George Zlati

Tratat de criminalitate informatică

Vol. I

solomon
2020

Cuprins

Titlul I
Conceptul de „criminalitate informatică" și aspecte terminologice

Capitolul I
Criminalitatea informatică

Secțiunea 1. Conceptul de „criminalitate informatică"

Menționăm *ab initio* că nu ne propunem o analiză *in extenso* cu privire la ce este criminalitatea informatică[9], ce nu este și cum este înțeles acest concept în doctrină, jurisprudență ori diferitele instrumente juridice la nivel internațional sau european. Despre acest concept se pot scrie, s-au scris și se vor scrie monografii întregi, în care analiza *in extenso* să surprindă toate particularitățile, dezbaterile doctrinare și consecințele juridice ce derivă din modalitatea în care acest concept este definit.

Ceea ce ne propunem este doar a evidenția câteva chestiuni punctuale, care să scoată în evidență ceea ce apreciem noi ca fiind esențial de reținut cu privire la conceptul de „criminalitate informatică". Ar putea părea că acest concept este cu vechime, dar, în realitate, până în anul 1970, în SUA nu se discuta cu adevărat despre criminalitatea informatică, infracțiuni prin intermediul calculatorului ori altele asemenea[10].

Începând cu această perioadă, conceptul de „criminalitate informatică" – indiferent de terminologia folosită – a început să câștige tot mai mult teren, iar progresele tehnologice și îndeosebi apariția Internetului nu au făcut decât ca interesul pentru criminalitatea informatică și importanța acesteia să crească exponențial. Totuși, 50 de ani în domeniul juridic nu reprezintă o perioadă de timp semnificativă. Nu este o perioadă scurtă de timp, dar, având în vedere că despre răspunderea penală a persoanei juridice se discută în *common law* de sute de ani[11] și, cu toate acestea, discuțiile în plan juridic nu sunt încă definitiv tranșate,

---

[9] Și ne vom rezuma la a folosi această noțiune, deși în literatura de specialitate întâlnim o terminologie cât se poate de variată precum: *e-crime*, *high-tech crime*, *IT crime*, *ICT crime*, *computer crime* etc. Vom evita traducerea acestor termeni în limba română, pentru a nu ajunge la descoperirea de noi noțiuni. În legătură cu diversitatea acestor termeni, apreciați ca fiind interschimbabili, se poate vedea J. Clough, Principles of Cybercrime, ed. a II-a, Cambridge University Press, UK, 2015, pp. 9-10; I. Vasiu, L. Vasiu, Criminalitatea în Cyberspațiu, op. cit., p. 119, n.s. nr. 5. Așa cum bine s-a evidențiat, oricare dintre acești termeni ar fi analizați gramatical, s-ar ajunge la concluzia că sunt deficitari, deoarece aduc limitări ce ar părea nejustificate – în acest sens, J. Clough, Principles of Cybercrime, op. cit., p. 10. Astfel, noțiunea de „computer" – cel puțin în sens tradițional – exclude alte dispozitive ce ar intra însă în accepțiunea noțiunii de „sistem informatic".

[10] A se vedea, în acest sens, un istoric al criminalității informatice, pe faze „de dezvoltare", în J.B. Hill, N.E. Marion, Introduction to Cybercrime. Computer Crimes, Laws, and Policing in the 21st Century [Kindle], Ed. Praeger, SUA, 2016, la Capitolul II – History of Cybercrime, *passim*.

[11] A se vedea, în acest sens, H.W. Edgerton, Corporate criminal responsability, în Yale Law Journal, nr. 5/1927, p. 827. Autorul citează cauze din *common law* din anul 1864 [*Statul c. Ohio R.R.*], 1841 [*Statul c. Great Works Co.*] etc. A se vedea, de asemenea, o analiză doctrinară din 1899, în C.J. Lindley, Criminal acts of corporations and their punishment, în American Lawyer, nr. 7/1899, p. 564 și urm.

credem că studiul criminalității informatice se află, momentan, doar într-o etapă adolescentină. Acest lucru înseamnă că mai avem multe de învățat, iar dezbaterile juridice ar trebui să fie considerate ca fiind într-o fază incipientă.

Cert este faptul că, deși acest concept a intrat deja în limbajul curent, este folosit extrem de des, a devenit deja un subiect de o importanță deosebită, acesta rămâne **un concept deosebit de vag**[12] **și dificil de definit**[13]. La întrebarea „Ce este criminalitatea informatică?" răspunsul nu poate fi decât unul complicat și plin de nuanțe.

Tocmai de aceea încă nu există o definiție legală[14]. În loc să se accepte faptul că acesta reprezintă un „concept-umbrelă" ce își schimbă sensul și conținutul în funcție de perspectivă, teoreticienii și decidenții politici încearcă în continuare să îl umple de conținut. În acest sens, au fost elaborate și vor fi elaborate în continuare definiții, clasificări și analize în legătură cu acest concept, însă, din punctul de nostru de vedere, este imposibil a se ajunge în viitorul apropiat la un consens. Explicația o regăsim în gama deosebit de variată de conduite infracționale, unele dintre acestea aflate, din perspectiva clasificării, la limita dintre infracțiunile tradiționale și cele informatice. Ne-am putea referi aici la infracțiunea de hărțuire prin mijloace de transmitere la distanță (art. 208 C.pen.) sau violarea vieții private (art. 226 C.pen.), prin raportare la o eventuală supraveghere tehnică. Sunt acestea niște infracțiuni tradiționale ce pot fi comise inclusiv prin mijloace tehnice sau intră în accepțiunea conceptului de „criminalitate informatică"? Un răspuns tranșant la o asemenea întrebare l-am aprecia ca fiind unul hazardat, existând argumente pentru a susține oricare dintre aceste teze.

O primă problemă ar putea fi chiar aceea dacă ar trebui să ne referim la „criminalitate informatică" sau la „criminalitatea în cyberspațiu". Aceasta deoarece, dacă termenul de criminalitate informatică pare a fi mai apropiat de ceea ce înțelegem prin „computer crime", criminalitatea în cyberspațiu ar fi mai apropiată de noțiunea de „cybercrime". Unii autori susțin că există o trecere de la categoria conceptuală a criminalității informatice [în engleză, *computer crime* / în italiană *reati informatici*] la criminalitatea în cyberspațiu [în engleză, *cybercrime* / în italiană, *reati cibernetici*][15].

Preferăm să nu polemizăm pe marginea acestui subiect, folosind în continuare noțiunea de „criminalitate informatică", care este oricum la fel de vagă precum noțiunea de „criminalitate în cyberspațiu". În opinia noastră, aceste noțiuni sunt interschimbabile. Apreciem, de asemenea, că infracțiunile care intră în accepțiunea acestor noțiuni ridică ele însele atât de

---

[12] În acest sens, S. Gordon, R. Ford, On the definition and classification of cybercrime, în Journal of Computer Virology, nr. 2/2006, p. 13; A. Završnik, Cybercrime definitional challenges and criminological particularities, în Masaryk University Journal of Law and Technology, nr. 2/2008, p. 2; V. Cioclei, A.-R. Ilie, Impactul dreptului penal european asupra noului Cod penal român. Privire asupra traficului de persoane și a criminalității informatice, în AUB (seria Drept), partea III-IV, 2012, p. 337.

[13] Recomandarea R (89) 9 privind criminalitatea informatică, p. 13; P. Kleve, R. De Mulder, K. van Noortwijk, The definition of ICT Crime, în Computer Law & Security Review, vol. 27, 2011, p. 162; M.D. Goodman, Why the Police don't care about computer crime, în Harvard Journal of Law & Technology, vol. 10, nr. 3, 1997, p. 468; E. Stancu, A.C. Moise, Considerații privind fenomenul de criminalitate informatică, în AUB (seria Drept), nr. 1/2010, p. 42; I. Slabu, Considerații generale cu privire la criminalitatea informatică, în Studii de Securitate Publică, vol. II, nr. 4(8)/2013, p. 105.

[14] I. Walden, Harmonizing Computer Crime Laws in Europe, în European Journal of Crime, Criminal Law and Criminal Justice, vol. 12, nr. 4/2004, p. 321.

[15] A se vedea, în acest sens, L. Picotti, Diritto penale e tecnologie informatiche: Una visione d'insiem, în A. Cadoppi, S. Canestrari, A. Manna, M. Papa (dir.), Cybercrime [Kindle], Ed. UTET Giuridica, Milano, 2019, la secțiunea a 3-a, *passim*.

multe probleme, încât aceste dezbateri juridice la nivel terminologic nu sunt decât o „perdea de fum", fără relevanță practică deosebită. Sau cel puțin așa ar trebui să fie, chiar dacă, uneori, legiuitorul național ori cel european ne demonstrează că în legislație se poate face trimitere și la astfel de noțiuni cu un conținut imprecis.

Revenind, apariția conceptului de „criminalitate informatică" – sau cum își dorește cititorul să îl numească – ține și de tendința de a grupa infracțiunile în funcție de specificul acestora. Așa este cazul, de exemplu, cu infracțiunile de criminalitate organizată (unde pot intra inclusiv cele privind criminalitatea informatică[16]), infracțiunile economice (unde nu vedem de ce nu s-ar încadra și anumite infracțiuni informatice precum frauda informatică)[17] etc. Observăm, de asemenea, că această încercare de a grupa anumite infracțiuni generează însă riscuri în plan juridic, deoarece nu tot timpul sintagmele folosite sunt cele mai fericite.

În acest sens, un exemplu potrivit ar fi sintagma „infracțiuni economice prevăzute în legi speciale", care a fost apreciată ca fiind neconstituțională – a se vedea, în acest sens, **Decizia CCR nr. 573/2011**[18], în legătură cu neconstituționalitatea art. 74[1] C.pen. anterior[19]. Nu putem decât să precizăm că atât frauda informatică, cât și efectuarea de operațiuni financiare în mod fraudulos erau prevăzute, anterior intrării în vigoare a noului Cod penal, în legislația specială – frauda informatică, în Legea nr. 161/2003, iar efectuarea de operațiuni, în Legea nr. 365/2002. Din punctul nostru de vedere, nu există niciun argument pentru a susține că aceste două infracțiuni nu intrau în categoria infracțiunilor economice[20] prevăzute în legi speciale la care făcea trimitere art. 74[1] C.pen. anterior. Prin urmare, raportat la aplicarea în timp a legii penale [aplicarea legii penale mai favorabile], art. 74[1] C.pen. anterior ar trebui să își găsească aplicabilitate în ceea ce privește infracțiunea de fraudă informatică și efectuarea de operațiuni financiare în mod fraudulos. Ambele infracțiuni sunt contra patrimoniului, infracțiunea de efectuare de operațiuni financiare în mod fraudulos privind chiar sistemul bancar, ce reprezintă un argument suplimentar în susținerea concluziei învederate anterior.

Practică judiciară. Înalta Curte de Casație și Justiție[21]: „(...) infracțiunile reținute în sarcina inculpaților, respectiv art. 48 din Legea nr. 161/2003 [*falsul informatic* – n.n.], ce constă în introducerea, modificarea și ștergerea fără drept de date informatice care au fost utilizate în scopul producerii de consecințe juridice, și art. 49 din Legea nr. 161/2003

[16] A se vedea, în acest sens, și L.C. Kövesi, S. Finta, Încadrarea juridică a unor fapte de fraudă informatică, în Dreptul, nr. 12/2006, p. 187.

[17] Există autori ce plasează falsul informatic în sfera criminalității economice, fapt ce ne pune pe gânduri referitor la înțelegerea corespunzătoare a acestei infracțiuni și raportul acesteia cu infracțiunea de fraudă informatică – a se vedea E. Stancu, A.C. Moise, op. cit., p. 48.

[18] Publicată în M. Of. nr. 363 din 25 mai 2011. Extras din Decizia CCR nr. 573/2011: „din redactarea aceluiași alineat nu se desprinde cu suficientă claritate și precizie care pot fi acele «unor infracțiuni economice prevăzute în legi speciale» [s.n.], putându-se ajunge la o înțelegere deficitară a conceptului de «infracțiuni economice» (cum ar fi, de pildă, infracțiunile împotriva intereselor financiare ale Comunităților Europene ori infracțiunile în legătură directă cu infracțiunile de corupție prevăzute în Legea nr. 78/2000 pentru prevenirea, descoperirea și sancționarea faptelor de corupție). Prin urmare, textul de lege criticat este deficitar din perspectiva lipsei de corelare atât cu alte prevederi similare din Codul penal, cât și cu cele reglementate în legi speciale la care se face trimitere, ceea ce este de natură să genereze confuzii, incertitudine și dificultăți în ceea ce privește interpretarea și aplicarea acestuia".

[19] Normă legală ce permitea reducerea limitelor de pedeapsă, aplicarea unei amenzi penale ori a unei sancțiuni administrative în funcție de cuantumul prejudiciului cauzat și recuperat.

[20] Detalii despre semnificația infracțiunilor economice se pot vedea în M.K. Guiu, Criteriul infracțiunilor economice, în Dreptul, nr. 12/2008, p. 173 și urm.

[21] ICCJ, s. pen., dec. nr. 749/2013.

[*frauda informatică* – n.n.], constând în introducerea, modificarea sau ștergerea de date informatice, restricționarea accesului la aceste date ori împiedicarea în orice mod a funcționării unui sistem informatic în scopul de a obține un beneficiu material, nu au caracterul unor infracțiuni economice de natură să atragă incidența dispozițiilor art. 74[1] C.pen. [*anterior* – n.n.]. Faptul că prin comiterea acestor infracțiuni se urmărește producerea unui prejudiciu în dauna părților vătămate le clasifică ca fiind infracțiuni de rezultat, însă *în niciun caz nu pot fi clasificate ca infracțiuni economice* [s.n.]". Credem că această soluție este în parte discutabilă, fiind de asemenea regretabilă omisiunea instanței de a explica motivele pentru care a ajuns la această concluzie. Simpla precizare că nu este suficient să se urmărească producerea unui prejudiciu nu reprezintă un argument pentru lipsirea de efecte a art. 74[1] C.pen. anterior. Dacă în ceea ce privește infracțiunea de fals informatic achiesăm opiniei instanței, credem că există argumente solide pentru respingerea tezei potrivit căreia frauda informatică este o infracțiune economică. De altfel, paralela făcută, de multe ori, între frauda informatică și înșelăciunea tradițională reprezintă un argument pentru aplicabilitatea art. 74[1] C.pen. anterior.

Revenind, dacă în ceea ce privește infracțiunea de acces ilegal la un sistem informatic [art. 360 C.pen.] nu ar exista dificultăți în a susține că face parte din conceptul de „criminalitate informatică", fiind chiar o infracțiune definitorie pentru acesta, analiza se complică atunci când discutăm despre frauda informatică, falsul informatic, pornografia infantilă, hărțuirea prin mijloace de transmitere la distanță, racolarea de minori prin mijloace de transmitere la distanță etc.

Prin urmare, înainte de a explora puțin acest concept al „criminalității informatice", credem că s-ar impune o concluzie tranșantă, și anume aceea că **trimiterea la criminalitatea informatică este deosebit de periculoasă atunci când ne propunem să atingem standardul impus de principiul legalității**[22]. Cu toate că am mai folosit – și vom folosi în continuare – trimiteri la acest concept, pentru a ne raporta în mod generic la anumite infracțiuni informatice, credem că, din perspectiva tehnicii legislative, este de evitat să se folosească această terminologie. Din punctul nostru de vedere, este de evitat a se folosi inclusiv trimiterea la „infracțiuni informatice" [sintagmă ce putea fi identificată în Legea nr. 21/1999][23] ori la „infracțiuni care se săvârșesc prin sisteme informatice sau mijloace de comunicare electronică" [sintagmă regăsită în cuprinsul art. 139 alin. (2) C.proc.pen.].

Găsim, așadar, ca fiind problematică prevederea din art. 139 alin. (2) C.proc.pen. în materia supravegherii tehnice, ce face trimitere la sintagma **„infracțiuni care se săvârșesc prin sisteme informatice sau mijloace de comunicare electronică"**. Aceasta este preluată prin intermediul unei norme de trimitere inclusiv în conținutul art. 152 alin. (1) lit. a) C.proc.pen. [Obținerea datelor de trafic și de localizare]. Sintagma devine **problematică din perspectiva respectării principiului legalității** prevăzut de art. 1 alin. (5) din Constituție, ridicând, implicit, serioase semne de întrebare din perspectiva constituționalității. Nimeni nu

[22] Pentru exemple de instrumente juridice supranaționale în care este folosită noțiunea de „criminalitate informatică", se poate vedea și R. Flor, Lotta alla „criminlità" e tutela di „tradizionali" e „nuovi" diritti fondamentali nell'era di Internet, în Diritto Penale Contemporaneo, 2012, pp. 3-4.

[23] A se vedea, în acest sens, art. 23 alin. (1) lit. a) din Legea nr. 21/1999 pentru prevenirea și sancționarea spălării banilor (publicată în M. Of. nr. 18 din 21 ianuarie 1999 și abrogată prin art. 31 din Legea nr. 656/2002), ce făcea trimitere la „infracțiunile săvârșite prin intermediul calculatoarelor". În contextul în care infracțiunile despre care vorbim în prezent ca fiind „informatice" au apărut pentru prima dată în legislația națională prin intermediul Legii nr. 161/2003 și al Legii nr. 365/2002, nu putem decât să ne întrebăm ce infracțiuni a avut în vedere legiuitorul și unde a fost controlul de constituționalitate.

ne va putea convinge că infracțiunile ce ar trebui să fie înglobate în această sintagmă sunt determinabile. Cu toate acestea, găsim drept fascinant faptul că, până în prezent, nu s-a ridicat în mod serios o problemă de constituționalitate cu privire la sintagma „infracțiuni care se săvârșesc prin sisteme informatice sau mijloace comunicare electronică", în ciuda faptului că aceasta stă la baza unei ingerințe majore în dreptul la viață privată garantat de art. 26 din Constituție. Mai mult, am putea să anticipăm inclusiv concluzia Curții Constituționale pe acest subiect, în sensul că sintagma criticată nu suferă sub aspectul previzibilității. Dacă se va ajunge aici, tot ce ne dorim reprezintă oferirea câtorva criterii obiective în baza cărora se poate concluziona ce infracțiuni intră în accepțiunea sintagmei „infracțiuni care se săvârșesc prin sisteme informatice sau mijloace de comunicare electronică" și să știm de ce în această categorie nu intră orice infracțiune tradițională, de la omor la viol.

În context, nu putem decât să observăm faptul că o asemenea sintagmă pare a se referi la conceptul de „criminalitate informatică" *lato sensu*, în care sistemul informatic nu este obiectul sau subiectul infracțiunii, ci doar o „unealtă" (un mijloc) ce poate fi folosită pentru a comite infracțiuni tradiționale. Or, doar imaginația ne oprește în a oferi exemple în care orice infracțiune prevăzută în Codul penal poate fi comisă – în cel puțin una dintre formele participației penale – prin intermediul unor sisteme informatice sau prin mijloace de comunicare electronică. Vedem, în acest sens, posibilitatea de a sustrage un autovehicul modern printr-un control exercitat asupra acestuia de la distanță [*remote access*] sau posibilitatea de a ucide o persoană prin dezactivarea de la distanță a unui dispozitiv tip *pacemaker*. În aceste condiții, enumerarea infracțiunilor prevăzute la art. 139 alin. (2) C.pen. nu ar mai fi una limitativă, supravegherea tehnică fiind susceptibilă de a produce o ingerință în dreptul la viață privată indiferent de infracțiunea la care ne raportăm.

Din perspectiva constituționalității acestei sintagme, un punct de plecare ar putea fi chiar **Decizia CCR nr. 553/2015**[24], referitoare neconstituționalitatea sintagmei „trafic de stupefiante" din cuprinsul dispozițiilor art. 223 alin. (2) C.proc.pen. Dispoziția legală ar putea ridica probleme inclusiv din perspectiva ingerinței în dreptul la viață privată [art. 8 din Conv. EDO], fiind discutabil în ce măsură sunt îndeplinite condițiile ce țin de calitatea legii, din perspectiva jurisprudenței CEDO – criteriul clarității și previzibilității normei legale[25]. Aceasta dincolo de faptul că lipsa de claritate poate genera o interpretare abuzivă, cu repercusiuni în ceea ce privește respectarea principiului proporționalității în contextul unei ingerințe în dreptul la viață privată generate de supravegherea tehnică – art. 8 par. 2 din Conv. EDO.

Un alt exemplu relevant se regăsește în cuprinsul art. 280 alin. (1) pct. 11 din Legea nr. 302/2004 privind cooperarea judiciară internațională în materie penală, republicată[26]. Astfel, într-un articol important referitor la lista infracțiunilor pentru care nu este necesară condiția

[24] Publicată în M. Of. nr. 707 din 21 septembrie 2015.

[25] Sub acest aspect, am subliniat cu o altă ocazie [a se vedea, în acest sens, G. Zlati, Comentariu, în M. Udroiu (coord.), Codul de procedură penală. Comentariu pe articole, ed. a II-a, Ed. C.H. Beck, București, 2017, p. 749, par. 72], faptul că, deși în Capitolul VI al titlului VII din Codul penal, se regăsesc infracțiunile contra siguranței sau integrității sistemelor și datelor informatice, infracțiunile care se săvârșesc prin intermediul unui sistem informatic sau prin mijloace de comunicare electronică sunt extrem de diverse. Astfel, amenințarea [art. 206 C.pen.], hărțuirea [art. 208 alin. (2) C.pen.], racolarea de minori [art. 222 C.pen.], violarea vieții private [art. 226 C.pen.], violarea secretului corespondenței [art. 302 alin. (2) C.pen.] etc. sunt infracțiuni ce pot fi comise prin sisteme informatice sau mijloace de comunicare electronice. Aceasta fără a pune în discuție posibilitatea de a comite un act de violență [art. 193 C.pen.] ori o lipsire de libertate [art. 205 C.pen.] prin intermediul unui sistem informatic (sic!).

[26] Republicată în M. Of. nr. 411 din 27 mai 2019.

dublei incriminări, se face trimitere la sintagma **„faptelor legate de criminalitatea informatică"**, trimitere care nu ar trebui să surprindă pe nimeni, având în vedere că sintagma este preluată din cuprinsul art. 2 din Decizia-cadru 2002/584/JAI privind mandatul european de arestare și procedurile de predare între statele membre – cu mențiunea că în instrumentul juridic european se face trimitere doar la criminalitatea informatică, nu și la faptele legate de aceasta[27].

Credem că reglementarea europeană este totuși superioară, deoarece sintagma „faptelor legate de", din dreptul național, poate genera mult mai multe discuții decât o trimitere generică la „criminalitatea informatică". Probabil cea mai radicală interpretare ar fi cea potrivit căreia faptele legate de criminalitatea informatică sunt altele decât cele ce intră în cuprinsul noțiunii de „criminalitate informatică". Altfel, dacă faptele la care face trimitere legiuitorul sunt chiar infracțiuni informatice, nu înțelegem de ce acestea ar fi legate de criminalitatea informatică, adică un ansamblu de infracțiuni informatice.

Cu toate acestea, rațiunea din spatele acestei formulări, mai ales dacă ne raportăm la instrumentul juridic european transpus în dreptul intern, pare destul de clară. Identificarea acestei rațiuni ține însă de elemente extrinseci actului normativ, deoarece, în acest caz, pare să existe un conflict între ceea ce și-a dorit legiuitorul național și ceea ce a rezultat din transpunerea deciziei-cadru.

Ar mai trebui poate precizat că inclusiv **Tratatul privind funcționarea Uniunii Europene** [TFUE] face trimitere la conceptul de „criminalitate informatică", în cuprinsul art. 83 alin. (1), referitor la competența Parlamentului European și a Consiliului de a legifera, prin intermediul directivelor, cu privire la definirea infracțiunilor și sancțiunilor în domenii considerate de o gravitate deosebită și având o dimensiune transfrontalieră. Această trimitere este una deosebit de periculoasă, deoarece poate conduce la o extindere nerezonabilă a competenței Parlamentului European și a Consiliului de a legifera în domeniul dreptului penal. Lipsa unei definiții legale a criminalității informatice poate reprezenta, așadar, un „cec în alb", fiind doar o chestiune de timp până ce vom putea discuta despre primul act de legiferare discutabil într-un domeniu apreciat ca făcând parte din conceptul „criminalității informatice".

De asemenea, **Directiva 2018/1673/UE privind combaterea prin măsuri de drept penal a spălării banilor**[28] include în gama de activități infracționale relevante și **„criminalitatea informatică** [s.n.], inclusiv orice infracțiune prevăzută în Directiva 2013/40/UE a Parlamentului European și a Consiliului" [art. 2 par. 1 lit. (v) din Directivă]. Din această formulare, pare să reiasă destul de clar faptul că legiuitorul european interpretează extensiv acest concept, fără a-l limita doar la infracțiunile ce fac obiectul art. 360-365 C.pen. Ceea ce rămâne neclar este până unde se întinde acesta din perspectiva conduitelor infracționale pe care le mai poate îngloba. Având în vedere lejeritatea cu care legiuitorul european tinde să se raporteze la acest concept în instrumentele juridice, așteptăm cu interes prima intervenție a Curții de Justiție a Uniunii Europene cu privire la respectarea principiului legalității.

Observăm, de asemenea, ezitarea legiuitorului european de a se raporta doar la „criminalitatea informatică", acesta simțind nevoia de a clarifica în mod expres că în acest concept ar intra *inclusiv* infracțiunile informatice prevăzute în Directiva 2013/40/UE. Dacă acest concept era unul clar din perspectiva conținutului, trimiterea la infracțiunile prevăzute în directivă nu ar fi fost necesară.

---

[27] Această trimitere din lista infracțiunilor excluse de la condiția dublei incriminări a fost apreciată, inclusiv în literatura de specialitate, ca fiind vagă – a se vedea, în acest sens, M. Fletcher, R. Lööf, B. Gilmore, EU Criminal Law and Justice, Elgar European Law Publisher, 2008, p. 115.

[28] Publicat în JOUE L 284 din 12 noiembrie 2018.