Consiliul
Uniunii Europene

Bruxelles, 8 martie 2016
(OR. en)

13022/1/15
REV 1 DCL 1

GENVAL 46
CYBER 99

DECLASIFICARE

a documentului:	13022/1/15 REV 1 RSTREINT UE/EU RESTRICTED
din data:	18 ianuarie 2016
Noul statut:	Public
Subiect:	Raport de evaluare privind cea de a şaptea rundă de evaluări reciproce „Punerea în aplicare la nivel practic şi funcţionarea politicilor europene de prevenire şi de combatere a criminalităţii informatice” - Raport privind România

În anexă, se pune la dispoziția delegațiilor versiunea declasificată a documentului sus-menționat.

Conținutul acestui document este identic cu cel al versiunii precedente.

Consiliul
Uniunii Europene

Bruxelles, 18 ianuarie 2016
(OR. en)

13022/1/15
REV 1

RESTREINT UE/EU RESTRICTED

GENVAL 46
CYBER 99

RAPORT

Sursă:	Secretariatul General al Consiliului
Destinatar:	Delegațiile
Subiect:	Raport de evaluare privind cea de a şaptea rundă de evaluări reciproce „Punerea în aplicare la nivel practic şi funcţionarea politicilor europene de prevenire şi de combatere a criminalităţii informatice” - Raport privind România

ANEXĂ

RAPORT DE EVALUARE PRIVIND

CEA DE A ŞAPTEA RUNDĂ DE EVALUĂRI RECIPROCE

„Punerea în aplicare la nivel practic şi funcţionarea politicilor europene de prevenire şi de combatere a criminalităţii informatice”

RAPORT PRIVIND ROMÂNIA

Cuprins

Rezumat

Misiunea în România a fost foarte bine organizată, inclusiv la nivel logistic. Autorităţile române întâlnite au fost foarte bine pregătite şi vizita a decurs într-o atmosferă foarte plăcută şi primitoare. Programul a fost intens şi cuprinzător. Echipa de evaluare a avut posibilitatea de a discuta cu reprezentanţi ai diverselor autorităţi implicate în prevenirea şi combaterea criminalităţii informatice, inclusiv cu funcţionari din cadrul Ministerului Afacerilor Interne, Ministerului Justiţiei, Ministerului Educaţiei, Institutului Naţional al Magistraturii, Poliţiei Naţionale, Ministerului Public, CERT-RO, etc. Toate autorităţile întâlnite au fost bucuroase să schimbe opinii într-un mod informal cu echipa de evaluare. Toate autorităţile manifestă un grad înalt de angajament faţă de prevenirea şi combaterea criminalităţii informatice.

Abordarea criminalităţii informatice de către România este împământenită şi multidisciplinară. România este angajată, atât la nivel naţional, cât şi la nivel internaţional, în prevenirea şi combaterea criminalităţii informatice. România este deosebit de interesată de prevenirea criminalităţii informatice şi, de asemenea, de asigurarea respectării legii. Autorităţile naţionale întâlnite sunt decise să facă din România o ţară model din punctul de vedere al combaterii criminalităţii informatice. Serviciul de informaţii, CERT-RO, poliţia, Ministerul Public şi magistratura cooperează între ele. În cadrul vizitei a reieşit clar că autorităţile poliţieneşti şi de urmărire penală conlucrează îndeaproape, cel puţin în ceea ce priveşte combaterea criminalităţii informatice, şi se pot baza pe o practică încetăţenită şi pe încredere reciprocă. Serviciul de informaţii şi CERT-RO sunt, de asemenea, foarte implicate în combaterea incidentelor cibernetice şi a criminalităţii informatice. Toate aceste autorităţi au părut perfect conştiente de rolul şi competenţa lor şi foarte familiarizate cu rolul lor. Acestor autorităţi le este întotdeauna clar (de exemplu, CERT-RO şi serviciului de informaţii) când să contacteze autorităţile poliţieneşti în cazurile în care o alertă care ar afecta securitatea cibernetică s-ar putea transforma în comportament infracţional. Coordonarea generală a diferitelor autorităţi implicate în securitatea cibernetică este efectuată de Consiliul Operativ de Securitate Cibernetică. Totuşi, nu a fost clar pentru echipa de evaluare cine are cu adevărat rolul de coordonator general.

O abordare mai coordonată a statisticilor ar fi, de asemenea, benefică pentru alinierea statisticilor poliţiei şi procurorilor pentru a avea statistici de încredere referitoare la rezultatul fiecărui caz în parte.

Începând cu anul 2000, România a fost în prima linie în combaterea criminalităţii informatice. La nivel naţional, au fost create unităţi specializate încă din 2003 în cadrul poliţiei şi totodată al Parchetului General, dedicate cercetării şi urmăririi penale a criminalităţii informatice. La nivel internaţional, România este angajată pe multe fronturi: participând în calitate de partener şi furnizând expertiză în cadrul proiectelor UE şi ale Consiliului Europei, a impulsionat lucrările EMPACT în 2012-2013, participă la toate cele trei domenii ale criminalităţii informatice din cadrul EMPACT şi în cadrul Comitetului Convenţiei privind criminalitatea informatică (T-CY) privind accesul transfrontalier la date şi este, de asemenea, membru al Grupului privind dovezile în cloud înfiinţat în decembrie 2014. Din iunie 2014, România este, de asemenea, vice-preşedinte al T-CY. În plus, România găzduieşte Oficiul Consiliului Europei la Bucureşti (C-PROC) care are rolul de a asista statele din întreaga lume în consolidarea capacităţii justiţiei de a răspunde provocărilor cauzate de criminalitatea informatică şi de probele electronice, având la bază standardele Convenţiei de la Budapesta privind criminalitatea informatică.

Combaterea criminalităţii informatice în România face parte dintr-o abordare mai generală a protecţiei şi garantării securităţii cibernetice. În România există un cadru juridic coerent, atât la nivel material, cât şi procedural. Punerea în aplicare a Directivei 2013/40/UE privind atacurile împotriva sistemelor informatice ar trebui să îmbunătăţească în continuare dreptul român în acest domeniu. Directiva 2011/93/UE a Parlamentului European şi a Consiliului privind combaterea abuzului sexual asupra copiilor, a exploatării sexuale a copiilor şi a pornografiei infantile a fost pusă în aplicare în mare măsură. Echipei de evaluare i-au fost prezentate, de asemenea, informaţii dintr-o propunere legislativă care vizează, printre altele, asigurarea unui flux de informaţii mai coerent şi mai de încredere din sectorul privat. Cu toate acestea, în cursul vizitei de evaluare, Curtea Constituţională a declarat neconstituţională legea de punere în aplicare a Strategiei de securitate cibernetică.

Cooperarea cu sectorul privat are loc *ad hoc*. S-a explicat, de asemenea, că au loc reuniuni cu poliţia şi procurori pentru a instrui sectorul privat cu privire la colectarea informaţiilor într-un mod care să permită utilizarea acestora ca dovezi în instanţă. Poliţia şi sectorul privat cooperează, de asemenea, destul de mult cu privire la formare (privind, de exemplu, mecanismele de raportare). Cooperarea cu furnizorii de servicii internet a avut loc prin intermediul asociaţiei române a internet service providerilor, poliţia discutând şi informând cu privire la cazuri posibile, *modus operandi* etc.

Foarte frecvent, a fost ridicată chestiunea păstrării datelor (data retention), precum şi urmările hotărârii Curţii de Justiţie a Uniunii Europene din 8 aprilie 2014 de declarare a Directivei 2006/24/CE ca fiind invalidă. Ca urmare a respectivei hotărâri, Curtea Constituţională a României a declarat neconstituţională şi Legea 82/2012 de transpunere a directivei. Datorită faptului că legi referitoare la păstrarea datelor au fost, de asemenea, anulate sau declarate neconstituţionale în alte state membre, autorităţile române şi-au manifestat îngrijorarea cu privire la impactul negativ al lipsei unui instrument de reglementare care să creeze obligaţia sectorului privat de a păstra date. O astfel de lacună are un impact negativ asupra cercetărilor şi urmăririlor penale ale cazurilor de criminalitate informatică în care datele nu sunt păstrate deloc sau sunt păstrate într-un grad prea restrâns care nu permite utilizarea loc ca informaţii operative şi în niciun caz ca dovezi.

În marja foarte strânsei colaborări dintre poliţie şi Ministerul Public, judecătorii se organizează, de asemenea, pentru a-şi mări gradul de cunoaştere şi disponibilitate pentru cazurile de criminalitate informatică. Pentru poliţişti, procurori şi judecători s-au organizat şi se organizează în continuare cursuri de formare în domeniul criminalităţii informatice. România a demarat un proiect numit CYBER-EX care vizează înfiinţarea unui centru de expertiză privind criminalitatea informatică la nivel naţional care include poliţişti, procurori şi judecători. Europol/EC3 şi Eurojust sunt binecunoscute şi li se solicită asistenţa.

Ţinând seama de abordarea ambiţioasă a României şi de rolul activ pe care România îl joacă în ceea ce priveşte combaterea criminalităţii informatice şi de resursele semnificative pe care ţara le-a alocat în acest scop, avizul evaluatorilor este indiscutabil pozitiv.

1 INTRODUCERE

Ca urmare a adoptării Acţiunii comune 97/827/JAI din 5 decembrie 1997[1], a fost înfiinţat un mecanism de evaluare a aplicării şi a punerii în aplicare pe plan naţional a angajamentelor internaţionale în domeniul luptei împotriva criminalităţii organizate. În conformitate cu articolul 2 din acţiunea comună, la 3 octombrie 2013 Grupul de lucru pentru chestiuni generale, inclusiv evaluare (GENVAL) a decis ca cea de a şaptea rundă de evaluări reciproce să fie dedicată punerii în aplicare la nivel practic şi funcţionării politicilor europene de prevenire şi de combatere a criminalităţii informatice.

Alegerea criminalității informatice drept tema celei de a şaptea runde de evaluare reciprocă a fost salutată de statele membre. Cu toate acestea, întrucât termenul „criminalitate informatică” acoperă o gamă largă de infracțiuni, s-a convenit ca evaluarea să se axeze asupra infracțiunilor considerate de statele membre ca necesitând o atenție deosebită. În acest scop, evaluarea acoperă trei domenii specifice – atacurile cibernetice, abuzul sexual asupra copiilor/pornografia infantilă online şi frauda cu carduri online – şi ar trebui să furnizeze o examinare cuprinzătoare a aspectelor juridice şi operaţionale ale abordării criminalităţii informatice, ale cooperării transfrontaliere şi ale cooperării cu agenţiile UE relevante. Directiva 2011/93/UE privind combaterea abuzului sexual asupra copiilor, a exploatării sexuale a copiilor şi a pornografiei infantile şi de înlocuire a Deciziei-cadru 2004/68/JAI a Consiliului[2] (termenul de transpunere - 18 decembrie 2013) şi Directiva 2013/40/UE[3] privind atacurile împotriva sistemelor informatice şi de înlocuire a Deciziei-cadru 2005/222/JAI a Consiliului (termenul de transpunere - 4 septembrie 2015) sunt deosebit de relevante în acest context.

1 Acţiunea comună din 5 decembrie 1997 (97/827/JAI), JO L 344, 15.12.1997, p. 7-9.
2 JO L 335, 17.12.2011, p. 1.
3 JO L 218, 14.8.2013, p. 8.

În plus, Concluziile Consiliului privind strategia de securitate cibernetică din iunie 2013 a UE[4] au anticipat ratificarea rapidă a Convenției Consiliului Europei privind criminalitatea informatică (Convenția de la Budapesta)[5] din 23 noiembrie 2001 de către toate statele membre şi evidențiază în preambulul acestora faptul că „UE nu face apel la crearea de noi instrumente juridice internaționale pentru aspectele cibernetice". Convenția este completată de un Protocol privind actele de natură rasistă și xenofobă săvârșite prin intermediul sistemelor informatice[6].

Experienţa evaluărilor trecute arată că statele membre vor fi în poziţii diferite în ceea ce priveşte punerea în aplicare a instrumentelor juridice relevante, iar procesul de evaluare actual ar putea furniza, de asemenea, informaţii utile statelor membre care este posibil să nu fi implementat toate aspectele diferitelor instrumente. Totuşi, evaluarea se doreşte largă şi interdisciplinară şi nu îşi propune să se axeze doar asupra punerii în aplicare a diferitelor instrumente referitoare la combaterea criminalității informatice, ci şi asupra aspectelor operaţionale din statele membre.

Prin urmare, pe lângă cooperarea cu parchetele, aceasta va include şi modul în care autorităţile poliţieneşti cooperează cu Eurojust, ENISA şi Europol/EC3 şi modul în care este canalizat feedback-ul de la aceste organizaţii către serviciile poliţieneşti şi sociale adecvate. Evaluarea se axează asupra punerii în aplicare a politicilor naţionale cu privire la suprimarea atacurilor cibernetice, fraudei şi pornografiei infantile. Evaluarea acoperă, de asemenea, practici operaţionale din statele membre cu privire la cooperarea internaţională şi sprijinul acordat persoanelor care cad victime criminalităţii informatice.

Ordinea vizitelor în statele membre a fost adoptată de GENVAL la 1 aprilie 2014. România este al patrulea stat membru evaluat în cursul acestei runde de evaluări. În conformitate cu articolul 3 din acţiunea comună, Preşedinţia a elaborat o listă de experţi în evaluările de efectuat. Statele membre au numit experţi cu cunoştinţe practice aprofundate în domeniu, în urma unei cereri scrise adresate delegaţiilor de către preşedintele GENVAL la 28 ianuarie 2014.

[4] 12109/13 POLGEN 138 JAI 612 TELECOM 194 PROCIV 88 CSC 69 CIS 14 RELEX 633 JAIEX 55 RECH 338 COMPET 554 IND 204 COTER 85 ENFOPOL 232 DROIPEN 87 CYBER-15 COPS 276 POLMIL 39 COSI 93 DATAPROTECT 94.

[5] STCE nr. 185, deschisă spre semnare la 23 noiembrie 2001, intrată în vigoare la 1 iulie 2004.

[6] STCE nr. 189, deschisă spre semnare la 28 ianuarie 2003, intrată în vigoare la 1 martie 2006.

Echipele de evaluare constau în trei experţi naţionali, sprijiniţi de doi funcţionari ai Secretariatului General al Consiliului şi de observatori. Pentru cea de a şaptea rundă de evaluări, GENVAL a convenit asupra propunerii Preşedinţiei conform căreia Comisia Europeană, Eurojust, ENISA şi Europol/EC3 ar trebui invitate în calitate de observatori.

Experţii însărcinaţi cu efectuarea evaluării României au fost dl Philippe Devred (Franţa) şi dna Lisanne van Dijk (Ţările de Jos). Au fost, de asemenea, prezenţi, următorii observatori: dl Michele Socco (Comisie), dna Anna Danieli (Eurojust) şi dl Jaroslav Jakubcek (Europol/EC3), împreună cu dl. Francisco Rodriguez Rosales şi dl Sławomir Buczma din partea Secretariatului General al Consiliului.

Prezentul raport a fost elaborat de echipa de experţi cu asistenţa Secretariatului General al Consiliului, pe baza elementelor care au reieşit în urma vizitei de evaluare, care a avut loc în România între 19 şi 23 ianuarie 2015, şi pe baza răspunsurilor detaliate din partea autorităţilor române la chestionarul de evaluare, precum şi a răspunsurilor detaliate ale acestora la întrebările ulterioare.

2 CHESTIUNI GENERALE ŞI STRUCTURI

2.1 Strategia naţională de securitate cibernetică

Strategia de securitate cibernetică şi Planul de acţiune la nivel naţional privind implementarea Sistemului naţional de securitate cibernetică (SNSC) au fost adoptate în România prin Hotărârea Guvernului nr. 271 (Monitorul Oficial nr. 296 din 23 mai 2013). SNSC reprezintă cadrul general de cooperare care reuneşte instituţii şi autorităţi publice cu responsabilităţi şi capabilităţi în domeniu, în vederea coordonării acţiunilor la nivel naţional pentru asigurarea securităţii spaţiului cibernetic, inclusiv prin cooperarea cu mediul academic şi cel de afaceri, asociaţiile profesionale şi organizaţiile neguvernamentale. Misiunea SNSC constă în asigurarea elementelor de cunoaştere, prevenire şi contracarare a ameninţărilor, vulnerabilităţilor şi riscurilor specifice spaţiului cibernetic care pot afecta securitatea infrastructurilor cibernetice naţionale, inclusiv managementul consecinţelor.

SNSC prezintă atât obiective pe termen scurt, cât şi obiective pe termen lung, afirmând că ţara depinde de funcţionarea reţelelor multiple care structurează vieţile şi economia cetăţenilor săi. Strategia subliniază, de asemenea, faptul că este necesară creşterea constantă a nivelurilor de securitate ale infrastructurii digitale din cauza numărului în creştere şi a complexităţii atacurilor cibernetice. Că răspuns la această situaţie, România urmăreşte să reducă riscurile şi să îmbunătăţească cunoştinţele, capabilităţile şi mecanismele de decizie. În această privinţă, eforturile se vor concentra, printre altele, asupra următoarelor acţiuni: constituirea şi operaţionalizarea unui sistem naţional de securitate cibernetică; completarea şi armonizarea cadrului legislativ naţional în domeniu, inclusiv stabilirea şi aplicarea unor cerinţe minimale de securitate pentru infrastructurile cibernetice naţionale; dezvoltarea cooperării dintre sectorul public şi cel privat, inclusiv prin stimularea schimbului de informaţii privind ameninţări, vulnerabilităţi, riscuri referitoare la incidente şi atacuri cibernetice; dezvoltarea capacităţilor naţionale de management al riscului în domeniul securităţii cibernetice şi de reacţie la incidente cibernetice în baza unui program naţional, inclusiv

crearea unui mecanism eficient de avertizare şi alertă la incidentele cibernetice; creşterea nivelului de rezilienţă a infrastructurilor cibernetice; dezvoltarea entităţilor de tipul Centrului Naţional de Răspuns la Incidente de Securitate Cibernetică (CERT), atât în cadrul sectorului public, cât şi în sectorul privat; derularea unor programe de sensibilizare a populaţiei şi dezvoltarea de programe educaţionale obligatorii privind utilizarea sigură a internetului; asigurarea formării profesionale adecvate a practicienilor care îşi desfăşoară activitatea în domeniul securităţii cibernetice în sectorul public şi privat şi dezvoltarea cooperării naţionale în domeniul securităţii cibernetice, inclusiv participarea la programe internaţionale care vizează domeniul securităţii cibernetice.

2.2 Priorităţi naţionale referitoare la criminalitatea informatică

România a definit priorităţile naţionale în ceea ce priveşte criminalitatea informatică: prevenirea, capacitatea instituţională, formarea, cooperarea internaţională, armonizarea legislaţiei şi consolidarea cooperării cu sectorul privat.

Prevenirea

În domeniul prevenirii, structurile de aplicare a legii organizează evenimente diferite care vizează în principal sectorul privat, precum şi cetăţenii (tineri) pentru a creşte gradul de conştientizare cu privire la pericolele şi riscurile puse de acest fenomen. De exemplu, au fost întreprinse următoarele acţiuni:

- activităţi în cadrul Zilei Siguranţei pe Internet şi al Lunii Securităţii Cibernetice, de exemplu conferinţe, reuniuni, grupuri de lucru la care participă sectorul public şi privat;
- proiectul SAFERNET, care vizează pornografia infantilă, urmărind să asigure un mod sigur şi rapid de raportare a activităţilor de pornografie infantilă desfăşurate pe internet. Proiectul a fost desfăşurat de Poliţia Română în colaborare cu ONG-uri.

Capacitatea instituţională

Din 2003, în cadrul Parchetului General şi al Poliţiei Române au fost create unităţi specializate pentru a efectua cercetări în domeniul criminalităţii informatice. Unităţile create în cadrul Poliţiei Române au evoluat în ceea ce priveşte responsabilităţile, numărul poliţiştilor, competenţele la nivel teritorial, resursele şi formarea personalului.

Formarea

Formarea poliţiştilor la nivel central este planificată şi asigurată anual şi include arii principale de interes. Conceptul de „cursuri comune de formare" pentru poliţişti, procurori şi judecători este folosit în diferitele evenimente care sunt organizate. Institutul Naţional al Magistraturii oferă formare judecătorilor şi procurorilor în domeniul securităţii cibernetice.

Cooperarea internaţională

Cooperarea internaţională este o prioritate atât la nivel operaţional, cu privire la cercetările în curs, cât şi la nivel strategic, pentru a obţine armonizarea între priorităţile naţionale şi standardele europene şi internaţionale. Cooperarea operaţională are loc, în principal, prin intermediul poliţiei şi al Ministerului Public specializat (DIICOT - Direcţia de Investigare a Infracţiunilor de Criminalitate Organizată şi Terorism), ţinând seama de schimbul de date şi de informaţii necesare pentru soluţionarea oricărui caz. Sunt utilizate instrumente europene şi internaţionale relevante, precum şi canalele relevante (Europol, Eurojust, Interpol, puncte de contact 24/7 etc.). România a participat în mod constant la iniţiative, proiecte şi grupuri de lucru europene şi internaţionale înfiinţate la nivelul Uniunii Europene, al Consiliului Europei şi al altor organizaţii; de exemplu:

- România a participat ca partener şi/sau a contribuit cu expertiză în proiecte comune ale UE şi ale Consiliului Europei (CyberCrime@IPA, CyberCrime@EAP, Project on Cybercrime in Georgia and Global Action against Cybercrime - Proiectul privind criminalitatea informatică în Georgia şi Acţiunea mondială împotriva criminalităţii informatice - GLACY).
- În perioada 2012-2013, România a participat în calitate de iniţiator la prioritatea privind criminalitatea informatică a proiectelor EMPACT şi în perioada 2014-2017 România participă la toate cele trei priorităţi privind criminalitatea informatică din cadrul proiectelor EMPACT (atacuri cibernetice, cărţi de credit şi sisteme care au la bază IT). În cadrul acestor proiecte, România are rolul de iniţiator în proiectul referitor la frauda cu cardurile de credit şi este coiniţiator în cadrul proiectului referitor la atacurile cibernetice.
- În cadrul Consiliului Europei, România a participat la lucrările Comitetului Convenţiei privind criminalitatea informatică (T-CY)[7] privind accesul transfrontalier la date şi este în prezent membră a Grupului privind dovezile în cloud înfiinţat în decembrie 2014.

[7] http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/t-cy/transborder%20access/tcy_transborder_EN.asp?

Legislaţie

În ultimii ani, Ministerul Justiţiei din România a întreprins un proces cuprinzător de reformă legislativă în vederea modificării ambelor coduri privind aspectele penale şi a revizuirii întregii legislaţii în materie penală; aceasta a avut ca rezultat adoptarea a două coduri noi şi a legilor de punere în aplicare a acestora[8]. În 2014 aceste legi au intrat în vigoare. În domeniul criminalităţii informatice, noile coduri pun în aplicare standarde internaţionale, în special pe cele ale Convenției Consiliului Europei privind criminalitatea informatică. În prezent, Ministerul Justiţiei analizează transpunerea Directivei 2013/40/UE a Parlamentului European şi a Consiliului privind atacurile împotriva sistemelor informatice, de înlocuire a Deciziei-cadru 2005/222/JAI (directiva). Prin punerea în aplicare a Convenției Consiliului Europei privind criminalitatea informatică, România a reuşit, în mare măsură, să transpună directiva.

Decizia Curţii de Justiţie a Uniunii Europene din 8 aprilie 2014, care a declarat Directiva 2006/24/CE a Parlamentului European şi a Consiliului din 15 martie 2006 privind păstrarea datelor generate sau prelucrate în legătură cu furnizarea serviciilor de comunicaţii electronice accesibile publicului sau de reţele de comunicaţii publice şi de modificare a Directivei 2002/58/CE[9] invalidă[10], a avut efecte asupra dispoziţiilor esenţiale ale Legii nr. 82/2012 de transpunere a directivei în dreptul român. Drept rezultat, Curtea Constituțională a României a admis excepția de neconstituționalitate privind Legea nr. 82/2012 și a decis că dispozițiile acesteia sunt neconstituționale (Decizia nr. 440 din 8 iulie 2014). În urma discuţiilor care au avut loc în cadrul unui grup de lucru inter-instituțional, se consideră necesară modificarea Codului de procedură penală şi a altor legi, de exemplu Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul comunicaţiilor electronice.

8 Legea nr. 286/2009 privind Codul penal, Legea nr. 135/2010 privind noul Cod de procedură penală, Legea nr. 187/2012 pentru punerea în aplicare a noului Cod penal, Legea nr. 255/2013 pentru punerea în aplicare a Legii nr. 135/2010.

9 JO L 105, 13.4.2006, p. 54.

10 Hotărâre în cauzele conexate C-293/12 şi C-594/12.

2.3 Statistici privind criminalitatea informatică

Autorităţile române au subliniat faptul că fiecare instituţie publică implicată în combaterea criminalităţii informatice păstrează statistici în funcţie de priorităţile care au nevoie de evidenţiere şi de activităţile relevante.

Poliţia păstrează statistici privind criminalitatea informatică într-o structură specializată, pe baza datelor furnizate de structuri operaţionale cu responsabilităţi în domeniul criminalităţii informatice. Aceste statistici sunt colectate lunar şi sunt evidenţiate în rapoarte de analiză şi evaluare. Statisticile poliţiei evidenţiază cazurile înregistrate (notificări şi descoperiri), dar şi cazurile soluţionate. Sunt identificate nu numai tipurile de infracţiuni, dar şi categoriile de infracţiuni, precum frauda comisă prin mijloace de plată electronică împotriva sistemelor informatice şi pornografia infantilă prin sisteme informatice. Următorii indicatori statistici au fost înregistraţi în ultimii doi ani:

- 2012: numărul cazurilor penale înregistrate - 2970, numărul punerilor sub acuzare - 209, numărul infracţiunilor cercetate - 1615, numărul persoanelor acuzate - 796, numărul persoanelor arestate - 512;
- 2013: numărul cazurilor penale înregistrate - 2944, numărul punerilor sub acuzare - 208, numărul infracţiunilor cercetate - 1574, numărul persoanelor acuzate - 627, numărul persoanelor arestate - 273.

Aceste statistici nu pot fi eşalonate în funcţie de tipul de infracţiune (de exemplu: acces neautorizat la sistemele informatice etc.), din cauza sistemelor utilizate pentru evidenţierea statisticilor.

În 2013, au fost raportate 3 032 de infracţiuni legate de mediul informatic la nivelul Poliţiei Române, reprezentând 0,46% din totalul de 659 832 de infracţiuni raportate. Statisticile colectate în primele zece luni ale anului 2014 arată 2 451 de infracţiuni legate de mediul informatic raportate la nivelul Poliţiei Naţionale Române dintr-un total de 548 449 de infracţiuni raportate (0,44%).

Statisticile Direcţiei de Investigare a Infracţiunilor de Criminalitate Organizată şi Terorism (DIICOT) reflectă numărul cazurilor înregistrate în cadrul unităţii, nu numărul infracţiunilor săvârşite de fiecare persoană cercetată. Statisticile nu disting între cazurile care privesc infracțiuni informatice *stricto sensu* şi infracţiuni informatice în sens larg; astfel, acestea includ infracţiuni referitoare la falsificarea instrumentelor de plată electronică, skimming (copierea conţinutului benzilor magnetice ale cărţilor de credit) sau utilizarea instrumentelor de plată electronică falsificate, inclusiv mediul online, precum şi frauda informatică. O analiză concretă a cazurilor soluţionate confirmă o tendinţă în creştere în statisticile pe 2013 (date standard pentru toate parchetele), luând act de faptul că numărul cazurilor în aşteptarea soluţionării din anii anteriori este în continuare în creştere (1 784 de dosare penale în 2013 în comparație cu 1 602 dosare penale în 2012), dat fiind numărul în creştere al noilor dosare penale (1 836 de dosare penale în 2013 comparativ cu 1 521 de dosare penale în 2012).

Din punct de vedere statistic, există o creştere a cazurilor soluţionate (1 121 de dosare penale în 2013, comparativ cu 852 de dosare în 2012), precum și un număr în creştere al punerilor sub acuzare (173 de puneri sub acuzare în 2013, comparativ cu 168 de puneri sub acuzare în 2012) şi al numărului persoanelor judecate (351 de persoane acuzate în 2012, comparativ cu 373 de persoane acuzate în 2013).

La nivelul Ministerului Justiţiei, statisticile colectate în bazele de date gestionate de Ministerul Justiţiei sunt analizate global. Nu există registre separate pentru articolele care incriminează diferite infracţiuni. Statisticile disponibile în modulul de statistici al bazei de date ECRIS sunt colectate la nivelul fiecărei instanţe în România. Respectivele date sunt periodic copiate pe serverele ministerului şi în procesul de colectare şi copiere a datelor nu sunt implicate alte organisme/agenţii[11].

[11] Autoritățile române au raportat că, deși situația actuală nu include într-adevăr posibilitatea de a separa registrele pentru diferite comportamente și circumstanțe oferită de un text juridic, această problemă va fi rezolvată în viitorul apropiat, întrucât s-au luat deja măsuri pentru introducerea tuturor circumstanțelor și comportamentelor descrise într-un text juridic oferit de Codul penal. Aceste măsuri vor fi în curând testate și, într-o etapă ulterioară, puse în aplicare de către fiecare instanță.

3.4 Bugetul naţional alocat prevenirii şi combaterii criminalităţii informatice şi sprijinul prin finanţarea din partea UE

Poliţia Română are un buget separat pentru îndeplinirea unor activităţi specifice în domeniul prevenirii şi combaterii criminalităţii, fără a exista secţiuni separate pentru domenii specifice de criminalitate. Conform dispoziţiilor Direcţiei financiare a IGPR, bugetul alocat pentru formarea personalului poliţiei în şcoli subordonate şi pentru finanţarea Poliţiei Române nu poate fi separat de bugetul total anual al instituţiilor vizate. În scopul formării practicienilor implicaţi în combaterea criminalităţii informatice, Institutul Naţional al Magistraturii a alocat aproximativ 3 500 EUR din bugetul propriu pentru a forma judecători în domeniul criminalităţii informatice în 2014.

România a declarat că finanţare din partea UE a fost implicată în finalizarea câtorva proiecte în domeniul criminalităţii informatice. De exemplu, au fost menţionate următoarele iniţiative:

- proiectul de înfiinţare a Centrului de Excelenţă CYBER-EX care caută să integreze cunoştinţe şi expertiză din mediul privat, mediul academic şi autorităţile de aplicare a legii;
- două proiecte privind criminalitatea informatică au fost aprobate în cadrul proiectelor finanţate de tip ISF (Fondurile pentru securitate internă) şi au fost transmise Comisiei Europene. Obiectivul acestora este dezvoltarea capacităţii instituţionale, garantarea instrumentelor de cercetare şi desfăşurarea programelor de formare.

În plus, Departamentul de informaţii şi protecţie internă (DIPI) a pus în aplicare proiectul „Implementarea unui sistem de apărare cibernetică la nivelul Ministerului Afacerilor Interne prin Departamentul de Informaţii şi Protecţie Internă, cod SMIS 32566” cu fonduri europene, care a dus la înfiinţarea unui cadru unitar pentru monitorizarea în timp real a evenimentelor de securitate, legat de o capacitate de intervenţie rapidă pentru a micşora impactul.

Proiectul privind „Sistemul naţional de combatere a criminalităţii informatice «Cyber Crime»” a fost implementat de CERT-RO[12]. Proiectul a fost finanţat de Fondul social european prin Programul operaţional „Dezvoltarea capacităţii administrative”. Obiectivul proiectului a fost acela de a crea un cadru adecvat pentru creşterea capacităţii de a formula politici publice şi de a obţine o mai bună reglementare şi planificare strategică prin consolidarea parteneriatelor dintre instituţii şi dintre instituţii publice şi reprezentanţi ai domeniilor interesate de combaterea criminalităţii informatice. Ca parte a proiectului, a fost înfiinţată o echipă română tehnică „Cybercrime”. În acelaşi timp, experţi din domeniul tehnic, al dreptului şi al politicii publice au prestat muncă de analiză, documentare şi sprijin, care a dus la elaborarea unui set de propuneri din domeniul politicii publice, propuneri de documente legislative şi propuneri de proceduri pentru combaterea criminalităţii informatice. Valoarea iniţială a proiectului a fost de 11 103 000 RON, plus 1 665 450 RON cofinanţare de la beneficiar.

Bugetul celui de al doilea proiect dezvoltat de CERT-RO prin intermediul celui de Al şaptelea program-cadru, şi anume ACDC- Advanced Cyber -Defence Centre (Centrul de Protecţie Anti-Botnet) este de 16 338 803 EUR, 50% din finanţare provenind de la Comisia Europeană. Circa 28 de parteneri din 14 ţări europene participă la proiect. Bugetul alocat de CERT-RO este de 470 200 EUR, la care partea română contribuie cu 235 100 EUR.

3.5 Concluzii

- Strategia naţională de securitate cibernetică există în România din 2013 şi include o serie de definiţii (ameninţare cibernetică, incident cibernetic, criminalitate informatică, terorism cibernetic etc.), obiective, acţiuni, analiza ameninţării, Sistemul naţional de securitate cibernetică (SNSC) şi cooperarea dintre sectorul public şi cel privat.

[12] http://www.cert-ro.eu/proiecte/cybercrime/articol.php?idarticol=708

- România a definit, de asemenea, prioritățile naționale în ceea ce privește criminalitatea informatică, și anume prevenirea, capacitatea instituțională, formarea, cooperarea internațională, armonizarea legislației, consolidarea cooperării cu sectorul privat și cooperarea internațională. Autoritățile române consideră criminalitatea informatică o amenințare gravă pentru stat și societate.

- În opinia evaluatorilor, strategia, alături de prioritățile definite în România, oferă o bază solidă pentru combaterea criminalității informatice. Cooperarea strânsă dintre organizațiile publice creează o ocazie unică de a implica o gamă largă de entități care conlucrează. Prin urmare, o gamă largă de actori sunt implicați în combaterea criminalității informatice. Pe de altă parte, sectorul privat este mai puțin implicat în abordarea acestui fenomen.

- Totuși, în realizarea respectivelor priorități se pot întâmpina unele dificultăți în ceea ce privește asigurarea unei legislații coerente. De exemplu, păstrarea datelor nu este reglementată, la momentul actual, în legislația națională. Legislația națională de punere în aplicare a Directivei 2006/24/CE privind păstrarea datelor a fost în vigoare până în iulie 2014, când Curtea Constituțională a României a decis că dispozițiile referitoare la păstrarea datelor sunt neconstituționale, ca urmare a invalidării directivei de către Curtea de Justiție a UE trei luni mai devreme, care a afirmat că legiuitorul UE și-a depășit limitele impuse de respectarea principiului proporționalității.

- Aceasta rămâne unul dintre cele mai importante instrumente juridice pentru aplicarea legii, dat fiind faptul că, în cele din urmă, cele mai multe cercetări în domeniul criminalității informatice presupun convertirea adreselor IP în detaliile abonatului respectiv. Prin urmare, faptul că nu se poate face acest lucru paralizează multe eforturi de a cerceta criminalitatea organizată și gravă, pe lângă criminalitatea informatică, și afectează negativ în mod semnificativ gradul de asistență pe care România îl poate pune la dispoziția altor țări. Prin urmare, autoritățile române trebuie să soluționeze această problemă în mod adecvat, deși, în opinia evaluatorilor, acesta nu este numai o problemă internă la nivelul României, ci trebuie soluționată în primul rând la nivelul UE.

- Fiecare instituţie publică cu responsabilităţi în ceea ce priveşte securitatea cibernetică păstrează statistici referitoare la criminalitatea informatică, în special Ministerul Justiţiei (numărul persoanelor condamnate pentru infracţiuni prin încălcarea Legii nr. 365/2002 privind comerţul electronic); DIICOT (cazuri de criminalitate informatică) şi Poliţia Naţională (cazuri de criminalitate informatică). CERT-RO păstrează, de asemenea, statistici detaliate cu privire la alerte colectate şi transmise de sistemele automate.

- În opinia evaluatorilor, par să nu existe statistici complet standardizate pentru actorii (poliție, procurori, judecători) implicați în cercetări şi urmăriri penale din motive practice legate de criminalitatea informatică. Statisticile referitoare la criminalitatea informatică sunt generate sub forma unei cifre unice[13]. Prin urmare, nu sete posibilă împărţirea diferitelor cazuri de criminalitate informatică în categorii. Ar fi, deci, oportun să existe cifre defalcate în funcţie de diferitele domenii de criminalitate informatică, de preferinţă atacuri cibernetice, abuzul asupra copiilor online şi frauda cu carduri online, pentru a obține o imagine mai clară a criminalității informatice.

- Poliţia Română are un buget separat pentru îndeplinirea unor activităţi specifice în domeniul prevenirii şi combaterii criminalităţii, dar nu dispune de secţiuni separate pentru domenii specifice de criminalitate. România a utilizat în mod frecvent finanţare din partea UE pentru a finaliza proiecte în domeniul criminalităţii informatice.

[13] În urma vizitei la fața locului, echipa de evaluare a primit o explicație conform căreia statisticile judiciare colectate de către instanțe sunt copiate/încărcate periodic pe serverele Ministerului Justiției și gestionate de minister, în timp ce datele statistice care se referă la etapa cercetării, executarea pedepsei, probațiune etc. sunt gestionate de alte autorități. Având în vedere că aplicația ECRIS include numai date pentru etapa judecății, nu există o corelare directă între datele colectate în etapa cercetării, care sunt gestionate de alte instituții, și datele privind persoanele condamnate. Prin urmare, Ministerul Justiției intenționează să obțină în temeiul POCA 2014-2020 finanțare pentru un proiect vizând crearea unui sistem de informații integrat în domeniul justiției, care va facilita colectarea și gestionarea datelor statistice atât pentru instanțe, cât și pentru parchete.

3 STRUCTURI NAȚIONALE

3.1 Autorități judiciare (parchete și instanțe judecătorești)

4.1.1 Structura internă

Ministerul Public este constituit din Parchetul de pe lângă Înalta Curte de Casaţie şi de Justiţie, 15 parchete de pe lângă curţi de apel, 41 de parchete de pe lângă tribunale (capitale de judeţe) şi 176 de parchete de pe lângă judecătorii[14]. Parchetul de pe lângă Înalta Curte de Casaţie şi de Justiţie este constituit din patru structuri componente: Direcţia Naţională Anticorupţie, Direcţia de Investigare a Infracţiunilor de Criminalitate Organizată şi Terorism, Secţia de urmărire penală şi criminalistică şi Secţia parchetelor militare[15].

Direcţia de Investigare a Infracţiunilor de Criminalitate Organizată şi Terorism (DIICOT) a fost înfiinţată prin Legea nr. 508/2004 ca o structură unică a Parchetului de pe lângă Înalta Curte de Casaţie şi de Justiţie, fiind specializată în combaterea celor mai grave infracţiuni, precum traficul de persoane, traficul de droguri, infracţiuni de terorism, criminalitate informatică, infracţiuni macroeconomice/financiare. Direcţia este condusă de un procuror-şef, asimilat funcţiei de prim adjunct al procurorului general, şi include următoarele servicii: Serviciul de prevenire şi combatere a criminalităţii organizate, Serviciul de prevenire şi combatere a traficului ilicit de droguri, Serviciul de prevenire şi combatere a criminalităţii economico-financiare, Serviciul de prevenire şi combatere a infracţiunilor de terorism şi a celor contra siguranţei statutului, Serviciul de prevenire şi combatere a criminalităţii informatice, Serviciul judiciar şi Biroul de cooperare, reprezentare şi asistenţă judiciară internaţională. Structura DIICOT este alcătuită din 15 servicii teritoriale şi 26 de birouri teritoriale. Direcţia dispune de un total de 280 de procurori, 40 de specialişti şi 200 de membri ai personalului administrativ (grefieri, personal contractual). În temeiul legii nr. 508/2004, articolul 9, procurorul poate delega anumite activităţi unor ofiţeri de poliţie judiciară anume desemnaţi. Potrivit autorităților române, ar putea fi contraproductiv în domenii în care criminalitatea informatică este doar ocazională. Totuşi, unul sau mai mulţi procurori conduc în principal urmărirea penală specializată a infracţiunilor informatice.

[14] A se vedea Legea nr. 304/2004 privind organizarea judiciară.
[15] A se vedea http://www.mpublic.ro/sectii.htm, http://www.pna.ro, http://www.diicot.ro.

Structura specializată în combaterea criminalităţii informatice este Serviciul de prevenire şi combatere a criminalităţii informatice care este condus de un procuror şef, doi procurori şefi subordonaţi şi patru procurori, fiecare dintre ei fiind îndrituiţi, prin lege, să exercite personal funcţii de urmărire penală în specializarea relevantă şi cazurile desemnate. Infracţiunile care intră în sfera de competenţă a acestui serviciu includ: accesul ilegal la un sistem informatic (articolul 360 din NCP), interceptarea ilegală a unei transmisii de date informatice (articolul 361 din NCP), alterarea integrităţii datelor informatice (articolul 362 din NCP), perturbarea funcţionării sistemelor informatice (articolul 363 din NCP), transferul neautorizat de date informatice (articolul 364 din NCP), operaţiuni ilegale cu dispozitive sau programe informatice (articolul 365 din NCP), tentativa la infracţiunile menţionate (articolele 360 - 365 din NCP), falsul informatic (articolul 325 din NCP), pornografia infantilă (articolul 374 din NCP), frauda informatică (articolul 249 din NCP), efectuarea de operaţiuni financiare în mod fraudulos (articolul 250 din NCP), acceptarea operaţiunilor financiare efectuate în mod fraudulos (articolul 251 din NCP), falsificarea de titluri de credit sau instrumente de plată [articolul 311 alineatul (2) din NCP], punerea în circulaţie de valori falsificate (articolul 313 din NCP), deţinerea de instrumente în vederea falsificării de valori [articolul 314 alineatul (2) din NCP] [numai dacă fapta este săvârşită de un grup infracţional organizat (articolul 367 din NCP)] şi orice alte infracţiuni.

Sistemul judiciar din România este organizat ca un sistem ierarhic de instanţe, cu un sistem de drept civil. Conform Constituţiei şi Legii nr. 304/2004 privind organizarea judiciară, instanţele sunt organizate după cum urmează:

- *Înalta Curte de Casaţie şi Justiţie*;
- 15 curţi de apel;
- 41 de tribunale şi Tribunalul Bucureşti;
- 188 de judecătorii.

Organizarea instanţelor din România nu prevede complete/judecători specializaţi în materie de criminalitate informatică.

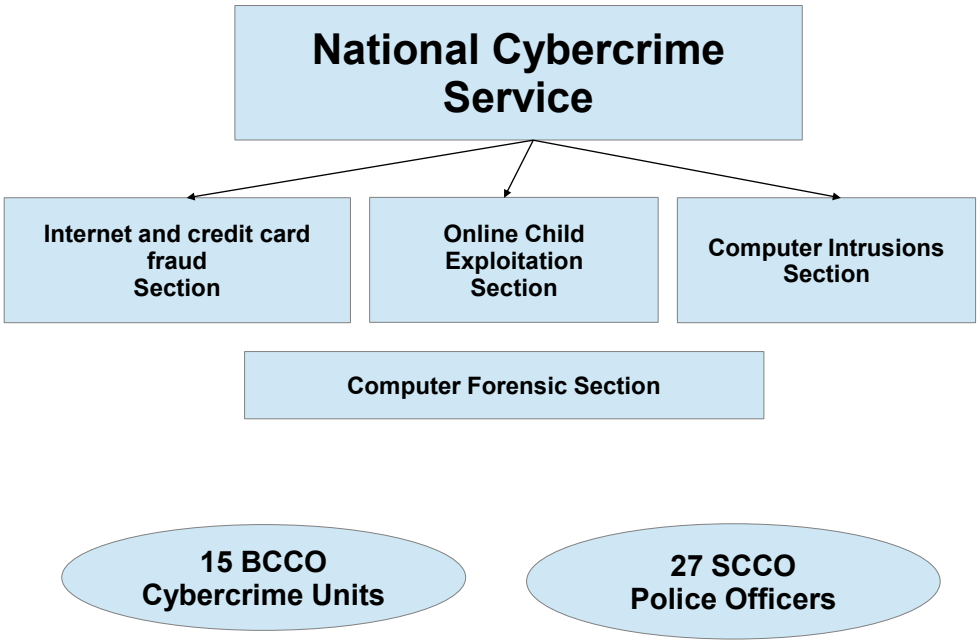
4.1.2 Capacitatea de a efectua o urmărire penală încununată de succes şi obstacole în calea acesteia

Autorităţile române au afirmat că principalele obstacole în cercetarea infracţiunilor informatice sunt următoarele:

- probleme de ordin tehnic ale echipamentului nou din partea soluţiilor IT&C, sisteme virtuale de plată care fac dificilă cercetarea produselor financiare, servicii de anonimizare, soluţii de criptare, chestiuni de ordin tehnic referitoare la probe;
- natura transfrontalieră a criminalităţii informatice şi insuficienta capacitate de cooperare cu partenerii străini, precum şi durata îndelungată pentru obţinerea probelor de la jurisdicţiile străine;
- soluţii comune pentru accesarea spațiilor de stocare a datelor din „cloud”;
- problema referitoare la păstrarea datelor care nu este reglementată în legislaţia naţională, în timp ce instrumentele disponibile pentru obţinerea datelor necesare nu permit obţinerea rapidă a datelor şi a informaţiilor.

4.2 Autoritățile de aplicare a legii

Serviciul de combatere a criminalităţii informatice din cadrul Direcţiei de Combatere a Criminalităţii Organizate din cadrul Poliţiei Române a fost înfiinţat în 2003 printr-un ordin intern al ministrului afacerilor interne. Respectivul serviciu are responsabilitatea de a preveni şi cerceta criminalitatea informatică, fraudele cu carduri de credit şi pornografia infantilă prin internet, precum şi de a percheziţiona sistemele informatice, şi este format din patru birouri, specializaţi în investigarea fraudelor online şi a mijloacelor de plată electronice, investigarea atacurilor cibernetice, investigarea pornografiei infantile prin internet şi efectuarea de percheziţii informatice. Organizarea acestei structuri corespunde priorităţilor stabilite în domeniul criminalităţii informatice în cadrul Europol, un birou specializat fiind înfiinţat pentru fiecare domeniu. Respectivul serviciu dispune de un total de 34 de poliţişti şi de aproximativ 150 de poliţişti la nivel local care îşi desfăşoară activitatea în domeniul cercetării criminalităţii informatice. Poliţiştii angajaţi în structurile centrale şi teritoriale au pregătire juridică şi informatică, fiind în principal recrutaţi din rândul absolvenţilor Academiei Române de Poliţie.



Principalele sarcini ale Serviciului de combatere a criminalităţii informatice sunt desfăşurarea şi coordonarea, împreună cu parchetele, de cercetări în domeniul criminalităţii informatice, promovarea de măsuri legale şi instituţionale pentru îmbunătăţirea activităţilor desfăşurate, cercetarea şi strângerea de informaţii prin internet, asigurarea de programe şi echipament de formare pentru poliţie la nivel central şi teritorial, elaborarea de proceduri standardizate pentru activităţi investigative, asigurarea corectei funcţionări a colaborării interinstituţionale, asigurarea unui parteneriat cu sectorul privat şi asigurarea bunei cooperări internaţionale.

La nivel teritorial, există, de asemenea, structuri specializate în prevenirea şi combaterea criminalităţii informatice în cadrul Poliţiei Naţionale Române.

Activitatea de obţinere şi prelucrare a probelor digitale este desfăşurată de Serviciul de combatere a criminalităţii informatice, Institutul Naţional de Criminalistică (INC) şi structuri specializate din cadrul Serviciului Român de Informaţii (SRI). Diferenţele se referă la statutul angajaţilor şi la natura activităţilor pe care le pot desfăşura. Serviciul de combatere a criminalităţii informatice poate colecta probe digitale şi poate efectua percheziţii informatice, în timp ce INC şi SRI pun la dispoziţie expertiză în domeniul probelor digitale. Pentru a consolida cooperarea la nivel operaţional 24/7, au fost înfiinţate puncte de contact. În cadrul poliţiei, există un al doilea punct de contact 24/7 pentru a oferi asistenţă punctului de contact din cadrul parchetului. Personalul desemnat preia sesizările care sosesc şi le prelucrează. În plus, Direcţia de Combatere a Criminalităţii Organizate conţine un birou specializat în cercetarea şi efectuarea de percheziţii informatice, cu poziţii specializate în percheziţii informatice, iar structurile teritoriale au departamente cu ofiţeri specializaţi în percheziţii informatice. În total, sunt 57 de poliţişti specializaţi în percheziţii informatice. De asemenea, în cadrul acesteia sunt angajaţi specialişti în prelucrarea şi exploatarea informaţiilor, în domeniul economic, financiar, bancar, vamal, IT şi în alte domenii, precum şi personal specializat auxiliar şi personal economic şi administrativ pentru poziţiile disponibile.

4.3 Alte autorităţi/instituţii/ parteneriatul public-privat

CERT-RO

CERT-RO este o structură independentă, cu expertiză în domeniul securităţii cibernetice, care dispune de capacitatea de a preveni, analiza, identifica şi răspunde la incidentele de securitate cibernetică care ameninţă spaţiul cibernetic naţional. CERT-RO este coordonat de Ministerul pentru Societatea Informaţională şi este finanţat integral de la bugetul de stat. Principalele sarcini ale CERT-RO sunt:

- organizarea şi menţinerea unei baze de date privind ameninţările, vulnerabilităţile şi incidentele de securitate cibernetică identificate sau raportate CERT-RO, tehnicile şi tehnologiile folosite pentru atacuri, precum şi bunele practici pentru protecţia infrastructurilor cibernetice;

- asigurarea cadrului organizatoric şi a suportului tehnic necesar schimbului de informaţii dintre diverse echipe de tip CERT, utilizatori, autorităţi de reglementare, producători de echipamente şi soluţii de securitate cibernetică, precum şi furnizori de servicii internet;
- asigurarea unui punct unic de contact pentru colectarea informaţiilor şi a sesizărilor despre incidente de securitate cibernetică atât automatizat și securizat, cât şi prin comunicare directă, după caz;
- elaborarea de propuneri legislative pe care le înaintează Ministerului Societăţii Informaţionale (MSINF) sau Consiliului Suprem de Apărare a Ţării (CSAT), privind modificarea cadrului legislativ în vederea stimulării dezvoltării securităţii cibernetice a sistemelor ce asigură servicii de interes public;
- constituirea „Sistemului de alertă timpurie şi informare în timp real" privind incidentele de securitate cibernetică, ceea ce se constituie în trimiterea de alerte în timp real cu privire la incidente de securitate cibernetică, emiterea de rapoarte cu privire la distribuţia şi natura incidentelor şi facilitarea colaborării cu autorităţile naţionale responsabile în asigurarea securităţii cibernetice, în vederea prevenirii şi înlăturării efectelor incidentelor;
- sprijinirea serviciilor publice prin: servicii de tip preventiv (anunţuri privind ameninţări sau vulnerabilităţi nou-identificate pe plan naţional și/sau internaţional; realizarea, la cerere, de auditări de securitate şi evaluări ale riscurilor sau teste de penetrare; rapoarte privind incidente de securitate cibernetică care ar putea afecta sau implica autorităţi române), servicii de tip reactiv (alerte şi atenţionări privind apariţia unor activităţi suspecte premergătoare atacurilor, gestiunea incidentelor de securitate cibernetică la nivel naţional) şi servicii de consultanţă (pregătirea echipelor de tip CERT, analize de risc aplicate la nivel local şi la nivel naţional privind infrastructurile cibernetice).

CERT-RO colectează din surse naţionale sau internaţionale date referitoare la incidente de securitate cibernetică şi evenimente care afectează sau implică entităţi din România. Astfel, din momentul în care incidentul este identificat, pe baza procedurilor interne, CERT-RO desfăşoară o serie de acţiuni care asigură activitatea de răspuns. Mai mult, CERT-RO asigură sprijin organizaţional şi tehnic pentru schimbul de informaţii între diferite entităţi (autorităţi naţionale, persoane sau companii, echipe de tip CERT, furnizori de soluţii de securitate, furnizori de servicii internet etc.) implicate în incidente de securitate cibernetică şi facilitează uşoara cooperare a acestora.

CERT–RO nu are autoritatea legală de a soluţiona toate tipurile de incidente de securitate cibernetică, de exemplu pe cele care apar ca urmare a unor infracţiuni informatice care intră sub responsabilitatea agenţiilor de aplicare a legii. Mai mult, incidentele de securitate cibernetică care ar putea constitui ameninţări la adresa securităţii naţionale sunt gestionate de instituţii cu competenţă în acest domeniu specific. Dacă CERT-RO primeşte o astfel de notificare, acesta o trimite autorităţii adecvate.

Centrul de coordonare a protecţiei infrastructurilor critice

Centrul de coordonare a protecţiei infrastructurilor critice joacă rolul de punct de contact naţional pentru celelalte state membre ale UE, Comisia Europeană, NATO şi alte organizaţii internaţionale pentru probleme legate de infrastructuri critice. Una dintre responsabilităţile sale este de a asigura punerea în aplicare a Directivei 2008/114/CE a Consiliului privind identificarea şi desemnarea infrastructurilor critice europene şi evaluarea necesităţii de îmbunătăţire a protecţiei acestora, precum şi managementul reţelei CIWIN la nivel naţional. Totuşi, nu a fost clar pentru echipa de evaluare dacă există un instrument juridic naţional care prevede atribuţii specifice pentru operatorii infrastructurilor critice şi ai sistemelor informatice care să permită împărtăşirea informaţiilor cu privire la incidente şi evoluţii în eventualitatea unui atac cibernetic.

Centre judeţene de resurse şi asistenţă educaţională

Centrele judeţene de resurse şi asistenţă educaţională, situate în judeţe şi în Bucureşti, joacă un rol important în prevenirea şi combaterea criminalităţii informatice şi în intervenţia pentru securitatea online. Date fiind obiectivele lor, aceste centre contribuie la consilierea victimelor sau potenţialelor victime. Sunt repartizate pe tot teritoriul ţării. Un Centru Judeţean de Resurse şi Asistenţă Educaţională (CJRAE) a fost înfiinţat în fiecare judeţ, iar în Bucureşti există Centrul Municipiului Bucureşti de Resurse şi Asistenţă Educaţională (CMBRAE). Aceste unităţi sunt legate de sistemul de învăţământ preuniversitar. Au personalitate juridică şi sunt subordonate Ministerului Educaţiei Naţionale. Acestea reprezintă o instituţie specializată în oferirea de educaţie specială integrată, coordonarea şi monitorizarea serviciilor de educaţie specifice oferite copiilor/studenţilor, profesorilor, părinţilor şi membrilor comunităţii, pentru a garanta faptul că fiecare are acces la o educaţie de calitate şi la asistenţa necesară în această privinţă.

Principalele obiective ale CJRAE/CMBRAE sunt acelea de a înscrie toţi copiii/tinerii în sistemul obligatoriu de învăţământ şi de face ca aceştia să rămână în sistem; de a informa şi ghida profesorii în vederea optimizării profesionale şi educaţionale; de a lucra cu factorii educaţionali implicaţi în dezvoltarea personalităţii studentului/tânărului pentru a-i integra mai bine în şcoală şi în viaţa socială şi profesională; de a implica părinţii în activităţi specifice pentru o relaţie eficientă şcoală-familie-comunitate, ca bază pentru adaptarea la şcoală şi integrarea socială a copiilor/tinerilor; şi de a elabora studii privind abandonul şcolar, comportamentul juvenil deviant, mediul negativ, activităţi extracuriculare/de petrecere a timpului liber.

Informaţii

Serviciul Român de Informaţii este, de asemenea, implicat în prevenirea şi combaterea criminalităţii informatice, în temeiul Legii nr. 14/1992 privind organizarea şi funcţionarea Serviciului Român de Informaţii, al unor dispoziţii din Codul de procedură penală şi al unei legislaţii conexe. Principalele obiective în domeniul respectiv sunt transmiterea organismelor de urmărire penală de date şi informaţii care indică pregătirea unui act incriminat de dreptul penal, în condiţiile prevăzute la articolul 61 din Codul de procedură penală. Totuşi, Serviciul Român de Informaţii nu are atribuţii de cercetare penală şi urmărire penală. Serviciul Român de Informaţii asigură coordonarea tehnică a Consiliului Operativ de Securitate Cibernetică (COSC) în domeniul securităţii cibernetice. Serviciul Român de Informaţii cooperează îndeaproape cu poliţia pentru obţinerea şi prelucrarea probelor digitale.

ANPDCA

În ceea ce priveşte responsabilităţile conferite de legislaţie Autorităţii Naţionale pentru Protecţia Drepturilor Copilului şi Adopţie (ANPDCA), aceasta nu are o autoritate specifică strict legată de combaterea securităţii cibernetice. Intervenţia sa în acest domeniu are loc din perspectiva generală de a asigura protecţie şi promovarea drepturilor tuturor copiilor. Totuşi, în toate mecanismele de cooperare interinstituţionale dedicate acestui aspect, rolul ANPDCA este de a facilita colaborarea şi implicarea structurilor locale în ceea ce priveşte asigurarea de servicii specializate pentru copii victime ale acestui fenomen, pentru a-i sprijini şi reabilita. În acelaşi timp, ANPDCA poate coopera cu alte instituţii în ceea ce priveşte raportarea cazurilor copiilor care au devenit victime ale acestui fenomen, pentru a iniţia verificări şi investigaţii specifice ale autorităţilor competente. Date fiind obligaţiile care revin cadrului general de reglementare care asigură protecţia şi promovarea drepturilor copilului, ANPDCA poate sprijini promovarea diferitelor acte juridice referitoare la acest domeniu, iniţiate de alte ministere sau autorităţi cu responsabilităţi distincte în această privinţă.

CYBER-EX

Centrul de Excelenţă pentru Combaterea Criminalităţii Informatice (CYBER-EX) a fost înfiinţat ca un partener viabil între autorităţile de aplicare a legii, autorităţile judiciare, instituţii de educaţie superioare sau specializate şi societăţi private. Centrul a fost creat pentru a integra cunoştinţe şi expertiză şi pentru a furniza dezvoltare profesională în combaterea criminalităţii informatice, prin utilizarea fondurilor UE (pentru mai multe informaţii a se vedea capitolul 8.1).

Autorităţile române au raportat, de asemenea, faptul că există parteneriate public/privat cu diferite instituţii private pentru a preveni şi combate criminalitatea informatică. De exemplu, a fost menţionat parteneriatul cu Poliţia Română şi Microsoft RO, scopul fiind acela de a organiza evenimente de prevenire şi de sensibilizare în domeniul criminalităţii informatice. Celălalt tip de parteneriat dintre Poliţia Română şi un ONG (şi anume „Salvaţi copiii") se referă la pornografie infantilă pe internet. Există, de asemenea, o reprezentanţă a Western Union în România pentru schimbul de informaţii.

4.4. Cooperarea şi coordonarea la nivel naţional

4.4.1 Obligaţii juridice sau de politică

Sistemul naţional de securitate cibernetică (SNSC) reprezintă cadrul general de cooperare între instituţii publice şi autorităţile însărcinate din acest domeniu pentru a asigura coordonarea naţională a acţiunilor pentru a asigura securitatea spaţiului cibernetic. În plus, misiunea SNSC constă în asigurarea elementelor de cunoaştere, prevenire şi contracarare a ameninţărilor, vulnerabilităţilor şi riscurilor specifice spaţiului cibernetic care pot afecta securitatea infrastructurilor cibernetice naţionale, inclusiv managementul. Conform Strategiei de securitate cibernetică a României, criminalitatea informatică reprezintă una dintre ameninţările la adresa spaţiului cibernetic, împreună cu terorismul cibernetic şi războiul cibernetic. Pentru a îndeplini sarcinile respective, Consiliul Operativ de Securitate Cibernetică (COSC) a fost înfiinţat la vârful structurilor naţionale.

COSC include reprezentanţi ai: Ministerului Afacerilor Externe, Ministerului Apărării Naţionale, Ministerului de Interne, Serviciului Român de Informaţii, Serviciul de Informaţii Externe, Serviciului de Telecomunicaţii Speciale, Serviciului de Protecţie şi Pază şi Oficiului Registrului Naţional al Informaţiilor Secrete de Stat la nivel de secretari de stat. Preşedintele COSC este consilierul prezidenţial privind securitatea naţională, iar vice-preşedintele său este consilierul prim-ministrului pe probleme de securitate naţională.

În opinia evaluatorilor, componenţa COSC nu reflectă toate părţile implicate în combaterea criminalităţii informatice, precum Ministerul Educaţiei. În plus, în ciuda rolului semnificativ pe care ar trebui să îl joace luând în considerare reprezentanţii desemnaţi, COSC nu are personalitate juridică şi, prin urmare, nu are competenţele de a lua decizii referitoare la securitatea cibernetică. COSC joacă numai un rol de acordare de consultanţă şi de coordonare între instituţiile competente. Totuşi, COSC face propuneri şi recomandări Consiliului Suprem de Apărare a Ţării (CSAT)[16] cu privire la, de exemplu, măsuri de armonizare a răspunsurilor la ameninţări şi atacuri cibernetice, solicitarea de asistenţă din partea altor state sau organizaţii şi organisme internaţionale şi răspunsuri la solicitări de asistenţă; planuri sau linii de acţiune, în funcţie de concluziile la care s-a ajuns şi evoluţia spaţiului cibernetic; programe privind securitatea cibernetică; politici referitoare la securitatea cibernetică pentru autorităţi şi instituţii publice). Totuşi, actele adoptate de CSAT nu au caracter normativ, ci caracter administrativ.

Rolul Ministerului Educaţiei între instituţiile cu responsabilităţi în prevenirea şi combaterea criminalităţii informatice se bazează, în principal, pe două componente, şi anume prevenire şi intervenţie, utilizând structurile subordonate (inspectorate şcolare, centre judeţene de psihologie educaţională/centre din Bucureşti de psihologie educaţională, reţeaua de consilieri şi psihologi şcolari, casele profesorilor, palatele şi cluburile copiilor) şi cooperarea cu parteneri educaţionali şi părţi interesate (ONG-uri, asociaţii profesionale, alte asociaţii etc.). Provocarea reprezentată de prevenirea şi combaterea criminalităţii informatice este abordată la următoarele niveluri: intracuricular, extracuricular şi în afara şcolii.

[16] CSAT este format din preşedintele României, în calitate de preşedinte al CSAT, prim-ministrul Guvernului României, vicepreşedinte al CSAT, ministrul apărării naţionale, ministrul afacerilor interne, ministrul afacerilor externe, ministrul justiţiei, ministrul economiei, comerţului şi turismului, ministrul finanţelor publice, directorul Serviciului Român de Informaţii, directorul Serviciului de Informaţii Externe, şeful Statului Major General şi consilierul prezidenţial pentru securitate naţională.

Din punctul de vedere al justiţiei penale, cooperarea interinstituţională este prevăzută între competenţele fiecărei instituţii, fiind reglementată de dispoziţii juridice, reglementări interne şi protocoale existente între acestea. Pentru fiecare instituţie, responsabilităţile sunt diferite, după cum urmează:

- poliţia răspunde de: primirea de plângeri, culegerea datelor şi a informaţiilor, desfăşurarea anchetelor, analizarea probelor tehnice şi utilizarea de mijloace speciale de investigaţie;
- Ministerul Public răspunde de: primirea de plângeri, desfăşurarea de cercetări penale şi instruirea unităţilor de poliţie în sensul adoptării de măsuri speciale de cercetare, precum şi de cooperarea cu instanţele pentru aprobarea măsurilor speciale de cercetare sau restrictive;
- Serviciul de Informaţii culege date şi informaţii specifice şi le pune la dispoziţia poliţiei sau procurorilor în vederea investigaţiei.
- instanţele au competenţa de a autoriza utilizarea de măsuri speciale de cercetare sau restrictive şi de a soluţiona cauza.

În temeiul Legii nr. 161/2003 referitoare la securitatea sistemelor informatice şi la protecţia datelor personale, instituţiile publice şi autorităţile însărcinate din acest domeniu, furnizorii de servicii, ONG-urile şi alţi reprezentanţi ai societăţii civile desfăşoară activităţi în comun şi programe pentru prevenirea criminalităţii informatice. Acestora li se solicită să promoveze politici, practici, măsuri, proceduri şi standarde minime de securitate pentru sistemele informatice şi să organizeze campanii de informare referitoare la criminalitatea informatică şi la riscurile la care sunt expuşi utilizatorii sistemelor informatice.

4.4.2 Resursele alocate îmbunătăţirii cooperării

Nivelul de resurse, capacitate instituţională şi de formare a personalului pus la dispoziţie pentru aplicarea legii este realmente satisfăcător, în opinia autorităţilor române, având în vedere situaţia criminalităţii informatice din România. Totuşi, există cerinţe de îmbunătăţire în continuare. De exemplu, la nivelul Serviciului de combatere a criminalităţii informatice şi al unităţilor teritoriale de poliţie, există soluţii hardware şi software (software Encase) pentru a efectua activităţi de criminalistică informatică.

Totuşi, nu există alocaţii bugetare speciale la nivelul structurilor de aplicare a legii privind cooperarea cu sectorul privat, dar în proiectele şi evenimentele întreprinse în comun există activităţi finanţate, de asemenea, de autorităţile publice.

Ar trebui arătat că în cursul vizitei la CERT-RO, echipa de evaluare a fost informată că statul de salarii acoperă numai aproximativ 60% din personalul pentru care s-a prevăzut un buget. Centrul pare să se fi angajat într-o activitate care îl depăşeşte şi ar avea de câştigat în mod semnificativ dintr-o alocare suplimentară a resurselor, care ar putea fi folosite pentru înfiinţarea unui centru de intermediere telefonică 24/7 şi pentru proiecte de monitorizare în timp real.

4.5 Concluzii

- În România sunt implicate în securitatea cibernetică şi în criminalitatea informatică, în special, un număr de părţi interesate. Toate acestea au roluri clare şi distincte, incluzând întregul spectru al criminalităţii informatice. Cadrul general de cooperare este reprezentat de Sistemul naţional de securitate cibernetică (SNSC) care răspunde, de asemenea, de abordarea cooperării cu mediul academic şi de afaceri, asociaţiile profesionale şi organizaţiile nonguvernamentale. Consiliul Operativ de Securitate Cibernetică (COSC) vizează facilitarea coordonării unitare a SNSC la nivel central.

- Echipei de evaluare i s-a comunicat în ocazii diferite şi de către autorităţi diferite că coordonarea între diferitele autorităţi implicate nu este o problemă şi că se desfăşoară în conformitate cu legile, reglementările interne şi protocoalele existente. Există o multitudine de actori, ceea ce pare să reflecte în mod adecvat abordarea multidisciplinară a criminalităţii informatice de către România (de la prevenire, la sensibilizare şi aplicarea legii). Aceştia par să coopereze bine, dar, totuşi, a fost dificil de înţeles cine coordonează toate aceste eforturi în practică. Mai mult, nu toţi actorii implicaţi în combaterea criminalităţii informatice sunt reprezentaţi în mod direct la nivelul COSC, ci la nivel ministerial.

- Parlamentului i-a fost prezentat un nou proiect de lege cu privire la securitatea cibernetică, dar acesta nu a trecut de scrutinul Curţii Constituţionale (*a se vedea* Decizia Nr. 17/2015). După vizita la faţa locului, echipa de evaluare a fost informată că legea a fost declarată neconstituţională în întregime prin decizia Curţii sus-menţionată, ceea ce are un efect final asupra actului legislativ care duce la încetarea procesului legislativ.

- Există o relaţie strânsă între procurori şi poliţie, care este prevăzută de lege, dar care se şi concretizează la nivel naţional şi regional. Procurorii DIICOT efectuează urmărirea penală în cazuri referitoare la criminalitatea informatică care cuprinde toate infracțiunile prevăzute în Convenția de la Budapesta și Directiva 2013/40/UE, cum ar fi infracțiunile dependente de calculator (*stricto sensu,* de exemplu accesul ilegal, împiedicarea funcționării unui calculator, utilizarea abuzivă de dispozitive etc.) și infracțiunile facilitate de un calculator (falsul informatic, frauda informatică, pornografia infantilă, ademenirea unei persoane în vederea săvârșirii de acte sexuale cu un minor, frauda cu carduri de credit etc.). Serviciului de combatere a criminalităţii informatice din cadrul Poliţiei Române efectuează investigaţii specializate în domeniul criminalităţii informatice. Ambele servicii au competenţe şi beneficiază de personal la nivel naţional şi local.

- Nu există judecători numiți pentru a se ocupa de criminalitatea informatică. Prin urmare, în opinia evaluatorilor, sensibilizarea judecătorilor cu privire la acest tip de criminalitate necesită formare periodică.

- Serviciul Român de Informații (SRI) este considerabil implicat în combaterea criminalităţii informatice şi, deşi nu are responsabilităţi de cercetare penală şi urmărire penală, acesta oferă sprijin, din punct de vedere tehnic (intercepții, expertiză) și cu informații la cerere sau *ex officio*, pentru cercetarea și urmărirea penală desfășurate de procuror. Evaluatorii consideră că această cooperare strânsă şi eficientă în combaterea criminalităţii informatice ar putea servi drept exemplu de cele mai bune practici.

- Munca şi activitatea CERT-RO sunt demne de lăudat şi includ atât aspecte referitoare la securitatea cibernetică, cât şi la criminalitatea informatică. Una din sarcinile principale ale CERT-RO este de a identifica şi preveni incidentele de securitate cibernetică care ameninţă spaţiul cibernetic naţional. Un proiect extrem de promiţător urmăreşte să realizeze o cooperare strânsă cu cel mai mare furnizor de servicii internet din România, ceea ce ar trebui să ducă la notificarea clienţilor infectaţi cu malware, în special a sistemelor compromise din România care fac parte din botneturi şi care sunt utilizate ca proxy pentru efectuarea de atacuri asupra unor ţine din afara ţării. Implicarea CERT-RO în criminalitatea informatică la nivel naţional şi internaţional ar trebui subliniată, în special dezvoltarea de către CERT-RO atât a unui program cuprinzător de formare cu privire la prevenirea şi combaterea criminalităţii informatice, cât şi a unui set de propuneri de politici pentru combaterea criminalităţii informatice.

- Ţinând seama de rolul important pe care îl joacă şi de resursele sale bugetare şi umane, evaluatorii consideră că ar trebui făcută o evaluare cu privire la creşterea numărului de angajaţi pentru a ajunge la grila de angajaţi avută în vedere şi, prin urmare, pentru a o face mai eficientă. Acesta este un efort realmente lăudabil, capabil de o prevenire activă foarte eficientă a atacurilor cibernetice. Prin urmare, în opinia evaluatorilor, eforturile făcute de CERT-RO pentru combaterea atacurilor cibernetice ar trebui văzute ca exemple de cele mai bune practici.

- Centrul de coordonare a protecţiei infrastructurilor critice este autoritatea naţională competentă în domeniul protecţiei infrastructurilor critice. Centrul este responsabil cu punerea în aplicare a Directivei 2008/114/CE a Consiliului privind identificarea şi desemnarea infrastructurilor critice europene, dar este în continuare neclar dacă există o listă cuprinzătoare a infrastructurilor critice naţionale, dat fiind faptul că cel puţin câteva dintre articolele din proiectul de lege referitor la securitatea cibernetică, care ar fi trebuit să reglementeze conceptul de „ICIN”, au fost declarate neconstituţionale, aşa că proiectul de lege nu va intra în vigoare în viitorul apropiat. Prin urmare, nu este clar pentru echipa de evaluare dacă există un instrument juridic naţional care să prevadă atribuţii specifice pentru operatorii infrastructurilor critice şi ai sistemelor informatice în eventualitatea unui atac cibernetic.

- Echipa de evaluare a recunoscut, în timpul vizitei pe teren, că cooperarea cu societăţile private este în creştere. Furnizorii de servicii internet cooperează cu CERT-RO pe bază de voluntariat şi există şi înţelegeri cu societăţile. Autoritățile române au raportat că, ținând seama de componența COSC, interacțiunea dintre sectorul privat și COSC are loc prin intermediul instituțiilor care sunt reprezentate în cadrul său, și anume prin intermediul Ministerului pentru Societatea Informațională și CERT-RO. Totuşi, persistă întrebarea cum interacţionează sectorul privat în practică cu acesta astfel încât să permită SNSC să îşi îndeplinească responsabilitatea pentru cooperare.

4 ASPECTE JURIDICE

4.1 Dreptul penal material referitor la criminalitatea informatică

5.1.1 Convenția Consiliului Europei privind criminalitatea informatică

La 15 mai 2004, România a fost printre primele state care au ratificat Convenția Consiliului Europei privind criminalitatea informatică. Legea nr. 161/2003[17] (Titlul III - Prevenirea şi combaterea criminalităţii informatice) a pus în aplicare îndeaproape dispoziţiile convenţiei şi a fost folosită de Consiliul Europei ca lege-model în cadrul a numeroase activități de asistență tehnică[18]. Dispoziţiile materiale şi procedurale ale acestei legi au fost mai târziu încorporate în noile coduri penale.

Din 2006, România a cooperat cu Consiliul Europei în domeniul criminalităţii informatice, sprijinind în mod activ promovarea convenţiei. Experienţa legislativă şi practică a României a fost utilizată în multe activităţi organizate de Consiliul Europei. Cele mai multe din proiectele Consiliului Europei în acest domeniu au folosit expertiză şi personal din România (Poliţia Română, DIICOT, Ministerul Justiţiei, CERT), iar în perioada 2009-2013 România a detaşat un expert din cadrul Ministerului Justiţiei la Consiliul Europei care a exercitat funcţia de şef al Unităţii de combatere a criminalităţii informatice.

În urma ofertei Guvernului României din octombrie 2013, Comitetul de Miniştri a decis să înfiinţeze Oficiul Consiliului Europei la Bucureşti în domeniul criminalităţii informatice (C- PROC). Astfel, la 15 octombrie 2013, la Bucureşti a fost semnat un Memorandum de înţelegere, care a fost ratificat de Parlamentul României în martie 2014 (Monitorul Oficial din 2 aprilie 2014)[19].

[17] Legea nr. 161/2003 privind unele măsuri pentru asigurarea transparenţei în exercitarea demnităţilor publice, a funcţiilor publice şi în mediul de afaceri, prevenirea şi sancţionarea corupţiei, publicată în Monitorul Oficial al României, partea I, nr. 279 din 21 aprilie 2003, cu modificările şi amendamentele ulterioare.

[18] www.coe.int/cybercrime

[19] Memorandumul de înţelegere dintre Guvernul României şi Consiliul Europei privind Oficiul Consiliului Europei în domeniul criminalităţii informatice din Bucureşti semnat la Bucureşti la 15 octombrie 2013 şi ratificat prin Legea nr. 33/2014.

La 7 aprilie 2014 C- PROC a devenit operaţional. C-PROC din Bucureşti, România, are rolul de a asista statele din întreaga lume în consolidarea capacităţii justiţiei penale de a răspunde provocărilor cauzate de criminalitatea informatică şi de probele electronice, având la bază standardele Convenţiei de la Budapesta privind criminalitatea informatică. Aceasta include suport pentru consolidarea legislațiilor, inclusiv respectarea standardelor statului de drept, a drepturilor omului şi protecţia datelor personale; pregătirea judecătorilor, procurorilor şi poliţiştilor; înfiinţarea de unităţi specializate în domeniul combaterii criminalităţii informatice şi în domeniul criminalisticii informatice şi întărirea cooperării interinstituţionale; promovarea cooperării dintre sectorul public şi cel privat; protecţia copiilor împotriva violenţei sexuale săvârşite online şi creşterea eficienţei cooperării internaţionale. C-PROC, prin funcția sa de consolidare a capacităților, completează activitatea Comitetului Convenţiei privind criminalitatea informatică (T-CY) prin intermediul căruia statele părţi asigură punerea în aplicare a Convenţiei de la Budapesta. România participă activ la activităţile Comitetului Convenţiei privind criminalitatea informatică (T-CY) şi din iunie 2014 deţine poziţia de vice-preşedinte.

5.1.2 Descrierea legislaţiei naţionale

A/ Decizia-cadru 2005/222/JAI a Consiliului privind atacurile împotriva sistemelor informatice şi Directiva 2013/40/UE privind atacurile împotriva sistemelor informatice

În dreptul român există o legislaţie bogată în materie de criminalitate informatică[20]. Decizia-cadru 2005/222/JAI a Consiliului privind atacurile împotriva sistemelor informatice a fost transpusă în dreptul român. Prin urmare, în Codul penal român (CP) incriminează următoarele fapte: frauda informatică (articolul 249), efectuarea de operaţiuni financiare în mod fraudulos (articolul 250), falsul informatic (articolul 325), accesul ilegal la un sistem informatic (articolul 360), interceptarea ilegală a unei transmisii de date informatice (articolul 361), alterarea integrităţii datelor informatice (articolul 362), perturbarea funcţionării sistemelor informatice (articolul 363), transferul neautorizat de date informatice (articolul 364), operaţiuni ilegale cu dispozitive sau programe informatice (articolul 365), actul sexual cu un minor (articolul 220), racolarea minorilor în scopuri sexuale (articolul 222), pornografia infantilă (articolul 374).

[20] Dat fiind numărul mare de pagini implicate, descrierea sa nu a fost inclusă în raport. Pentru mai multe informaţii a se vedea anexa D.

Legea prevede faptul că şi tentativele de săvârşire a acestor infracţiuni se pedepsesc, cu excepţia celor prevăzute la articolele 220, 222 şi 325 din CP. Instigarea şi complicitatea sunt, de asemenea, incriminate în temeiul dreptului român. Entităţile juridice, cu excepţia autorităţilor de stat şi publice, pot fi răspunzătoare penal pentru infracţiuni săvârşite în exercitarea obiectului activităţii entităţilor juridice sau în interesul sau în numele acestora.

În Codul penal nu există o definiție a criminalității informatice, dar aceasta apare în Strategia națională de securitate cibernetică din motive de politică.

La momentul vizitei la fața locului, România analiza transpunerea Directivei 2013/40/UE. Conform autorităţilor române, prin punerea în aplicare a Convenţiei privind criminalitatea informatică, România asigură, în mare măsură, transpunerea directivei, rămânând ca numai anumite aspecte, precum necesitatea introducerii de circumstanţe agravante speciale, să fie perfecţionate, să fie clarificate unele definiţii şi să fie furnizate statistici. Noul Cod penal şi dispoziţiile din titlul III, capitolul 2 din Legea nr. 161/2003 privind unele măsuri pentru asigurarea transparenţei în exercitarea demnităţilor publice, a funcţiilor publice şi în mediul de afaceri, prevenirea şi sancţionarea corupţiei, cu modificările şi amendamentele ulterioare, pun în aplicare Convenţia privind criminalitatea informatică şi, implicit, şi directiva[21].

Directiva 2011/93/UE privind combaterea abuzului sexual asupra copiilor, a exploatării sexuale a copiilor și a pornografiei infantile

O serie de acte normative au transpus dispoziţii ale Directivei 2011/93/UE, în special noul Cod penal. Totuşi, transpunerea nu a fost încă încheiată. Autorităţile române au afirmat că un nou proiect de lege prin care se transpun dispoziţiile rămase este în curs de aprobare şi, după dezbaterea publică, va fi transmis guvernului.

[21] În urma vizitei la fața locului, echipa de evaluare a fost informată că legislația română este deja conformă cu Directiva 2013/40/UE, nefiind necesare modificări legislative suplimentare. România a informat Comisia Europeană în iulie 2015 cu privire la transpunerea integrală a directivei.

C/ Frauda cu carduri online

Dreptul român combate orice operaţiuni financiare efectuate online în mod fraudulos. Conform articolului 250 din CP, se pedepsesc următoarele acţiuni:
a) efectuarea unei operaţiuni de retragere de numerar, încărcare sau descărcare a unui instrument de monedă electronică ori de transfer de fonduri, prin utilizarea, fără consimţământul titularului, a unui instrument de plată electronică sau a datelor de identificare care permit utilizarea acestuia;
b) acţiuni înfăptuite prin utilizarea neautorizată a oricăror date de identificare sau prin utilizarea de date de identificare fictive;
c) transmiterea neautorizată către altă persoană a oricăror date de identificare, în vederea efectuării uneia dintre operaţiuni.

4.2 Chestiuni procedurale

5.2.1 Tehnici de cercetare

Codul de procedură penală (articolul 138 din CPP) prevede următoarele metode speciale de supraveghere sau cercetare:
a) **interceptarea comunicațiilor ori a oricărui tip de comunicare la distanță** (acoperă interceptarea, accesul, monitorizarea, colectarea sau înregistrarea comunicărilor efectuate prin telefon, sistem informatic sau prin orice alt mijloc de comunicare);
b) **accesul la un sistem informatic** (pătrunderea într-un sistem informatic sau mijloc de stocare a datelor informatice fie direct, fie de la distanţă, prin intermediul unor programe specializate ori prin intermediul unei reţele, în scopul de a identifica probe);
c) **supravegherea video, audio sau prin fotografiere** (fotografierea persoanelor, observarea sau înregistrarea conversaţiilor, mişcărilor ori a altor activităţi ale acestora);

d) **localizarea sau urmărirea prin mijloace tehnice** (folosirea unor dispozitive care determină locul unde se află persoana sau obiectul la care sunt ataşate);

e) **obţinerea datelor referitoare la tranzacţiile financiare ale unei persoane** (operaţiunile prin care se asigură cunoaşterea conţinutului tranzacţiilor financiare efectuate sau care urmează să fie efectuate prin intermediul unei instituții de credit sau al altei entități financiare, precum și obţinerea de la o instituție de credit sau de la altă entitate financiară de înscrisuri ori informaţii aflate în posesia acesteia referitoare la tranzacţiile sau operațiunile unei persoane);

f) **reţinerea, predarea sau percheziţionarea trimiterilor poştale** (verificarea, prin mijloace fizice sau tehnice, a scrisorilor, a altor trimiteri poştale sau a obiectelor transmise prin orice alt mijloc);

g) **utilizarea investigatorilor sub acoperire și a colaboratorilor** (folosirea unei persoane cu o altă identitate decât cea reală în scopul obţinerii de date şi informaţii cu privire la săvârşirea unei infracţiuni);

h) **participarea autorizată la anumite activități** (înseamnă comiterea unei fapte similare laturii obiective a unei infracțiuni de corupție, efectuarea de tranzacții, operațiuni sau orice fel de înțelegeri privind un bun sau privind o persoană despre care se bănuiește că ar fi dispărută, că este victima traficului de persoane ori a unei răpiri, efectuarea de operațiuni privind droguri, precum și prestarea unui serviciu, desfășurate cu autorizarea organului judiciar competent, în scopul obținerii de mijloace de probă);

i) **livrarea supravegheată** (o tehnică de supraveghere și cercetare prin care se permite intrarea, tranzitarea sau ieşirea de pe teritoriul ţării a unor bunuri în privinţa cărora există o suspiciune cu privire la caracterul ilicit al deţinerii sau obţinerii acestora, sub supravegherea ori cu autorizarea autorităţilor competente, în scopul investigării unei infracţiuni sau al identificării persoanelor implicate în săvârşirea acesteia);

j) **obţinerea datelor generate sau prelucrate de furnizorii de reţele publice de comunicaţii electronice** sau de furnizorii de servicii de comunicaţii electronice destinate publicului, altele decât conţinutul comunicaţiilor, reţinute de aceştia în temeiul legii speciale privind reţinerea datelor generate sau prelucrate de furnizorii de reţele publice de comunicaţii electronice și de furnizorii de servicii de comunicaţii electronice destinate publicului[22].

Există distincţii procedurale între metodele speciale de supraveghere şi tehnicile speciale de cercetare, precum şi condiţii de fond referitoare la tipul de infracţiune investigată. Supravegherea tehnică se poate dispune numai în cazul infracţiunilor considerate grave şi care sunt enumerate la articolul 139 alineatul (2). Celelalte tehnici, deşi respectă dispoziţiile referitoare la necesitatea de a le utiliza, pot fi dispuse indiferent de natura infracţiunii comise.

Supravegherea tehnică se dispune de judecătorul de drepturi şi libertăţi atunci când există o suspiciune rezonabilă cu privire la pregătirea sau săvârşirea unei infracţiuni enumerate mai jos, măsura este proporţională cu restrângerea drepturilor şi libertăţilor fundamentale, date fiind particularităţile cauzei, importanţa informaţiilor ori a probelor ce urmează a fi obţinute sau gravitatea infracţiunii şi probele nu ar putea fi obţinute în alt mod sau obţinerea lor ar presupune dificultăţi deosebite ce ar prejudicia ancheta ori există un pericol pentru siguranţa persoanelor sau a unor bunuri de valoare. Supravegherea tehnică se poate dispune în cazul infracţiunilor contra securităţii naţionale prevăzute de Codul penal şi de legi speciale, precum şi în cazul altor infracţiuni enumerate în mod special, inclusiv în cazul infracţiunilor care se săvârşesc prin sisteme informatice sau mijloace de comunicare electronică.

[22] A se vedea Decizia nr. 440 din 8 iulie 2014 a Curţii Constituţionale referitoare la excepţia de neconstituţionalitate a dispoziţiilor Legii nr. 82/2012 privind reţinerea datelor generate sau prelucrate de furnizorii de reţele publice de comunicaţii electronice şi de furnizorii de servicii de comunicaţii electronice destinate publicului, precum şi pentru modificarea şi completarea Legii nr. 506/2004 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul comunicaţiilor electronice şi ale art. 152 din Codul de procedură penală.

Supravegherea tehnică poate fi dispusă în cursul urmăririi penale, pe o durată de cel mult 30 de zile, la cererea procurorului, de judecătorul de drepturi şi libertăţi competent. În cazul în care apreciază că cererea este întemeiată, judecătorul de drepturi şi libertăţi emite mandatul de supraveghere tehnică (articolul 140 din CPP). Totuşi, procurorul poate autoriza, pe o durată de maximum 48 de ore, măsuri de supraveghere tehnică, având obligaţia de a sesiza, în termen de cel mult 24 de ore de la expirarea măsurii, judecătorul de drepturi şi libertăţi, înaintând totodată un proces-verbal de redare rezumativă a activităţilor de supraveghere tehnică efectuate şi dosarul cauzei.

În conformitate cu articolul 147 din CPP, reţinerea, predarea şi percheziţionarea trimiterilor poştale se poate dispune de judecătorul de drepturi şi libertăţi de la instanţa căreia i-ar reveni competenţa să judece cauza în primă instanţă sau de la instanţa corespunzătoare în grad acesteia în a cărei circumscripţie se află sediul parchetului din care face parte procurorul care a întocmit propunerea, cu privire la scrisorile, trimiterile poştale sau obiectele trimise ori primite de făptuitor, suspect, inculpat sau de orice persoană care este bănuită că primeşte ori trimite prin orice mijloc aceste bunuri de la făptuitor, suspect sau inculpat ori bunuri destinate acestuia, dacă:
a) există o suspiciune rezonabilă cu privire la pregătirea sau săvârşirea unei infracţiuni;
b) măsura este necesară şi proporţională cu restrângerea drepturilor şi libertăţilor fundamentale, date fiind particularităţile cauzei, importanţa informaţiilor sau a probelor ce urmează a fi obţinute ori gravitatea infracţiunii;
c) probele nu ar putea fi obţinute în alt mod sau obţinerea lor ar presupune dificultăţi deosebite ce ar prejudicia ancheta ori există un pericol pentru siguranţa persoanelor sau a unor bunuri de valoare.

Conservarea datelor informatice (art. 154)
Dacă există o suspiciune rezonabilă cu privire la pregătirea sau săvârşirea unei infracţiuni, în scopul strângerii de probe ori identificării făptuitorului, suspectului sau a inculpatului, procurorul care supraveghează sau efectuează urmărirea penală poate dispune conservarea imediată a anumitor date informatice, inclusiv a datelor referitoare la traficul informaţional, care au fost stocate prin intermediul unui sistem informatic şi care sunt în posesia sau sub controlul unui furnizor de reţele publice de comunicaţii electronice sau al unui furnizor de servicii de comunicaţii electronice destinate publicului, în cazul în acre există pericolul pierderii sau modificării acestora.

Conservarea se dispune de procuror din oficiu sau la cererea organului de cercetare penală, pe o durată de maximum 60 de zile, prin ordonanţă care trebuie să cuprindă menţionarea obligaţiei persoanei sau furnizorului de reţele publice de comunicaţii electronice sau a furnizorului de servicii de comunicaţii electronice destinate publicului de a conserva imediat datele informatice şi de a le menţine integritatea, în condiţii de confidenţialitate. Măsura conservării poate fi prelungită pe o durată de maxim 30 de zile.

În cazul în care datele referitoare la traficul informaţional se află în posesia mai multor furnizori de reţele publice de comunicaţii electronice sau furnizori de servicii de comunicaţii electronice destinate publicului, furnizorul în posesia sau sub controlul căruia se află datele informatice are obligaţia de a pune, de îndată, la dispoziţia organului de urmărire penală informaţiile necesare identificării celorlalţi furnizori, în vederea cunoaşterii tuturor elementelor din lanţul de comunicare folosit. Procurorul care supraveghează sau efectuează urmărirea penală poate , cu încuviinţarea prealabilă a judecătorului de drepturi şi libertăţi, să solicite unui furnizor de reţele publice de comunicaţii electronice ori unui furnizor de servicii de comunicaţii electronice destinate publicului transmiterea datelor conservate potrivit legii ori poate dispune ridicarea acestei măsuri. Judecătorul de drepturi şi libertăţi soluţionează cererile organelor de cercetare penală referitoare la transmiterea de date în termen de 48 de ore. Până la terminarea urmăririi penale, procurorul este obligat să încunoştinţeze, în scris, persoanele faţă de care se efectuează urmărirea penală şi ale căror date au fost conservate.

Strângerea probelor

Prin percheziţie în sistem informatic sau a unui suport de stocare a datelor informatice se înţelege procedeul de cercetare, descoperire, identificare şi strângere a probelor stocate într-un sistem informatic sau suport de stocare a datelor informatice, realizat prin intermediul unor mijloace tehnice şi proceduri adecvate, de natură să asigure integritatea informaţiilor conţinute de acestea (articolul 168 din CPP). În cursul urmăririi penale, judecătorul de drepturi şi libertăţi de la instanţa căreia i-ar reveni competenţa să judece cauza în primă instanţă sau de la instanţa corespunzătoare în grad acesteia poate dispune efectuarea unei percheziţii informatice, la cererea procurorului, atunci când pentru descoperirea şi strângerea probelor este necesară cercetarea unui sistem informatic sau a unui suport de stocare a datelor informatice. Cererea se soluţionează în camera de consiliu, fără citarea părţilor.

În cazul în care există o suspiciune rezonabilă cu privire la pregătirea sau săvârşirea unei infracţiuni şi sunt temeiuri de a se crede că un obiect ori un înscris poate servi ca mijloc de probă în cauză, organele de urmărire penală sau instanţa de judecată pot dispune persoanei fizice sau juridice în posesia căreia se află să le prezinte şi să le predea, sub luare de dovadă (art. 170 din CPP).

5.2.2 Criminalistică şi criptare

Codul român de procedură penală nu prevede în mod special expertiza criminalistică la distanţă. Cadrul general pentru dispunerea efectuării unei expertize sau pentru efectuarea unei constatări este prevăzut la articolul 172 din CPP. Efectuarea unei expertize se dispune când pentru constatarea, clarificarea sau evaluarea unor fapte sau împrejurări ce prezintă importanţă pentru aflarea adevărului în cauză este necesară şi opinia unui expert. De asemenea, dacă există pericolul dispariţiei probelor sau al schimbării unei situaţii de fapt, sau atunci când este necesară clarificarea urgentă a faptelor sau împrejurărilor unei cauze, organele de urmărire penală pot dispune prin ordonanţă efectuarea unei constatări. Aceasta este efectuată de un specialist care funcţionează în cadrul organelor judiciare sau de un specialist extern.

Criptarea asigură securitatea şi siguranţa transmiterii datelor informatice, dar există aspecte care sunt generate pentru structurile de aplicare a legii în efectuarea anchetelor, pentru identificarea comunicaţiilor sau a datelor informatice protejate de criptare, care sunt folosite de suspecţi. În cazul activităţilor investigative efectuate de structuri poliţieneşti specializate, identificarea datelor informatice sau a comunicaţiilor criptate are loc în cooperare cu posesorul acestora, în măsura în care acesta/aceasta doreşte acest lucru sau este de bună credinţă. Nu există dispoziţii legale referitoare la criptare prin care să se incrimineze lipsa cooperării posesorului sau circumstanţe agravante care să poată fi aplicate în astfel de situaţii.

Pentru soluţionarea cauzelor care implică criptarea datelor sau a comunicaţiilor, poliţia utilizează instrumente şi aplicaţii disponibile. Există şi o colaborare cu structurile specializate în acest domeniu din cadrul Serviciului Român de Informaţii. La nivelul poliţiei, aceste activităţi sunt anchetate de structura specializată în criminalitate informatică. Cooperarea este, de asemenea, posibilă cu sectorul privat în soluţionarea cauzelor specifice referitoare la criptare prin furnizarea sprijinului (aplicaţiilor) tehnic(e) autorităţilor publice. Cooperarea instituţională este efectuată pe baza cadrului juridic actual şi în temeiul acordurilor şi protocoalelor de cooperare. Institutul pentru Tehnologii Avansate (Serviciul Român de Informaţii) are structuri care desfăşoară activităţi de cercetare tehnică şi ştiinţifică în domenii precum informatica şi comunicaţiile. Conform protocoalelor de cooperare cu instituţiile competente şi pe baza documentelor de autorizare emise de organele judiciare, Institutul pentru Tehnologii Avansate, prin personal special desemnat, poate desfăşura activităţi de criminalistică.

Autorităţile române au devenit conştiente de unele probleme legate de criptare în cadrul constatărilor experţilor/ştiinţifice, există obiecte (dosare, volume de date etc.) cifrate extrem de complex, au fost identificaţi algoritmi digitali pentru care nu există atacuri eficiente în lipsa informaţiilor referitoare la parolă sau cheie. Chestiunea a fost abordată prin utilizarea instrumentelor disponibile pe piaţă şi prin dezvoltarea de noi instrumente.

Până acum nu s-a înregistrat o cooperare cu societăţi private de decriptare.

5.2.3 Probe electronice

Codul de procedură penală prevede o definiţie a probelor şi a mijloacelor de probă, precizând faptul că proba se obţine în procesul penal prin mijloace de probă şi este prezentată prin intermediul mijloacelor de probă prevăzută de lege.
Practica admite faptul că „probele electronice” (probele digitale) reprezintă orice element de fapt creat sau care există într-un mediu electronic (digital) care serveşte la constatarea existenţei sau inexistenţei unei infracţiuni, la identificarea persoanei care a săvârşit o infracţiune şi la stabilirea circumstanţelor necesare pentru corecta soluţionare a unei cauze. Conform articolului 100 din CPP, în cursul urmăririi penale, organul de urmărire penală strânge şi administrează probe, inclusiv probe electronice, atât în favoarea, cât şi în defavoarea suspectului sau a inculpatului, din oficiu sau la cerere.

Articolul 197 alin. (1) şi (2) din CPP prevede că obiectele care conţin sau poartă o urmă a faptei săvârşite sunt mijloace materiale de probă (de exemplu un HDD, CD, DVD, router, stick de memorie sau orice alt echipament), iar obiectele folosite pentru săvârşirea unei infracţiuni sunt corpuri delicte (de exemplu sistemul informatic folosit). Ţinând seama de natura specială a unui mijloc de probă care este produs, transmis sau păstrat într-un sistem informatic, CPP a stabilit norme speciale referitoare la modul în care se desfăşoară supravegherea tehnică, modul în care se efectuează o percheziţie informatică şi modul în care sunt predate sau păstrate date informatice.

Supravegherea tehnică (articolele 142-143)
Orice persoană autorizată care realizează activități de supraveghere tehnică are posibilitatea să asigure semnarea datelor rezultate din măsurile de supraveghere tehnică, utilizând o semnătură electronică bazată pe un certificat calificat eliberat de un furnizor de servicii de certificare acreditat.
Procurorul sau organul de cercetare penală întocmeşte un proces-verbal pentru fiecare activitate de supraveghere tehnică, în care sunt consemnate rezultatele activităţilor efectuate care privesc fapta ce formează obiectul cercetării sau contribuie la identificarea ori localizarea persoanelor, datele de identificare ale suportului care conţine rezultatul activităţilor de supraveghere tehnică, numele persoanelor la care se referă, dacă sunt cunoscute, sau alte date de identificare, precum şi, după caz, data şi ora la care a început activitatea de supraveghere tehnică şi data şi ora la care s-a încheiat.

Orice persoană autorizată care realizează copii ale unui suport de stocare a datelor informatice care conţine rezultatul activităţilor de supraveghere tehnică are posibilitatea să verifice integritatea datelor incluse în suportul original şi, după efectuarea copiei, să semneze datele incluse în aceasta, utilizând o semnătură electronică extinsă bazată pe un certificat calificat eliberat de un furnizor de servicii de certificare acreditat şi care permite identificarea neambiguă a persoanei autorizate, aceasta asumându-şi astfel responsabilitatea în ceea ce priveşte integritatea datelor.

Percheziţia informatică (articolul 168)

Prin percheziţie în sistem informatic sau a unui suport de stocare a datelor informatice se înţelege procedeul de cercetare, descoperire, identificare şi strângere a probelor stocate într-un sistem informatic sau suport de stocare a datelor informatice, realizat prin intermediul unor mijloace tehnice şi proceduri adecvate, de natură să asigure integritatea informaţiilor conţinute de acestea. În vederea executării percheziţiei dispuse, pentru asigurarea integrităţii datelor informatice stocate pe obiectele ridicate, procurorul dispune efectuarea de copii. Dacă ridicarea obiectelor care conţin datele informatice ar afecta grav desfăşurarea activităţii persoanelor care deţin aceste obiecte, procurorul poate dispune efectuarea de copii, care servesc ca mijloc de probă.

Predarea obiectelor, înscrisurilor sau a datelor informatice (art. 170)

În cazul în care există o suspiciune rezonabilă cu privire la pregătirea sau săvârşirea unei infracţiuni şi sunt temeiuri de a se crede că un obiect ori un înscris poate servi ca mijloc de probă în cauză, organele de urmărire penală sau instanţa de judecată pot dispune persoanei fizice sau juridice în posesia căreia se află să le prezinte şi să le predea, sub luare de dovadă.

Nu există norme speciale cu privire la admisibilitatea probelor electronice, mai ales dacă acestea sunt obţinute în afara României. Normele obișnuite se aplică indiferent dacă probele sunt colectate la nivel național sau prin asistență judiciară reciprocă.

5.3 Apărarea drepturilor omului/libertăţilor fundamentale

Comunicarea prin internet şi alte mijloace de comunicare este protejată şi garantată de dreptul român. În acelaşi timp, datele cu caracter personal sunt protejate de legislaţia română în vigoare, iar diseminarea lor ilegală pe internet se sancţionează cu amendă.

Constituţia României garantează o serie de drepturi şi libertăţi fundamentale, printre care dreptul la viaţa intimă, familială şi privată (articolul 26); inviolabilitatea domiciliului (articolul 27); secretul corespondenţei (articolul 28) şi libertatea de exprimare (articolul 30). Respectivele principii constituţionale sunt reflectate, de asemenea, în legislaţia penală, inclusiv Codul de procedură penală şi Codul penal, prin incriminarea faptelor care încalcă dreptul la domiciliu şi viaţă privată (capitolul IX).

Ţinând seama de apartenenţa României la Consiliul Europei şi la Uniunea Europeană, reforma în materie penală în România a încercat să alinieze legislaţia în materie penală la exigenţele şi cerinţele Convenţiei europene pentru apărarea drepturilor omului şi a libertăţilor fundamentale, precum şi ale altor instrumente internaţionale şi comunitare relevante. Prin urmare, Legea nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date (Monitorul Oficial nr. 790, 12 decembrie 2001) prevede cadrul general pentru protecţia persoanelor, scopul fiind acela de a garanta şi proteja libertăţile fundamentale şi libertăţile persoanelor, în special dreptul la viaţă privată, familială, cu privire la prelucrarea datelor cu caracter personal. Activităţile ilegale legate de criminalitatea informatică sunt incriminate de legislaţia în vigoare.

Obiectivele noului Cod de procedură penală au inclus protecţia unitară a drepturilor omului şi a libertăţilor garantate de Constituţie şi de instrumentele juridice internaţionale, precum şi reglementarea adecvată în legislaţia penală a obligaţiilor internaţionale asumate de România. În ceea ce priveşte respectarea dreptului la viaţă privată şi corespondenţă, Codul de procedură penală prevede norme procesuale referitoare la metode speciale de supraveghere şi

cercetare, care îndeplinesc criteriul accesibilităţii, predictibilităţii şi proporţionalităţii. Atunci când se autorizează astfel de măsuri, dreptul penal impune existenţa unei suspiciuni rezonabile cu privire la pregătirea unei infracţiuni, respectarea principiului subsidiarităţii - fiind de menţionat caracterul excepţional al imixtiunii în viaţa privată - precum şi a principiului proporţionalităţii măsurii în raport cu restrângerea exercitării dreptului la viaţă privată, legat de specificitatea cauzei, importanţa informaţiilor sau a probelor care urmează a fi obţinute, sau de gravitatea infracţiunii.

Având acelaşi obiectiv de a garanta dreptul prevăzut la articolul 8 din Convenţia europeană pentru apărarea drepturilor omului şi a libertăţilor fundamentale, Codul de procedură penală prevede, ca principiu, obligaţia procurorului ca, după încetarea măsurii de supraveghere tehnică, să informeze, în scris, pe fiecare subiect al unui mandat despre măsura de supraveghere tehnică ce a fost luată în privinţa sa.

5.4 Competența

5.4.1 Principii care se aplică pentru anchetarea criminalităţii informatice

Codul penal face trimitere la principiul personalităţii legii penale, al realităţii şi al universalităţii legii penale. Legea penală română se aplică infracţiunilor săvârşite pe teritoriul României, prin care se înţelege întinderea de pământ, marea teritorială şi apele cu solul, subsolul şi spaţiul aerian, cuprinse între frontierele de stat. Infracţiunea se consideră săvârşită pe teritoriul României şi atunci când pe acest teritoriu ori pe o navă sub pavilion românesc sau pe o aeronavă înmatriculată în România s-a efectuat un act de executare, de instigare sau de complicitate ori s-a produs, chiar în parte, rezultatul infracţiunii.

Legea penală română se aplică, de asemenea, infracţiunilor săvârşite în afara teritoriului României de către un cetăţean român sau de o persoană juridică română, dacă pedeapsa prevăzută de legea română este detenţiunea pe viaţă ori închisoarea mai mare de 10 ani. În celelalte cazuri, legea penală română se aplică infracţiunilor săvârşite în afara teritoriului României de către un cetăţean român sau de o persoană juridică română, dacă fapta este prevăzută ca infracţiune şi de legea penală a ţării unde a fost săvârşită ori dacă a fost comisă într-un loc care nu este supus jurisdicţiei niciunui stat. Punerea în mişcare a acţiunii penale se face cu autorizarea prealabilă a procurorului general al parchetului de pe lângă curtea de apel în a cărei rază teritorială se află parchetul mai întâi sesizat sau, după caz, a procurorului general al parchetului de pe lângă Înalta Curte de Casaţie şi Justiţie.

În acelaşi timp, legea penală română se aplică infracţiunilor săvârşite în afara teritoriului ţării de către un cetăţean străin sau o persoană fără cetăţenie, contra statului român, contra unui cetăţean român ori a unei persoane juridice române. Punerea în mişcare a acţiunii penale se face cu autorizarea prealabilă a procurorului general al Parchetului de pe lângă Înalta Curte de Casaţie şi Justiţie şi numai dacă fapta nu face obiectul unei proceduri judiciare în statul pe teritoriul căruia s-a comis. Legea penală română se aplică şi altor infracţiuni săvârşite în afara teritoriului României de un cetăţean străin sau o persoană fără cetăţenie, care se află de bunăvoie pe teritoriul României, în următoarele cazuri:
a) s-a săvârşit o infracţiune pe care statul român şi-a asumat obligaţia să o reprime în temeiul unui tratat internaţional, indiferent dacă este prevăzută sau nu de legea penală a statului pe al cărui teritoriu a fost comisă;
b) s-a cerut extrădarea sau predarea infractorului şi aceasta a fost refuzată.

Nicio persoană nu poate fi urmărită sau judecată pentru săvârşirea unei infracţiuni atunci când faţă de acea persoană s-a pronunţat anterior o hotărâre penală definitivă cu privire la aceeaşi faptă, chiar şi sub altă încadrare juridică.

5.4.2 Norme aplicabile în caz de conflicte de competenţă şi trimiterea la Eurojust

Decizia-cadru 2009/948/JAI a Consiliului din 30 noiembrie 2009 privind prevenirea și soluționarea conflictelor referitoare la exercitarea competenței în cadrul procedurilor penale a fost transpusă în legislaţia română pe baza Legii nr. 300/2013. Totuşi, autorităţile române nu au raportat cazuri în care să fi apărut această chestiune.

5.4.3 Competenţa pentru fapte de criminalitate informatică săvârşite în „cloud”

Aceleaşi norme se aplică pentru a investiga infracţiuni săvârşite în „cloud” ca şi infracţiunilor săvârşite în afara teritoriului României de un cetăţean român, de un cetăţean străin sau de o persoană fără cetăţenie împotriva statului român, a unui cetăţean român sau a unei persoane juridice române (a se vedea punctul 5.4.1).

5.4.4 Percepţia României cu privire la cadrul juridic pentru combaterea criminalităţii informatice

Cadrul juridic naţional face posibilă gestionarea cauzelor referitoare la infracţiuni săvârşite în străinătate. Totuşi, principalul obstacol în calea investigării infracţiunilor săvârşite în afara teritoriului naţional este prezentarea probelor, dat fiind faptul că urmele specifice acestor infracţiuni se găsesc, parţial, pe teritoriul unui alt stat. Obţinerea probelor prin comisii rogatorii este costisitoare, în special în ceea ce priveşte timpul necesar pentru desfăşurarea anumitor activităţi. Mai mult, obstacolele pot include, de asemenea, obţinerea datelor de identificare a adreselor IP, conţinutul comunicărilor (căsuța poștală) și supravegherea tehnică și fizică a persoanelor. Deşi legislaţia statelor s-a schimbat ca rezultat al adoptării de instrumente de cooperare internaţională, inclusiv a Convenţiei de la Budapesta, structura instituţiilor care răspund de executarea cererilor de asistenţă judiciară internaţională nu a suferit schimbări reale, nici în ceea ce priveşte numărul real de persoane desemnate per activitate, nici în ceea ce priveşte formarea personalului referitor la noi tipuri de infracţiuni, precum criminalitatea informatică. Autorităţile române au subliniat, de asemenea, necesitatea de a identifica soluţii comune pentru strângerea de probe electronice, precum accesarea spațiilor de stocare a datelor din „cloud” sau executarea de percheziţii autorizate ale acestor spaţii.

5.5 Concluzii

- România a semnat și a ratificat Convenția privind criminalitatea informatică, fiind una dintre primele țări din Europa care a făcut acest lucru. Convenția a intrat în vigoare pentru România la 1 septembrie 2004. Modul în care România a pus în aplicare convenția este utilizat de Consiliul Europei drept lege-model în cadrul a numeroase activități de asistență tehnică. Participarea activă la T-CY și implicarea în promovarea convenției au avut drept rezultat decizia de a institui C-PROC în România. În opinia echipei de evaluare, instituirea C-PROC consolidează sprijinul activ al României pentru promovarea Convenției drept un instrument global.

- Decizia-cadru 2005/222/JAI a Consiliului privind atacurile împotriva sistemelor informatice a fost pusă în aplicare în dreptul român. Punerea în aplicare a Convenției privind criminalitatea informatică a facilitat foarte mult transpunerea Directivei 2013/40/UE privind atacurile împotriva sistemelor informatice. Autoritățile române au raportat că legislația română este în concordanță cu directiva.

- Directiva 2011/93/UE a Parlamentului European și a Consiliului privind combaterea abuzului sexual asupra copiilor, a exploatării sexuale a copiilor și a pornografiei infantile a fost pusă în aplicare în mare măsură.

- Combaterea fraudei cu carduri de credit este abordată în Codul penal român.

- În Codul penal nu există o definiție a criminalității informatice, dar aceasta este definită în Strategia națională de securitate cibernetică. Prin urmare, tendința este de a utiliza definiția din Strategia națională de securitate cibernetică, care se referă la orice fapte prevăzute de legea penală sau de alte dispoziții penale și care prezintă pericol social, sunt săvârșite cu vinovăție, prin intermediul ori asupra infrastructurilor cibernetice. În consecință, părțile interesate din domeniul criminalității informatice pot să nu împărtășească o înțelegere comună amplă a aceluiași concept.

- În februarie 2014 au intrat în vigoare noul Cod penal și noul Cod de procedură penală. Modificările care privesc criminalitatea informatică sunt, printre altele, ademenirea unei persoane în vederea săvârșirii de acte sexuale cu un minor și efectuarea de operațiuni financiare în mod fraudulos. Metodele de cercetare și activitățile conexe legate de domeniul informaticii sunt prevăzute în Codul de procedură penală. Cinci dintre cele nouă tehnici de cercetare sunt definite drept supraveghere electronică, aceasta putând fi impusă numai în cazul unor infracțiuni considerate grave sau care necesită măsuri specifice. De asemenea, sunt descrise alte activități legate de domeniul informaticii, cum ar fi perchezițiile informatice, păstrarea datelor informatice și, în special, utilizarea semnăturilor electronice.

- În pofida cooperării strânse dintre poliție și Serviciul Român de Informații și a eforturilor acestora în materie de cunoștințe de specialitate, formare și dezvoltare de instrumente tehnice, criptarea a fost identificată drept unul dintre aspectele care împiedică desfășurarea cu succes a cercetărilor poliției. În opinia evaluatorilor, lipsa cooperării cu societățile private la decriptarea datelor și lipsa unor dispoziții legale pentru incriminarea, cel puțin în cazul infracțiunilor grave, a împotrivirii persoanelor suspectate de a coopera la deschiderea fișierelor criptate pe computerele lor ar putea fi menționate ca motive care creează respectivele piedici. Un mod de abordare pentru sporirea eficienței cercetărilor ar putea fi introducerea conceptului de ordin de decriptare, care ar trebui elaborat la nivel european pe baza celor mai bune practici ale statelor membre.

- România recunoaște faptul că autoritățile de aplicare a legii se confruntă cu dificultăți în ceea ce privește prezentarea probelor - inclusiv obținerea datelor de identificare a adreselor IP și a conținutului comunicărilor (căsuța poștală) - în cazul infracțiunilor săvârșite în afara teritoriului național, nu în ultimul rând din cauza implicațiilor transfrontaliere ale criminalității informatice. O problemă similară cu care se confruntă autoritățile de aplicare a legii se referă la accesarea spațiilor de stocare a datelor din „cloud”, precum și la utilizarea probelor colectate în străinătate.

- Dreptul român impune o obligație de a cerceta infracțiunile săvârșite pe teritoriul României. În plus, Codul penal român prevede temeiuri de jurisdicție pentru multe infracțiuni specifice săvârșite în afara României. Codul penal român stabilește jurisdicția cu privire la aproape toate infracțiunile informatice atunci când sunt săvârșite de cetățeni români în străinătate.

- În timpul vizitei la fața locului, autoritățile române au indicat probleme legate de lipsa unor dispoziții la nivel european privind administrarea păstrării datelor. Întrucât Curtea de Justiție a Uniunii Europene a declarat nulă Directiva 2006/24/CE a Parlamentului European și a Consiliului privind păstrarea datelor, acest lucru a afectat dispoziții esențiale din Legea nr. 82/2012 de transpunere a directivei în legislația română. Drept rezultat, Curtea Constituțională a României a admis excepția de neconstituționalitate privind Legea nr. 82/2012 și a decis că dispozițiile acesteia sunt neconstituționale. A fost înființat un grup de lucru pentru a găsi soluții la această situație. O nouă lege privind securitatea cibernetică se află în curs de pregătire. În opinia evaluatorilor, ar trebui luate măsuri la nivelul UE pentru a acoperi lacuna care a rezultat în urma hotărârii Curții de Justiție, întrucât probleme similare ar putea apărea în alte state membre ale UE ca urmare a punerii în aplicare a directivei declarate nule.

5 ASPECTE OPERAŢIONALE

5.1 Atacurile cibernetice

6.1.1 Natura atacurilor cibernetice

Nu există statistici privind atacurile cibernetice asupra sistemelor informatice ale autorităților publice, dar există statistici generale privind criminalitatea informatică. Instituțiile publice (cum ar fi instanțele judecătorești, Ministerul Public și poliția) își colectează propriile statistici privind cercetările și cauzele penale (a se vedea mai multe detalii în capitolul 3.3).

În 2013, CERT-RO a primit următoarele alerte:
1. Numărul total de alerte automate primite: 43 231 149;
2. Numărul total de adrese IP unice extrase din toate alertele: 2 213 426.

Majoritatea alertelor analizate de CERT-RO, din segmentele alertelor automate sau individuale, se referă la entități din România, victime ale atacurilor/atacatorilor care au profitat de obicei de vulnerabilități tehnice. Principalul obiectiv al atacurilor era de a infecta sistemele informatice cu diverse aplicații rău-intenționate pentru a le integra în diferite tipuri de botneturi (*zombies*). Aceste sisteme compromise (victime) sunt adesea utilizate cu rol de „proxy" pentru desfășurarea altor atacuri asupra unor ținte din afara României. Există avantaje semnificative pentru atacatorul care utilizează o astfel de abordare, de exemplu abilitatea de a-și ascunde adevărata identitate și, de asemenea, de a utiliza un număr mare de computere (în funcție de numărul de sisteme informatice infectate) pentru a lansa atacurile. Totodată, pe baza analizei tipurilor de malware specifice spațiului cibernetic român și a tipurilor de sisteme compromise, reiese faptul că cele mai multe atacuri sunt îndreptate împotriva unor sisteme învechite, depășite moral, fără posibilități native de securizare (de ex. sisteme afectate de Conficker) sau care nu sunt actualizate cu ultimele patch-uri/actualizări de securitate.

Potrivit datelor furnizate de autoritățile române, entități române au devenit din ce în ce mai frecvent ținta amenințărilor de tip APT, respectiv atacuri cibernetice cu un grad ridicat de complexitate, lansate de grupuri care au capacitatea și motivația de a ataca în mod persistent o țintă în scopul obținerii anumitor beneficii (de obicei, acces la informații sensibile).

6.1.2 Mecanismul de răspuns la atacurile cibernetice

România aplică principiul legalității în ceea ce privește cercetarea infracțiunilor. Potrivit articolului 3 din Codul de procedură penală, funcțiile judiciare se exercită din oficiu, în afară de cazul când, prin lege, se dispune altfel. Prin urmare, pentru o gamă largă de infracțiuni, printre care și criminalitatea informatică, urmărirea penală se desfășoară din oficiu. Cu toate acestea, în anumite circumstanțe, procurorul poate decide să renunțe la urmărirea penală în temeiul articolului 314 alineatul (1) litera (b) din Codul de procedură penală (în cazul infracțiunilor pentru care legea prevede pedeapsa amenzii sau pedeapsa închisorii de cel mult șapte ani).

Denunțarea activităților ilegale reprezintă o obligație pentru cei care au cunoștință despre astfel de activități, inclusiv atacurile cibernetice. În temeiul articolului 16 din Legea nr. 365/2002 privind comerțul electronic, furnizorii de servicii sunt obligați să informeze de îndată autoritățile publice competente despre activitățile cu aparență nelegală desfășurate de destinatarii serviciilor lor sau despre informațiile cu aparență nelegală furnizate de respectivii destinatari [articolul 16 alineatul (1)]. De asemenea, furnizorii de servicii sunt obligați să întrerupă transmiterea într-o rețea de comunicații sau stocarea informației furnizate de un destinatar al serviciului respectiv, în special prin eliminarea informației sau blocarea accesului la aceasta, accesul la o rețea de comunicații sau prestarea oricărui alt serviciu al societății informaționale, dacă aceste măsuri au fost dispuse de o autoritate publică [articolul 16 alineatul (3)]. Un furnizor de servicii care încalcă condițiile stabilite la articolul 16 alineatele (1)-(3) din Legea nr. 365/2002 poate fi sancționat cu amendă.

Cu toate acestea, dreptul național nu prevede o atribuție specifică pentru operatorii de infrastructuri critice și operatorii sistemelor informatice. Absența unor dispoziții legale specifice privind responsabilitățile referitoare la notificarea, răspunsul, combaterea și eliminarea efectelor incidentelor de securitate de către autoritățile publice sau entitățile private, absență care are efectul de a aduce atingere răspunsului în timp real la astfel de incidente, reprezintă una dintre principalele dificultăți raportate de autoritățile române în ceea ce privește răspunsul la incidentele de securitate cibernetică. În acest context, furnizorii de servicii internet răspund uneori cererilor autorităților publice, iar alteori susțin că se vor produce pierderi materiale sau costuri sporite în cazul în care dau curs unor astfel de cereri.

În cazul în care există indicii clare ale unor încălcări ale legii, furnizorii de servicii internet dau curs cererilor statului, dar uneori simpla întârziere în furnizarea răspunsurilor la cereri generează efecte nedorite. Totuși, echipa de evaluare a fost informată că proiectul de lege privind securitatea cibernetică reglementează conceptul de „infrastructuri cibernetice de interes național" (ICIN), precum și atribuțiile care sunt de competența tuturor deținătorilor de astfel de infrastructuri privind asigurarea securității rețelei și diminuarea efectelor atacurilor cibernetice.

Denunțarea activităților ilegale (inclusiv a atacurilor cibernetice) poate fi realizată direct, prin fax, telefon, e-mail sau alte mijloace de comunicare, către parchetele sau secțiile de poliție specializate în criminalitatea informatică. Poliția a creat un site internet pentru primirea sesizărilor online referitoare exclusiv la criminalitatea informatică[23]. Aceste sesizări acoperă toate tipurile de infracțiuni informatice. Printre principalele dificultăți raportate referitoare la activitatea de răspuns la incidente s-a numărat lipsa unor reglementări juridice explicite privind responsabilitățile pentru notificarea, răspunsul, prevenirea și atenuarea incidentelor de securitate cibernetică de către instituțiile publice sau societățile din sectorul privat. Cetățenii au acceptat instrumentul, sute de incidente fiind denunțate prin intermediul site-ului, lucru care, după verificare, poate constitui baza pentru cercetările penale sau poate constitui sursa de informații pentru *intelligence*. De asemenea, poliția a elaborat un set de unsprezece proceduri-standard de operare care sprijină punerea în aplicare a legislației privind criminalitatea informatică, oferind, așadar, un compendiu armonizat de practici pentru utilizarea de către toate unitățile de poliție atunci când cercetează infracțiuni informatice.

Printre principalele obstacole cu care autoritățile române se confruntă atunci când răspund la un atac cibernetic se numără cele referitoare la provocările reprezentate de noile dispozitive TIC, lipsa unei legislații privind păstrarea datelor, probele stocate în străinătate în diverse sisteme informatice, serviciile anonime, soluțiile de criptare, perioada scurtă disponibilă pentru analiza datelor și lipsa unui răspuns de la anumiți deținători/proprietari ai sistemelor informatice. Cu toate acestea, în opinia evaluatorilor, simplificarea utilizării SNSC pentru discutarea incidentelor, tendințelor și evoluțiilor cu reprezentanții sectorului privat ar putea facilita cooperarea cu sectorul privat.

[23] www.efrauda.ro.

6.2 Măsuri împotriva pornografiei infantile și a abuzului sexual asupra copiilor online

6.2.1 Baze de date informatice de identificare a victimelor și măsuri de evitare a revictimizării

Potrivit autorităților române, au fost create baze de date speciale utilizând aplicațiile informatice Netclean Analyze și C4ALL, aceste aplicații fiind în prezent folosite pentru analiza imaginilor și a înregistrărilor video care rezultă din cercetări. Aceste baze de date conțin semnături ale HASH MD 5 și PhotoDNA ale fișierelor analizate, organizate în patru categorii, în funcție de un standard de categorie stabilit prin metodologia cercetării pornografiei infantile prin intermediul sistemelor informatice. De asemenea, poliția stochează fișiere imagine și video care reprezintă probe ale pornografiei infantile rezultate în urma unor cercetări specifice. Furnizorii de servicii internet au obligația de a înlătura materialele ilegale implicând minori pentru a evita revictimizarea.

6.2.2 Măsuri de combatere a exploatării sexuale/abuzului sexual online, a sextingului și a hărțuirii cibernetice (*cyber-bullying*)

În temeiul Codului penal, România incriminează următoarele fapte referitoare la exploatarea sexuală/abuzul sexual online, sextingul, hărțuirea cibernetică (*cyber-bullying*):

- traficul de minori (articolul 211 din Codul penal);
- exploatarea unei persoane (articolul 182 din Codul penal);
- violul (articolul 218 din Codul penal);
- agresiunea sexuală (articolul 219 din Codul penal);
- actul sexual cu un minor (articolul 220 din Codul penal);
- coruperea sexuală a minorilor (articolul 221 din Codul penal);
- hărțuirea (articolul 208 din Codul penal);
- racolarea minorilor în scopuri sexuale (articolul 222 din Codul penal);
- pornografia infantilă (articolul 374 din Codul penal).[24]

[24] Conținutul acestora a fost introdus în anexa D.

6.2.3 Măsuri de prevenire a turismului sexual, a spectacolelor pornografice cu implicarea copiilor și a altor fapte

România asigură transpunerea articolului 21 din Directiva 2011/93/UE prin incriminarea, în Codul penal, a persoanelor care, cu intenție, determină o altă persoană să săvârșească o faptă prevăzută de legea penală (articolul 47 – Instigatorul) și/sau care, cu intenție, înlesnesc sau ajută în orice mod la săvârșirea unei fapte prevăzute de legea penală sau care promit că vor tăinui bunurile provenite din săvârșirea infracțiunii sau că vor favoriza pe făptuitor, chiar dacă, după săvârșirea faptei, promisiunea nu este îndeplinită (articolul 48 – Complicele).

Autoritățile române au raportat că în decursul ultimilor ani s-au înregistrat cazuri de cetățeni străini condamnați în propriile lor țări pentru pornografie infantilă săvârșită pe internet, care, ulterior, au venit în România și au desfășurat activități de racolare a minorilor și de abuz sexual asupra minorilor. Identificarea și cercetarea respectivelor persoane au fost desfășurate pe baza informațiilor deținute sau a notificărilor primite de la autoritățile străine. Atunci când sunt primite/există date sau informații despre persoane care călătoresc în România în scopul săvârșirii unor fapte de exploatare sexuală a minorilor, respectivele persoane sunt monitorizate pentru a stabili dacă ele călătoresc în scopul săvârșirii unor infracțiuni și pentru a preveni eventuale activități infracționale. Activitățile de monitorizare sunt desfășurate, printre altele, cu ajutorul structurilor poliției locale, cu notificarea țărilor de destinație ale persoanelor suspectate, după caz. Ținând seama de gradul înalt de dificultate pe care îl presupune dovedirea acestui tip de exploatare sexuală a minorilor, unitatea specializată a poliției desfășoară activități specifice în mediul online pentru a identifica și cerceta activitatea infracțională a persoanelor care săvârșesc astfel infracțiuni.

Au fost luate următoarele măsuri pentru a preveni pornografia infantilă online:

- Ministerul Justiției administrează un site internet pe care sunt publicate detaliile liniei telefonice (telverde) pentru informarea victimelor infracțiunilor, după cum urmează: 0800 800 886, de luni până vineri, între orele 09.00 - 17.00.

- Centrul de informare și consiliere Internet Helpline, înființat în cadrul proiectului Safe Internet, oferă un număr de telefon gratuit (031 80 80 000) și numere la tarif normal (0744 300 476, 0762 639 300, 0722 753 744).
- Complexitatea mediului școlar a făcut necesară crearea unui parteneriat educațional, un caz de bune practici fiind cooperarea dintre Ministerul Educației Naționale și Asociația Telefonul Copilului. Centrul de intermediere telefonică, care furnizează servicii sociale, axat pe copii, dispune de un număr de telefon gratuit de asistență, numărul unic european de asistență pentru copii, 116111.

Ministerul Educației Naționale colaborează cu Asociația Telefonul Copilului la punerea în practică a Strategiei Ministerului Educației cu privire la reducerea fenomenului de violență în unitățile de învățământ preuniversitar. Această cooperare are drept scop monitorizarea, combaterea și reducerea crizei din școli, adesea concretizată prin manifestări violente. Copiii și părinții pot semnala problemele cu care se confruntă prin e-mail, la adresa: telefonulcopilului@gmail.com. În plus, numărul unic european de asistență pentru copii, 116111, este afișat în fiecare școală într-un loc vizibil - aproape de intrarea elevilor. Asociația Telefonul Copilului oferă sprijin copiilor care au nevoie de îngrijire și de protecție, copiilor ale căror drepturi au fost încălcate și părinților care au nevoie de consiliere, orientând problemele semnalate de instituții și organisme și oferind consiliere psihologică și educațională. Centrul de intermediere telefonică gratuit facilitează comunicarea dintre Ministerul Educației Naționale și beneficiarii educației (elevi, părinți, entități ale societății civile), promovând inițiativele și politicile în materie de educație ale ministerului.

- *Sigur.Info*

Programul național *Sigur.Info* este multianual și este pus în practică de Organizația Salvați Copiii din România, în parteneriat cu Positive Media Iași și cu Centrul FOCUS - Centrul Român pentru Copii Dispăruți și Exploatați Sexual, cu finanțare din partea Comisiei Europene (Safer Internet). Următoarele instituții și organizații s-au implicat în dezvoltarea programului: Ministerul Educației Naționale, Ministerul pentru Societatea Informațională, Autoritatea Națională pentru Administrare și Reglementare în Comunicații, Asociația Națională a Internet Service Providerilor, Poliția Română, Autoritatea Națională pentru Protecția Drepturilor Copilului și Adopție, Microsoft, UPC, Orange, Vodafone, Cosmote, Kaspersky Lab, ECDL etc.

Scopul programului este de a promova siguranța pe internet prin activități multiple, organizate pe trei niveluri:

1. Conștientizare - sporirea gradului de conștientizare și educarea cu privire la beneficiile utilizării noilor tehnologii și măsurile de prevenire a riscurilor disponibile pe internet;
2. O linie de consiliere (helpline) - informare și consiliere permanentă pentru copii și adulți;
3. O linie de raportare (hotline) - pentru raportarea către autorități a conținutului ilegal.

Așadar, au fost dezvoltate atât instrumente online (jocuri, anunțuri publicitare, înregistrări video), cât și offline (broșuri specifice grupului țintă: copii, adolescenți, cadre didactice, părinți). De asemenea, au fost dezvoltate instrumente/resurse în cadrul altor proiecte (de exemplu, proiectul Tineri în Siguranță pe Internet, materiale video ale CEOP traduse etc.). Programul național *Sigur.Info* s-a dovedit a avea un rol important în sporirea gradului de conștientizare de către copii, părinți și cadre didactice a beneficiilor/avantajelor utilizării internetului și a noilor tehnologii online, precum și a pericolelor/riscurilor asociate acestora, prin desfășurarea de campanii naționale de promovare a siguranței copiilor pe internet și atunci când utilizează telefoane mobile; de asemenea, programul s-a dovedit deosebit de eficient în activarea unor parteneriate efective între instituțiile menționate anterior. Până în prezent, de la începutul punerii sale în aplicare, programul a implicat peste 650 de voluntari în activități, informând peste 43 000 de părinți și cadre didactice și 98 000 de copii cu privire la beneficiile și riscurile pe care le presupune o utilizare nesupravegheată a internetului de către minori.

- *Ghidul școlar*

În februarie 2014, în România a fost lansat primul ghid școlar destinat utilizării sigure și eficiente a internetului, cu scopul de a forma cadrele didactice pentru a-l utiliza în cadrul INSAFE, *European Safer Internet Network* (Programul *Safer Internet Plus* al Comisiei Europene). Ghidul școlar conține atât informații teoretice, cât și aplicații practice pentru a promova utilizarea în siguranță a internetului de către elevi. Scopul acestui ghid este de a furniza resurse ușor de înțeles cadrelor didactice și adulților care doresc să lucreze cu copiii și tinerii pe tematica utilizării sigure și eficiente a internetului. Aspectele teoretice sunt întărite de aplicații practice care nu necesită utilizarea calculatorului sau tehnologiilor avansate. Ghidul cuprinde diferite teme (conținut ilegal, hărțuirea cibernetică, protecția datelor cu caracter personal etc.), recomandări (pagini privind rolul școlilor, consilierea cadrelor didactice), activități în sala de clasă (introducere tematică, un set de lecții, concluzii, materiale suplimentare pentru copii/părinți) și include o componentă de evaluare (evaluarea activităților desfășurate în sala de clasă, chestionare).

- *Safernet.ro*

Cealaltă inițiativă demnă de menționat este Safernet.ro, un exemplu de site internet care își propune să asigure o modalitate sigură de raportare rapidă a activităților de pornografie infantilă desfășurate pe internet. Site-ul este administrat de poliție, în parteneriat cu un ONG.

Deși există atât de multe inițiative și atât de multe organizații implicate, în opinia poliției, rezultatele au demonstrat utilitatea acestei cooperări.

6.2.4 Actori și măsuri de combatere a site-urilor internet care conțin sau diseminează pornografie infantilă

Potrivit articolului 25 alineatul (2) din Directiva 2077/93/UE, măsura blocării este opțională. Dacă site-urile internet au conținut ilegal, acestea pot fi blocate sau eliminate de furnizorii de servicii internet care găzduiesc respectivul conținut, după cum dispune legea, pe baza unei cereri făcute de organismul competent. În temeiul legii române, poliția le solicită furnizorilor de servicii internet din România să elimine materialele ilegale cu minori, după verificarea acestora potrivit unor proceduri speciale. În cazurile în care se descoperă că imaginile sunt găzduite de furnizori de servicii din alte state, sunt informate autoritățile judiciare din respectivele țări.

Cu toate acestea, autoritățile române au informat că în prezent nu sunt folosite instrumente specifice pentru a filtra accesul la site-uri care găzduiesc materiale ilegale implicând minori. Totuși, odată ce pe un anumit site este descoperit conținut ilegal, accesul la site-ul respectiv este blocat. Autoritățile competente care pot autoriza blocarea accesului și eliminarea materialelor ilegale implicând minori sunt poliția și parchetul sau, după caz, instanța judecătorească a cărei competență în materie a fost stabilită prin dispozițiile legale în vigoare. Sectorul privat este responsabil pentru punerea în aplicare a măsurilor luate de autoritățile competente sau prin blocarea sau eliminarea conținutului ilegal. În general, furnizorii de servicii nu sunt responsabili pentru conținut în cazul serviciilor pe care le furnizează; persoana care a închiriat sau care utilizează serviciul este responsabilă pentru conținut.

Totuși, dacă furnizorii de servicii au cunoștință de orice conținut ilegal, aceștia dispun eliminarea conținutului respectiv și raportează acest lucru autorităților competente, în vederea cercetării. În practică, această situație constă în verificarea sursei site-ului internet - dacă aceasta ține de jurisdicția națională - și a naturii ilegale a conținutului prezentat, după care furnizorului de servicii i se transmite o solicitare de a aplica imediat măsura dispusă (blocare, eliminare etc.).

Nu există proceduri de urgență separate, însă există puncte de contact pentru principalii furnizori de servicii care sunt utilizate în astfel de cazuri. Autoritățile române au arătat faptul că, în cazul în care sectorul privat raportează astfel de activități, autoritățile competente dispun imediat măsurile necesare și cercetarea cazului, în funcție de natura conținutului ilegal. În cazul în care serverul care găzduiește materialul ilegal se află în afara țării, statul vizat este informat prin intermediul Europol, prin punctul de contact 24/7 sau prin intermediul rețelei ofițerilor de legătură, în funcție de natura conținutului și de gravitatea infracțiunii. Un aspect important de care se ține seama la utilizarea instrumentului prin care un stat este informat este etapa cercetării în România. Principalele instrumente utilizate pentru a solicita măsuri de asistență sunt cererile poliției de conservare și de comisie rogatorie. Pentru țările din afara UE, principalele instrumente utilizate sunt punctele de contact 24/7 și Interpolul.

Pentru a denunța fapte legate de pornografia infantilă pe internet, a fost creat un site internet al poliției care este administrat în comun cu Organizația Salvați Copiii din România, Positive Media Iași și Centrul FOCUS - Centrul Român pentru Copii Dispăruți și Exploatați Sexual.

În cadrul poliției române există o unitate specializată în prevenirea și cercetarea infracțiunilor de pornografie infantilă prin internet (în cadrul Serviciului de combatere a criminalității informatice), iar la nivel local, în fiecare județ, există cel puțin un ofițer numit și format în mod special pentru a desfășura activități în acest domeniu. Această unitate specializată este formată din șase ofițeri în total și are următoarele atribuții: cercetarea pornografiei infantile prin internet; colectarea și utilizarea datelor și informațiilor disponibile pe internet privind pornografia infantilă prin intermediul sistemelor informatice; realizarea de studii, analize și evaluări ale evoluției fenomenului infracțional în domeniu și propunerea

de măsuri corespunzătoare; coordonarea cercetării pornografiei infantile la nivel național; activități de cooperare cu sectorul privat și cooperare internațională; promovarea unor evenimente de prevenire în domeniu; activități de identificare a victimelor din materialele pornografice cu minori și gestionarea bazelor de date speciale. În ceea ce privește pornografia infantilă care nu are legătură cu mediul online, există structuri specializate în cadrul Direcției de Investigații Criminale a Poliției Române.

6.3 Frauda cu carduri online

În 2012, Serviciul de combatere a criminalității informatice al Poliției Naționale Române (PNR) a inițiat o investigație privind intruziuni în terminalele POS (Point-of-Sale) și vânzarea de date privind cărți de credit compromise pe site-uri internet de vânzare automată, activități care s-au soldat cu pierderi în valoare de 25 000 000 USD pentru industria bancară australiană. PNR a efectuat activități de supraveghere, investigații sub acoperire și operații sub acoperire online pentru a-i identifica pe suspecți. Procurorul DIICOT responsabil de cazul respectiv a solicitat și a obținut de la Tribunalul București circa 100 de mandate de interceptare a datelor telefonice și internet. PNR a realizat localizări ale turnurilor de telefonie mobilă pentru a identifica locurile din care suspecții își desfășurau activitatea infracțională, clonarea serverelor autorizate la distanță și interceptări de date. Ofițeri ai PNR și ai Poliției Federale Australiene (PFA) au realizat teleconferințe săptămânale care au avut drept rezultat primirea de plângeri, rapoarte criminalistice și informații privind citațiile obținute de PFA și utilizate în cercetarea penală de către PNR. Ofițeri ai PFA au călătorit în România pentru a transfera către PNR clonele computerelor compromise folosite drept probe judiciare, pentru a furniza informații operative și pentru a depune depoziții scrise.

PNR a identificat noi sisteme POS compromise și date privind carduri de credit compromise localizate în SUA, Canada, Brazilia și Franța. Agenți ai PNR, PFA, FBI și USSS au participat la București la reuniuni de coordonare a cazurilor. PFA, FBI și USSS au furnizat autorităților române informații privind citațiile referitoare la victimele identificate, precum și jurnalele de acces pentru autentificare din conturile de e-mail și conturile de utilizator de forum utilizate de suspecți în cadrul activității lor ilicite. PNR a citat furnizori români de servicii de internet și de telefonie pentru a identifica suspecții, fiind de o importanță vitală accelerarea fluxului de informații dintre autoritățile străine de aplicare a legii și PNR.

A fost identificată o persoană de cetățenie română, suspectată de gestionarea unui centru de date care cuprindea servere utilizate de hackeri din toată lumea pentru a lansa atacuri cibernetice. Acesta era renumit în rândul hackerilor pentru furnizarea de găzduire extrem de sigură (*bulletproof hosting*). La sfârșitul investigației, au fost efectuate simultan 34 de percheziții domiciliare. Una dintre adrese era locul în care se găsea principalul centru de date suspectat utilizat pentru găzduirea extrem de sigură (*bulletproof hosting*) (au fost confiscate peste 400 TB de date). Centrul de date a fost desființat. A fost confiscată o sumă de circa 400 000 USD bani lichizi. Au fost cercetate șaisprezece persoane suspectate, iar șapte au fost arestate.

6.3.1 Raportarea online

Autoritățile române au garantat că activitățile de fraudă cu carduri online sunt raportate autorităților, iar entitățile din sectorul privat, în special instituțiile financiare, oferă asistență pentru desfășurarea cercetărilor prin furnizarea datelor necesare autorităților, în conformitate cu legea.

6.3.2 Rolul sectorului privat

În opinia autorităților române, cooperarea dintre autorități și instituțiile financiare este pozitivă sub toate aspectele în ceea ce privește prevenirea și combaterea fraudelor cu carduri online. Instituțiile financiare și poliția au stabilit puncte de contact, pentru un schimb de informații rapid și eficace. De asemenea, instituțiile financiare și reprezentanții autorităților publice realizează formări comune și activități de sensibilizare.

Posibilele lacune din legislația națională privind aplicarea măsurilor care ar ajuta la îmbunătățirea securității cibernetice și, prin urmare, la prevenirea criminalității informatice au fost soluționate prin semnarea unor acorduri de cooperare între instituții publice și entități private. Astfel, CERT-RO a semnat până în prezent peste 20 de astfel de documente cu reprezentanți ai sectorului privat, inclusiv ai sectorului bancar, care fac schimb de informații pentru a preveni sau a combate efectele incidentelor de securitate din sistemele informatice.

6.4 Concluzii

- România colectează anual statistici privind criminalitatea informatică. Acestea cuprind statistici privind incidentele colectate de CERT-RO și altele, care au o mai mare legătură cu procedurile penale în curs, colectate de instanțe judecătorești, de Ministerul Public și de poliție. Cu toate acestea, nu există o instituție responsabilă de colectarea tuturor statisticilor și de transmiterea acestora organelor de decizie pentru a realiza o imagine de ansamblu a acestui fenomen în România (precum COSC). Evaluatorii consideră că acest lucru ar putea contribui la măsurarea evoluției criminalității informatice în România și la luarea unor măsuri adecvate.

- România aplică principiul legalității, ceea ce ar putea avea drept rezultat consolidarea politicii de combatere mai eficace a criminalității informatice. Celălalt exemplu al răspunsului la criminalitatea informatică este obligația existentă de raportare a activităților ilegale adresată celor care au cunoștință de astfel de activități, inclusiv de atacuri cibernetice. Cu toate acestea, nu există dispoziții speciale adresate sectorului privat. În opinia evaluatorilor, o obligație clară care să precizeze situațiile în care ar fi obligatoriu pentru societățile private să genereze un raport automat ar putea contribui la combaterea criminalității informatice.

- Mai mult, dreptul național nu prevede un rol specific pentru operatorii de infrastructuri critice și operatorii sistemelor informatice. Totuși, echipa de evaluare a fost informată că proiectul de lege privind securitatea cibernetică reglementează conceptul de „infrastructuri cibernetice de interes național” (ICIN), precum și atribuțiile care sunt de competența tuturor deținătorilor de astfel de infrastructuri privind asigurarea securității rețelei și diminuarea efectelor atacurilor cibernetice. În opinia evaluatorilor, s-ar putea aduce îmbunătățiri în ceea ce privește cooperarea cu sectorul privat. Cooperarea structurată proactivă cu sectorul bancar ar trebui extinsă la celelalte sectoare relevante. Organizarea unor reuniuni periodice sau a unei structuri pentru discutarea incidentelor, a tendințelor și a evoluțiilor cu reprezentanți ai sectorului privat (din partea băncilor, furnizorilor de servicii de internet și societăților IT) ar putea, de asemenea, să consolideze această cooperare.

- Poliția a elaborat un set de proceduri-standard de operare care sprijină punerea în aplicare a legislației privind criminalitatea informatică, oferind, așadar, un compendiu armonizat de practici pentru utilizarea de către toate unitățile de poliție atunci când cercetează infracțiuni informatice. Procedurile au fost pregătite de unitatea centrală a poliției, după consultarea serviciilor regionale, și acoperă diferite aspecte ale cercetării infracțiunilor informatice, precum percheziții informatice, interceptarea sau păstrarea datelor informatice stocate, infracțiunile de pornografie infantilă săvârșite prin intermediul sistemelor informatice etc.

- România dispune de un instrument pentru raportarea online a incidentelor de criminalitate informatică: www.efrauda.ro. Astfel de incidente pot fi raportate de cetățeni în ceea ce privește toate tipurile de criminalitate informatică. Acestea sunt utilizate de poliția română pentru a deschide o investigație sau pot servi drept informații operaționale.

- De asemenea, există site-uri create în mod special pentru a combate pornografia infantilă. Safernet.ro este un exemplu de site internet care își propune să asigure o modalitate sigură de raportare rapidă a activităților de pornografie infantilă desfășurate pe internet. Proiectul Sigur.Info este conceput pentru a spori gradul de conștientizare de către copii, părinți și cadre didactice a beneficiilor/avantajelor utilizării internetului și a noilor tehnologii online, precum și a pericolelor/riscurilor asociate acestora, prin desfășurarea de campanii naționale de promovare a siguranței copiilor pe internet și atunci când utilizează telefoane mobile; de asemenea, programul este conceput pentru a fi foarte eficient în activarea unor parteneriate efective între instituțiile naționale.

- Potrivit autorităților române, există o sinergie între instrumentele menționate anterior, întrucât acestea sunt administrate de Poliția Română. În eventualitatea unor incidente adresate eronat, cererea va fi redirecționată către autoritatea competentă în vederea cercetării. Cu toate acestea, nu s-au înregistrat cazuri de rapoarte adresate eronat. Evaluatorii consideră raportarea online a criminalității informatice o abordare lăudabilă, un model similar putând fi avut în vedere pentru a fi dezvoltat în statele membre.

- Pornografia infantilă prin intermediul sistemelor informatice are loc în România mai ales prin distribuirea și schimbul de imagini pe internet. Cazurile de racolare de minori și de producere de materiale pornografice sunt rare. S-a înregistrat o creștere a numărului de cazuri implicând distribuirea de imagini, dar producerea de astfel de imagini este scăzută comparativ cu tendințele internaționale.

- Potrivit autorităților române, furnizorii de servicii internet au obligația de a elimina materialele ilegale implicând minori, o procedură care există de la intrarea în vigoare a Legii privind comerțul electronic în 2002. Totuși, dezvoltarea și utilizarea de către polițiști a unor instrumente speciale pentru a filtra site-urile internet pentru conținut pornografic implicând minori ar spori posibilitatea de a utiliza dispozițiile vizate la maximum.

- Autoritățile române iau măsuri preventive, inclusiv activități de monitorizare, atunci când se aduce la cunoștința autorităților că persoane cercetate pentru fapte de exploatare sexuală a minorilor călătoresc în România în scopul săvârșirii unor infracțiuni și pentru a preveni eventuale activități infracționale. Echipa de evaluare a fost informată că nu există dispoziții pentru astfel de măsuri în cazul opus, astfel încât nu se transmite nicio înștiințare țării de destinație atunci când există informații că un cetățean român condamnat pentru orice abuz sexual grav asupra minorilor călătorește în străinătate, cu excepția cazului în care în hotărârea judecătorească de condamnare se dispune acest lucru. Evaluatorii consideră că absența unei opțiuni de a transmite un mesaj în cazul opus lasă loc pentru îmbunătățiri.

- România investește în relația dintre partenerii publici și privați în diverse moduri. O metodă este schimbul de informații cu partenerii privați cu privire la incidente, măsuri tehnice și posibile soluții. Poliția și parchetele organizează numeroase conferințe în care partenerii privați dispun de o platformă pentru a-și comunica abordarea.

7 COOPERAREA INTERNAȚIONALĂ

7.1 Cooperarea cu agențiile UE

7.1.1 Cerințe formale de a coopera cu Europol/EC3, Eurojust, ENISA

România a creat mediul legal pentru cooperarea cu Eurojust prin punerea în aplicare a Deciziei 2002/187/JAI a Consiliului din 28 februarie 2002 de instituire a Eurojust în scopul consolidării luptei împotriva formelor grave de criminalitate (Ordonanța nr. 123 din 5 noiembrie 2007) și a Deciziei 2009/426/JAI a Consiliului privind consolidarea Eurojust (Legea nr. 35 din 19 martie 2012). Dispozițiile actului legislativ sunt organizate în trei rubrici, dedicate măsurilor instituționale și operaționale necesare pentru schimbul de magistrați de legătură (titlul I), cooperării cu Eurojust (titlul II) și funcționării rețelelor existente și viitoare la nivel național și la nivelul UE în domeniul cooperării judiciare (titlul III). Acesta prevede o obligație de a face schimb de informații în temeiul articolului 13 alineatele (5)-(7) din Decizia consolidată privind Eurojust. De la DIICOT, informațiile sunt transmise prin intermediul unei conexiuni securizate, în mod structurat, utilizând modelele create de Eurojust.

În cadrul Poliției Naționale Române, există o vastă experiență de cooperare între Europol și Direcţia de Combatere a Criminalităţii Organizate. Aceasta a vizat mai multe domenii, cum ar fi atacurile cibernetice, exploatarea sexuală a minorilor pe internet și fraudele cu carduri. În plus, în cadrul EMPACT, România a îndeplinit rolul de inițiator în domeniul fraudelor cu carduri, precum și rolul de coinițiator în domeniul atacurilor cibernetice. Reprezentanți ai poliției române participă la evenimentele organizate de Europol/EC3, fie sub formă de seminarii/ateliere, fie sub formă de reuniuni cu experți din diferite domenii, fie sub formă de reuniuni de coordonare. Reprezentanți ai Europol au participat la activități desfășurate în România, în anumite operații, pentru a asigura un schimb de date eficace și pentru a furniza sprijinul necesar. Reprezentantul poliției române participă la reuniunile Consiliului de administrație al Europol/EC3 și este inițiatorul proiectului EMPACT privind fraudele cu carduri de credit. În plus, România conduce alături de alte părți o acțiune operațională (din 18) și două acțiuni operaționale (din 23) din cadrul planurilor de acțiune operaționale (PAO) privind fraudele cu carduri de plată online și, respectiv, privind atacurile cibernetice. De asemenea, România participă la 29 (din 66) de acțiuni operaționale din cadrul PAO, precum și la punctele focale ale Europol care desfășoară activități privind aceste trei subpriorități ale criminalității informatice (*FPs Twins*, *Cyborg* și *Terminal*).

CERT-RO colaborează cu ENISA în cadrul unor programe de sprijinire a CERT naționale. Colaborarea cu ENISA se concretizează în participarea la grupuri de lucru, ateliere și conferințe privind securitatea cibernetică referitoare la cooperarea dintre CERT naționale și agențiile de aplicare a legii, precum exercițiile de securitate cibernetică (CYBER-EX) din 2012 și 2014. CERT-RO coordonează calendarul activităților desfășurate la nivel național în cadrul ECSM (evenimente de securitate în luna securității cibernetice). Reprezentantul CERT-RO participă la reuniunile Consiliului de administrație al ENISA. În plus, reprezentanți ai Ministerului Afacerilor Interne au participat la exercițiul cibernetic din cadrul evenimentului paneuropean Europa cibernetică 2014 (CE 2014) organizat de ENISA.

7.1.2 Evaluarea cooperării cu Europol/EC3, Eurojust, ENISA

Potrivit autorităților române, capacitatea Eurojust de a facilita comunicarea cu autoritățile străine și de a accelera executarea solicitărilor urgente este consolidată de DIICOT. Posibilitatea de finanțare din partea Eurojust este apreciată de practicieni. Sprijinul pe care Eurojust îl poate oferi este considerat foarte util în ceea ce privește facilitarea cooperării cu țările terțe. Evaluarea cooperării dintre autoritățile competente din România și Eurojust este pozitivă; cooperarea constă în organizarea de reuniuni de coordonare privind cazuri concrete. Este demn de menționat că membrul național al României la Eurojust este și punctul de contact al Eurojust la Europol/EC3 de la Haga, fiind și punctul de contact al Eurojust la punctul focal *Terminal* al Europol privind fraudele cu carduri de plată. Practicienii întâlniți au considerat utilă colectarea de Eurojust a celor mai bune practici și a jurisprudenței din alte jurisdicții, precum și diseminarea acestor informații în toate statele membre.

Înființarea Europol/EC3 a adus valoare adăugată în ceea ce privește prevenirea și combaterea criminalității informatice la nivel european, dar și la nivelul statelor membre. Abordarea integrată a criminalității informatice în ceea ce privește atacurile cibernetice, fraudele online și pornografia infantilă prin intermediul sistemelor informatice demonstrează importanța celor trei domenii și legăturile dintre acestea, în ceea ce privește instrumentele tehnice și juridice de investigare.

Autoritățile române au remarcat o îmbunătățire în modul în care noile evoluții ale tehnologiei și modurile de funcționare sunt identificate și prezentate statelor membre pentru a lua măsuri și pentru a dispune măsuri specifice preventive și investigative. Rapoartele de analiză realizate la nivelul Europol/EC3 au o valoare ridicată și conțin date integrate din baze de date. Resursele disponibile statelor membre în special pentru reuniuni de coordonare operaționale sunt de un nivel înalt. Un alt aspect pozitiv este implicarea sporită a Europol/EC3 în cooperarea cu sectorul privat, dar și cu țări terțe. Autoritățile române au subliniat faptul că Europol/EC3 ar trebui să continue să evalueze noile tendințe infracționale și să disemineze rezultatele în statele membre, precum și să își îmbunătățească capacitățile privind atacurile cibernetice și criminalistica informatică.

Programul ENISA de sprijinire a cooperării operaționale a CERT naționale cu agențiile de aplicare a legii la nivel național și european reprezintă un bun început. Programul ar trebui să fie continuat și axat pe schimbul de informații. În prezent, cele două părți, CERT naționale și agențiile de aplicare a legii, nu cunosc destul de bine atribuțiile, responsabilitățile și limitările celeilalte părți, în special în ceea ce privește realizarea prevenției și a acțiunilor de combatere. Astfel, capabilitățile site-urilor CERT naționale nu sunt întotdeauna utilizate în mod eficace pentru a sprijini activitatea agențiilor de aplicare a legii. Potrivit autorităților române, acest lucru s-ar putea schimba prin modificarea legislației naționale și europene, pentru a introduce obligații specifice de cooperare în vederea evitării dublării eforturilor și a cheltuielilor. De asemenea, ENISA ar putea elabora un format standardizat pentru statisticile analizate de CERT pentru ca alertele înregistrate să devină comparabile și armonizate în întreaga UE.

7.1.3 Performanța operațională a echipelor comune de anchetă și a patrulelor informatice

Autoritățile române au raportat numeroase cazuri de cooperare în materie de criminalitate informatică cu Europol/EC3 în care cetățeni români erau făptuitorii unor activități ilegale sau în care cetățeni români, autorități sau instituții private din România erau victime ale criminalității informatice. Colaborarea a implicat schimburi de date și informații, realizarea de reuniuni operaționale cu alte state membre sau

cu țări terțe și participarea, alături de biroul mobil al Europol, la activitățile desfășurate în România. De exemplu, o echipă comună de anchetă privind criminalitatea informatică (atacuri cibernetice și obținerea de baze de date cu detalii privind carduri de credit) a fost stabilită între Regatul Unit, Finlanda, Slovenia, România și SUA. De asemenea, au fost desfășurate anchete în cazuri comune de criminalitate informatică cu alte state membre ale UE sau cu state din afara UE. Experiența dobândită cu respectiva ocazie a fost pozitivă întrucât au fost stabilite în mod eficace anchete comune, precum și coordonarea măsurilor de anchetă, a răspunsului rapid în obținerea probelor etc.

A fost acordată finanțare din partea UE (Eurojust sau Europol/EC3) numai pentru sprijinirea organizării reuniunilor de coordonare cu statele membre ale UE și cu țările terțe.

România participă la Grupul strategic al Uniunii Europene al șefilor unităților naționale ale Europol de combatere a criminalității din domeniul înaltei tehnologii. Poliția Română participă în calitate de membru în cadrul Grupului operativ al UE pentru combaterea criminalității informatice (EUCTF) și a participat la activitățile grupului de la înființarea acestuia. Conceptul de „patrulă informatică” are multe avantaje, dar are nevoie de anumite resurse pentru a funcționa bine. La nivelul CERT-RO a fost dezvoltat un proiect care a avut drept rezultat mai multe propuneri, inclusiv punerea în practică a conceptului de „patrulă informatică” în cadrul poliției române. În prezent, conceptul de „patrulă informatică” este utilizat în cadrul poliției române pentru cazuri specifice, dar nu este instituționalizat și nu este realizat la nivel internațional. Aceste instrumente de cooperare sunt utile din mai multe motive, inclusiv la instituirea și identificarea cazurilor comune și la obținerea mai rapidă a probelor. Cu toate acestea, în opinia autorităților române, instrumentele nu sunt destul de eficace în ceea ce privește criptarea, serviciile anonime, cloudul și cooperarea cu țările terțe.

7.2 Cooperarea dintre autoritățile române și Interpol

Autoritățile române apreciază evenimentele organizate de Interpol și schimbul de date și informații furnizate de biroul național al Interpol. La invitația Interpol, ofițeri ai acestei unități au participat la două ateliere organizate de Interpol în cadrul proiectului „Baseline” privind instituirea unei liste de semnături ale fișierelor conținând materiale pornografice care prezintă minori prepubescenți care sunt implicați în activități sexuale explicite, această listă urmând să fie pusă ulterior la dispoziția furnizorilor de servicii internet pentru a bloca prezența online a fișierelor cu semnăturile respective și pentru a informa autoritățile judiciare competente cu privire la entitățile care inițiază transmisia de astfel de activități în mediul lor online.

Din 2010, prin intermediul unității specializate în cercetarea cazurilor de exploatare sexuală a minorilor pe internet, poliției române i s-a acordat acces la baza de date ICSE a Interpol și aceasta a început să o utilizeze, desfășurând următoarele activități:

- introducerea de materiale prezentând victime identificate în România;
- cooperarea cu alți utilizatori pentru a identifica victimele materialelor introduse în ICSE, atât prin introducerea unor materiale cu victime neidentificate, cât și prin analizarea unor astfel materiale existente în ICSE.

În 2011, aceeași unitate a început să utilizeze bazele de date ICACOPS și CPS conținând date și informații privind entitățile care săvârșesc fapte de pornografie infantilă prin intermediul sistemelor informatice în medii online specifice (P2P, Tor etc.).

7.3 Cooperarea cu statele terțe

Temeiul legal pentru cooperarea cu țările terțe este reprezentat de instrumente internaționale, precum și de canalul Interpol, punctele de contact 24/7, rețeaua de ofițeri de legătură sau contactele directe stabilite. Autoritățile române au indicat faptul că există țări terțe care sunt furnizori de activități ilegale, iar lipsa de reacție a acestora în cadrul cooperării internaționale face anumite investigații imposibile. Europol/EC3 a adus valoare adăugată în cadrul cooperării cu țările terțe prin resursele disponibile pentru reuniunile de coordonare operaționale și contactele cu respectivele țări terțe, care pot fi utilizate pentru a asista statele membre.

Cererile de asistență judiciară internațională făcute în cazuri de criminalitate informatică (inclusiv în cazuri de fraude cu carduri bancare) reprezintă aproape 40% din activitatea de cooperare judiciară internațională a DIICOT. În perioada 2013-2014, la nivelul DIICOT s-au înregistrat 262 de cereri, provenind din alte țări, de asistență judiciară internațională privind criminalitatea informatică. La rândul său, DIICOT a transmis 397 de astfel de cereri autorităților din alte state.

În ceea ce privește relațiile cu țări terțe, în respectiva perioadă s-au înregistrat următoarele cereri.

ȚARA	*PRIMITE*	*TRANSMISE*
ALBANIA	1	-
AUSTRALIA	-	6
BELARUS	1	-
BRAZILIA	-	2
CANADA	-	5
CHINA	-	4
COREEA DE SUD	1	2
ELVEȚIA	6	7
FEDERAȚIA RUSĂ	2	2
HONG KONG	-	1
ISRAEL	-	1
JAPONIA	1	1
LIECHTENSTEIN	2	-
MALAYSIA	-	2
MEXIC	-	3
NIGERIA	5	-
NORVEGIA	3	2
NOUA ZEELANDĂ	-	2
PALESTINA	-	2
PERU	-	2
PRINCIPATUL ANDORRA	2	-
REPUBLICA DOMINICANĂ	-	1
REPUBLICA MOLDOVA	-	2
SERBIA	1	-
SUA	32	19
TURCIA	2	1
UCRAINA	-	3

7.4 Cooperarea cu sectorul privat

Autoritățile române au declarat că cooperarea internațională privind fraudele cu carduri online pentru cazurile cu implicații transfrontaliere este foarte importantă pentru succesul unei investigații. De asemenea, cooperarea este posibilă în cazul în care societățile private își au sediul principal într-un stat terț, dar depinde de organizarea și funcționarea lor. În cazul în care societățile respective cooperează în conformitate cu statutul și dispozițiile juridice care li se aplică, schimbul de date și informații este mai rapid. Birourile societăților private pot face obiectul unor investigații și percheziții.

În timpul vizitei de evaluare, s-a subliniat faptul că cooperarea cu Western Union funcționează, de asemenea, foarte bine, datorită prezenței unui punct de contact în România. În plus, Western Union-SUA cooperează, de asemenea, bine, mulțumită bunelor relații dintre poliția română și FBI din SUA. Cu toate acestea, cooperarea cu societățile din domeniul transferului de bani ar putea fi îmbunătățită. În timpul vizitei, s-a subliniat faptul că reprezentanți ai poliției și ai Ministerului Public se întâlnesc ad-hoc cu reprezentanți ai sectorului privat pentru a dezbate aspectele tehnice ale colectării de informații, măsurile care trebuie adoptate pentru a garanta că aceste informații sunt admisibile în instanță etc.

7.5. Instrumentele cooperării internaționale

În domeniul cooperării în materie penală, România utilizează instrumente multilaterale și bilaterale la care este parte (tratate ale Consiliului Europei, în special Convenția privind criminalitatea informatică, Convenția ONU împotriva criminalității transnaționale organizate, Acordul UE-Japonia privind asistența judiciară reciprocă, Tratatul bilateral cu SUA etc.). Pentru a asigura o cooperare internațională imediată și continuă în ceea ce privește combaterea criminalității informatice, a fost instituit un punct de contact în cadrul Serviciului de combatere a criminalității informatice din cadrul Parchetului de pe lângă Înalta Curte de Casație și Justiție. Aceste instrumente sunt foarte importante pentru colectarea probelor digitale și pentru desfășurarea activităților de investigare în alte jurisdicții. Dificultățile întâmpinate privesc volatilitatea probelor digitale și probleme legate de „cloud”.

7.5.1 Asistența judiciară reciprocă

Cererile de asistență judiciară reciprocă în cazurile de criminalitate informatică sunt executate în temeiul Legii privind cooperarea judiciară internațională în materie penală (Legea nr. 302/2004) și în temeiul dispozițiilor Legii nr. 161/2003. În plus, ținând seama de dispozițiile constituționale care dispun că tratatele devin parte din dreptul intern după ratificare, diverse tratate regionale și internaționale pot fi utilizate drept temei legal pentru cooperarea cu UE sau cu țările terțe. În acest caz, Legea nr. 302/2004 este aplicabilă cooperării judiciare internaționale în materie penală numai pentru a completa respectivele instrumente în cazurile care nu sunt reglementate de acestea. Dreptul intern stabilește norme numai atunci când respectivele norme nu sunt deja reglementate de tratatul internațional sau numai pentru a le completa. Legea nr. 161/2003, care pune în aplicare Convenția privind criminalitatea informatică, prevede dispoziții speciale referitoare la cererile în materie de criminalitate informatică.

În funcție de instrumentele juridice aplicabile, pot fi competente diferite autorități pentru primirea sau trimiterea de cereri de asistență judiciară internațională în cadrul cercetărilor în materie de criminalitate informatică. La nivelul UE, sunt încurajate contactele directe dintre autoritățile judiciare care emit și care execută cererile, indiferent de stadiul în care este emisă cerere (cercetare, urmărire penală, judecată sau executare). Astfel, procurorii sau judecătorii pot comunica direct, acest lucru realizându-se în practică.

În cazul țărilor terțe, de obicei în temeiul tratatului juridic aplicabil, pot fi întâlnite două situații în legătură cu autoritățile centrale competente pentru a trimite/primi cererea de asistență judiciară reciprocă:

- două autorități centrale: Ministerul Public, pentru cererile de asistență judiciară reciprocă făcute în timpul etapei cercetării și urmăririi penale, și Ministerul Justiției, pentru cererile făcute în timpul etapei judecății și executării, sau
- o autoritate centrală: Ministerul Justiției, în cazul în care cererea a fost emisă în absența unui tratat și pe baza reciprocității sau dacă tratatul aplicabil desemnează Ministerul Justiției drept autoritate centrală unică.

În plus, pentru cererile referitoare la caziere, care sunt înregistrate în mod diferit față de cererile de asistență judiciară reciprocă, autoritatea centrală este Ministerul Afacerilor Interne.

În ceea ce privește canalele de comunicare, la nivelul UE există un canal direct utilizat între autoritățile judiciare care emit și care execută cererile. În anumite cazuri, este preferabilă transmiterea prin intermediul autorităților centrale, în speciale de țările care, deși sunt părți la Convenția din 29 mai 2000 privind asistența judiciară în materie penală între statele membre ale Uniunii Europene și Protocolul adițional la aceasta, continuă să utilizeze autoritățile centrale. Altfel, în ceea ce privește țările terțe, transmiterea are loc între autoritățile centrale sau chiar prin intermediul misiunilor diplomatice.

Date statistice privind cazurile de asistență judiciară reciprocă soluționate prin intermediul Ministerului Justiției[25]

Anul	Active	Pasive
2013	15	11
2014	34	12

Cererile de asistență judiciară reciprocă pot fi transmise și prin intermediul Parchetului de pe lângă Înalta Curte de Casaţie şi de Justiţie și direct între autoritățile judiciare în ceea ce privește țările UE. Potrivit statisticilor privind asistența judiciară reciprocă referitoare la cazurile de criminalitate informatică cercetate de DIICOT, România a primit 139 de cereri de asistență juridică reciprocă și a trimis 220 de cereri în 2013, iar în 2014 a primit 140 și trimis 150 de astfel de cereri.

Prin intermediul asistenței judiciare reciproce pot fi solicitate diverse forme de cooperare în ceea ce privește infracțiunile informatice, în funcție de tipul de infracțiune informatică constituit de comportamentul ilegal. Majoritatea cererilor se referă la fraude și falsificări informatice, infracțiuni legate de carduri de credit și, cel mai recent, încălcări ale drepturilor de autor prin intermediul sistemelor informatice. În consecință, multe dintre cereri se referă la furnizarea de informații privind abonații, date privind autentificarea, date privind conținutul (în mai mică măsură), percheziții și confiscări ale unor sisteme informatice, producerea de documente, interogarea unor martori etc.

[25] Aceste date se referă la cererile procesate prin intermediul Ministerului Justiției din România, exclusiv în calitate de autoritate centrală, după cum se dispune în instrumentele juridice internaționale.

Potrivit autorităților române, dificultățile care rezultă la executarea cererilor apar în general din cauza diferențelor dintre sistemele juridice și din cauza perioadei premergătoare executării cererii. În multe cazuri, instrumentul juridic aplicabil sau lipsa unui tratat aplicabil impune transmiterea prin intermediul canalelor diplomatice, ceea ce durează mai mult și duce la întârzieri evidente.

7.5.2 Instrumente de recunoaștere reciprocă

Nu sunt furnizate statistici specifice cu privire la aplicarea diferitelor instrumente de recunoaștere reciprocă. În plus, numai câteva ar fi aplicabile cazurilor de criminalitate informatică. De exemplu, datele statistice (pentru luna iunie 2014) referitoare la aplicarea Deciziei-cadru 2008/909/JAI arată că au fost primite șase cereri din partea altor state membre în legătură cu clonarea cardurilor de credit (trei cu Italia, una cu Belgia și două cu Polonia).

7.5.3 Predarea/extrădarea

Predarea

Procedura de predare în temeiul Deciziei-cadru privind mandatul european de arestare și procedurile de predare între statele membre stabilește un contact direct între autoritatea judiciară emitentă și autoritatea judiciară de executare, aspect preluat de legislația română. Ministerul Justiției în calitate de autoritate centrală intervine rar în proces, jucând un simplu rol administrativ. Autoritățile competente pentru primirea mandatelor europene de arestare sunt parchetele de pe lângă curțile de apel, în timp ce autoritățile competente pentru executarea mandatelor europene de executare sunt curțile de apel. În ceea ce privește emiterea unui mandat european de arestare, în funcție de tipul de infracțiune, toate instanțele române pot fi implicate (pe baza competenței materiale).

Date statistice privind mandatele europene de arestare emise în cazuri de criminalitate informatică în 2013 și 2014

Curtea de Apel	Active	Pasive
1.Oradea	4	7
2.Craiova	25	17
3. Ploiești	4	7
4.Pitești	5	7
5. Galați	-	4
6. Bacău	9	8
7. București	48	27
8. Brașov	1	1
9. Suceava	7	1
10. Timișoara	-	4
11. Constanța	4	2
12. Iași	6	70
TOTAL	**113**	**155**

Articolul 96 din Legea nr. 302/2004 menționează lista celor 32 de infracțiuni pentru care este eliminată verificarea dublei incriminări. Criminalitatea informatică, exploatarea sexuală a copiilor și falsificarea de monedă sunt incluse pe lista respectivă. Această tipologie foarte amplă permite includerea pe listă a unei ample game de infracțiuni informatice prevăzute de Codul penal român. Cu toate că pot fi remarcate limite ale infracțiunilor informatice și ale infracțiunilor conexe astfel cum sunt prevăzute în noul Cod penal, poate fi remarcat faptul că majoritatea infracțiunilor respectă pragul de trei ani. În plus, în cele mai multe cazuri, infracțiunile informatice sunt săvârșite cu participarea la un grup infracțional organizat și, prin urmare, pragul de trei ani este cel mai probabil întotdeauna atins.

Extrădarea

Autoritatea responsabilă de trimiterea și primirea cererilor de extrădare este Ministerul Justiției. În cazul în care cerințele legale prevăzute în instrumentul juridic internațional aplicabil și în Legea nr. 302/2004 nu sunt îndeplinite, Ministerul Justiției are dreptul să solicite informații suplimentare sau să returneze cererile. În cazul cererilor active, Ministerul Justiției este responsabil de redactarea cererii, pe baza documentelor anexate furnizate de instanța relevantă.

Articolul 26 din Legea nr. 302/2004 dispune că gravitatea infracțiunii este criteriul care trebuie luat în considerare pentru a stabili dacă extrădarea poate fi acordată sau nu în cazul unei infracțiuni anume. Prin urmare, România nu mai utilizează o listă de infracțiuni. Au fost instituite două praguri - un prag de cel puțin un an - în cazul în care se urmărește extrădarea în vederea urmăririi penale sau a judecății unei persoane și un prag de patru luni - în cazul în care extrădarea este solicitată în vederea executării unei pedepse.

Cererile de extrădare și/sau de mandat european de arestare sunt prelucrate în regim de urgență, dreptul român impunând termene stricte în acest sens, indiferent dacă cererea este activă sau pasivă (coroborat cu alte instrumente juridice aplicabile). De exemplu, în ceea ce privește executarea mandatului european de arestare, dreptul român impune o perioadă maximă de 90 de zile. Dacă persoana consimte, decizia de predare se pronunță în termen de zece zile. În medie, predarea în temeiul mandatului european de arestare are loc în mai puțin de o lună. În ceea ce privește extrădarea, procesul de extrădare în România durează în medie de la două la trei luni. Cu toate acestea, se înregistrează variații, în funcție de instrumentul juridic aplicabil și de termenele arestării preventive.

Nu există proceduri specifice care trebuie îndeplinite cu privire la cererile privind criminalitatea informatică. Există o procedură aplicabilă în general, indiferent de infracțiunea săvârșită. Pe de altă parte, cererile de extrădare privind criminalitatea informatică sau privind un mandat european de arestare emis pentru o infracțiune informatică au anumite particularități care sunt stabilite de caracterul transnațional. De asemenea, în multe cazuri, pot apărea conflicte pozitive de competență, și, pentru a evita astfel de conflicte, este necesară o coordonare prealabilă între autoritățile relevante.

În ambele cazuri, atunci când România este statul de executare în cadrul extrădării sau al mandatelor europene de arestare, autoritățile judiciare (instanțele române - mai exact, curțile de apel) hotărăsc cu privire la extrădare/predare.

7.6 Concluzii

- Se pare că România utilizează la scară largă serviciile oferite de Eurojust și Europol, precum și posibilitățile de cooperare și coordonare în ceea ce privește criminalitatea informatică. România recunoaște sprijinul furnizat de Eurojust în ceea ce privește facilitarea comunicării cu autoritățile străine și în ceea ce privește accelerarea executării cererilor urgente primite din partea altor țări din UE sau adresate acestora, schimbul de date şi informaţii, precum și în ceea ce privește desfășurarea de reuniuni operaționale cu alte state membre și părți terțe. Cu toate acestea, practicienii întâlniți în timpul vizitei la fața locului au semnalat faptul că Eurojust ar putea avea un rol în asistarea practicienilor prin colectarea de cele mai bune practici și de jurisprudență din celelalte jurisdicții și ar putea disemina respectivele informații în toate statele membre.

- Autoritățile întâlnite, în special din cadrul poliției, cunosc foarte bine Europol/EC3. Poliția română a participat la reuniuni ale Consiliului de administrație al Europol/EC3 și a apreciat în special rapoartele de analiză realizate de Europol/EC3 şi cooperarea Europol/EC3 cu sectorul privat și cu țările terțe. Sprijinul oferit de biroul mobil al Europol pentru activitățile desfășurate în România și abordarea sa integrată a criminalității informatice în cadrul Europol/EC3 în ceea ce privește atacurile cibernetice, fraudele online și pornografia infantilă prin intermediul sistemelor informatice au fost, de asemenea, lăudate de practicieni.

- Experiența României în materie de criminalitate informatică este, așadar, un element valoros în lupta împotriva infracțiunilor informatice identificate de UE ca priorități. Ca exemplu, România a adoptat rolul de inițiator în ceea ce privește fraudele cu carduri chiar de la începutul ciclului UE de elaborare a politicilor (EMPACT) în 2012; ulterior, a devenit coinițiator pentru atacurile cibernetice în 2014 și 2015 și participant în ceea ce privește exploatarea sexuală a copiilor online în 2014 și 2015.

- Există o gamă amplă de exemple de colaborare a CERT-RO cu ENISA, cum ar fi în ceea ce privește programele realizate de aceasta din urmă, sprijinirea CERT naționale și identificarea capabilităților acestora de sprijinire a activității agențiilor de aplicare a legii, participarea la grupuri de lucru și ateliere, conferințe privind criminalitatea informatică și exerciții cibernetice (Europa cibernetică 2012 și 2014), participarea la reuniunile Consiliului de administrație al ENISA etc. Cu toate acestea, ENISA ar putea elabora un format standardizat pentru statisticile analizate de CERT pentru ca statisticile respective să devină comparabile și armonizate în întreaga UE.

- România participă în calitate de membru în cadrul Grupului operativ al UE pentru combaterea criminalității informatice (EUCTF) și a participat activ la activitățile și reuniunile EUCTF. Cooperarea cu Interpol pare a fi bună. România beneficiază de serviciile oferite de Interpol, cum ar fi baza de date ICSE pentru identificarea victimelor abuzului asupra copiilor.

- România este deschisă cooperării cu țări terțe, fiind parte la multe instrumente internaționale care constituie un temei pentru asistența juridică. Cel mai adesea se utilizează acorduri bilaterale (mai ales cu SUA și Canada), acorduri multilaterale (Convenția privind criminalitatea informatică, Convenția din 1959 și cele două protocoale adiționale la aceasta, Convenția ONU împotriva criminalității transnaționale organizate, Acordul UE-Japonia privind asistența judiciară reciprocă, Convenția din 29 mai 2000 privind asistența judiciară în materie penală între statele membre ale Uniunii Europene) sau acorduri bilaterale coroborate cu acorduri multilaterale (Tratatul bilateral cu SUA coroborat cu Convenția de la Budapesta din 2001 sau Tratatul bilateral cu SUA coroborat cu Convenția ONU împotriva criminalității transnaționale organizate și cu Convenția de la Budapesta din 2001). În vederea unei bune cooperări, România utilizează canalele Interpol, punctele de contact 24/7, rețeaua ofițerilor de legătură sau contactele directe stabilite.

- În ceea ce privește mandatele europene de arestare, România își întemeiază cooperarea pe contactele directe dintre autoritățile judiciare. Ministerul Justiției în calitate de autoritate centrală intervine rar în proces, jucând un simplu rol administrativ. Există statistici care arată o tendință de a aplica mandate europene de arestare și în cazuri de criminalitate informatică.

8 FORMARE, SENSIBILIZARE ȘI PREVENIRE

8.1 Formare specifică

România oferă formare în materie de criminalitate informatică, adresată unor grupuri specifice de practicieni, cum ar fi judecătorii, polițiștii și experții IT, dar și publicului larg.

Institutul Național al Magistraturii (INM) oferă judecătorilor și procurorilor formare în materie de criminalitate informatică. Activitățile de formare au drept scop familiarizarea judecătorilor și a procurorilor cu metodele de cercetare a infracțiunilor din acest domeniu, oferindu-le magistraților cunoștințe privind noile *modi operandi* și informațiile care pot fi obținute de la societățile private și care sunt utile pentru desfășurarea cercetărilor sau la instrumentarea dosarelor. INM organizează în fiecare an aproximativ 2-3 seminarii referitoare la evoluțiile criminalității informatice în România, inclusiv privind importanța activității de cercetare criminalistică privind noile caracteristici și funcții ale dispozitivelor mobile, probele digitale, impactul criminalității informatice asupra sistemului de plăți electronice, tendințe și metode de investigare, cooperarea societăților private cu instituțiile de aplicare a legii, regulile pentru realizarea percheziților informatice și resursele speciale de investigare. În 2011, INM și Europol au realizat un proiect care a inclus trei seminarii de două zile pentru magistrați la Cluj, Brașov și București. Aproximativ 25 de judecători și procurori sunt invitați să participe la fiecare seminar.

În plus, în fiecare an este organizată o conferință intitulată „Justiție și criminalitate informatică”, ca formare decentralizată continuă, cu sprijinul Tribunalului Gorj. Există de asemenea evenimente regionale privind criminalitatea informatică organizate chiar de judecători, precum cel desfășurat la Tribunalul Târgu Jiu (în ultimii șapte ani) cu participarea unor judecători, procurori și polițiști. Printre formatori s-au numărat și reprezentanți ai sectorului privat.

CERT-RO este o altă instituție foarte activă în promovarea luptei împotriva criminalității informatice. În cadrul proiectului „Sistemul național de combatere a criminalității informatice «Cyber Crime»” desfășurat de CERT-RO și sprijinit de un grant din partea programului operațional sectorial Dezvoltarea capacității administrative 2007-2013, a fost dezvoltat un program de formare în materie de prevenire și combatere a criminalității informatice. Programul de formare a fost împărțit în patru module:

Modulul I -	Aspecte de ordin juridic și politici publice cu referire la securitatea cibernetică (40 de participanți) 27.1.2014 - 31.1.2014 5 zile, 2 serii de câte 20 de persoane - simultan
Modulul II -	Certified Ethical Hacking (20 de participanți) 3.2.2014 - 7.2.2014 (prima serie) 10.2.2014 - 14.2.2014 (a doua serie) 5 zile, 2 serii de câte 10 persoane
Modulul III -	Computer Hacking Forensic Investigator (20 de participanți) 3.3.2014 - 7.3.2014 (prima serie) 10.3.2014 – 14.3.2014 (a doua serie) 5 zile, 2 serii de câte 10 persoane Analiză malware (10 participați, în funcție de rezultatele după evaluare) 7.4.2014 - 11.4.2014 5 zile, 1 serie de 10 persoane
Modulul IV -	Exercițiu cibernetic (40 de participanți) 7.5.2014 – 9.5.2014 3 zile, 1 serie de 40 de persoane

Obiectivul general al proiectului îl reprezintă crearea unui cadru adecvat în vederea creșterii capacității de formulare a politicilor și de punere în aplicare a acestora și de realizare a unei mai bune reglementări și planificări strategice, prin consolidarea parteneriatelor atât la nivel interinstituțional, cât și între instituțiile publice și reprezentanți ai altor domenii vizate de combaterea criminalității informatice.

În plus, activitățile din programa de formare și din afara acesteia cuprind materiale realizate în cadrul proiectului *Sigur.Info*, precum și resurse elaborate de alte proiecte care abordează această temă. Proiectul *Sigur.Info* include și o componentă de formare, astfel încât există în fiecare țară o persoană responsabilă cu resursele (cadru didactic/inspector), formată în cadrul proiectului. De asemenea, sunt organizate sesiuni de formare pentru voluntari pe tema siguranței online.

În plus, ar trebui evidențiat și rolul Ministerului Educației în formarea referitoare la criminalitatea informatică. Proiectul ministerului, intitulat „Dezvoltarea competențelor manageriale ale personalului didactic cu funcții de conducere, îndrumare și control din sistemul preuniversitar, în societatea cunoașterii - OSCINT 2009 ID – 63376", se adresează inspectoratelor școlare județene și instituțiilor de învățământ. Obiectivul general al proiectului este popularizarea în rândul personalului didactic cu funcții de conducere, îndrumare și control din sistemul de învățământ a principalelor repere conceptuale din cadrul OSCINT, domeniile inteligenței competitive și managementului cunoștințelor; cunoașterea organizării OSCINT - resursele umane, cadrul juridic și competențele OSCINT; rațiunea de a exista a inteligenței competitive și a managementului cunoștințelor în cadrul învățământului preuniversitar; înțelegerea contextului în care cunoștințele/informațiile sunt create, gestionate și utilizate; familiarizarea cu principiile inteligenței colaborative și cu instrumentele OSCINT pentru activitatea colaborativă - platforma informatică de instruire.

Polițiștilor le este oferită formare în materie de criminalitate informatică prin intermediul Planului național anual de formare, care include teme de interes, și, de asemenea, prin intermediul altor evenimente organizate cu instituții publice, autorități străine sau parteneri privați. Participarea individuală la cursurile de formare de către polițiști este un alt mod de a asigura nivelul de cunoștințe necesar. În 2014, în cadrul ISOP a fost organizat cursul anual de formare privind „Percheziționarea sistemelor informatice" pentru polițiștii care lucrează în structuri care combat criminalitatea organizată. Programa cursului a inclus prezentări ale procedurilor speciale de percheziționare a sistemelor informatice, aspecte de ordin juridic și procedural privind perchezițiile informatice, identificarea, securizarea și colectarea probelor digitale, copierea suporturilor de stocare a datelor - aspecte procedurale și aplicații, prezentarea software-ului utilizat în activitățile de percheziționare a sistemelor informatice, o prezentare generală a caracteristicilor de bază și configurarea software-ului *EnCase Forensic*, precum și multe alte teme.

Există de asemenea module educaționale specializate orientate către criminaliștii IT sau către anchetatorii specializați în criminalitate informatică. În cadrul Serviciului de combatere a criminalității informatice al Poliției Române sunt desfășurate periodic sau ori de câte ori este nevoie sesiuni de formare pentru polițiștii care lucrează în domeniul criminalisticii informatice. Cursurile sunt ținute de formatori din cadrul Serviciului de combatere a criminalității informatice pentru polițiștii noi sau locali pentru a acoperi nevoia de formare privind noile evoluții IT.

De asemenea, România participă la Grupul european privind formarea și educația în combaterea criminalității informatice (ECTEG) și contribuie la noile materii de studiu care sunt identificate și dezvoltate. Astfel, la sfârșitul lui 2014, România a participat la un proiect european, coordonat de ECTEG și de University College Dublin, cu scopul de a actualiza trei cursuri de formare specifică în domeniul criminalității informatice. Polițiștii au participat și la formarea specializată a personalului din agențiile de aplicare a legii, organizată de Colegiul European de Poliție (CEPOL) alături de Europol, privind: criminalistica în cazuri de criminalitate informatică și probele digitale, la Tallinn, Estonia, în noiembrie 2014; criminalitatea informatică vs. securitatea cibernetică, la Tampere, Finlanda, în octombrie 2014; abuzurile asupra copiilor în spațiul cibernetic, la Barcelona, Spania, în aprilie 2014 și un curs privind combaterea exploatării sexuale a copiilor pe internet, la Selm, Germania, în octombrie 2014.

Formarea profesională în materie de criminalitate informatică se află în sarcina autorităților publice competente în ceea ce privește prevenirea și combaterea acestui fenomen. Primul proiect național pentru formarea în comun a poliției, a procurorilor și a judecătorilor - Centrul de Excelență pentru Combaterea Criminalității Informatice (CYBER-EX) - a fost inițiat de Poliția Română în cooperare cu DIICOT, Institutul Național al Magistraturii și alții. În prezent, sunt desfășurate acțiuni specifice pentru a permite centrului să devină funcțional și, prin urmare, să ofere formare specifică începând cu al doilea trimestru al anului 2015 (cursuri, sesiuni de formare etc.) care vor facilita promovarea, dezvoltarea și punerea în practică a unor metode și instrumente orizontale de combatere a criminalității informatice. Cu toate acestea, merită menționat faptul că la momentul vizitei la fața locului fuseseră deja organizate mai multe evenimente cu participarea unor polițiști, procurori și judecători.

8.2 Sensibilizare

Decizia din 30.9.2014 a Consiliului Suprem de Apărare a Țării menționează includerea unor cursuri în domeniul securității cibernetice în formarea școlară. Pentru a atinge acest obiectiv, sectorul privat are un rol important în ceea ce privește dezvoltarea unor campanii de informare și evenimente de sensibilizare, în special pentru tineri, cu privire la amenințările online și la necesitatea de a respecta măsurile de securitate informatică. Sectorul privat este implicat în evenimente de informare și sensibilizare precum Ziua Siguranței pe Internet și Luna Securității Cibernetice.

În Ziua Siguranței pe Internet 2014, a fost lansat în România eSafety Label, o platformă online gratuită care sprijină specialiștii TIC și cadrele didactice în crearea unui mediu școlar sigur în ceea ce privește accesarea mediului online. Platforma oferă mai multe fișe de lucru pe teme cum ar fi cyber-bullyingul (hărțuirea cibernetică) și gestionarea incidentelor din mediul online, un forum în care cadrele didactice pot face schimb de experiență cu alte cadre didactice din întreaga Europă și asigură o comunicare directă cu experții eSafety care vor răspunde la întrebările acestora prin intermediul platformei. Prin completarea unui formular de evaluare de 30 de întrebări, care acoperă aspecte legate de infrastructură, politici și practici, reprezentantul școlii poate descărca un plan de acțiune personalizat. Acesta prezintă măsuri concrete de îmbunătățire a eSafety în școala lor. Această etichetă unică la nivel european demonstrează părinților și instituțiilor că principiile eSafety sunt luate în serios și că acestea sunt esențiale în educația tinerei generații.

Concursul „Eu și internetul” face parte din Ziua Siguranței pe Internet 2014; în cadrul acestuia, copii cu deficiențe de auz ajută la crearea unui mediu mai sigur pentru ei și pentru alți copii hipoacuzici. Participanții realizează o galerie de tip Photo Voice în care să surprindă prin zece fotografii reprezentative activitatea lor online și atitudinea lor față de internet dobândită în cadrul proiectului eSign, înscriind o colecție de resurse pentru persoane cu deficiențe de auz (selectarea unor site-uri sau bloguri educaționale, resurse în format electronic, clipuri video, creații artistice, grupuri de discuție etc. specifice pentru persoanele cu deficiențe de auz).

Recent, Comisia pentru învățământ din cadrul Camerei Deputaților din Parlamentul Român a dezbătut cu reprezentanți ai instituțiilor publice, ai sectorului privat și ai ONG-urilor crearea unui curs privind criminalitatea informatică care să fie introdus în școli, o activitate aflată în curs de desfășurare. Cursurile școlare ar trebui să prezinte teme referitoare la transmiterea datelor personale pe internet, securitatea online a copiilor și amenințările cibernetice.

8.3 Prevenție

Strategia Națională de Ordine și Siguranță Publică stipulează necesitatea de consolidare instituțională pentru a preveni și combate criminalitatea, în timp ce planul de acțiune al poliției prevede măsuri concrete de îmbunătățire a prevenției. De asemenea, aceasta este dezvoltată de Legea nr. 161/2003 care reglementează prevenirea și combaterea criminalității informatice prin intermediul unor măsuri speciale de prevenire, detectare și pedepsire a infracțiunilor săvârșite prin intermediul sistemelor informatice, asigurând respectarea drepturilor omului și protecția datelor cu caracter personal. Legea respectivă prevede că autoritățile publice, furnizorii de servicii, ONG-urile și alți reprezentanți ai societății civile desfășoară activități și programe comune pentru a preveni criminalitatea informatică, în vederea asigurării securității sistemelor informatice și a protecției datelor cu caracter personal. Prin urmare, ar trebui ca aceștia să organizeze campanii de informare privind criminalitatea informatică și riscurile la care sunt expuși utilizatorii sistemelor informatice.

Protecția copiilor împotriva abuzurilor săvârșite prin intermediul internetului este limitată în ceea ce privește cadrul de reglementare pentru apărarea drepturilor copiilor, general față de dispozițiile legii speciale privind protecția copilului împotriva tuturor formelor de abuz, neglijare și exploatare. Potrivit Legii nr. 272/2004 privind protecția și promovarea drepturilor copilului, copilul are dreptul de a fi protejat împotriva abuzului, neglijării, exploatării, traficului, migrației ilegale, răpirii, violenței, pornografiei prin internet, precum și a oricăror forme de violență. Orice persoană fizică, inclusiv un copil, poate sesiza direcția generală de asistență socială și protecția copilului din județul/sectorul de domiciliu să ia măsurile corespunzătoare pentru a proteja un copil împotriva oricăror forme de violență, inclusiv violență sexuală, vătămare sau de abuz fizic sau mental, de rele tratamente sau de exploatare.

În același timp, Strategia națională pentru protecția și promovarea drepturilor copilului, care acoperă perioada 2014-2020, se referă la prevenirea și combaterea tuturor formelor de violență și la punerea în aplicare a unor acțiuni de sensibilizare, inclusiv măsuri de reducere a gradului de expunere a copiilor la violență în mass-media și în mediul online. Autoritățile române au indicat că, pentru a îndeplini acest obiectiv, ar trebui modificată legislația privind protecția copilului împotriva formelor de violență.

Cealaltă inițiativă, intitulată *Împreună facem internetul mai bun*, realizată în cadrul *Sigur.Info*, este un proiect care urmărește implicarea copiilor, a tinerilor, a părinților și a cadrelor didactice în conturarea unor idei prin care utilizatorii pot construi împreună un internet mai bun, fie prin moderarea propriului comportament sau modelarea unor comportamente pozitive pentru alți utilizatori, fie prin raportarea conținuturilor ilegale, necorespunzătoare sau dăunătoare, precum și prin crearea unor oportunități de colaborare, lucru în echipă și împărtășire a informațiilor. Tema concursului din 2014 s-a axat pe responsabilitatea pe care societatea (inclusiv copiii, părinții, cadrele didactice, educatorii și politicienii) trebuie să și-o asume pentru a face internetul un loc mai bun și mai sigur. În plus, această competiție urmărește să sporească gradul de conștientizare în rândul copiilor, tinerilor, cadrelor didactice și părinților cu privire la oportunitățile pe care le oferă internetul și să identifice comportamente prin intermediul cărora utilizatorii pot crea un mediu online mai bun, propunând modalități inovatoare prin care utilizatorii, reprezentanții industriei (Facebook, Google etc.) și instituțiile publice pot contribui în acest sens. Competiția este deschisă atât școlilor, cluburilor de tineret, cât și copiilor. Competiția *Împreună facem internetul mai bun* include și categorii speciale, de premiere a persoanelor și instituțiilor celor mai implicate în promovarea și asigurarea unei activități responsabile online în anul 2013:

- Profesorul anului - profesorul cel mai implicat în activități de promovare și sensibilizare a siguranței online în rândul studenților și al comunității;
- Școala anului - școala cu cel mai mare număr de activități de promovare și conștientizare privind siguranța online în rândul elevilor;
- Grădinița anului - grădinița care prezintă cel mai clar și creativ într-un proiect de echipă tema competiției naționale *Împreună facem internetul mai bun!*;
- Voluntarul *Sigur.Info* al anului - cel mai activ voluntar *Sigur.Info* care a promovat siguranța online în rândul grupurilor-țintă și a inițiat proiecte și activități proprii în vederea asigurării unui comportament responsabil la utilizarea internetului.

Autoritățile române au dat, de asemenea, exemple de cele mai importante evenimente privind prevenirea criminalității informatice organizate în 2014 privind:

- Securitatea cibernetică, pentru a realiza o platformă interactivă pentru dialog între factorii de decizie și specialiștii IT, la 2 octombrie 2014;
- riscurile cibernetice în serviciile financiare, la 9 octombrie 2014;
- Seminarul tehnologic NEC, la 14 octombrie 2014 - organizat de Corporația NEC și CERT-RO;
- Viitorul și siguranța plăților electronice, la 16 octombrie 2014 - organizat de Asociația Română a Băncilor (ARB), Asociația Națională pentru Securitatea Sistemelor Informatice (ANSSI) și CERT-RO;
- Securitatea cibernetică UTI, la 29 octombrie 2014 (inclus în seria de evenimente legate de Luna Securității Cibernetice a ENISA);
- Noile provocări globale de securitate cibernetică, la 3 noiembrie 2014;
- Conferința „CYBERTHREATS", la 13 noiembrie 2014.

Institutul Bancar Român (IBR) a organizat cea de a șaptea ediție a conferințelor „CyberThreats", în parteneriat cu CIO Council România și cu contribuții din partea unor funcționari ai Serviciului Român de Informații, CERT-RO, Băncii Naționale Române (BNR) și ARB, din partea instituțiilor financiare și a instituțiilor guvernamentale, precum și din partea firmelor de audit și a unor societăți din domeniul tehnologiei și al securității. Această ediție s-a axat pe riscurile principale asociate cu amenințările vechi și noi și pe metodele de a ține pasul atât cu principiile tehnologice, cât și procedurale, precum și pe metodele de management al crizelor.

În cadrul proiectului „Sistemul național de combatere a criminalității informatice «Cyber Crime»", desfășurat de CERT-RO, au fost elaborate patru seturi de propuneri de politică, menite să îmbunătățească mediul de lucru astfel încât să fie consolidată capacitatea de a formula politici publice și de a obține o mai bună reglementare și planificare strategică, prin consolidarea parteneriatelor, atât la nivel interinstituțional, cât și între instituțiile publice și reprezentanții altor domenii interesate de combaterea criminalității informatice.

8.4 Concluzii

- Institutul Național al Magistraturii oferă judecătorilor și procurorilor formare în materie de criminalitate informatică, iar Academia de Poliție oferă o astfel de formare polițiștilor. În plus, conceptul de „formare în comun” pentru polițiști, procurori și judecători a fost deja utilizat în cadrul mai multor evenimente organizate de autoritățile române.

- În plus, această inițiativă ar trebui consolidată atunci când Centrul de Excelenţă pentru Combaterea Criminalității Informatice (CYBER-EX) devine pe deplin funcțional, lucru preconizat să se întâmple în 2016. Deschiderea CYBER-EX ar trebui să faciliteze promovarea, dezvoltarea și punerea în aplicare a unor metode orizontale și instrumente pentru combaterea criminalității informatice. Această posibilitate va avea probabil o valoare deosebită pentru sectorul judiciar în ceea ce privește sporirea cunoștințelor de specialitate în materie de criminalitate informatică. CYBER-EX ar putea, de asemenea, să furnizeze consiliere la nivel de experți și un punct de contact pentru probleme legate de criminalitatea informatică, în special pentru judecătorii care instrumentează cazuri de criminalitate informatică, întrucât nu există judecători specializați în acest domeniu, spre deosebire poliție și procurori.

- Prin urmare, evaluatorii consideră că înființarea CYBER-EX în vederea organizării de formări pentru toate autoritățile implicate în cercetarea, urmărirea și judecarea cazurilor de criminalitate organizată, cu formatori din toate sectoarele, ar trebui considerată drept un exemplu de bună practică.

- Echipa de evaluare a fost de asemenea informată că judecătorii se organizează în ceea ce privește formarea în materie de criminalitate organizată, de exemplu, Tribunalul Târgu Jiu. Au fost implicați și formatori din sectorul privat. Evaluatorii consideră că faptul că judecătorii au avut inițiativa de a organiza mai multe ocazii de formare în materie de criminalitate organizată și în legătură cu poliția și procurorii reprezintă un exemplu de bună practică demnă de urmat. În opinia evaluatorilor, stabilirea unei rețele de magistrați specializați în materie de criminalitate informatică ar putea, de asemenea, să răspândească cunoștințele despre criminalitatea informatică.

- Ar trebui menționat și faptul că multe dintre celelalte instituții organizează formări pentru avocați și experți IT. Printre organizațiile care oferă formare în materie de criminalitate informatică se numără ECTEG și Europol. Cu toate acestea, respectiva formare se axează din ce în ce mai mult pe e-learning și pe instrumente din surse deschise mai degrabă decât pe instrumente comerciale. Cu toate că România utilizează cu succes resursele oferite de Eurojust, Europol și ENISA, practicienilor nu le este oferită multă formare privind posibilitățile oferite de respectivele instituții.

- Din moment ce România este o țară relativ mare, oferirea de formare unor unități dispersate geografic poate constitui o provocare. În opinia evaluatorilor, punerea în practică a metodei e-learning pentru anumite tipuri de formare (formarea celor care asigură răspunsul imediat, informații din surse deschise, *scripting*, introducere în analiza malware-ului static etc.) ar putea duce la o învățare mai eficace și la îmbunătățirea resurselor. Fie materialele de formare ar putea fi oferite de ECTEG, fie cursurile ar putea fi dezvoltate intern sau în cooperare cu UCD sau cu Universitatea Română.

- De asemenea, CERT-RO este foarte activ în materie de formare și campanii de sensibilizare. Acesta organizează miniseriale TV, seminarii tehnice și conferințe și emite alerte de impact ridicat pe site-ul internet CERT.

- Ministerul Educației este foarte implicat în prevenirea criminalității informatice și în securitatea cibernetică. Acesta sprijină inițiative de sensibilizare, de asemenea în bună cooperare cu actori relevanți din sectorul privat, în special linii telefonice de urgență și instituții similare (Asociația Telefonul Copilului), în special în domeniul abuzului împotriva copiilor. De asemenea, ministerul elaborează materiale de studiu pentru școlile primare și organizează diverse evenimente pentru a crește gradul de conștientizare privind securitatea cibernetică. Materialele urmăresc (similar proiectului *Sigur.Info*) să împiedice ca cetățenii să devină victime ale criminalității informatice (formări pentru cadre didactice, elevi și părinți). Acest tip de campanii de sensibilizare și educare oferite societății ar trebui să fie considerat un exemplu de bună practică.

- Sectorul privat este, de asemenea, implicat în organizarea de campanii de sensibilizare și de cursuri de formare în comun cu autoritățile de aplicare a legii. Potrivit autorităților române, colaborarea cu sectorul privat în domeniul prevenirii și combaterii criminalității informatice se desfășoară în condiții bune. Cu toate acestea, organizarea unor reuniuni periodice sau a unei structuri pentru a discuta incidentele, tendințele și evoluțiile în ceea ce privește criminalitatea informatică ar putea consolida această cooperare.

- Prevenirea infracțiunilor săvârșite prin intermediul internetului sau pe internet ar putea să aibă beneficii ca urmare a unei activități sporite și mai orientate din partea autorităților publice relevante și ca urmare a dezvoltării unui parteneriat privat/public. Acest lucru ar putea include activități de sporire a gradului de conștientizare cu privire la fraude și securitatea cibernetică, precum și măsuri de prevenire luate de sectorul privat, cum ar fi furnizorii de servicii de internet și sectorul bancar.

9 OBSERVAȚII FINALE ȘI RECOMANDĂRI

9,1. Sugestii din partea României

Criminalitatea și securitatea cibernetică reprezintă preocupări majore pentru guvernul român întrucât România se confruntă cu criminalitate organizată transfrontalieră, inclusiv cu criminalitate informatică. Din perspectiva României, caracterul transfrontalier al activității infracționale aferent criminalității informatice și dificultățile legate de obținerea de probe prin intermediul cooperării internaționale sau de obținerea identificărilor pentru adresele IP sau a altor date se numără printre principalele obstacole care limitează combaterea cu succes a criminalității informatice. În plus, consolidarea capacităților instituționale, armonizarea legislației și alocarea de resurse financiare trebuie să fie realizate în conformitate cu standardele și evoluțiile internaționale.

România dorește să continue sprijinirea eforturilor comunității internaționale de combatere a criminalității informatice.

9.2 Recomandări

În ceea ce privește punerea în aplicare concretă și funcționarea deciziei-cadru și a directivelor, echipa de experți implicată în evaluarea României a putut să analizeze în mod satisfăcător sistemul din România.

România ar trebui să întreprindă acțiuni ulterioare recomandărilor făcute în prezentul raport 18 luni după evaluare și să raporteze cu privire la progresele sale Grupului de lucru pentru chestiuni generale, inclusiv evaluare (GENVAL).

Echipa de evaluare a considerat adecvat să facă o serie de sugestii în atenția autorităților din România. Pe baza unor bune practici diverse, sunt, de asemenea, prezentate recomandări conexe adresate UE, instituțiilor acesteia, Eurojust, Europol și ENISA.

9.2.1 Recomandări adresate României

1. România ar trebui să elaboreze o metodă de colectare a unor statistici standardizate și generale cu privire la cercetările și urmăririle penale și condamnările aferente criminalității informatice, defalcate pe domenii specifice de criminalitate informatică, de preferință cele identificate la nivelul UE, și anume abuzul online asupra copiilor, fraude cu carduri online și atacurile cibernetice; (cf. 3.3 și 3.5)

2. România ar trebui să intensifice activitatea CERT-RO prin sporirea numărului de angajați pentru a atinge efectivele stabilite prin buget; (cf. 3.1, 4.3, 4.4.2 și4.5)

3. România ar trebui să reglementeze conceptul de „infrastructuri cibernetice de interes național" (ICIN) și să instituie un instrument juridic național care să prevadă atribuții specifice pentru operatorii ICIN, inclusiv societățile private răspunzătoare de infrastructurile critice în eventualitatea unui atac cibernetic, precum și să organizeze o structură care să permită partajarea informațiilor cu privire la evoluții și incidente; (cf. 4.3 și 4.5)

4. România ar trebui să aibă în vedere consolidarea rolului Consiliului Operativ de Securitate Cibernetică (COSC), drept organism de coordonare a eforturilor instituțiilor publice implicate în securitatea cibernetică, și să analizeze posibilitatea includerii altor organisme în componența acestuia (cum ar fi Ministerul Educației) și a instituirii unui mecanism care să faciliteze contribuțiile sectorului privat la sistemul național de securitate cibernetică; (cf. 4.4.1 și 4.5)

5. România ar trebui să pună în aplicare pe deplin Directiva 2011/93/UE a Parlamentului European și a Consiliului privind combaterea abuzului sexual asupra copiilor, a exploatării sexuale a copiilor și a pornografiei infantile; (cf. 5.1.2 și 5.5)

6. România ar trebui să aibă în vedere stabilirea unui concept de „criminalitate informatică" comun care să fie împărtășit de toate părțile interesate care combat criminalitatea informatică; (cf. 5.1.2 și 5.5)

7. România ar trebui să aibă în vedere organizarea unor reuniuni periodice sau a unei structuri pentru discutarea incidentelor, a tendințelor și a evoluțiilor cu reprezentanți ai sectorului privat (din partea băncilor, furnizorilor de servicii de internet și societăților IT) în materie de criminalitate informatică (cf. 6.1.2 și 6.4)

8. România ar trebui să aibă în vedere dezvoltarea și utilizarea unor instrumente specifice pentru a filtra site-urile internet în ceea ce privește conținutul de pornografie infantilă, pentru a completa posibilitățile de utilizare la potențial maxim a obligației legale a furnizorilor de servicii internet de a elimina materialele ilegale implicând minori; (cf. 6.2.4 și 6.4)

9. România ar trebui să fie încurajată să continue activitățile de formare implicând poliția, procurorii și judecătorii și să includă în cadrul acestor activități de formare informații privind sprijinul care poate fi oferit autorităților naționale de Eurojust, Europol și ENISA; (cf. 8.1 și 8.4)

9.2.2 Recomandări adresate Uniunii Europene, instituțiilor sale și altor state membre

1. Statele membre ar trebui să analizeze toate posibilitățile disponibile, printre altele prin trimiteri la Directiva 2002/58/CE, și să se implice într-un dialog cu sectorul privat, în vederea găsirii unor posibilități de păstrare a datelor; (cf. 3.2, 3.5 și 5.5)

2. Statele membre ar trebui să aibă în vedere analizarea cooperării dintre agențiile de aplicare a legii și serviciile naționale de informații în combaterea criminalității informatice, cum ar fi cea existentă în România, în special în ceea ce privește obținerea și prelucrarea probelor digitale; (cf. 4.3 și4.5)

3. Statele membre ar trebui să aibă în vedere participarea la un dialog cu sectorul privat pentru a discuta metodele de asigurare a faptului că colectarea informațiilor are loc astfel încât acestea să fie admisibile în instanță; (cf. 5.2 și 5.5)

4. Statele membre ar trebui să urmărească găsirea unei soluții juridice la lacuna provocată de lipsa unor soluții juridice care să permită localizarea și accesarea datelor din cloud; (cf. 5.4.3, 5.4.4 și 5.5)

5. Statele membre ar trebui să aibă în vedere furnizarea unor proceduri standard de funcționare pentru practicieni, în vederea punerii în aplicare a legislației privind criminalitatea informatică, similare celor pregătite de poliția română; (cf. 6.1.2 și 6.4)

6. Statele membre ar trebui să utilizeze la maxim serviciile oferite de Eurojust și Europol în ceea ce privește criminalitatea informatică și să prevadă o cooperare strânsă între CERT naționale ale acestora și ENISA; (cf. 7.1.2 și 7.6)

7. Statele membre ar trebui să fie încurajate să implice o gamă largă de actori și programe în prevenirea criminalității informatice, inclusiv instituțiile responsabile de educarea elevilor și a studenților, după modelul acțiunilor realizate de Ministerul Educației din România; (cf. 4.3, 4.4.1, 4.4.2, 6.2.3, 8.1, 8.3 și 8.4)

8. Statele membre ar trebui să analizeze fiabilitatea desfășurării unor formări în comun în materie de criminalitate informatică (care să acopere ciclul de viață al cazurilor de criminalitate informatică) pentru polițiști, procurori și judecători, precum și fiabilitatea utilizării, în acest scop, a unei platforme precum CYBER-EX în România, care să implice reprezentanți ai poliției, ai autorităților de urmărire penală și judiciare și ai sectorului privat drept participanți și formatori; (cf. 8.1 și 8.4)

9. Statele membre ar trebui să încurajeze și să sprijine judecătorii care au inițiative de organizare a mai multor ocazii de formare pentru a ridica gradul de conștientizare cu privire la criminalitatea informatică, în cooperare cu poliția și procurorii; (cf. 8.1 și 8.4)

10. Statele membre ar trebui să aibă în vedere înființarea unei rețele de magistrați specializați în materie de criminalitate informatică, printre altele în vederea facilitării diseminării celor mai bune practici în rândul practicienilor; (cf. 8.1 și 8.4)

11. Instituțiile UE ar trebui să încurajeze și să sprijine în continuare inițiative de organizare a unor formări care să acopere întregul ciclu de viață al cazurilor de criminalitate informatică, adresate poliției, procurorilor și judecătorilor; (cf. 8.1 și 8.4)

12. Instituțiile UE ar trebui să adreseze problema păstrării datelor cât mai curând posibil; (cf. 3.2 și 3.5)

9.2.3 Recomandări adresate Eurojust/Europol/ENISA

1. ENISA ar trebui să analizeze modalități de standardizare a conceptului de „alerte cibernetice” colectate și transmise de sistemele automate, care ar permite ca statisticile privind aceste alerte să fie comparabile și armonizate în toate statele membre; (cf. 7.1.2 și 7.6)

2. Eurojust ar trebui să aibă în vedere colectarea și diseminarea celor mai bune practici la nivel național, identificate din cazurile Eurojust, în special în cazurile în care este implicată cooperarea judiciară în materie penală; (cf. 7.1.2 și 7.6).

ANNEX A: PROGRAMME FOR THE ON-SITE VISIT AND PERSONS INTERVIEWED/MET

Monday, 19 January 2015, Bucharest		Participants
	Arrival of the delegation	
17h30 – 19h00	Informal meeting at the hotel bar	Romanian Police, Ministry of Justice, Public Ministry
Tuesday, 20 January 2015, Bucharest (The National Police headquarters)		
9h00- 10h00	Welcoming remarks	High-level officials from the Ministry of Internal Affairs, Romanian Police, Ministry of Justice, Public Ministry, Romanian Intelligence Service, CERT-RO, Ministry of National Education
Short break		
10h00-10h45	Introduction from the evaluation team and general discussion	Representatives from the Ministry of Internal Affairs, Romanian Police, Ministry of Justice, Public Ministry, Romanian Intelligence Service, CERT-RO, National Authority on the Protection of Children, Ministry of Education
10h45-11h00	*Coffee break*	
11h00-11h15	Presentation of the relevant substantive law provisions on cybercrime	Ministry of Justice
11h15-11h30	Presentation of the procedural law provisions on cybercrime	Directorate for the Investigation of Organised Crime and Terrorism (DIOCT) within the Public Ministry - the Service for the Prevention and Fight against Cybercrime
11h30 – 12h30	Discussion	Representatives of the Ministry of Justice, Public Ministry and Romanian National Police
12h30-14h00	*Lunch break*	
14h00-14h10	Transfer to the Public Ministry	
14h10-15h10	Meeting with DIOCT	Representatives of the Service for the Prevention and Fight against Cybercrime and representatives of the International Cooperation Service
15h10-15h30	Transfer to the Romanian National Police	
15h30-17h00	Visit to the Romanian Cybercrime Unit Discussion on: organisation, responsibilities, inter-agency cooperation, cooperation with the private sector and international cooperation	Representatives of the Cybercrime Unit from the Romanian National Police
17h00	Closing and transfer to the hotel	

Wednesday, 21 January 2015, Bucharest		
9h00-9h30	Transfer to CERT-RO	
9h30-10h30	Meeting at CERT-RO Discussion on: organisation, responsibilities, running projects, inter-agency cooperation, international cooperation	Representatives of CERT-RO
10h30-11h00	Transfer to the Romanian Intelligence Service	
11h00-12h00	Meeting with the Romanian Intelligence Service Discussion on: organisation, responsibilities, the cyber security strategy, inter-agency cooperation, international cooperation	Representatives of the Romanian Intelligence Service
12h00-14h00	*Lunch break*	
14h00-14h30	Transfer to SELEC	
14.30-15.30	Meeting with SELEC	Representatives of Southeast European Law Enforcement Centre (SELEC)
15h30-16h00	Transfer to C-PROC	
16h00-17h30	Meeting with C-PROC	Representatives of the Council of Europe's Office on Cybercrime
19h30-22h00	*Dinner*	
Thursday, 22 January 2015, Craiova		**Participants**
8h00-11h00	Travel from Bucharest to Craiova	
11h00-13h00	Meeting at Prosecutor's Office and Police Cybercrime Unit from Craiova Discussion on: organisation, responsibilities, cases, cooperation	Representatives of the Prosecutor's Office, the Police Cybercrime Unit (Craiova),
13h00-14h30	*Lunch break*	
14.30-17.30	Travel from Craiova to Bucharest	

Friday, 23 January 2015, Bucharest (The National Police)		**Participants**
9h00-9h30	Transfer to the Romanian National Police	
9h30-10h00	Overview of the evaluation visit	Representatives from the Ministry of Internal Affairs, Romanian Police, Ministry of Justice, Public Ministry, Romanian Intelligence Service, CERT-RO, National Authority on the Protection of Children, Ministry of Education
10h30-10h45	*Coffee break*	
10h45-12h00	General remarks and conclusions	
12h00	*Lunch and departure of the experts*	
End of the visit		

-/-

ANNEX B: PERSONS INTERVIEWED/MET

MEMBERS OF THE DELEGATIONS			
	Name	**Institution**	**Contact details**
ROMANIA	**Ministry of Internal Affairs**		
	Ms Claudia VIŞOIU	Deputy Director Directorate for European Affairs and International Relations	claudia.visoiu@mai.gov.ro
	Ms Simona ŞTEFAN	Head of Service Directorate for European Affairs and International Relations	
	Ms Diana BĂDESCU	Expert Directorate for European Affairs and International Relations	sae@mai.gov.ro
	The General Inspectorate of the Romanian Police		
	Mr Virgil SPIRIDON	Deputy Inspector-General General Inspectorate of the Romanian Police	virgil.spiridon@root.ro
	Mr Marius ROMAN	Director Directorate for European Affairs, Missions and International Relations	marius.roman@mai.gov.ro
	Mr Marcel PATATU	Head of Service Service for Combating Cybercrime Directorate for Combating Organised Crime	cybercrime@politiaromana.ro
	Mr Andrei LINŢĂ	Head of Office European Affairs Unit Directorate for European Affairs, Missions and International Relations	integrare@politiaromana.ro
	Ms Mihaela RADU	Specialist officer European Affairs Unit Directorate for European Affairs, Missions and International Relations	mihaela.radu@politiaromana.ro

	Mr Daniel FILIP	Head of office Service for Combating Cybercrime Directorate for Combating Organised Crime	Dl. Daniel FILIP
	Mr Paul ROMAN	Head of Office Service for Combating Cybercrime Directorate for Combating Organised Crime	Dl. Paul ROMAN
	Mr Silviu CRIŞAN	Head of Office Service for Combating Cybercrime Directorate for Combating Organised Crime	Dl. Silviu CRIŞAN
	Mr Bogdan BADIU	Head of Office Service for Combating Cybercrime Directorate for Combating Organised Crime	Dl. Bogdan BADIU
	The Public Ministry Directorate for the Investigation of Organised Crime and Terrorism (DIOCT) Service for the Prevention and Fight against Cybercrime		
	Ms Ioana ALBANI	Chief Prosecutor	albani_ioana@mpublic.ro
	Ms Camelia STOINA	Prosecutor	
	Mr Viorel BADEA	Chief Prosecutor	
	Mr Cătălin CAMBURI	Chief Prosecutor	
	Ms Silvia POPA	Prosecutor	
	Ms Elena DINU	Prosecutor	
	Mr Marius CRIVAT	Prosecutor	

	Ministry of Justice		
	Ms Viviana ONACA	Director Directorate for International Law and Judicial Cooperation	vonaca@just.ro
	Ms Cristina SCHULMAN	Legal adviser having the status of judge/prosecutor Treaties, International Relations and Liaison Magistrates Unit Directorate for International Law and Judicial Cooperation	cschulman@just.ro
	Ms Raluca SIMION	Legal adviser having the status of judge/prosecutor Service for Judicial Cooperation in Criminal Matters Directorate for International Law and Judicial Cooperation	rsimion@just.ro
	Ms Mihaela MEREUȚĂ	Counsellor for European Affairs Directorate for European Affairs and Human Rights	mihaela.mereuta@just.ro
	Romanian Intelligence Service		
	Mr Florin COSMOIU	Colonel	florin.cosmoiu@cyberint.ro
	Mr Gabriel MAZILU	Colonel	
	Mr Lucian MARINESCU	Captain	
	Mr Cristian CONDREA	Colonel	
	Ms Luiza IORDACHE	Major	
	CERT-RO		
	Mr Augustin JIANU	Director-General	
	Mr Mircea GRIGORAS	Deputy Director-General	
	Mr Dan TOFAN	Technical Director	
	Mr Daniel IONITA	Head of the Legal, Analyses and Policies Department	daniel.ionita@cert-ro.eu

	National Authority on the Protection of Children		
	Mr Octavian CIOBA	Senior Counsellor	octavian.cioba@anpdca.ro
	Ministry of Education and Scientific Research		
	Mr Eugen STOICA	Department for Education and Lifelong Learning	eugen.stoica@medu.edu.ro
	Ms Megdonia PĂUNESCU	Counsellor Department for Education and Lifelong Learning	megdonia@gmail.com megdonia.paunescu@medu.edu.ro
	Ms Daniela CĂLUGĂRU	General Inspector Department for Education and Lifelong Learning	calugaru.daniela@gmail.com daniela.calugaru@medu.edu.ro

-//-

ANNEX C: LIST OF ABBREVIATIONS/GLOSSARY OF TERMS

LIST OF ACRONYMS, ABBREVIATIONS AND TERMS	ROMANIAN ACRONYM OR ACRONYM IN ORIGINAL LANGUAGE	ROMANIAN ACRONYM OR ACRONYM IN ORIGINAL LANGUAGE	ENGLISH
AFP	*AFP*		Australian Federal Police
BCEAR	*BCEAR*		Bucharest Centre for Educational Assistance and Resources
CCEAR	*CCEAR*		County Centre for Educational Assistance and Resources
CEPOL	*CEPOL*		European Police College
CERT-RO	*CERT-RO*		Romanian National Computer Security Incident Response Team
CINI	*CINI*		Cyber-Infrastructures of National Interest
CPC	*CPC*		Criminal Procedure Code
C-PROCMSINF	*C-PROC*		Cybercrime Programme Office of the Council of Europe
CSAT	*CSAT*		Supreme Council of National Defence
	CSNS		Cyber-Security National System
CYBER-EX	*CYBER-EX*		Cybercrime Centre of Excellence
DIOCT	*DIOCT*		Directorate for Investigating Organised Crime and Terrorism
DIPI	*DIPI*		Department for Information and Internal Protection
ECTEG	*ECTEG*		European Cybercrime Training and Education Group

LIST OF ACRONYMS, ABBREVIATIONS AND TERMS	ROMANIAN ACRONYM OR ACRONYM IN ORIGINAL LANGUAGE	ROMANIAN ACRONYM OR ACRONYM IN ORIGINAL LANGUAGE	ENGLISH
EWS	*EWS*		Early Warning and real-time information System
ISF	*ISF*		Internal Security Funds
MSINF	*MSINF*		Ministry for the Information Society
NACPA	*NACPA*		National Authority for Child Protection and Adoption
NFSI	*NFSI*		National Forensic Science Institute
OCCS	*OCCS*		Operational Council of Cyber-Security
RIS	*RIS*		Romanian Intelligence Service
RNP	*RNP*		Romanian National Police's Service for Combating Crime
SCND	*SCND*		Supreme Council of National Defence

-//-

ANNEX D: ROMANIAN LEGISLATION

The relevant crimes are criminalised under the following chapters in the **Criminal Code**:

Title II. Offences against property. Chapter IV - Fraud perpetrated using computer systems and electronic payment methods

Title VI. Forgery offences. Chapter III - Counterfeiting documents

Title VII. Offences against public security. Chapter VI - Offences against the security and integrity of computer systems and data

Title I. Offences against individuals. Chapter VIII- Offences against sexual freedom and integrity

Title VIII. Offences that harm social cohabitation relationships. Chapter I - Offences against public order

Title II. Offences against property. Chapter IV- Fraud perpetrated using computer systems and electronic payment methods

Article 249 - Computer fraud

Entering, altering or deleting computer data, restricting access to such data or hindering in any way the operation of a computer system in order to obtain a benefit for oneself or another, if it has caused damage to a person, shall be punishable by no less than two and no more than seven years of imprisonment.

Article 250 - Making fraudulent financial operations

(1) Making cash withdrawal operations, loading or unloading of an electronic money instrument or a fund transfer instrument, by using, without the consent of the owner, an electronic payment instrument or the identification information that allows its use, shall be punishable by no less than two and no more than seven years of imprisonment.

(2) The same penalty is applicable to the operations referred to in paragraph (1), performed by means of the unauthorised use of any identification information or by using false identification data.

(3) The unauthorised transmission to another person of any identification information, in order to perform one of the operations referred to in paragraph (1), shall be punishable by no less than one and no more than five years of imprisonment.

Title VI. Forgery offences. Chapter III - Counterfeiting documents

Article 325 - Computer data forgery

Unauthorised input, alteration or deletion of computer data, or unauthorised restriction of access to such data, resulting in inauthentic data to be used to produce legal consequences, constitutes an offence and shall be punishable by no less than one and no more than five years of imprisonment.

Title VII. Offences against public security. Chapter VI - Offences against the security and integrity of computer systems and data

Article 360 - Illegal access to a computer system

(1) Unauthorised access to a computer system shall be punishable by no less than three months and no more than three years of imprisonment or by a fine.

(2) The act referred to in paragraph (1), perpetrated in order to obtain computer data, shall be punishable by no less than six months and no more than five years of imprisonment.

(3) If the act referred to in paragraph (1) was perpetrated a computer system to which, through processes, devices or specialised programmes, access is restricted or prohibited for certain categories of users, it shall be punishable by no less than two and no more than seven years of imprisonment.

Article 36 - Illegal interception of computer data transmissions

(1) Unauthorised interception of a computer data transmission which is not public and which is intended for a computer system, originates from such a computer system or is carried out within a computer system shall be punishable by no less than one and no more than five years of imprisonment.

(2) The same penalty shall apply to the unauthorised interception of electromagnetic emissions from a computer system containing computer data which is not for public information.

Article 362 - Altering computer data integrity

Illegally altering, deleting or damaging computer data or restricting access to such data shall be punishable by no less than one and no more than five years of imprisonment.

Article 363 - Disruption of the operation of computer systems

The act of seriously disrupting, without authorisation, the operation of a computer system by inputting, transmitting, modifying, deleting or damaging data, or by restricting access to data, shall be punishable by no less than two and no more than seven years of imprisonment.

Article 364 Unauthorised transfer of computer data

The unauthorised transfer of computer data from a computer system or from a data storage device shall be punishable by no less than one and no more than five years of imprisonment.

Article 365 Illegal operations with devices or software

(1) Any person who illegally produces, imports, distributes or makes available in any form:

(a) devices or software designed or adapted for the purpose of perpetrating any of the offences referred to in Articles 360 - 364;

(b) passwords, access codes or other such computer data allowing full or partial access to a computer system for the purpose of perpetrating any of the offences referred to in Articles 360 - 364shall be punishable by no less than six months and no more than three years of imprisonment or by a fine.

(2) Illegally owning a software program, password, access code or other data as mentioned in paragraph (1), with the purpose of perpetrating any of the offences referred to in Articles 360 - 364, shall be punishable by no less than three months and no more than two years of imprisonment or by a fine.

Title VIII. Offences that harm relationships of social cohabitation. Chapter I - Offences against public order

Article 374 - Child pornography

(1) The production, possession for display or distribution, purchase, storage, display, promotion, distribution and provision, in any manner, of child pornography shall be punishable by no less than one and no more than five years of imprisonment.

(2) If the acts referred to in paragraph ?? are perpetrated via a computer system or other means of data storage, they shall be punishable by no less than two and no more than seven years of imprisonment.

(3) The act of unlawfully accessing child pornography through computer systems or other means of electronic communication shall be punishable by no less than three months and no more than three years of imprisonment or by a fine.
(4) Child pornography means any material that shows a minor displaying sexually explicit behaviour or that, even if not showing a real person, simulates in a credible manner a minor displaying such behaviour.
(5) Any such attempt shall be also punished.

Article 6 of Law No 365/2002 (republished) sets out the legal conditions for transmitting commercial communications via electronic mail, i.e commercial communications via electronic mail are forbidden, except where the recipient has expressed his or her agreement to receiving such communications.
Infringement of this rule is considered a contravention, pursuant to Article 22, indent 1, item a, of Law No 365 (republished).
In practice, however, depending on the content or the amount of communications, the act of transmitting commercial communications via electronic mail may constitute an actual offence, either as committed by a perpetrator (Article 363 of the Criminal Code or Article 325 of the Criminal Code) or by an accomplice to one or more computer offences.

Trafficking in underage persons (Article 211)
(1) Recruitment, transportation, transfer, harbouring or receipt of a minor for the purpose of his her exploitation shall be punishable by no less than three and no more than 10 years of imprisonment and a ban on the exercise of certain rights.
(2) If such act was perpetrated under the terms of Article 210 paragraph (1) or by a public servant while fulfilling his or her professional duties and prerogatives, it shall be punishable by no less than five and no more than twelve years of imprisonment and a ban on the exercise of certain rights.
(3) The consent of an individual who is a victim of trafficking does not represent grounds for justification of the act.

Exploitation of persons **(Article 182)**

Exploitation of persons means:

(a) forcing a person to carry out work or tasks;

(b) enslavement or other similar procedures implying deprivation of freedom;

(c) forcing persons into prostitution, pornography - with a view to obtaining and distributing pornographic material - or any other types of sexual exploitation;

(d) forcing persons into mendicancy;

(e) illegal collection of body organs, tissues or other cells.

Rape **(Article 218)**

(1) Sexual intercourse, oral or anal intercourse with a person, perpetrated by constraint, by rendering the person in question unable to defend themselves or to express their will, or by taking advantage of such state, shall be punishable by no less than three and no more than 10 years of imprisonment and a ban on the exercise of certain rights.

(2) The same penalty shall apply to any act of vaginal or anal penetration perpetrated under paragraph (1).

(3) It shall be punishable by no less than five and no more than twelve years of imprisonment and a ban on the exercise of certain rights, when:

(a) the victim is entrusted to the perpetrator for care, protection, education, safeguarding or treatment;

(b) the victim is a first degree relative, i.e. brother or sister;

(c) the victim has not reached the age of 16 years;

(d) the act was perpetrated for the production of pornography;

(e) the act resulted in bodily injury;

(f) the act was perpetrated by two or more individuals, acting together.

(…)

Sexual assault **(Article 219)**

(1) An act with a person that is sexual in nature, other than the acts referred to in Article 218, and is perpetrated by constraint, by rendering the person in question unable to defend themselves or to express their will or by taking advantage of such state, shall be punishable by no less than two and no more than seven years of imprisonment and a ban on the exercise of certain rights.

(2) It shall be punishable by no less than three and no more than 10 years of imprisonment and a ban on the exercise of certain rights, when:

(a) the victim is entrusted to the perpetrator for care, protection, education, safeguarding or treatment;

(b) the victim is a first degree relative, i.e. brother or sister;

(c) the victim has not reached the age of 16 years;

(d) the act was perpetrated for the production of pornography;

(e) the act resulted in bodily injury;

(f) the act was perpetrated by two or more individuals, acting together.

(…)

Sexual intercourse with a minor **(Article 220)**

(1) Sexual intercourse, oral or anal sex, as well as any act of vaginal or anal penetration perpetrated against a minor aged 13 to 15 years old, shall be punishable by no less than one and no more than five years of imprisonment.

(2) The acts referred to in paragraph (1), perpetrated against a minor who has not reached the age of 13, shall be punishable by no less than two and no more than seven years of imprisonment and a ban on the exercise of certain rights.

(3) The acts referred to in paragraph (1), perpetrated against a minor aged 13 to 18 by a person of the age of majority who abused their authority or influence over the victim, shall be punishable by no less than two and no more than seven years of imprisonment and a ban on the exercise of certain rights.

(4) The acts referred to in paragraphs (1) to (3) shall be punishable by no less than three and no more than 10 years of imprisonment and a ban on the exercise of certain rights, when:

(a) the minor is a first degree relative, i.e. brother or sister;

(b) the minor is entrusted to the perpetrator for care, protection, education, safeguarding or treatment;

(c) the act was perpetrated for the production of pornography.

(…)

Sexual corruption of minors **(Article 221)**

(1) Perpetrating an act that is sexual in nature, other than the acts referred to in Article 220, against a minor who has not reached the age of 13, as well as forcing a minor to endure or carry out such an act, shall be punishable.

(4) Child pornography means any material which shows a minor displaying sexually explicit behaviour or which, even if not showing a real person, simulates in a credible manner a minor displaying such behaviour.

(5) Any such attempt shall be also punished.

Note: Romania penalises the transmission of pornographic material involving minors irrespective of the manner in which such material is transmitted (for example, via mobile phone).

Harassment (Article 208)

(1) The act of an individual who repeatedly, with or without a legitimate interest, pursues an individual or observes their domicile, workplace or other places frequented by them, thus provoking a state of fear in them, shall be punishable by no less than three and no more than five years of imprisonment.

(2) It shall be punishable by no less than two and no more than seven years of imprisonment and a ban on the exercise of certain rights, when:

(a) the minor is a first degree relative, i.e. brother or sister;

(b) the minor is entrusted to the perpetrator for care, protection, education, safeguarding or treatment;

(c) the act was perpetrated for the production of pornography.

(3) A sexual act of any nature, perpetrated by a person of the age of majority in the presence of a minor who has not reached the age of 13, shall be punishable by no less than six months and no more than two years of imprisonment or by a fine.

(4) Where a person of the age of majority forces a minor who has not yet reached the age of 13 to witness the perpetration of acts that are exhibitionist in nature or shows or performances in which sexual acts of any kind are perpetrated, and makes available to the minor materials that are pornographic in nature, such act shall be punishable by no less than three months and no more than one year of imprisonment or by a fine.

(5) The acts referred to in paragraph (1) shall not be punished if the age difference does not exceed three years.

Recruitment of minors for sexual purposes **(Article 222)**

The act of an individual of the age of majority proposing to a minor who has not yet reached the age of 13 to meet for the purposes of the perpetration of one of the acts referred to in Article 220 or Article 221, including when such proposal has been made using remote means, shall be punishable by no less than one month and no more than one year of imprisonment or by a fine.

The following definitions are used in Romanian law:

Article 35 of Law No 161/2003

(1) In this title, the following words and expressions have the following meaning:

(a) 'computer system' means any device or group of interconnected or related devices, of which one or more ensure the automatic processing of data by using a computer program;

(b) 'automatic data processing' means the process by which data from a computer system are processed through a computer program;

(c) 'computer program' means a set of instructions that can be performed by a computer system to achieve a specific result;

(d) 'computer data' means any representation of facts, information or concepts in a form that can be processed by a computer system. This category includes any computer program that can determine performance of a function by a computer system;

(e) 'service provider' shall mean:

1. any natural or legal person that offers users the ability to communicate through computer systems;

2. any other natural or legal person that processes or stores data for the persons referred to under point 1 and for users of services provided by them;

(f) 'data on traffic information' shall mean any computer data related to a communication made via a computer system and its products, which is part of the communication chain, indicating the origin, destination, route, time, date, size, volume and duration, and type of service used for communication;

(g) 'user data' shall mean any information that may lead to the identification of a user, including type of communication and service used, address, geographical location, phone numbers or any other access numbers and manner of payment of that service, and any other data that may lead to identification of the user;

(h) 'security measures' shall mean the use of procedures, tools or specialised computer programmes by which access to a computer system is restricted or prohibited for certain categories of users;

(i) 'child pornography' shall mean any material that shows a minor displaying explicit sexual behaviour or an adult who is presented as a minor displaying explicit sexual behaviour or images which, while not representing a real person, simulates in a credible manner a minor displaying explicit sexual behaviour.

(2) Within the meaning of this Title, persons in one of the following situations are deemed to act illegally if:

(a) they are not authorised by law or a contract;

(b) they exceed the limits of authorisation;

(c) they do not have permission from the person or entity responsible, by law, to grant, use, manage or control a computer system or to conduct scientific research or perform any other operation in a computer system.

The Criminal Code

Article 181 - Computer systems and electronic data

(1) 'Computer systems' means any device or group of (functionally) interconnected devices, where one or several of such systems ensure automatic processing of data, using a computer program.

(2) 'Electronic data' means any representation of acts, information or concepts in a manner which allows processing by means of a computer system.

The Criminal Procedure Code

Article138

(4) A 'computer system' is any device or combination of devices interconnected between them or in a functional relationship, one or more of which provide automatic data processing by means of a computer program.

(5) 'Computer data' is any representation of facts, information or concepts in a form appropriate for processing in a computer system, including a program able to determine the performance of a function by a computer system.