Nume: Ciuchi
Prenume: Rareș Andrei
Clasa: a-XI-a
Unitatea de învățământ: Liceul Teoretic Nicolae Iorga - București

SIGURANȚA CIBERNETICĂ ÎN RÂNDUL ADOLESCENȚILOR

Securitatea cibernetică se referă la activitățile necesare pe care cetățenii și companiile le pot face pentru a-și proteja rețelele și aplicațiile informatice, de a proteja utilizatorii acestor sisteme în fața amenințărilor cibernetice. De asemenea, amenințările din spațiul virtual sunt diverse și pot produce atât efecte psihologice cât și juridice asupra vieții de zi cu zi a adolescenților(1). Datorită riscurilor la care se pot expune în mediul online, adolescenții trebuie învățați că, deși utilizarea internetului are o multitudine de efecte benefice, nu este în totalitate lipsită de pericole(2).

Principalul obiectiv al acestui eseu este de a evidenția importanța asigurării siguranței cibernetice și de a evidenția aspectele juridice pe care le implică anumite activități malițioase desfășurate în mediul online. Eseul abordează aspecte privind comunicarea(transmiterea de mesaje) și realizarea de tranzacții financiare prin intermediul spațiului virtual, a infracțiunilor ce se pot comite prin intermediul aplicațiilor de mesagerie și social media precum și a implicațiilor juridice și de răspundere în fața legii pentru adolescenți. Prin cercetarea și aprofundarea acestor aspecte, lucrarea evidențiază necesitatea unei mai bune înțelegeri a metodelor și a motivației infractorilor cibernetici din mediul online, precum și a repercursiunilor juridice a acțiunilor și activităților desfășurate de adolescenți în spațiul virtual. Prezența adolescenților în mediul online se realizează, în cele mai multe cazuri, prin intermediul aplicațiilor de mesagerie și social media. Aceste aplicații, deși au implementate arhitecturi și măsuri tehnice de securitate bine puse la punct, pot deveni periculoase pentru utilizatori din cauza neglijenței și a neatenției acestora.

Utilizarea aplicațiilor de mesagerie și social media poate aduce adolescenții în situația de a fi victime sau de a încalcă legislația fără a avea cunoștințe juridice privind consecințele legale a acțiunilor realizate.

Publicarea de fotografii și materiale video fără acordul persoanelor, începerea de discuții cu persoane necunoscute, întâlniri cu persoane pe care nu le-ai cunoscut anterior (față în față) prin intermediul aplicațiilor online, transmiterea cu mare ușurință a datelor personale și financiare sunt doar o parte din pericolele pe care majoritatea adolescenților le ignoră și care au implicații juridice de răspundere în fața legii.

Una dintre cele mai frecvente metode utilizate este metoda „loverboy”(3) prin care persoane adulte conving adolescenți să aibă încredere în ei cu scopul de a-i manipula sau șantaja în vederea exploatării sexuale. Metoda „loverboy” este una dintre practicile folosite pentru a atrage tinere adolescente în rețele de trafic de persoane. Agenția Națională Împotriva Traficului de Persoane spune că ăsta e modul prin care traficanții de persoane se folosesc de atașamentul emoțional al unei femei pentru a o exploata.

Una dintre situațiile în care se găsesc din ce în ce mai frecvent adolescenții este intimidarea și constrângerea lor pentru a lua parte la activități infracționale cum ar fi transport și comercializare de substanțe interzise de mare risc (droguri, steroizi). În majoritatea cazurilor tinerii sunt folosiți pentru realizarea schimbului propriu-zis de substanțe ca intermediari între părțile implicate în tranzacție.

O mare parte a problemelor menționate mai sus derivă din efectul bullying-ului asupra tinerilor, aceștia simțindu-se marginalizați de restul grupului din care fac parte. Aplicațiile de social media au și ele un rol în acest sens, trimiterea de mesaje intimidante precum „sinucide- te” sau „n-ai tupeu să” pot afecta adolescenții care suferă de anumite afecțiuni (de orice natură), iar aceste manifestări sunt cuprinse în infracțiunile de amenințare/hărțuire (după natura lor).

Astfel, aplicațiile de mesagerie și social media reprezintă principalele canalele de șantaj și cyberbullying cu scopul de a intimida, speria, sau umili pe adolescenți prin postarea de fotografii indecente, transmiterea de mesaje neadevărate sau de amenințări, copierea identității unei persoane și transmiterea în numele acesteia de mesaje răuvoitoare(4).

Un aspect cu implicații juridice majore este reprezentat de șantajul care are ca scop obținerea de bani sau bunuri prin intermediul tehnologiei care se realizează prin metode de păcălire a adolescenților. Cea mai întâlnită metodă este cea în care șantajistul solicită informații personale (informații propriu-zise, imagini, videoclipuri), iar odată ce se află în posesia acestora, el va cere o sumă de bani victimei pentru a nu le publica. Aceasta se încadrează la infracțiunea de șantaj, indiferent de faptul că a fost comis în mediul online.

Odată cu apariția tehnologiei, sectorul bancar a început să fie din ce în ce mai digitalizat, prin apariția cardurilor bancare și a altor metode de plată online ce nu implică bani fizici. Cardurile bancare, deși eficientizează procesul de a plăti, pot fi abuzate dacă ajung la îndemâna copiilor și tinerilor. Copii (sub 14 ani) sunt atrași cel mai ușor în astfel de capcane, spre exemplu cheltuirea de bani pe un joc sau o aplicație fără limită, dacă cardul a fost deja introdus în acea aplicație, dar cu toate astea nici adolescenții nu sunt în siguranță când vine vorba de cumpărături online.

Un aspect în ceea privește siguranța online a adolescenților este reprezentat de utilizarea instrumentelor financiare în realizarea de cumpărături online (carduri bancare, monede virtuale - cryptomonede) care prezintă o un pericol la adresa tinerilor prin intermediul înșelătoriilor (scams). Utilizarea piețelor online reprezintă un risc datorită unor incertitudini cum ar fi: identitatea vânzătorului/cumpărătorului este anonimă, introducerea datelor de identificare a cardurilor bancare, a adreselor de domiciliu(în cazul livrării acasă), posibilitatea că produsul listat spre vânzare să nu fie la fel în realitate ca în pozele de pe site etc.

Site-urile de e-commerce reprezintă o piață pe care utilizatorii pot cumpăra/vinde diferite tipuri de produse și servicii. Aceste site-uri facilitează o relație directă și anumite servicii, cum ar fi transportul produselor și a diversității mediilor de plată, pentru ca procesul să fie cât mai simplu și facil atât pentru vânzător cât și pentru cumpărător. Chiar dacă platformele de comerț electronic au fost gândite cu intenții bune, și acestea prezintă o serie de factori de risc. Cea mai mare parte a site-urilor de comerț electronic se implică în schimbul propriu-zis, fiind un moderator între vânzător și cumpărător (de ex. eMAG.ro, mediagalaxy.ro), prin verificarea vânzătorilor și a calității produselor acestora, etc., dar există anumite platforme în care intermedierea nu poate fi verificată, în care interacțiunea dintre vânzător și cumpărător se realizează în mod direct, facilitând astfel apariția scam-urilor. Acest model de business permite asocierea unor scheme frauduloase pentru persoane rău-intenționate. În general, adolescenții și personale vârstnice sunt victimele preferate ale acestora, prin lipsa de educație financiară și digitală privind pericolele din mediul online. Cel mai des întâlnit tip de fraudă în mediul online este cea de scam.

Scamming-ul este apelativul modern pentru înșelătoriile care se întâmplă de mii de ani. De la apariția internetului, respectiv de la apariția piețelor și tranzacțiilor online, înșelătoriile(5) au apărut și în spațiul virtual. Acestea presupune ca una dintre părți implicată în schimb să nu se țină de promisiune (vânzătorul să nu trimită produsul, cumpărătorul să nu trimită banii). Ceea ce face scamming-ul să fie atât de răspândit este fenomenul cunoscut ca „Social

Engineering”(6), ce implică manipularea psihologică a oamenilor, astfel încât aceştia să lase garda jos şi să îşi transmită de bună voie datele personale/financiare.

Ingineria socială ce implică o uzurpare de identitate în mediul online sau folosind mijloace de comunicare la distanță poate intra sub incidența infracțiunii de fals informatic. Obținerea de beneficii financiare și materiale în spațiul virtual prin metode de păcălire a unei persoane reprezintă una dintre cele mai întâlnite metode în rândul adolescenților. Mediul unde acest tip de înșelătorii se petrec cel mai des sunt jocurile video cu achiziții în aplicație, unde platforma permite realizarea de schimburi direct între jucători.

Pentru a preveni astfel de situații, piețele online au început să ia măsuri, cum ar fi verificarea utilizatorilor, securizarea datelor personale etc. Pe de altă parte și băncile care eliberează carduri bancare au luat măsuri de tipul autentificarea cu doi factori, necesitarea unei autorizări pentru plăți mai mari de o anumită sumă, pentru ca tinerii să aibă o marjă de siguranță când le folosesc.

Pe lângă aceste măsuri de siguranță pe care companiile le iau pentru a preveni criminalitatea în spațiul cibernetic, adolescenții trebuie și ei la rândul lor să fie instruiți cum să își protejeze echipamentele cu care accesează spațiul virtual. Câteva exemple de astfel de măsuri tehnice care sunt necesar fi incluse în educația adolescenților pot fi implementate prin instalarea și utilizarea corectă a sistemelor de operare și de programe licențiate, aplicații dedicate și suite de securitate antivirus, înțelegerea unor noțiuni avansate cu ar fi criptarea datelor, autentificarea cu doi factori și în mod special o gestionare corectă a parolelor(7).

Înțelegerea metodelor folosite de infractorii cibernetici și a motivației(8) acestora reprezintă un factor cheie pentru asocierea corectă a consecințelor și riscurilor juridice posibile și necesită elaborarea de strategii eficiente de prevenire a infracționalității în mediul online, școlar și familial(9). Astfel, sunt necesare realizarea unor campanii de informare în rândul adolescenților în cadrul unităților de învățământ cu referire la implicațiile juridice pe care acțiunile lor le au, chiar dacă se petrec în spațiul virtual. Folosirea tehnologiei în comiterea de infracțiuni nu te absolvă de răspunderea în fața legii, această fiind un instrument care face posibilă săvârșire unor acțiuni ilegale. De asemenea, pot fi introduse programe de educație juridică(10) și civică în școli și licee, pentru că toți tinerii să fie informați și protejați.

În concluzie, educația digitală, cunoașterea principalelor amenințări din spațiul cibernetic și a măsurilor tehnice, procedurale și legale reprezintă ansamblul de instrumente care pot fi utilizate pentru asigurarea siguranței în mediul online pentru adolescenți. Conștientizarea în rândul adolescenților a riscurilor existente privind utilizarea Internetului necesită și o abordare din punct de vedere legislativ pentru conștientizarea consecințelor juridice și a răspunderii în fața legii.

Dezvoltarea tehnologică și digitalizarea societății transformă relaționarea și interacțiunea dintre componentele acesteia. Pe măsură ce mai multe date sunt colectate, stocate și schimbate electronic, nu numai că apar noi oportunități de monetizare, ci și noi riscuri și responsabilități, care dacă nu sunt cunoscute pot produce consecințe juridice grave pentru cetățeni.

Educația juridică reprezintă o componentă importantă pentru societatea în care trăim, și fiecare cetățean, indiferent de statutul său, ar trebui să își cunoască atât drepturile cât și responsabilitățile pe care le are în mediul online.

Bibliografie:

(1) Siguranța Cibernetică. Recomandări pentru părinți si copii, *https://ag.politiaromana.ro/ro/prevenirea-criminalitatii/recomandari/siguranta-cibernetica* accesat la data de 15.09.2023
(2) În siguranță pe internet - *https://youth.europa.eu/get-involved/your-rights-and-inclusion/be-safe-online_ro*, accesat la data de 16.09.2023
(3) Mototolea, C., *Metodica cercetării traficului de ființe umane cu metoda de recrutare „Loverboy”,* Acta Universitatis George Bacovia. Juridica - Volume 7. Issue 2/2018 - *https://www.ugb.ro/Juridica/Issue14ROEN/7._Metodica_cercetarii_traficului_de_fiinte_umane.Cornel_Mototolea.RO.pdf*, accesat la data de 15.09.2023
(4) Ce este cyberbullying-ul? *https://www.unicef.org/romania/ro/pove%C8%99ti/cyberbullying-ce-este-%C8%99i-cum-%C3%AEi-punem-cap%C4%83t*, accesat la data de 15.09.2023
(5) Cele mai frecvente tipuri de fraude din România - *https://sigurantaonline.ro/cele-mai-frecvente-tipuri-de-fraude-din-romania/*, accesat la data de 15.09.2023
(6) Ghid de conștientizare a tehnicilor de inginerie sociala, *https://certmil.ro/wp-content/uploads/2022/04/20220408_N_Social-Engineering.pdf*, accesat la data de 15.09.2023
(7) Ghid de Securitate Cibernetica, *https://dnsc.ro/vezi/document/ghid-securitate-cibernetica-2021*, accesat la data de 15.09.2023
(8) Cum să vă protejați de infractorii cibernetici, *https://www.europarl.europa.eu/news/ro/headlines/society/20200327STO76003/cum-sa-va-protejati-de-infractorii-cibernetici*, accesat la data de 15.09.2023
(9) Manual de educație (alfabetizare) în domeniul internetului, *https://rm.coe.int/internet-handbook-ro/16809f0b11* , accesat la data de 16.09.2023
(10) Materiale educație juridica, *https://www.csm1909.ro/PageDetails.aspx?PageId=195&FolderId=356* , accesat la data de 15.09.2023