INTERCEPTAREA ILEGALA A UNEI TRANSMISII DE DATE INFORMATICE – CAUZE ȘI EFECTE

Crina Mușuroi și Florentina Necula
Cibernetică Economică, III, 1058
Coordonator științific: Lector univ. dr. Valentine Charlotte Ene

REZUMAT
Criminalitatea informatică reprezintă un domeniu foarte important în materie penală, oferind multe oportunități pentru dezvoltarea dinamicii și diversificării tehnologiei existente, ducând în paralel la înfăptuirea de activități ce contravin bunelor acțiuni care se doresc a se petrece în mediul informațional și virtual. Deoarece tehnologiile devin din ce în ce mai avansate într-un ritm foarte alert, la fel și personalul ocupat cu securitatea și siguranța informațiilor care circulă între utilizatori trebuie să se adapteze în mod corespondent. În acest context, criminalitatea informatică reprezintă un domeniu de mare actualitate, cu multe posibilități de exploatare, implementare și adaptare, propice activităților infracționale. Prin urmare, lucrarea prezentă își propune să analizeze cauzele și efectele unei anumite infracțiuni informatice din cele existente, prevăzută în Noul Cod Penal, intrat în vigoare la 1 februarie 2014, art. 361, și numită "Interceptarea ilegală a unei transmisii de date informatice".

CUVINTE CHEIE: Criminalitatea informatică, Noul Cod Penal, Interceptarea datelor

1. INTRODUCERE

Se cunoaște fapul că tehnologia se află într-o continuă dezvoltare, iar viteza sa de progresare din ultimii ani a reușit să întreacă așteptările. Pe lângă beneficiile nenumărate generate de rezultatele acestui proces, a apărut și problema conturării unui cadru legal de activitate în domeniul informaticii. În acest context, în ultimii ani s-a pus problema identificării infracțiunilor din acest domeniu și crearea reglementărilor penale în conformitate cu acestea.

Infracțiunile în domeniul informaticii sunt una dintre cele mai noi materii ale vieții juridice, atât la nivel mondial, dar mai ales în cazul țării noastre. Se poate spune că forma actuală a legislației referitoare la domeniul menționat anterior derivă din informațiile generate de către Consiliul European și de alte documente internaționale, România nefiind capabilă să construiască această legislație pe cont propriu din cauza lipsei experiențelor referitoare la acest subiect.

În România există în vigoare o serie de legi speciale care , prin prevederile legale conținute, determină reglementarea unei mulțimi de fapte referitoare la sistemele informatice sau la societățile informaționale.

Subiectul acestei lucrări îl constituie următoarea infracțiune informatică prevăzută în Noul Cod Penal, intrat în vigoare la 1 februarie 2014, art. 361, numită „Interceptarea ilegală a unei transmisii de date informatice". Această infracțiune reprezintă un punct de interes din cauza impactului pe care comiterea sa îl are asupra vieții private a oamenilor, dar și din cauza modalităților sale de comitere.

Textul articolului de lege referitor la infracțiunea discutată este următorul: "(1) Interceptarea, fără drept, a unei transmisii de date informatice care nu este publică şi care este destinată unui sistem informatic, provine dintr-un asemenea sistem sau se efectuează în cadrul unui sistem informatic se pedepseşte cu închisoarea de la unu la 5 ani. (2) Cu aceeaşi pedeapsă se sancţionează şi interceptarea, fără drept, a unei emisii electromagnetice provenite dintr-un sistem informatic, ce conţine date informatice care nu sunt publice."

Ceea ce e de remarcat la textul prezentat anterior este faptul că nu se referă doar la interceptarea transmisiilor de date, ci și la interceptarea emisiilor electromagnetice. Se poate spune, deci, că aceasta îngrădește corespunzător libertatea de acțiune a celor interesați să obțină informații evitând crearea unui acord cu posesorul acestora, de asemenea, entitățile implicate în transmisiile de date sunt protejate corespunzător din punct de vedere legal. Deși această infracțiune se pedepsește conform legii, multe dintre entitățile din industria tehnologiei informației își continuă activitățile ilegale prin diferite mijloace. Motivul principal al efortului de interceptare a unor transmisii de date îl reprezintă revoluția creată de conceptul "Big Data" și importanța mare care i s-a atribuit de către majoritatea firmelor de pe piață. Se poate menționa faptul că o metodă populară de interceptare a transmisiilor de informații este prin intermediul aplicaților mobile care solicită accesul la diferite informații despre utilizator, dar și la diferite funcționalități ale aparatului mobil. Astfel, o aplicație poate prelua date de care nu are nevoie și le poate transmite părților interesate, fără să primească în mod specific acordul utilizatorului.

2. CONȚINUTUL COSTITUTIV

Din textul legii prezentat anterior reiese faptul că obiectul juridic la care se referă aceasta este reprezentat de relațiile de comunicare dintre sistemele informatice, în particular transmisia de date, și de activitățile de telecomunicație. Obiectul material propriu-zis la care reglementarea se referă este reprezentat de șirurile de biți care sunt trimise de la un calculator la altul. În anumite cazuri, obiectul material este reprezentat de echipamentele tehnice care mijlocesc comunicațiile de date dintre calculatoare.

În cel de-al doilea alineat se vorbește despre interceptarea emisiilor electromagnetice, acestea fiind strâns legate de echipamentele electrice, aflându-se în vecinătatea acestora. Interceptarea acestor unde este considerată infracțiune atunci când echipamentele în cauză sunt conectate la un sistem informatic şi contribuie la transmisia, stocarea sau prelucrarea de date.

Pentru interceptarea ilegală a transmisiilor de date pot fi pedepsiți cetățenii responsabili penal care utilizează echipamente speciale pentru efectuarea acestei activități ilegale, cunoștințele individului în cauză despre acest domeniu fiind irelevante.

Persoanele dispuse să săvârșească astfel de acțiuni sunt cele care au interesul de a spiona victima, fiind cunoscut faptul că interceptarea transmisiilor de e-mail-uri și apeluri telefonice sunt tehnici foarte populare în domeniul spionajului.

De asemenea, în categoria persoanelor interesate de interceptarea transmisiilor de date sunt incluși hackerii. Aceștia au scopul de a fura date despre anumite persoane necesare pentru validarea unor conturi (de exemplu datele pentru accesarea cardurilor bancare), astfel preluând fie alte informații, fie bunuri materiale sau bani.

În cazul acestei infracțiuni se consideră drept victimă persoana care deține sistemul informatic sau componentele care leagă două sisteme informatice. Astfel, victima este entitatea care are drept de deținere asupra datelor informatice interceptate sau care are dreptul de prelucrare a acestor date în condiți legale.

Termenul de "interceptare" utilizat în articolul din Noul Cod Penal se referă la acțiunea de captare cu ajutorul unor dispozitive electronice concepute special a impulsurilor electrice, a variațiilor de tensiune sau a emisiilor electromagnetice care călătoresc într-un sistem, care rezultă din acesta sau care se află pe calea de legătură dintre mai multe sisteme de calcul.

Pentru prevenirea atacurilor cibernetice care au drept scop interceptarea transmisiilor de date și emisii electromagnetice, în majoritatea cazurilor administratorii de sistem apelează la utilizarea unor sisteme de siguranță care să permită autentificarea utilizatorilor prin intermediul unor scheme de identificare. De exemplu, majoritatea băncilor care oferă servicii online obligă utilizatorii să se autentifice în sistem pe baza unor parole unice care sunt valabile o singură dată. La următoarea autentificare se va genera o nouă parolă printr-un algoritm și va fi preluată de către utilizator prin intermediul unui dispozitiv numit "token". Însă, majoritatea platformelor online utilizează autentificarea pe baza unei parole unice generate de către sistem sau de către utilizator, acest lucru ducând la scăderea securității contului în cauză. Autentificarea pe baza de parolă prin cele două metode împiedică hackerii să își desfășoare activitățile malițioase într-un mod facil, însă pentru mărirea gradului de securitate cei care administrează sistemele și platformele în cauză trebuie să aibă în vedere criptarea fluxului de date.

Atacurile prin interceptarea datelor se pot realiza prin două metode: fie informația care circulă prin sistem este observată de către intrus, acesta nemodificând conținutul datelor, fie intrusul realizează modificări ale datelor, adaugă date false sau fură conținutul transmis.

3. MODALITĂȚI DE COMITERE A INFRACȚIUNII

Interceptarea transmisiilor de date se poate realiza prin mai multe modalități. Dacă se ia în considerare modul fizic de realizare a acesteia, se poate aminti faptul că intrusul se poate conecta la un canal de transmitere a informației dintre două sau mai multe sisteme de calcul prin intermediul unui cablu pe care îl conectează la propriul calculator.

O altă modalitate de realizare a interceptării datelor este cea prin intermediul IP-ului. Fiecare transmisie de date de la un calculator la altul dintr-o rețea cuprinde adresa IP a destinației și un număr de secvență. Hackerul determină o predicție a numărului de secvență și astfel poate avea acces la sistem asemenea unui utilizator normal, putând accesa toate informațile transmise serverului de la sistemul de calcul: parole, nume de utilizatori, date confidențiale etc.

De asemenea, această infracțiune se poate realiza prin intermediul unor aplicații specializate care au capacitatea de a supraveghea transmisiile de date dintr-o rețea și de a salva informațiile importante în cadrul unor fișiere. Aceste aplicații sunt de obicei utilizate de către furnizorii de internet pentru a analiza traficul dintr-o rețea, adică în scop de întreținere. Pe lângă furnizorii de internet, printre entitățile care pot folosi astfel de aplicații în mod legal se numără și marile corporații. Aceste firme utilizează astfel de programe în vederea

monitorizării activității angajaților și pentru a preveni scurgerile de informații care ar putea fi de ajutor concurenței. De asemenea, corporațiile utilizează astfel de aplicații pentru a se asigura că în incinta firmei angajații nu desfășoară activități ilegale precum instalarea și folosirea unor programe la care aceștia nu au licență, vizionarea și expunerea materialelor cu conținut pornografic, etc. Prin intermediul acestor programe, conducerea poate avea o evidență a modului în care angajații își petrec timpul în rețea.

În urma unor studii realizate de către cei de la Universitatea Berkley din California, s-a dovedit faptul că se poate descifra un text pe baza sunetelor pe care le produce tastatura la introducerea acestuia în sistemul informatic. Această metodă de interceptare a informațiilor este una dintre cele mai simple, dar performante dintre metodele existente. În această situație nu există modalități prin care victima se poate apăra de un astfel de atac, deoarece evoluția tehnologiei a permis crearea unor microfoane care pot înregistra sunete de o intensitate slabă de la distanțe destul de mari, ceea ce înseamnă că persoana în cauză nu poate depista faptul că e urmărită și nu poate lua măsuri în acest sens.

Pe lângă metodele prezentate anterior de interceptare a transmisiilor de date, există și posibilitatea folosirii unor programe specializate de tip spyware, adware sau keylogger. Acestea sunt numite generic "viruși" și se descarcă în mod automat în calculatorul victimei în momentul accesării anumitor site-uri. Programele de tip adware, împreună cu cele de tip spyware, au scopul de a urmări traseul utilizatorului în mediul web și de a transmite informații cu privire la acest traseu către cei care au realizat programul. Astfel de programe sunt utilizate de către comercianții din mediul online care folosesc informațiile obținute pentru a transmite către utilizator reclame și oferte în conformitate cu preferințele și interesele sale. Programele de tip keylogger sunt utilizate pentru a intercepta fiecare tastă apăsată de către utilizator, trimițând aceste informații către cel care a creat programul.

Cel de-al doilea alineat vizează interceptarea ilegală a unor emisii electromagnetice. Acest lucru se referă la interceptarea câmpurilor magnetice care se găsesc în apropierea dispozitivelor prin care circulă impulsuri electrice sau impulsuri electromagnetice. În prezent, captarea radiațiilor electromagnetice cu ajutorul unor dispozitive specializate are drept finalitate transformarea acestora în impulsuri electrice și, în final, în caractere alfanumerice.

Putem spune că infracțiunea menționată anterior se poate realiza numai prin intenția directă a făptașului. Nu există situații în care intrusul interceptează transmisii de date între sistemele de calcul sau emisii eletromagnetice ale unor aparate electronice din întâmplare, ci pentru a reuși acest lucru trebuie să aibă intenția de a săvârși acest act.

Spionajul populației în mediul online este una dintre activitățile desfășurate de serviciile secrete guvernamentale, lucru care încalcă în mod direct dreptul la o viață privată al indivizilor. De exemplu, Biroul Federal de Investigații al Statelor Unite ale Americii au implementat un sistem numit Carnivore care avea scopul de a monitoriza poșta electronică și comunicațiile electronice. Programul a stârnit îngrijorarea, iar grupuri precum Fundația Frontierei Electronice și Centrul Intimității Informației Electronice au realizat demersuri pentru a opri implementarea și folosirea acestui sistem, prezentând pericolele pe care le-ar genera.

Utilizarea unui astfel de program îngrădește libertatea de exprimare a oamenilor prin faptul că presupune monitorizarea e-mail-urilor și a apelurilor telefonice. Deși ar trebui ca această activitate să vizeze doar mesajele care ar putea forma dovezi în instanță pentru comiterea unor infracțiuni, oamenii sunt conștienți de faptul că pentru a descoperi punctele de interes, agenția guvernamentală trebuie să filtreze toate mesajele trimise între cetățeni.

Cele mai populare aplicații de interceptare a transmisiilor de date sunt cele de tip keylogger. Acestea nu servesc doar spionilor cibernetici cu scopuri complexe, ci și persoanelor obișnuite. Unele dintre cele mai comune situații care presupun utilizarea unui astfel de program sunt cele în care părinții sunt îngrijorați cu privire la activitatea copilului în mediul online, astfel, hotărând să achiziționeze un software care să le permită monitorizarea sa. Un alt exemplu de utilizare a acestor programe de către persoanele obișnuite îl constituie dorința unuia dintre soți de verificare a fidelității partenerului.

Deși aceste programe sunt destul de eficiente în desfășurarea activității de interceptare a datelor, o problemă a acestora este reprezentată de dificultatea instalării. Pentru a realiza acest lucru este necesar ca persoana interesată să aibă acces direct la sistemul de calcul pe care dorește să îl supravegheze, deoarece instalarea de la distanță presupune aceleași etape, iar făptuitorul trebuie să descopere modalități de păcălire a utilizatorului pentru a-l face să instaleze singur produsul.

Un plus al programelor de interceptare de tip keylogger pentru intrus îl constituie capacitatea acestora de funcționare în modul invizibil, acest lucru permițându-le să își desfășoare activitatea într-un sistem informatic fără a fi detectate de către programele antivirus sau antispyware.

Se cunoaște faptul că orice echipament care funcționează utilizând energie electrică va produce emisii electromagnetice. În cazul anumitor sisteme informatice, echipamentele utilizate pot produce emisii electromagnetice în jurul lor care să conțină informații. Intrușii utilizează aparatură specială pentru a prelua aceste emisii și a le transforma în informații.

Capacitatea de a produce radiații a echipamentelor din cadrul unui sistem informatic este consecința modalității de fabricare, instalare și utilizare a acestora. Pe lângă faptul că aceste radiații pot fi folosite pentru descifrarea transferurilor de informații, ele reprezintă și un pericol pentru oameni, aceștia desfășurându-și activitățile zilnice în medii foarte populate de astfel de echipamente. În vederea protejării de astfel de radiații s-au construit echipamente speciale care determină diminuarea acestora.

Interceptarea emisiilor electromagnetice și interpretarea acestora este foarte dificil de realizat, făptuitorul având nevoie de echipamente complexe și multe cunoștințe în domeniu pentru a putea duce misiunea la capăt. Pentru a preveni astfel de activități, persoanele care lucrează cu date importante și sunt vizate pentru a deveni victimele unei astfel de fapte pot lua diverse măsuri pentru prevenirea sau îngreunarea realizării acesteia.

În primul rând, telefoanele trebuie ținute la distanță de monitoare și imprimante pentru a nu transmite date către exterior. De asemenea, obiectele metalice trebuie evitate în camerele în care se găsesc imprimante sau monitoare care sunt utilizate pentru prelucrarea unor informații importante.

Pentru desfășurarea activităților fără a se îngrijora de aspectul interceptării emisiilor electromagnetice, entitatea în cauză trebuie să realizeze controale serioase ale persoanelor care intră în clădirea organizației și ale mașinilor situate în vecinătatea acesteia. Echipamentele vizate de către făptuitorii ilegalității trebuie să fie plasate cât mai departe de ferestrele incintei. Utilizarea celor mai noi modele de echipamente reprezintă un mare avantaj în astfel de situații, deoarece acestea sunt concepute astfel încât să emită cât mai puține radiații pentru a proteja expunerea utilizatorilor la acestea. Utilizatorii trebuie să ia în

considerare afișarea datelor secrete pe ecran pentru o perioadă foarte scurtă, iar imprimarea acestora să se facă în cât mai puține exemplare pentru a împiedica intrușii să intercepteze datele respective. O altă modalitate de prevenire a interceptării emisiilor electromagnetice o reprezintă generarea unor radiații electromagnetice în jurul echipamentelor care să conțină informații irelevante, pentru a deruta intrusul.

4. CONTEXTUL GENERAL

Calculatoarele adaugă o nouă dimensiune dreptului penal, prezentând mai multe probleme de aplicare a legii. În prim-planul preocupărilor de aplicare a legii stă necesitatea de a asigura o formare adecvată pentru a combate aceste crime, acest lucru necesitând resurse suplimentare. Astfel, gradul de sofisticare tehnică necesar pentru a urmări "traseul electronic" depășește cu mult metodele tradiționale de investigare. În majoritatea cazurilor, datele sunt criptate, ceea ce face dificilă pentru autorități discernerea conținutului informațiilor. Detectarea comportamentului penal poate fi, de asemenea, împiedicată de reticența entităților de a raporta un acces neautorizat la un calculator sau la anumite date.

În plus, corporațiile se pot teme de publicitatea negativă care ar putea rezulta ca urmare a compromiterii sistemelor acestora. Accesul neautorizat la un calculator sau interceptarea ilegală a transmisiilor de date de la un calculator sau alt dispozitiv electronic poate trece neobservat de către persoana sau entitatea al cărei sistem informatic a fost invadat. La fel de provocatoare sunt problemele politice și juridice. Este necesar să se adopte legislația care să interzică suficient abuzurile tehnologiei noi și în curs de dezvoltare. Viteza cu care se dezvoltă tehnologia face din aceasta o preocupare continuă. În unele cazuri, linia de demarcație dintre ce va fi luat în considerare ca fiind comportament penal și ceea ce va fi civil rămâne incertă.

O dezbatere comună în discuțiile infracțiunilor de afaceri constă în faptul, dacă activitatea realizată este fie o practică de afaceri agresivă, fie o crimă. În plus, problemele de competență și de putere de aplicare prezintă probleme speciale, dat fiind faptul că internetul funcționează la nivel internațional. Acest lucru poate deveni deosebit de problematic atunci când țările adoptă standarde diferite de ceea ce constituie infracțiune sau diferite sancțiuni pentru activitățile infracționale referitoare la calculatoare, mediul online, transmisia și interceptarea de date, în mod ilegal.

Un mod de definire a criminalității informatice surprinde diferite etape precum, prevenirea, cercetarea, reprimarea și impunerea de sancțiuni celor ce înfăptuiesc acțiunile în cauză. Securitatea informatică face referire la o colecție de instrumente, politici, abordări de gestionare a riscurilor, acțiuni, formări, întreprinderi a celor mai bune practici, asigurări și tehnologii care pot fi utilizate pentru a proteja mediul cibernetic, precum și activele organizațiilor sau informațiile utilizatorilor.

5. PARTICULARIZAREA INFRACȚIUNII

Legea, în cauză, care se ocupă de criminalitatea informatică, definește și pedepsește diferite acte, în cazul de față, făcând referire la interceptarea ilegală a transmisiilor de date informatice. Interceptarea este realizată prin mijloace tehnice, fără drepturi de transmitere non-publice de date informatice la, de la, sau în cadrul unui sistem informatic, incluzând și emisiile electromagnetice provenite de la un sistem informatic, care transportă astfel de date informatice. De asemenea, interceptarea se referă și la ascultarea, înregistrarea, monitorizarea

sau supravegherea conținutului comunicațiilor, inclusiv procurarea conținutului datelor, fie direct, prin accesul și utilizarea unui sistem informatic sau indirect, prin utilizarea diferitelor dispozitive de interceptare în același timp în care comunicația are loc.

Printre diferitele metode amintite anterior de interceptare a datelor informatice, pot fi menționate și cele de interceptare și divulgare, în mod ilegal, a comunicațiilor radio, prezentând sancțiuni penale severe. Astfel, există situații în care se interzice utilizarea neautorizată a informațiilor furnizate de alte persoane prin intermediul conexiunilor radio pentru propriul beneficiu; în cazul unei companii de taximetrie în care se interceptează comunicațiile radio dintre dispeceri și șoferii unei companii rivale, cu scopul de a obține avantaje competitive; interceptarea neautorizată a semnalelor de la serviciile de televiziune cu plată, cum ar fi televiziunea prin cablu sau prin satelit; punerea la vânzare sau publicarea unei înregistrări sau conținutului conversației telefonice a unei alte persoane ș.a.

Echipamentele folosite pentru a intercepta comunicațiile radio sunt foare variate și, prin urmare, este interzisă autorizarea echipamentelor de scanare care:

- pot primi transmisii în intervalul frecvențelor alocate serviciilor de telefonie mobilă de pe piața internă;
- pot fi ușor modificate de către utilizator pentru a intercepta comunicațiile celulare;
- pot fi echipate cu decodoare care convertesc transmisiile digitale către voci audio analogice.

Interzicerea interceptării ilegale a transmisiilor de date are ca scop protejarea dreptului la viața privată. Această infracțiune prezintă încălcarea intimității comunicării prin ascultarea și înregistrarea convorbirilor orale între persoane. Convenția cere statului să stabilească interceptarea drept infracțiune, conform legilor interne, fără dreptul de a fi realizate transmisiile non-publice de date informatice. De asemenea, este obligat să legifereze stabilirea competențelor și a procedurilor penale sau de investigații specifice împotriva infracțiunilor de colectare a datelor, săvârșite prin intermediul unui calculator sau a unui dispozitiv electronic.

În timp ce sunt stabilite standarde diferite de drepturi și libertăți, măsurile de protecție trebuie să includă o supraveghere independentă sau judiciară, motive care să justifice procedura, precum și o limită privind domeniul de aplicare sau durata procedurii. În plus, păstrarea datelor informatice trebuie să se realizeze în siguranță, departe de orice tip de acțiune ce poate duce la modificarea, deteriorarea sau ștergerea acestora. Acest lucru este necesar, în special, în cazul în care, existe motive pentru a crede că datele prezintă vulnerabilitate.

Traficul de date se poate dovedi important pentru a determina sursa și destinația comunicațiilor, astfel încât să se poată identifica persoanele implicate în activități criminale informatice. Pentru că aceste date sunt adesea stocate pentru o perioadă scurtă de timp, sunt necesare măsuri pentru a fi păstrate în siguranță. Furnizorii de servicii, care se ocupă cu această sarcină, trebuie să prezinte o cantitate suficientă de date de trafic pentru a permite identificarea altor furnizori de servicii implicați în calea comunicării.

Astfel, subiectul activ al infracțiunii informatice poate fi orice orice persoană fizică sau juridică care întrunește, în mod general, condițiile și limitările răspunderii penale. Acesta prezintă, de obicei, cunoștințe în domeniul calculatoarelor, informaticii sau electronicii, având acces și utilizând dispozitive electronice special destinate interceptărilor din mediul informatic, pentru a duce la bun sfârșit acțiunea întreprinsă.

Pe de altă parte, subiectul pasiv reprezintă o persoană fizică sau juridică, care are în proprietate un sistem informatic sau un mijloc de transmisie dintre două sau mai multe sisteme informatice. Prin urmare, deținerea sistemelor informatice conferă și dreptul deținerii datelor informatice, ce sunt vizate pentru a fi interceptate și utilizate.

Realizarea acestei infracțiuni este luată în considerare în momentul în care acțiunea este întreprinsă fără drept, în termenii legislației actuale, fiind necesar ca datele informatice să nu fie făcute publice. Interceptarea prin mijloace tehnice și dispozitive speciale a semnalelor electrice sau electromagnetice, ce se află în interiorul sistemului informatic țintă se manifestă în timpul funcționării acestuia sau în timpul comunicării și transmisiei datelor dintre două sau mai multe sisteme informatice.

Interceptarea constă în monitorizarea atentă a traficului de comunicații pentru a obține datele informatice vizate. Acțiunile ce sunt întreprinse de către infractor pot fi de două tipuri: acțiuni pasive, prin intermediul cărora nu se modifică conținutul datelor, doar este observată informația care traversează traficul respectiv; precum și acțiuni active, în care interceptarea constă în furtul, alterarea, modificarea datelor obținute. Astfel, latura obiectivă a fraudei o constituie elementul material, ce este caracterizat a fi interceptat, prin orice mijloace sau tipuri de tehnologii de natură informatică, iar latura subiectivă este caracterizată de intenția celui ce realizează acțiunea în cauză. Consumarea se realizează în momentul în care datele sunt interceptate și se epuizează în momentul în care interceptarea încetează.

Un caz special, reprezentat de interceptarea, fără drept, de la distanță, descrie captarea undelor electromagnetice de la o anumită distanță în jurul unui dispozitiv prin care trec impulsuri electromagnetice. Radiațiile electromagnetice, captate cu ajutorul dispozitivelor speciale, sunt amplificate, filtrate și transformate în semnale electrice, și ulterior în mesaje ușor de înțeles. Tentativa de a realiza interceptarea transmisiilor de date informatice, dar și a emisiilor electromagnetice se pedepsește conform prevederilor legii în vigoare, iar sancționarea celor ce o înfăptuiesc constă în pedeapsa principală cu închisoarea de la 1 la 5 ani. Astfel, se încearcă păstrarea ordinii și protecției drepturilor și a libertății, într-un mediu în care dezvoltarea tehnologică a sistemelor informatice crează posibilitatea de încălcare a valorilor și relațiilor sociale, mărind prejudiciile și ducând la creșterea numărului de infractori virtuali. Prin urmare, este necesară o supervizare cât mai atentă a mediului informatic.

În mod concludent, pe măsură ce tehnologia se dezvoltă, legea trebuie sa raspundă noilor evoluții în cadrul acestui tip de crime informaționale, pentru a descuraja pe cei care abuzează de noua tehnologie.

6. CYBER SMART DEFENCE

Un exemplu românesc în cadrul asigurării securității transmisiilor informației îl constituie Cyber Smart Defence (prescurtat CSD), o companie de dezvoltare web fondată în anul 2004. Pentru a îndeplini cerințele clienților din România și din străinătate, pentru a verifica și securiza site-urile web, sistemele livrate și informația transmisă între utilizatori, societatea a abordat un nou domeniu complex de protecție cibernetică, devenind un furnizor de încredere în testarea de vulnerabilități și de securitate IT. În ultimii ani, siguranța clienților a fost susținută prin gestionarea securității datelor acestora, evaluarea vulnerabilităților în sistemele lor și eliminarea riscurilor de hacking într-o mare măsură.

Având parteneriate strategice cu un număr de experți în domeniul securității cibernetice, compania oferă un set complet de servicii de securitate cibernetică, special adaptate și perfect montate în conformitate cu cerințele specifice ale fiecărui client în parte. Cu toate acestea, experții nu sunt specialiști IT obișnuiți. Ei sunt indivizi talentați care cunosc modul de funcționare a celor mai complexe și cuprinzătoare programe de calculator. Excelează la găsirea și neutralizarea amenințărilor de securitate ale sistemelor IT, capacitățile și competența personalului fiind bine cunoscute de către un număr mare de companii multinaționale. Prin urmare, oferă un nivel ridicat de protecție pentru rețele, sisteme și aplicații împotriva oricăror amenințări cibernetice și alte activități rău intenționate.

Este folosită o gamă largă de instrumente, de la testarea securității interne pe propriile sisteme, la testarea internă sau externă pentru clienții care folosesc baze de date vaste stocate în modul clasic sau în formatele Cloud. În plus, se poate emite, pentru fiecare client, un raport complet, inclusiv un set de recomandări pentru a elimina toate amenințările și încălcările securității, îmbunătățirea performanțelor sistemului și a nivelului de securitate.

7. CONCLUZII

Amenințările în mediul cibernetic și informatic sunt într-o continuă evoluție și diversificare, iar combinate împreună de către suspecți, se poate ajunge la formarea de noi atacuri. Conștiința de sine este primul pas în protejarea identității private, de aceea este indicat a fi conștient dacă cineva ar încerca și ar putea fura informațiile personale.

Cu toate acestea, pentru a preveni și a combate criminalitatea informatică, sunt adoptate principii precum legalitatea, drepturile și libertățile fundamentale, eficiența, inevitabilitatea pedepsei, securitatea calculatoarelor și protecția datelor cu caracter personal, folosirea unui complex de măsuri preventive (juridice, sociale, economice), parteneriate sociale, colaborarea administrației publice cu organizații internaționale, organizații neguvernamentale sau alți reprezentanți ai societății civile.

Prin urmare, concluzionând, infracțiunea informatică prevăzută în Noul Cod Penal, intrat în vigoare la 1 februarie 2014, art. 361, numită "Interceptarea ilegală a unei transmisii de date informatice" are ca scop protejarea comunicațiilor și datelor transmise, care nu sunt făcute publice, împreună cu ajutorul unui sistem informatic, interceptarea realizată fără drept, utilizarea mijloacelor tehnice, precum și interceptarea fără drept de emisii electromagnetice provenite de la un sistem informatic ce conține date informatice care nu sunt informații publice.

Oricine realizează în mod ilegal, prin orice mijloace electronice, o interceptare a datelor informatice ale unei alte persoane, care sunt transmise într-un sistem informatic și nu consideră un beneficiu publicului sau nu este disponibil pentru alte persoane de a utiliza, este, prin urmare, predispus la a executa anumite pedepse, reglementate în conținutul articolului corespunzător infracțiunii prezente.

BIBLIOGRAFIE

Amza, T., Amza, C. P. (2003) *Criminalitatea informatică*, Ed. Lumina Lex, Bucureşti

Dobrinoiu, M. (2006) *Infracţiuni în domeniul informatic*, Ed. C.H. Beck, Bucureşti

Vasiu, I. (1998) *Criminalitatea informatică*, Ed. Nemira, Bucureşti

https://cybersmartdefence.com/index.csd

https://www.legi-internet.ro

https://www.criminalitatea-informatica.ro

https://legeaz.net/noul-cod-penal/art-361

https://books.google.ro