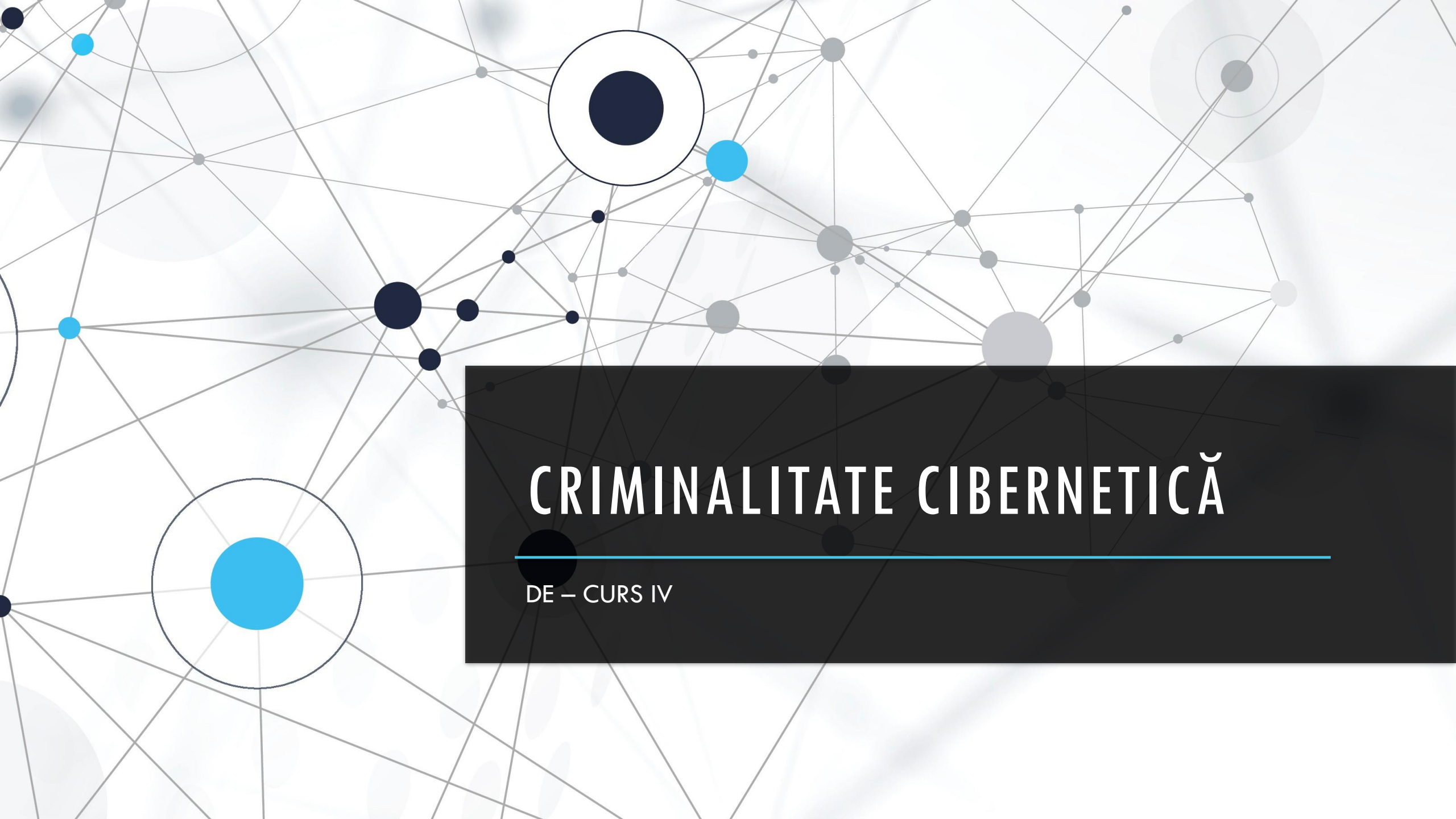




CRIMINALITATE CIBERNETICĂ

DE – CURS IV

CRIMINALITATE CIBERNETICĂ

REGLEMENTAREA CRIMINALITĂȚII INFORMATICE

Conținut

- Conceptul de criminalitate informatică
 - Infracțiuni informatice
 - Regulamente
 - Cadre legislative

REGLEMENTAREA CRIMINALITĂȚII INFORMATICE INCIDENTE

Reglementare în Convenția privind criminalitatea informatică

- Obținerea de informații cu privire la o posibilă țintă (sondare, scanare): ARTICOLUL 6 - Abuzurile asupra dispozitivelor
- Compromiterea sistemului prin executarea de cod neautorizat: ARTICOLUL 4 - Afectarea integrității datelor, ARTICOLUL 5 - Afectarea integrității sistemului
- Refuzul serviciului: ARTICOLUL 5 - Afectarea integrității sistemului
- Compromiterea sistemului (furt, modificare, ștergere): ARTICOLUL 2 - Accesarea ilegală
- Încercare de intruziune: ARTICOLUL 2 - Accesarea ilegală, coroborat cu ARTICOLUL 11 - Tentativa și complicitatea
- Accesul neautorizat la informații: ARTICOLUL 2 - Accesarea ilegală, ARTICOLUL 3 - Interceptarea ilegală
- Accesul neautorizat la transmiterea datelor: ARTICOLUL 3 – Interceptarea ilegală
- Alterarea informațiilor: ARTICOLUL 4 - Afectarea integrității datelor
- Accesul ilegal la sisteme de comunicații: ARTICOLUL 2 - Accesarea ilegală

REGLEMENTAREA CRIMINALITĂȚII INFORMATICE

CONCEPTUL DE CRIMINALITATE INFORMATICĂ

Criminalitatea informatică reprezintă un fenomen al zilelor noastre, reflectat în mod frecvent în mass-media. Un studiu indică chiar că teama de atacuri informatice depășește în intensitate pe cea față de furturi sau fraude obișnuite.

Doar o mică parte din faptele penale legate de utilizarea sistemelor informatice ajung la cunoștința organelor de cercetare penală, astfel încât este foarte greu de realizat o privire de ansamblu asupra amplitudinii și evoluției fenomenului.

Dacă este posibil să se realizeze o descriere adecvată a tipurilor de fapte penale întâlnite, este foarte dificilă prezentarea unei sinteze fundamentate asupra întinderii pierderilor cauzate de acestea, precum și a numărului real de infracțiuni comise.

Numărul cazurilor de infracțiuni informatice este în continuă creștere.

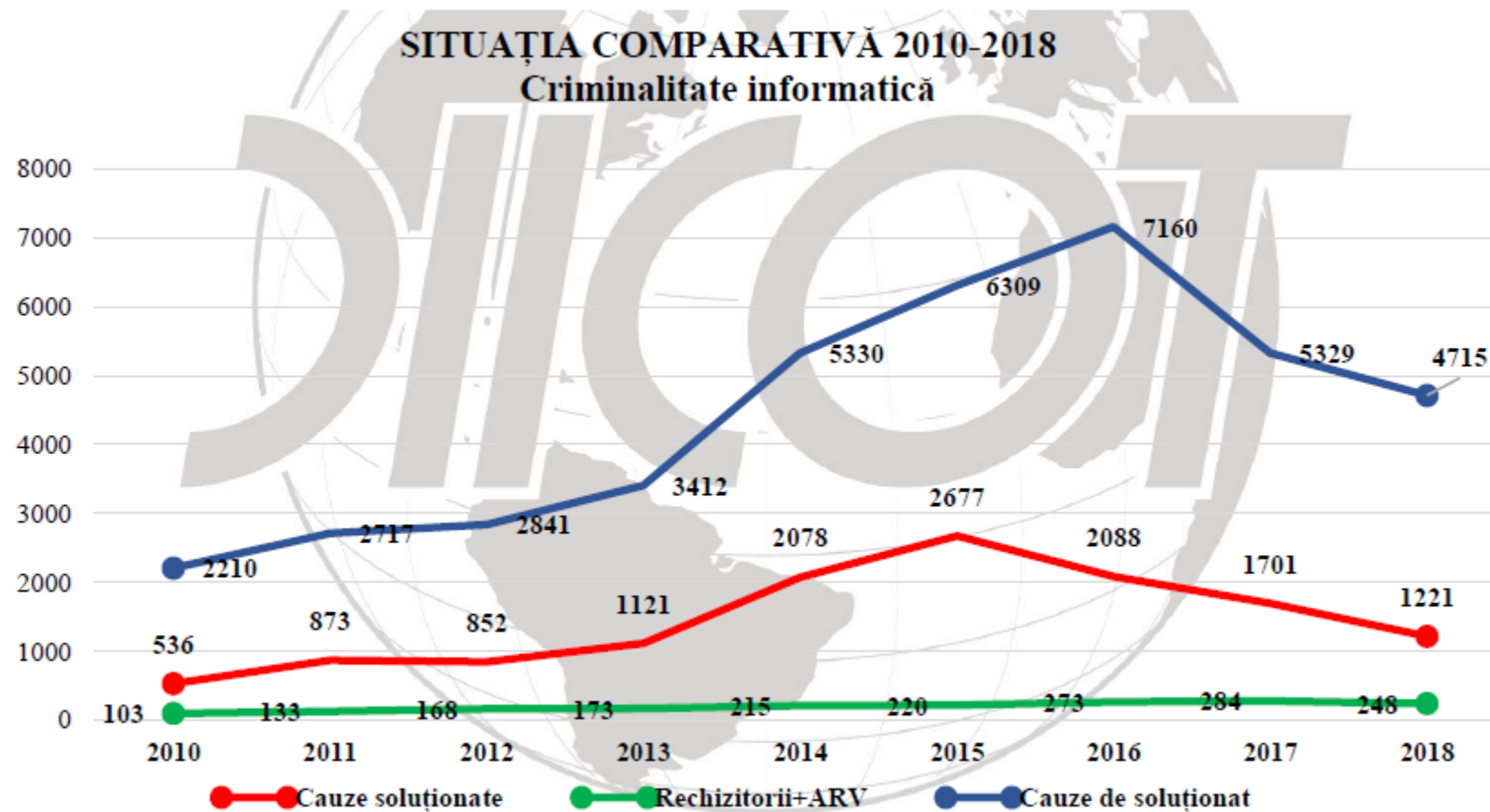
REGLEMENTAREA CRIMINALITĂȚII INFORMATICE

CRIMINALITATEA INFORMATICĂ - RO

RAPORT

DIICOT

2018



REGLEMENTAREA CRIMINALITĂȚII INFORMATICE

CRIMINALITATEA INFORMATICĂ - RO (DIICOT)

În cursul anului 2018, din cele **4.715** cauze de soluționat, din care **1.369** cauze nou înregistrate în perioada de referință, a fost soluționat un număr de **1.221** cauze, față de **1.701** cauze soluționate în 2017, din cele **5.329** cauze de soluționat, din care **1.294** nou înregistrate în 2017. Cifrele arătate indică o scădere cu **11,52%** a cauzelor de soluționat, o creștere cu **5,80%** a cauzelor nou intrate și o scădere cu **28,22%** a cauzelor soluționate.

Dintre acestea, au fost soluționate prin rechizitoriu și acorduri de recunoaștere a vinovăției un număr de **248** cauze (167+81), față de **284** (210+74) în anul 2017 (scădere cu **12,68%**), cu **355** inculpați trimiși în judecată, față de **418** inculpați trimiși în judecată în 2017 (scădere cu **15,07%**), dintre care **61** inculpați arestați preventiv trimiși în judecată, față de **104** inculpați arestați preventiv în anul 2017 (scădere cu **41,35%**).

REGLEMENTAREA CRIMINALITĂȚII INFORMATICE TENDINȚE .

Tendințele de manifestare a formelor de criminalitate informatică în România sunt similare cu cele înregistrate la nivel internațional, raportul IOCTA 2018.

Atacurile **ransomware**, chiar dacă au înregistrat o oarecare stagnare, reprezintă o manifestare importantă a criminalității informatice, în special prin formele auto-propagatoare, **ransomworms** (WannaCry, Arena Dharma). Totodată, se estimează că în următorii ani atacurile de acest tip vor avea un trend ascendent și vor reprezenta o veritabilă amenințare la adresa sectorului public și/sau privat.

Odată cu atacurile cibernetice, tehnicile de inginerie socială au devenit o tactică esențială pentru comiterea fraudelor. Și în cursul anului 2018 amenințările de tip **man-in-the-browser** sau **man-in-the-middle** au fost folosite tot pe scară largă pentru obținerea de beneficii pecuniare importante, acestea vizând deturnarea directă a destinației unor transferuri de bani sau interpunerea în comunicările dintre comercianți și determinarea efectuării unor transferuri de bani către alte conturi bancare.

REGLEMENTAREA CRIMINALITĂȚII INFORMATICE

TENDINȚE ..

Anul 2018 a readus în actualitate atacurile îndreptate împotriva instituțiilor bancare, de tip **malware**, cu ajutorul cărora, prin intermediul fișierelor executabile cu capacități de tip backdoor, fișiere create cu ajutorul platformei Cobalt Strike, s-a reușit infectarea sistemelor informatice și transferarea frauduloasă a unor sume de bani către conturi din România în scopul retragerii acestora de la bancomate sau comercianți din țară sau din străinătate. Preluarea controlului de la distanță a unor stații de lucru denotă o specializare a făptuitorilor și o înaltă calificare în ceea ce privește utilizarea unor aplicații, cum ar fi RDP Wrapper20, precum și o bună coordonare între făptuitori.

Componenta online devine din ce în ce mai obișnuită în ceea ce privește comerțul ilicit, piețele dezvoltate în **Darknet** intersectând și favorizând toate zonele de criminalitate. Principala modalitate de plată folosită pentru operațiunile piețelor dezvoltate în Darknet, **criptomonedă**, (în special Bitcoin, Ethereum, Monero), este din ce în ce mai exploatată de către infractorii cibernetici, fiind folosită în prezent pentru încasarea răscumpărării în cazurile atacurilor de tip ransomware. Totodată, compromiterea unor sisteme informatice **și utilizarea ilicită a puterii de procesare pentru minarea de criptomonede** se înscrie în direcțiile de evoluție a criminalității informatice.

REGLEMENTAREA CRIMINALITĂȚII INFORMATICE

TENDINȚE ...

Numărul grupurilor infracționale specializate în atacuri directe și complexe asupra ATM-urilor sau sistemelor bancare este de asemenea în creștere, iar activitățile infracționale care vizează echipamentele de copiere a datelor inscripționate pe banda magnetică a cardurilor bancare, **deep insert skimming**, rămân în continuare de actualitate.

Deși materiale de exploatare sexuală a copiilor sunt încă produse de către infractori, se înregistrează o creștere a volumului materialelor auto-generate, de cele mai multe ori rezultând din acțiuni de constrângere sau șantaj, tendință similară cu cea din anul precedent. Pe fondul obținerii facile a unor câștiguri importante, se remarcă propagarea aplicațiilor care oferă servicii de tip live-streaming și implicarea minorilor, de vârste tot mai fragede.

An de an se remarcă creșterea specializării în domeniul criminalității informatice (softuri destinate comiterii infracțiunilor asupra sau prin intermediul sistemelor informatice, precum și instrucțiunile necesare folosirii lor fiind disponibile în mediul virtual oricărui utilizator) și apariția tot mai pregnantă a bunurilor de larg consum dotate cu sisteme informatice ori cu inteligență artificială, ceea ce are drept consecință diversificarea modurilor în care infracțiunile informatice pot fi comise.

REGLEMENTAREA CRIMINALITĂȚII INFORMATICE

DEFINIRE TERMENI

Faptele penale de natură informatică:

orice comportament ilegal, neetic sau neautorizat ce privește un tratament automat al datelor și/sau o transmitere de date (grupul de experți OECD 1983)

Prin infracțiune informatică în sens larg se înțelege:

orice infracțiune în care un calculator sau o rețea de calculatoare este obiectul unei infracțiuni, sau în care un calculator sau o rețea de calculatoare este instrumentul sau mediul de înlăptuire a unei infracțiuni. (UNAFEI)

Prin infracțiune informatică în sens restrâns se înțelege:

orice infracțiune în care făptuitorul interferează, fără autorizare, cu procesele de prelucrare automată a datelor.

REGLEMENTAREA CRIMINALITĂȚII INFORMATICE

CATEGORII DE INFRAȚIUNI .

Raportul Comitetului European pentru probleme criminale

- fraudă informatică;
- fals în informatică;
- prejudiciere a datelor sau programelor informatice;
- sabotaj informatic;
- acces neautorizat la un calculator;
- interceptare neautorizată;
- reproducere neautorizată a unui program informatic protejat de lege;
- reproducere neautorizată a unei topografii;
- alterare fără drept a datelor sau programelor informatice;
- spionaj informatic;
- utilizare neautorizată a unui calculator;
- utilizare neautorizată a unui program informatic protejat de lege.

REGLEMENTAREA CRIMINALITĂȚII INFORMATICE

CATEGORII DE INFRAȚIUNI ..

Manualul Națiunilor Unite pentru prevenirea și controlul infracționalității informatice

- fraude prin manipularea calculatoarelor electronice;
- fraude prin falsificarea de documente;
- alterarea sau modificarea datelor sau a programelor pentru calculator;
- accesul neautorizat la sisteme și servicii informatice;
- reproducerea neautorizată a programelor pentru calculator protejate de lege.

REGLEMENTAREA CRIMINALITĂȚII INFORMATICE

CATEGORII DE INFRAȚIUNI ...

Studiul COMCRIM (UE)

- atingeri aduse dreptului la viața privată;
- infracțiuni cu caracter economic:
- penetrarea sistemelor informatice în scopul depășirii dificultăților tehnice de securitate (“hacking”);
- spionajul informatic;
- pirateria programelor pentru calculator;
- sabotajul informatic;
- fraudă informatică;
- distribuirea de informații cu caracter ilegal sau prejudiciabil (propagandă rasistă, difuzare de materiale pornografice, etc.);
- alte infracțiuni:
- infracțiuni contra vieții;
- infracțiuni legate de crima organizată;
- război electronic.

REGLEMENTAREA CRIMINALITĂȚII INFORMATICE

CLASIFICARE INFRAȚIUNI INFORMATICE

Criteriul rolului avut de sistemele informatice în comiterea infracțiunii

- *infracțiuni săvârșite cu ajutorul sistemelor informatice*, în care sistemele informatice constituie un instrument de facilitare a comiterii unor infracțiuni. Este vorba de infracțiuni “tradiționale” perfecționate prin utilizarea sistemelor informatice;
- *infracțiuni săvârșite prin intermediul sistemelor informatice*, în care sistemele informatice, incluzând și datele stocate în acestea, constituie ținta infracțiunii. Aceste infracțiuni pot fi săvârșite doar prin intermediul sistemelor informatice. Ele au făcut obiect de reglementare în ultimii ani.

Amintim aici și un alt rol pe care sistemele informatice îl pot juca în ancheta criminalistică: rolul de mediu de stocare și regăsire a indiciilor sau probelor ce privesc modul de săvârșire a unei infracțiuni.

REGLEMENTAREA CRIMINALITĂȚII INFORMATICE

INFRAȚIUNI SĂVÂRȘITE CU AJUTORUL SISTEMELOR INFORMATICE

Perfecționarea modalităților de înfăptuire a infracțiunilor prin recurgerea la ajutorul dat de sistemele informatice. Infracțiunea nu este îndreptată împotriva funcționării corespunzătoare a unui sistem informatic, sau asupra informațiilor cuprinse în el, ci *rezultatul procesării datelor este utilizat pentru înfăptuirea unor infracțiuni clasice*. Făptuitorii fac astfel apel la mijloace „netradiționale” pentru înfăptuirea unor infracțiuni cu caracter „tradițional”.

Exemple

- Infracțiunea de aducere, fără drept, a operei (creației intelectuale protejate prin legea dreptului de autor) la cunoștință publică, reglementată de art. 140, lit. a din legea nr. 8/1996 privind dreptul de autor și drepturile conexe;
- Infracțiunea de reproducere, fără drept, a unei opere, reglementată de art. 142, lit. a din legea nr. 8/1996 privind dreptul de autor și drepturile conexe;
- Infracțiunea de spălare a banilor, reglementată de art. 268 din Codul Penal;

REGLEMENTAREA CRIMINALITĂȚII INFORMATICE

... EXEMPLE

- Infracțiunea de trădare prin transmitere de informații secrete de stat, reglementată de art. 395 din Codul Penal;
- Infracțiunea de divulgare a secretului care periclitează securitatea națională, reglementată de art. 407 din Codul Penal și art. 12 alin. 2 din legea 51/1991 privind siguranța națională;
- Infracțiunea de divulgare a secretului profesional, reglementată de art. 227 din Codul Penal;
- Infracțiunea de gestiune frauduloasă, reglementată de art. 242 din Codul Penal;
- Infracțiunea de falsificare de monede sau de alte valori, reglementată de art. 310 din Codul Penal;
- Infracțiunea de *falsificare a instrumentelor oficiale*, reglementată de art. 317 din Codul Penal.
- Infracțiunea de *fals material în înscrisuri oficiale*, reglementată de art. 320 din Codul Penal.
- Infracțiunea de *divulgare a informațiilor secrete de serviciu sau nepublice*, reglementată de art. 304 din Codul Penal.
- Infracțiunea de *deturnare de fonduri*, reglementată de art. 307 din Codul Penal.
- Infracțiunea de *propagandă naționalist-șovină*, reglementată de art. 363 din Codul Penal.

REGLEMENTAREA CRIMINALITĂȚII INFORMATICE

INFRAȚIUNI SĂVÂRȘITE PRIN INTERMEDIUL SISTEMELOR INFORMATICE

Legea nr. 21 / 1999, pentru prevenirea și sancționarea spălării banilor a introdus pentru prima oară în legislația română noțiunea de “infrațiuni săvârșite prin intermediul calculatoarelor”. Potrivit textului art. 23, lit. a, *constituie infrațiunea de spălare a banilor [...] schimbarea sau transferul de valori, cunoscând ca acestea provin din săvârșirea unor infrațiuni: [...] infrațiunile săvârșite prin intermediul calculatoarelor, [...] în scopul ascunderii sau disimulării originii ilicite acestora, precum și în scop de tăinuire sau de favorizare a persoanelor implicate în astfel de activități sau presupuse că s-ar sustrage consecințelor juridice ale faptelor lor.*

În momentul de față, legea penală română reglementează un număr de 10 infrațiuni ce corespund definiției de mai sus. Ele sunt prevăzute în Titlul III (Prevenirea și combaterea criminalității informatice) din Legea privind unele măsuri pentru asigurarea transparenței în exercitarea demnităților publice, a funcțiilor publice și în mediul de afaceri, prevenirea și sancționarea corupției (Legea 161 / 2003) precum și în Legea dreptului de autor și a drepturilor conexe (Legea nr. 8 / 1996).

REGLEMENTAREA CRIMINALITĂȚII INFORMATICE

LEGEA CRIMINALITĂȚII INFORMATICE

1. Infracțiuni contra confidențialității și integrității datelor și sistemelor informatice:

- o Infracțiunea de *acces ilegal la un sistem informatic*;
- o Infracțiunea de *interceptare ilegală a unei transmisii de date informatice*;
- o Infracțiunea de *alterare a integrității datelor informatice*;
- o Infracțiunea de *perturbare a funcționării sistemelor informatice*;
- o Infracțiunea de *a realiza operațiuni ilegale cu dispozitive sau programe informatice*.

2. Infracțiuni informatice

- o Infracțiunea de *fals informatic*;
- o Infracțiunea de *fraudă informatică*.

3. Pornografie infantilă prin sisteme informatice

- o Infracțiunea de *pornografie infantilă prin intermediul sistemelor informatice*.

REGLEMENTAREA CRIMINALITĂȚII INFORMATICE

LEGEA DREPTULUI DE AUTOR

Legea dreptului de autor reglementează următoarele infracțiuni:

- Infracțiunea de *permitere a accesului public la bazele de date pe calculator, care conțin sau constituie opere protejate;*
- Infracțiunea de *punere la dispoziția publicului de unor mijloace tehnice de neutralizare a protecției programelor pentru calculator.*

REGLEMENTAREA CRIMINALITĂȚII INFORMATICE

ACCESUL ILEGAL LA UN SISTEM INFORMATIC

Art. 360 din Codul Penal. Textul de lege prevede:

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

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

(3) Dacă fapta prevăzută la alin. (1) sau (2) este săvârșită prin încălcarea măsurilor de securitate, pedeapsa este închisoarea de la 3 la 12 ani.

Sistemul informatic - orice dispozitiv sau ansamblu de dispozitive interconectate sau aflate în relație funcțională, dintre care unul sau mai multe asigură prelucrarea automată a datelor, cu ajutorul unui program informatic. Un *program informatic* - un ansamblu de instrucțiuni care pot fi executate de un sistem informatic în vederea obținerii unui rezultat determinat. Prin *măsuri de securitate* - proceduri, dispozitive sau programe informatice specializate cu ajutorul cărora accesul la un sistem informatic este restricționat sau interzis pentru anumite categorii de utilizatori.

REGLEMENTAREA CRIMINALITĂȚII INFORMATICE

INTERCEPTAREA ILEGALĂ A UNEI TRANSMISII DE DATE INFORMATICE

Infrațiunea de interceptare, fără drept, a unei transmisii de date informatice care nu este publică este prevăzută în art. 361 din Codul Penal. Textul de lege prevede:

(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, constituie infracțiune și se pedepsește cu închisoare de la 2 la 7 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.

Reglementarea legală protejează transmisiile de date informatice din cadrul sau între sisteme informatice, indiferent de modul cum se realizează acestea. *Datele informatice* sunt definite ca fiind orice reprezentare a unor fapte, informații sau concepte într-o formă care poate fi prelucrată printr-un sistem informatic, în aceeași categorie fiind inclus și orice program informatic care poate determina realizarea unei funcții de către un sistem informatic.

REGLEMENTAREA CRIMINALITĂȚII INFORMATICE

ALTERAREA INTEGRITĂȚII DATELOR INFORMATICE

Infracțiunea este reglementată de art. 362 din Codul Penal, textul de lege precizând:

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.

Reglementarea legală urmărește să protejeze datele informatice stocate în cadrul sistemelor informatice, urmărind să împiedice modificarea, ștergerea sau deteriorarea datelor informatice, restricționarea accesului la ele, transferul neautorizat de date dintr-un sistem informatic sau dintr-un mijloc de stocare a datelor informatice

REGLEMENTAREA CRIMINALITĂȚII INFORMATICE

PERTURBAREA FUNCȚIONĂRII SISTEMELOR INFORMATICE

Infracțiunea este reglementată de art. 363 din Codul Penal, textul de lege precizând:

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.

Reglementarea legală urmărește să protejeze datele informatice stocate în cadrul sistemelor informatice. Observăm că spre deosebire de infracțiunea reglementată în articolul 362, accentul este pus aici pe efectul pe care îl au pentru sistemele informatice afectate acțiunile asupra datelor informatice (introducere, transmitere, modificare, ștergere, deteriorare, restricționarea accesului).

REGLEMENTAREA CRIMINALITĂȚII INFORMATICE

TRANSFERUL NEAUTORIZAT DE DATE INFORMATICE

Infracțiunea este reglementată de art. 364 din Codul Penal, textul de lege precizând:

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.

Reglementarea legală urmărește să protejeze datele informatice stocate în cadrul sistemelor informatice, urmărind să împiedice modificarea, ștergerea sau deteriorarea datelor informatice, restricționarea accesului la ele, transferul neautorizat de date dintr-un sistem informatic sau dintr-un mijloc de stocare a datelor informatice.

REGLEMENTAREA CRIMINALITĂȚII INFORMATICE

Operațiuni ilegale cu dispozitive sau programe informatice

Art 365 din Codul Penal. Textul de lege prevede:

(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.

Înscrierea acestei infracțiuni în lege urmărește să limiteze accesul la instrumente (dispozitive, programe informatice, parole, coduri de acces etc.) care permit săvârșirea infracțiunilor reglementate de legea criminalității informatice.

REGLEMENTAREA CRIMINALITĂȚII INFORMATICE

FALSUL INFORMATIC

Art. 325 din Codul Penal

Fapta de a introduce, modifica sau șterge, fără drept, date informatice ori de a restricționa, fără drept, accesul la aceste date, rezultând date necorespunzătoare adevărului, în scopul de a fi utilizate în vederea producerii unei consecințe juridice, constituie infracțiune și se pedepsește cu închisoarea de la unu la 5 ani.

Reglementarea urmărește protejarea securității juridice prin încriminarea tuturor acelor acțiuni care pot, prin modificarea unor date aflate pe suport informatic, să atragă după sine consecințe juridice nedorite de sau pentru persoanele care au conceput, realizat, implementat sau asupra cărora își manifestă efectele informația modificată.

REGLEMENTAREA CRIMINALITĂȚII INFORMATICE

FRAUDA INFORMATICĂ

Art 249 din Codul Penal

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.

REGLEMENTAREA CRIMINALITĂȚII INFORMATICE

.PORNOGRAFIA INFANTILĂ

Art 374 din Codul Penal

(1) Producerea, deținerea în vederea expunerii sau distribuirii, achiziționarea, stocarea, expunerea, promovarea, distribuirea, precum și punerea la dispoziție, în orice mod, de materiale pornografice cu minori se pedepsesc cu închisoarea de la un an la 5 ani.

(2) Dacă faptele prevăzute în alin. (1) au fost săvârșite printr-un sistem informatic sau alt mijloc de stocare a datelor informatice, pedeapsa este închisoarea de la 2 la 7 ani.

(3) Accesarea, fără drept, de materiale pornografice cu minori, prin intermediul sistemelor informatice sau altor mijloace de comunicații electronice, se pedepsește cu închisoare de la 3 luni la 3 ani sau cu amendă.

(4) Prin materiale pornografice cu minori se înțelege orice material care prezintă un minor având un comportament sexual explicit sau care, deși nu prezintă o persoană reală, simulează, în mod credibil, un minor având un astfel de comportament.

(5) Tentativa se pedepsește.

Directiva 2011/93/UE a Parlamentului European și Consiliului din 13 decembrie 2011.

REGLEMENTAREA CRIMINALITĂȚII INFORMATICE

OPERE PROTEJATE

Permiterea accesului public la bazele de date pe calculator ce conțin sau constituie opere protejate

Infrațiunea de permitere, fără drept, a accesului public la bazele de date pe calculator care conțin sau constituie opere protejate este prevăzută în art. 140, lit. c din legea nr. 8/1996, privind dreptul de autor și drepturile conexe. Textul de lege prevede:

Constituie infrațiune și se pedepsește cu închisoare de la o lună la 2 ani sau amendă, dacă nu constituie o infrațiune mai gravă, fapta persoanei care, fără a avea autorizarea sau, după caz, consimțământul titularului drepturilor recunoscute prin prezenta lege:

...

c) permite accesul public la bazele de date pe calculator, care conțin sau constituie opere protejate

Reglementarea legală urmărește să protejeze drepturile autorului unor baze de date pe calculator, baze de date ce constituie în sine opere protejate, sau conțin astfel de opere protejate. Prin *autor*, legea înțelege persoana fizică sau persoanele fizice care au creat opera. Prin *operă protejată*, legea înțelege opera originală de creație intelectuală în domeniul literar, artistic sau științific, oricare ar fi modalitatea de creație, modul sau forma concretă de exprimare și independent de valoarea și destinația acesteia. Legea nu definește noțiunea de bază de date. Prin *bază de date* se înțelege o colecție de date organizată conform unei structuri conceptuale care descrie caracteristicile acestor date și relațiile dintre entitățile lor corespondente, destinată unuia sau mai multor domenii de aplicație.

REGLEMENTAREA CRIMINALITĂȚII INFORMATICE

NEUTRALIZAREA PROTECȚIEI PROGRAMELOR

Infracțiunea de punere la dispoziția publicului în orice mod și cu orice titlu a unor mijloace tehnice de ștergere neautorizată sau de neutralizare a dispozitivelor tehnice de protecție a programelor pentru calculator este reglementată de art. 143, lit. a din legea nr. 8/1996 privind dreptul de autor și drepturile conexe. Textul legal prevede:

Constituie infracțiune și se pedepsește cu închisoare de la 3 luni la 2 ani sau cu amendă, dacă nu constituie o infracțiune mai gravă, fapta persoanei care:

a) pune la dispoziția publicului prin vânzare sau prin orice alt mod de transmitere cu titlu oneros ori cu titlu gratuit mijloace tehnice destinate ștergerii neautorizate sau neutralizării dispozitivelor tehnice care protejează programul pentru calculator.

Înscrierea acestei infracțiuni în lege urmărește să apere dreptul titularului dreptului de autor asupra unui program pentru calculator de a proteja programul împotriva oricărui acces neautorizat la funcțiile acestuia, ori la datele obținute sau oferite de calculator în urma utilizării lor.