THE IMPACT OF DIGITISATION ON CRIMINAL LAW

Vicențiu-Traian RÂMNICEANU[1]

Abstract:
Digitization has become an integral element of our technical-scientific and industrial-economic civilization in recent years. By serving the ultra-fast and mass logical processing of information, digitization finds countless applications in all fields, from mathematics to sociology and history.
Keywords: *the impact; digitization; criminal law; cybernetic.*

În domeniul dreptului cercetătorii din lumea întreagă sunt preocupați cu eleborarea unor metode cibernetice de rezolvare a problemelor complexe din toate ramurile științelor juridice: drept penal[2], dreptul muncii, statistica judiciară, etc.

Precizăm, însă, că progresul metodelor cibernetice in drept implică, între altele crearea unui limbaj special al informațiilor și un dicționar de simboluri cu care să se poată stabili raporturile dintre diversele noțiuni juridice[3]. Societatea umană funcționează în baza generării, a stocării și a schimbului de informații. Forma scrisă a informației a contribuit în mod esențial la perpetuarea acesteia de-a lungul generațiilor, la consolidarea, completarea și sintetizarea sa. Patrimoniul umanității s-a construit prin intermediul și în jurul formelor de manifestare și stocare a informației sub toate formele sale culturale de scrieri, arta plastică, dramatică, muzicală, prin numeroasele ansambluri arhitectonice, amenajări peisagistice și toate celelalte forme ale creației și intervenției umane asupra sau în strânsă legătură cu mediul înconjurător"[4].

Mediile timpurii de stocare a informației și-au relevat însă caracterul efemer, fiind constant sub pericolul distrugerii intenționate sau accidentale, iar până la descoperirile științifice ale secolelor XIX și XX, hârtia a rămas mediul predilect de păstrare a informațiilor.

Necesitatea schimbului de informații între centrele de cercetare academică precum și crearea de soluții de comunicare în cazul unui atac nuclear au condus la formarea ARPANET, o rețea experimentală de calculatoare, funcționând fără nod central sau bază de operațiuni, pornind de la care s-a dezvoltat internetul, ca legătură între rețelele de mașini de calcul, începând cu anul 1983. De la acel moment, omenirea a asistat la o explozie a tehnicilor informaționale[5], sistemele informatice schimbând definitiv modul de viață al societății în ansamblul său, prin intervenția mașinilor de calcul, devenite calculatoare, în toate domeniile publice și privat, în baza unui fenomen pe cât de atrăgător pe atât de complex ca efecte, și anume automatizarea procesării și stocării datelor.

Meritul calculatoarelor este de a crea spațiu pentru stocarea și gestionarea informațiilor referitoare la componente ale realității înconjurătoare cărora distanțele, volumele sau caracteristicile specifice nu le îngăduiau o alăturare. Clasificarea informației, distingerea asemănărilor și a deosebirilor, secvențierea operațiunilor de procesare a informației sunt valoarea adaugată a unei noi ere industriale in care informația transgresează simpla utilitate de referință în legătură cu subiectul principal, devenind o valoare în sine, tranzacționabilă sau

[1] Drd., Universitatea de Studii Politice și Economice Europene "Constantin Stere", Republica Moldova
[2] Ion Ifrim, *Unele reflecţii asupra sistematizării infracţiunilor informatice*, Revue européennee du droit social, 2016. revue europeenne-du-droitsocial.ro/fr/revue.php,indexata;Revue europennee du droit social Drept-2016.pdf, pp.142-148.
[3] C.A. Diaconu, *Teoria Informației și probele judiciare*, Revista Română de Drept, nr. 2/1972, p. 54.
[4] Szczepanski, J., "*Noțiuni elementare de sociologie*„, Editura Științifică, București, 1972.
[5] Amza Tudor, Amza Cosmin-Petronel, "*Criminalitatea informatică*", Ed. Lumina Lex 2003, pg.9.

parte a unui șir de operațiuni care produc o valoare tranzacționabilă. Noua realitate virtuală, care preia coordonatele temporal-spațiale obișnuite și le transformă într-o dimensiune atemporală și aspațială, reprezintă un univers aparte, cu reguli și procese noi. Simplul fapt al eliminării condiționărilor de timp și spațiu face ca reguli existente în lumea fizică să fie dezagregate până la dispariție în aria virtuală, iar creativitatea să dobândească valențe nocive, atunci când valorile sociale ocrotite prin lege, sunt abuzate sub protecția anonimatului dobândit prin subterfugiile cibernetice.

În intervalul celor câteva decade de dezvoltare a spațiului cibernetic, acesta a fost rapid aglomerat cu date, dezvoltarea tehnică susținând conținutul diversificat, asfel încât provocarea prezentă numai este cea de accesare a informației, operațiune extrem de facilă, susținută de motoarele de căutare, ci organizarea și procesarea metadatelor, respectiv a datelor despre date, care odată prelucrate în concordanță cu cerințele informaționale, poate sta la baza unor decizii[1].

Astfel cum se relevă în literatura dedicată studiului criminalității informatice, ”prin internet, informația a devenit arma cea mai ieftină din lume”[2], punându-se problema unui nou domeniu al luptei, care este informația. Aceasta este definită ca fiind sensul, înțelesul, semnificația unei date sau ale unui program introdus într-un sistem de calcul”.[3]

Dezvoltarea conexiunilor de internet a generat, alături de accesul aproape instantaneu la orice fel de informație, și o probabilitate de malversație a acesteia, internetul reprezentând în fapt un alter ego al societății în ansamblul său, prin urmare dezvoltând propriile forme de infracționalitate. Astfel, informațiile încărcate în pagini de internet, bazele care sunt sursa acestoa, putând fi accesate virtual din orice locație dotată cu un calculator, sunt supuse riscului accesului și copierii nepermise, alterării, ștergerii, suprimării sau infectării acestora.

Cunoscând amploarea internațională a faptelor incriminate ca infracțiuni ce fac parte din domeniul criminalității informatice, se pot decela valorile sociale protejate prin raportarea la modul de reglementare la nivel internațional, regional și național.

În legătură cu studiile privind *infracţiunile prin calculatoare,,* in doctrina penală[4], se arata că, subliniază necesitatea luării unor măsuri pe planul legii penale şi procesual penale împotriva faptelor ilicite care pot fi comise prin intermediul calculatoarelor cum ar fi infracţiunea de fraudă informatică, de fals în informatica, de prejudiciere a datelor sau a programelor informatice, de sabotaj informatic, de acces neautorizat la un calculator, de interceptare neautorizată, de reproducere neautorizată a unei topografii, alterarea fără drept a datelor sau a programelor informatice, spionajul informatic, utilizarea neautorizate a unui calculator, utilizarea neautorizată a unui program informatic protejat de lege. De altfel, în anul 2021, statele membre ale Organizației Națiunilor Unite au început negocierea unui tratat internațional privind combaterea criminalității informatice. Până la adoptarea și ratificarea acestuia, în prezent nu există o definiție agreată la nivel internațional. Criminalitatea informatică înglobează infracțiunile comise prin intermediul tehnologiilor de informatică și de comunicații. Acestea se împart la rândul lor în infracțiuni informatice având ca obiect calculatorul, programele și informațiile stocate pe acesta și infracțiuni înfăptuite prin intermediul calculatorului. Preocuparea privind combaterea criminalității cibernetice și întărirea protecției drepturilor omului în societatea informațională a fost de altfel inclusă în declarația politică a Comitetului de Miniștri ai Consiliului Europei sub forma Planului de acțiune[5]. În capitolul II – ”Consolidarea securității cetățenilor europeni,,, Comitetul de Miniștri propune elaborarea viitoarelor principii și orientări pentru a asigura respectarea drepturilor omului și a statului de drept în societatea informațională. În același timp, Planul de

[1] Mârșanu R., ”*Sisteme de calcul*”, Ed. Didactică și Pedagogică, București, 1995, pg.3, citat în Vasiu I., op.cit.
[2] Vasiu, Ioana – ”*Criminalitatea informatică*”, Ed a II a revizuită și adăugită, Ed. Nemira, 2001, pg.7.
[3] Vasiu, I., op.cit. pg. 21.
[4] Ion Ifrim, *Unele reflecţii asupra sistematizării infracţiunilor informatice*, p.143.
[5] Planul de acțiune a fost adoptat de Comitetul Miniștrilor al Consiliului Europei la conferința de la Varșovia, Polonia (16-17 mai 2005).

acțiune condamnă toate formele de utilizare a tehnologiilor informatice și de comunicații în activitatea criminală și îndeamnă statele membre să continue adoptarea Convenției din 2001 și a Protocolului aditional la aceasta. Preambulul Convenției din 2001 face referire la setul de valori pe care societatea trebuie să le protejeze în fața criminalității informatice, apărarea acestora constituindu-se în interesul ocrotit de lege și totodată în obiect juridic al infracțiunii.

Conform Evaluării Europol privind amenințarea pe care o reprezintă criminalitatea organizată online (Internet Organised Crime Threat Assessment – IOCTA)[1], criminalitatea informatică continuă să reprezinte o amenințare tot mai mare la adresa securității cetățenilor și a întreprinderilor din Uniunea Europeană.

Există tratate internaționale și tratate regionale privind criminalitatea cibernetică. Combaterea criminalității informatice este o prioritate pentru Uniunea Europeană, astfel cum se arată în Strategia UE din 2020 privind o uniune a securității și în Strategia UE din 2021 privind criminalitatea organizată[2].

În cadrul instituțiilor Uniunii Europene s-a preconizat faptul că negocierile privind convenția internațională vor face referire la norme comune ale UE pentru a combate criminalitatea informatică. Printre acestea s-ar putea număra Directiva 2011/93/UE privind combaterea exploatării sexuale a copiilor online și a pornografiei infantile[3], care abordează noile evoluții din mediul online, cum ar fi ademenirea (infractorii care pretind că sunt copii pentru a-i atrage pe minori cu scopul de a-i abuza sexual); Directiva 2013/40/UE privind atacurile împotriva sistemelor informatice[4], care vizează să combată atacurile informatice la scară largă, solicitând statelor membre să își consolideze legislațiile naționale în materie de criminalitate informatică și să introducă un nivel ridicat de sancțiuni penale; și Directiva (UE) 2019/713 privind combaterea fraudelor și a contrafacerii în legătură cu mijloacele de plată fără numerar[5] , care armonizează actele infracționale săvârșite de persoane fizice sau juridice în legătură cu mijloacele de plată fără numerar și extinde răspunderea penală la monede virtuale și portofele electronice.

Cadrul juridic actual al UE include instrumente privind asigurarea respectării legii și cooperarea judiciară în materie penală, cum ar fi Directiva 2014/41/UE privind ordinul european de anchetă în materie penală[6], Convenția cu privire la asistența judiciară reciprocă în materie penală între statele membre ale Uniunii Europene[7] , Regulamentul (UE) 2018/1727 privind Eurojust[8], Regulamentul (UE) 2016/794 privind Europol[9], Regulamentul (UE) 2017/1939 de punere în aplicare a unei forme de cooperare consolidată în ceea ce privește instituirea Parchetului European (EPPO)[10], Decizia-cadru 2002/465/JHA a Consiliului privind echipele comune de anchetă[11], Decizia-cadru 2009/948/JHA a Consiliului privind prevenirea și soluționarea conflictelor referitoare la exercitarea competenței în cadrul procedurilor penale[12] . Pe plan extern, Uniunea Europeană a încheiat o serie de acorduri bilaterale între Uniune și țări terțe, cum ar fi Acordul privind asistența judiciară reciprocă între Uniunea Europeană și Statele Unite ale Americii și Acordul privind asistența judiciară

[1] Evaluarea din 2021 a Europol privind amenințarea pe care o reprezintă criminalitatea organizată online (IOCTA) www.europol.eu.
[2] COM(2021) 170 final (14.4.2021)
[3] Directiva 2011/93/UE (13.12.2011).
[4] Directiva 2011/93/UE (13.12.2011).
[5] Directiva (UE) 2019/713 (17.4.2019).
[6] Directiva 2014/41/UE (3.4.2014).
[7] Convenția cu privire la asistența judiciară reciprocă în materie penală între statele membre ale Uniunii Europene (29.5.2020).
[8] Regulamentul (UE) 2018/1727 (14.11.2018).
[9] Regulamentul (UE) 2016/794 (11.5.2016).
[10] Regulamentul (UE) 2017/1939 al Consiliului (12.10.2017).
[11] Decizia-cadru 2002/465/JHA a Consiliului (13.6.2022).
[12] Decizia-cadru 2009/948/JHA a Consiliului (30.11.2009).

reciprocă între Uniunea Europeană și Japonia[1]. Uniunea a adoptat mai multe directive care consolidează drepturile procedurale ale persoanelor suspectate și ale celor trimise în judecată[2].

Dreptul fundamental al persoanelor la respectarea vieții private și de familie[3], a domiciliului și a comunicațiilor[4] este, de asemenea, consacrat la articolul 7 din Carta drepturilor fundamentale. Aceasta include respectarea confidențialității comunicațiilor, precum și protecția echipamentelor terminale ale utilizatorului, ca elemente esențiale. Datele transmise în cadrul comunicațiilor electronice trebuie să fie prelucrate în conformitate cu Directiva 2002/58/CE (Directiva asupra confidențialității și comunicațiilor electronice)[5].

Codul penal al Germaniei incriminează infracţiunile informatice însă nu concentrate într-un titlu distinct, ci ca articole separate care tratează modalităţile electronice de comitere a unor infracţiuni. Astfel, în Capitolul 22 (Frauda şi delapidarea), articolul 263a se referă la frauda informatică și interzice obținerea ilegală a unui avantaj, cauzând un prejudiciu patrimonial prin influențarea rezultatului unei procesări automate de date. Pedepsele includ închisoarea până la 5 ani sau amenda. De asemenea legea penală germane prevede circumstanțe agravante pentru cazurile deosebit de grave cum sunt cele în care: (i) făptuitorul acţionează în mod calificat sau ca membru al unei asocieri care s-a constituit în scopul comiterii infracţiunilor de înşelăciune sau falsificare de documente, (ii) cauzează un prejudiciu material însemnat sau acţionează cu intenţia ca prin repetarea infracţiunii de înşelăciune să pricinuiască un prejudiciu material unui număr mare de persoane, (iii) pricinuieşte unei alte persoane o criză financiară, (iv) face abuz de drepturile pe care le are în calitate de funcţionar public sau de funcţia sa de funcţionar public sau (v) 5. simulează un caz de asigurare, după ce el sau o altă persoană a incendiat, cu acest scop, sau a distrus, în parte sau în totalitate, prin incendiere, un bun de o valoare însemnată sau a provocat scufundarea sau naufragiul unei nave.

Marea Britanie incriminează accesul neautorizat la resursele unui sistem informatic, modificarea neautorizată a acestora și alte activități de hacking prin Computer Misuse Act, în vigoare din 1990. La data de 25 mai 2011 Marea Britanie a ratificat Convenţia Consiliului Europei privind criminalitatea informatică şi deja a întreprins un şir de modificări legislative în acest sens. A fost elaborat Programul naţional privind criminalitatea informatică „Cyber security – A new national programme SN/SC/5832", care are drept obiective de bază crearea unei agenţii naţionale pentru lupta cu criminalitatea informatică (National Cybercrime Unit NCU) în cadrul Agenţiei naţionale de combatere a criminalităţii care va avea patru direcţii de activitate şi anume: Crima organizată, Poliția de frontieră, Investigarea fraudelor şi crime împotriva minorilor precum şi centrul de protecţie on-line (care deja există). Paralel cu armonizarea legislaţiei, Agenţia va fi complet operaţională până în decembrie 2013, iar Agenţia naţională pentru lupta cu criminalitatea informatică se va preocupa de toate cazurile ce vor ţine de criminalitatea şi infracţiunile cibernetice ca o crimă în sine. De-a lungul anilor, Computer Misuse Act a fost modificată pentru a ține pasul cu progresele tehnologice și cu amenințările cibernetice în evoluție. Acesta joacă un rol crucial în descurajarea și urmărirea penală a persoanelor care se angajează în activități ilegale legate de sistemele informatice și de date. În mai 2021, ministrul de interne al Marii Britanii a anunțat o revizuire a Legii privind utilizarea abuzivă a computerelor. Pasul inițial în această revizuire a implicat o

[1] Acord privind asistența judiciară reciprocă între Uniunea Europeană și Statele Unite ale Americii (25.6.2003).Acord între Uniunea Europeană și Japonia privind asistența judiciară reciprocă în materie penală (2009).

[2] Directiva 2010/64/UE (20.10.2010); Directiva 2012/13/UE (22.5.2012); Directiva 2013/48/UE (22.10.2013); Directiva (UE) 2016/1919 (26.10.2016); Directiva (UE) 2016/800 (11.5.2016); Directiva (UE) 2016/343 (9.3.2016).

[3] Ion Ifrim, *Ocrotirea penală a vieţii intime a persoanei*, Ed. Universul Juridic, Bucureşti, 2012, p.108.

[4] Ion Ifrim, *Reflecţii asupra infracţiunii de violare a secretului corespondenţei*. Revista de Drept Penal nr.1/2012, Ed. Monitorul Oficial în colaborare cu Ed. Universul Juridic,Bucureşti, pp.127.

[5] Directiva 2002/58/CE (12.7.2002), modificată prin Directiva 2009/136/CE (25.11.2009).

consultare publică, prin care s-au solicitat contribuții din partea părților interesate și a publicului larg. Scopul a fost identificarea și înțelegerea oricăror activități din sfera de competență a CMA care provoacă prejudicii, care ar putea să nu fie reglementate în mod adecvat de cadrul juridic existent.

Domeniul de aplicare a cuprins o evaluare a faptului dacă agențiile de aplicare a legii dețin puteri suficiente pentru a investiga și contracara atacurile asupra sistemelor informatice și dacă legislația a rămas eficientă având în vedere progresele tehnologice de la înființarea CMA. Propunerile de lege ferenda includ: eliminarea și confiscarea numelui de domeniu și a adresei IP; incriminarea utilizării infracționale a numelor de domeniu și a adreselor IP atunci când infractorii exploatează nume de domenii și adrese IP pentru diverse activități ilicite. Deși eforturile voluntare conduse de organizații precum Action Fraud și Centrul Național de Securitate Cibernetică (NCSC) sunt eficiente, părțile interesate propun competențe formale pentru cazurile în care aranjamentele voluntare sunt insuficiente.

Codul penal elveţian reglementează „Utilizarea frauduloasă a unui calculator” în în articolul 147 unde este incriminate frauda informatică definita ca rezultand din: „acţiunile unei persoane care cu intenţia de a obţine pentru sine sau pentru altă persoană un avantaj material ilicit foloseşte de o manieră incorectă sau incompletă date informatice, influenţând un proces electronic de prelucrare automată sau de transmitere de date, obţinând prin aceasta date contrare cu adevărul sau un transfer de patrimoniu, dacă prin aceasta s-a produs un prejudiciu unei persoane, va suporta o pedeapsă privativă de libertate pe o perioadă de maxim 5 ani sau va suporta o amendă”.

Conform articolului 147 alin. (2) din Codul penal elvețian: „În cazul în care făptuitorul acţionează pentru câştig comercial, el va fi pasibil de o privaţiune de libertate care nu depăşeşte zece ani sau de o amendă care nu va fi mai mică de 90 de unităţi de penalizare pe zi”. Un element de noutate se regăsește în art.147 alin. (3) din Codul penal elvețian, şi anume, în cazul în care frauda informatică se realizează în detrimentul unui membru al familiei persoana va fi trasă la răspundere doar în baza existenţei unei plângeri.

În general, legislaţia elveţiană reglementează, fără o sistematizare specifică, atât infracţiuni de drept comun săvârşite prin intermediul sistemelor informatice, cât şi infracţiuni îndreptate împotriva confidenţialităţii, integrităţii şi securităţii datelor şi sistemelor informatice, acoperindu-se însă prevederile Convenţiei din 2001.

Am încercat în cele expuse să prezentăm importanța teoretică și practică pe care o are digitalizarea asupra dreptului penal. Aprofundarea multiplelor aspect de aplicare a digitalizarii in dreptul penal ridică știința penală la nivelul actual și ne exprimăm speranța că va ține toată atenția cercetătorilor noștri.

Bibliografie

Amza Tudor, Amza Cosmin-Petronel, ”Criminalitatea informatică/ Cybercrime”, Ed. Lumina Lex 2003.

B. Bulai, Note de curs la materia Infracţiuni prevăzute în legi special/ Course notes on the subject of Offenses provided for in special laws, master Ştiinţe penale, anul 2011-2012.

C. R. Romiţan, Protecţia penală a proprietăţii intelectuale/ Criminal protection of intellectual property, Editura C. H. Beck, 2006.

Carta drepturilor fundamentale a Uniunii Europene/ Charter of Fundamental Rights of the European Union.

Council of Europe Convention on Cybercrime of 23.11.2001, act published in the Official Gazette, Part I no. 343 of 20 April 2004.

Convention on mutual legal assistance in criminal matters between the Member States of the European Union (29.5.2020).

Guiu, Mioara-Ketty, ”Pornografia infantilă/ Child pornography”, Revista Dreptul nr.7/2016/ Law Journal no.7/2016

Ion Ifrim, *Ocrotirea penală a vieţii intime a persoanei/ Criminal protection of a person's intimate life*, Ed. Universul Juridic, Bucureşti, 2012

Ion Ifrim, *Unele reflecţii asupra sistematizării infracţiunilor informatice/ Some reflections on the systematization of computer crimes, Revue européennee du droit social/ European Review of Social Law,* 2016, pp.142-148.

https://fedlex.data.admin.ch/filestore/fedlex.data.admin.ch/eli/cc/54/757_781_799/20230123/en/pdf-a/fedlex-data-admin-ch-eli-cc-54-757_781_799-20230123-en-pdf-a-1.pdf

Ion Ifrim, *Reflecţii asupra infracţiunii de violare a secretului corespondenţei/ Reflections on the crime of violating the secrecy of correspondence*. Revista de Drept Penal/ Criminal Law Jounal nr.1/2012, Ed. Monitorul Oficial în colaborare cu Ed. Universul Juridic, Bucureşti, pp. 127.

https://www.europol.eu

https://www.gesetze-im-internet.de/englisch_stgb/

https://www.legis.md/cautare/getResults?doc_id=121991&lang=ro

https://www.legislation.gov.uk

https://www.refworld.org/docid/4c358dd22.html

https://www.undocs.org

https://www.warnathgroup.com/wp-content/uploads/2017/11/Switzerland-Penal-Code-2017.pdf

Law 8/1996 on copyright and related rights.

Law no. 286/2009 on the Criminal Code.

Mârșanu R., ”Sisteme de calcul/ Computing systems”, Ed. Didactică și Pedagogică, București, 1995.

Neamțu, George, ”Enciclopedia asistenței sociale/ Encyclopedia of Social Work”, Ed.Polirom, 2016.

Emergency Ordinance No. 18/2016 amending and supplementing Law No. 286/2009 on the Criminal Code, Law No. 135/2010 on the Criminal Procedure Code, as well as supplementing Art. 31 para. (1) of Law No. 304/2004 on the judicial organization.

United Nations International Covenant on Civil and Political Rights (1966).

Szczepanski, J., ” Basic notions of sociology, Editura Științifică, București, 1972.

Treaty on the Functioning of the European Union (TFEU)

Vasiu, Ioana, Criminalitatea informatică/ Computer Crime, 2nd Ed revised and added, Ed. Nemira, 2001.