

SIGURANȚA TINERILOR ÎN MEDIUL ONLINE

Important!

• **Noul Cod Penal al României** – *Titlul II, Infracțiuni contra patrimoniului*, prevede la capitolul IV - Fraude comise prin sisteme informatice și mijloace de plată electronice:

ART. 249 Frauda informatică

Introducerea, modificarea sau ștergerea de date informatice, restricționarea accesului la aceste date ori împiedicarea în orice mod a funcționării unui sistem informatic, în scopul de a obține un beneficiu material pentru sine sau pentru altul, dacă s-a cauzat o pagubă unei persoane, se pedepsește cu închisoarea de la 2 la 7 ani.

ART. 250 Efectuarea de operațiuni financiare în mod fraudulos

(1) Efectuarea unei operațiuni de retragere de numerar, încărcare sau descărcare a unui instrument de monedă electronică ori de transfer de fonduri, prin utilizarea, fără consimțământul titularului, a unui instrument de plată electronică sau a datelor de identificare care permit utilizarea acestuia, se pedepsește cu închisoarea de la 2 la 7 ani.

(2) Cu aceeași pedeapsă se sancționează efectuarea uneia dintre operațiunile prevăzute în alin. (1), prin utilizarea neautorizată a oricăror date de identificare sau prin utilizarea de date de identificare fictive.

(3) Transmiterea neautorizată către altă persoană a oricăror date de identificare, în vederea efectuării uneia dintre operațiunile prevăzute în alin. (1), se pedepsește cu închisoarea de la unu la 5 ani.

ART. 251 Acceptarea operațiunilor financiare efectuate în mod fraudulos

1) Acceptarea unei operațiuni de retragere de numerar, încărcare sau descărcare a unui instrument de monedă electronică ori de transfer de fonduri, cunoscând că este efectuată prin folosirea unui instrument de plată electronică falsificat sau utilizat fără consimțământul titularului său, se pedepsește cu închisoarea de la unu la 5 ani.

(2) Cu aceeași pedeapsă se sancționează acceptarea uneia dintre operațiunile prevăzute în alin. (1), cunoscând că este efectuată prin utilizarea neautorizată a oricăror date de identificare sau prin utilizarea de date de identificare fictive.

Titlul VII - Infracțiuni contra siguranței publice, la Capitolul VI Infracțiuni contra siguranței și integrității sistemelor și datelor informatice:

ART. 360 Accesul ilegal la un sistem informatic

(1) Accesul, fără drept, la un sistem informatic se pedepsește cu închisoare de la 3 luni la 3 ani sau cu amendă.

(2) Fapta prevăzută în alin. (1), săvârșită în scopul obținerii de date informatice, se pedepsește cu închisoarea de la 6 luni la 5 ani.

(3) Dacă fapta prevăzută în alin. (1) a fost săvârșită cu privire la un sistem informatic la care, prin intermediul unor proceduri, dispozitive sau programe specializate, accesul este restricționat sau interzis pentru anumite categorii de utilizatori, pedeapsa este închisoarea de la 2 la 7 ani.

ART. 361 Interceptarea ilegală a unei transmisii de date informatice

(1) Interceptarea, fără drept, a unei transmisii de date informatice care nu este publică și care este destinată unui sistem informatic, provine dintr-un asemenea sistem sau se efectuează în cadrul unui sistem informatic se pedepsește cu închisoarea de la unu la 5 ani.

(2) Cu aceeași pedeapsă se sancționează și interceptarea, fără drept, a unei emisii electromagnetice provenite dintr-un sistem informatic, ce conține date informatice care nu sunt publice.

ART. 362 Alterarea integrității datelor informatice

Fapta de a modifica, șterge sau deteriora date informatice ori de a restricționa accesul la aceste date, fără drept, se pedepsește cu închisoarea de la unu la 5 ani.

ART. 363 Perturbarea funcționării sistemelor informatice

Fapta de a perturba grav, fără drept, funcționarea unui sistem informatic, prin introducerea, transmiterea, modificarea, ștergerea sau deteriorarea datelor informatice sau prin restricționarea accesului la date informatice, se pedepsește cu închisoarea de la 2 la 7 ani.

ART. 364 Transferul neautorizat de date informatice

Transferul neautorizat de date dintr-un sistem informatic sau dintr-un mijloc de stocare a datelor informatice se pedepsește cu închisoarea de la unu la 5 ani.

ART. 365 Operațiuni ilegale cu dispozitive sau programe informatice

(1) Fapta persoanei care, fără drept, produce, importă, distribuie sau pune la dispoziție sub orice formă:

a) dispozitive sau programe informatice concepute sau adaptate în scopul comiterii uneia dintre infracțiunile prevăzute în art. 360-364;

b) parole, coduri de acces sau alte asemenea date informatice care permit accesul total sau parțial la un sistem informatic, în scopul săvârșirii uneia dintre infracțiunile prevăzute în art. 360-364,

se pedepsește cu închisoare de la 6 luni la 3 ani sau cu amendă.

(2) Deținerea, fără drept, a unui dispozitiv, a unui program informatic, a unei parole, a unui cod de acces sau a altor date informatice dintre cele prevăzute în alin. (1), în scopul săvârșirii uneia dintre infracțiunile prevăzute în art. 360-364, se pedepsește cu închisoare de la 3 luni la 2 ani sau cu amendă.

Pe lângă aceste capitole distincte dedicate, același act normativ mai conține referiri la infracțiunile comise în mediul informatic la articolele: **230, furtul în scop de folosință; 302, violarea secretului corespondenței; 311-313 și 324-325, infracțiuni de fals; art. 374, pornografia infantilă; art. 388, 391 – infracțiuni electorale.**

RECOMANDĂRI PENTRU PĂRINȚI

Recomandările adresate părinților trebuie să vizeze:

➤ *Elemente generale privind fenomenul:*

- Să conștientizeze existența riscurilor asociate navigării pe internet și să cunoască în ce mod pot fi expuși copiii lor la acestea;
- Să comunice deschis cu copiii lor despre Internet, despre beneficiile și pericolele existente în lumea virtuală. Comunicarea trebuie să îmbrace forma unui dialog între părinte și copil, nu a unui monolog. Copilul trebuie să știe că poate discuta cu părinții despre orice aspect întâlnit în lumea virtuală;
- Să stabilească **împreună cu copiii** reguli de utilizare a internetului și să urmărească respectarea lor de către aceștia;
- Să nu restricționeze excesiv și nejustificat accesul copiilor la internet;
- Să le prezinte copiilor riscurile la care se pot expune în mediul online. Ei trebuie învățați că, deși utilizarea internetului are o multitudine de efecte benefice, nu este în totalitate lipsită de pericole;
- Să se asigure că știu parola/parolele de acces ale copiilor la contul de email, rețele de socializare etc. și să fie atenți la „prietenii” online pe care ei le întrețin. De asemenea, să încerce să cunoască programele și aplicațiile folosite de copii pe dispozitivele de accesare a internetului.

➤ *Soluții tehnice de control parental al posibilităților de navigare a copilului pe internet:*

- Soluții complete de aplicații antivirus actualizate;
- Programe de filtrare care pot bloca automat accesul copiilor către anumite categorii de site-uri;
- Motoare de căutare pentru copii (ex. Google Search Engine for Kids) – acestea filtrează automat rezultatele căutărilor de pe internet, excluzând paginile inadecvate minorilor.

➤ *Semne de recunoaștere a posibilei expuneri la risc în mediul online a copilului* – acest subiect este unul extrem de sensibil, mulți părinți având tendința de a-și „apăra” copiii, refuzând nejustificat

(necunoaștere a fenomenului, pudoare excesivă etc.) discuțiile sau acceptarea existenței unora din aceste semne:

- Copilul petrece perioade foarte mari de timp singur pe internet, în special noaptea;
 - Începe să cheltuiască sume de bani mai mari decât cele puse la dispoziție de părinți sau, din contră, solicită acestora, în mod nejustificat, astfel de sume;
 - Părinții găsesc materiale pornografice în calculatorul/lap-top-ul/tableta/telefonul copilului;
 - Copilul primește telefoane de la persoane necunoscute ori sună astfel de persoane și se ferește de părinți când vorbește;
 - Are tendințe de izolare față de familie și prietenii apropiați;
 - Folosește conturi de internet (mail, rețele de socializare) care nu îi aparțin sau altele decât cele pe care le cunosc părinții.
- *Posibilități de raportare a posibilelor abuzuri* –
- Sesizarea directă a organelor de poliție competente - www.efrauda.ro;
 - Solicitarea de sprijin ONG-urilor care gestionează website-uri în domeniu. Ex. www.safernet.ro sau www.sigur.info.

RECOMANDĂRI PENTRU COPII

Printre recomandările ce pot fi adresate copiilor pe această temă, putem menționa:

- Fiți prudenți în a oferi persoanelor cunoscute pe Internet informații personale despre tine sau familia ta, cum ar fi: numele, vârsta, CNP-ul, numărul de telefon, fotografiile personale, adresa, școala la care înveți; dacă anumite persoane insistă să afle aceste detalii, anunță-ți imediat părinți, căci este foarte probabil că au intenții necurate;
- Nu spune parola de la e-mail-ul tău altor persoane în afara părinților; dacă le comunică această parolă prietenilor sau altor persoane, acestea pot trimite mesaje jignitoare în numele tău sau pot intra pe site-uri interzise;
- Prietenii din mediul online trebuie să fie doar persoane pe care le cunoașteți în realitate. Nu accepta niciodată să te întâlnești direct cu o persoană pe care ai cunoscut-o pe Internet; oamenii pot fi foarte diferiți de ceea ce au pretins că sunt și astfel poți deveni victima traficului de persoane și a altor întâmplări tragice. Nu folosi telefonul personal pentru a suna pe cineva cunoscut pe Internet;
- Manifestați atenție în utilizarea rețelelor de socializare. Este de preferat să restricționați accesul la acestea, astfel încât să poată fi vizualizate dor de către prietenii;

- Evită să postezi pe Internet fotografii cu tine sau cu familia ta; acestea sunt personale și nu trebuie să ajungă la cunoștința oricui navighează pe Internet; ele pot fi folosite pentru a vă face rău, ție sau celor apropiați;
- Nu uita că nu tot ceea ce citești sau vezi pe Internet este adevărat! Informațiile aflate pe o pagină web pot fi postate de oricine, adult sau copil, multe din ele fiind neverificate sau eronate; de asemenea, fotografiile sau filmele pot fi modificate pe calculator și pot înfățișa situații care nu s-au petrecut niciodată;
- Nu instala pe dispozitivul tău programe sau aplicații fără a-ți consulta părinții. Ele pot conține malware și produce pagube irecuperabile;
- În cazul în care primești pe e-mail mesaje de la persoane necunoscute, nu le deschide; de asemenea, nu accesa link-uri sau atașamente primite odată cu astfel de mesaje;
- Dacă cineva te face să te simți inconfortabil pe Internet, poți oricând să renunți la comunicarea cu acea persoană. Nu ești obligat să stai pe Internet mai mult decât consideri tu și nici să suporti ceea ce îți provoacă neplăcere sau teamă; poți oricând să îi scoți de pe lista de contacte pe cei cu care nu vrei să mai comunici!
- În cazul în care o persoană cu care comunici pe internet te jignește, te amenință, îți transmite mesaje cu tentă sexuală, îți cere să îi trimiți poze nud cu tine sau îți trimite poze cu conținut pornografic, te îndeamnă să consumi alcool ori droguri, anunță-ți părinții sau fă o sesizare pe unul din site-urile specializate;
- Cere ajutorul, în orice situație, persoanelor în care ai încredere, părinți, profesori sau prieteni apropiați.