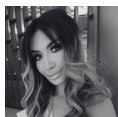


CYBERCRIME - O AMENINȚARE ÎN EVOLUȚIE. CRIMINALITATE FĂRĂ CONTACT FIZIC



Cons. jur. Ștefania ZORCĂ

Abstract: *The rapid evolution of criminality in the context of advanced technology requires increased attention of all bodies concerned with the safety of citizens in the rule of law. Traditional criminality is changing as societies evolve and is becoming increasingly inventive, taking advantage of the benefits that technology offers. Cybercrime is therefore one of the forms that demonstrate criminal adaptability, offering criminals significant advantages such as anonymity and the lack of need for physical contact with victims.*

This article briefly explores the definitions of crime, the types of cybercrime that are widespread and the advantages that technology offers to modern criminals. The conclusions briefly underline the need for international cooperation to combat this growing global phenomenon.

Keywords: *cybercrime, contactless crime, technological advances, international cooperation*

Criminalitatea - definiții

Criminalitatea nu este nicidecum un aspect nou cu care societățile se confruntă, însă modul în care aceasta evoluează impune specialiștilor și persoanelor interesate în domeniu să se concentreze asupra determinării unor noi mijloace de pregătire și specializare astfel încât să preîntâmpine evoluția inventivității criminale și efectele negative pe care aceste practici le au asupra cetățenilor oricărui stat de drept.

În sens larg, criminalitatea poate fi înțeleasă sub forma oricăror acțiuni care sunt de natură a produce consecințe dăunătoare unui individ fie prin atingerea directă a integrității acestuia, fie prin daunele produse asupra unor elemente pe care individul le deține.

Conform marelui sociolog Emile Durkheim, infracțiunea este un act care jignește anumite sentimente colective foarte puternice, în timp ce unul dintre cei mai influenți criminologi, Edwin H. Sutherland, alege să definească infracțiunea drept un comportament învățat prin interacțiuni cu alții care comunică valori criminale. Printre cele mai scurte definiții ale criminalității se numără cea a lui Donal R. Cressey, cunoscut pentru studiile sale concentrându-se asupra criminalității organizate și înșelăciunilor financiare, menționând că infracțiunea implică un comportament care încalcă legile.

În confirmarea evoluției fenomenului criminal sub forma unei problematice permanente care necesită atenția deosebită a tuturor agențiilor de aplicare a legii și specialiștilor care fac parte din acestea, unul dintre fondatorii criminologiei moderne, Cesare Lombroso, statuează faptul că fenomenul criminal nu este unul static, ci unul care evoluează odată cu societatea și sub condițiile în care aceasta se desfășoară, se adaptează și se schimbă sub structurile sociale, dar și în funcție de normele pe care le are la bază și evoluțiile tehnologice pe care le trăiește.

Adaptabilitatea criminală și infracțiunile digitale

Evoluția tehnologiilor a condus la o nouă formă de adaptabilitate criminală care dezvoltă potențialitatea infracțională în sfera digitală prin folosirea instrumentelor care avantajează făptuitorii primordial prin lipsa nevoii de contact fizic. Reiterăm așadar faptul că tehnologia nu este doar apanajul indivizilor care o folosesc în scopul obținerii unui trai mai facil, sub spectrul respectării fundamentelor legale, ci și apanajul infractorilor care au suficiente abilități și a căror capacitate intelectuală permite dezvoltarea unor planuri infracționale ale căror etape presupun exploatarea uneltelor tehnologice în îndeplinirea interesului lor.

Fenomenul infracțiunilor digitale, cunoscut și sub termenul de „cybercrime”, a ajuns unul larg răspândit, întrucât multiple organizații, agenții, instituții și personalități au procedat la construirea unor definiții care să contribuie la înțelesul acestor practici ilegale.

În acest sens, Europol definește cybercrime sub forma unui fenomen care include toate activitățile criminale fie comise prin folosirea calculatoarelor, fie prin targetarea unor sisteme și rețele tehnologice. Pe de altă parte, Interpol definește cybercrime drept un fenomen cu ascensiune rapidă în care tot mai mulți criminali ajung să exploateze viteza, conveniența și anonimitatea internetului pentru a comite o varietate de infracțiuni. Thomas Holt, unul dintre specialiștii preocupați de cercetarea fenomenului criminalității cibernetice subliniază infracționalitatea cibernetică sub forma unei palete largi criminale care cuprinde orice activitate ilegală ce implică un computer sau un dispozitiv în rețea.

Tipuri de infracțiuni digitale și avantajele cybercrime

Pentru o mai bună înțelegere a ceea ce înseamnă infracțiunile din sfera criminalității cibernetice enumerarea câtorva dintre acestea este crucială. Prin urmare, de la grupuri de criminalitate organizată, la fraudatori online, hackeri independenți, cyberteroriști și alte categorii, acești indivizi se concentrează asupra folosirii avantajelor tehnologiei în scopul destabilizării structurilor pe care le vizează pentru

obținerea unor foloase proprii. Printre cele mai cunoscute forme de infracțiuni digitale se numără: hacking-ul, phishing-ul, randomware-ul, fraudă cu carduri de credit, atacurile DDoS, fraudele online, cuberstalking-ul, și altele.

Activitățile criminale cibernetice oferă un spectru larg de avantaje pe care infractorii le valorifică în comparație cu infracțiunile tradiționale. Astfel, în afara anonimatului și a dificultății de a fi detectați, infractorii se bucură de posibilitatea de a comite infracțiunile pe care și le propun fără a fi necesar contactul fizic cu victimele ceea ce reduce pe de o parte riscul de a fi descoperiți și pe de altă parte generează oportunitatea unui time management mai eficient în comiterea unui număr vast de infracțiuni într-un timp mai scurt.

Într-o altă ordine de idei, infracțiunile cibernetice acoperă un număr mare de victime simultan, locația acestora fiind irelevantă ceea ce înseamnă o scalabilitate și răspândire globală cu evoluție îngrijorătoare.

Din punctul de vedere al câștigurilor semnificative, aceste atacuri sunt avantajate de posibilitatea impunerii unor practici diverse precum cererea de răscum-părări, inclusiv sub forma criptomonedelor, ceea ce facilitează posibilitatea realizării unor tranzacții mai greu de identificat.

Din punctul de vedere al costurilor reduse, infractorii cibernetici pot folosi sisteme a căror sofisticare nu este în mod necesară un aspect fundamental, întrucât de cele mai multe ori simplul acces la internet este suficient pentru înlesnirea comiterii unor astfel de infracțiuni.

Desigur, cu cât tehnologia evoluează oferind posibilitatea specialiștilor de a conduce activități mai performante de identificare a unor astfel de infractori și infracțiuni, cu atât sunt avantajați și indivizii cu astfel de interese. În sens practic, în timp ce inteligența artificială devine un liant extraordinar al evoluției rapide în cunoașterea de care omul beneficiază pe scară largă, aceasta devine și o oportunitate dinamică și iminentă în îmbunătățirea atacurilor cibernetice.

Concluzii

Evoluția criminalității este așadar un fenomen cu dinamică extinsă. Criminalitatea cibernetică devine un aspect central al siguranței lumii moderne, iar evoluția tehnologică devine pivotul îngrijorărilor față de instrumentele de care indivizii din sfera infracțiunilor digitale se folosesc în atingerea intereselor lor. Criminalitatea cibernetică este o amenințare constantă, dezvoltarea acestor practici dovedind o adaptare permanentă nu doar din perspectiva fenomenului criminal, ci și din perspectiva necesității autorităților și specialiștilor de a-și actualiza cunoștințele și practicile în eficientizarea combaterii criminalității digitale. În timp ce

inteligența artificială constituie o tehnologie emergentă, aceasta se dovedește și o provocare în ceea ce privește menținerea securității cibernetice

Prin urmare, evoluția amenințătoare a fenomenului criminalității cibernetice impune atenția sporită a tuturor organelor legislative de a impune norme și jurisdicții limitate care să controleze eficient răspândirea acestor practici, concentrându-se totodată și asupra esențialității cooperării internaționale între forțele de ordine în scopul actualizării informațiilor acestor fenomene care traversează cu multă ușurință granițele internaționale.