

THE INFLUENCE OF EUROPEAN STANDARDS ON COMBATING CYBERCRIME ON ROMANIAN LEGISLATION

Oana Elena Gălățeanu
Assoc. Prof., PhD., „Dunărea de Jos” University of Galați

Abstract: Computer crime is one of the serious forms of cross-border crime, with its own manifestation features, which often make it difficult for the perpetrators to identify them. In this field of transnational crime, the different ways of interpreting certain legal terms of his own, as well as the various sanctions applicable at national level, represent obstacles in the conduct of police and criminal judicial cooperation, at least at European level. However, there are also some sectors of this crime, in which a unitary interpretation of relevant terms has been achieved, and among them is that of cybercrime.

The present study presents the concrete concerns and norms elaborated at European level in this field of cybercrime, as well as the way in which Romania understood, from the perspective of the criminal law, to comply with these European norms. In this regard, all the legal provisions, adopted at national level for the prevention and combating of this serious form of crime- the computer one- which, as observed worldwide, are gaining scope and, extremely quickly, new and ingenious modalities are specified of achievement.

Keywords: computer crime, European law, Romanian national law

I. Normele europene în materia criminalității informatice

Tehnologia și lumea virtuală în prezent reprezintă un domeniu de care se dovedește că actuala societate umană este total dependentă. Această dependență are în vedere aspect de la cele mai elementare pentru om-precum cel de a putea comunica și a se putea informa- până la domeniul mai complexe ale socialului precum, de exemplu, derularea vieții economice.

Acest tip de comunicare-virtual, mediul on-line- a dobândit în timp relativ scurt, puterea de a schimba vieți și mentalități, devenind un mediu prin care oamenii își pot exercita drepturi fundamentale. Însă, din păcate, acesta s-a dovedit a fi și un spațiu în care infracționalitatea a luat o mare amploare, devenind extrem de anevoioasă combaterea ei. În mediul on-line se produc, cu o frecvență în creștere, diverse forme de infracționalitate, de la furt de identitate, spionaj economic, control abuziv asupra a mase largi de cetățeni, până la pornografia infantilă prin sisteme informatice. Toate aceste forme grave de criminalitate, cu caracter transfrontalier (datorat tocmai acestui mediu virtual neîngrădit de frontiere terestre convenționale) îngrijorează toate statele lumii, conștiente că spațiul on line ar trebui să reprezinte un mediu sigur și de încredere pentru populație. Evident că aceeași preocupare există și la nivelul Uniunii Europene care este interesată ca în această sferă să intensifice cooperarea între statele membre și să elaboreze politici și strategii commune de Securitate cibernetică în domeniul virtual.

Până în prezent, în plan internațional nu s-a elaborat o definiție unitară a infracționalității informatice. La nivel european, Comunicarea Comisiei Europene adresată Parlamentului European, Consiliului și Comitetului European al Regiunilor, denumită " Către o politică generală de luptă împotriva criminalității cibernetice", vede această criminalitate ca

reprezentată de " infrafracțiunile comise prin utilizarea rețelelor de comunicare electronice și a sistemelor de informare sau împotriva unor astfel de rețele sau sisteme. " ¹

O caracteristică a criminalității informatice este adaptarea metodelor utilizate de infractori și dezvoltarea extrem de rapidă a lor, legate direct de evoluția tehnicilor informaționale și a varietății modalităților de utilizare a internetului.

În Europa, la nivelul U.E, cât și al Consiliului Europei, atenția a fost îndreptată către acest tip de infracționalitate începând din anii 2000, când s-a ajuns la înțelegerea realității că numai printr-o muncă comună și dispoziții legale asociate, s-ar putea soluționa cazuri grave care pun în pericol siguranța relațiilor comerciale și a cetățenilor.

La nivelul Consiliului Europei, printre instrumentele legislative inițiale stabilite în acest domeniu, e de menționat planul adoptat de șefii de state și de guverne membre ale acestuia, la cel de-al douăzecilea Summit, de la Strasbourg, din octombrie 1997, ce avea ca obiect identificarea unor rezolvări comune la realitatea dezvoltării tehnologiei și informaticii, bazate pe valorile și normele Consiliului. În acest sens a fost semnată la Budapesta, la 23 noiembrie 2001, Convenția privind criminalitatea informatică. Această convenție a fost ratificată și de state nemembre ale Consiliului Europei, printre care SUA și Canada. La această Convenție a fost elaborate și un Protocol additional, în 28 ianuarie 2003, la Strasbourg, care viza pedepsirea faptelor xenofobe și rasiste realizate cu sprijinul structurilor informatice.

România a ratificat Convenția Consiliului Europei prin Legea nr.64/2004². Convenția adoptată urmărește trei domenii³, respectiv:

1. armonizarea normelor de drept material în domeniul criminalității informatice;
2. definirea procedurilor de anchetă și de realizare a urmăririi penale în mod potrivit pentru realitatea globalizării rețelelor informatice;
3. constituirea unei colaborări la nivel internațional, eficiente și rapide.

La nivelul U.E, infracționalitatea informatică face prte din cele opt direcții de colaborare sub aspect operational ce sunt cuprinse în politicile unionale pentru lupta contra criminalității organizate și a infracțiunilor grave în plan internațional⁴.

În scopul găsirii acelor modalități de luptă contra acestui gen de criminalitate, a fost adoptat Regulamentul CE nr.460/2004 al Parlamentului European și Consiliului, în 10 martie 2004; prin acesta a fost create Agenția Europeană pentru Securitatea Rețelelor Informatice și a Datelor. S-a urmărit astfel realizarea unei cooperări globale reale pentru a se aduce îmbunătățiri normelor referitoare la optimizarea informațiilor, siguranță și recurgere la o viziune internațională unanimă față de aspectele ce țin de securitatea datelor și rețelelor informatice.

În anul 2013 a fost înființat Centrul European de combatere a criminalității informatice, ca fiind parte a Europol. Crearea lui a avut ca obiectiv formarea unui scop unic al acțiunii din cadrul Uniunii contra infracționalității cibernetice. S-a dorit ca în atribuțiile Centrului să intre următoarele elemente importante legate de criminalitatea informatică:

- acțiunile de criminalitate informatică ale grupurilor de criminalitate organizată și, cu precădere, cele care au ca urmare profituri mari;
- acte de criminalitate informatică orientate contra sistemelor informatice ale U.E

¹ Comunicarea Comisiei Europene adresată Parlamentului European, Consiliului și Comitetului European al Regiunilor, denumită " Către o politică generală de luptă împotriva criminalității cibernetice", COM(2007)

² Publicată în M.Of nr.343/20 apr.2004

³ I.Vasiu, L.Vasiu, Criminalitatea în cyberspațiu, Ed. Universul Juridic, București 2011, p.473

⁴ Ligia-Valentina Mirișan, Influența dreptului Uniunii Europene asupra dreptului penal român, Ed. Universul Juridic, București 2017,p.209

- acte de criminalitate informatică cu daune mari aduse victimelor(precum, de exemplu, exploatarea sexuală a minorilor pe internet)⁵.

Vizând același domeniu, Parlamentul European și Consiliul, în 12 august 2013 au adoptat Directiva 2013/40/UE⁶ referitoare la atacurile contra sistemelor informatice și înlocuirea Deciziei-cadru 2005/222/JAI a Consiliului ce avea același obiect. Ea are ca scop armonizarea sistemelor de drept penal ale statelor membre în ce privește atacurile contra sistemelor informatice prin instituirea unor norme minime privind definirea sancțiunilor și a infracțiunilor relevante, precum și îmbunătățirea cooperării dintre autoritățile competente⁷.

II. Dispozițiile penale naționale actuale în materie

România a înțeles faptul că dezvoltarea infracționalității informatice este sprijinită, printre alți factori(precum posibilitatea de a face să dispară certitudinile cu privire la modul și momentul exacte de comitere a acestui tip de infracțiuni, sau spațiul larg de acțiuni) și de caracterul ei transfrontalier, având în vedere că utilizarea sistemelor informatice și a rețelilor de comunicare se extend peste frontierele de stat⁸. ca stat european, România a conștientizat necesitatea implementării tuturor regulilor comunitare în domeniul prevenirii și combaterii criminalității informatice, transpunând în legislația internă normele cu caracter obligatoriu și manifestându-se în sensul îmbunătățirii modalităților de cercetare, identificare și sancționare a celor care comit asemenea fapte extrem de grave.

În acest sens, în anul 2013 guvernul României a încheiat la Strasbourg un Memorandum de înțelegere cu Consiliul Europei privitor la crearea Oficiului Consiliului Europei în sfera criminalității informatice și statutul acestuia, la 15 octombrie, la București. Scopul principal al acestui Oficiu e reprezentat de garantarea punerii în practică a proiectelor de asistență tehnică în acest domeniu, de către Consiliul Europei, chiar avându-se în vedere proiecte commune cu Uniunea Europeană.⁹

În plan intern a fost adoptată legea nr.161/2003 privind unele măsuri pentru asigurarea transparenței în exercitarea demnităților publice, funcțiilor publice și în mediul de faceri, prevenirea și sancționarea corupției¹⁰. Această lege trepune marea parte a dispozițiilor Convenției Consiliului Europei.

Actualul Cod penal cuprinde învinuirile, în sfera infracționalității informatice, aproape identice cu cele cuprinse anterior în Legea 161/2003, care însă, au fost abrogate din aceasta prin Legea 187/2012.¹¹ Noul Cod penal include, în Titlul VII al Părții speciale, în Cap. VI al lui, infracțiuni împotriva siguranței și integrității sistemelor și datelor informatice, transpunând astfel, în legislația internă, prevederile Convenției Consiliului Europei privind criminalitatea informatică, din 23 noiembrie 2001. Astfel, în prezent, potrivit dispozițiilor penale naționale, sunt sancționate ca fapte incluse în infracționalitatea de tip informatic:

I. *infracțiuni împotriva siguranței și integrității sistemelor și datelor informatice* precum: accesul ilegal la un sistem informatic(art.360Cod penal), interceptarea ilegală a unei transmisii de date informatice(art.361 Cod penal), alterarea integrității datelor informatice(art.362Cod penal), perturbarea funcționării sistemelor informatice(art.363 Cod penal),

⁵ Idem, p.210

⁶ Publicată în JOUE L 218/8 din 14 august 2013

⁷ Directiva 2013/40/UE, par.1, <http://eurlex.europa.eu/legal-content/RO/>

⁸ Vezi și Ghe.Ionuț Iulian, Infracțiunile din sfera criminalității informatice, incriminare, investigare, prevenire și combatere, Ed. Universul Juridic, București 2011, p.53

⁹ www.criminalitate-informatică.ro

¹⁰ Publicată în M.Of. nr. 279/21 aprilie 2003

¹¹ M.Of nr.737/12 nov.2012, lege de punere în aplicare a Legii 286/2009 privind Codul penal

transferul monitorizat de date informatice(art.364 Cod penal), operațiuni ilegale cu dispozitive sau programe informatice(art.365 Cod penal);

II. *infrațiuni informatice* precum: falsul informatic(art.325 Cod penal- Cap.III denumit Falsuri în înscrisuri, din Titlul VI- Infrațiuni de fals- al Părții speciale a Codului penal),frauda informatică(art.249Cod penal) ;

III. *pornografia infantilă* prin intermediul sistemelor informatice- potrivit art.374 alineatele (1) și (2) Cod penal care incriminează (la alin.(2)) cu o pedapsă cu închisoarea, mai mare- respectiv de la 2 ani la 7 ani- faptele prevăzute în alin.(1) ale aceluiași text de lege, comise "printr-un sistem informatic sau alt mijloc de stocare a datelor informatice".

Potrivit Hotărârii de Guvern nr.1040/13 octombrie 2010¹² pentru aprobarea Strategiei naționale de ordine publică 2010-2013, "cunoașterea, prevenirea și combaterea criminalității informatice" a ajuns să fie un obiectiv strategic pentru România.

A fost adoptată și Hotărârea de Guvern nr.271/2013¹³ pentru aprobarea Strategiei de Securitate cibernetică a României și a Planului de acțiune național referitor la implementarea Sistemului național de securitate cibernetică. Prin aceasta a fost decis ca fiind obiectiv strategic păstrarea unui mediu virtual sigur, cu grad de încredere ridicat, fundamentat pe infrastructurile cibernetice naționale, care să reprezinte un suport important pentru securitatea națională și buna guvernare, sporirea la maxim a beneficiilor cetățenilor, mediului de afaceri și societății românești în ansamblu.¹⁴

III. Concluzii

Intensificarea fenomenului infracțional cu elemente de extraneitate și transfrontaliere impune, evident, și la nivel european, o cooperare și o armonizare a statelor în materia penală, având în vedere sporirea pericolozității acestor infracțiuni care evoluează în forme de criminalitate organizată. Ideea de Uniune Europeană a fost bazată și pe conceperea unui spațiu de libertate și de securitate pentru cetățenii ei. Acesta a fost, credem, și unul dintre motivele care au determinat statele membre să accepte renunțarea la o parte dintre atributele propriei suveranități, în vederea exercițiului, în comun, la nivel de U.E a lor, cu intenția de a găsi cele mai bune soluții pentru bunul mers al acestei forme de organizare unională și pentru binele resortisanților lor. Dreptul penal este unul dintre domeniile politicii statale extrem de important în lupta anticriminalitate, motiv pentru care, constituie la nivelul U.E o preocupare reală. Se apreciază, pe bună dreptate credem, că un drept penal la nivelul U.E poate garanta faptul că infractorii nu se pot sustrage de la răspundere folosindu-se de deosebirile ce există între sistemele juridice ale diferitelor state, ori adăpostindu-se între anumite granițe de stat. Când vorbim de un drept penal la nivelul U.E, nu avem în vedere un cod penal european unic. Acesta este, deocamdată cel puțin, imposibil tocmai datorită diferențelor sistemelor de drept naționale. Însă, se are în vedere o armonizare și o potrivire a normelor de drept penal ale statelor membre, o apropiere a lor, care să permită o cooperare a acestora în combaterea criminalității transfrontaliere. În acest sens Tratatul privind funcționarea Uniunii Europene a prevăzut în art.83 că Parlamentul European și Consiliul, în domeniul penal, pot decide norme referitoare la definirea unor infracțiuni și la sancțiunile de aplicat în zone de gravitate mare a criminalității transfrontaliere, gravitate dovedită prin urmările acestor fapte. Considerentul pentru aceasta este, credem, că pornind de la o bază comună, el pot fi prevenite și sancționate.

¹² M.Of. nr. 721/28.10.2010

¹³ M.Of. nr.296/23.05.2013

¹⁴ Vasile Păvăleanu, Drept penal european, ed. Lumen Iași, 2018, p.202

Se consideră, pe bună dreptate, că armonizarea legislativă în materie penală este o condiție existențială pentru formarea și păstrarea unui spațiu de libertate, siguranță și justiție, adică tocmai a acelui spațiu la care se aspiră a fi conceput prin intermediul normelor U.E.

În îndeplinirea acestor deziderate menționate, acțiunile derulate la nivelul Consiliului Europei și al U.E în sfera luptei contra criminalității informatice au constat în adoptarea unor documente prin care s-a impus puterilor legislative ale statelor membre să legifereze prevederi legale armonizate între ele sau uniforme.¹⁵

În prezent putem constata că, în materie penală, la nivelul statelor membre UE, s-a reușit darea unor definiții unitare anumitor termeni în zone ale infraționalității precum: corupție, trafic ilicit de droguri, de persoane, de arme, exploatare sexuală a femeilor și copiilor, criminalitate organizată, criminalitate informatică.

În baza dispozițiilor tratatelor unionale, Consiliul poate da decizii spre a fi descoperite și alte zone de infraționalitate care o necesită, în funcție de evoluția fenomenului criminalității. Astfel se dorește înlăturarea acelor inconveniente determinate de lipsa sancțiunilor și de lipsa unor definiții unitare a infracțiunilor.

În ceea ce privește criminalitatea informatică, în prezent, la nivel mondial, nu există o definiție unitară a acesteia, însă, pentru acest domeniu, încă din anii 2000 s-au conturat preocupări la nivelul Consiliului Europei și a U.E, având loc mai multe Convenții și fiind adoptate o serie de norme în materie, pe care le-am menționat în studiul de față. Pentru statele membre UE, în domeniu, libertatea lor de alegere este foarte limitată, având în vedere că normele unionale, cât și Convenția Consiliului Europei menționată, sunt elaborate foarte detaliat, prevăzând inclusiv sancțiunile și quantumul minim al lor. Dăm spre exemplificare prevederile art.9 alin.(1) în referire la art.3-8, art.9 alin.(2) în referire la art.3-7, art.9 alin.(3) și (4) în referire la art.4 și art.5, toate din Directiva 2013/40/UE a Parlamentului European și Consiliului, care se referă la quantumul minim al maximului pedepselor pentru infracțiunile de criminalitate informatică precum: accesare ilegală a sistemelor informatice, afectarea ilegală a integrității sistemului, afectarea ilegală a integrității datelor, interceptarea ilegală, și ele au ca destinatari, conform art.19 al aceleiași Directive, statele membre ale Uniunii Europene.

În România, Codul penal actual răspunde condițiilor cerute de documentele internaționale europene. Trebuie însă, credem, să existe în mod permanent preocuparea statului român pentru a modifica actuala legislație raportându-se la modalitățile de comitere a acestor infracțiuni, care sunt în permanentă schimbare și modernizare.

BIBLIOGRAPHY

1. Ghe.Ionuț Iulian, *Infracțiunile din sfera criminalității informatice, incriminare, investigare, prevenire și combatere*, Ed. Universul Juridic, București 2011
2. Ligia-Valentina Mirișan, *Influența dreptului Uniunii Europene asupra dreptului penal român*, Ed. Universul Juridic, București 2017
3. Vasile Păvăleanu, *Drept penal european*, ed. Lumen Iași, 2018
4. I.Vasiu, L.Vasiu, *Criminalitatea în cyberspațiu*, Ed. Universul Juridic, București 2011

Alte surse:

5. www.criminalitate-informatică.ro
6. Directiva 2013/40/UE, par.1, <http://eurlex.europa.eu/legal-content/RO/>

¹⁵ Idem, p.196

7. Codul penal al României