CAPITOLUL VII
CRIMINALITATEA INFORMATICĂ

1. Concept şi caracterizare

Dezvoltarea permanentă a tehnicilor informaţionale şi apariţia unor mijloace noi de legătură şi comunicarea între persoane au avut o influenţă benefică pentru viaţa economică, socială şi politică a lumii, însă au dus la proliferarea fenomenului infracţional, care a înregistrat noi forme de manifestare a criminalităţii. Este vorba de criminalitatea informatică ce reprezintă o ameninţare gravă, în condiţiile în care aproape toate domeniile vieţii sociale se bazează pe sisteme informatice[442].

Criminalitatea informatică cunoaşte o evoluţie rapidă datorită vulnerabilităţilor asociate sistemelor informatice, posibilităţilor de acţionare la distanţă mare şi de a îndepărta complet evidenţele privind momentul şi modul clar de săvârşire a infracţiunilor informatice[443].

Evoluţia criminalităţii informatice este favorizată şi de caracterul său transfrontalier, în condiţiile în care folosirea sistemelor informatice şi a reţelelor de comunicaţii, legitimă sau nu, depăşeşte frontierele statelor.[444] S-a exprimat opinia că mondializarea reţelelor informatice a dus la apariţia unor noi forme ale delincvenţei, însă şi la dezvoltarea unei conştiinţe

[442] Maxim Dobrinoiu, Infracţiuni în domeniul informatic, Ed.C.H.Beck, Bucureşti, 2006, p.59.
[443] Ioana Vasiu, Lucian Vasiu, Criminalitatea în cyberspaţiu, Ed.UJ, Bucureşti, 2011, p.121.
[444] Gheorghe Ionuţ Iulian, Infracţiunile din sfera criminalităţii informatice, - Încriminare; investigare, prevenire şi combatere, Ed.UJ, Bucureşti, 2011, p.53.

internaţionale pentru organizarea luptei împotriva acestui fenomen nociv[445].

Unii autori vorbesc de un drept penal informatic care va constitui pe viitor, în aproape toate ordinile juridice, un sector nou şi autonom marcat de trăsăturile specifice, rezultat dintr-o activitate legislativă şi jurisprudenţială în expansiune în creştere în ultimii ani[446]. Totuşi, acest drept prezintă o mare eterogeneitate cât priveşte izvoarele normative, modelele de inspiraţie, termenele şi domeniile de intervenţie, ceea ce impune legiuitorilor naţionali introducerea unor reglementări uniforme şi armonizate între ele în domeniul criminalităţii informatice.

2. Reglementarea criminalităţii informatice la nivel european

Caracterul specific al criminalităţii informatice a impus o soluţie combinată, în care agenţiile şi oficiile create pentru a asigura aplicarea reglementărilor în domeniu, şi organizaţiile din sectorul public şi privat colaborează în vederea identificării soluţiilor optime[447].

Activitatea desfăşurată la nivelul Consiliului Europei şi a Uniunii Europene pentru combaterea criminalităţii informatice s-a materializat în adoptarea unor documente prin care s-a dispus legiuitorilor naţionali adoptarea unor reglementări uniforme sau armonizate între ele.

[445] Jean Pradel, Droit pénal européen (2009), op. cit., p.209.
[446] Lorenzo Picotti, Biens juridiques protégés et techniques de formulation des incriminations en droit pénal de l'informatique, Revue internationale de Droit Pénal, nr.77(314), 2, érès, 2006, p.525.
[447] Mariana Zainea, Raluca Simion, Infracţiuni în domeniul informatic,Culegere de practică judiciară, Ed. C.H. Beck, Bucureşti, 2009, p.20.

2.1. Reglementări ale Consiliului Europei în domeniul criminalităţii informatice.

La nivelul Consiliului Europei au fost adoptate mai multe Recomandări şi anume[448]: R/85/10 despre aplicarea în practică a Convenţiei de extrădare judiciară cu privire la comisia rogatorie pentru supravegherea telecomunicaţiilor; R/88/2 despre măsurile vizând combaterea pirateriei în domeniul drepturilor de autor; R/87/15 privind reglementarea folosirii datelor cu caracter personal în sectorul poliţiei; R/95/4 despre protecţia datelor cu caracter personal în domeniul serviciilor de telecomunicaţie şi R/89/9 despre criminalitatea în relaţia cu ordinatorul, adoptată la 13 septembrie 1989. Asociaţia Internaţională de Drept Penal a aprobat liniile directoare propuse legiuitorilor naţionali conţinute în această recomandare, în cadrul Congresului internaţional de drept penal, care a avut loc la Rio de Janeiro, în perioada 4 – 10 septembrie 1994[449]. Lista minimală a actelor pentru care Consiliul Europei recomandă încriminarea, dacă sunt comise intenţionat este cuprinsă în Secţiunea a II-a privind infracţiunile informatice şi alte crime împotriva tehnologiei informatice, inclusă în rezoluţia adoptată de congres şi se referă la[450]: frauda privind ordinatorul; falsul informatic; prejudiciul cauzat datelor şi programelor informatice; sabotarea ordinatorilor; accesul neautorizat; interceptarea neautorizată; reproducerea neautorizată a unui program informatic protejat; reproducerea neautorizată a unei topografii.

Rezoluţia nr.1 a fost adoptată de către miniştrii europeni de justiţie la cea de a 21-a Conferinţă ţinută la Praga în luna iulie 1997, prin care se recomandă Comitetului de

[448] Jean Pradel, în colab., op.cit. (2009), p.209.
[449] Résolutions des Congrès de l'Association Internationale de Droit Penal (1926-2014), RIDP , nr.86(1/2), érès, 2015, p.147.
[450] Ibidem, p.154.

ministri să susţină activitatea asupra criminalităţii informatice desfăşurate de Comitetul european pentru probleme criminale, în vederea apropierii legislaţiilor penale naţionale şi de a permite folosirea mijloacelor de investigare eficiente în materia infracţiunilor informatice[451].

Prin planul de acţiune adoptat de către şefii de state şi de guverne membre ale Consiliului Europei, cu prilejul celui de-al 20-lea Summit, desfăşurat la Strasbourg, în luna octombrie 1997, s-a pus problema găsirii unor soluţii comune la dezvoltarea noilor tehnologii de informaţie, bazate pe normele şi valorile Consiliului Europei.

La 23 noiembrie 2001 a fost adoptată la Budapesta Convenţia privind criminalitatea informatică, care a fost ratificată de România prin Legea nr.64/2004[452]. Acest instrument a fost completat prin Protocolul adiţional privind încriminarea actelor de natură rasistă şi xenofobă comise cu ajutorul sistemelor informatice, semnat la Strasbourg la 28 ianuarie 2003. Această Convenţie a fost aprobată de numeroase state,chiar din afara Europei, cum ar fi SUA, Canada, Japonia şi Africa de Sud[453].

Convenţia a definit în Secţiunea I, nouă tipuri de încriminări fundamentale şi anume[454]: accesul ilegal (art.2), interceptarea ilegală (art.3), atentate la integritatea datelor (art.4) şi la sistemele informatice (art.5), abuzul de dispozitive (art.6), infracţiuni clasice, falsul informatic (art.7) şi frauda infomatică (art.8), delicte privind pornografia infantilă (art.9) şi infracţiuni legate de atentate la proprietatea intelectuală (art.10).

Recomandările Consiliului Europei din 1989 sau Convenţia privind criminalitatea informatică din 2001 au lăsat întotdeuna o largă marjă de apreciere legiuitorilor naţionali în

[451] J. Pradel, Droit pénal européen (2009), op. cit., p.209.
[452] Publicată în M.Of. nr.343 din 24.04.2004.
[453] Lorenzo Picotti, op. cit., p.536.
[454] Ibidem, p.536.

alegerea formulărilor normative, a tipului şi de stabilire a sancţiunilor[455].

La 15 octombrie 2013 a fost semnat la Strasbourg un memorandum de înţelegere între Consiliul Europei şi Guvernul României prin care s-a convenit instituirea la Bucureşti a Oficiului Consiliului Europei în domeniul criminalităţii informatice, cu misiunea de a asigura implementarea proiectelor de asistenţă tehnică în domeniul criminalităţii informatice de către Consiliul Europei, inclusiv proiecte comune cu Uniunea Europeană[456].

2.2. Reglementările Uniunii Europene în domeniul criminalităţii informatice.

În elaborarea unor documente privind criminalitatea informatică Uniunea Europeană a avut în vedere reglementările adoptate de Consiliul Europei, în deosebi Convenţia din 28 ianuarie 1981 pentru protecţia persoanelor în ceea ce priveşte prelucrarea automatizată a datelor cu caracter personal, care a fost ratificată de toate statele[457]. S-a constatat că sistemele informatice privind acest tip de date fac obiectul unor atacuri, inclusiv teroriste. Pentru a contracara o atare situaţie, Comisia şi Consiliul UE au elaborat un plan de acţiune, care a fost aprobat de către Consiliul European de la Santa Maria da Feira, din luna iunie 2000 şi cuprindea acţiuni privind întărirea securităţii reţelelor şi de combatere a delincvenţei informatice.

Prin Regulamentul CE nr.460/2004 al Parlamentului European şi al Consiliului din 10 martie 2004 s-a instituit Agenţia Europeană pentru Securizarea Reţelelor Informatice şi a Datelor cu scopul de a asigura o cooperare mai strânsă la

[455] Ibidem, p.528.
[456] www.just.ro.
[457] J. Pradel, Droit pénal européen (2009), op. cit., p.561.

nivel global pentru îmbunătățirea normelor de securitate a rețelelor informatice şi a datelor[458].

La 24 februarie 2005 a fost adoptată Decizia – cadru 2005/222/JAI a Consiliului privind atacurile împotriva sistemelor informatice[459], care reprezintă un punct de referință în cadrul reglementărilor în domeniul combaterii criminalității informatice la nivelul Uniunii Europene.

Obictivele acestei decizii- - cadru sunt de două feluri: garantarea ca atacurile împotriva sistemelor informatice să fie pasibile de sancţiuni penale efective, proporţionale şi disuasive prin armonizarea regulilor de drept penal, ameliorarea şi favorizarea cooperării judiciare. Prin decizia – cadru se defineşte sistemul informatic şi datele informatice (art.1 lit.a) şi b), accesul ilicit la sistemele informatice (art.2), atentatul la integritatea unui sistem (art.3), atentatul la integritatea datelor (art.4) ş.a.

Prin Strategia de securitate internă a Uniunii Europene în acțiune: cinci paşi către o Europă mai sigură[460] s-a prevăzut creşterea nivelui de securitate pentru cetăţeni şi întreprinderi în spațiul cibernetic.

În luna ianuarie 2013 a fost înfiinţat Centrul European pentru combaterea criminalității informatice (EC_3) ca parte a Europol, cu scopul de a constitui un punct de convergenţă în lupta împotriva criminalităţii cibernetice la nivelul Uniunii Europene.

La 12 august 2013 Parlamentul European şi Consiliul au adoptat Directiva 2013/40/UE[461] privind atacurile împotriva sistemelor informatice şi de înlocuire a Deciziei – cadru 2005/222/JAI a Consiliului, prin care se defineşte

458 Publicată în J.Of.L. 77/1 din 13.03.2013.
459 Publicată în J.Of.L 69/67 din 16.03.2005; Serge de Biolley, în colab., Code de droit pénal de l'UE (2013), op. cit., p.1247.
460 COM (2010) 673, 22.11.2010.
461 Publicat în J.Of. L 218/8/ din 14.08.2013.

conceptul de date informatice ca o reprezentare de fapte, informaţii sau concepte într-o formă adecvată pentru prelucrare într-un sistem informatic, inclusiv, un program care permite unui sistem informatic să execute o funcție.

3. Reglementarea criminalităţii informatice în România

3.1.Evoluţia legislativă .

Prin ratificarea Convenției Consiliului Europei privind criminalitatea informatică[462], adoptată la Budapesta la 23 noiembrie 2001 şi intrată în vigoare la 1 martie 2006, România şi-a asumat obligaţia de a transpune pe plan intern reglementările europene referitoare la acest domeniu.

Însă anterior, a fost adoptată Legea nr.16 din 6 martie 1995 privind protejarea topografiilor produselor semiconductoare[463], prin care s-a transpus pe plan intern Directiva nr.87/54/CEE din 16 decembrie 1986 a Consiliului privind protecţia juridică a topografiilor produselor semiconductoare[464].

La 14 martie 1996 a fost adoptată Legea nr.8 privind drepturile de autor şi drepturile conexe[465], modificată prin art.54 din Legea nr.187/2012, care a transpus pe plan intern Directiva nr.93/83/CEE din 27 septembrie 1993 a Consiliului privind armonizarea anumitor dispoziţii referitoare la dreptul de autor şi drepturile conexe aplicabile difuzării de programe prin satelit şi retransmise prin cablu[466].

[462] Legea nr.64/2004, publicată în M.Of. nr.343 din 20.04.2004.
[463] Republicată în M.Of. nr.824 din 6.10.2006.
[464] J.O.L 24 din 27.01.1987.
[465] Publicată în M.Of. nr.60 din 26.03.1996.
[466] J.O. L 248 din 6.10.1993.

Legea nr.161 din 19 aprilie 2003[467], cuprinde Titlul III privind prevenirea şi combaterea criminalităţii, fiind prevăzute prin art.42 – 47 infracţiunile contra confidenţialităţii şi integrităţii datelor şi sistetemelor informatice, texte care au fost abrogate prin art.130 pct.1 din Legea nr.167/2012.

Codul penal adoptat prin Legea nr.301/2004, care a fost abrogat prin art.446 alin.(2) din Legea nr.286/2009, a prevăzut în Capitolul I al Titlului X din Partea specială delicte contra confidenţialităţii şi integrităţii datelor şi sistemelor informatice.

În fine, prin noul Cod penal, adoptat prin Legea nr.286/2009[468], în vigoare de la 1 februarie 2014, sunt prevăzute în Capitolul VI din Titlul VII al Părţii speciale, infracţiunile contra siguranţei şi integrităţii sistemelor şi datelor informatice, fiind transpuse pe plan intern dispoziţiile Convenţiei Consiliului Europei privind criminalitatea informatică din 23 noiembrie 2001.

În baza Hotărârii Guvernului nr.1040 din 13 octombrie 2010[469], prevenirea şi combaterea criminalităţii informatice a devenit un obiectiv strategic.

Prin Hotărârea Guvernului nr.271/2013 pentru aprobarea Strategiei de securitate cibernetică a României şi a Planului de acţiune la nivel naţional privind implementarea Sistemului naţional de securitate cibernetică[470], s-a stabilit ca obiectiv strategic menţinerea unui mediu virtual sigur, cu un înalt grad de încredere, bazat pe infrastructurile cibernetice naţionale, care să constituie un important suport pentru securitatea naţională şi buna guvernare, pentru maximizarea beneficiilor cetăţenilor, mediului de afaceri şi ale societăţii româneşti în ansamblul ei.

[467] Publicată în M.Of. nr.279 din 21.04.2003.
[468] Publicat în M.Of. nr.510 din 24.07.2009.
[469] Publicată în M.Of. nr.721 din 28.10.2010.
[470] Publicată în M.Of. nr.296 din 23.05.2013.

3.2.Infracţiuni contra siguranţei şi integrităţii sistemelor şi datelor informatice.

3.2.1. Accesul ilegal la un sistem informatic[471].

Potrivit art.360 alin. (1) C.pen. infracţiunea constă în accesul fără drept, la un sistem informatic.

În baza alin. (2), infracţiunea este mai gravă, dacă fapta prevăzută în alin. (1), este săvârşită în scopul obţinerii de date informatice.

În fine, infracţiunea este mult mai gravă,, conform alin. (3), dacă fapta prevăzută în alin. (1) a fost săvârşită cu privire la un sistem informatic la care, prin intermediul unor proceduri, dispozitive sau programe specializate, acecesul este restricţionat sau interzis pentru anumite categorii de utilizatori.

Infracţiunea este preluată, fără modificări semnificative, din art.42 al Legii nr.161/2003 şi se regăseşte în art.615-ter. C.pen. italian, art.323-1 C.pen. francez şi art. 259 alin. (1) C.pen. al R. Moldova[472].

Prin sistem informatic, în sensul art.181 alin. (1) C.pen., se înţelege orice dispozitiv sau ansamblu de dispozitive interconectate sau aflate în relaţie funcţională, dintre care unul sau mai multe asigură prelucrarea automată a datelor, cu ajutorul unui program informatic.

Prin date informatice se înţelege orice reprezentare a unor fapte, informaţii sau concepte într-o formă care poate fi prelucrată printr-un sistem, aşa cum se menţionează în art.181 alin.(2) C.pen.

Prin acces se înţelege acţiunea de a programa, a executa un program, a intercepta, a instrui, a comunica, a depozita/arhiva/stoca, a recupera date sau oricare altă folosinţă

[471] Ioana Vasiu, în Explicaţiile noului Cod penal, vol. IV, Ed. U.J., Bucureşti, 2016, p.852; V. Păvăleanu, Drept penal special (2014), op,. cit., p.516.
[472] V.Păvăleanu, Drept penal special (2014), op. cit., p.516.

a unei surse oferită de computere, incluzând date sau programe pentru computere, sisteme de computere sau baze de date.

Pentru existenţa infracţiunii, fapta trebuie comisă fără drept.

Prin art.35 alin.(2) din Legea nr. 161/2003 se stabileşte sfera persoanelor care acţionează fără drept, respectiv persoanele care se află în una din următoarele situaţii: nu sunt autorizate în temeiul legii sau al unui contract, depăşesc limitele autorizării, nu au permisiunea din partea persoanei fizice sau juridice competente potrivit legii să acorde, de a folosi, administra sau controla un sistem informatic, ori de a desfăşura cercetări ştiinţifice sau de a efectua orice operaţiune într-un sistem informatic.

În practica judiciară s-a reţinut această infracţiune, în forma agravată prevăzută de art.42 alin.(1) şi (3) din Legea nr.161/2003, într-o cauză în care inculpatul a montat fără drept un dispozitiv de citire a benzii magnetice a cardurilor cu minicameră în scopul clonării de carduri pentru efectuarea de retrageri de numerar [473].

3.2.2. Interceptarea ilegală a unei transmisii de date informatice.

Infracţiunea este prevăzută de art.361 C.pen. în două variante normative: una în alin.(1), constând în interceptarea, fără drept, a unei trasmisii de date informatice care nu este publică şi care este destinată unui sistem informatic, provine dintr-un asemenea sistem sau se efectuează în cadrul unui sistem informatic, iar alta în alin.(2) şi priveşte interceptarea, fără drept, a unei emisii electromagnetice provenite dintr-un sistem informatic.

Această infracţiune a fost reglementată prin art.43 alin. (1) şi (2) din Legea nr.161/20003 şi face obiectul art.617-quarter şi art. 617-quinquies, art.617-sexies şi art.623 bis din

[473] ICCJ, s.pen., dec. nr.371 din 2.02. 2010, apud. T.Toader, Infracţiuni prevăzute în legi speciale, Ed. Hamangiu, ed. a 4-a, Bucureşti, 2011, p.311.

Codul penal italian[474], precum şi a art.260[1] C.pen. al R. Moldova, text introdus prin Legea nr.278-XVI din 18.12.2008.

Noua reglementare este în concordanţă cu exigenţele impuse prin art.3 din Convenţia Consiliului Europei privind criminalitatea informatică din 23 noiembrie 2001 şi art.6 al Directivei 2013/40/UE din 12 august 2013.

Încriminarea interceptării ilegale în legislaţia penală face parte dintre măsurile (juridice şi tehnice) care vizează protejarea dreptului la secretul comunicaţiilor, în care se include şi dreptul la protecţia corespondenţei, statuat prin art.8 din Convenţia Europeană a Drepturilor Omului şi art.7 din Carta drepturilor fundamentale a Uniunii Europene, aplicabil tuturor formelor de transmitere electronică[475].

Prin interceptare se înţelege acţiunea de a capta, cu ajutorul unui dispozitiv electronic confecţionat în acest scop sau a unui computer, impulsurile electrice, variaţiile de tensiune sau emisiile electromagnetice care tranzitează interiorul unui sistem informatic sau se manifestă ca efect al funcţionării acestuia ori se află pe traseul de legătură dintre două sau mai multe sisteme informatice care comunică.

În toate cazurile, este vorba de interceptarea unei transmisii de date informatice, fără drept, care nu sunt publice.

3.2.3. Alterarea integrităţii datelor informatice.

Prin art.362 C.pen. se prevede fapta de a modifica, şterge sau deteriora date informatice ori de a redirecţiona accesul la aceste date, fără drept.

Infracţiunea a fost prevăzută de art.44 alin.(1) din Legea nr.161/2003, care reprezenta forma de bază, iar infracţiunile din alin.(2) şi (3) au fost încriminate separat prin art.364 C.pen.

[474] Ioana Vasiu, în Explicaţiile noului Cod penal (2016), vol.IV, op. cit., p.870.
[475] Ibidem, p.866.