multe site-uri folosesc tehnologia SSL (*Secure Socket Layer*). Căutați pictograma lacăt și o adresă de site web care indică faptul că aceasta este sigură: „https” în loc de „http”.
- Salvați o copie a comenzii dumneavoastră fie prin imprimarea unei copii, fie prin realizarea unei capturi de ecran. În caz de contestație, veți putea folosi acest lucru drept dovadă.
- Verificați-vă cu regularitate extrasele bancare pentru a vă asigura că nu vi s-au extras bani pentru o achiziție pe care nu ați realizat-o.



## IDEI PENTRU LUCRUL ÎN CLASĂ

- Instruiți elevii că este necesar să afle informații despre vânzătorul cu amănuntul și despre condițiile de vânzare.
- Invitați elevii, singuri sau în grupuri, să caute produse sau servicii pe site-uri comerciale specifice, reieșind dintr-un anumit scop. De exemplu, planificarea unei vacanțe conform unui buget fix (a se vedea Fișa 10 cu privire la căutarea informațiilor).
- Planificați crearea unui site web de comerț electronic cu elevii dumneavoastră (de exemplu, pentru a vinde produse școlare) sau continuați să lucrați la inițiativele de acest tip pe care le aveți deja în cadrul școlii. Studiați structura unui site web de comerț electronic bun.



## BUNE PRACTICI

- Aflați informații despre comerciantul cu amănuntul sau vânzător. De exemplu, eBay permite vânzătorilor să își construiască o reputație în funcție de istoricul și de feedback-ul lor. Nu cumpărați din surse care nu sunt de încredere, în special cele cărora li se face publicitate prin spam (a se vedea Fișa 19).
- Verificați că sunteți asigurat împotriva utilizării frauduloase a cardurilor dumneavoastră de credit. Verificați cu atenție extrasele dumneavoastră de cont pentru a depista orice achiziții neautorizate.
- Citiți termenii și condițiile. Textul poate fi lung și tehnic, dar nu dați clic pe opțiunea „citiți și înțeles” dacă nici nu ați citit și nici nu ați înțeles.

- Verificați costurile ascunse. Acestea pot fi taxe sau costuri de livrare din partea vânzătorului. De asemenea, în cazul în care comandați produse din străinătate, este posibil să fie încasate și taxe vamale.
- Oare site-ul este sigur? Simbolul care reprezintă un lacăt sau o cheie în colțul din dreapta jos al browserului web va indica paginile securizate. Căutați certificatele SSL<sup>3</sup>, care asigură că datele sunt criptate înainte de a fi trimise.
- Asigurați-vă că aveți control asupra datelor dumneavoastră personale și consultați Regulamentul General privind Protecția Datelor pentru o mai bună înțelegere. Acordați atenție căsuțelor aferente opțiunilor comerciantului cu amănuntul de a vă păstra datele sau de a vă contacta în scopuri de marketing.
- Dacă aveți vreo îndoială cu privire la seriozitatea unui site web, nu ezitați să efectuați o cercetare online și să căutați testimoniale, recenzii sau experiențe ale clienților. Site-urile web, cum ar fi Trustpilot, sunt de obicei un bun indicator al seriozității unui site web și al experienței clienților<sup>4</sup>.



## INFORMAȚII SUPLIMENTARE

- Consultați pagina de web a Uniunii Europene privind achizițiile online: [http://europa.eu/youreurope/citizens/shopping/buy-sell-online/rights-e-commerce/index\\_en.htm](http://europa.eu/youreurope/citizens/shopping/buy-sell-online/rights-e-commerce/index_en.htm).
- Explicați elevilor dumneavoastră ce este comerțul online, de exemplu utilizând site-ul Microsoft: <http://web.archive.org/web/20050405134258/http://www.microsoft.com/office/previous/frontpage/columns/edcolumn04.asp>.
- ECC-Net „promovează înțelegerea drepturilor consumatorilor din UE și ajută la soluționarea plângerilor aferente achiziției făcute într-o altă țară a rețelei, în cazul călătoriilor sau al achizițiilor online” [http://ec.europa.eu/consumers/solving\\_consumer\\_disputes/non-judicial\\_redress/ecc-net/index\\_en.htm](http://ec.europa.eu/consumers/solving_consumer_disputes/non-judicial_redress/ecc-net/index_en.htm).
- TrustArc (fostă TRUSTe) este o inițiativă independentă, non-profit, globală, menită să consolideze încrederea în ceea ce privește tranzacțiile online: <https://www.trustarc.com>.
- Site-ul web Europa.eu oferă informații despre achizițiile online pe pagina: [http://europa.eu/youreurope/citizens/consumers/shopping/index\\_en.htm](http://europa.eu/youreurope/citizens/consumers/shopping/index_en.htm).
- Pentru informații cu privire la Regulamentul General privind Protecția Datelor, a se vedea: [http://ec.europa.eu/justice/data-protection/index\\_en.htm](http://ec.europa.eu/justice/data-protection/index_en.htm).
- Paypal oferă sfaturi pentru prevenirea fraudei: <https://www.paypal.com/eBay/cgi-bin/webscr?cmd=p/gen/fraud-tips-buyers-outside>.
- Pentru informații cu privire la Recomandarea OCDE privind protecția consumatorilor în comerțul electronic, adoptată în 2016, a se vedea: <https://www.oecd.org/sti/consumer/ECommerce-Recommendation-2016.pdf>.

3. [http://en.wikipedia.org/wiki/Secure\\_Sockets\\_Layer](http://en.wikipedia.org/wiki/Secure_Sockets_Layer)

4. <https://www.trustpilot.com/>

## 4. Internetul – Pentru toată lumea

---

”Creativitatea necesită curajul de a renunța la certitudini.”

*Erich Fromm, psiholog*

### LISTA DE VERIFICARE PENTRU FIȘA 14 – VIDEOCLIPURILE, MUZICA ȘI IMAGINILE PE INTERNET

---

Verificați licența oricărui conținut pe care doriți să îl reutilizați.

Utilizați clasificarea Creative Commons pentru conținutul pe care îl creați și postați în mediul online.

Sprrijiniți modelele de afaceri echitabile din mediul online, care vă permit să plătiți pentru conținut de la artiștii, muzicienii sau creatorii dumneavoastră de conținut preferați.

### LISTA DE VERIFICARE PENTRU FIȘA 15 – CREATIVITATEA

---

O imagine valorează cât o mie de cuvinte, mai ales dacă nu suntem atenți la informațiile noastre confidențiale și la cele ale altora.

Știți cum să vă asigurați că proprietatea dumneavoastră asupra producției creative este respectată de ceilalți?

Plagiatul demonstrează lipsa de respect față de proprietatea creativă și poate avea impact major asupra multiplelor aspecte ale societății. Sunteți conștient de multiplele moduri în care plagiatul poate avea implicații asupra societății?

### LISTA DE VERIFICARE PENTRU FIȘA 16 – JOCURILE

---

Echilibrul de viață este important: timpul pe care îl petreceți în mediul online, jucând, vă afectează activitățile în aer liber și interpersonale?

Atunci când jocurile pe care le jucați în mediul online au ca rezultat comunicarea cu străinii, nu uitați că oamenii nu sunt întotdeauna ceea ce pretind a fi. Alegeți jocuri cu „moderator uman” sau jocuri cu „discuții în condiții de siguranță” pentru copiii foarte mici prin intermediul expresiilor pre-selectate.

În anumite jocuri, achizițiile in-app pot constitui o capcană pentru persoanele care nu sunt precaute. Ați verificat recomandările din Fișa 13?

### LISTA DE VERIFICARE PENTRU FIȘA 17 – CETĂȚENIA DIGITALĂ

---

Vă cunoașteți drepturile și responsabilitățile în mediul online?

Cât de recent ați verificat amprenta digitală? Introduceți numele dumneavoastră într-un motor de căutare și vedeți ce descoperiți.

Care sunt competențele digitale necesare pentru a deveni pe deplin un cetățean digital?

### LISTA DE VERIFICARE PENTRU FIȘA 18 – PARENTAJUL DIGITAL: POZITIV ȘI PROACTIV

---

Fiți pozitivi în relația părinte-copil în această nouă epocă digitală și depuneți toate eforturile pentru a comunica cu copilul dumneavoastră despre ceea ce face în mediul online, ce site-uri vizitează în mediul online și cu cine vorbește în mediul online.

Înțelegeți, deși tehnologia a avansat în salturi, parentajul rămâne, în linii generale, același: să rămâneți activi în viața copiilor dumneavoastră, încurajându-i să fie buni cetățeni (digitali) și punând accent pe bunătate și empatie.

Indiferent dacă sunteți părintele unui copil de doi ani sau a unui adolescent, fiți conștient de marile provocări induse de tehnologii, care ar putea apărea în parcursul de dezvoltare al copilului dumneavoastră. Utilizați tehnologia în așa fel, încât aceasta să sprijine dezvoltarea copilului dumneavoastră, nu să-l împiedice.





Fișa 14

## Videoclipurile, muzica și imaginile pe Internet



Internetul, ca platformă multimedia, oferă un număr mare de moduri de comunicare, inclusiv schimbul de fișiere audio și video și fotografii digitale. Aplicațiile și platformele online au facilitat în mare măsură generarea și difuzarea acestui tip de conținut, depășind barierele lingvistice, culturale și naționale și ridicând probleme importante, referitoare nu numai la dezvăluirea informațiilor personale (a se vedea Fișa 9 cu privire la confidențialitate), ci și la încălcarea drepturilor de autor și la conținutul ilegal sau dăunător.



### DREPTURILE DE AUTOR

- Acest domeniu este expus într-un număr de legi și acorduri internaționale în vigoare. În 1996, peste 100 de țări au semnat două tratate ale Organizației Mondiale a Proprietății Intelectuale (OMPI), vizând abordarea conținutului digital<sup>1</sup>.
- A creator of audio-visual material automatically has copyright unless he or she waives it.

1. <http://www.wipo.int/treaties/en/>

- Un creator de material audio-vizuale se bucură, în mod automat, de drepturi de autor, cu excepția cazului în care renunță la acestea.
- Legile majorității țărilor mențin drepturile de autor timp de 50-70 de ani după moartea creatorului.
- În cazul unei piese muzicale, de obicei, există, mai mulți proprietari de drepturi de autor. Autorul, artistul interpret, compania de înregistrări și editorul pot deține cu toții drepturile sau „drepturile conexe”.
- În afară de aspectul economic, un creator de conținut audio-vizual are „drepturi morale”<sup>2</sup>. Aceasta se referă la dreptul de a fi recunoscut în calitate de creator și dreptul ca lucrarea să nu fie modificată sau editată fără permisiune.
- Muzica și filmele pot fi achiziționate online (a se vedea Fișa 13 cu privire la cumpărăturile online). Există multe site-uri pentru achiziția online de muzică, de exemplu, iTunes<sup>3</sup> și Amazon<sup>4</sup>. Dar există și multe alte magazine online pentru achizițiile de muzică, imagini sau videoclipuri, deci nu ezitați să le găsiți.
- Achiziționarea de muzică sau filme online oferă, de obicei, un drept limitat sau niciun drept de a le copia sau distribui. De exemplu, magazinul online de muzică iTunes de la Apple permite ca o piesă muzicală achiziționată să fie autorizată pentru până la cinci calculatoare per gospodărie<sup>5</sup>.
- Odată cu modificarea consumului de conținut multimedia, apar noi modele de afaceri. În locul achiziției unei melodii, se poate, de asemenea, plăti o taxă lunară de abonament pe o platformă de transmitere online și se poate asculta orice melodie sau viziona orice film disponibil pe respectiva platformă. Exemple de astfel de servicii sunt Netflix<sup>6</sup> pentru filme și Spotify<sup>7</sup> pentru muzică. Din nou, există multe alte platforme, deci nu ezitați să le căutați.
- Industria muzicală a inițiat proceduri juridice atât împotriva companiilor de programe de la egal la egal (P2P), cât și împotriva distribuitorilor de fișiere individuale. Un utilizator care a încărcat fișiere – o persoană care pune la dispoziție fișiere – are mai multe șanse de a fi urmărită penal, decât o persoană care descarcă fișiere.
- Creative Commons<sup>8</sup> este o organizație non-profit care oferă o alternativă la dreptul de autor integral.



## CONSIDERAȚII DE ORDIN ETIC ȘI RISCURI

- În prezent, vânzările de muzică digitală reprezintă 46% din vânzările totale ale industriei de înregistrări, cu o creștere de 6,9% în anul 2014. Acest lucru se datorează creșterii numărului de puncte autorizate pentru vânzarea sau difuzarea muzicii digitale (a se vedea <http://www.ifpi.org/facts-and-stats.php>).
- Industria muzicală a răspuns, de asemenea, pirateriei, intentând o serie de procese împotriva site-urilor web și a utilizatorilor individuali.
- Utilizarea programului de la egal la egal<sup>9</sup> poate reprezenta un risc de securitate pentru calculatorul dumneavoastră, deoarece codurile ostile (*malware*) sunt adesea distribuite prin anexarea acestora la fișiere de muzică și imagini.
- Consumul de conținut multimedia s-a modificat considerabil o dată cu Internetul. În locul ascultării la nesfârșit a aceluiași CD preferat, utilizatorii de Internet preferă să asculte o mare varietate de cântece și melodii, având în vedere opțiunile vaste pe care le oferă Internetul. De exemplu, un american ascultă zilnic trei ore și jumătate de muzică<sup>10</sup>.

2. [https://en.wikipedia.org/wiki/Moral\\_rights](https://en.wikipedia.org/wiki/Moral_rights)

3. <http://www.apple.com/itunes/>

4. <http://www.amazon.com/>

5. <http://www.apple.com/itunes/overview/>

6. <https://www.netflix.com>

7. <https://www.spotify.com>

8. <http://creativecommons.org/>

9. <https://en.wikipedia.org/wiki/Peer-to-peer>

10. [http://www.digitalstrategyconsulting.com/intelligence/2014/10/us\\_media\\_consumption\\_trends\\_music\\_tops\\_the\\_charts.php](http://www.digitalstrategyconsulting.com/intelligence/2014/10/us_media_consumption_trends_music_tops_the_charts.php)

În mod ironic, pirateria a contribuit la forțarea industriei în a revizui modelul „tradițional” de cumpărare a unui album complet și a opta pentru platformele de streaming nelimitat pe bază de abonament. Rețineți faptul că prin deciziile pe care le luați în alegerea unei platforme de streaming, sprijiniți modelul de afaceri al acesteia.



## EDUCAȚIA

— În anumite cazuri, instituțiile de învățământ sunt autorizate să reproducă lucrări și să le comunice publicului. Consultați legislația dumneavoastră națională sau Directiva 2001/29/CE a Uniunii Europene din 22 mai 2001 privind armonizarea anumitor aspecte ale dreptului de autor și drepturilor conexe în societatea informațională. Următoarele condiții trebuie respectate:

- ▶ Lucrările trebuie să fie utilizate exclusiv pentru scopuri didactice sau de cercetare științifică.
- ▶ Trebuie indicată sursa, inclusiv numele autorului – cu excepția cazurilor în care acest lucru este imposibil.
- ▶ Utilizarea acestui conținut nu trebuie să aducă niciun beneficiu economic sau comercial direct sau indirect.

— Înainte de a publica fotografii cu copii sau tineri în mediul online, obțineți permisiunea scrisă din partea părintelui sau a tutorelui.

— În cazul conținutului publicat pe site-ul web al școlii, tot conținutul, inclusiv conținutul provenit de la copii și tineri, se află sub autoritatea și responsabilitatea școlii.



## ÎN CLASĂ

- Inițiați o discuție cu privire la aspectele morale. Pirateria materialelor audiovizuale constituie un furt?
- Informați copiii și tinerii despre riscurile prezentate de viruși și programele spion în cazul descărcărilor.
- Informați copiii și tinerii despre existența amenzilor în cazul descărcării de piese muzicale și filme protejate prin drepturi de autor.
- Rugați copiii și tinerii să producă o lucrare artistică/creativă în echipe. Aceasta poate fi scrierea unei poezii, desenarea unei imagini, scrierea unei povestiri, producerea unui videoclip sau compunerea unei melodii. Solicitați-le să examineze licențele Creative Commons și să aleagă tipul de licență pe care doresc să o aplice conținutului lor. Când sunt gata, rugați-i să vorbească despre decizia privind licența aleasă și motivul alegerii: de exemplu, au ales să aibă o licență foarte restrictivă deoarece intenționează să își vândă creația sau sunt deschiși oricăror modificări și reutilizări și înțeleg pe deplin că munca lor ar putea fi reutilizată sau transformată de altcineva.



## CONȚINUTUL ILEGAL

- Definiția conținutului ilegal variază de la o țară la alta, dar se referă cel mai frecvent la pornografia infantilă sau la abuzul asupra copiilor, violența extremă, extremismul politic, defăimarea sau incitarea la ură împotriva grupurilor minoritare.
- Multe țări au o linie telefonică pentru raportarea conținutului ilegal. INHOPE<sup>11</sup> este o rețea de linii telefonice de urgență la nivel național.
- Luarea de măsuri împotriva conținutului ilegal poate fi dificilă sau lentă, în funcție de natura conținutului și de locul în care acesta este găzduit. Liniile telefonice de urgență colaborează cu prestatorii de servicii Internet (PSI) și cu poliția și dețin pârghiile pentru a aborda conținutul ilegal.

11. <http://www.inhope.org/gns/home.aspx>

- Majoritatea platformelor online utilizează o varietate de metode pentru identificarea și eliminarea conținuturilor ilegale, de exemplu, prin utilizarea tehnologiei de moderare umană și/sau automatizată, tehnologia ADN-ului foto/video și a mecanismelor de raportare.



## CONSIDERAȚII DE ORDIN ETIC ȘI RISCURI

- Conținutul ilegal este, fără îndoială, o infracțiune mult mai gravă decât încălcarea dreptului de autor. Deși există noțiuni precum „utilizarea corectă” în ceea ce privește dreptul de autor și excepțiile în scopuri nonprofit sau educaționale, conținutul ilegal va fi întotdeauna tratat ca o infracțiune gravă, în special când este vorba de materialele privind abuzul sexual asupra copiilor sau terorismul. În timp ce testarea limitelor diferitelor libertăți, cum ar fi libertatea de exprimare, este o trăsătură firească a ființelor umane, în special în cazul copiilor și tinerilor, există anumite limite care nu trebuie depășite niciodată.
- Conținutul ilegal este adesea asociat altor activități ilegale, cum ar fi vânzarea de arme ilegale sau de droguri. O mare parte a acestei activități are loc pe „darknet” (Internetul întunecat), o parte a Internetului care nu este accesibilă prin intermediul motoarelor de căutare tradiționale. Prin urmare, publicarea, partajarea sau căutarea de conținuturi ilegale ar putea duce cu ușurință la infracțiuni foarte grave.
- Școala sau compania dumneavoastră ar trebui să aibă o politică de utilizare acceptabilă (PUA) sau, ca alternativă, o politică de utilizare responsabilă (PUR), care include aspecte privind drepturile de autor și materialele ilegale.
- Ori de câte ori găsiți conținut online pe care doriți să îl utilizați, asigurați-vă că verificați licența. Există mai multe tipuri de licențe. Conținutul produs de internauți are o varietate de licențe. Licența cea mai „deschisă” vă autorizează să refolosiți și să modificați conținutul fără a fi nevoie să notificați proprietarul, chiar și în proiecte comerciale. Alte licențe solicită recunoașterea meritului, limitând utilizarea pentru non-profit sau interzicând orice modificări. Motoarele de căutare, cum ar fi Google sau Bing, propun filtrarea pe bază de licență a căutărilor de imagini și video. De asemenea, există multe platforme de pe care puteți cumpăra conținut care să îl utilizați în cadrul proiectelor dumneavoastră.
- Asigurați-vă că aplicați o licență de drepturi de autor pentru materialele dumneavoastră. Puteți alege între un drept de autor mai tradițional, cum ar fi o companie de înregistrări sau puteți utiliza clasificările Creative Commons<sup>12</sup> pentru materialul pe care îl creați, pentru a elucida modul în care acesta poate fi utilizat de alții.
- Deși poate fi tentant să căutați muzică, imagini sau videoclipuri „gratuite” online, nu uitați că, într-un fel sau altul, într-un final, întotdeauna veți plăti pentru acesta prin faptul că veți fi atacat la nesfârșit de publicitate, vi se va infecta calculatorul cu coduri ostile, care vă pot fura datele sau chiar veți fi dat în judecată de titularii de drepturi. Platformele de suport care oferă servicii bune și un bun raport calitate-preț contribuie la modelarea eficientă a Internetului, evitând invadarea acestuia de publicitatea care irosește timpul, de conținut de slabă calitate sau dăunătoare și recompensează artiștii pentru munca lor la justa valoare.
- Actualmente, conținutul este produs masiv în fiecare zi de utilizatori din întreaga lume: clipuri postate pe o platformă de transmisie video, cum ar fi YouTube sau Dailymotion, fotografii și imagini postate pe rețelele sociale sau muzică încărcată pe platformele de difuzare de muzică. Indiferent dacă utilizatorul care le-a încărcat a specificat sau nu o licență, nu uitați că orice conținut încărcat este protejat. Legea cu privire la drepturile de autor nu este aplicabilă numai în cazul în care autorul a menționat expres că renunță la orice drepturi cu privire la conținutul pe care l-a produs.

12. <http://creativecommons.org/>

- O altă limită în ceea ce privește utilizarea conținutului o constituie protecția datelor. Repostarea unui videoclip sau a unei imagini jenante, de exemplu, reprezintă o încălcare a confidențialității datelor unui alt utilizator și ar putea constitui cyberbullying. Ca regulă generală, întrebați întotdeauna utilizatorul care a postat conținutul inițial, dacă îl puteți reutiliza, modifica, re-posta etc. Solicitarea permisiunii și recunoașterea meritului cuvenit este mai mult decât o obligație juridică; aceasta contribuie la crearea unui mediu mai pozitiv și mai atrăgător în ceea ce privește creativitatea și participarea online. Pentru informații mai detaliate cu privire la protecția datelor, vizitați site-ul Justiției UE referitoare la „Reforma normelor UE privind protecția datelor”<sup>13</sup>.



## BUNE PRACTICI

- Filtrele programelor pot ajuta la blocarea unor site-uri ilegale, dar nu sunt niciodată o soluție reală. Niciun filtru nu vă poate proteja în cazul în care căutați, proactiv, conținuturi ilegale.
- Ca părinte, cadru didactic sau frate/soră mai mare, asigurați-vă că inițiați discuții în familie și în clasă despre experiențele online. Conținuturile ilegale nu reprezintă doar o problemă de drepturi de autor. Deseori, acestea vizează conținuturi dăunătoare sau șocante, coduri ostile, mesaje comerciale nesolicitate și altele similare.
- Raportați conținutul ilegal la o linie telefonică de urgență (a se vedea INHOPE de mai jos) sau utilizați mecanismele de raportare furnizate de platforma pe care o utilizați.
- Asigurați-vă că școala dumneavoastră are o politică strictă în ceea ce privește conținutul ilegal și că copiii și tinerii sunt informați corespunzător despre posibilele consecințe ale publicării, partajării sau vizualizării conținutului ilegal.
- Discutați despre conținutul dăunător și ilegal. Sondajele arată că mulți copii și tineri găsesc acest tip de conținut pe Internet, deliberat sau accidental, dar puțini dintre aceștia comunică faptul dat unui adult.



## INFORMAȚII SUPLIMENTARE

- Visit the World Intellectual Property Organisation (WIPO) website for more information on copyright and related issues: <http://www.wipo.int>.
- Vizitați pagina web a Organizației Mondiale a Proprietății Intelectuale (OMPI) pentru mai multe informații despre drepturile de autor și problemele conexe: <http://www.wipo.int>.
- Aflați care este părerea grupului muzical preferat al dumneavoastră despre pirateria muzicală accesând „Artiștii vorbesc răspicat despre pirateria muzicală”: <https://www.upvenue.com/article/1590-musician-stances-on-music-piracy.html>.
- INHOPE este rețeaua de linii telefonice de urgență pentru raportarea conținutului ilegal pe Internet: <http://www.inhope.org/gns/home.aspx>.
- Pagina media a Consiliului Europei conține informații despre activitatea sa în domeniul dreptului de autor: <http://www.coe.int/media>.
- Pagina web a Comisiei Europene oferă informații privind drepturile de proprietate intelectuală: [http://europa.eu/youreurope/business/start-grow/intellectual-property-rights/index\\_en.htm](http://europa.eu/youreurope/business/start-grow/intellectual-property-rights/index_en.htm).
- IFPI, care reprezintă industria înregistrărilor la nivel mondial, oferă un ghid pentru părinți și cadrele didactice pentru a ajuta la explorarea sigură și autorizată a muzicii pe Internet: <http://www.ifpi.org/music-and-the-internet-guide.php>.
- Agenda digitală europeană a Comisiei Europene oferă consultanță suplimentară privind drepturile de autor: <https://ec.europa.eu/digital-agenda/en/copyright>.

13. [http://ec.europa.eu/justice/data-protection/reform/index\\_en.htm](http://ec.europa.eu/justice/data-protection/reform/index_en.htm)

- A se vedea pagina Wikipedia pentru mai multe informații despre Internetul întunecat: <https://en.wikipedia.org/wiki/Darknet>.
- Articolele relevante din Convenția ONU cu privire la drepturile copilului:
  - Articolul 13** – Copiii au dreptul de a obține și difuza informații, cu excepția cazului când acest fapt ar leza drepturile altora.
  - Articolul 17** – Copiii au dreptul la informații de încredere din partea mass-media. Televiziunea, radioul și ziarele trebuie să ofere informații pe înțelesul copiilor și care nu dăunează bunăstării acestora.
  - Articolul 33** – Guvernul trebuie să ia măsuri pentru a proteja copiii împotriva drogurilor periculoase.
  - Articolul 34** – Guvernul se angajează să protejeze copiii contra oricărei forme de abuz sexual.
  - Articolul 36** – Copiii trebuie protejați împotriva oricăror activități care le-ar putea afecta bunăstarea.
  - Articolul 37** – Nici un copil nu trebuie supus pedepselor crude sau violente. Copiii care încalcă legea nu trebuie supuși tratamentelor crude. În caz de privare de libertate, aceștia vor fi deținuți separat de adulți și le va fi asigurat dreptul de a păstra legătura cu familiile lor.
  - Articolul 40** – Copiii care sunt acuzați de încălcarea legii au dreptul la asistență juridică și tratament echitabil într-un sistem de justiție care le respectă drepturile. Guvernele trebuie să stabilească o vârstă minimă sub care copiii nu pot fi trași la răspundere penală și să ofere garanții minime pentru corectitudinea și soluționarea rapidă a procedurilor judiciare sau alternative.

## Creativitatea



### CUM PROMOVEAZĂ INTERNETUL CREATIVITATEA?

- Din cauza naturii flexibile a Internetului, configurația actualelor săli de clasă este mai puțin rigidă decât oricând. Tehnologia care evoluează rapid oferă elevilor oportunitatea enormă de a explora subiecte care îi interesează și de a învăța în moduri netradiționale (a se vedea Fișa 3 cu privire la Web 2.0, 3.0 și alte versiuni).
- Utilizând instrumentele oferite de tehnologia modernă, elevii pot crea materiale de tip profesional, care pot fi publicate pentru audiențele de oriunde în lume. Aceștia își pot produce propriile produse online și pot efectua experimente și simulări de tot felul în clasă sau de o manieră interactivă, împreună cu alți elevi, pe Internet.
- Internetul a globalizat educația și oferă elevilor oportunitatea de contacta colegi din întreaga lume în timp real. Pentru a exploata pe deplin aceste oportunități, este important ca tinerii inter-nauți să devină creatori și nu doar consumatori, un obiectiv care stă la baza numeroaselor inițiative

de codificare (de exemplu, a se vedea <<http://codeweek.eu>>) care în prezent sunt puse în aplicare în multe țări.



## CONSOLIDAREA PROCESELOR CREATIVE ÎN ÎNVĂȚĂMÂNT

- Integrarea reușită a tehnologiei în sala de clasă oferă elevilor șansa de a-și arăta inovația, individualitatea și creativitatea și de a-și dezvolta capacitățile de antreprenori.
- Utilizarea programelor de creativitate și a Internetului stimulează motivația și îmbunătățește semnificativ învățarea nu doar în sala de clasă, ci și în afara ei. Codificarea ajută la dezvoltarea unei înțelegeri mai profunde a modului în care funcționează tehnologia și prin urmare, poate contribui la apariția unor strategii mai responsabile ale utilizatorilor.
- Posibilitatea de a-și exprima creativitatea și de a-și asuma un rol mai activ în procesul de învățare încurajează implicarea și participarea, două elemente esențiale ale cetățeniei.
- Internetul și tehnologia mobilă oferă o multitudine de posibilități interesante pentru cadrele didactice și elevi, pentru ca aceștia să își creeze și încarce propriul conținut audio-vizual. Aceștia pot, de asemenea, utiliza Internetul pentru a contacta artiștii din întreaga lume, pentru a le cere sfaturi și opinii despre munca lor. Artiștii pot utiliza instrumente de videoconferință<sup>1</sup> și întâlniri virtuale (a se vedea Fișa 12 cu privire la învățământul la distanță) pentru a organiza ateliere de lucru.
- Utilizarea rețelelor sociale<sup>2</sup> și a platformelor sociale dedicate<sup>3</sup> în clasă, încurajează elevii să lucreze împreună, colaborând online pe proiecte comune. Aceasta reprezintă o nouă activitate creativă, iar schimbul de idei poate stimula procesul creativ.



## CONSIDERAȚII DE ORDIN ETIC ȘI RISCURI

- **Aspecte legate de echitate:** toată lumea dispune de echipamentele și conexiunile necesare pentru a accesa Internetul? Toți copiii și tinerii din întreaga lume, indiferent de vârstă, capacitate sau nevoi speciale, sunt capabili să beneficieze de șanse egale de a fi creativi și anume, de a folosi toate tehnologiile disponibile pentru a fi creativi?
- **Factorul de siguranță în mediul online:** Filtrele<sup>4</sup>, create pentru a proteja utilizatorii tineri, în special copiii foarte mici și cei cu nevoi educaționale speciale, împiedică în orice fel accesul la materialul necesar pentru a fi creativi? Ce se poate de făcut pentru ca elevii să poată beneficia de acces sigur la conținutul de care au nevoie (a se vedea Fișa 20 cu privire la etichetare și filtrare).
- **Posibilități de formare pentru cadrele didactice:** elevii pot fi de multe ori mult mai abili decât profesorii lor la utilizarea Internetului. Cadrele didactice trebuie să beneficieze de mai multe oportunități de formare pentru a ghida corespunzător elevii în toate aspectele aferente TIC, inclusiv utilizarea telefonului mobil (a se vedea Fișa 5 cu privire la tehnologia mobilă și Fișa 12 cu privire la învățământul la distanță).
- **Problemele de suport tehnic:** este necesar un suport tehnic adecvat în școli, astfel încât programele și proiectele să nu fie stopate.
- **Un mediu protector:** creativitatea permite unei persoane să își exprime sentimentelor sale ca individualitate. Deși, în mod ideal, ar trebui să evităm impunerea oricăror constrângeri asupra proceselor creative ale tinerilor, este important să subliniem principiile toleranței, empatiei și respectului, în ceea ce privește rezultatele obținute de alții, în special când un grup face schimb de idei. Un cadru didactic sau un delegat din partea clasei va trebui să fie prezent pentru a ghida lucrul într-un mod constructiv.

1. <http://web.archive.org/web/20080614214250/http://www.netlingo.com/right.cfm?term=video%20conferencing>

2. <http://www.eun.org/teaching/smile>

3. <http://www.etwinning.net>

4. [https://en.wikipedia.org/wiki/Content-control\\_software](https://en.wikipedia.org/wiki/Content-control_software)



- **Confidențialitatea:** Web 2.0 și 3.0 au facilitat, în mare măsură, încărcarea pe Internet a fotografiilor și a imaginilor. Elevii trebuie să fie conștienți de faptul că o singură imagine valorează cât o mie de cuvinte și ar putea pune în pericol informația lor privată și pe cea a altora.
- **Drepturile de autor:** tinerii trebuie să învețe de la vârsta cea mai fragedă să respecte dreptul de proprietate asupra producției creative și să înțeleagă costul plagiatului pentru societate<sup>5</sup>



## CONSOLIDAREA CREATIVITĂȚII ÎN CLASĂ

- Un webquest<sup>6</sup> este o abordare bazată pe întrebări în vederea integrării Internetului în sala de clasă.
- Elevii pot testa creativitatea, învățând elementele de bază ale codării<sup>7</sup> pentru a-și construi propriile site-uri web. Acest lucru stimulează procesele gândirii creative în diferite moduri prin solicitarea de informații despre grafică și conținut.
- Elevii pot colabora la proiecte care dezvoltă abilități de scriere și de producție audio-vizuală, prin crearea de povești și alte materiale în mediul online. Telefoanele mobile pot fi utilizate, de exemplu, pentru a înregistra și a face schimb de imagini și videoclipuri despre aspectele culturale sau profesionale din propria țară, cu elevi din străinătate. Acest lucru îi poate ajuta să învețe prin practică despre concepte referitoare la viața privată, permisiuni pentru fotografii și altele.
- Încurajați elevii să creeze chestionare interactive și activități pentru web cu programe precum Hot Potatoes<sup>8</sup> sau povestiri interactive cu rezultate multiple folosind programe precum este cel disponibil pe site-ul web al Quia<sup>9</sup>.
- Liceenii și studenții își pot crea propriul mediu de învățare 3D cu programe precum Active Worlds<sup>10</sup>. Aceștia își pot construi peisajul ideal sau propriul campus virtual și pot colabora cu alți elevi/studenți în proiecte pe diferite teme.



## BUNE PRACTICI

- Internetul poate fi utilizat ca un instrument principal de cercetare pentru a găsi informații generale, pe teme diferite. Elevii pot aplica apoi cunoștințele pe care le-au obținut la realizarea unei sarcini care le stimulează creativitatea. Tehnologia oferă elevilor/studentilor oportunitatea și libertatea de a dezvolta abilități de gândire de ordin superior.
- Internetul și alte tehnologii moderne permit o comunicare și o colaborare puternică între elevii/studentii din diferite țări și culturi. Mai mult decât oricând, elevii/studentii au posibilitatea de a genera soluții creative prin schimburi de idei cu un număr mare de colegi.
- Programele cu sursă deschisă permite elevilor/studentilor din întreaga lume, în special copiilor din familiile defavorizate, să își exprime creativitatea gratuit. Programele precum Open Office, Gimp, Audacity sau Blender le permit copiilor să creeze documente, să editeze imagini sau fișiere audio sau chiar să realizeze animații 3D fără costuri. În plus, programele cu sursă deschisă oferă posibilitatea de a învăța despre codificare și de a partaja cunoștințe și competențe prin aderarea la o comunitate de codificatori voluntari care sunt motivați de a îmbunătăți și actualiza programul pe care îl utilizează. Asigurați-vă că comunicați despre astfel de alternative copiilor / elevilor / studenților dumneavoastră.
- Cadrele didactice au stabilit că implementarea tehnologiei în sala de clasă, în cadrul activităților practice, oferă elevilor șansa de a găsi soluții la probleme și de a fi inovatori.
- Țineți cont de obiectivele de învățare: cheia pentru atingerea acestor obiective este să vă concentrați asupra procesului pentru a obține un rezultat și nu asupra rezultatului.

5. <https://www.teachingcopyright.org/handout/copyright-faq.html>

6. <http://webquest.org>

7. <https://scratch.mit.edu/educators/>

8. <http://hotpot.uvic.ca/>

9. <http://www.quia.com/>

10. <http://www.activeworlds.com/>

- Când elevii/studentii publică rezultatele activităților de creație online, aceștia trebuie să respecte drepturile de autor.<sup>11</sup> Mai multe detalii pot fi găsite citind despre Creative Commons<sup>12</sup>. Reamintiți-le să citeze sursele, atunci când folosesc materiale create de alții.



## INFORMAȚII SUPLIMENTARE

- Un număr de site-uri web pot fi folosite ca punct de plecare pentru a implica elevii/studentii în proiecte în care creativitatea este încurajată și colaborarea este esențială:
- International Schools Cyberfair este un loc de întâlnire în mediul online unde părinții, elevii/studentii și educatorii pot colabora, interacționa, dezvolta, publica și descoperi resurse de învățare <<http://www.globalschoolnet.org/GSH/>>. European Schoolnet oferă resurse similare pentru școli: <<http://www.eun.org>>.
- Future Problem Solving Program International implică elevii/studentii în rezolvarea creativă a problemelor, prin simularea competențelor de gândire critică și creativă: <<http://www.fpsp.org>>.
- Idei și resurse pentru promovarea creativității pot fi găsite la Education Scotland: <<http://www.educationscotland.gov.uk/learningandteaching/approaches/creativity/>>.
- New Horizons for Learning ale Școlii de Educație John Hopkins <<http://education.jhu.edu/PD/newhorizons/>> este un repertoriu al noilor practici didactice de promovare a învățării creative.
- Capitolul 6, „Artistul din tine”, în manualul „Web We Want” <<http://www.webwewant.eu>> oferă o serie de activități care îi determină pe tineri să își analizeze propria creativitate și să afle mai multe despre plagiat, drepturile de autor și altele.

11. <https://en.wikipedia.org/wiki/Copyright>

12. [https://en.wikipedia.org/wiki/Creative\\_Commons](https://en.wikipedia.org/wiki/Creative_Commons)

Fișa 16

## Jocurile



Jocurile video pot fi descrise ca fiind un divertisment care implică interacțiunea omului cu o interfață de utilizator pentru a genera feedback vizual pe un dispozitiv video, cum ar fi un ecran de televiziune, un calculator, o tabletă sau un telefon inteligent. Termenul cuprinde o gamă imensă de genuri de la săli de jocuri și jocuri de rol, la jocuri de strategie și lumi fantastice. „eSports” este termenul pentru competițiile de jocuri sportive și nu doar, în care participanții (adesea jucători semi-profesioniști) concurează pentru premii bănești în fața unei audiențe live și online tot mai serioase din punct de vedere numeric. Jocurile pot implica un singur participant, parteneri din cercuri închise sau mii și chiar milioane de străini care joacă împreună. Printre astfel de jocuri online în masă cu mulți jucători (MMOG) se află „World of Warcraft” și „Game of Thrones”. Jocurile video constituie acum al treilea cel mai mare sector de pe piața de divertisment din lume, după programele de radio și televiziunea prin cablu, generând vânzări de 74 de miliarde dolari SUA în 2015, după dublarea veniturilor între anii 2013 și 2014<sup>1</sup>.

1. [https://en.wikipedia.org/wiki/Video\\_game](https://en.wikipedia.org/wiki/Video_game)

— telefoanele inteligente și tabletele, precum și prezența utilizatorilor tineri și în vârstă pe Internet au avut un impact considerabil asupra tendințelor în materie de jocuri; un studiu din 2015<sup>2</sup> arată că aproximativ 1 din 3 copii cu vârsta sub 18 ani joacă jocuri online, dar vârsta medie a jucătorilor din mediul online este de 31 de ani. Anterior, acest domeniu era dominat mai mult de bărbați, iar în prezent, femeile constituie 50% din totalul achizițiilor, 48% dintre jucătorii de jocuri electronice la nivel global și 52% din Marea Britanie. Utilizarea consolelor de jocuri dedicate a evoluat, de asemenea, proprietarii acestora petrecând acum mai mult de jumătate din timpul lor pe console pentru a urmări televiziunea și transmisiile video, pentru a viziona discuri Blu-ray și a explora Internetul<sup>3</sup>.

— Jocurile au câștigat și mai mult teren, devenind atât o activitate de familie, cât și o activitate pentru sălile de clasă. Din cadrele didactice K-8 (ciclul cuprins între grădiniță și clasa a VIII-a), 74% spun că includ jocurile online în activitățile de la clasă, 4 din 5 fiind jocuri „educative”. De asemenea, 56% dintre părinți declară că jocurile îi afectează în mod pozitiv pe copiii lor. Având în vedere popularitatea crescândă a jocurilor și impactul pe care acestea îl pot avea asupra drepturilor omului, Consiliul Europei a publicat un set de ghiduri pentru furnizorii de jocuri, dezvoltat în colaborare cu furnizorii de jocuri și experți din domeniile protecția copilului, educație și drepturile omului<sup>4</sup>.

— Acest lucru arată că jocurile online constituie într-adevăr un sector major, cu o gamă foarte largă de jocuri de care zilnic se bucură milioane de utilizatori pe Internet și pe telefoanele mobile.



## DEZVOLTAREA PERSONALĂ ȘI VALOAREA EDUCAȚIONALĂ

- Jocul este mai mult decât divertisment; este o eficientă activitate de colaborare de care se bucură copiii și adulții de toate vârstele. Acesta promovează creativitatea și interacțiunea și joacă un rol important în dezvoltarea socială și intelectuală.
- Jocurile reprezintă una dintre ocaziile rare în care adulții și copiii pot face schimb de idei de la egal la egal (comunicare între generații).
- Copiii învață despre democrație jucând în diferite structuri sociale, într-un mediu ghidat de reguli și parametri.
- Jocurile implică adesea partajarea și respectarea drepturilor și proprietății altora, uneori punând față-n față jucători aparținând diferitor culturi și având diferite practici interculturale. Copiii pot exersa abilitățile sociale fără teama de eșec, având în același timp un sentiment de control. Deoarece jocurile necesită ca copiii să respecte regulile și să urmeze instrucțiunile, acestea le sporesc capacitatea de autodisciplină și autonomie.
- Puzzle-urile, jocurile de masă, aventurile și jocurile de cercetare oferă jucătorilor posibilitatea de a-și dezvolta gândirea strategică și abilitățile de soluționare de probleme. Anumite jocuri pot fi folosite pentru a dezvolta abilitățile motorii fine și spațiale la copiii mai mici și în scopuri terapeutice, ca în cazul persoanelor cu dizabilități fizice.
- Unele studii presupun că jocurile, în special jocul Minecraft, pot fi utile în cazul persoanelor cu autism.
- Jocurile online sunt utile pentru familiarizarea nou-veniților cu tehnologia și codificarea și, favorizarea, în general, a interesului și înțelegerii TIC<sup>5</sup>.
- Jocurile pot fi integrate în aproape orice domeniu al programului de studii, de la matematică până la științe sociale și limbi străine.

2. <http://web.archive.org/web/20160420163852/http://www.bigfishgames.com/blog/2015-global-video-game-stats-whos-playing-what-and-why/>

3. <http://web.archive.org/web/20151023082205/http://www.nielsen.com/us/en/insights/news/2015/game-consoles-in-2015-one-stop-shop-for-games-and-entertainment.html>

4. <http://www.coe.int/en/web/portal/guidelines-for-providers>

5. [https://en.wikipedia.org/wiki/Information\\_technology](https://en.wikipedia.org/wiki/Information_technology)



## CONSIDERAȚII DE ORDIN ETIC ȘI RISCURI

- Legăturile dintre jocurile video și dependență, agresiune, violență, dezvoltarea socială precară și o varietate de stereotipuri și aspecte legate de moralitatea sexuală sunt discutate deja de câteva decenii, însă, încă nu există dovezi concludente că jocurile ar avea o mai mare influență asupra lor decât alte mijloace media<sup>6</sup>.
- Alegerea jocurilor corespunzătoare vârstei este importantă, cu atât mai mult pentru copiii foarte mici.
- Dependența este adesea menționată ca risc. Asociația Americană de Psihiatrie (AAP) a concluzionat în 2013 că nu există suficiente dovezi pentru a include dependența de joc pe lista oficială a tulburărilor mintale, dar a propus termenul de „tulburare psihică generată de dependența de jocuri video pe Internet” și a solicitat studii suplimentare pentru a-i defini criteriile. Deși tulburarea psihică generată de dependența de jocuri video pe Internet este propusă pentru a fi calificată drept tulburare, experții încă discută în ce măsură jocurile ar putea cauza această tulburare și dacă această tulburare este, într-un fel, un efect al altor tulburări<sup>7</sup>.
- Când e vorba de jocuri, dar și alte activități online, echilibrul de viață este foarte important. Timpul petrecut cu jocurile nu trebuie să afecteze activitățile în aer liber și cu ceilalți.
- Unele jocuri online vă permit să faceți cunoștință și să comunicați cu străinii. Asigurați-vă că jocurile care încurajează interacțiunea utilizatorilor, în special cele destinate copiilor foarte mici, sunt supravegheate de un moderator uman sau prevăd o „discuție sigură” cu expresii preselectate.
- Prin achiziții în cadrul aplicațiilor pentru unele jocuri, există posibilitatea ca copiii să cheltuiască accidental o sumă mare din banii părinților pe piese de colecții și instrumente.



## BUNE PRACTICI

- Sistemele de etichetare și de evaluare încurajează actorii industriei jocurilor să acționeze în mod responsabil, impunându-i să își definească și să își descrie produsele. Acest lucru e util și pentru cumpărătorii jocurilor, care pot aprecia conținutul și adecvarea în funcție de vârstă a jocurilor, precum și pot naviga mai sigur pe piața jocurilor. Sistemul paneuropean de clasificare a jocurilor video în funcție de vârstă (Pan European Game Information – PEGI) este singurul sistem paneuropean de clasificare care oferă recomandări detaliate privind adecvarea în funcție de vârstă a conținutului jocului. Clasificările a aproximativ 20.000 de jocuri pot fi găsite pe site-ul web al acestuia, <[www.pegi.info](http://www.pegi.info)>. PEGI este, de asemenea, parte a Coaliției Internaționale de Evaluare a Vârstei (International Age Rating Coalition – IARC), care oferă un sistem global de evaluare și clasificare a vârstei pentru jocurile și aplicațiile livrate digital<sup>8</sup>. Ca urmare, ratingurile PEGI sunt acum disponibile și pentru toate produsele Google Play Store și pentru Mozilla Firefox Marketplace. Magazinele aplicațiilor Microsoft Windows Mobile și Windows 10 vor urma foarte curând.
- Monitorizați numărul de ore petrecute jucând. Luați măsuri în cazul în care alte activități sociale sunt evitate sau copiii și tinerii absentează de la școală pentru a petrece timpul jucând.
- Comunitățile de jocuri pot stimula un sentiment de apartenență și pot determina copiii să aibă încredere prea ușor. Amintiți-le că prietenii din mediul online nu pot fi întotdeauna cei care spun că sunt. Este important să nu oferiți informații personale nimănui din mediul online.
- Jocurile online sunt o activitate familială populară și oferă o deschidere valoroasă pentru conversații de familie despre utilizarea responsabilă a Internetului. Dacă părinții sau cadrele didactice sunt îngrijorați de faptul că copiii lor își petrec prea mult timp cu jocurile electronice,

6. [https://en.wikipedia.org/wiki/Video\\_game\\_controversies#Crime\\_and\\_violence](https://en.wikipedia.org/wiki/Video_game_controversies#Crime_and_violence)

7. [https://en.wikipedia.org/wiki/Video\\_game\\_addiction](https://en.wikipedia.org/wiki/Video_game_addiction)

8. <http://www.globalratings.com>

încercați numeroasele „teste privind dependența de jocuri” pe care le puteți găsi pe motoarele de căutare – acestea constituie un bun reper pentru a iniția o discuție.

- Consiliul Europei a produs un joc online<sup>9</sup> atractiv, interactiv, cu scopul de a promova drepturile copiilor și de a-i proteja de orice formă de violență.
- Alegeți un joc de rol pentru lecția sau familia dumneavoastră, pe o problemă de actualitate la adresa <<http://www.playdecide.eu>>. De asemenea, puteți să vă creați propriul joc urmând modelul Play-Decide și partajați-l cu alte persoane încărcându-l pe acest site web.
- Achizițiile integrate în joc, anume, conținutul nou, funcționalitatea jocului, caracteristicile și/sau actualizările pentru un anumit joc sau aplicație, dar, de asemenea, uneori și alte articole din magazinele online din afara unui joc, reprezintă o zonă de îngrijorare crescândă, în special pentru părinți. Filtrele de control parental pot adesea preveni acest lucru.



## INFORMAȚII SUPLIMENTARE

- Vizionați „Întrebați despre jocuri” <<http://www.askaboutgames.com/>> pentru o mai bună înțelegere a jocurilor video.
- Citiți despre studiile actuale cu privire la jocuri în Revista Internațională de Cercetare a Jocurilor pe Calculator: <<http://www.gamestudies.org/>>.
- Legislația privind jocurile video este un subiect vast care poate implica aspecte din dreptul penal, de reglementare, constituțional, administrativ, al societăților comerciale, al contractelor și, în anumite jurisdicții, din dreptul concurenței. Secțiunea cu privire la politica publică a ISFE (Federația Interactivă de Software din Europa - <<http://www.isfe.eu/objectives/public-policy>>) aduce informații utile despre legislația europeană și internațională relevantă.
- Site-ul web al Sistemului paneuropean de clasificare a jocurilor video în funcție de vârstă (Pan European Games Information – PEGI) conține informații despre rating și etichetare: <<http://www.pegi.info/pegi/index>>. PEGI Online, o completare la acest sistem, vizează crearea unui mediu mai sigur pentru jocurile online. Furnizorii de jocuri licențiați cu eticheta PEGI Online respectă standardele Codului de siguranță al PEGI Online <[www.pegionline.eu](http://www.pegionline.eu)> care includ, printre altele, obligațiile de a asigura site-uri web libere de conținut ilegal și ofensator creat de utilizatori și de link-uri nedorite, pentru a proteja viața privată și care au un mecanism de reclamații independent.
- Verificarea vârstei reprezintă o provocare pentru industria jocurilor, la fel ca pentru alte sectoare online destinate copiilor mici. În Europa se desfășoară proiecte pilot pentru a vedea dacă este posibilă configurarea unui „schimb de atribute” prin care companiile care vând sau furnizează acces la bunuri și servicii pentru consumatorii de o anumită vârstă, ar putea face schimb de experiență și informații, pentru ca verificarea vârstei să fie mai eficientă.
- În fiecare săptămână sunt publicate știri despre jocurile online, deoarece aceasta este piața de divertisment cu cea mai rapidă creștere. Consultați mai multe site-uri pentru a obține un tablou complet al celor mai bine vândute jocuri, al știrilor, descrierilor, rapoartelor de cercetare și statisticilor despre jocuri. Puncte de pornire utile sunt site-urile web Bigfishgames, IFSE, PEGI și Nielsen. De asemenea, puteți să vă abonați la fluxurile de știri/buletinele de știri ale acestor site-uri sau să creați o alertă Google clar definită pentru a rămâne informat.

9. <http://www.wildwebwoods.org>

## Cetățenia digitală



**U**tilizarea pe scară largă a Internetului și a noilor tehnologii de comunicare a constituit o puternică forță motrice pentru creștere și apariția locurilor de muncă și a îmbunătățit calitatea vieții multor cetățeni. Utilizarea zilnică a Internetului a devenit pentru mulți un eveniment obișnuit; cu toate acestea, lipsește o înțelegere mai profundă a cetățeniei digitale și a drepturilor digitale.

— Participarea informată a tuturor cetățenilor la ceea ce este cunoscut ca mediul digital depinde de o dezvoltare mai vastă a competențelor de utilizare. Aceasta include abilitatea de a analiza critic diversitatea informațiilor la care suntem expuși (adică conținutul audio-vizual), de a forma opinii independente, de a fi implicați activ în soluționarea problemelor comunității și de a însuși noi forme de interacțiune socială. În urmă cu două decenii, într-o publicație, UNESCO a descris aceste competențe ca fiind cei patru piloni ai educației: a învăța pentru a cunoaște, a face, a fi și a trăi împreună<sup>1</sup>. Mai mult decât atât, a fi cetățean digital înseamnă a fi capabil de a utiliza instrumente web (a se vedea Fișa 3 cu privire la Web 2.0, Web 3.0 și alte versiuni) și de a înțelege problemele legate de privind viața privată în mediul online (a se vedea Fișa 9).

1. [http://www.unesco.org/education/pdf/15\\_62.pdf](http://www.unesco.org/education/pdf/15_62.pdf)



## CE ESTE CETĂȚENIA DIGITALĂ?

- Cetățenia digitală este un termen care descrie modul în care ar trebui să acționeze o persoană<sup>2</sup> în timp ce utilizează tehnologia digitală online<sup>3</sup>.
- Unii experți propun nouă elemente din care se constituie cetățenia digitală: accesul digital, consumul digital, comunicarea digitală, competențele digitale de utilizare, eticheta digitală, dreptul digital, drepturile și responsabilitățile digitale, sănătatea și bunăstarea digitală și securitatea digitală<sup>4</sup>.
- Indiferent de structura cetățeniei digitale, este clar că toți utilizatorii Internetului au responsabilitatea și, eventual, datoria de a acționa responsabil atunci când utilizează Internetul și tehnologiile de comunicații.

### Amprenta digitală

- O amprentă digitală reprezintă datele rămase în urma utilizării serviciilor digitale.
- O amprentă digitală pasivă este creată atunci când datele sunt colectate fără ca proprietarul să cunoască despre acest lucru, în timp ce amprentele digitale active sunt create atunci când datele cu caracter personal sunt eliberate din propria voință a unui utilizator, în scopul partajării de informații cu privire la propria persoană, prin intermediul site-urilor web sau a rețelelor sociale<sup>5</sup>.

### Identitatea digitală

- O identitate digitală este o informație utilizată pentru a reprezenta persoane, organizații sau echipamente în sistemele și rețelele informatice<sup>6</sup>.

### Educația digitală

- Alfabetizarea digitală reprezintă cunoștințele, competențele și comportamentele necesare pentru a utiliza o gamă largă de dispozitive digitale, cum ar fi telefoanele mobile, tabletele, laptop-urile și calculatoarele de birou<sup>7</sup>.
- Tehnologiile informației și a comunicațiilor au pătruns deja în fiecare aspect al vieților noastre, schimbând tipul de competențe necesare pentru a fi membri activi ai societății.
- Pe măsură ce Internetul continuă să evolueze în paralel cu dezvoltarea rețelelor fără fir (wireless)<sup>8</sup>, o importanță tot mai mare va fi acordată capacității oamenilor de a utiliza tehnologia actuală pentru a recepționa și transmite informații în mod eficient, într-un mod care transcende atât competențele mediatice, cât și competențele de utilizare a Internetului.

### Drepturile digitale

- Consiliul Europei a elaborat un ghid privind „Drepturile omului pentru utilizatorii de Internet” care explică drepturile și responsabilitățile digitale într-un format ușor de utilizat și subliniază faptul că drepturile omului se aplică în mod egal, atât în mediul online, cât și offline<sup>9</sup>.
- Termenul „drepturi digitale”<sup>10</sup> descrie drepturile omului<sup>11</sup> care permit persoanelor să acceseze, utilizeze, creeze și publice medii digitale sau să acceseze și utilizeze calculatoare și alte dispozitive electronice sau rețele de comunicații.
- Termenul se referă, în special, la protecția și la realizarea drepturilor existente, cum ar fi dreptul la viață privată<sup>12</sup>, în contextul noilor tehnologii digitale și, mai ales, a Internetului<sup>13</sup>.

2. [https://en.wikipedia.org/wiki/Digital\\_citizen](https://en.wikipedia.org/wiki/Digital_citizen)

3. [https://en.wikipedia.org/wiki/Digital\\_electronics](https://en.wikipedia.org/wiki/Digital_electronics); [https://en.wikipedia.org/wiki/Etiquette\\_in\\_technology#Online\\_etiquette](https://en.wikipedia.org/wiki/Etiquette_in_technology#Online_etiquette)

4. [http://www.digitalcitizenship.net/Nine\\_Elements.html](http://www.digitalcitizenship.net/Nine_Elements.html)

5. [https://en.wikipedia.org/wiki/Digital\\_footprint](https://en.wikipedia.org/wiki/Digital_footprint)

6. [https://en.wikipedia.org/wiki/Digital\\_identity](https://en.wikipedia.org/wiki/Digital_identity)

7. [https://en.wikipedia.org/wiki/Digital\\_literacy](https://en.wikipedia.org/wiki/Digital_literacy)

8. [https://en.wikipedia.org/wiki/Wireless\\_network](https://en.wikipedia.org/wiki/Wireless_network); <http://en.wikipedia.org/wiki/3G>

9. <https://www.coe.int/en/web/internet-users-rights/guide>

10. [https://en.wikipedia.org/wiki/Digital\\_rights](https://en.wikipedia.org/wiki/Digital_rights)

11. [https://en.wikipedia.org/wiki/Human\\_rights](https://en.wikipedia.org/wiki/Human_rights)

12. [https://en.wikipedia.org/wiki/Right\\_to\\_privacy\\_or\\_freedom\\_of\\_expression](https://en.wikipedia.org/wiki/Right_to_privacy_or_freedom_of_expression) [https://en.wikipedia.org/wiki/Freedom\\_of\\_speech](https://en.wikipedia.org/wiki/Freedom_of_speech)

13. <https://en.wikipedia.org/wiki/Internet>



- În ceea ce privește drepturile digitale ale tinerilor din Europa, Manifestul tinerilor din UE este o „declarație” online a tinerilor europeni cu privire la modul de îmbunătățire a Internetului<sup>14</sup>.

### Cetățenia digitală și democrația electronică (e-democrație)

- E-democrația, include utilizarea tehnologiilor de comunicații electronice, cum ar fi Internetul, în sporirea proceselor democratice în cadrul unei republici democratice sau a unei democrații reprezentative. Acesta este un progres politic consolidat prin utilizarea rețelelor sociale care permit utilizatorilor să aibă propria lor voce și să comenteze „în public” problemele relevante. O teorie este că utilizarea rețelelor sociale în democrația electronică ar putea permite o influență mai largă asupra rezultatelor politicilor, deoarece implicarea mai multor persoane ar putea genera politici mai inteligente și duce la sporirea transparenței și a răspunderii.
- În zilele noastre, politicienii din multe țări folosesc site-urile de socializare pentru a discuta cu tineri și pentru a le afla opiniile. Acest lucru este contestat de unii, dar este important să se meargă în locurile în care sunt tinerii pentru a a-i aborda.
- O preocupare legată de democrația electronică este impactul decalajului digital asupra celor care nu au acces la mijloacele media. Cu toate acestea, pe măsură ce un număr tot mai mare de persoane de toate vârstele accesează Internetul, acest lucru nu ar trebui privit ca un considerent pentru nerecunoașterea beneficiilor rețelelor de socializare în democrația electronică.
- În comunicarea offline, puterea este adesea văzută ca fiind ierarhică, în timp ce în mediul online, aceasta devine difuză și se schimbă constant. În mod similar, granițele online devin permeabile, rolurile sunt flexibile, se schimbă și nu se bazează pe caracteristici sau pe ierarhii non-verbale. Numai aceste motive ilustrează deja beneficiile utilizării site-urilor de socializare pentru promovarea democrației electronice.
- Cu toate acestea, pentru ca democrația electronică să aibă un efect pozitiv, utilizatorii trebuie să fie deschiși comunicării non-violente și opiniilor contradictorii și să fie dispuși să participe la dezbateri pacifiste și respectuoase. Atunci când comunitățile de persoane având aceeași gândire formează și discută probleme fără a lua în considerare alte perspective, acest lucru poate mai degrabă să slăbească, decât să consolideze democrația electronică și chiar să conducă la radicalizarea opiniilor.



### IMPORTANȚA ÎN EDUCAȚIE

- Internetul face posibilă nu numai publicarea mai rapidă a mult mai multor informații, ci și actualizarea permanentă a acestor informații, astfel încât cetățenii să fie informați cu privire la ultimele evoluții din domeniile lor de interes.
- Dreptul la informare și dreptul la participare sunt drepturi acordate tuturor copiilor în temeiul articolelor 13 și 17 din Convenția Națiunilor Unite cu privire la drepturile copilului.
- În trecut, trebuia să ne bazăm pe versiunile declarațiilor și evenimentelor pe care presa alegea să le publice pentru a ne informa; în zilele noastre, putem foarte des accesa direct sursa pentru a găsi informațiile la prima mână.
- Pe măsură ce cetățenii din întreaga lume devin jurnaliști zilnici cu ajutorul telefoanelor lor inteligente echipate cu posibilitatea de a filma videoclipuri, suntem adesea inundați de scene „live” care se petrec în fața ochilor noștri. Abilitatea de a analiza ceea ce prezintă videoclipul și ceea ce s-a întâmplat înainte și după începerea filmării, lipsește adesea în cazul unui astfel de jurnalism zilnic, evidențiat prin fluxurile Twitter, videoclipurile de pe YouTube, transmisiunile Vine și alte platforme de socializare.
- Faptul că cetățenii sunt mai bine informați îi împuternicește să participe mai activ la viața democratică la nivel național, paneuropean și internațional. În plus, cetățenii pot folosi Internetul pentru a găsi detalii imparțiale despre majoritatea aspectelor ce-i interesează.
- Informațiile geografice, culturale și turistice, datele despre trafic colectate de agențiile din sectorul public și privat îmbogățesc în mod considerabil viața cetățenilor. În unele țări, cetățenii pot chiar

14. <http://www.youthmanifesto.eu/>

să utilizeze Internetul pentru a-și schimba oficial adresa, a aplica pentru reînnoirea pașaportului sau pentru a efectua diverse alte activități pentru care anterior, pierdeau mult timp. Rețineți însă faptul că trebuie să fie luate anumite măsuri de precauție atunci când oferiți informații private în mediul online (a se vedea Fișele 9 cu privire la viața privată și 19 cu privire la securitate).

- Internetul permite, de asemenea, cetățenilor să participe la discuții și dezbateri online despre subiecte de interes pentru viața publică sau locală și chiar să participe la alegeri prin vot electronic<sup>15</sup>.
- Pe lângă implicarea politică, cetățenii pot face cumpărături online, pot studia online (a se vedea Fișa 12 cu privire la învățământul la distanță), se pot implica în discuții culturale, pot medita, face yoga – aproape orice activitate este disponibilă online.



## CONSIDERAȚII DE ORDIN ETIC ȘI RISCURI

- Având acces la informații permanent actualizate, de calitate, cetățenii se află într-o poziție mai bună de a-și exercita drepturile fundamentale ale omului. Cu toate acestea, trebuie să rămânem atenți la efectele negative pe care tehnologia le-ar putea avea asupra acestor drepturi, în special:
- Nu toate persoanele au acces egal la informații. Diviziunea digitală descrie societatea actuală pe două niveluri și decalajul dintre cei care „au” și „nu au” acces la informații. Dacă situația continuă, democrația va fi amenințată, deoarece cei mai puțin norocoși își vor pierde treptat autonomia de exprimare. Fără accesul direct la informații, suntem mai puțin capabili să ne formăm propria opinie și, prin urmare, putem fi mai ușor manipulați de cei care sunt fluenți în utilizarea noilor tehnologii. În plus, informațiile din sectorul public sunt foarte importante pentru viața democratică și civică și, mai ales, reprezintă o resursă-cheie pentru activitatea economică. Dacă vrem să asigurăm egalitatea de șanse pentru toți, atunci trebuie să asigurăm accesul egal la informații și competențe robuste în gândirea critică pentru toți.
- Tehnologia și platformele online nu sunt neapărat neutre în ceea ce privește accesarea informațiilor. Algoritmii utilizați de motoarele de căutare sau cenzura pe rețelele sociale modelează informațiile care sunt afișate în prim plan.
- Tehnologiile informației și comunicațiilor joacă astăzi un rol atât de important în viețile noastre, încât în curând numai cei fluenți în utilizarea acestora vor putea într-adevăr să-și facă auzită vocea. Cu toate acestea, TIC în sine nu sunt decât facilitatori tehnici și o mai largă comunicare nu înseamnă respectarea libertății de exprimare. Valori precum dezbaterile și discursurile pacifiste, gândirea critică și lipsa de prejudecăți sunt esențiale pentru promovarea unui mediu online pozitiv și a libertății de exprimare.
- Creșterea uriașă a mijloacelor de transfer și de schimb de informații înseamnă că trebuie să avem grijă să protejăm datele despre propria persoană și, prin urmare, dreptul nostru la viață privată (a se vedea în continuare „Bune practici”).



## INSTRUCȚIUNI

- Pentru a deveni un cetățean digital angajat, toți internauții trebuie să-și înțeleagă drepturile și responsabilitățile de bază. Utilizatorii trebuie să înțeleagă ce le este permis să facă, precum și ceea ce au voie să facă sectorul privat, guvernul și alți utilizatori de Internet.
- O înțelegere de bază a cookie-urilor și a modului în care site-urile web pot să colecteze și să utilizeze datele dumneavoastră personale este esențială (a se vedea Fișa 9 cu privire la viața privată).
- Pentru a evita complicarea problemelor în cazul copiilor mici, aceleași principii fundamentale de bună cetățenie ar trebui pur și simplu să se răsfrângă și asupra activităților online: respect, bunăvoință și gândire înainte de a acționa.

<sup>15</sup>. [https://en.wikipedia.org/wiki/Electronic\\_voting](https://en.wikipedia.org/wiki/Electronic_voting)



## IDEI PENTRU LUCRUL ÎN CLASĂ

- Rugați elevii să examineze Convenția Națiunilor Unite cu privire la drepturile copilului și să analizeze ce secțiuni se referă expres la drepturile digitale<sup>16</sup>.
- Solicitați elevilor să aleagă câțiva vorbitori de pe Twitter, Facebook și/sau Periscope care abordează aspecte legate de cetățenie și să se implice într-o discuție cu aceștia. Întrebați vorbitorii care este punctul lor de vedere în ceea ce privește cetățenia digitală și responsabilitățile utilizatorilor. Cereți elevilor să se gândească și la alte întrebări pe care să le adreseze.
- Elevii pot fi rugați să acceseze site-urile web europene care oferă asistență în materie de drepturile digitale. Cereți elevilor să efectueze o analiză a drepturilor digitale europene, ale Consiliului Europei și ale Comisiei Europene.
- O resursă bună care ar putea servi drept bază pentru programul dumneavoastră de studiu în domeniul civic este programul de activitate online în domeniul drepturilor omului al Consiliului Europei<sup>17</sup>. De asemenea, puteți solicita clasei dumneavoastră să întocmească o cartă proprie a drepturilor omului. Lăsați-i să își aplice noile cunoștințe despre drepturile omului în mediile virtuale, de exemplu, să explice cum ar putea face Internetul un loc mai bun de lucru și de joacă pentru ei.
- De exemplu, la disciplina istorie, când discutați despre Revoluția franceză, ajutați elevii să facă distincția dintre fapte și ipoteze, comparând picturile eroice revoluționare despre asaltul Bastiliei cu relatările moderne. Aceștia ar trebui să poată „explica cum și de ce asaltul Bastiliei a fost interpretat diferit”. Probabil, subiectul dat va putea fi legat de conceptele educației media, cum ar fi modul în care realitatea este reprezentată în scopuri diferite și cât de fiabile sunt informațiile afișate.
- Ca parte a unui proiect geografic, de exemplu „Un pașaport pentru lume”, invitați elevii să discute despre modalitățile în care diferite locuri din lume sunt reprezentate pe Internet și să analizeze modul în care site-urile web diferă în ceea ce privește accentul pus sau atitudinea față de un anumit loc.
- Pentru a ajuta elevii să învețe despre analiza conținutului, alegeți un subiect, apoi căutați-l pe site-urile de știri din diferite surse și analizați-le în clasă. Ați observat că diferite organizații folosesc abordări diferite? De ce credeți că este așa?
- Deoarece telefoanele mobile fac parte integrantă din viața elevilor în afara școlii, examinați în clasă modul în care acestea pot fi utilizate pentru a aduna informații comunitare și a participa activ la democrație. Listați serviciile pe care le pun la dispoziție și discutați despre efectele acestora asupra vieții private și a democrației (a se vedea Fișa 5, „Internetul în mișcare”, pentru informații privind serviciile mobile).
- Simulați o dezbatere online prin postarea unui mesaj pe tablă și distribuind notițe autoadezive (post-its) elevilor. Fiecărui elev i se va atribui un număr și va putea să se ridice în picioare și să citească bilețelul după un anumit număr prestabilit de minute corespunzătoare numărului său. După ce au citit mesajul lor original și au ascultat comentariile propuse, elevilor li se va permite să scrie și să posteze propriul comentariu și să monitorizeze discuția pentru a „răspunde” la alte postări. Elevii vor avea, de asemenea, opțiunea de a „susține” postarea unui alt elev, care va fi plasată la vedere, lângă postul inițial. Acest exercițiu își propune să îi învețe pe elevi cum diferă o dezbatere în mediul online de o dezbatere în viața reală și abordează, de asemenea, întrebările referitoare la „libertatea de exprimare” și evitarea atacurilor verbale sau a altor comportamente online inadecvate.

16. <http://web.archive.org/web/20160501101507/http://blogs.lse.ac.uk/mediapolicyproject/2014/09/12/sonia-livingstone-digital-media-and-childrens-rights>

17. [https://www.coe.int/t/dg4/youth/Training/Training\\_courses/HRE\\_Youth\\_Programme\\_en.asp](https://www.coe.int/t/dg4/youth/Training/Training_courses/HRE_Youth_Programme_en.asp)



## BUNE PRACTICI

- Fiecare cetățean are dreptul de a-și controla propriile date cu caracter personal, ceea ce necesită cunoașterea informațiilor personale colectate despre acestea. Regulamentul General privind Protecția Datelor a fost introdus în Uniunea Europeană în 2016, în parte pentru a ajuta cetățenii să își exercite aceste drepturi, precum și alte drepturi fundamentale privind viața privată și protecția datelor<sup>18</sup>. Punctele-cheie pentru cetățeni sunt rezumate într-un comunicat de presă al Comisiei Europene din 15 decembrie 2015<sup>19</sup>.
- Citiți întotdeauna textul scris cu litere foarte mici din chestionare pentru a vedea cum vor fi utilizate informațiile pe care le oferiți despre dumneavoastră și, pentru mai multe sfaturi, nu uitați să consultați Fișa 9 cu privire la viața privată.
- Comunicarea competențelor de utilizare și transferul acestora în întreaga școală, în învățământul superior și în societatea civilă este esențială dacă se dorește creșterea participării la procesul democratic.
- Luați în considerare participarea la un curs online privind cetățenia digitală sau drepturile digitale.
- În prezent, o serie de școli lucrează asupra programelor de dobândire a competențelor de utilizare a Internetului, pentru a se asigura că elevii lor dezvoltă competențele necesare pentru a trăi, a lucra și a se recrea în societatea informațională de astăzi. Acestea includ:
  - ▶ competențe de navigare în labirintul informațiilor disponibile pe Internet;
  - ▶ dezvoltarea capacității de a face diferența între informare și dezinformare;
  - ▶ analizarea informațiilor din punctul de vedere al relevanței și valabilității;
  - ▶ înțelegerea implicațiilor etice ale instrumentelor online asupra democrației;
  - ▶ utilizarea informațiilor în învățarea bazată pe proiecte;
  - ▶ înțelegerea și utilizarea oportunităților multiple pe care le pot oferi un browser și Internetul.



## INFORMAȚII SUPLIMENTARE

- Pentru informații cu privire la Regulamentul General privind Protecția Datelor, a se vedea: [http://ec.europa.eu/justice/data-protection/reform/index\\_en.htm](http://ec.europa.eu/justice/data-protection/reform/index_en.htm).
- Manifestul tinerilor din UE este o „declarație” online a tinerilor europeni cu privire la modul de îmbunătățire a Internetului: <http://www.youthmanifesto.eu>.
- Pentru mai multe informații privind drepturile digitale europene, consultați: <https://edri.org>.
- Amnesty International <http://www.amnesty.org/> și Human Rights Watch <http://www.hrw.org/> sunt organizații neguvernamentale care organizează campanii de susținere a drepturilor omului. Amnesty are un manual multilingv pentru cadrele didactice numit „Primii pași”, conceput să ajute tinerii să învețe despre drepturile omului, în special în Europa Centrală și de Est.
- Comisia Europeană deține informații privind protecția copiilor și a demnității umane în serviciile audiovizuale: [http://ec.europa.eu/avpolicy/index\\_en.htm](http://ec.europa.eu/avpolicy/index_en.htm).
- Mai multe informații despre drepturile copiilor pot fi găsite în Convenția ONU cu privire la drepturile copilului: <http://www.ohchr.org/en/professionalinterest/pages/crc.aspx>.

18. [http://ec.europa.eu/justice/data-protection/reform/index\\_en.htm](http://ec.europa.eu/justice/data-protection/reform/index_en.htm)

19. [http://europa.eu/rapid/press-release\\_IP-15-6321\\_en.htm](http://europa.eu/rapid/press-release_IP-15-6321_en.htm)

- Codul drepturilor online al UE este setul de drepturi și principii consacrate în legislația UE care protejează cetățenii atunci când accesează și utilizează rețele și servicii online: <https://ec.europa.eu/digital-agenda/en/code-eu-online-rights>.
- Pentru cele nouă elemente ale cetățeniei digitale, consultați: [http://www.digitalcitizenship.net/Nine\\_Elements.html](http://www.digitalcitizenship.net/Nine_Elements.html).
- Declarația de la Paris, adoptată de Comisia Europeană și Consiliul European de Miniștri în 2015, promovează cetățenia și valorile comune ale libertății, toleranței, nediscriminării și incluziunii prin educație: [http://ec.europa.eu/education/library/study/2016/neset-education-tolerance-2016\\_ro.pdf](http://ec.europa.eu/education/library/study/2016/neset-education-tolerance-2016_ro.pdf).
- Documentele relevante ale Consiliului Europei includ „Drepturile omului pentru utilizatorii de Internet”: <http://www.coe.int/en/web/internet-users-rights/guide> (subiectele cheie de mai jos):
  - ▶ accesul și nediscriminarea
  - ▶ libertatea de exprimare și de informare
  - ▶ întrunirea, asocierea și participarea
  - ▶ viața privată și protecția datelor
  - ▶ educația și competențele de utilizare
  - ▶ copiii și tinerii
  - ▶ remedii juridice efective și reparații



## Parentajul digital: pozitiv și proactiv



■ **„Nativii digitali”** sunt copiii născuți în epoca digitală, această eră a tehnologiei. Aceștia sunt copii care, după doar câteva minute petrecute cu o tabletă sau un telefon inteligent în mână, nu simt nicio frică sau îngrijorare în a utiliza tehnologia. Aceștia își plimbă degetele, ciupesc, ciocănesc fără a înțelege întotdeauna ceea ce fac, dar având încrederea că ceva se întâmplă pe ecran. Potrivit lui Marc Prensky, „elevii noștri din prezent sunt toți ‘vorbitori nativi’ ai limbajului digital al computerelor, jocurilor video și Internetului” (Prensky, M. (2001) „Nativii digitali, Imigranții digitali Partea 1” *La orizont* 9(5) pp 1-6, 1. Disponibilă la: <<http://web.archive.org/web/20160413070431/http://www.marcprensky.com/writing/Prensky%20-%20Digital%20Natives,%20Digital%20Immigrants%20-%20Part1.pdf>>).

■ **„Imigranții digitali”** sunt oameni care s-au născut înainte de apariția tehnologiei. Aceasta este o expresie la fel propusă de Prensky în 2001 și utilizată pentru a descrie generația de oameni care nu au crescut în epoca digitală. Din nou, Prensky o descrie perfect spunând: „Acea dintre noi care nu s-au născut în lumea digitală, dar care, într-un moment ulterior al vieții noastre, am devenit fascinați și am adoptat multe sau cele mai multe dintre aspectele noii tehnologii suntem, și întotdeauna vom fi, în comparație cu ceilalți, Imigranți digitali” (Prensky (2001), 1-2 <<http://web.archive.org/web/20160413070431/http://www.marcprensky.com/writing/Prensky%20-%20Digital%20Natives,%20Digital%20Immigrants%20-%20Part1.pdf>>)

■ **„Parentajul digital”** este noțiune ce se referă la îndrumarea „părinților imigranți digitali” pentru ca ei să înțeleagă ce fac astăzi „copiii lor nativi digitali”. Singurul scop este acela de a proteja copiii, de a abilita părinții și de a menține comunicarea deschisă între ambele părți

#### **Parentajul digital este:**

- comunicarea deschisă cu copilul dumneavoastră privind riscurile și beneficiile pe Internet;
- implicarea sistematică în activitățile online ale copilului dumneavoastră;
- protecția activă a reputației și a identității digitale ale copilului dumneavoastră;
- învățarea împreună cu copilul dumneavoastră a oportunităților pe care le poate prezenta Internetul;
- protejarea copilului dumneavoastră de pericolele pe care le poate prezenta Internetul;
- aplicarea competențelor dumneavoastră de parentaj offline, în lumea online.

#### **Parentajul pozitiv este:**

- asigurarea disciplinei pozitive și a îndrumării pozitive pentru copilul dumneavoastră;
- buna educare fără strictețe a copilului dumneavoastră;
- învățarea copilului dumneavoastră, de la o vârstă fragedă, a bunelor comportamente, arătându-i repercusiunile comportamentului „rău” și beneficiile faptelor „bune”;
- claritate în privința lucrurilor pe care copilul ar trebui să le facă;
- stabilirea unor granițe specifice și adecvate;
- demonstrarea consecvenței în toate privințele.

■ Există o legătură vădită între aceste două, iar părintele și îngrijitorul digital au nevoie de toate instrumentele disponibile pentru a fi proactivi, pozitivi și pentru a se asigura că copilul lor folosește în mod responsabil Internetul și dispozitivele dotate cu Wi-Fi.



### **IMPORTANȚA ÎNȚELEGERII PROBLEMELOR**

- Omniprezența Internetului, a telefoanelor mobile și a dispozitivelor conectate la Wi-Fi, induce un sentiment de frustrare, deoarece părinților le lipsesc cunoștințele și expertiza tehnică concretă. Iar acei părinți care sunt cunoscători ai tehnologiilor, se confruntă cu un alt sentiment: îngrijorare din cauza vitezei cu care copiii lor îmbrățișează Internetul și tehnologia.
- Este posibil ca părinții să nu știe cum să se ocupe de copiii care petrec ore întregi jucând Minecraft atunci când rămân peste noapte la un coleg sau cum să stabilească limite la expedierea mesajelor seara pentru tânărul de 17 ani, sau dacă să folosească o aplicație care să le învețe copilul de 2 ani să stea pe oliță. Întrebările sunt infinite, pe măsură ce tehnologia avansează și dispozitivele devin mai eficiente și mai inteligente.
- Deoarece structurile familiale se schimbă, părinții pot avea dificultăți în menținerea aceluiași reguli de utilizare a dispozitivelor acasă la un prieten, la bunici sau în alt mediu familial.
- Pe măsură ce tehnologia avansează, avansează și cercetările privind dezvoltarea copilului și implicațiile utilizării mediului online, dar constatările pe termen lung nu vor fi disponibile încă câțiva ani.





## CONSIDERAȚII DE ORDIN ETIC ȘI RISCURI

- Cercetarea inițială a demonstrat că utilizarea unui telefon inteligent sau a unui dispozitiv pentru a „calma” copiii, poate împiedica abilitatea acestora de auto-reglare (autocontrol)<sup>1</sup>.
- Creșterea unui copil în prezent simultan implică creșterea unui cetățean digital responsabil, deoarece copiii trebuie să știe cum să folosească Internetul și tehnologia în siguranță și chibzuit.
- Părinții trebuie să îi ajute pe copii să înțeleagă competențele digitale: capacitatea de a utiliza eficient informațiile, mijloacele media și tehnologiile digitale și dezvoltarea cetățeniei digitale.
- Lumea digitală și Internetul au un impact profund și asupra parentajului „offline”. A vedea lumea „online” ca fiind separată de lumea „offline” este o concepție greșită. Cu posibilitățile nesfârșite oferite de lumea online, copiii se pot confrunta cu un anumit conținut sau experiențe într-o etapă mai timpurie decât ar face-o în lumea „offline”. Aceasta include conținut „pozitiv”, cum ar fi învățarea de a citi mai devreme, studiarea muzicii, expunerea la o limbă străină și așa mai departe. În același timp, copiii pot fi, de asemenea, expuși la conținut sexual explicit, violență, frică, hărțuire și alte lucruri similare.
- Atenție la partea comercială a Internetului. Majoritatea serviciilor online care sunt „gratuite” se bazează pe modele de afaceri opace și structuri de costuri sau exploatarea datelor personale pentru publicitate. De exemplu, așa-numitele jocuri „freemium”, vă vor ademeni copilul să cheltuiască mulți bani pentru a avansa în joc, în timp ce „advergamae” estompează granița dintre joc și publicitate prin plasarea de publicitate a unui produs sau mărci în cadrul jocului.
- Pentru cele nouă elemente ale cetățeniei digitale, a se vedea „Cetățenia digitală: utilizarea adecvată a tehnologiei”<sup>2</sup> și consultați Fișa 17 cu privire la cetățenia digitală.
- Constatările studiilor recente efectuate de Centrul Comun de Cercetare al Comisiei Europene, care se concentrează asupra utilizării tehnologiei de către familiile cu copii mici, sunt utile în înțelegerea problemelor și a riscurilor<sup>3</sup>.
- EU Kids Online publică articole despre îngrijorările părinților din întreaga Europă pe blogul său despre parentaj<sup>4</sup>.



## INSTRUCȚIUNI

- Fiți un model pentru copiii dumneavoastră și limitați propria utilizare a tehnologiilor.
- Fiți informat despre cele mai recente aspecte ale spațiului online și discutați despre activitățile online ale copiilor dumneavoastră.
- Discutați cu școala copiilor dumneavoastră pentru a afla dacă există un program privind siguranța în mediul online.
- Aveți grijă atunci când interziceți dispozitivele preadolescentului sau adolescentului dumneavoastră ca măsură disciplinară, deoarece privarea copilului de conexiunile și rețelele lui sociale poate avea consecințe nedorite.
- Vorbiți cu alți părinți pentru a afla despre practici bune, aplicabile la orice vârstă.
- Pentru a-i învăța pe copiii dumneavoastră cum să își gestioneze timpul online, stabiliți limite de timp pentru mediul online, acționând similar cu situația în care i-ați învăța cum să nu depășească bugetul alocat pentru banii de buzunar. Dați-le un anumit timp pe care aceștia îl pot „cheltui” săptămânal și lăsați-i să îl gestioneze.
- Subliniați importanța timpului petrecut cu familia offline și mențineți activitățile săptămânale de familie.

1. <http://web.archive.org/web/20160424230408/https://www.theguardian.com/technology/2015/feb/01/toddler-brains-research-smartphones-damage-social-development>

2. [http://www.digitalcitizenship.net/Nine\\_Elements.html](http://www.digitalcitizenship.net/Nine_Elements.html)

3. <http://publications.jrc.ec.europa.eu/repository/handle/JRC93239>

4. <http://web.archive.org/web/20160415215157/http://blogs.lse.ac.uk/parenting4digitalfuture/2015/06/26/svenjas-post-on-little-kids-european-comparison/>



## IDEI PENTRU LUCRUL ÎN CLASĂ

- Cereți elevilor să scrie o scurtă postare pentru blog dedicată părinților lor, oferind sfaturi privind parentajul în era digitală.
- Lansați-vă într-o discuție cu elevii despre utilizarea tehnologiei în zilele noastre. Care sunt beneficiile? Care sunt riscurile? Ce anume pot face elevii pentru a promova beneficiile și pentru a contracara riscurile?
- După o discuție cu privire la bunele practici în cazul utilizării Internetului, solicitați elevilor să își prezinte principalele sfaturi pe care să le împărtășească fraților/surorilor, nepoților, nepoatelor sau vecinilor mai mici. Cum pot învăța copiii mai mici din experiențele elevilor?
- Solicitați elevilor să compare tehnologiile din anii 1960 și cele de astăzi. Aveau părinții aceleași preocupări? De ce? De ce nu?



## BUNE PRACTICI

- Discutați cu copiii dumneavoastră despre cei cu care vorbesc online, despre activitățile online, despre site-urile pe care le vizitează și despre timpul când accesează mediul online.
- Păstrați dialogul deschis – chiar și atunci când subiectul poate fi incomod pentru dumneavoastră – deoarece este cel mai bun mod de a rămâne informat cu privire la activitățile online ale copilului dumneavoastră.
- Pe lângă discuțiile cu copiii dumneavoastră despre „sexul sigur”, luați în considerare o discuție despre „tehnologiile sigure” și „conținutul sigur” pe Internet și explicați pericolul și riscul legat de fotografii, discuții sau mesaje cu caracter sexual sau extremist.
- Fiți pregătiți să discutați despre aspecte precum violența, atacurile verbale, hărțuirea, sexualitatea, stereotipurile și rolurile de gen, deoarece copiii dumneavoastră se pot confrunța cu acestea pe neașteptate în mediul online și vor avea nevoie de îndrumarea dumneavoastră pentru a deveni mai rezilienți și a adopta, ca răspuns, un comportament pozitiv în mediul online.
- Fiți conștienți de utilizarea setărilor de confidențialitate și explicați copilului dumneavoastră cum să le pună în aplicare și de ce acest lucru este util.
- Informați-vă despre modelul de afaceri din spatele jocurilor, serviciilor sau a site-urilor web pe care copilul dumneavoastră le utilizează. Pentru copiii mai mici, asigurați-vă că conținutul nu prezintă publicitate, costuri ascunse sau funcții „premium”. Este mai bine să achiziționați o sumă mică pentru un joc sau un abonament lunar la un serviciu de calitate, decât să vă expuneți copilul tentativelor de exploatare comercială.
- Asigurați-vă că copiii dumneavoastră înțeleg modelele de afaceri din spatele serviciilor sau a jocurilor pe care le utilizează sau a conținutului pe care îl citesc.
- Asigurați-vă că copiii dumneavoastră nu distribuie în exces (informații personale, caracteristici de identificare, fotografii necorespunzătoare etc.).
- Găsiți un echilibru sănătos între utilizarea Internetului și timpul petrecut în fața ecranului și demonstrați că sunteți un model digital demn de urmat.
- Amintiți copiii dumneavoastră că tot ceea ce scriu, postează sau distribuie va rămâne pe Internet pe un termen nelimitat – și, de asemenea, că acesta poate fi modificat și distribuit mai departe.
- Învățați-vă copiii cum să utilizeze instrumentele de raportare, astfel încât să poată semnala orice conținut necorespunzător.



## INFORMAȚII SUPLIMENTARE

- Pentru informații privind efectul iPad-urilor asupra dezvoltării copiilor, urmăriți reportajul: <https://www.youtube.com/watch?v=VrQhmcPrhFw>.
- Pentru a citi lucrarea lui Marc Prensky „Nativii digitali, imigranții digitali” (2001), a se vedea: <http://web.archive.org/web/20160413070431/http://www.marcprensky.com/writing/Prensky%20-%20Digital%20Natives,%20Digital%20Imigrants%20-%20Part1.pdf>.
- COFACE, Confederația Europeană a Familiilor oferă informații utile familiilor: <http://www.coface-eu.org/>.
- Parent Zone (Zona Părinților) este un site din Regatul Unit care oferă o multitudine de informații: <http://www.theparentzone.co.uk/>.
- Consultați publicația Institutului pentru siguranța familiilor în mediul online: <https://www.fosi.org/good-digital-parenting/>.
- Vodafone a elaborat ghiduri pentru părinți, precum și reviste de parentaj digital: <https://www.vodafone.com/content/parents/howto-guides.html>.
- Centrul Medical al Universității din Boston a publicat un raport privind utilizarea dispozitivelor mobile: [http://web.archive.org/web/20160607121811/http://www.eurekaalert.org/pub\\_releases/2015-01/bumc-mai013015.php](http://web.archive.org/web/20160607121811/http://www.eurekaalert.org/pub_releases/2015-01/bumc-mai013015.php).
- Centrul Comun de Cercetare al Comisiei Europene a publicat un raport privind copiii mici și tehnologia digitală: <http://publications.jrc.ec.europa.eu/repository/handle/JRC93239>.
- „Joaca și învățarea: a fi online” conține activități pentru copiii de 4-8 ani pentru a oferi suport părinților și cadrelor didactice în a discuta cu copiii lor despre utilizarea responsabilă a Internetului: <https://www.betterinternetforkids.eu/web/portal/news/detail?articleID=198308>.
- Îndrumați-vă copiii mai mici către site-uri adaptate vârstei lor; există o gamă largă de astfel de site-uri, inclusiv „Junior: căutarea sigură pentru copii” („Junior: safe search for kids”) <https://www.juniorsafesearch.com/> și Copiii YouTube (YouTube Kids) <https://kids.youtube.com/>.
- Articole relevante ale Consiliului Europei sunt incluse pe pagina web a Consiliului Europei „Copiii în mediul digital” <http://www.coe.int/en/web/children/the-digital-environment>.



## 5. Internetul – Răspuns la provocări

---

” „A le suprima oamenilor drepturile umane înseamnă a le pune la îndoială umanitatea.”

*Nelson Mandela, laureat al Premiului Nobel pentru Pace din 1993, activist anti-apartheid, Președintele Africii de Sud 1994-1999*

„Drepturile tuturor oamenilor sunt diminuate atunci când sunt amenințate drepturile unui singur om.”

*John F. Kennedy, Președintele SUA 1961-1963*

### LISTA DE VERIFICARE PENTRU FIȘA 19 – CRIMINALITATEA INFORMATICĂ: MESAJELE COMERCIALE NESOLICITATE (SPAM), CODURILE OSTILE (MALWARE), FRAUDA ȘI SECURITATEA

---

Ați creat parole puternice și diferite pentru conturile dumneavoastră și ați configurat o securitate cu doi factori?

Ați explorat setările de securitate pentru dispozitivele/conturile dumneavoastră?

Ați actualizat sistemul de operare și aplicațiile dumneavoastră?

Ați făcut o copie de rezervă a celor mai importante date?

### LISTA DE VERIFICARE PENTRU FIȘA 20 – ETICHETAREA ȘI FILTRAREA

---

V-ați gândit la implicațiile culturale și morale ale filtrării?

Cunoașteți diferența dintre o „listă neagră” și o „listă albă”?

Sunteți familiarizați cu sistemele de etichetare cel mai frecvent utilizate pentru conținutul copiilor și ce semnifică acestea?

### LISTA DE VERIFICARE PENTRU FIȘA 21 – HĂRȚUIREA ÎN MEDIUL ONLINE: BULLYING-UL, URMĂRIREA ÎN SCOP DE HĂRȚUIRE (STALKING) ȘI TROLLING-UL

---

Aveți implementată o politică clară a familiei sau a școlii în așa fel încât copiii să înțeleagă repercusiunile atunci când sunt implicați în hărțuirea în mediul online?

Vă protejați suficient detaliile personale? Multe probleme în mediul online sunt cauzate de partajarea nechibzuită a fotografiilor și a informațiilor.

Ați cercetat cum să dezvoltați competențe sociale și emoționale îmbunătățite (cunoscute și sub numele de capacități sociale) pentru a depăși anonimatul și „lipsa unui chip” în cazul comunicării online, care facilitează bullying-ul, trolling-ul și hărțuirea, în general?

### LISTA DE VERIFICARE PENTRU FIȘA 22 – SOLICITAREA ASISTENȚEI

---

Dumneavoastră și copiii / elevii dumneavoastră știți unde să raportați conținutul ilegal?

Verificați vreodată statisticile raportate de către liniile de asistență pentru a înțelege tendințele și riscurile emergente?

Care sunt primele cinci competențe digitale care vă vor proteja cel mai bine în mediul online?

Înțelegeți suficient geolocalizarea și Bluetooth-ul pentru a utiliza dispozitivele mobile confortabil și în siguranță?

M-learning și portofelele mobile sunt domenii în care utilizarea dispozitivelor mobile schimbă modul în care învățăm, lucrăm și cumpărăm. Ce știți despre aceste progrese recente?



## Criminalitatea informatică: mesajele comerciale nesolicitate (spam), codurile ostile (malware), fraudă și securitatea



Internetul este o modalitate excelentă de a accesa conținut și servicii de calitate, însă acesta poate servi, de asemenea, scopului persoanelor rău intenționate, prin difuzarea de mesaje comerciale nesolicitate, viruși, coduri ostile și escrocherii.

- **Criminalitatea informatică** cuprinde infracțiuni îndreptate împotriva calculatoarelor și a datelor, de exemplu, accesul ilegal la un calculator (numit și hacking), interceptarea unei comunicări, împiedicarea funcționării unui calculator sau deteriorarea sau ștergerea datelor, dar și infracțiunile comise prin intermediul calculatoarelor, cum ar fi fraudă sau violența sexuală împotriva copiilor. Codurile ostile, mesajele comerciale nesolicitate și phishing-ul, precum și alte forme de furt de identitate sunt unele dintre instrumentele utilizate de infractorii cibernetici.

- **Codurile ostile (malware)**<sup>1</sup> este un termen umbrelă utilizat pentru a denumi o varietate de forme de programe ostile sau intruzive, care includ viruși, cai troieni și altele. Obiectivele codurilor ostile sunt foarte diverse. Acestea pot avea ca scop pur și simplu perturbarea funcționării calculatorului prin deteriorarea programului sau coruperea echipamentului sau pot fura informații și date care pot fi monetizate, într-un fel sau altul. De asemenea, calculatorul dumneavoastră infectat poate deveni un „bot”, care este controlat de infractori fără știrea dumneavoastră; acesta poate fi utilizat împreună cu milioane de alte calculatoare infectate, ca parte a unui „botnet”, pentru a răspândi mesaje comerciale nesolicitate, a comite fraude sau a efectua atacuri împotriva spitalelor, aeroporturilor sau băncilor.
- **Mesajele comerciale nesolicitate (spam)**<sup>2</sup> se referă la trimiterea în masă de mesaje nesolicitate către mai mulți destinatari. Acestea sunt cel mai frecvent asociate cu emailul, dar se aplică și rețelelor sociale, mesageriei instant, telefoanelor mobile și așa mai departe. Din fericire, majoritatea serviciilor de email au filtre de spam eficiente. Mesajul comercial nesolicitat poate servi, de asemenea, ca vector pentru a răspândi diferite tipuri de coduri ostile, de exemplu, când un destinatar deschide un atașament sau un link indicat în mesajul comercial nesolicitat.
- **Phishingul**<sup>3</sup> derivă din „pescuirea parolelor” și reprezintă o formă de furt de identitate. De exemplu, destinatarii primesc mesaje comerciale nesolicitate, care apar sub forma unor mesaje legitime din partea unei instituții cunoscute, cum ar fi o bancă sau o rețea socială. Aceste mesaje conțin adesea link-uri către site-uri web false, care sunt utilizate pentru a colecta informații sensibile despre utilizatori, cum ar fi numerele sau parolele cardurilor de credit. Aceste informații despre identitate furate sunt adesea folosite pentru a comite fraude.
- **Frauda pe Internet**<sup>4</sup> s-a intensificat foarte mult în ultimii ani, deoarece s-au extins posibilitățile de comerț electronic și de efectuare a plăților online. Infracțiunea dată înglobează diferite tipuri de fraudă, cum ar fi contrafacerea, fraudă imobiliară, servicii de tip premium tonuri de apel prin SMS, fraudă în cazul transferului de bani și așa mai departe.



## AȘADAR, CUM PUTEȚI RĂMÂNE ÎN SIGURANȚĂ?

— Securitatea dumneavoastră în mediul online poate fi comparată cu securitatea la domiciliu. Protejați conținutul cu ferestrele închise și ușa încuiată. O doză sănătoasă de scepticism, o gândire critică și competențele TIC vă vor ajuta, de asemenea, să nu fiți înșelat prin fraudă, phishing, coduri ostile sau escrocherii online.

— Multe dintre aspectele relevante pentru securitate sunt, de asemenea, relevante și pentru viața privată (a se vedea Fișa 9).



## DEZVOLTAREA PERSONALĂ ȘI VALOAREA EDUCAȚIONALĂ

— Securitatea este la fel de importantă pentru dumneavoastră, ca și pentru toți internauții. Codurile ostile, virușii și mesajele comerciale nesolicitate se răspândesc în mare parte prin intermediul utilizatorilor înșiși! Dacă computerul sau dispozitivul dumneavoastră nu este în siguranță, toți prietenii și persoanele de contact ar putea fi expuse, de asemenea, riscurilor de securitate!

— Cunoștințele despre securitatea și siguranța Internetului sunt foarte valoroase pentru dezvoltarea în continuare a competențelor digitale de utilizare, deoarece acestea îi fac pe utilizatori să analizeze mai profund parametrii și setările dispozitivelor lor și a serviciilor online pe care le utilizează și să obțină cunoștințe tehnice mai bune despre modul în care funcționează dispozitivele, sistemele lor de operare și Internetul.

1. <https://en.wikipedia.org/wiki/Malware>

2. <https://en.wikipedia.org/wiki/Spamming>

3. <https://en.wikipedia.org/wiki/Phishing>

4. [https://en.wikipedia.org/wiki/Internet\\_fraud](https://en.wikipedia.org/wiki/Internet_fraud)





## RISCURI POTENȚIALE

### Mesajele comerciale nesolicitate

- Mesajele comerciale nesolicitate sunt, de obicei, benigne și consecințele sunt, în general, o mare pierdere de timp, prin faptul că acestea trebuie sortate sau o pierdere de timp prin accesarea link-urilor.
- Mesajele comerciale nesolicitate conțin adesea informații false sau frauduloase. Deoarece expeditorul rămâne anonim, de obicei, nu este posibilă urmărirea penală pentru relațiile false.
- Expeditorii mesajelor nesolicitate („*spammeri*”) se bazează adesea pe bunăvoința destinatarilor pentru a colecta adrese de poștă electronică pentru bazele lor de date. De exemplu, pot fi trimise emailuri solicitând destinatarilor să își adauge informațiile personale într-o listă pentru a susține o petiție sau o cauză. Menționând adesea o cauză precum un copil bolnav care necesită o intervenție chirurgicală, acestea afirmă, în mod fals, că o companie sau o organizație a promis că banii vor fi plătiți de fiecare dată când mesajele sunt retransmise.
- Noi tehnici privind mesajele comerciale nesolicitate apar în fiecare zi. Spre exemplu, pe rețelele sociale, mesajele comerciale nesolicitate poate lua forma „clickjacking-ului”<sup>5</sup>, cu postări distribuite de prieteni care includ titluri atractive precum „cele mai eficiente 10 modalități de a pierde în greutate” sau „nu veți crede ce face această fată în fața camerei web”. Consecința poate fi faptul că vizitați o pagină web care vă expune unei vaste publicități, pentru a genera venituri sau vă forțează să dați „like” unei pagini, care vă va trimite mesaje comerciale nesolicitate cu mult mai multe postări.
- Există multe tipuri de fraude în mediul online și, în fiecare zi, apar altele noi, pe măsură ce tehnologia evoluează. O fraudă frecventă este „419”, denumită după o lege nigeriană care interzice acest tip de activitate. Aceasta implică, de regulă, promisiunea partajării unei sume mari de bani, în schimbul ajutorului acordat pentru transferuri bancare. O altă fraudă constă în a cere victimei să trimită banii ca o garanție de depozit pentru chirie prin Western Union, înainte de a vizita apartamentul de închiriat.

### Phishing-ul și furtul de identitate

- Riscurile de a cădea pradă phishingului și furtului de identitate sunt mult mai grave. În funcție de informațiile pe care le-ați furnizat în cazul tentativei de phishing, prejudiciul poate fi oricare, de la pierderea controlului asupra unui cont online relativ neimportant, cum ar fi un forum online, până la pierderea controlului asupra unor conturi extrem de importante, cum ar fi adresa dumneavoastră principală de email, ceea ce poate duce la compromiterea tuturor conturilor dumneavoastră în mediul online!
- Odată ce conturile dumneavoastră au fost compromise, datele dumneavoastră pot fi în pericol. De exemplu, conținutul tuturor email-urilor dumneavoastră poate fi descărcat. Aceste date se pot dovedi a fi foarte valoroase pentru a extorca bani de la dumneavoastră sau de la contactele dumneavoastră, pentru a comanda articole utilizând conturile dumneavoastră online sau cardul dumneavoastră de credit și pentru a vă uzurpa identitatea în mediul online etc.

### Codurile ostile

- Riscurile de instalare a codurilor ostile sunt asemănătoare cu phishingul, cu mesajele comerciale nesolicitate sau chiar și mai mari. Codurile ostile pot fi folosite în scopuri de phishing pentru a fura informații despre conturile dumneavoastră (utilizând, de exemplu, un înregistrator cheie<sup>6</sup>), în scopul trimiterii de mesaje comerciale nesolicitate, pentru a vă bombarda cu ferestre pop-up, notificări sau ecrane de pornire implicite în browserele dumneavoastră, precum și în alte scopuri, cum ar fi furtul de informații și date, direct din calculatorul dumneavoastră sau perturbarea funcționării calculatorului dumneavoastră, preluarea controlului asupra calculatorului dumneavoastră în scopul comiterii de infracțiuni, activării microfoanelor sau a camerelor de luat vederi ale dispozitivului dumneavoastră pentru a vă spiona și eventual, a distrugerii complete a conținutului.

5. <https://en.wikipedia.org/wiki/Clickjacking>

6. [https://en.wikipedia.org/wiki/Keystroke\\_logging](https://en.wikipedia.org/wiki/Keystroke_logging)

- Tehnicile care urmăresc să păcălească utilizatorul să instaleze coduri ostile se dezvoltă rapid. Un exemplu este o fereastră falsă de tip pop-up, care emulează realist o scanare antivirus a calculatorului. La sfârșitul scanării false, niște presupuși viruși periculoși sunt identificați pe calculatorul dumneavoastră și pentru a scăpa de aceștia trebuie să instalați un program – care este de fapt un cod ostil sau un virus!



## IDEI PENTRU LUCRUL ÎN CLASĂ

- Divizați copiii și tinerii în grupuri de lucru a câte trei sau patru și rugați-i să propună o parolă puternică pentru un cont online fals. Explicați-le clar că trebuie să creeze o parolă nouă, nu să utilizeze o parolă existentă pe care o folosesc deja! Solicitați diferitelor echipe să își prezinte parola și să ceară restului grupului să examineze propunerile și să identifice caracteristicile unei parole puternice.
- O parolă puternică:
  - ▶ are cel puțin opt caractere;
  - ▶ nu conține un cuvânt găsit într-un dicționar, nu conține o referință la viața dumneavoastră personală sau la numele dumneavoastră de utilizator, numele dumneavoastră real sau numele companiei dumneavoastră;
  - ▶ conține caractere din fiecare din următoarele categorii: majuscule, litere mici, cifre și simboluri.
- CERT (echipa de răspuns pentru situații de urgență informatică), cunoscută și sub denumirea de CSIRT (echipa de răspuns pentru incidente de securitate informatică), este un grup de experți care gestionează incidentele de securitate informatică. Solicitați elevilor dumneavoastră să caute un CERT/CSIRT din țara dumneavoastră și să afle mai multe despre rolul și funcționarea acestor echipe.
- Adesea, victimele infracțiunilor informatice nu raportează infracțiunea la poliție și astfel, infractorii își continuă activitățile ilegale și găsesc noi victime.
  - ▶ Solicitați elevilor dumneavoastră să afle informații despre modul în care trebuie să raporteze o infracțiune la poliție sau la alte autorități publice, inclusiv prin linii telefonice de urgență.
  - ▶ Solicitați elevilor dumneavoastră să afle ce prevede legislația națională la capitolul criminalitate informatică.



## BUNE PRACTICI

- Una dintre consecințele faptului că internauții așteaptă să obțină totul în mediul online „gratuit” a fost dezvoltarea continuă a codurilor ostile sau a mesajelor comerciale nesolicitate anexate la programele sau la serviciile „gratuite” folosite online. Mediul online constituie o responsabilitate comună și este rezultatul comportamentului și alegerilor individuale online ale utilizatorilor. Prin susținerea financiară a serviciilor/conținuturilor/programele de calitate (prin donații pentru acțiuni cu sursă deschisă sau achiziționarea de licențe sau abonamente de la organizații comerciale), contribuiți la îmbunătățirea siguranței mediului online.
- Ușurința în utilizare poate fi inamicul securității. De exemplu, puteți să vă configurați sistemul de operare să solicite o parolă de administrator ori de câte ori se efectuează o acțiune importantă (de exemplu, instalarea unui nou program). Poate fi extrem de frustrant și plictisitor, dar acesta este prețul care trebuie plătit pentru mai multă siguranță! Țineți cont de acest lucru atunci când configurați parametrii de securitate ai sistemului dumneavoastră de operare.

- Dacă gestionați mai mulți utilizatori ai unui calculator sau ai unei rețele, asigurați-vă că fiecare utilizator are drepturi corespunzătoare. Restricționarea drepturilor de utilizator inutile poate ajuta la evitarea problemelor de securitate accidentale sau deliberate.
- Asigurați-vă că aveți încredere în sursă înainte de a descărca ceva pe calculatorul dumneavoastră. Fiți conștienți, în mod deosebit, cu privire la programele de la egal la egal<sup>7</sup>, celebre pentru faptul că ajută la distribuirea codurilor ostile (a se vedea Fișa 14 cu privire la muzică și imagini). Ori de câte ori instalați un program, asigurați-vă că ați citit toți pașii înainte de a da clic pe butonul „următorul”. Acordați o atenție specială căsuțelor pre-bifate care pot instala coduri ostile pe calculatorul dumneavoastră!
- Instalați programul anti-virus<sup>8</sup> și mențineți-l actualizat.
- Instalați patch-uri de securitate sau actualizări ale sistemului de operare imediat ce acestea devin disponibile. Puteți seta unele sisteme de operare și programe să se actualizeze automat sau să vă informeze imediat ce un patch este disponibil pentru descărcare.
- Instalați un firewall<sup>9</sup> pentru a controla traficul spre și dinspre calculatorul dumneavoastră.
- Utilizați diferite conturi de email pentru diferite scopuri, evitând să divulgați în permanență adresa de email „personală” (de exemplu, în cazul înregistrării pe forumuri, completării de formulare etc.) și să distribuiți adresa dumneavoastră de email pe scară largă. Rețineți faptul că, dacă includeți adresa dumneavoastră de email pe un site web, roboții web/de căutare (web crawlers) o pot prelua și o pot adăuga în listele de distribuire pentru mesajele comerciale nesolicitate. De asemenea, nu răspundeți mesajelor comerciale nesolicitate. Aceasta va confirma adresa dumneavoastră de email celor care trimit mesajele comerciale nesolicitate. Fiți conștienți de faptul că link-urile care promit să vă ștergă de pe lista lor de corespondență pot să nu fie reale.
- În cazul în care sunteți nevoit să postați adresa dumneavoastră de email, puteți să o camuflați adăugând caractere precum Tom(punct)Smith(arond)gmail(punct)com sau postând-o ca imagine, astfel încât să nu poată fi copiată în mod automat.
- Fiți atenți la emailurile pe care le primiți. Nu deschideți emailuri dacă nu aveți încredere în sursă. Verificați întotdeauna adresa de email a oricărei notificări pe care o primiți pentru a verifica dacă este autentică.
- Fiți extrem de precaut cu anexele. Dacă primiți ceva care pare suspicios sau ceva ce nu ați solicitat, ștergeți imediat fără a deschide.
- Nu dați niciodată clic pe link-uri de la destinatarii în care nu aveți încredere și mai ales pe link-urile care utilizează URL-uri prescurtate și în cazul cărora este imposibil să vedeți adresa URL „originală”. Rețineți faptul că chiar și destinatarii în care aveți încredere vă pot trimite mesaje infectate, în cazul în care contul sau dispozitivul acestora a fost compromis.
- Nu trimiteți sau postați niciodată informații private, cum ar fi un nume de utilizator și o parolă sau un număr de card de credit, prin email. Niciun serviciu online nu vă va solicita să vă trimiteți numele de utilizator și parola prin email, iar detalii precum numărul cardului de credit vor fi solicitate în cazuri foarte rare (de exemplu, atunci când rezervați o cameră de hotel este posibil să fie necesar să trimiteți aceste informații pe adresa oficială de email pentru rezervări a hotelului).
- Utilizați diferite parole pentru conturile dumneavoastră cele mai importante și asigurați-vă că configurați măsuri de securitate cu doi factori ori de câte ori este posibil (adăugând numărul dumneavoastră de telefon mobil sau o frază/întrebare suplimentară de securitate). Asigurați-vă că parolele dumneavoastră nu au nicio legătură evidentă cu dumneavoastră, au cel puțin opt caractere și folosesc o combinație de litere (litere mici și majuscule), cifre și simboluri.

7. <https://en.wikipedia.org/wiki/Peer-to-peer>

8. [https://en.wikipedia.org/wiki/Antivirus\\_software](https://en.wikipedia.org/wiki/Antivirus_software)

9. [https://en.wikipedia.org/wiki/Firewall\\_\(computing\)](https://en.wikipedia.org/wiki/Firewall_(computing))

- Faceți în mod periodic copii de rezervă ale tuturor datelor dumneavoastră pe o unitate de hard disk externă. Există multe programe de backup și acestea realizează backup-ul automat și periodic al datelor dumneavoastră. Unele dintre acestea sunt incluse chiar și în interiorul sistemului dumneavoastră de operare (Windows, MacOS, Linux etc.). Asigurați-vă că sunteți mereu informat<sup>10</sup>.



## INFORMAȚII SUPLIMENTARE

- Truth or Fiction (Adevăr sau ficțiune) este un site web pe care utilizatorii de Internet pot verifica mesajele ce se conțin în emailurile frecvent expediate: [<http://www.truthorfiction.com/>](http://www.truthorfiction.com/).
- Aflați mai multe despre combaterea mesajelor comerciale nesolicitate la adresele: [<http://spam.abuse.net>](http://spam.abuse.net) și [<http://www.spamhelp.org/>](http://www.spamhelp.org/).
- Pentru informații despre securitatea Microsoft, consultați: [<http://www.microsoft.com/security/>](http://www.microsoft.com/security/).
- Pentru informații despre securitatea Apple, consultați: [<http://www.apple.com/support/security/>](http://www.apple.com/support/security/).
- Agenția Uniunii Europene pentru Securitatea Rețelelor și a Informațiilor (European Union Agency for Network and Information Security – ENISA) furnizează actualizări periodice privind aspectele aferente securității digitale: [<http://enisa.europa.eu>](http://enisa.europa.eu).
- Consiliul Europei are o pagină web care se numește „Acțiune împotriva criminalității cibernetice”: [<www.coe.int/cybercrime>](http://www.coe.int/cybercrime).
- TechTarget este o revistă privind securitatea informațiilor: [<http://informationsecurity.techtarget.com/>](http://informationsecurity.techtarget.com/).
- Informații utile și teste ale utilizatorilor pe numeroase subiecte: de la cookie-uri la adrese IP, până la verificări ale browserului, pot fi găsite la: [<http://www.2privacy.com/>](http://www.2privacy.com/).
- Recomandările privind securitatea online din partea Guvernului britanic pot fi găsite la [<https://www.getsafeonline.org>](https://www.getsafeonline.org) și pentru Statele Unite la [<http://www.us-cert.gov/>](http://www.us-cert.gov/).
- Căutați pe Internet echipa dumneavoastră națională de răspuns pentru situații de urgență informatică culegând acronimul CERT și denumirea țării dumneavoastră.
- Deși liniile directe privind securitatea informațiilor oferite de Asociația de Marketing Direct [<http://www.the-dma.org/guidelines/informationsecurity.shtml>](http://www.the-dma.org/guidelines/informationsecurity.shtml) sunt destinate comercianților direcți, acestea oferă, de asemenea, sfaturi utile pentru oricine este preocupat de securitatea în mediul online.
- Articole relevante din Convenția ONU cu privire la drepturile copilului:
  - Articolul 16** – Copiii au dreptul la viață personală. Copilul are dreptul la protecția legii contra unor atacuri asupra vieții lor personale, reputației, familiei și domiciliului.
  - Articolul 17** – Copiii au dreptul la informații de încredere din partea mass-media. Televiziunea, radioul și ziarul trebuie să ofere informații pe înțelesul copiilor și care nu dăunează bunăstării acestora.
  - Articolul 34** – Guvernul se angajează să protejeze copiii contra oricărei forme de abuz sexual.
  - Articolul 36** – Copiii trebuie protejați împotriva oricăror activități care le-ar putea afecta bunăstarea.

<sup>10</sup>. [https://en.wikipedia.org/wiki/List\\_of\\_backup\\_software](https://en.wikipedia.org/wiki/List_of_backup_software)

## Etichetarea și filtrarea



### ETICHETAREA

Etichetarea și filtrarea sunt ambele metode de restricționare a accesului la conținutul de Internet, cum ar fi videoclipuri, imagini, pagini web și jocuri. În ciuda asigurărilor primite cu zece ani în urmă, din partea agențiilor tehnice și a organismelor de protecție a copilului, de a crea un sistem electronic de etichetare care ar putea fi încorporat în site-uri web în scopul filtrării, în zilele noastre, etichetarea adoptă, în mod obișnuit, forma unui simbol vizibil cu ochiul liber, care indică faptul că regulamentele sau standardele specifice sunt întrunite. Cu toate acestea, dezvoltarea de criterii pentru sistemele de marcare și etichetare de încredere, care să permită copiilor și familiilor acestora să identifice conținuturile adecvate din mediul online și să facă schimb de bune practici internaționale în acest domeniu continuă să fie o prioritate pentru Consiliul Europei, în special prin Forumul pentru Guvernarea Internetului, care se întrunește anual sub egida Organizației Națiunilor Unite<sup>1</sup>. Etichetarea site-urilor nu este doar un mijloc de a proteja minorii și de a spori încrederea publicului în utilizarea tranzacțiilor online, aceasta încurajează, de asemenea, respectarea standardelor legale de către furnizorii de conținut.

1. [www.intgovforum.org](http://www.intgovforum.org)

— PEGI este un sistem european de etichetare online, susținut de Comisia Europeană, deoarece oferă ghiduri privind restricțiile de vârstă și tipurile de conținut care se găsesc în jocuri și aplicații (a se vedea Fișa 16 cu privire la jocuri). Acesta oferă ghiduri privind restricțiile de vârstă în cazul jocurilor, aplicațiilor și anumitor conținuturi online, precum și o indicație a tipului de conținut pe care îl includ. Acesta arată, de asemenea, că furnizorii de conținut respectă standardele de calitate care includ, printre altele, obligațiile prin care se încearcă a interzice conținutul ilegal și ofensator creat de utilizator și link-urile nedorite pe site-urile web, pentru a proteja viața privată și care au un mecanism independent de reclamații.

— Etichetarea mărcilor de calitate și de încredere poate fi găsită și pe site-urile de cumpărături și pe alte site-uri de tranzacții online pentru a indica faptul că acestea respectă reglementările și recomandările cu privire la tranzacțiile sigure (a se vedea Fișa 13 cu privire la cumpărăturile online). Unul dintre simbolurile cele mai frecvente pe care le puteți vedea este pictograma lacăt, care indică faptul că pagina de pe site-ul pe care vă aflați utilizează protocolul SSL (nivel conexiuni securizate – *secure sockets layer*) (un standard de securitate al transferului de date care criptează datele și autentifică serverul și integritatea mesajului) sau protocolul TLS (securitatea nivelului de transport – *transport layer security*). Prin urmare, puteți presupune, în mod rezonabil, că datele dumneavoastră, mai ales detaliile bancare, sunt securizate.



## FILTRAREA

— Filtrarea este înțeleasă, în general, ca procesul de detectare și blocare a platformelor și/sau a conținuturilor necorespunzătoare pe Internet. Aceasta se poate face în browsere și proxy-uri sau prin instalarea de cenzori de programe, cum ar fi controalele parentale. Filtrele sunt configurate potrivit regulilor stabilite de părinți, școli, întreprinderi, guverne și alte entități. Acestea funcționează, în general, prin listele „negre” (de conținut care trebuie blocat) sau listele albe (care interzic accesul la toate conținuturile de pe Internet, cu excepția elementelor aprobate de filtru). Uneori, listele albe sunt adunate în cadrul unui sistem de programe în care operatorul de transport sau prestatorul de servicii are control asupra aplicațiilor, conținutului și suporturilor media și restricționează accesul convenabil la aplicațiile sau la conținutul care nu este aprobat. Când un astfel de sistem este creat pentru copii, acesta este denumit „grădină fortificată” sau „platformă închisă”<sup>2</sup>, spre deosebire de o platformă deschisă, în care consumatorii au acces nerestricționat la aplicații, conținut și multe altele.

— O altă metodă de filtrare este atunci când regulile sunt introduse prin cuvinte-cheie sau termeni, restricționând sau blocând complet accesul la orice pagini web care conțin cuvintele sau expresiile interzise. Prin intermediul unei parole, persoana care a stabilit regulile de filtrare poate, de asemenea, să permită ad-hoc accesul la diferite site-uri<sup>3</sup>.

— În prezent, există filtre pentru dispozitive multiple. Programul sau aplicația de filtrare poate fi încărcată pe mai multe dispozitive, cum ar fi un laptop, tabletă, telefon inteligent, televizor sau eReader (*cititor de cărți digitale*) și poate fi, de exemplu, controlat centralizat de către părinte. Pot fi stabilite reguli diferite pentru copiii de vârste diferite și acestea pot evolua automat, odată cu vârsta copilului. Regulile de filtrare pot fi aplicate pentru a restricționa timpul petrecut în mediul online și accesul la contacte, precum și pentru monitorizarea geolocalizării și multe altele.



## EDUCAȚIA

- Listele albe sunt cu atât mai valoroase atunci când copiii fac primii pași pe Internet, permițându-le să recunoască și să acceseze rapid site-urile lor preferate. Nu numai că acest lucru va contribui la dezvoltarea discriminării lor vizuale, o cerință prealabilă pentru lectură, ci va ajuta ca activitățile de Internet să devină activități comune de familie – un element crucial pentru a garanta siguranța copilului dumneavoastră în mediul online.

2. [https://en.wikipedia.org/wiki/Closed\\_platform](https://en.wikipedia.org/wiki/Closed_platform)  
3. <http://internet-filter-review.toptenreviews.com>

- Filtrarea poate fi un supliment foarte util pentru a proteja minorii de conținutul necorespunzător existent pe Internet sau pentru a monitoriza utilizarea acestuia, dar trebuie utilizată împreună cu o îndrumare adecvată din partea părinților, a cadrelor didactice și a îngrijitorilor copiilor.
- În cazul sălilor de clasă, filtrele pot fi valoroase pentru a reduce riscul ca elevii să acceseze materiale nepotrivite sau dăunătoare. Cu toate acestea, ele nu exclud necesitatea de a verifica în prealabil site-urile care urmează a fi propuse elevilor pentru realizarea sarcinilor bazate pe utilizarea Internetului.
- Studiul de referință al Programului pentru un Internet mai sigur (SIP-Bench) arată că instrumentele de filtrare de astăzi sunt capabile să filtreze conținuturile potențial dăunătoare, fără a reduce drastic oportunitățile pe care Internetul le oferă copiilor și tinerilor. Mai multe detalii sunt disponibile pe site-ul Programului Internet mai sigur<sup>4</sup>.
- Problemele ridicate de practicile de etichetare și de filtrare abundă în materialele privind teme de cetățenie și/sau studiilor sociale. Începeți o dezbatere pe tema filtrării în mediul online. Este aceasta o formă acceptabilă și necesară de cenzură?



## PROBLEME

- Filtrarea conținutului poate bloca accesul la informații și resurse valoroase, de exemplu la cele ce țin de istoria războaielor mondiale sau educația sexuală, din cauza anumitor cuvinte-cheie pe care le conțin.
- Etichetarea și clasificarea site-urilor web rămâne o practică în mare parte voluntară, cu excepția cazului în care țările au legi care să aplice anumite standarde. Trăim într-o lume globală, iar eficiența acestora este, într-o oarecare măsură, afectată de adoptarea limitată a acestora de către furnizorii de platforme și de conținut și de lipsa sistemelor comune de etichetare și de clasificare.
- Legislația nu poate ține pasul cu evoluția tehnologică și, chiar și în zilele noastre, serviciile programelor de filtrare tind să eticheteze paginile în funcție de propriile lor sisteme de valori și agende sociale.
- Este dificil să se decidă ce conținut este în realitate dăunător copiilor de o anumită vârstă, cine trebuie să decidă asupra regulilor generale pe care furnizorii de conținut trebuie să le respecte și asupra aplicării acestor reguli. De aceea, instrumentele de filtrare trebuie să fie foarte flexibile, pentru a permite îngrijitorilor copiilor să modeleze regulile de filtrare în funcție de valorile familiale. Furnizorii de filtre trebuie să elaboreze tehnici pentru a se asigura că filtrează în conformitate cu aceste criterii.
- Filtrele pot deveni, de asemenea, un instrument de cenzură utilizat pentru a modela opinia publică și a suprima opoziția politică. Unele țări blochează site-urile partidelor politice sau ideologiilor opuse; acesta poate fi un punct de plecare interesant pentru discuții în clasă despre drepturile omului și democrație.
- Unii oameni consideră că filtrarea este o formă de cenzură și, prin urmare, e contrară spiritului Internetului. Alții susțin că dacă nu ar exista programele de filtrare, guvernele ar fi supuse presiunii de a reglementa conținutul online.
- Furnizorii de programe de filtrare se străduiesc din răspuțeri să facă față provocărilor create de rețelele sociale, dispozitivele mobile și utilizarea Internetului de către copiii din ce în ce mai mici.
- Există discuții la nivel internațional pentru a crea un domeniu *.kids* care să înlocuiască *.org*, *.com* și altele similare, pentru site-uri care sunt adaptate copiilor, pentru a-i proteja de conținuturile online care ar putea fi potențial dăunătoare, rău intenționate sau necorespunzătoare. Pe măsură ce site-urile care utilizează numele de domeniu *.kids* ar fi obligate să adere la regulamentul de înregistrare, numeroasele provocări includ stabilirea de standarde acceptabile la nivel internațional, selectarea unei agenții internaționale de monitorizare și așa mai departe.

4. <http://www.sipbench.eu>



## INSTRUCȚIUNI

- Dacă sunteți un dezvoltator de jocuri sau aplicații care dorește ca creația sa să fie evaluată conform standardelor naționale sau internaționale sau un părinte sau îngrijitor care dorește, pur și simplu, să înțeleagă procesul, vizionați videoclipul „Inițiere” pe site-ul web al Coaliției Internaționale pentru Evaluarea Vârstei (*International Age Rating Coalition – IARC*)<sup>5</sup>. Majoritatea browserelor și sistemelor de operare au comenzi parentale integrate, pe care le puteți seta pentru a filtra conținutul nedorit. Blogul „Cum configurez controalele parentale neagasant pe toate dispozitivele mele?”<sup>6</sup> oferă informații despre cum să faceți acest lucru pe o gamă largă de dispozitive și programe. Pentru majoritatea programelor de filtrare, puteți specifica tipurile de conținut pe care doriți să le filtrați sau să le permiteți. Cu toate acestea, filtrele preinstalate ar putea să nu îndeplinească toate cerințele dumneavoastră, mai ales dacă doriți să stabiliți diferite reguli pentru doi sau mai mulți utilizatori. Va trebui să achiziționați un program dedicat pentru o abordare mai sofisticată față de filtrarea site-urilor și monitorizarea utilizării. Cel mai recent raport privind Programul Internet mai sigur<sup>7</sup>, dar și revizuirile programelor pentru Internet<sup>8</sup> pot fi utile în alegerea dintr-o multitudine de produse disponibile pe piață.



## BUNE PRACTICI

- Analizați cu atenție modul în care funcționează un filtru înainte de a-l instala. Filtrarea se face reieșind din decizii ideologice sau culturale cu care nu sunteți de acord?
- Utilizați mijloacele electronice cu discernământ și nu vă încredeți în publicitatea exagerată. Testați produsele prin raportare la experiența personală. Niciun filtru nu poate înlocui vreodată „filtrul gândirii critice” pe care toți utilizatorii de Internet trebuie să îl dezvolte, indiferent de vârstă.
- Vorbiți cu regularitate elevilor, părinților și personalului despre utilizare și nevoile acestora. Crearea unui mediu deschis pentru discuții va aduce plus valoare experienței elevilor dumneavoastră legate de utilizarea Internetului decât cenzura sau „vânătoarea de vrăjitoare”. Experții consideră că cheia pentru o utilizare responsabilă a Internetului de către copii este ca părinții să se intereseze de activitățile lor online și să petreacă timpul cu copiii în mediul online.
- Luați în considerare opțiunile privind „listele albe” care permit accesul numai la site-urile aprobate pentru cei mai mici utilizatori de Internet. Marcați în browserul dumneavoastră site-urile web preferate și cele prietenoase copiilor pentru a crea o listă personală pentru copiii dumneavoastră, astfel încât aceștia să poată accesa cu ușurință site-urile sigure pe care le-au utilizat înainte.
- Copiii și tinerii ar trebui încurajați să vorbească despre materialele inadecvate pe care le găsesc pe Internet. Adolescenții afirmă în mod repetat că cea mai mare provocare pentru ei este faptul că nu pot să vorbească cu părinții despre problemele morale cu care se confruntă în mediul online. Raportați conținuturile potențial ilegale la o linie telefonică de urgență<sup>9</sup>.
- Monitorizați activitățile copiilor dumneavoastră pe site-urile web de jocuri și căutați eticheta PEGI Online pentru a recunoaște site-urile sigure.
- Din ce în ce mai multe comunități din mediul online se bazează chiar pe utilizatori pentru a ajuta la etichetarea conținutului, mai ales când acesta este generat de utilizatori. Asigurați-vă că etichetați orice conținut pe care îl încărcați și că ajutați la semnalarea conținutului care este etichetat necorespunzător.

5. <https://www.globalratings.com>

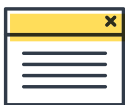
6. <http://web.archive.org/web/20160528132556/http://liferhacker.com/5868750/how-do-i-set-up-non-annoying-parental-controls-on-all-my-devices>

7. <http://www.sipbench.eu/>

8. <http://internet-filter-review.toptenreviews.com>

9. <http://www.inhope.org>



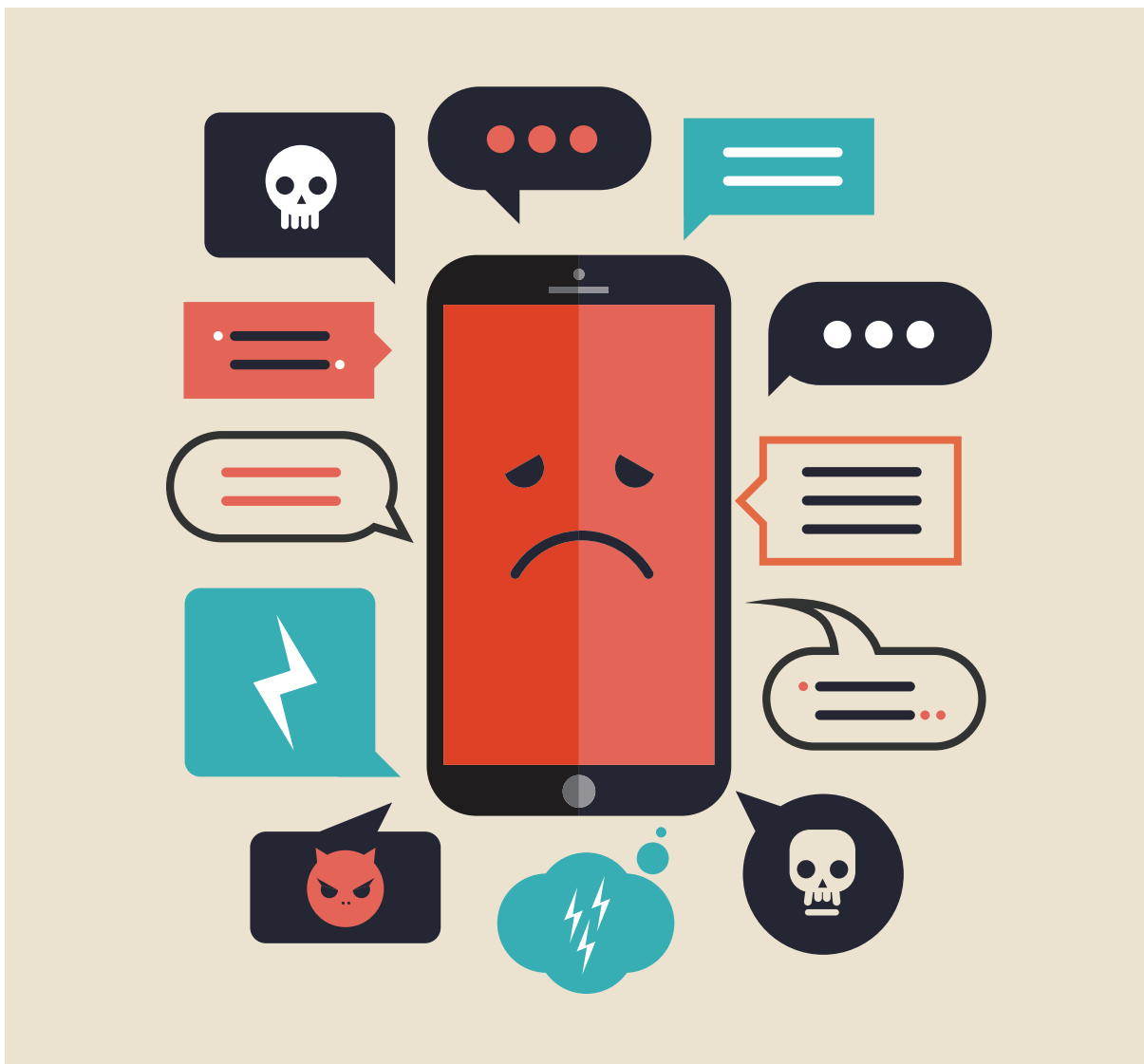


## INFORMAȚII SUPLIMENTARE

- Wikipedia are un articol despre cenzura în spațiul cibernetic: [http://en.wikipedia.org/wiki/Censorship\\_in\\_cyberspace](http://en.wikipedia.org/wiki/Censorship_in_cyberspace).
- Site-ul Diviziunii Mass-media a Consiliului Europei oferă informații despre activitatea acestuia privind promovarea auto-reglementării și a abilitării utilizatorului: <http://www.coe.int/media>.
- NetNanny la <http://www.netnanny.com> și Cyberpatrol la <http://www.cyberpatrol.com> sunt printre cele mai cunoscute produse de filtrare comerciale.
- Fundația Electronic Frontier (EFF) își propune să apere libertățile civile pe Internet: <http://www.eff.org/>.
- Proiectul SIP-Bench finanțat de UE publică anual, în nouă limbi, rezultatele unor studii comparative privind produsele de filtrare: <http://www.sipbench.eu/>
- Un studiu al Consiliului Europei privind tinerii, bunăstarea și riscul online (2006) explorează semnificația conținutului dăunător în ceea ce privește protecția copiilor și a tinerilor în societatea informațională: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680483b30>.
- Sistemul de etichetare PEGI Online oferă informații despre jocurile, categoriile, riscurile, sfaturile de siguranță în mediul online și o listă de site-uri web etichetate: <http://www.pegonline.eu>.
- Recomandarea CM/Rec(2008)6 a Comitetului de Miniștri către statele membre privind măsurile pentru promovarea respectării libertății de exprimare și de informare referitor la filtrele pentru rețeaua Internet: [https://wcd.coe.int/ViewDoc.jsp?p=&Ref=CM/Rec\(2008\)6&Language=lanEnglish&Ver=original&direct=true](https://wcd.coe.int/ViewDoc.jsp?p=&Ref=CM/Rec(2008)6&Language=lanEnglish&Ver=original&direct=true).
- Documente relevante ale Consiliului Europei: pentru mai multe informații cu privire la etichetare și filtrare: [www.coe.int/en/web/freedom-expression/internet-standard-setting](http://www.coe.int/en/web/freedom-expression/internet-standard-setting).



## Hărțuirea în mediul online: bullying-ul, stalking-ul și trolling-ul



**P**e măsură ce Internetul și tehnologia câștigă o arie de acoperire mai mare, numărul tentativelor de hărțuire a cunoscut o creștere.

— Potrivit unui studiu efectuat de Centrul de Cercetare Pew în 2014 în rândul adulților americani, există cel puțin șase forme diferite de hărțuire în mediul online: insultarea persoanelor (porecle obscene), punerea intenționată într-o situație jenantă a unei persoane, amenințarea fizică a unei persoane, hărțuirea continuă a unei persoane, hărțuirea sexuală sau urmărirea în scop de hărțuire a unei persoane. În același studiu, cercetătorii au identificat cinci fapte esențiale despre hărțuirea în mediul online:

1. Dintre persoanele intervievate, 40% de utilizatorii de Internet s-au confruntat personal cu hărțuirea în mediul online.
2. Adulții tineri constituie grupul demografic cel mai expus hărțuirii în mediul online.
3. Bărbații și femeile au experiențe diferite de hărțuire în mediul online.

4. Jumătate dintre persoanele hărțuite online nu cunosc cine este vinovatul.

5. Rețelele sociale au fost cel mai frecvent menționate ca fiind scena hărțuirii.

— Hărțuirea în mediul online presupune îndreptarea repetată de comentarii deranjante sau ofensive către anumite persoane vizate. Aceasta poate lua diverse forme, cum ar fi hărțuirea cibernetică, urmărirea cibernetică, trolling-ul sau răspândirea urii.



## CYBERBULLYING-UL

- Organizația Mondială a Sănătății definește bullying-ul drept „aplicarea intenționată a forței sau puterii fizice și psihologice, amenințătoare sau reale, împotriva sa, a altei persoane sau împotriva unui grup sau comunități, care duce sau poate duce la vătămare, deces, traume psihologice, anomalii de dezvoltare sau carență” (Organizația Mondială a Sănătății – 2002) *Raportul mondial privind violența și sănătatea: rezumat*<sup>1</sup>.
- Bullying-ul este o acțiune inițiată împotriva altei persoane pentru a provoca vătămări, repetată în diverse forme, pe parcursul unei perioade de timp. Părinții și copiii nu au, de obicei, aceeași percepție asupra amploarei acestei probleme.
- Bullying-ul poate lua diferite forme: abuz fizic, verbal, relațional, sexual, prejudiciabil, extorcare și cyberbullying (hărțuire cibernetică).
- Cyberbullying-ul reprezintă hărțuirea prin intermediul Internetului sau a telefonului mobil, implicând mesaje, emailuri, publicarea de comentarii jignitoare sau rău-intenționate în camerele de discuții sau forumurile de mesaje sau, chiar mai extrem, dezvoltarea de site-uri web cu intenția de a aduce prejudicii unei persoane sau anumitor grupuri de persoane.
- Agresorii care inițiază hărțuirea cibernetică utilizează, de asemenea, telefoanele mobile pentru a realiza fotografii jenante ale altor persoane sau pentru a trimite mesaje SMS sau MMS jignitoare. Toate formele de bullying online au un impact mult mai mare decât bullying-ul obișnuit, deoarece autorii trăiesc cu fermitate un sentiment de anonim, iar victimele nu au unde să se ascundă de agresor – persoanele pot fi victime zi și noapte, oriunde s-ar afla.
- Stalking-ul online reprezintă utilizarea Internetului sau a altor mijloace electronice pentru a urmări sau a hărțui o persoană, un grup sau o organizație<sup>2</sup>.
- Trolling-ul este acțiunea de a provoca probleme pe Internet prin inițierea de certe sau supărarea persoanelor, prin postarea de mesaje incendiare, care nu sunt la subiect sau mesaje în afara subiectului, într-o comunitate online, cum ar fi un grup tematic<sup>3</sup> sau un blog.
- Trolling-ul se face cu intenția deliberată de a provoca cititorii la un răspuns emoțional sau de a perturba, în alt mod, discuția normală pe un anumit subiect<sup>4</sup>.
- Deoarece stalking-ul online, trolling-ul și bullying-ul sunt, în general, considerate sub umbrela mai largă a hărțuirii în mediul online, liniile directe și informațiile de mai jos pot fi adaptate în funcție de cazurile individuale.



## IMPORTANȚA REZILIENȚEI ȘI A ÎNVĂȚĂRII SOCIALE ȘI EMOȚIONALE

- Reziliența și bunăstarea socială și emoțională sunt factori cruciali pentru a ajuta tinerii să învețe a se proteja împotriva bullying-ului, precum și a altor comportamente agresive online.
- Un climat școlar pozitiv sau o comunitate pozitivă poate atenua bullying-ul online și offline și, în general, hărțuirea online.
- Părinții își pot ajuta copiii să își dezvolte reziliența, ajutându-i să își sporească conștiința de sine și stima de sine, arătându-le că sunt acceptați și iubiți așa cum sunt, învățându-i să se adapteze,

1. [http://www.who.int/violence\\_injury\\_prevention/violence/world\\_report/en/summary\\_en.pdf](http://www.who.int/violence_injury_prevention/violence/world_report/en/summary_en.pdf)

2. <https://en.wikipedia.org/wiki/Cyberstalking>

3. [https://en.wikipedia.org/wiki/Usenet\\_newsgroup](https://en.wikipedia.org/wiki/Usenet_newsgroup), forum, chat room <[https://en.wikipedia.org/wiki/Chat\\_room](https://en.wikipedia.org/wiki/Chat_room)

4. [https://en.wikipedia.org/wiki/Internet\\_troll](https://en.wikipedia.org/wiki/Internet_troll)

să facă față și să depășească situațiile dificile, prin inspirarea emoțiilor pozitive, găsirea plăcerii și a umorului în viață, prin promovarea abilităților de rezolvare a problemelor, prin a-i învăța să fie flexibili în răspunsurile lor și arătându-le importanța empatiei.



## CONSIDERAȚII DE ORDIN ETIC ȘI RISCURI

- Bullying-ul și hărțuirea în sălile de clasă pot reduce moralul întregii clase, creând o atmosferă de frică și neîncredere și făcând învățarea aproape imposibilă.
- Cele mai frecvente consecințe cu care se confruntă cei care sunt victime ale bullying-ului sau ale hărțuirii includ depresia, anxietatea, stima de sine scăzută, dificultățile de adaptare socială și singurătatea.
- Pentru făptuitori, cele mai frecvente consecințe includ anxietatea sporită, riscul de eșec școlar și, adesea, comportamente delincvente și o probabilitate crescută de infracționalitate la vârsta adultă.
- O măsură preventivă pentru a evita ca bullying-ul sau hărțuirea să devină o problemă este introducerea în programul de învățământ a unor aspecte precum managementul relațiilor sociale, controlul furiei și soluționarea conflictelor. Atunci când sunt bine alese, acest tip de programe vor permite copiilor și adolescenților să își descopere propriile talente ca potențiali mediatori în cazul unor conflicte. În acest fel, riscul ca anumite conflicte minore să escaladeze într-un comportament amenințător va fi redus atât în mediul offline, cât și cel online.
- Școala dumneavoastră trebuie să aibă în vigoare o politică clară – numită și politică de utilizare responsabilă sau acceptabilă (PUR sau PUA)<sup>5</sup> – pentru a monitoriza când și cum elevii și personalul utilizează Internetul și telefoanele mobile la școală. Acest document trebuie să prevadă expres că limbajul și acțiunile vulgare, agresive sau hărțuitoare nu vor fi tolerate, iar cei care nu vor utiliza corespunzător Internetul sau telefonul vor fi subiecți ai unor sancțiuni.
- Trebuie să existe o procedură în vigoare care să poată documenta utilizarea Internetului, să identifice cine, când și unde este online, deși acest lucru poate ridica anumite probleme privind protecția datelor.
- Elevilor trebuie să li se comunice să întrerupă contactul cu orice persoană care îi hărțuiește sau îi face să se simtă inconfortabil atunci când se află online.
- Elevii trebuie să comunice imediat unui adult de încredere despre cele întâmplate și, dacă este posibil, să demonstreze materialul ofensator. Apoi, adultul va acționa conform procedurilor specificate în PUA sau PUR a școlii.
- Procedura este aceeași ca și în viața reală, când un copil este hărțuit de cineva. Acesta trebuie să întrerupă contactul cu făptuitorul și să informeze un adult de încredere despre incident. Copiii nu trebuie să simtă ca sunt singuri sau că trebuie să se ocupe singuri de problemă.

În concluzie, politica școlară privind utilizarea Internetului și a telefonului mobil trebuie să includă metode de intervenție, cum ar fi rezolvarea conflictelor, instruirea elevilor și a personalului cu privire la acțiunile întreprinse în caz de hărțuire online, oferirea de susținere pozitivă victimelor abuzului și, atunci când este posibil, ajutor pentru abuzatori în vederea schimbării de comportament. Cu o astfel de politică în vigoare, școlile nu ar trebui să se confrunte cu dificultăți în abordarea bullying-ului sau a hărțuirii.



## INSTRUCȚIUNI

— Educatorii s-au confruntat dintotdeauna cu bullying-ul și hărțuirea, în și în afara sălii de clasă. Este imperativ acum să înțelegem modul în care acest tip de hărțuire implică și Internetul.

5. [https://en.wikipedia.org/wiki/Acceptable\\_use\\_policy](https://en.wikipedia.org/wiki/Acceptable_use_policy)

- Elevii trebuie să fie capabili să își asume responsabilitatea pentru propriile acțiuni, însă bullying-ul și hărțuirea subminează încrederea și stima de sine. Atunci când o persoană este hărțuită sau abuzată psihologic, învățarea este restricționată, deoarece aceasta nu este capabilă să se concentreze, se simte amenințată și își pierde încrederea în sine.
- Elevii care se simt amenințați (fie online, fie offline) au nevoie de ajutorul unui adult de încredere. În același timp și persoana care inițiază bullying-ul sau hărțuirea are, de asemenea, nevoie de îndrumare, pentru ca acest comportament să nu se mai repete în viitor.
- Abordarea bullying-ului și a hărțuirii trebuie să fie globală, prin discuții deschise în familie sau în clasă, despre natura și posibila cauză a comportamentului inacceptabil și măsurile de remediere care pot fi implementate colectiv.
- Bullying-ul și hărțuirea sunt probleme sociale. Este responsabilitatea cadrelor didactice și a părinților să investigheze orice alegație privind o astfel de conduită și să lucreze în familie sau în clasă pentru a oferi cel mai bun mediu de învățare posibil: în sala de clasă, pe terenul de joacă și online.
- Cadrele didactice trebuie să fie instruite despre dinamica bullying-ului și hărțuire, precum și modul în care Internetul și telefoanele mobile sunt utilizate în acest scop. Acestea trebuie să învețe cum să citească semnalele victimelor, dar și ale persoanei care se face vinovată și cum să reacționeze atunci când observă astfel de semnale.
- Școlile trebuie să aibă în vigoare ghiduri specifice. Ar fi o idee bună să încorporați măsuri de prevenție cu privire la Internet în politica școlii dumneavoastră, pentru a face față bullying-ului și hărțuirii.
- Elevii trebuie să cunoască cele patru reguli de aur pentru a face față cyberbullying-ului sau hărțuirii online:
  1. Faceți o copie a materialului ofensator, dacă este posibil.
  2. Nu transmiteți altora materialul ofensator.
  3. Deconectați dispozitivul de recepție (calculator sau telefon mobil).
  4. Raportați incidentul unui adult de încredere.



## IDEI PENTRU LUCRUL ÎN CLASĂ

- Jocul de rol: elevii participă la un proces simulat de rezolvare a conflictului. Cadrul didactic atribuie rolurile și organizează grupuri în care elevii sunt responsabili pentru rezolvarea unei dispute. În faza următoare, rolurile sunt inversate, permițând elevilor să abordeze problema dintr-o perspectivă diferită.
- Grupuri de discuții: elevii participă în grupuri de discuții pentru a evalua participarea lor la lucrul în grup, impresiile lor pe teme cum ar fi bullying-ul în general, sugestii cu privire la ceea ce trebuie sau nu trebuie să faci pe Internet și responsabilități.



## BUNE PRACTICI

Iată câteva idei despre modul de a face față bullying-ului în mediul online și hărțuirii de orice gen prin emailuri sau mesaje:

- Elevii trebuie sfătuiți să nu deschidă emailurile din surse necunoscute.
- Dacă se deschide un mesaj email sau text și acesta este considerat ofensator, faceți o copie a materialului ofensator pentru a o arăta unui adult de încredere. Totuși, o victimă nu trebuie să reacționeze niciodată la mesaje ofensatoare, deoarece aceasta nu face decât să încurajeze cealaltă persoană să continue comportamentul ofensator.
- Dacă o persoană continuă să trimită emailuri sau mesaje ofensatoare sau hărțuitoare și este

posibil (prin intermediul adresei de email) să se afle de unde sunt acestea trimise, contactați imediat prestatorul de servicii<sup>6</sup> sau operatorul de telefonie mobilă vizat pentru a raporta hărțuirea.

- Politicile unei școli cu privire la bullying și/sau politica de utilizare acceptabilă trebuie să conțină dispoziții privind gestionarea cazurilor de hărțuire a elevilor în mediul online.
- Elevii trebuie să știe că se pot adresa unui părinte, cadru didactic sau altui adult de încredere ori de câte ori sunt hărțuiți în mediul online sau prin intermediul telefonului lor mobil. Este rolul acestui adult de încredere să ia relatarea în serios și să liniștească victima.
- Ocupați-vă de agresori sau de cei responsabili de hărțuire explicându-le că comportamentul lor nu poate fi tolerat și că trebuie să înceteze imediat, dar, de asemenea, aflați tot ceea ce puteți despre motivele acestora. Ar îndrăzni să spună sau să facă aceleași lucruri și în viața reală?
- Depuneți eforturi pentru a vă asigura că părinții sunt informați că copilul lor este abuzat psihologic sau fizic sau el/ea este un agresor. Atunci când un agresor folosește Internetul sau telefonul mobil pentru a abuza psihologic sau fizic, comportamentul ofensator nu se oprește, de obicei, la poarta școlii și va continua, probabil, și de acasă.
- ENABLE<sup>7</sup> (Rețeaua europeană împotriva bullying-ului în mediile de învățare și petrecere a timpului liber – European Network Against Bullying in Learning and Leisure Environments) este un proiect finanțat de Comisia Europeană și furnizează informații aprofundate cu privire la cele mai reușite abordări privind bullying-ul, precum și a învățării sociale și emoționale și furnizează pachete pentru părinți și seturi de instrumente de instruire pentru școli.



## INFORMAȚII SUPLIMENTARE

- Pagina web a Consiliului Europei „Învinge bullying-ul” („Beat bullying”) oferă instrumente împotriva acestui fenomen: <[www.coe.int/en/web/edc/beat-bullying](http://www.coe.int/en/web/edc/beat-bullying)>.
- NoBullying.com oferă resurse privind bullying-ul online și offline: <<http://nobullying.com/>>.
- Site-ul Zâmbetul Copilului (Smile of the Child), cu sediul în Grecia, oferă ajutor pentru problemele zilnice cu care se confruntă copiii: <<http://www.hamogelo.gr/1.2/home>>.
- „Alungați bullying-ul” („Stomp Out Bullying”): <<http://www.stompoutbullying.org>> „Oprțiți bullying-ul acum!” („Stop bullying now!”) este un site din SUA care vizează reducerea bullying-ului: <<http://www.stopbullyingnow.com/>>.
- „#DeleteCyberbullying” este o aplicație interactivă Android care oferă sfaturi cu privire la bullying-ul online: <<https://deletecyberbullying.wordpress.com/app/>>.
- „Cunoașteți riscurile: înfruntarea bullying-ului online” („Know the risks: challenging cyber bullying”) este destinat părinților și cadrelor didactice: <[http://web.archive.org/web/20100923133231/http://awareness.ca/english/teachers/wa\\_teachers/safe\\_passage\\_teachers/risks\\_bullying.cfm](http://web.archive.org/web/20100923133231/http://awareness.ca/english/teachers/wa_teachers/safe_passage_teachers/risks_bullying.cfm)>.
- „Ce este bullying-ul online?” („What is cyber bullying”) – o pagină web a Guvernului australian care oferă consultanță familiilor: <[http://web.archive.org/web/20090703064421/http://www.netalert.gov.au/advice/risks/cyber-bullying/What\\_is\\_cyber\\_bullying.html](http://web.archive.org/web/20090703064421/http://www.netalert.gov.au/advice/risks/cyber-bullying/What_is_cyber_bullying.html)>.
- Raportați bullying-ul și conținutul dăunător în rețeaua Insafe: <<http://www.betterinternetforkids.eu>>.

6. [https://en.wikipedia.org/wiki/Internet\\_service\\_provider](https://en.wikipedia.org/wiki/Internet_service_provider)

7. <http://enable.eun.org>

- Centrul de Cercetare Pew a publicat rezumatul constatărilor sale din 2014 privind „bullying-ul online”: <<http://web.archive.org/web/20160703044152/http://www.pewinternet.org/2014/10/22/online-harassment/>>.
- Mișcarea „Fără Instigare la Ură” este o campanie de tineret a Consiliului Europei: <<http://www.nohatespeechmovement.org/>>.
- Aflați mai multe despre bullying și descărcați planuri de lecții, pachete pentru părinți și echipamente de instruire pentru colegi: <<http://enable.eun.org/>>.



## Obținerea de asistență



Internetul este un sistem global de rețele informatice interconectate care utilizează suita de protocoale Internet (TCP/IP) pentru a conecta miliarde de dispozitive la nivel mondial<sup>1</sup>. Prin urmare, este destul de diferit de alte medii în sensul că este cel mai descentralizat mediu de comunicare care există. Nu are un punct unic de control datorită faptului că aceste miliarde de dispozitive slab conectate dispun de multiple și diferite canale pentru a permite comunicarea și transferul de informații. În plus, de la apariția Web 2.0, utilizatorii de rețele online nu sunt numai spectatori, ci și producători de informație (a se vedea Fișa 1 cu privire la conectare).

— În prezent, deoarece oricine poate publica aproape orice în mediul online și multe dintre datele noastre sunt stocate în locuri impalpabile cunoscute sub numele de „nor” (cloud), se pun multe întrebări despre viitorul Internetului și cum poate fi posibilă controlarea chiar și a unei mici părți a acestui flux de informații. Ne întrebăm adesea cine decide ce constituie limbaj și informație ofensatoare sau periculoasă pentru copiii noștri, pentru familia noastră și pentru noi. Și, mai important, cum putem să ne protejăm pe noi înșine și pe cei apropiați de acestea?

1. <https://en.wikipedia.org/wiki/Internet>



## CONȚINUT ILEGAL

— Fiecare țară definește ce conținut și acțiuni sunt legale și ilegale, prin legislația națională. În consecință, Internetul, ca mijloc de comunicare, funcționează ca un domeniu reglementat. Orice acțiune considerată a fi ilegală în „viața reală” trebuie considerată ilegală și pe Internet. Cu toate acestea, imensa acoperire a

— Internetului poate amplifica tentativele de încălcare a drepturilor altor persoane și poate multiplica impactul; de exemplu, „tachinarea” online poate deveni defăimare sau ceva mult mai grav.

— Conținutul ilegal poate fi definit drept orice activitate, material, informație etc. care contravine legii și poate dăuna și/sau provoca prejudicii unei persoane sau entități.

— Conținutul ilegal include imagini și site-uri web cu abuzuri asupra copiilor, activități ilegale în camerele de discuții (cum ar fi ademenirea copiilor), ura în mediul online, mesajele și site-urile web xenofobe și altele similare. Acestea și alte forme de comportament ilegal sunt reglementate de Convenția Consiliului Europei privind infracționalitatea informatică<sup>2</sup>, primul tratat internațional privind infracțiunile comise prin Internet și alte rețele informatice și Protocolul Adițional la Convenția privind infracționalitatea informatică ce ține de incriminarea actelor rasiste și xenofobe comise prin intermediul sistemelor informatice<sup>3</sup>. Convenția Consiliului Europei privind protecția copiilor împotriva exploatarei sexuale și a abuzului sexual (sau Convenția de la Lanzarote)<sup>4</sup> prevede, de asemenea, colectarea și stocarea neautorizată de date și exploatarea informațiilor. Această convenție este primul tratat internațional care impune pedepse penale pentru toate formele de violență sexuală împotriva copiilor, inclusiv ademenirea.



## OBȚINEREA DE ASISTENȚĂ ESTE UN DREPT FUNDAMENTAL!

— Internetul este un instrument care este ușor de accesat de oriunde și de oricine și, prin urmare, conținutul considerat ca fiind dăunător sau necorespunzător poate ajunge cu ușurință la copii, tineri și alte categorii vulnerabile ale populației. Dreptul la protecție împotriva prejudiciilor și la căile de atac împotriva discriminării sau încălcării de orice fel este un drept fundamental al omului, conform Declarației Universale a Drepturilor Omului<sup>5</sup>. În plus, Convenția ONU cu privire la drepturile copilului (CDC) subliniază rolul adulților de a acționa în interesul superior al copilului, protejându-l astfel de conținutul și acțiunile dăunătoare și pune responsabilitatea asupra guvernelor și familiilor, care trebuie să ia toate măsurile pentru a se asigura că drepturile copiilor sunt respectate, protejate și exercitate. Aceasta include furnizarea de servicii sociale, precum și instituirea de sisteme juridice, de sănătate și educaționale care să susțină copiii și să ofere un mediu în care aceștia să poată crește și atinge potențialul. Liniile de asistență și alte mecanisme de raportare constituie un element esențial în cadrul acestor sisteme.

— Împreună cu alte organizații internaționale, în special în cadrul activităților Forumului internațional pentru guvernarea Internetului, Consiliul Europei încearcă să dezvolte conștiința socială și familială cu privire la protecția copiilor și a tinerilor pe Internet. Aceasta include punerea la dispoziție a unor informații accesibile despre instrumentele și procedurile disponibile pentru obținerea asistenței adecvate.



## INSTRUCȚIUNI

- Conținutul ilegal de orice natură găsit pe Internet poate fi raportat la o linie telefonică de urgență. O linie telefonică de urgență<sup>6</sup> este un serviciu la care orice persoană poate raporta despre orice conținut online considerat a fi ilegal. INHOPE este o asociație care coordonează linia telefonică de urgență pentru Internet în multe țări din întreaga lume<sup>7</sup>.

2. <http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?CL=ENG&NT=185>

3. <http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189>

4. <http://www.conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=201&CM=8&DF=12/18/2008&CL=ENG;http://www.coe.int/en/web/children/lanzarote-convention>

5. <http://www.un.org/en/universal-declaration-human-rights/index.html>

6. <http://en.wikipedia.org/wiki/Hotline>

7. <http://inhope.org/gns/who-we-are/at-a-glance.aspx>

- Puteți găsi informații suplimentare despre tipul de conținut ilegal de care se ocupă INHOPE pe site-ul său web<sup>8</sup>.
- Pentru a raporta conținutul ilegal, accesați <<http://www.inhope.org/tns/contact-us/details.aspx>> și urmați pașii indicați. Linia telefonică de urgență va investiga raportul<sup>9</sup> pentru a vedea dacă conținutul este ilegal și, dacă da, va urmări originea acestuia și va contacta organele de drept din țara gazdă, precum și prestatorul de servicii Internet, pentru eliminarea conținutului în cauză.

### Solicitarea de asistență de la o linie telefonică

- Copiii și tinerii pot solicita asistență apelând la o linie telefonică<sup>10</sup> – un serviciu care oferă asistență prin telefon și/sau consiliere prin email, web sau SMS.
- În multe țări, centrele de informare ale Insafe<sup>11</sup> cooperează cu linii de asistență naționale pentru a răspunde la întrebările și preocupările tinerilor referitoare la experiențele acestora în mediul online sau la conținutul online dăunător sau ilegal cu care se confruntă. De asemenea, multe linii de asistență care se ocupă de problemele legate de Internet pot ajuta tinerii preocupați de alte chestiuni „din lumea reală”.
- Child Helpline International<sup>12</sup> este un punct important de contact în multe țări europene și non-europene. Această rețea globală de linii de asistență pentru copii operează în aproape 150 de țări pentru a proteja drepturile copilului.
- De regulă, liniile de asistență telefonică sunt disponibile 24 de ore pe zi, 7 zile pe săptămână. Serviciile acestora sunt gratuite și confidențiale și nu urmăresc apelurile, emailurile sau textele. Copiii și adolescenții pot trimite mesaje pe diverse subiecte și există facilități pentru a permite tinerilor să comunice prin chat, email și forumuri, precum și prin metode mai tradiționale. Personalul liniilor de asistență telefonică este acolo ca să asculte și să-i ajute să își găsească propriile soluții.
- Pentru a găsi o linie de asistență telefonică în țara dumneavoastră, dați în căutare pe Internet denumirea țării și cuvintele „raport” și „linie de asistență”.

### Utilizarea serviciilor de raportare dedicate pe platformele sociale

- Majoritatea platformelor sociale media, cum ar fi Facebook, Twitter, Instagram sau Google, au un centru de siguranță pentru a oferi îndrumare utilizatorilor și un serviciu de raportare online pentru a semnaliza conținutul sau activitatea necorespunzătoare. Acest lucru se găsește de obicei în meniul „Suport” sau „Ajutor”. De exemplu, raportarea cazurilor de bullying rețelelor de socializare, poate duce la eliminarea conținutului ofensator și chiar la ștergerea conturilor persoanelor care au încălcat termenii de utilizare. Majoritatea site-urilor lucrează similar: de exemplu, pe Facebook, fiecare element de conținut are un meniu derulant, care permite utilizatorilor să raporteze o postare sau o fotografie și să spună de ce nu doresc să o vadă. Această pagină, de exemplu, conține informații despre întocmirea unui raport<sup>13</sup>.
- Toți operatorii de telefonie mobilă oferă asistență prin telefon, webchat sau email și mulți oferă, de asemenea, recomandări adresate în mod special familiilor și copiilor. De exemplu, Vodafone are un site web despre „Parentajul digital”<sup>14</sup> care oferă consiliere părinților și copiilor și ghiduri de „instruire” pentru configurarea controalelor parentale. Acesta propune și servicii de control parental și alte funcții de siguranță prin intermediul SecureNet<sup>15</sup>. Aplicația Guardianul Vodafone de pe dispozitivele Android permite, de asemenea, blocarea contactelor nedorite.

8. <http://www.inhope.org/gns/internet-concerns/overview-of-the-problem/illegal-content.aspx>

9. <http://www.inhope.org/en/about/faq.html>

10. <http://en.wikipedia.org/wiki/Helpline>

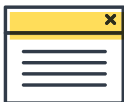
11. <http://www.betterinternetforkids.eu>

12. <http://www.childhelplineinternational.org>

13. <https://www.facebook.com/help/181495968648557/>

14. <http://www.vodafone.com/content/digital-parenting.html>

15. <https://securenet.vodafone.com/>



## INFORMAȚII SUPLIMENTARE

- Consultați CONUDR <<http://www.ohchr.org/en/professionalinterest/pages/crc.aspx>> și/sau documentul general elaborat de UNICEF <[http://www.unicef.org/crc/files/Rights\\_overview.pdf](http://www.unicef.org/crc/files/Rights_overview.pdf)> pentru informații suplimentare despre dreptul copiilor la protecție și asistență.
- Pentru informații detaliate privind protecția împotriva violenței și raportarea acesteia, Strategia integrată a Consiliului Europei împotriva violenței oferă informații utile la: <<http://www.coe.int/en/web/children/integrated-strategies>>.
- Pentru a raporta conținut ilegal, puteți contacta INHOPE: <<https://www.inhope.org/>>.
- Portalul Insafe, rețeaua europeană a centrelor de siguranță pe Internet <<http://www.betterinternetforkids.eu/>> oferă informații despre punctele naționale de contact și liniile de asistență din Europa.
- Pentru a raporta cyberbullying-ul sau pentru a obține asistență, puteți contacta Childline <<http://www.childline.org.uk/>>, o linie telefonică gratuită de 24 de ore pentru copii și tineri (Telefon: 0800 1111).
- Befrienders.org <<http://www.befrienders.org>> este un site pe care puteți găsi cea mai apropiată linie telefonică de asistență anti-suicid.
- Europe Direct <[http://ec.europa.eu/europedirect/index\\_en.htm](http://ec.europa.eu/europedirect/index_en.htm)> este un serviciu gratuit în cadrul căruia puteți obține răspunsuri imediate la întrebările generale privind problemele UE și detaliile de contact ale organizațiilor relevante, cum ar fi liniile de asistență naționale.

## 6. Internetul – o privire în viitor

---

” „Expresia liberă este temelia drepturilor omului, sursa umanității și mama adevărului. A ucide libertatea de exprimare înseamnă să încalci drepturile omului, să sugrumi omenirea și să suprimi adevărul.”

*Liu Xiaobo, laureat al Premiului Nobel pentru Pace din 2010 și activist pentru drepturile omului*

### LISTA DE VERIFICARE PENTRU FIȘA 23 – INTERNETUL OBIECTELOR

---

În același mod în care vă protejați deja calculatorul și alte dispozitive împotriva intruziunilor de securitate, asigurați-vă că aplicați respectivele măsuri dispozitivelor dumneavoastră împotriva „Internetului obiectelor”.

Este dificil să protejați fiecare dispozitiv în parte, dar vă puteți proteja rețeaua și reduce zonele de vulnerabilitate.

Analizați cu atenție orice articole de tipul „Internetul jucăriilor” pe care intenționați să le introduceți în casa dumneavoastră și să le prezentați copilului dumneavoastră. Verificați parametrii de securitate și de confidențialitate ai jucăriei și puneți-vă întrebarea: „Cât de necesară este această jucărie?”

### LISTA DE VERIFICARE PENTRU FIȘA 24 – INTELIGENȚA ARTIFICIALĂ, AUTOMATIZAREA ȘI TEHNOLOGIILE PERTURBATOARE

---

V-ați informat despre ultimele noutăți în domeniul inteligenței artificiale și al automatizării?

Ați investit în competențele dumneavoastră interpersonale, sociale și emoționale?

V-ați configurat dispozitivele „inteligente” pentru a asigura niveluri adecvate de securitate și de protecție a utilizatorilor?

### LISTA DE VERIFICARE PENTRU FIȘA 25 – REALITATEA VIRTUALĂ ȘI REALITATEA AUGMENTATĂ

---

Ați discutat cu copilul / elevul dumneavoastră despre subiecte cheie precum sexismul, sexualitatea, rasismul, abuzul psihologic, stereotipurile și alte forme de discriminare?

V-ați asigurat că dispozitivele pe care le utilizează copilul / elevul dumneavoastră sunt configurate corect, cu o protecție ridicată a vieții private și a securității?

Ați verificat dacă copilul / elevul dumneavoastră menține echilibrul unei vieți sănătoase atunci când utilizează tehnologia virtuală sau augmentată?

### LISTA DE VERIFICARE PENTRU FIȘA 26 – SUNTEȚI PRODUSUL? VOLUMELE MARI DE DATE (BIG DATA), EXTRAGEREA DE DATE ȘI VIAȚA PRIVATĂ

---

V-ați făcut timp să examinați modul în care datele dumneavoastră private sunt tratate de serviciile online pe care le utilizați și să configurați setările de confidențialitate adecvate?

Ați revizuit recent conținutul pe care l-ați postat online pentru a vă asigura că încă este corect și că sunteți în continuare dispus să îl distribuiți?

V-ați informat cu privire la ultimele evoluții în domeniul „big data” pentru a înțelege modul în care aceste schimbări vă pot afecta și ce puteți face în legătură cu aceasta?



## Internetul obiectelor



**P**rogresele tehnologice evidențiate de recenta dezvoltare a conectivității prin Internet și wireless la dispozitivele adaptate pentru transferuri de date, provoacă entuziasm în multe domenii. Acest domeniu emergent, cunoscut sub numele de „Internetul obiectelor” (IO), în care dispozitivele conectate la Internet îmbunătățesc eficiența companiei și confortul stilului de viață pot, de asemenea, provoca îngrijorări uriașe nu doar părinților, ci tuturor.

Preocupările legate de securitate, viață privată și colectarea datelor sunt doar câteva aspecte pe care experții și decidenții politici încearcă să le abordeze, pe măsură ce tot mai multe dispozitive sunt proiectate și vândute. Cu toate acestea, IO prezintă o provocare specială prin faptul că experții și factorii de decizie trebuie să găsească modalități unice de a promova beneficiile acestei noi tehnologii, dar restrângând și chiar reducând, în același timp, riscurile.

■ Faptul că „obiectele încep să gândească” pune în gardă consumatorii, care trebuie să își facă griji și de spărgătorii de coduri care pot să le acceseze „obiectele”. Citiți acest articol recent „Hackeriiucid de la distanță un Jeep pe o autostradă”<sup>1</sup> în care doi spărgători de coduri s-au jucat de la distanță cu climatizorul, radio-ul și ștergătoarele de parbriz, înainte de a opri motorul unui vehicul. Acțiunile celor doi hackeri au declanșat dezbateri cu privire la securitatea digitală pentru autoturisme și camioane.

■ Un alt domeniu de dezbateri este ideea că IO reprezintă următoarea revoluție industrială. În prezent există aproximativ 10 miliarde de dispozitive conectate, însă potrivit prognozelor, se preconizează o creștere, cifra atingând până în 2020, între 26 miliarde și 30 miliarde de dispozitive, cu o valoare estimată a pieței între 6 și 9 trilioane de dolari SUA<sup>2</sup>.

■ Acest lucru va duce la o explozie a dispozitivelor conectate și la o explozie corespunzătoare a datelor. Regulamentul General privind Protecția Datelor se va confrunta cu noi provocări pentru protecția vieții private, atunci când datele vor fi omniprezente.



## INTERNETUL OBIECTELOR

- Termenul „Internetul obiectelor” a apărut pentru prima dată în 1999, dar abia câțiva ani mai târziu am văzut existența reală a obiectelor conectate la Internet.
- IO<sup>3</sup> este rețeaua de obiecte fizice sau obiecte echipate cu electronică, programe, senzori și conectivitate pentru a le permite să colecteze și să facă schimb de date.
- IO este utilizat pentru a descrie totul, de la termostatele inteligente care pornesc căldura înainte ca dumneavoastră să ajungeți acasă, la frigiderul care comandă suc de portocale atunci când acesta s-a terminat. Oamenii poartă dispozitive de monitorizare a sănătății și de fitness, iar animalele sunt dotate cu dispozitive de monitorizare a sănătății și localizării<sup>4</sup>.
- IO înseamnă, pur și simplu, conectivitate la Internet, dispozitivele comunicând unele cu celelalte, facilitând controlul și automatizarea sarcinilor – colectarea datelor.
- Centrul de Cercetare Pew crede că IO și „dispozitivele portabile” vor avea efecte larg răspândite și benefice<sup>5</sup> până în 2025.



## TEHNOLOGIA WEARABLE (PURTATĂ DE UTILIZATOR)

- „Tehnologia purtată” sau „dispozitivele purtate” sunt articole de îmbrăcăminte și accesorii care încorporează calculatoare și tehnologii electronice avansate.
- Dispozitivele purtate sunt numite, de asemenea, tehnologii la modă, dispozitive purtate, îmbrăcăminte tech sau electronice fashion<sup>6</sup>.
- Dispozitivele portabile oferă date instantanee utilizatorului și utilizatorul poate monitoriza instantaneu tehnologia, le poate descărca pentru utilizare ulterioară sau poate trimite datele pentru imprimare.



## INTERNETUL JUCĂRIILOR

- IO poate fi, de asemenea, aplicat jucăriilor pentru copii. Conectivitatea wireless va permite unei jucării să interacționeze cu alte dispozitive cu date sau cu alte jucării.
- Internetul jucăriilor prezintă noi modalități de a-i familiariza pe tineri cu tehnologia și îi încurajează adesea să interacționeze cu jucăria.

1. <http://web.archive.org/web/20160703222843/https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway>

2. <https://securityintelligence.com/data-protection-in-the-internet-of-things/>

3. [https://en.wikipedia.org/wiki/Internet\\_of\\_Things](https://en.wikipedia.org/wiki/Internet_of_Things)

4. <http://web.archive.org/web/20160310125239/http://www.theguardian.com/technology/2015/mar/30/internet-of-things-convenience-price-privacy-security>

5. [http://www.pewinternet.org/files/2014/05/PIP\\_Internet-of-things\\_0514142.pdf](http://www.pewinternet.org/files/2014/05/PIP_Internet-of-things_0514142.pdf)

6. [https://en.wikipedia.org/wiki/Wearable\\_technology](https://en.wikipedia.org/wiki/Wearable_technology)



- Hello Barbie este o afacere legată de Internetul jucăriilor, lansată de Mattel în 2015, centrată pe păpușa Barbie care poate asculta copiii. Acest fapt a provocat îngrijorare în rândul părinților și experților în materie de confidențialitate, precum și psihologilor de top, care se întrebă dacă aceste tipuri de jucării pot provoca probleme de dezvoltare la copii, afectându-le capacitatea de a crea, imagina și învăța în mod autonom. ToyTalk, o companie înființată în 2011, oferă o opinie diferită și susține că jucăriile care vorbesc și jucăriile echipate cu Wi-Fi pot oferi copiilor oportunități de învățare<sup>7</sup>.
- În ciuda confortului oferit de Internetul lucrurilor și dispozitivele purtate și în ciuda amuzamentului și distracției oferite de Internetul jucăriilor, utilizatorii ar putea să nu fie suficient de conștienți de faptul că IO și dispozitivele jucării, la fel ca telefoanele inteligente și calculatoarele, pot prezenta riscuri de securitate și confidențialitate. În cazul jucăriilor, pot exista chiar și riscuri pentru dezvoltarea copilului.



## IMPORTANȚA ÎNȚELEGERII PROBLEMELOR

- IO include dispozitive purtate pe care mulți utilizatori nu le consideră „dispozitive de calcul”; astfel, aceștia riscă să ignore problemele legate de viața privată.
- Viziunile tehnofuturiste ale IO și ale dispozitivelor purtate sunt atractive pentru multă lume. Cu toate acestea, disponibilitatea IO implică și nevoia de a efectua mai multe cercetări, deoarece firmele de securitate cibernetică au constatat în trecut că persoanele cu intenții infracționale acționează tenace și mai rapid pentru a inventa noi modalități de a-și atinge scopul final.
- Progresul companiilor de jucării în domeniul IO înseamnă jucării noi fantastice pentru tineri, dar părinții trebuie să înțeleagă riscul de a avea dispozitive cu microfon deschis în mâinile tinerilor și legături de date deschise în casele lor.



## CONSIDERAȚII DE ORDIN ETIC ȘI RISCURI

Scopul final al IO este creșterea eficienței, însă interconectivitatea care însoțește această eficiență sporită poate prezenta riscuri considerabile.

- Ideea că oamenii vă pot accesa de la distanță dispozitivele și datele este o perspectivă înspăimântătoare.
- Majoritatea dispozitivelor și articolelor purtate nu sunt concepute pentru o siguranță sau confidențialitate optimă.
- Intruziunile recente au arătat că spărgători de coduri îi văd pe oameni în casele lor, prin sistemele de monitorizare bebeluși și camerele web<sup>8</sup>.
- Consumatorii pot fi la fel de expuși „riscului” de intruziune cibernetică în casele lor, cum erau pe vremuri expuși intruziunii fizice.
- Consumatorii trebuie să fie conștienți de faptul că Regulamentul General privind Protecția Datelor le oferă controlul asupra datelor lor și aceștia ar trebui să se informeze despre punerea acestuia în practică.



## INSTRUCȚIUNI

- Dispozitivele IO variază în dependență de design și funcție. Citirea instrucțiunilor și înțelegerea funcționalităților dispozitivului este esențială pentru utilizarea corectă a dispozitivului.
- Este necesar să treceți prin setările pentru funcții, în scop de a dezactiva sau a activa parametrii de confidențialitate în dependență de dorințele dumneavoastră.

7. [http://web.archive.org/web/20150604014333/http://www.nytimes.com/2015/03/29/technology/a-wi-fi-barbie-doll-with-the-soul-of-siri.html?\\_r=0](http://web.archive.org/web/20150604014333/http://www.nytimes.com/2015/03/29/technology/a-wi-fi-barbie-doll-with-the-soul-of-siri.html?_r=0)  
 8. <http://web.archive.org/web/20160406200102/http://www.bbc.com/news/technology-30121159>

- Este necesar de a examina dispozitivul înainte de cumpărare deoarece unele dispozitive purtate au fost retrase de pe piață sau nu funcționează după cum au fost comercializate.
- Rețineți faptul că acesta este un domeniu în curs de dezvoltare și, dacă așteptați câteva săptămâni sau luni, întotdeauna va apărea ceva mai nou, mai bun și adesea mai ieftin pe piață.



## IDEI PENTRU LUCRUL ÎN CLASĂ

- Rugați elevii să creeze o listă cu toate dispozitivele posibile care ar putea fi conectate într-o locuință. Apoi, cereți-le să prezinte potențiale riscuri de securitate sau confidențialitate. Ce poate face utilizatorul pentru a reduce riscurile? Ce poate face furnizorul de dispozitive? Ce poate face prestatorul de servicii Internet?
- După o discuție referitoare la IO, rugați elevii să elaboreze potențiale instrucțiuni pentru consumatori, pentru a-i ajuta să înțeleagă problemele de securitate.
- Citiți un rezumat al Regulamentului General privind Protecția Datelor și solicitați elevilor să enumere toate clauzele referitoare la IO9.
- Descărcați videoclipul despre campania de conștientizare a drepturilor consumatorilor<sup>10</sup> și implicați elevii într-o discuție despre drepturile consumatorilor și IO.
- Rugați tinerii să „dezvolte” noi jucării pentru Internetul jucăriilor. Care sunt avantajele jucăriei? Care sunt riscurile? Cum pot aceștia să îi protejeze pe tinerii utilizatori? Cum pot să îi convingă pe părinți că jucăria este sigură?



## BUNE PRACTICI

- Este important să fim deschiși față de adoptarea acestei noi tehnologii, dar trebuie să vă asigurați că luați măsurile de securitate adecvate pentru a vă proteja datele și viața privată.
- Limitați informațiile personale pe dispozitivele adaptate pentru transferuri de date.
- Îmbunătățiți securitatea rețelei wireless de acasă.
- Alegeți parole puternice.
- Dacă este posibil, păstrați anumite dispozitive separate de celelalte.
- Limitați interacțiunile Internetului jucăriilor cu celelalte dispozitive ale dumneavoastră și asigurați-vă că monitorizați capacitățile acestora.

### **Consumatorii trebuie să fie atenți la mai multe aspecte atunci când selectează un dispozitiv IO:**

- Compatibilitatea și interoperabilitatea: dispozitivul este compatibil cu cele produse de alte companii sau trebuie să rămâneți în același „ecosistem” pentru a-l putea utiliza? Acest lucru este extrem de important, deoarece altfel, vă veți limita la acel producător, fără nicio modalitate de a comuta sau integra alte dispozitive de la alți producători.
- Conectivitatea: dispozitivul IO se bazează numai pe conectivitatea la Internet pentru a funcționa corect? În mod ideal, ar trebui să puteți accesa dispozitivul fără a trebui să vă conectați la Internet. Acest lucru este cu atât mai important, cu cât, în cazul în care producătorul de dispozitive închide platforma online pentru accesarea dispozitivului dumneavoastră, acesta va deveni efectiv inutil.
- Limit Internet of toy interactions with your other devices, and be sure to monitor their capabilities.

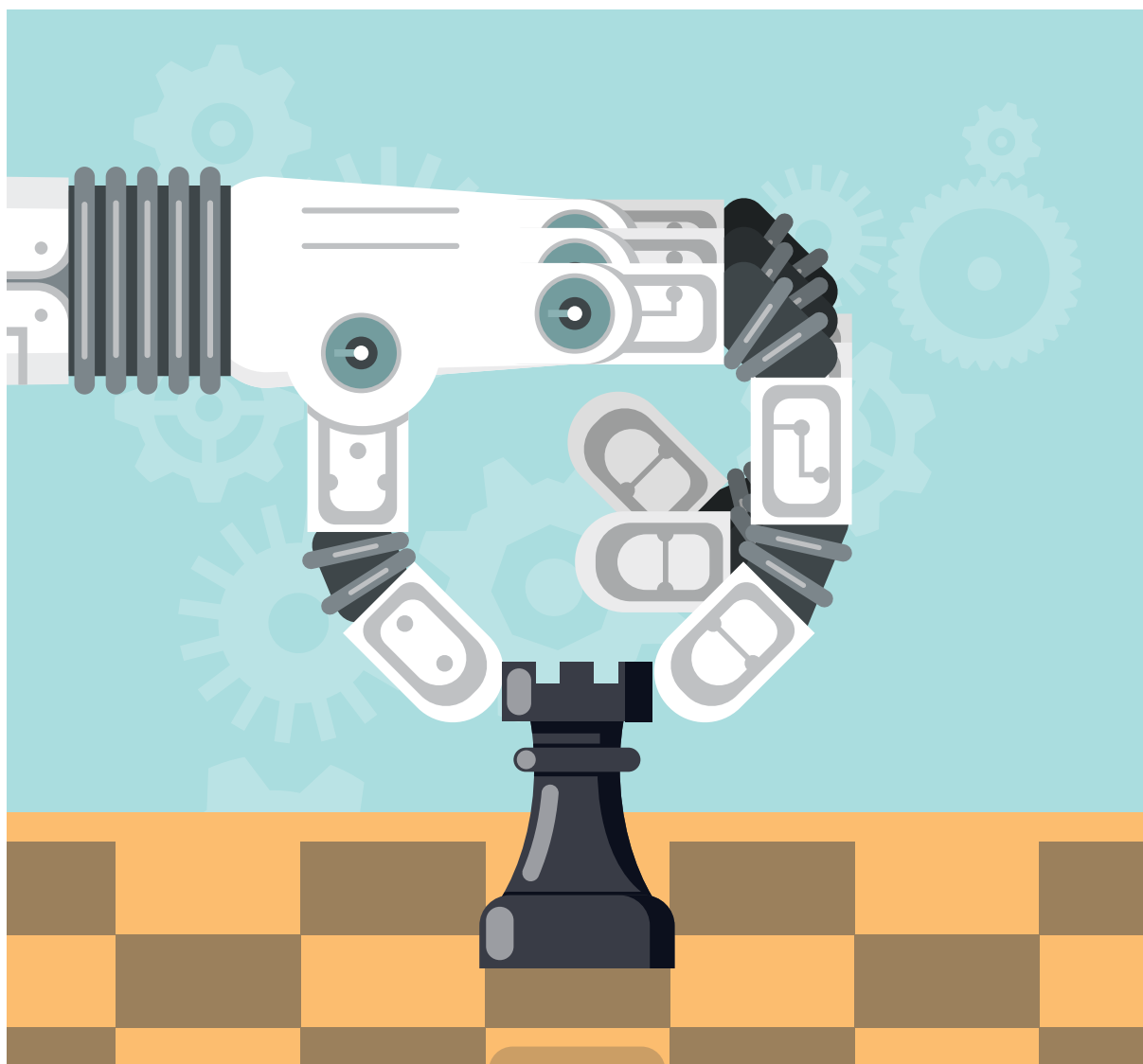


## INFORMAȚII SUPLIMENTARE

- Mai multe informații despre „Dreptul și legislația UE cu privire la consumatori” pot fi găsite la: [http://ec.europa.eu/consumers/consumer\\_rights/index\\_en.htm](http://ec.europa.eu/consumers/consumer_rights/index_en.htm).
- The Guardian a realizat rapoarte cu privire la Internetul obiectelor: <http://www.theguardian.com/technology/internet-of-things>.
- Mai multe informații referitoare la Internetul obiectelor pot fi găsite în infograficele Intel: [www.intel.com/content/www/us/en/internet-of-things/infographics/guide-to-iot.html](http://www.intel.com/content/www/us/en/internet-of-things/infographics/guide-to-iot.html).
- Disney a realizat cercetări despre Internetul jucăriilor: <http://www.disneyresearch.com/project/calipso-internet-of-things/>.
- Un ghid despre Internetul jucăriilor poate fi găsit la adresa: <http://www.mutualmobile.com/posts/iot-internet-toys>.
- Există, de asemenea, informații detaliate de la Centrul de Media Digital pentru Copii: <http://cdmc.georgetown.edu/publications-and-papers/textbooks/>.
- Documente relevante ale Consiliului Europei: „Drepturile omului pentru utilizatorii de Internet – Copiii și tinerii” <http://www.coe.int/en/web/internet-users-rights/children-and-young-people>.



## Inteligența artificială, automatizarea și tehnologiile perturbatoare



■ „Automatizarea”<sup>1</sup> este procesul prin care orice acțiune sau funcție operată de o persoană umană este înlocuită de o mașină, iar „intelența artificială”<sup>2</sup> este intelența mașinilor sau a programelor.

■ În multe momente de-a lungul istoriei, progresul tehnologic a distrus locuri de muncă și a creat altele noi. De exemplu, ca profesie, operatorul de telefonie a dispărut complet, odată cu evoluția tehnologiei telecomunicațiilor. Perturbările de pe piața muncii cauzate de revoluțiile tehnologice nu sunt un fenomen nou, dar de fiecare dată societatea se teme că nu vor exista suficiente locuri de muncă noi pentru a le compensa pe cele pierdute.

■ Până în prezent, astfel de temeri au fost, în mare parte, nejustificate deoarece au fost create locuri de muncă pe care nimeni nu și le putea imagina: acestea au fost create în număr suficient pentru a compensa locurile de muncă dispărute. De exemplu, nimeni nu își imagina în urmă cu două decenii, că va exista o funcție precum „manager de rețele sociale” sau „optimizer al motoarelor de căutare”.

1. <https://en.wikipedia.org/wiki/Automation>

2. [https://en.wikipedia.org/wiki/Artificial\\_intelligence](https://en.wikipedia.org/wiki/Artificial_intelligence)

■ În același timp, evoluțiile tehnologice actuale în domeniul inteligenței artificiale, al învățării automate și al automatizării amenință o proporție mult mai mare a pieței muncii, nu doar locurile de muncă slab calificate.



## NOI PROGRESE

### Mașinile autonome

■ Deși avem de făcut un drum lung înainte ca autovehiculele autonome să fie disponibile și produse în masă, progresul în acest domeniu este incontestabil. De exemplu, Tesla face deja mașini capabile să se conducă singure pe o autostradă. Urmare a primului accident fatal din mai 2016, cauzat de o eroare de program la o mașină Tesla, se va determina viitorul tehnologiei auto-conducerii. Cel mai mare obstacol nu este tehnologia însăși, ci problema responsabilității în caz de accident și ajustarea necesară a legii la situațiile în care mașinile iau decizii critice. Dar odată ce aceste obstacole vor fi eliminate, taximetriștii, șoferii de camion și conducătorii de transport public (metrou, autobuz, tramvai) vor dispărea. În UE, industria transporturilor reprezintă 4,5% din totalul locurilor de muncă.

### Site-uri web, aplicații, jocuri generate automat

■ Web design-ul este o profesie recentă, dar e posibil să dispară chiar mai repede decât operatorii de telefonie. În zilele noastre, având constructori de site-uri web, crearea unui site a devenit tot mai ușoară, utilizatorul trebuind doar să manipuleze, pur și simplu, conținutul prin glisarea și plasarea acestuia pe ecran. Algoritmii complecși sunt acum capabili să vă genereze site-ul în mod automat, în funcție de preferințele dumneavoastră. „The Grid”<sup>3</sup> este primul serviciu care propune generarea automată de site-uri web, în funcție de preferințele dumneavoastră. Acesta are nevoie doar de imagini, de conținut și de anumite informații privind scopul site-ului dumneavoastră web și preferințele dumneavoastră, pentru a genera un site web complet accesibil (compatibil pentru toate ecranele, de la calculatoare la telefoane inteligente). Acesta este doar începutul. Pe măsură ce inteligența artificială, algoritmii și învățarea automatizată avansează, multe locuri de muncă care necesitau abilități de programare vor fi automatizate, rămânând doar locurile de muncă ce necesită foarte multă creativitate, personalizare sau inovare.

### Arta generată aleatoriu

■ Datorită progreselor înregistrate în domeniul învățării automatizate, calculatoarele au acum posibilitatea de a realiza creații artistice variind de la imagini și picturi, la muzică. Generatorul Google „Deep Dream”<sup>4</sup> vă analizează imaginea și vă prezintă obiecte imaginare în interior, la fel ca atunci când priviți norii și vi se pare că vedeți un câine sau o floare. Alte programe sunt capabile să imite stilul unui pictor, precum Van Gogh sau Picasso și să îl aplice oricărei fotografii pe care ați realizat-o<sup>5</sup>. În muzică, Emily Howell<sup>6</sup> este un program capabil să analizeze partiturile muzicale, deducând „regulile” sau „tiparele” și să compună muzică într-un gen similar. Deși acest lucru nu înseamnă dispariția artiștilor, cu siguranță va avea un impact asupra artei.

### Roboții și autoservirea

■ Marii comercianți cu amănuntul online, cum ar fi Amazon, investesc din greu în roboți pentru ca aceștia să îndeplinească sarcinile, cum ar fi sortarea și organizarea produselor sau împachetarea produselor pentru livrare. Primul hotel administrat în întregime de roboți și-a deschis ușile în Japonia. Auto-scanarea la casele din supermarketuri, autoservirea în restaurante, liniile industriale de asamblare robotizate, asistenții roboți în asistență medicală și îngrijirea vârstnicilor, procesele automatizate de expediere a cumpărăturilor online și servicii precum hotelurile, încep să fie gestionate de roboți. La nivel global, vor apărea tot mai multe exemple de automatizare. Odată cu apariția imprimării 3D, chiar și lucrările de construcție pot fi automatizate!

3. <https://thegrid.io/>

4. <http://deepdreamgenerator.com/>

5. <http://web.archive.org/web/20160114142911/http://arxiv.org/pdf/1508.06576v2.pdf>

6. <http://artsites.ucsc.edu/faculty/cope/Emily-howell.htm>

## Algoritmi predictivi și exacti

— Datorită combinării big data, a super-calculatoarelor și a algoritmilor puternici, multe sectoare precum sănătatea vor suferi o nouă revoluție. Cu cantități masive de date disponibile în domeniul dat, algoritmi devin mai buni decât medicii la stabilirea unei diagnoze reieșind din simptome, informațiile transmise de senzori în timp real și datele din anamneză.

## IA și învățarea automatizată

— Cu ajutorul programelor și a calculatoarelor avansate, astăzi este posibil ca mașinile să învețe fie prin observarea acțiunilor umane ca să deducă anumite „reguli” sau „tipare” și să le imite, fie prin practicare, examinând rezultatele anumitor acțiuni, inferând astfel „regulile”. De exemplu, programele de calculator au reușit cu succes să încheie jocuri video, „învățând” cum să învingă inamicii, să sară peste obstacole și așa mai departe. Nu se poate spune cât de mult vor putea aparatele să „învețe” în viitor, dar în prezent este deja clar că sarcinile repetitive sunt la îndemâna acestora.



## BENEFICIILE EDUCAȚIONALE

- Învățarea codificării permite o mai bună înțelegere a roboticii și a programelor, inclusiv aspectele de bază ale IA și ale automatizării. Acest lucru este extrem de important pentru identificarea și îmbunătățirea competențelor care nu sunt încă accesibile calculatoarelor și roboților și pentru dezvoltarea competențelor care vor fi necesare pentru a îmbunătăți și mai mult aceste tehnologii. Având în vedere că locurile de muncă repetitive și care implică o calificare redusă sunt preluate de roboți, nu ne mai rămâne altceva decât să învățăm și mai mult.
- În același timp, învățarea despre automatizare și IA va contribui la modelarea opiniilor privind politicile care vor asigura că impactul acestora va aduce beneficii societății în ansamblu. De exemplu, mulți autori care scriu despre automatizare și IA susțin existența unui salariu universal și a unui program de lucru redus. O serie de oameni de știință, cercetători și figuri proeminente, precum Stephen Hawking, au semnat o scrisoare deschisă prin care solicită o direcție clară privind dezvoltarea IA pentru a evita înrobirea într-o bună zi a umanității de către roboți<sup>7</sup>.



## CONSIDERAȚII DE ORDIN ETIC ȘI RISCURI

### Lipsa locurilor de muncă

— Riscul cel mai evident al IA și al automatizării este crearea unui număr mai mic de locuri de muncă comparativ cu cele care sunt înlocuite. Deși este imposibil să se prevadă locurile de muncă care ar putea fi create odată cu avansarea acestor tehnologii, aceste noi locuri de muncă vor necesita o forță de muncă de înaltă calificare și vor exista puține oportunități de angajare pentru persoanele care vor avea doar studii medii.

### Creșterea inegalităților

— Deoarece locurile de muncă slab calificate devin tot mai limitate, va exista o inegalitate tot mai mare între cei care dispun de competențe vandabile și cei ale căror competențe sunt înlocuite treptat de roboți. O altă formă de inegalitate va afecta, de asemenea, țările; unele țări vor avea expertiza tehnologică pentru a face tranziția la automatizare și inovațiile IA, în timp ce altele se vor baza pe forța de muncă manuală. În lipsa unor politici sociale, de ocupare a forței de muncă, de educație și de formare corespunzătoare, inegalitățile ar putea provoca neliniști sociale.

### Încrederea excesivă în roboți

— Automatizarea și IA nu reprezintă soluția miraculoasă. În prezent, acestea necesită încă supraveghere umană și ajută doar la îndeplinirea unei sarcini mai complexe. De exemplu, în timp ce conducerea unei aeronave cu autopilot la altitudine de croazieră nu pune probleme programului, aterizarea și decolarea încă trebuie să fie efectuate manual, de către oameni. Cu toate acestea, dacă

7. [http://futureoflife.org/AI/open\\_letter](http://futureoflife.org/AI/open_letter)

piloții umani sunt mai puțin instruiți și au mai puțină practică, este posibil ca aceștia să nu poată să gestioneze o situație „critică”, care nu poate fi soluționată de pilotul automat. Același lucru e valabil și pentru autoturismele autonome. Într-un viitor în care transportul va fi automat, ce se va întâmpla în cazul în care programul va eșua și nicio persoană nu va mai ști să conducă? Și cel mai important, ce vor face oamenii, dacă roboții ajung să facă totul pentru noi și chiar vor fi capabili să se creeze și să se repare singuri? Acest lucru ar putea declanșa o regresie masivă a unei părți din populație, care ar opta, pur și simplu, pentru divertisment în detrimentul îmbunătățirii competențelor și cunoștințelor, iar aceasta ar determina accentuarea inegalităților și a tensiunilor sociale.

### Ajustarea și dezvoltarea lentă sau inadecvată a competențelor

■ Nimeni nu știe ce va realiza automatizarea și IA în viitor și, prin urmare, a ghici ce competențe ar trebui promovate deoarece sunt „sigure pentru viitor”, este o sarcină foarte dificilă. De exemplu, lumea educației își dă seama încet-încet că programarea și codificarea ar trebui predată în școli, dar ultimele evoluții ale IA arată că automatizarea programării în sine este posibilă, deoarece se bazează pe logică și reguli clare. Generarea automată de web design este doar un exemplu.

### Securitatea

■ Ca și în cazul oricărui dispozitiv conectat la Internet sau bazat pe programe, IA și automatizarea sunt, de asemenea, vulnerabile la hacking. Dar consecințele ar putea fi mult mai grave decât furtul sau distrugerea datelor dumneavoastră personale. O echipă de specialiști în securitate a demonstrat că este posibilă spargerea codurilor și preluarea unei mașini conectate și efectuarea de acțiuni, cum ar fi oprirea motorului sau chiar preluarea volanului la viteze reduse. Imaginați-vă consecințele în cazul pirătăriei unei mașini autonome fără volan.

### Sfârșitul muncii plictisitoare, începutul unei lumi plictisitoare

■ Probabil, cele mai mari provocări generate de IA și de automatizare sunt de natură filosofică. Ce anume face interesantă lumea noastră? Oare oamenii vor fi fericiți într-o lume care este pe deplin înțeleasă, previzibilă și optimizată, în care totul funcționează „în conformitate cu planul”? Dar cum rămâne cu spontaneitatea umană, alegerea deliberată de a face o greșală și de a învăța din ea sau chiar dreptul de a lua o decizie nerezonabilă pur și simplu pentru că putem? Introducerea deciziilor „automate” este urmarea logică a societăților noastre conduse de știință, fapte și rațiune, dar este oare acest lucru sănătos pentru oameni? Deși în urmă cu un secol, mulți oameni de știință și intelectuali au prezis sfârșitul religiei datorită iluminării prin știință, vedem acum o revenire a interesului pentru spiritualitate și religie. Poate că este un simptom al unei lumi care nu poate oferi oamenilor un sens vieții lor și luptă împotriva lucrurilor care ne fac umani: emoții, sentimente, impulsivitate și iraționalitate?

### IDEI PENTRU LUCRUL ÎN CLASĂ



- O bună activitate introductivă în clasă pentru prezentarea inteligenței artificiale este așa-numita activitate „hârtia inteligentă”. Aceasta constă în prezentarea unei pagini cu instrucțiuni tipărite care poate învinge orice copil sau tânăr la jocul X și zero (tic-tac-toe). Consultați instrucțiunile detaliate aici: <http://web.archive.org/web/20160326100226/http://csunplugged.org/artificial-intelligence/>.
- Ca o continuare a acestei activități de bază, întrebați copiii sau elevii dumneavoastră dacă sunt conștienți de inteligența artificială pe care o folosesc în viața de zi cu zi.
- Elevii dumneavoastră au probabil un telefon inteligent, iar majoritatea telefoanelor inteligente au propriii „asistenți personali” și anume Siri pentru iOS/Apple, Google Now pentru Android/Google și Cortana pentru Windows/Microsoft. Acestea trei prezintă caracteristici ale inteligenței artificiale: au o caracteristică de recunoaștere a vocii, care se îmbunătățește pe măsură ce ascultă milioane de voci umane, au un algoritm pentru a răspunde întrebărilor pe care le adresați și personalizează informațiile pe care vi le afișează, pe baza datelor pe care le introduceți dumneavoastră (date de căutare, detalii de contact, date despre un anumit loc etc.).



Același lucru este valabil și pentru caracteristicile de bază cum ar fi tastarea predictivă. Și aceasta este o tehnologie IA.



## BUNE PRACTICI

- Inteligența artificială, automatizarea și învățarea automatizată pot fi foarte utile, dar niciodată nu trebuie să uităm să păstrăm anumite competențe manuale în cazul în care primele nu mai funcționează. De exemplu, chiar dacă aplicațiile GPS sunt acum un lucru obișnuit pe telefoanele inteligente, nu veți pierde timpul dacă veți învăța să citiți o hartă și să vă dezvoltați simțul de orientare.
- Păstrați totul sub control. Există multe niveluri de automatizare, cea mai extremă fiind un robot care ia decizii fără a primi comenzi sau fără a fi validat de oameni. La fel ca în tastarea predictivă unde utilizatorul are întotdeauna posibilitatea de a accepta sau respinge propunerea făcută de program, tot așa trebuie să configurați și dumneavoastră orice dispozitiv sau program automat sau dotat cu IA pentru ca să vă solicite validarea.
- Fiți pregătiți pentru schimbare și fiți versatili în dezvoltarea mai multor competențe. Pe măsură ce aceste tehnologii perturbatoare intră pe piață, cei care vor reuși să se adapteze vor fi cei mai ageri și mai flexibili lucrători. În viitor, este foarte probabil că lucrătorii vor fi nevoiți să se „recalifice” sau să se reîntoarcă frecvent la studii pentru a dezvolta noi seturi de competențe. Învățarea pe tot parcursul vieții va reprezenta o normă.
- Îmbunătățiți-vă competențele interpersonale, sociale și emoționale, deoarece acestea nu vor fi afectate de nicio formă de automatizare. În timp ce roboții și algoritmi vor putea să înlocuiască multe locuri de muncă slab calificate, aceștia nu vor putea să înlocuiască niciodată calitatea și interacțiunea umană.
- IA și automatizarea se bazează pe programe. Asigurați-vă că orice dispozitiv „inteligent” pe care îl dețineți rulează cea mai recentă versiune de program, verificând periodic actualizările și ajustați parametrii de securitate la cel mai ridicat nivel. Dacă dispozitivul dumneavoastră nu necesită conectare permanentă la Internet pentru a funcționa, asigurați-vă că acesta este deconectat pentru a reduce probabilitatea de piratare.
- Pentru a corela faptele și a avea o privire globală asupra a ceea ce poate aduce viitorul, asigurați-vă că citiți Fișele ce descriu volumele mari de date, realitatea augmentată și virtuală și Internetul obiectelor. Trebuie să înțelegeți că inteligența artificială și automatizarea sunt alimentate de volumele mari de date, că realitatea augmentată și virtuală sunt modalități noi de interacțiune cu IA și dispozitivele, că Internetul obiectelor nu va fi doar un alt mod de a interacționa cu IA și dispozitivele, ci și un mijloc de alimentare a acestora cu date valoroase care vor contribui la dezvoltarea lor. Doar cunoscând întreaga situație, cetățenii vor putea lua decizii conștiente și informate despre valorificarea acestor schimbări pentru o societate mai bună.



## INFORMAȚII SUPLIMENTARE

- Acesta este un articol al BBC despre inteligența artificială: <http://web.archive.org/web/20160509115227/http://www.bbc.com/news/technology-34224406>.
- Google oferă o pagină de cercetare despre inteligența artificială și învățarea automatizată: <http://research.google.com/pubs/ArtificialIntelligenceandMachineLearning.html>.
- Știri cu privire la automatizare sunt disponibile aici: <http://www.automationworld.com/>.
- Aceasta este site-ul web oficial al Consumer Electronics Show, care prezintă adesea cele mai recente inovații din domeniul tehnologiei: <https://www.cesweb.org/>.
- Știri despre ultimele cercetări și inovații în domeniul TIC sunt disponibile în Revista de Cercetare și Inovație a Comisiei UE: <http://horizon-magazine.eu/topics/ict>.



## Realitatea virtuală și realitatea augmentată



**R**ealitatea virtuală<sup>1</sup> este o experiență multimedia imersivă, care reproduce un mediu ce simulează prezența fizică în lumea reală. Experiența senzorială creată poate implica văzul, auzul, atingerea, mirosul și gustul, primele două fiind cele mai des utilizate.

■ Realitatea augmentată<sup>2</sup> reprezintă adăugarea de informații senzoriale generate de calculator, cum ar fi sunetul sau imaginile, în medii din lumea reală.

■ În timp ce ideea de realitate virtuală și augmentată există de câteva decenii, abia recent tehnologia a evoluat suficient de mult pentru a viza comercializarea dispozitivelor, serviciilor și

1. [https://en.wikipedia.org/wiki/Virtual\\_reality](https://en.wikipedia.org/wiki/Virtual_reality)

2. [https://en.wikipedia.org/wiki/Augmented\\_reality](https://en.wikipedia.org/wiki/Augmented_reality)

programele de realitate virtuală și augmentată. Aplicațiile privind realitatea augmentată au crescut rapid prin intermediul telefoanelor inteligente, al Internetului mobil și al tehnologiei de geolocalizare.

■ Câteva exemple de progrese recente în domeniul realității virtuale și augmentate includ:

- disponibilitatea sporită a căștilor de realitate virtuală, cum ar fi Oculus Rift, Samsung Gear VR, HTC Vive sau Sony Playstation VR, cu o serie de jocuri lansate, în special prin intermediul platformelor mobile Android și iOS, PlayStation 4, Xbox One și a jocurilor tradiționale pe calculator sau Mac;
- disponibilitatea crescută a căștilor sau a ochelarilor de realitate augmentată, cum ar fi Google Glass și Microsoft HoloLens; Microsoft intenționează să lanseze o versiune de realitate augmentată a Minecraft, care poate fi redată în camera dumneavoastră de zi;
- lansarea jocurilor de masă de realitate augmentată, precum Pokemon Go, care vă permite să prindeți Pokemoni în lumea reală cu ajutorul telefonului dumneavoastră inteligent (iOS și Android).



## BENEFICIILE EDUCAȚIONALE

- Realitatea virtuală, prin posibilitatea de a simula o experiență din lumea reală, prezintă un număr mare de oportunități de învățare. De exemplu, învățarea modului de a conduce o mașină poate fi simulată cu exactitate.
- Având în vedere nivelul de imersiune al realității virtuale, experiențele sunt deja promițătoare în ceea ce privește utilizarea realității virtuale în scopuri terapeutice, cum ar fi eliminarea arahnofobiei sau depășirea tulburărilor de stres posttraumatic (TSPT). De asemenea, aceasta a fost utilizată cu succes pentru a crește nivelul de empatie și înțelegere a celorlalți, permițând unui utilizator să experimenteze ceea ce se simte o persoană cu dizabilități (o persoană nevăzătoare, o persoană în scaun cu rotile) sau cum e să fii parte dintr-o minoritate care suferă de discriminare.
- Deși nimic nu poate înlocui realitatea, nu toată lumea are ocazia să călătorească. Realitatea virtuală poate simula vizitarea unui monument sau a oricărui alt loc, creând senzația că ai fi tu însuși fizic acolo. Aceasta poate merge și mai departe, permițându-vă să vizitați locuri pe care nu le-ați putea vizita în mod normal, cum ar fi luna sau spațiul cosmic sau interiorul unui vulcan, sau poate chiar să vă ducă înapoi în timp pentru a simula aflarea pe un câmp de luptă din secolul al XVIII-lea ori prezența dumneavoastră alături de dinozauri.
- Realitatea augmentată are prea multe aplicații benefice pentru a putea fi enumerate. Deoarece aceasta constă în suprapunerea informațiilor „extra” sau a obiectelor la lumea reală, posibilitățile sunt nesfârșite. În cazul realității augmentate, nu este nevoie de un ghid turistic deoarece, în timp ce vă uitați la un monument, o statuie sau orice altceva, peste acestea se pot suprapune informații utile. Suprapunerea informațiilor nu are limite. Aceasta poate fi un meniu sau recenzie pentru un restaurant, memento-uri despre numele persoanelor sau informații despre aceștia atunci când îi vedeți și așa mai departe. În ceea ce privește învățarea, aceasta oferă, de asemenea, posibilități nelimitate: arătându-vă cum să reparați/înlocuiți o piesă la mașină prin suprapunerea pașilor pe care trebuie să îi faceți, ajutând un chirurg în timpul unei operații, arătându-vă cum să pregătiți o rețetă prin simularea modului în care ar trebui să tăiați ingredientele și cum să le amestecați. Orice priviți poate fi „augmentat” cu informații suplimentare. Astfel, o clasă poate fi transformată într-o scenă pe care pot fi adăugate obiecte virtuale, arătând, de exemplu, un model semi-transparent al unui corp uman.



## CONSIDERAȚII DE ORDIN ETIC ȘI RISCURI

### Riscul comportamental

— O serie de studii au analizat legătura dintre jocurile video și comportamentele din viața reală, cum ar fi creșterea violenței și agresivității. Totuși, concluziile sunt încă controversate. Unele studii indică o agresivitate „pe termen scurt” și un comportament violent după un joc video violent, alte studii subliniază efectul de „descărcare” pe care aceste jocuri îl au asupra copiilor. Alte detalii, precum jocul cu mai mulți jucători cu un element de cooperare afectează, de asemenea, rezultatele. Adevărul este că suntem încă departe de a înțelege efectele pe termen lung ale jocurilor video asupra copiilor și tinerilor adulți. Realitatea virtuală și realitatea augmentată vor adăuga un plus de realism jocurilor video, apropiindu-le tot mai mult de „realitate” și nu se știe aproape nimic despre cum vor fi afectați copiii. Recent, s-au iscat multe controverse în jurul unor jocuri video, precum GTA V, în care un element terț suplimentar dezvoltat de o anumită persoană, a permis jucătorilor să simuleze violul pe un personaj feminin virtual. Sexismul în jocurile video este un fenomen bine-cunoscut, jucătorii de sex feminin prefăcându-se adesea că sunt „bărbați” pentru a evita hărțuirea. Și nu este vorba numai de conținutul formal al jocurilor video. Discuțiile în direct prin jocurile video au fost utilizate pentru diseminarea conținutului extremist, promovarea sexismului, bullying-ului, discursului de ură etc. Jocurile video care utilizează realitatea virtuală și augmentată vor face parte din mijloacele pe care copiii le vor consuma în viitor și vor contribui, în mod inevitabil, la modelarea, într-o oarecare măsură, a atitudinilor și comportamentelor acestora. În cazul în care dezvoltatorii irresponsabili prezintă un conținut extrem de violent, extremist, sexist, rasist, homofob în jocurile lor, aceasta ar putea afecta negativ utilizatorii.

### Viața privată

— Realitatea augmentată se bazează pe analiza permanentă în timp real a lumii fizice pentru a o „augmenta” cu precizie cu elementele virtuale. Aceasta înseamnă că localizarea dumneavoastră și ceea ce priviți trebuie trimis supercalculatoarelor, de obicei online, pentru a calcula cu exactitate ce ar trebui afișat. Fără o protecție adecvată a vieții private, realitatea augmentată ar putea deveni o modalitate de a spiona oamenii mult mai îndeaproape, în timp real.

### Securitatea

— Cu dispozitive conectate permanent la Internet, piratarea în direct de la distanță a devenit mai ușoară. Pe măsură ce vom începe să folosim dispozitive de realitate augmentată și virtuală, cum ar fi ochelarii sau chiar lentilele de contact, ar putea apărea noi situații potențial periculoase de piratare. De exemplu, un șofer utilizează afișajul de realitate augmentată pentru a se orienta. Dacă afișajul este piratat, șoferul va fi distras de la drum.

### Manipularea și consumerismul

— Realitatea augmentată și realitatea virtuală vor aduce, de asemenea, noi strategii de publicitate. Deoarece nu există nicio reglementare cu privire la ceea ce este permis, atunci, totul este permis și putem presupune cu ușurință că vor fi utilizate tehnici cum ar fi „augmentarea” locuinței cu ajutorul reclamei. De exemplu, ați putea deschide frigiderul și un dispozitiv publicitar ar „augmenta” conținutul frigiderului dumneavoastră pentru a afișa produsele pe care „ar trebui” să le aveți înăuntru. La supermarket, în timp ce scanați un produs cu telefonul dumneavoastră inteligent, o notificare v-ar putea sugera cumpărarea unui alt produs.

### Dependență și adicție

— Progresul din domeniul neuroștiințelor a dus la descoperirea numeroaselor lucruri despre creierul nostru. Creierul obține multă plăcere de la activarea unor stimuli rapizi, cum ar fi acțiunea rapidă, mișcarea și altele similare. Acesta este motivul pentru care jocurile video și filmele de acțiune cu ritm rapid au succes. Din nefericire, lumea „reală” necesită dobândirea și practicarea unor abilități precum abținerea, auto-controlul, răbdarea, perseverența și proactivitatea. Nu putem transforma totul în joc sau plăcere prin tehnologie. Un astfel de exemplu este învățarea cântatului la vioară. Pe mă-

sură ce copiii vor crește cu realitatea virtuală și augmentată, există riscul ca aceștia să nu poată face față unei lumi care nu este „augmentată” sau care nu este la fel de „bogată” și stimulative ca realitatea lor „virtuală”. Jocul de rol online masiv multi-jucător (massively multiplayer online role playing games – MMORPG) este un bun exemplu în acest sens. În timp ce astfel de jocuri contribuie la dezvoltarea unui mare număr de aptitudini, cum ar fi sentimentul de organizare, planificare, leadership și cooperare, acestea vin cu o curbă de învățare foarte „plăcută”, care este suficient de dificilă pentru a menține jucătorii interesați, dar nu prea complexă, pentru a nu-i descuraja. Realitatea augmentată și virtuală va exacerba această problemă și ar putea crea o dependență și adicție față de o lume mai puțin frustrantă și mult mai stimulative decât lumea reală, în care le este mai ușor să se descurce.

### **Pierderea competențelor interpersonale și comportamentele asociale**

■ Deși este încă un fenomen limitat, în unele țări, cum ar fi Japonia, se observă o tendință crescândă de retragere a adolescenților și adulților denumiți „Hikikomori”, din viața socială. Deși acest fapt nu este direct legat de mass-media, televiziune sau Internet, aceste medii fac retragerea socială mai suportabilă, deoarece distrag atenția de la dificultățile vieții „reale”. Realitatea virtuală și augmentată poate exacerba fenomenul și mai mult, deoarece este mai ușor și mai plăcut să faci față realităților virtuale decât unor interacțiuni umane „problematic”. Chiar și sexul, și relațiile sexuale își au partea lor de emoții negative, iar presiunea de a reuși și rușinea referitoare la propriul corp, dispar într-o lume virtuală, în care utilizatorul deține controlul deplin asupra tuturor lucrurilor.

### **Sănătatea fizică**

■ Realitatea augmentată și realitatea virtuală oferă, de asemenea, oportunitatea de a rezolva probleme de inactivitate fizică în rândul utilizatorilor care stau pasiv în spatele ecranelor timp de ore întregi. Jocurile bazate pe localizare, de exemplu, pot avea loc în lumea reală cu o realitate augmentată, iar proiectele pot crea încăperi speciale pentru mediile de realitate virtuală. În același timp, experiențele imersive ridică noi probleme, cum ar fi ignorarea semnelor de durere sau utilizarea excesivă datorită puterii conținutului virtual sau augmentat de a ne capta întreaga atenție. Mișcările repetitive în interiorul unui joc pot duce la tendință, așa cum se poate vedea la unele jocuri Wii. De asemenea, răul de mișcare și greața pot fi un efect secundar puternic al experienței imersive a realității augmentate, deoarece imaginile care sunt transmise creierului printr-un afișaj montat pe cap sunt în contradicție cu informațiile oferite de senzorii de mișcare din urechea internă. În cele din urmă, mulți testerii beta au raportat faptul că s-au rănit prin cădere sau lovire cu un obiect, în timp ce erau implicați în realitatea virtuală sau chiar în realitatea augmentată, deoarece priveau ecranele telefoanelor inteligente în timp ce jucau jocuri de realitate augmentată în lumea reală.

### **Hărțuirea, cyberbullying-ul și riscurile aferente contactului**

■ Deoarece limita între ceea ce este real și ceea ce este virtual se schimbă, realitatea virtuală și, în special, cea augmentată, ar putea fi utilizate ca un mijloc instantaneu și direct de a umili o persoană, de exemplu prin programarea suprapunerii unui cap de șobolan peste o persoană prin recunoașterea facială sau prin distribuirea video în direct cu o persoană aflată într-o situație umilitoare.

■ Realitatea augmentată și, într-o mai mică măsură, realitatea virtuală, prezintă riscuri legate de „contacte”. Jocurile de realitate masiv augmentate se bazează pe jocul în lumea reală împotriva unor persoane străine adevărate. Situații problematice precum jaful sau actele de violență se pot întâmpla în viața reală.



### **IDEI PENTRU LUCRUL ÎN CLASĂ**

- Realitatea augmentată și virtuală se bazează foarte mult pe echipamente. De exemplu, dacă școala sau instituția dumneavoastră de învățământ nu dispune de tablete, atunci nu veți putea profita din plin de aceste tehnologii. În anumite cazuri, pot fi utilizate chiar dispozitivele

copiilor și tinerilor (cum ar fi telefoanele lor inteligente), dar acest lucru poate fi contrar politicii școlii, deoarece unele școli interzic utilizarea telefoanelor inteligente pe durata orelor. Utilizarea telefoanelor poate duce la apariția cazurilor de discriminare, deoarece este posibil ca unii elevi să nu dețină un telefon mobil suficient de puternic pentru a participa la activități de realitate augmentată sau virtuală sau ar putea să nu dețină un telefon mobil.

- Acestea fiind spuse, există multe resurse disponibile în mediul online pentru a vă ajuta să utilizați realitatea augmentată și virtuală în sala de clasă. Realitatea augmentată este mai ușor de utilizat, deoarece nu necesită o cască care oferă o experiență complet imersivă și poate funcționa cu dispozitivele existente, cum ar fi telefoanele inteligente și tabletele.
- Dacă sunteți interesat de utilizarea realității augmentate, puteți găsi o listă de tutoriale, ghiduri și aplicații pe site-ul web<sup>3</sup> al lui Kathy Schrock „A guide to everything”<sup>4</sup> (Un ghid pentru tot).

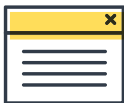


## BUNE PRACTICI

- Ca întotdeauna, din moment ce se cunosc prea puține despre efectele utilizării prelungite sau a expunerii la aceste noi tehnologii, menținerea unui echilibru sănătos de viață este o necesitate. Asigurați-vă că dumneavoastră și/sau copilul dumneavoastră vă echilibrați activitățile „conectate”, virtuale sau augmentate cu sporturile „tradiționale” sau alte hobby-uri. Acest lucru este valabil și pentru școală. Realitatea augmentată și realitatea virtuală sunt afaceri prospere și, în timp ce se pretinde că utilizarea acestora în educație este benefică, nu există o soluție miraculoasă pentru a avea o educație de calitate. Calea de urmat este echilibrul sănătos între metodele de predare tradiționale și noi.
- Alegeți cu atenție conținutul pe care îl cumpărați pentru copiii dumneavoastră, în cazul în care utilizează dispozitive virtuale sau augmentate și verificați în permanență la ce au acces. Citiți restricțiile și etichetele referitoare la vârstă, de exemplu etichetele PEGI (a se vedea Fișa 20 cu privire la etichetare și filtrare și Fișa 16 cu privire la jocuri) și activați instrumentele de control parental pe dispozitivele utilizate de copiii mai mici pentru a vă asigura că nu pot accesa liber conținutul. Pentru copiii mai mici, utilizați liste albe de calitate, dacă sunt disponibile în țara/limba dumneavoastră, deoarece este cel mai bun mod de a-i proteja și de a vă asigura că aceștia sunt expuși unui conținut pozitiv, care a fost revizuit de profesioniști.
- Este mai important ca niciodată să vorbiți deschis cu copiii și tinerii despre violență, cyberbullying, sexualitate, drepturi și responsabilități. Stabilirea unor standarde etice solide de la vârstă fragedă reprezintă cea mai eficientă modalitate de a neutraliza mesajul sexist, rasist sau orice alt mesaj discriminatoriu sau negativ pe care copiii dumneavoastră l-ar putea întâlni la un moment dat în mediul online sau pe dispozitivele lor de realitate virtuală și augmentată.
- Pentru copiii mai mici, configurați setările de confidențialitate și de securitate la cel mai înalt nivel. Consultați Fișa 9. Rețineți faptul că aceste dispozitive sunt expuse riscului de a fi piratate.
- Asigurați-vă că verificați modelul de afaceri din spatele conținutului sau a dispozitivului pe care îl utilizați pentru realitatea virtuală și/sau augmentată, deoarece dumneavoastră sau copilul dumneavoastră ați putea fi expus publicității nedorite.

3. <http://www.onlineuniversities.com/blog/2012/09/20-coolest-augmented-reality-experiments-education-so-far/>

4. <http://web.archive.org/web/20160318145342/http://www.schrockguide.net/augmented-reality.html>; OnlineUniversities.com



## INFORMAȚII SUPLIMENTARE

- Știri despre ultimele progrese în domeniul realității virtuale sunt disponibile pe Venture Beat: <http://venturebeat.com/tag/virtual-reality/>.
- Există un articol despre realitatea virtuală și educație de la Universitatea Stanford: <https://teachingcommons.stanford.edu/teaching-talk/virtual-reality-and-education>.
- Știri despre ultimele progrese în domeniul realității augmentate sunt disponibile și pe Venture Beat: <http://venturebeat.com/tag/augmented-reality/>.
- Informații generale despre realitatea augmentată pot fi găsite în Ghidul de cercetare al Bibliotecii Colegiului Dartmouth: <http://researchguides.dartmouth.edu/AR>.



## Sunteți produsul? Examinarea volumelor mari de date (big data), extragerea de date și viața privată



**B**ig data<sup>1</sup> (volumele mari de date) este un termen larg, ce se referă la datele care sunt atât de vaste încât nu pot fi analizate sau prelucrate prin metode tradiționale (de exemplu, utilizând un calculator sau o simplă aplicație).

— Volumele mari de date își au rădăcinile în combinațiile:

- unei creșteri spectaculoase a capacității digitale de stocare;
- unei creșteri a datelor generate de societățile noastre (din ce în ce mai mult, tot ceea ce facem lasă o urmă digitală);
- unei lumi interconectate prin Internet care permite conectarea tuturor acestor date; și
- unei capacități crescânde de a analiza și de a înțelege toate datele generate.

1. [https://en.wikipedia.org/wiki/Big\\_data](https://en.wikipedia.org/wiki/Big_data)

■ Exemplele de servicii online care folosesc volumele mari de date includ rețele sociale precum Facebook, motoare de căutare precum Google sau Bing și comercianți cu amănuntul online, cum ar fi Amazon. Dar volumele mari de date reprezintă mai mult decât un aspect „online”; acestea sunt prezente și în viața noastră zilnică, offline.

- Supermarketurile utilizează carduri de magazin pentru a analiza tiparele de cumpărături și pentru a-și ajusta inventarul în timp real sau pentru a programa un eveniment special organizat de magazin (marketing, vânzare etc.).
- Datele generate de șoferi, senzorii de la autovehicule și dispozitivele GPS ajută la furnizarea în timp real a informațiilor despre trafic.
- În spitale, analiza în timp real a datelor de la senzori, cum ar fi frecvența cardiacă, poate ajuta la identificarea infecțiilor sau a altor probleme de sănătate înainte ca orice semne și simptome externe să poată fi depistate.

■ Datele au devenit, de asemenea, unele dintre cele mai populare monede online. În locul plății cu bani propriu-ziși pentru serviciile online pe care le utilizați, cum ar fi rețelele sociale sau motoarele de căutare, plătiți cu datele pe care le transmiteți acestor servicii. Aceste date permit serviciilor să personalizeze publicitatea și marketingul preferințelor dumneavoastră, făcându-le mai eficiente. Cu toate acestea, „plata” cu datele este o comparație slabă. Spre deosebire de bani, datele sunt mult mai sensibile. Acestea pot fi refolosite de mai multe ori și pot fi revândute. O comparație mai corectă ar fi: „schimb cheia de la casa mea pe accesul la un serviciu!”

■ Suntem doar la începutul acestei revoluții, deoarece datele devin și mai extinse, de exemplu, prin intermediul Internetului obiectelor (a se vedea Fișa 23 cu privire la Internetul obiectelor) și deoarece analiza datelor devine mai eficientă prin creșterea puterii de calcul și a progresului la nivel de tehnici de analiză a datelor (inteligența artificială etc.).



## BENEFICIILE EDUCAȚIONALE

- Volumele mari de date au un potențial foarte mare de a optimiza și de a ușura multe activități ale vieții dumneavoastră: de exemplu, asigură căutări mai exacte, eficientizează naveta dumneavoastră către/de la serviciu sau școală din punct de vedere al timpului și vă ajută în permanență să găsiți produsele alimentare pe care le doriți în magazinul dumneavoastră local și așa mai departe.
- Învățarea despre volumele mari de date și modul în care funcționează acestea este esențial pentru a le valorifica potențialul și pentru a vă asigura că acestea acționează în favoarea și nu împotriva dumneavoastră. Aceasta implică alegerea cu grijă a tipurilor de date pe care sunteți dispus să le partajați și selectarea serviciilor și produselor bazate pe felul în care acestea utilizează datele.
- Volumele mari de date pot, de asemenea, servi scopului de a ajuta la înțelegerea societăților noastre, făcând posibilă, pentru prima dată în istoria omenirii, analiza și înțelegerea cantităților mari de date generate de oameni. Pentru științele sociale, psihologie, științele comportamentale, sănătate, marketing și multe alte domenii de cercetare, volumele mari de date reprezintă un adevărat salt înainte. Constatările din aceste domenii pot fi valorificate de către cadrele didactice pentru a ilustra anumite concepte sociologice cu exemple și cifre din viața reală.
- Prevalența modelelor de afaceri online bazate mai degrabă pe date și nu pe moneda tradițională, ca sursă principală de venituri, creează, de asemenea, necesitatea unor noi competențe, cum ar fi competențele de gestionare a datelor cu caracter personal și de protecție a vieții private. Prin urmare, în mod asemănător cu gestionarea responsabilă a bugetului personal și a finanțelor dumneavoastră fără a depăși cheltuielile, va trebui, de asemenea, să învățați să vă gestionați cu responsabilitate datele personale și să nu partajați prea mult.



## CONSIDERAȚII DE ORDIN ETIC ȘI RISCURI

### Viața privată și protecția datelor

■ Deși multe legi protejează datele și viața privată a persoanelor, în realitate, acestea sunt dificil de implementat. Regulamentul General privind Protecția Datelor (GDPR) impune serviciilor să solicite consimțământul explicit al utilizatorului, dar acest lucru nu va face altceva decât să extindă, cel mai probabil, exercițiul de „bifare a căsuței”, în mod asemănător cu cel al „Termenilor și condițiilor”: acceptați sau refuzați. Adesea, utilizatorii nu au un control granular și detaliat asupra datelor proprii și se confruntă cu opțiuni de a partaja totul sau nimic. Chiar dacă GDPR încearcă să abordeze problema consimțământului consumatorilor prin introducerea principiului proporționalității (doar dacă serviciul care solicită accesul la datele consumatorilor are într-adevăr nevoie de astfel de date pentru furnizarea serviciului), interpretarea și aplicarea în practică pot să nu fie suficiente pentru a proteja utilizatorii. De exemplu, oare rețelele sociale au nevoie de a utiliza datele dumneavoastră pentru a efectua o sortare a știrilor dumneavoastră?

■ În următorii ani, vor trebui dezvoltate în continuare însăși conceptele de viață privată și protecție a datelor. Ce înseamnă viața privată? Pot fi datele dumneavoastră exploatate atâta timp cât acestea nu vă dezvăluie? Cum puteți controla mai bine felul în care datele dumneavoastră sunt partajate și utilizate, având în vedere cantitatea mare de date generate zilnic de utilizatori?

### Standardizarea, conformismul și stagnarea

■ Volumele mari de date constituie o binecuvântare pentru optimizare. Transportul public, asistența medicală și spitalele, planificarea urbană, toate aceste sectoare pot beneficia de pe urma analizării datelor generate de utilizatori, pacienți și cetățeni, pentru a fi mai eficiente. Dar dacă dumneavoastră aveți o situație diferită? Dacă mergeți la lucru la ore neobișnuite, dacă aveți o boală unică, dacă nu doriți să vă conformați tiparului „obișnuit” de viață? Dacă toate serviciile din jurul dumneavoastră sunt proiectate mai eficient pe baza volumelor mari de date, dumneavoastră ca persoană, împreună cu aspirațiile și nevoile dumneavoastră unice, ați putea fi ignorat.

■ Dar volumele mari de date pot fi utilizate și pentru a ajusta un serviciu la nevoile dumneavoastră: de exemplu, motoarele de căutare personalizează rezultatele căutării reieșind din căutările anterioare și oricare alte date despre dumneavoastră, iar rețelele sociale vă arată postări care ar putea să vă placă. Cu toate acestea, faptul că vi se arată doar ceea ce doriți să vedeți sau ceea ce vă place să vedeți poate declanșa un efect secundar al stagnării personale. De exemplu, în cazul în care preferințele și convingerile dumneavoastră politice sunt mai de dreapta sau mai de stânga, a primi doar informații și conținut care vă susține opiniile poate fi măgulitor pentru ego-ul dumneavoastră, dar ar putea fi teribil pentru promovarea unor valori fundamentale precum democrația, dezbaterea și dezvoltarea personală – de fapt, nu va face altceva decât să vă blocheze.

### Discriminarea

■ Ori de câte ori obțineți o asigurare de viață, aplicați la un loc de muncă, solicitați un împrumut sau faceți asigurarea mașinii, competențele dumneavoastră sau riscul pe care îl prezentați sunt evaluate. Acest lucru poate fi realizat printr-un chestionar despre sănătate care vă întreabă dacă fumați sau faceți sport, un interviu pentru a vă testa competențele sau un test pentru a verifica cum ați gestionat recent bugetul și dacă ați rambursat orice împrumut pe care l-ați luat. Dar unde este granița dintre evaluarea „corectă” și simpla încălcare a vieții dumneavoastră private? Mulți angajatori utilizează deja informațiile online cu privire la candidații pentru locurile de muncă, pentru a lua decizii de angajare și există numeroase indicii ale companiilor de asigurări și ale băncilor care arată că acestea au tendința de a analiza datele online pentru a evalua probabilitatea de neplată a unui împrumut sau a unei probleme grave de sănătate. Deși volumele mari de date pot salva vieți prin capacitatea lor predictivă, acestea pot, de asemenea, împiedica unele persoane să aibă acces la servicii financiare sau asistență medicală de bază.

## Comerț cu anti-discriminarea

■ Pe Internet au început să apară companii de gestionare a reputației online. Întreprinderile și persoanele fizice pot plăti acestor companii pentru a le gestiona reputația și pentru a se asigura că datele lor nu le exclud accesul la anumite servicii, cum ar fi creditarea/investițiile, asigurările sau locurile de muncă. Acesta este un exemplu de exploatare comercială a unui ciclu de factori externi, asemănător situației când poluăm un râu, vindem medicamente cetățenilor care au consumat apa și s-au otrăvit și apoi plătim o companie ca să curețe râul.

## Manipularea și consumerismul

■ Având în vedere faptul că cel mai popular model de afaceri pentru aplicații și servicii online este publicitatea „gratuită”, bazată adesea pe exploatarea datelor de utilizator, există riscul ca consumatorii să fie expuși la tot mai multe mesaje care îi încurajează să consume. Publicitatea în mediul online crește în fiecare an și noile tehnici care îi obligă pe consumatori să privească sau să dea clic pe publicitate evoluează rapid. De exemplu, videoclipurile de pre-vizualizare au apărut în urmă cu doar câțiva ani. Volumele mari de date stimulează creșterea publicității, făcând-o mai eficientă și adaptând-o la obiceiurile și interesele persoanelor, definind, în același timp, în baza masei de date cel mai eficient concept, loc și metodă pentru ca un anunț publicitar să fie văzut și persoana să interacționeze cu acesta.

## Persecutarea politică

■ În timp ce unele guverne respectă viața privată și nu își spionează cetățenii, există numeroase guverne care nu fac acest lucru. Dezvăluirile lui Edward Snowden au arătat că guvernele din întreaga lume spionează utilizatorii de Internet. În unele cazuri, acest lucru este justificat din motive de securitate, cum ar fi combaterea terorismului și prevenirea unui atac terorist, însă proporționalitatea acestor acțiuni trebuie întotdeauna pusă la îndoială. De exemplu, poliția poate investiga profilurile de pe rețelele sociale pentru a identifica cetățenii prezenți la un marș de protest.

## Drepturile consumatorilor

■ Volumele mari de date constituie noua monedă online, dar ce primesc utilizatorii în schimb? Dreptul de a utiliza un serviciu online, însoțit de hărțuire și o publicitate supărătoare? Atunci când utilizatorii plătesc o taxă lunară pentru utilizarea unui serviciu, aceștia sunt protejați în conformitate cu legile cu privire la drepturile consumatorilor și sunt în drept să solicite despăgubiri dacă serviciul sau conținutul nu corespunde așteptărilor lor sau prezintă neajunsuri grave. Un utilizator ar putea primi o rambursare din partea unei platforme video online în cazul în care acesta nu poate viziona un film, dar ce se întâmplă în cazul în care rețeaua dumneavoastră socială preferată are viruși sau este inutilizabilă? La ce despăgubiri aveți dreptul? La urma urmei, rețeaua socială a folosit datele dumneavoastră pentru a vă demonstra reclame și a obținut bani din aceasta. Noul model de afaceri bazat pe date privesc multe probleme pentru drepturile consumatorilor; deoarece se presupune că este „gratuit”, adesea utilizatorii nu beneficiază de nicio compensație, iar drepturile acestora sunt foarte limitate.

## Sfârșitul anonimatului

■ În timp ce pseudonimele și porecele încă nu au dispărut, anonimatul este serios amenințat ca urmare a apariției volumelor mari de date. Prin realizarea de legături între diferite date anonime, este posibilă identificarea unei persoane pe baza numelui în mediul online. Chiar și fiind foarte prudenți în ceea ce privește informațiile pe care le postăm, în viitorul apropiat va fi greu pentru oricine să rămână anonim online, indiferent de circumstanțe.

## Internetul nu uită niciodată

■ „Dreptul de a fi uitat” a reușit să se impună, deoarece Uniunea Europeană a luat măsuri juridice pentru ca acest lucru să devină o realitate. Cu toate acestea, în practică, acest lucru este încă dificil. Conținutul digital poate fi cu ușurință „repostat”, ușor modificat pentru a nu fi recunoscut de boții sau moderatorii automatizați de pe Internet sau găzduit pe servere sau servicii online, care sunt în afara

jurisdicției UE. În prezent, oricine, în orice moment, poate realiza cu ușurință imagini sau videoclipuri cu propriul telefon inteligent ceea ce înseamnă că nimeni nu mai poate apărea într-o postură ridicolă și acționa în mod iresponsabil în timpul unui festival, de exemplu, deoarece apare riscul de a vedea imaginea/materialul video încărcat online și de a fi ridiculizat de întreaga lume. Încă nu a fost găsit acel echilibru bun între dreptul de a trage făptașul la răspundere și dreptul de a fi uitat.

### Conținut și servicii de calitate slabă

Având în vedere faptul că serviciile online și creatorii de conținut se bazează din ce în ce mai mult pe publicitate pentru a obține venituri, aceștia vor căuta să optimizeze atractivitatea serviciului sau a conținutului lor. Volumele mari de date ajută la identificarea detaliilor care fac ca un articol, o fotografie sau un videoclip să fie atractive, dar oare acest aspect va avea impact sau nu asupra calității conținutului sau a serviciilor? Tot mai multe articole online se bazează pe „clicurile momeală” pentru a atrage utilizatorii să apese pe un link sau post și să fie atrași pe pagina plină de anunțurile acestora. Titluri precum „cele mai importante trei secrete pentru a pierde în greutate”, „nu veți crede ce face această fată în fața camerei de luat vederi” sau „cele mai drăguțe 10 pisici de pe Internet” se găsesc din ce în ce mai frecvent în mediul online. Deși nu este nimic rău în conținutul de divertisment și anecdotic, modelul de afaceri bazat pe publicitate creează un stimulent puternic pentru a dezvolta numai acel tip de conținut, în detrimentul unui conținut corect din punct de vedere al faptelor sau a unui conținut educațional.



### IDEI PENTRU LUCRUL ÎN CLASĂ

- Pentru tinerii cu vârsta de peste 14 ani: rugați tinerii să își caute numele și/sau să examineze datele online disponibile despre ei, apoi să le analizeze din perspectiva unui angajator, a unui asigurător și a unui reprezentant al organelor de drept. Rugați-i să discute despre modul în care ar fi percepuți de organizațiile date în cazul în care acestea ar analiza datele disponibile despre ei. De exemplu, partajarea articolelor despre beneficiile procrastinării sau statusuri actualizate, care conțin multe greșeli ortografice, pot lăsa o impresie negativă asupra unui angajator. Fotografii în care fumați, beți sau faceți activități periculoase nu vor arăta deloc bine din perspectiva unui asigurător. Și, în sfârșit, postările care critică guvernul și fac apel la schimbări radicale, pot părea suspecte pentru instituțiile de aplicare a legii.



### BUNE PRACTICI

- În cele din urmă, Internetul și volumele mari de date nu sunt decât niște etape noi ale revoluției tehnice și rezultatele finale vor fi bune sau rele pentru omenire și societate, în dependență de modul în care le vom utiliza. În calitate de cetățean și de utilizator de Internet, puteți configura modul în care volumele mari de date vor fi utilizate, puteți încuraja inițiativele care funcționează în beneficiul societății și le puteți suprima pe acelea care contravin interesului public. De exemplu, în calitate de cetățean, puteți vota pentru factorii de decizie care promovează standarde etice solide privind utilizarea datelor; în calitate de utilizator de Internet puteți să sprijiniți serviciile și companiile care vă gestionează datele etic și responsabil.
- Rămâneți informat cu privire la ultimele evoluții în materie de volume mari de date, deoarece acestea vor avea repercusiuni profunde asupra vieții dumneavoastră de zi cu zi. Acestea vă vor ajuta să decideți în privința datelor pe care doriți și alegeți să le partajați și vă vor ajuta să identificați și să susțineți decidenții politici și companiile care respectă standardele dumneavoastră etice referitoare la modul în care datele dumneavoastră confidențiale ar trebui utilizate.

- Monitorizați toate serviciile pe care le-ați utilizat și tot conținutul pe care l-ați postat în mediul online chiar de la începutul prezenței datelor dumneavoastră confidențiale online, mai ales dacă ați început acest lucru din tinerețe! Comentariile sau postările pe care le-ați făcut ca copil sau adolescent pot cu ușurință să reapară și să vă bântuie viața dumneavoastră de adult. Acordați-vă timp pentru a reevalua ceea ce ați postat și arhivați sau ștergeți conținutul care nu vă mai reprezintă în prezent.
- Alocați-vă timp să examinați modul în care serviciile online vă utilizează datele cu caracter personal și alegeți-le reieșind din aceasta. Verificați întotdeauna toate setările de confidențialitate disponibile pentru a configura protecția potrivită pentru datele dumneavoastră.



## INFORMAȚII SUPLIMENTARE

- Exemple de volume mari de date care sunt utilizate în beneficiul societății pot fi găsite pe pagina web a Comisiei UE: <https://ec.europa.eu/digital-agenda/en/what-big-data-can-do-you>.
- De asemenea, sunt disponibile informații despre Regulamentul UE privind dreptul de a fi uitat: [http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet\\_data\\_protection\\_en.pdf](http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf).
- Datele și Societatea reprezintă un grup de reflecție american care se axează pe aspectele sociale, etice și culturale ce decurg din dezvoltarea tehnologică bazată pe date: <http://www.datasociety.net/>.
- Raportul cu privire la „Drepturile civile, volumele mari de date și viitorul nostru algoritmic” este disponibil la: <https://bigdata.fairness.io/>.
- Fundația Frontiera Electronică oferă informații despre protecția drepturilor dumneavoastră în lumea digitală: <http://www.eff.org>.
- Drepturile Digitale Europene oferă, de asemenea, informații privind apărarea drepturilor și libertăților în mediul digital: <http://www.edri.org>.



**D**e la publicarea primei ediții a Manualului de educație (alfabetizare) în domeniul Internetului în 2003, lumea Internetului s-a schimbat dramatic. Numărul internaților a crescut, utilizatorii sunt din ce în ce mai tineri, tendințele de utilizare și căutare pe Internet evoluează, iar noile capcane, ca de exemplu, în domeniul securității personale, apar vertiginos.

Această nouă ediție ia în considerare nenumăratele schimbări, deși obiectivul manualului rămâne, în continuare, același și anume, de a oferi familiilor, cadrelor didactice și factorilor de decizie, cunoștințe tehnice suficiente pentru a naviga cu tinerii prin tehnologia comunicațiilor. Noua ediție extinde, de asemenea, domeniul de aplicare al Fișelor care consolidează conceptele ce erau anterior „noi”, precum cel de cetățenie digitală și parentaj digital. Această ediție include 26 de Fișe organizate în 6 capitole tematice, incluzând un capitol special dedicat viitorului Internetului. Manualul este conceput pentru a fi ușor de utilizat și practic, așa cum este ilustrat în Fișa intitulată „Găsirea informațiilor de calitate pe web”. De asemenea, acesta este disponibil online, de unde poate fi descărcat integral sau fiecare fișă poate fi descărcată separat.

RON

[www.coe.int](http://www.coe.int)

Consiliul Europei este organizația lider în domeniul drepturilor omului pe continentul european. Aceasta include 47 de state membre, inclusiv toate statele membre ale Uniunii Europene. Toate statele membre ale Consiliului Europei au semnat Convenția Europeană a Drepturilor Omului, un tratat conceput să protejeze drepturile omului, democrația și preeminența dreptului. Curtea Europeană a Drepturilor Omului supraveghează punerea în aplicare a Convenției în statele membre.

COUNCIL OF EUROPE



CONSEIL DE L'EUROPE