DOI: https://www.doi.org/10.31178/AUBD-FJ.2024.2.10

Forum Juridic nr. 2 / 2024

ANALELE UNIVERSITĂȚII DIN BUCUREȘTI - SERIA DREPT

Înțelesul unor termeni și expresii din dreptul penal în cyberspațiu

Asist. univ. dr. Dorel Herinean
Facultatea de Drept, Universitatea din București

Rezumat: Articolul include o analiză a unor concepte specifice dreptului penal atunci când discutăm de conduite infracționale comise în cyberspațiu sau în mediul online, atât a termenilor proprii dreptului penal, definiți potrivit autonomiei conceptuale, cât și termeni preluați din limbajul curent ori alte ramuri de drept. Prima parte cuprinde analiza termenilor și expresiilor definite în Partea generală a Codului penal, iar partea a doua înglobează reflecțiile asupra unora regăsiți în Partea specială. În ambele părți, după cum sugerează și titlul lucrării, ne propunem să subliniem specificul termenilor în ceea ce privește cyberspațiul și mediul online, analizând modalitățile de comitere a unor infracțiuni și specificul conținutului acestora în cadrul stabilit.

Cuvinte-cheie: cyberspațiu, online, sistem informatic, date informatice, criptomonede, NFT, viață privată, cerșetorie, bun mobil.

The definition of Criminal Law terms or phrases in cyberspace

Abstract: The article provides an analysis of criminal law concepts as they apply to cyberspace and the online environment, focusing on terms specific to criminal law—either defined based on the conceptual autonomy or borrowed from common language or other areas of law. The first part examines terms and expressions defined in the general section of the Criminal Code, while the second part incorporates reflections on those found in the special section. In both parts, as the title of the work suggests, the aim is to highlight the particularities of these terms in relation to cyberspace and the online environment, analysing the ways in which certain offenses are committed and the specific nature of their elements within the established framework.

Keywords: cyberspace, online, computer system, computer data, cryptocurrency, NFT, private life, begging, movable good.

INTRODUCERE

Continua dezvoltare a cyberspațiului și a lumilor virtuale poate să ridice anumite întrebări în ceea ce privește incidența unor termeni și expresii din legea penală, atât regăsite în partea generală, cât și în partea specială. Ne propunem în continuare câteva dintre aceste

expresii, fără a pretinde o analiză exhaustivă, alegând pe acelea care au ridicat sau pot ridica discuții interesante în contextul cyberspațiului.

Când ne referim la cyberspațiu, discutăm despre *rețeaua de infrastructuri ale tehnologiei informației interdependente, care include Internetul, rețelele de telecomunicații, computerele, sistemele informatice, sistemele de control industrial, rețelele, precum și procesoarele și controlerele integrate*[1]. Pe baza acestei definiții, dorim să subliniem că tot ceea ce înseamnă internetul (rețeaua *www),* mediul online, rețelele sociale și lumile virtuale sunt incluse în cyberspațiu.

I. TERMENI ȘI EXPRESII DIN PARTEA GENERALĂ

Definițiile incluse în Titlul X al Părții generale din Codul penal au rolul de a conceptualiza anumiți termeni utilizați în legea penală, atât pentru a oferi o previzibilitate destinatarilor legii penale, cât și pentru a crea o coerență în cadrul părții speciale atunci când se face referire în mod repetat la aceștia. Rolul acestor definiții este de a sistematiza noțiunile folosite, de a garanta inclusiv caracterul unitar al dreptului penal[2], dar mai ales de a exercita caracterul autonom al acestuia, sub aspectul autonomiei conceptuale[3]. Dezbaterile jurisprudențiale și doctrinare au fost ample în privința unora dintre acești termeni – a se vedea, spre exemplul, situația funcționarului public (art. 175 C.pen.) sau a membrului de familie (art. 177 C.pen.)[4], alți termeni însă nefiind la fel de populari în dezbaterile juridice, fie datorită clarității definițiilor, fie, mai ales – credem noi – datorită lipsei incidenței unor probleme frecvente cu privire la aplicarea lor în practica judiciară.

În continuare, vom trece în revistă acei termeni din acest titlu a căror analiză ni se pare relevantă în contextul mediului online și a cyberspațiului. Deși poate părea surprinzătoare lipsa analizei expresiei *faptă săvârșită în public,* această expresie a fost subiectul unui studiu anterior dedicat[5].

1. Sistem informatic și date informatice (art. 181 C.pen.)

Sistemul informatic este definit în art. 181 alin. (1) C.pen. ca fiind „*orice dispozitiv sau ansamblu de dispozitive interconectate sau aflate în relație funcțională, dintre care unul sau mai multe asigură prelucrarea automată a datelor, cu ajutorul unui program informatic*”. Același articol, la alin. (2), statuează că „*Prin date informatice se înțelege orice reprezentare a unor fapte, informații sau concepte într-o formă care poate fi prelucrată printr-un sistem informatic*”.

Potrivit definiției arătate, vor fi considerate sisteme informatice calculatoarele, laptopurile, telefoanele (doar *smartphone*-urile), bancomatele, PoS (point of sale) orice alte

[1] Pentru aceasta și alte definiții ale cyberspațiului, a se vedea, de exemplu, https://csrc.nist.gov/glossary/term/cyberspace (consultat 15.12.2024).
[2] Pentru detalii asupra acestui caracter, a se vedea *L.V. Lefterache*, Drept penal. Partea generală, Ediția a 4-a, Ed. Hamangiu, București, 2024, pp. 14-15; *C. Mitrache, Cr. Mitrache*, Drept penal român, Partea generală, Ediția a V-a, Ed. Universul Juridic, București, 2023, p. 30.
[3] *L.V. Lefterache,* op. cit., pp. 12-12; *F. Streteanu, D. Nițu,* Drept penal. Partea generală. Volumul I, Editura Universul Juridic, București, 2014, pp. 17-19.
[4] Deși niciunul din acești termeni nu sunt de interes pentru demersul nostru.
[5] *D. Herinean,* Infracțiunile comise în mediul online – infracțiuni comise în public? în AUBD – Forum juridic nr. 2/2024, disponibil online.

obiecte care fac parte din categoria *smart objects,* adică acelea care au un sistem de operare propriu sau care fac parte din IoT (*internet of things)*. În doctrină s-a arătat că o rețea formată din mai multe sisteme informatice nu devine un sistem informatic distinct, astfel încât un *blockchain* nu poate fi considerat în integralitate un sistem informatic unic, fiind de fapt o asociere de mai multe sisteme informatice participante pe baza căreia funcționează această tehnologie[6].

Tot sisteme informatice vor fi și acelea care sunt dotate cu inteligență artificială. Observăm așadar în acest context că deși inteligența artificială nu are nicio reglementare specifică în domeniul dreptului penal, orice sistem care integrează o formă de inteligență artificială va putea fi calificat ca un sistem informatic[7].

Datele informatice pot fi explicate din mai multe perspective. Pe de-o parte, din punct de vedere informatic, ele sunt șiruri de 0 și 1 care pot fi decodate prin utilizarea unui sistem de citire a limbajului de programare în care sunt scrise (a unui sistem informatic). Tot date informatice sunt și liniile de cod în baza cărora funcționează o platformă sau un program. Toate fișierele din laptopurile fiecăruia dintre noi reprezintă ori sunt formate din date informatice.

Practic, simplificând discuția, sistemele informatice funcționează pe baza datelor informatice care sunt decodate și prelucrate utilizând un algoritm de calcul.

În cazul mediului online și al cyberspațiului, acestea au la bază de o rețea de sisteme informatice care interacționează între ele pentru crearea și funcționarea platformelor și a lumii digitale. În această privință, există un cadru special creat de infracțiuni care protejează tocmai integritatea sistemelor și a datelor informatice: Titlul VII (Infracțiuni contra siguranței publice), capitolul VI (infracțiunile contra siguranței și integrității sistemelor și datelor informatice), respectiv art. 360-365 C.pen., infracțiunile care sunt denumite infracțiuni informatice *stricto sensu*[8].

În ceea ce privește încadrarea acestor termeni în conținutul juridic[9] al infracțiunilor, sistemele informatice și datele informatice ar fi cel mai apropiate de obiectul material, obiectul juridic generic fiind integritatea sistemelor și datelor informatice. Discuția privind „dematerializarea" obiectului material a fost amplu tratată într-un articol de specialitate[10]. Printr-o interpretare evolutivă, credem că este posibil să considerăm că inclusiv datele

---

[6] În același sens, a se vedea *C.-T. Stănescu*, Evoluția infracțiunii de fraudă informatică. Scurte considerații, publicat în Revista Themis nr. 1-2/2022, disponibil online, p. 132.

[7] În același sens, a se vedea *G.-M. Husti*, Acțiunea, inacțiunea și legătura de cauzalitate în cazul inteligenței artificiale, publicat în Revista Themis nr. 1-2/2021, disponibil online, p. 45. În sensul în care discuțiile privind inteligența artificială s-ar plasa în sfera datelor informatice, iar nu a sistemelor informatice, a se vedea *C.-T. Stănescu*, op. cit., p. 127.

[8] A se vedea, în acest sens, *D. Herinean*, Provocările criminalității digitale pentru dreptul penal. Dreptul penal în combaterea criminalității în mediul online, publicat în Revista Română de Drept al Afacerilor nr. 3/2023, p. 23. Prin acest articol am propus și utilizarea termenului *infracțiuni digitale*, care înglobează atât infracțiunile informatice *stricto sensu,* cât și infracțiunile comise *în mod digital* – definite ca acele infracțiuni care au fost comise în mod întâmplător prin tehnologia digitală, deși această utilizare nu este cerută de conținutul lor constitutiv.

[9] Reamintim că diferența între conținutul juridic al unei infracțiuni și conținutul constitutiv al acelei infracțiuni constă în faptul că primul – definit ca totalitatea condițiilor necesare pentru existența unei infracțiuni – îl include pe cel de-al doilea, care reprezintă totalitatea condițiilor cerute de norma de incriminare cu privire la actul de conduită. Pentru această distincție, a se vedea *L.V. Lefterache*, op. cit., p. 178.

[10] *G. Zlati,* Dematerializarea obiectului material al infracțiunii în contextul evoluției tehnologice și consecințele acesteia, în Dreptul, nr. 9/2013.

informatice au o corporalitate (chiar dacă minimă, însă) suficientă pentru a fi avute în vedere ca un obiect material.

Mai observăm că tipicitatea tuturor acestor infracțiuni presupune o interacțiune logică între subiectul activ și sistemul informatic, respectiv utilizarea acelui sistem informatic în maniera în care acesta este destinat a fi folosit. Dacă discutăm doar de interacțiuni fizice, fără operarea sistemului informatic, vom rămâne în sfera infracțiunilor clasice, unde sistemul informatic – ca obiect corporal – va fi obiectul material al infracțiunilor de furt ori distrugere, spre exemplu.

Pentru a oferi un exemplu în acest sens în privința punerii în imposibilitate de utilizare a unui laptop, dacă aceasta se realizează prin distrugerea cu un ciocan, va fi incidentă o infracțiune de distrugere. Dacă însă laptopul este blocat prin criptarea de la distanță (ceea ce se întâmplă în cazul *ransomware*[11]), atunci vom discuta de infracțiunea de *perturbarea funcționării sistemelor informatice*[12] cu privire la punerea în imposibilitate de utilizare a laptopului respectiv. În acest sens, odată ce se utilizează (sau mai bine spus operează) sistemele informatice, orice infracțiuni care vor avea ca obiect material sistemul informatic ori datele informatice vor fi încadrate în aceste norme de incriminare, neputând discuta, de exemplu, de furtul unor date informatice prin copiere în sensul art. 228 C.pen., acestea nefiind *bunuri mobile.* Cu toate acestea, există o infracțiune dedicată în acest sens care ar putea fi aplicabilă, respectiv infracțiunea de la art. 364 C.pen.: *Transferul neautorizat de date informatice*[13]. De asemenea, distrugerea unor date informatice nu va fi încadrată ca o infracțiune de distrugere, ci ca o infracțiune de *alterare a integrității datelor informatice,* prevăzută în art. 352 C.pen.[14]*.* Mai trebuie menționat că, în doctrină s-a arătat că datele informatice sunt diferite de simplele informații, cele două categorii neputând fi asimilate[15].

Dacă sistemele informatice vor fi în marea majoritate a cazurilor bunuri corporale și astfel este indiscutabil că pot face obiectul material al unor infracțiuni clasice (furt, distrugere ș.a.), discuția este mai interesantă în cazul datelor informatice, unde definiția lor pare a exclude acest lucru. Trebuie remarcat însă că deseori datele informatice primesc, în mediul digital, aparența unor bunuri corporale, obiecte de artă (a se vedea de exemplul cazul celebrelor NFT-uri) sau chiar aparența unor ființe*:* plante, animale sau chiar avataruri umane. Cu toate acestea, discuția prezintă relevanță doar atunci când interacțiunea este directă cu

---

[11] Ceea ce presupune inclusiv formularea unor pretenții, de regulă de natură pecuniară, pentru deblocarea sistemului. În aceste condiții, se poate reține un concurs de infracțiuni cu infracțiunea de șantaj, prevăzută în art. 207 alin. (3) C.pen. Pentru mai multe detalii în legătură cu termenul *ransomware,* a se vedea https://www.ncsc.gov.uk/ransomware/home (accesat 19.11.2024).

[12] Art. 363 C.pen.: *Fapta de a perturba grav, fără drept, funcţionarea unui sistem informatic, prin introducerea, transmiterea, modificarea, ştergerea sau deteriorarea datelor informatice sau prin restricţionarea accesului la date informatice, se pedepseşte cu închisoarea de la 2 la 7 ani.*

[13] *Transferul neautorizat de date dintr-un sistem informatic sau dintr-un mijloc de stocare a datelor informatice se pedepseşte cu închisoarea de la unu la 5 ani.*

[14] *Fapta de a modifica, şterge sau deteriora date informatice ori de a restricţiona accesul la aceste date, fără drept, se pedepseşte cu închisoarea de la unu la 5 ani.*

[15] A se vedea *G. Zlati,* Dematerializarea obiectului material al infracțiunii în contextul evoluției tehnologice și consecințele acesteia, în Dreptul, nr. 9/2013, p. 168: „*Soluția a fost acceptată și în jurisprudența common law (a se vedea cauza Oxford contra Moss, citată în J. Herring, Criminal Law, Third Edition, Ed. Palgrave Macmillan, Bristol, 2002, p. 244), unde s-a analizat acțiunea unui student de a se uita fără drept peste conținutul unei lucrări. Astfel, din moment ce agentul a captat doar informația, fără a intra în posesia suportului fizic pe care aceasta era stocată, instanța a considerat că fapta nu reprezintă un furt. Vedem noțiunea de informație în acest context ca fiind diferită de datele informatice*".

datele informatice, iar nu cu suportul pe care acestea se află. Spre exemplu, dacă discutăm de un *memory stick* pe care se află date informatice care este furat, obiectul material va fi *memory stick*-ul, iar nu datele informatice.

În cazurile despre care discutăm, întrebarea care se pune este dacă ele rămân date informatice în mediul digital sau, din contră, atunci când interacțiunea cu ele are loc exclusiv în acest mediu, ele ar putea fi calificate pe baza aparenței în care sunt decodate de către sistemul informatic – ca bunuri, de exemplu.

Din definiția datelor informatice pare că ar rezulta că această noțiune este aplicabilă doar atunci când faptele, informațiile sau conceptele sunt reprezentate *„într-o formă care poate fi prelucrată printr-un sistem informatic”*. *Per a contrario,* am putea considera că faptele, informațiile sau conceptele nu sunt catalogate ca date informatice atunci când sunt reprezentate într-o formă prelucrată deja de un sistem informatic. În egală măsură, aplicând raționamentul *a fortiori,* am putea considera că ele vor fi date informatice și atunci când sunt reprezentate în forma deja prelucrată.

Soluția nu credem că poate fi una categorică, ambele argumente prezentate putând să fie utilizate pentru a tranșa problema, în funcție de specificul speței și de infracțiunea analizată.

Un criteriu primar este posibilitatea calificării respectivei reprezentări a datelor informatice într-o altă categorie cu relevanță pentru legea penală, cum ar fi un bun mobil, o operă de artă protejată de drepturi de proprietate intelectuală, un secret comercial ș.a. Dacă această posibilitate lipsește, credem că soluția ce se va impune va fi reținerea unei infracțiuni contra integrității sistemelor și a datelor informatice. În cazul existenței acestei posibilități, opinăm în sensul că reținerea incidenței unei alte infracțiuni se va verifica și tranșa de la caz la caz.

2. Mijloace de plată fără numerar (art. 180 C.pen.)

Articolul 180 C.pen. reglementează *de lege lata* definițiilor mijloacelor de plată fără numerar, respectiv *instrument de plată fără numerar*, *instrument de plată electronică*, *monedă electronică* și *monedă virtuală*. Trebuie menționat că anterior Legii nr. 207/2021[16], în art. 180 C.pen., care avea denumirea marginală *Instrument de plată electronică* exista o singură definiție: *„Prin instrument de plată electronică se înțelege un instrument care permite titularului să efectueze retrageri de numerar, încărcarea și descărcarea unui instrument de monedă electronică, precum și transferuri de fonduri, altele decât cele ordonate și executate de către instituții financiare”,* operând astfel o reformare semnificativă (cel puțin în aparență) a acestei materii, prin implementarea în legislația internă a dispozițiilor *Directivei non-cash*[17]*.*

Aceste expresii sunt utilizate în mai multe norme de incriminare din Codul penal, cum sunt art. 250 C.pen. (*efectuarea de operațiuni financiare în mod fraudulos*), art. 250[1] (*operațiuni ilegale cu instrumente de plată fără numerar*), art. 251 (*acceptarea operațiunilor financiare efectuate în mod fraudulos*), art. 311 (*falsificarea de titluri de credit sau instrumente de plată*), art. 313 (*dobândirea de instrumente de plată fără numerar falsificate*), art. 314

[16] M.Of. nr. 720 din 22.07.2021. Prin aceeași lege au fost modificate și art. 249, 250, 251, 313, 314, 316 C.pen. și s-a introdus art. 250[1] C.pen.

[17] Directiva (UE) 2019/713 a Parlamentului European și a Consiliului din 17 aprilie 2019 privind combaterea fraudelor și a contrafacerii în legătură cu mijloacele de plată fără numerar și de înlocuire a Deciziei-cadru 2001/413/JAI a Consiliului.

(*deținerea de instrumente în vederea falsificării de valori*) și art. 316 (*falsificarea de valori străine*).

Vom prezenta în continuare fiecare definiție, acestea fiind preluate din directiva menționată, dublată de exemple pentru a facilita înțelegerea acestora:

Instrument de plată fără numerar

„(1) Prin instrument de plată fără numerar se înțelege un dispozitiv, un obiect sau o înregistrare, protejat, respectiv protejată, material ori nematerial, respectiv materială ori nematerială, sau o combinație a acestora, altul, respectiv alta decât o monedă cu valoare circulatorie și care, singur, respectiv singură sau împreună cu o procedură sau un set de proceduri, permite deținătorului sau utilizatorului transferul de bani sau valoare monetară, inclusiv prin monedă electronică sau monedă virtuală".

Exemple de instrumente de plată fără numerar: cardurile bancare (care sunt mijloace de stocare a datelor informatice[18]); servicii de tipul Internet Banking sau Mobile Banking; instrumente care permit transferul de monede virtuale (criptomonede); aplicațiile de transfer bani (de tipul *Revolut*); instrumentele cu acces la distanță tip *token;* brățările *contactless* folosite la festivaluri[19] ș.a.

Definiția aceasta este cea mai largă dintre cele prevăzute în acest articol, în categoria ei intrând atât instrumentele de plată electronice, cât și moneda virtuală[20]. Conform definiției, instrumentele de plată fără numerar pot fi atât materiale (cum este cazul cardurilor), cât și nemateriale (o aplicație de internet banking de exemplu).

Aceste instrumente de plată pot face inclusiv obiectul unor infracțiuni de fals, cum este cea de la art. 311 alin. (2) C.pen., art. 313 alin. (4) C.pen. și art. 314 alin. (2)-(3) C.pen., fiind incriminată inclusiv dobândirea pentru sine în vederea utilizării frauduloase a unui instrument de plată fără numerar falsificat – un card falsificat, de exemplu.

Instrument de plată electronică

„(2) Prin instrument de plată electronică se înțelege un instrument care permite efectuarea de retrageri de numerar, încărcarea și descărcarea unui instrument de monedă electronică, precum și transferuri de fonduri, altele decât cele ordonate și executate de către instituții financiare".

Exemple de instrumente de plată electronică: cardurile bancare (chip-card); instrumentele cu acces la distanță tip *token;* brățările *contactless* folosite la festivaluri.

Trebuie observat că instrumentele de plată electronice se subscriu categoriei mai largi a instrumentelor de plată fără numerar. Apoi, observăm o neconsecvență a legiuitorului, care deși definește instrumentul de plată electronică, în art. 250 alin. (1) C.pen. și art. 251 alin. (1) C.pen. folosește noțiunea de *instrument de monedă electronică,* deși o definiție pentru această sintagmă nu este nicăieri prevăzută. Cu toate acestea, credem că în fapt va fi aplicabilă această definiție pentru delimitarea sferei de aplicare a normei. De altfel, în codul penal, această noțiune nu este utilizată în nicio normă de incriminare (cu excepția celor 2 deja menționate), toate normele de incriminare făcând referire la noțiunea prezentată anterior, *instrumente de plată fără numerar.*

[18] *G. Zlati*, Tratat de criminalitate informatică, op.cit., p. 98.
[19] *G. Zlati,* Frauda informatică. Aspecte controversate, publicat în Caiete de Drept penal nr. 4/2018, p. 147.
[20] *G. Zlati,* Tehnologia blockchain, monedele virtuale și dreptul penal, publicat în Penalmente Relevant nr. 1/2021, p. 61.

Monedă electronică

„(3) Prin monedă electronică se înțelege valoarea monetară stocată electronic, inclusiv magnetic, reprezentând o creanță asupra emitentului, emisă la primirea fondurilor în scopul efectuării de operațiuni de plată și care este acceptată de o persoană, alta decât emitentul de monedă electronică”.

Exemple de **monede electronice**: sumele de bani ce pot fi accesate prin intermediul unui card bancar[21] sau prin intermediul internet banking / mobile banking; sumele de bani din alte conturi de plată - PayPal, Revolut, Cardurile de credit emise de IFN-uri ș.a..

Conform literaturii de specialitate, moneda electronică este o monedă „preplătită”[22], o monedă clasică transpusă în mediul virtual. Caracteristicile monedelor electronice au fost grupate în aceeași lucrare[23], inspirate din Legea nr. 210/2019[24], în trei părți:

- Activitatea de emitere de monedă electronică se realizează doar de către entități autorizate[25];
- Moneda electronică reprezintă o creanță asupra emitentului, în cuantumul valorii stocate electronic – cuantum care corespunde monedei fizice[26];
- Moneda electronică trebuie să fie acceptată la plată pentru achiziționarea de bunuri și servicii în mod general, inclusiv de alte persoane decât emitentul[27];

Se observă așadar că monedele electronice sunt strict legate de un caracter oficial, public și general acceptat al acestora, neputând discuta de monede electronice private sau cu utilizare limitată. Totodată, este important de observat că moneda electronică se materializează într-un drept de creanță asupra emitentului, nefiind bunuri corporale sau individualizate.

---

[21] Având în vedere această definiție, credem că în dreptul penal, termenii *monedă electronică* și *monedă de cont* pot fi folosiți în mod sinonimic. În doctrina de drept privat se arată că moneda de cont ar fi *„o formă monetară incorporală emisă de o instituție de credit şi înregistrată – de regulă, în mediu electronic – în conturile bancare ale acesteia*”, în timp ce moneda electronică ar fi *„o formă monetară incorporală emisă de o instituție emitentă de monedă electronică şi stocată pe un suport electronic specific*”, definiția din urmă fiind inspirată de art. 4 alin. (1) lit. f) din Legea nr. 127//2011, conform celor indicate de autor. În acest sens, a se vedea *L. Bercea,* „Prețul constă într-o sumă de bani”. De la moneda de cont la „moneda” virtuală (și înapoi), în Revista română de drept privat nr. 3/2017, p. 69.

[22] *G. Zlati,* Tehnologia blockchain, monedele virtuale și dreptul penal, op. cit., p. 27; *L. Bercea,* „Prețul constă într-o sumă de bani”. De la moneda de cont la „moneda” virtuală (și înapoi), în Revista română de drept privat nr. 3/2017, p. 65; *D.-M. Ilucă,* De la sare la Libra coin: scurt istoric al formelor monetare şi aspectul lor juridic, disponibil online (accesat 25.11.2024), p. 224.

[23] *G. Zlati,* Tehnologia blockchain, monedele virtuale și dreptul penal, op.cit., pp. 28-29.

[24] M.Of. nr. 914 din 13.11.2019.

[25] Potrivit art. 2 alin. (1) din Legea nr. 210/2019:

a) instituţiile de credit […];

b) instituţii emitente de monedă electronică - persoane juridice autorizate să emită monedă electronică, conform legii;

c) furnizori de servicii poştale care emit monedă electronică potrivit cadrului legislativ naţional aplicabil;

d) Banca Centrală Europeană şi băncile centrale naţionale, atunci când acestea nu acţionează în calitate de autorităţi monetare sau în altă calitate ce implică exerciţiul autorităţii publice;

e) statele membre şi autorităţile lor regionale ori locale, atunci când acestea acţionează în calitatea lor de autorităţi publice.

[26] *G. Zlati,* Tehnologia blockchain, monedele virtuale și dreptul penal, op.cit., pp. 27-28.

[27] *Ibidem.*

Dacă se creează „monede" în spațiul digital de către entități private, chiar unele care imită funcțional monedele electronice (fără a sugera o încercare de falsificare), acestea vor putea fi eventual calificate drept monede virtuale.

Monedă virtuală

„(4) Moneda virtuală înseamnă o reprezentare digitală a valorii care nu este emisă sau garantată de o bancă centrală sau de o autoritate publică, nu este în mod obligatoriu legată de o monedă instituită legal și nu deține statutul legal de monedă sau de bani, dar este acceptată de către persoane fizice sau juridice ca mijloc de schimb și poate fi transferată, stocată și tranzacționată electronic".

Exemple de monede virtuale (criptomonede): *Bitcoin, Ether, eGold, XRP, Litecoin, etc.* Exemple de monede virtuale care nu sunt criptomonede: cardurile cadou ce pot fi folosite la un singur magazin / la un singur lanț de magazine; creditul pe care o persoană îl are pe o anumită platformă; punctele de fidelitate care pot fi folosite pentru plata parțială a unor bunuri/servicii la un anumit distribuitor.

Deși în marea parte a cazurilor în care discutăm de monede virtuale ne gândim automat la criptomonede, credem că prima categorie este mai largă, incluzând-o pe cea de-a doua[28]. Din perspectiva noastră, noțiunea de monedă virtuală se poate referi inclusiv la diferiți bani virtuali utilizați drept „credit" în diferite aplicații, cum ar fi jocurile online, platforme de cumpărături, aplicații de livrare ș.a., inclusiv punctele de fidelitate care pot fi folosite ca mijloc de plată[29]. Or, acestea din urmă, nu ar fi catalogate în mod uzual drept *criptomonede.* De aceea, fără a încerca să oferim o definiția a criptomonedelor, putem afirma că, în sensul curent, nu toate monedele virtuale sunt criptomonede, dar toate criptomonedele – dacă le avem în vedere ca mijloace de schimb – sunt monede virtuale.

În egală măsură, dacă ne raportăm la noțiunea mai largă de criptoactive[30], în literatura de specialitate s-a arătat că toate monedele virtuale sunt criptoactive, însă nu toate criptoactive sunt monede virtuale[31], dându-se exemplul NFT-urilor care sunt criptoactive, deși nu sunt monede virtuale.

Într-un studiu al Băncii Centrale Europene, s-a arătat că există trei tipuri de monede virtuale, clasificarea făcându-se în funcție de modalitatea în care acestea interacționează cu monedele clasice: (i) schemele închise, care nu au aproape nicio legătură cu economia reală și presupun că monedele virtuale nu pot fi cumpărate cu monede clasice și nici nu pot fi

---

[28] În același sens, dându-se exemplu aurul din *World of Warcraft,* a se vedea *G. Zlati,* Tehnologia blockchain, monedele virtuale și dreptul penal, op.cit., p. 21, nota de subsol 66. Autorul însă menționează în altă parte a aceleiași lucrări că noțiunile sunt interschimbabile (*Idem,* p. 17, nota de subsol 32), concluzie cu care suntem totuși de acord (fără însă a uita distincția menționată) având în vedere că vasta majoritate a monedelor virtuale sunt într-adevăr criptomonedele.

[29] Dacă nu se folosesc tehnologiile specifice *blockchain* – ceea ce ar determina ca acești bani să devină criptomonede.

[30] Definite, în art. 3 alin. (1) pt. 5 din Regulamentul (UE) 2023/1114 al Parlamentului European și al Consiliului din 31 mai 2023 privind piețele criptoactivelor și de modificare a Regulamentelor (UE) nr. 1093/2010 și (UE) nr. 1095/2010 și a Directivelor 2013/36/UE și (UE) 2019/1937 (în continuare, „Regulamentul MiCA") ca *„o reprezentare digitală a unei valori sau a unui drept care poate fi transferată și stocată electronic, utilizând tehnologia registrelor distribuite sau o tehnologie similară"*.

[31] *A.-R. Trandafir, G. Zlati,* Monedele virtuale: între obținerea datelor privind tranzacțiile financiare și luarea măsurilor asigurătorii în procesul penal, publicat în AUBD – Forum juridic nr. 1/2022, disponibil online, p. 60 (accesat 25.11.2024).

schimbate în astfel de monede (cel puțin în teorie), ci doar pot fi dobândite prin diferite prin diferite moduri și utilizate în interiorul platformei / lumii virtuale, de cele mai multe ori o lume virtuală atașată unui joc; (ii) schemele cu flux unidirecțional de monedă virtuală, când moneda clasică poate fi transformată în monedă virtuală, însă reciproca nu e valabilă; (iii) scheme cu flux bidirecțional, în care sunt posibile schimburile reciproce[32]. Criptomonedele se află în această ultimă categorie.

Având în vedere că marea majoritate a monedelor virtuale utilizează tehnologia *blockchain*[33], este important de subliniat că nu trebuie confundat numele criptomonedei cu denumirea *blockchain*-ului utilizat, deși uneori denumirile sunt similare[34]. Pentru a oferi câteva exemple, există identitate între numele monedei *bitcoin (*BTC) și blockchain-ul *Bitcoin,* dar nu și între numele monedei eGold (EGLD) și blockchain-ul *Elrond* sau între numele monedei XRP și blockchain-ul Ripple, nefiind exclus totodată ca în același blockchain să funcționeze mai multe criptomonede[35].

Ca trăsături caracteristice ale unei monede virtuale, desprinse din definiția menționată în Codul penal, reies următoarele:

- nu este emisă sau garantată de o bancă centrală sau o autoritate publică, neexistând însă vreo indicație cu privire la cine ar putea să fie titularul unei astfel de emisiuni;
- nu este în mod obligatoriu legată de o monedă instituită legal, însă această posibilitate nu este exclusă, iar simplul fapt că o monedă virtuală ar fi legată de o monedă instituită legal (în sensul că valoarea acesteia ar fi indexată corespunzător) nu o transformă într-o monedă electronică[36];
- nu deține statutul legal de *monedă* sau de *bani* – această condiție este o nouă deosebire în raport de moneda electronică;
- este acceptată de către persoane fizice sau juridice ca mijloc de schimb – de aici reiese că natura contractului eventual încheiat va fi cea a unui contract de schimb, iar nu cea a unui contract de vânzare cumpărare; totodată, se mai observă că nu se cere ca această acceptare să fie una generală, putând fi acceptate doar de anumite persoane sau companii;
- poate fi transferată, stocată și tranzacționată electronic – de unde rezultă că monedele virtuale nu este necesar (dar nici exclus) să aibă un corespondent material.

Mai trebuie menționat că, din punct de vedere fiscal, veniturile din tranzacționarea cu monede virtuale nu sunt impozabile decât la momentul în care monedele virtuale sunt schimbate într-o monedă fiduciară (clasică)[37].

Prin incorporarea tuturor acestor definiții în legislația noastră se observă că legiuitorul a urmărit (impulsionat de modelul european[38]) să țină pasul atât cu dezvoltările tehnologice

[32] European Central Bank, Eurosystem, Virtual Currency Schemes, October 2012, p. 13, disponibil la https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf (accesat 23.11.2024).
[33] Există și criptomonede care nu utilizează însă această tehnologie. În acest sens, a se vedea, de exemplu, https://www.bitstamp.net/en-gb/learn/blockchain/do-all-cryptocurrencies-use-the-blockchain/ (accesat 25.11.2024).
[34] *Idem,* p. 15.
[35] A se vedea *idem,* pp. 15-16.
[36] *Idem,* p. 22.
[37] Pentru mai multe detalii în acest sens, a se vedea *D.-S. Chertes,* Venitul din transferul de monedă virtuală și evaziunea fiscală, în Penalmente Relevant nr. 1/2021, disponibil (accesat 25.11.2024).
[38] Aspect care reiese inclusiv din expunerea de motive a Legii nr. 207/2021.

și cu tendințele sociale referitoare la modalități de plată și de utilizare a activelor, cât și cu inerenta transferare a criminalității în cyberspațiu și online, unde se pot obține și tranzacționa sume foarte mari de bani, fie ei electronici sau virtuali.

Nu în ultimul rând, în doctrină s-a arătat că definiția aceasta este problematică întrucât se axează pe diferența dintre monede virtuale și monede electronice, fără însă a anticipa necesitatea de diferențiere în raport cu alte criptoactive[39]. Spre exemplu, suntem de acord că un NFT nu poate fi considerat o monedă virtuală[40]. Regretabil, după cum s-a susținut și în doctrină[41], cadrul legal stabilit prin aceste definiții este mult depășit de evoluția tehnologică, cea mai recentă reglementare europeană în materie - Regulamentul MiCA – nefolosind deloc noțiunea de monedă virtuală, definind alți termeni precum criptoactiv[42], token raportat la active[43], token de monedă electronică[44], token utilitar[45] ș.a.

3. Arme (art. 179 C.pen.)

Noțiunea de armă este definită în art. 179 alin. (1) C.pen., printr-o definiție cadru *(Arme sunt instrumentele, dispozitivele sau piesele declarate astfel prin dispoziții legale),* fiind necesare dispoziții speciale care să declare ca arme diferitele obiecte pentru ca această definiție să aibă un conținut efectiv. Totodată, în alineatul (2) al art. 179 C,pen. avem definiția armelor asimilate (*Sunt asimilate armelor orice alte obiecte de natură a putea fi folosite ca arme și care au fost întrebuințate pentru atac*), care face trimitere la noțiunea de atac, acesta sugerând în mod clar un atac fizic.

Legea nr. 295/2004[46] prevede cele mai multe definiții ale armelor, nefiind util pentru studiul nostru să reproducem în integralitate aceste definiții la acest moment[47], toate definițiile vizând doar ceea ce în mod natural și convențional se înțelege prin armă, adică obiecte care pot fi folosite în luptă (identic cu sensul uzual al cuvântului). Desigur, noțiunea de armă asimilată ridică anumite discuții interesante în legătură cu conținutul constitutiv al unor infracțiuni, însă aceste discuții excedează prezentului studiu, nefiind vorba de infracțiuni comise în cyberspațiu.

---

[39] *G. Zlati,* Obținerea fără drept de monede virtuale sau a altor criptoactive în Revista Română de Drept al Afacerilor nr. 3/2023, p. 40.

[40] În acest sens, a se vedea *Idem*, p. 41.

[41] În același sens, *G. Zlati,* Obținerea fără drept de monede virtuale sau a altor criptoactive, op. cit., p. 38.

[42] *„O reprezentare digitală a unei valori sau a unui drept care poate fi transferată și stocată electronic, utilizând tehnologia registrelor distribuite sau o tehnologie similară”.* Definiția a mai fost citată *supra.*

[43] *„Un tip de criptoactive care nu este un token de monedă electronică și care vizează menținerea unei valori stabile, prin raportare la o altă valoare sau la un alt drept ori la o combinație între acestea, inclusiv la una sau mai multe monede oficiale*”.

[44] *„Un tip de criptoactive care vizează menținerea unei valori stabile prin raportare la valoarea unei monede oficiale”.*

[45] *„Un tip de criptoactive care este destinat exclusiv să asigure accesul la un bun sau un serviciu furnizat de către emitentul său*”.

[46] M.Of., Partea I nr. 425 din 10.06.2014.

[47] Spre exemplu, noțiunea de *armă* este definită ca *„orice obiect sau dispozitiv a cărui funcționare determină aruncarea unuia sau mai multor proiectile, substanțe explozive, aprinse sau luminoase, amestecuri incendiare ori împrăștierea de gaze nocive, iritante sau de neutralizare, în măsura în care se regăsește în una dintre categoriile prevăzute în anexă”.* Există însă definiții pentru arme de foc, arme albe cu lamă ș.a. Pentru mai multe detalii, a se consulta, în acest sens, Legea nr. 295/2004. Este de observat că nicio definiție nu poate să acopere eventuale „arme” care pot fi folosite în mediul online.

Din aceste definiții putem observa așadar că *de lege lata* prin noțiunile de arme ne vom referi întotdeauna la armele din mediul fizic, care sunt apte să lezeze în mod material o persoană sau să distrugă într-o manieră materială obiecte. Tot timpul când legea face referire la *arme* vom avea în vedere deci exclusiv aceste ipoteze.

Ce se întâmplă cu *armele* din mediul online? După cum am văzut, când discutăm de reprezentări grafice/digitale ale unor arme în mediul online sau în lumi virtuale nu va fi vorba de arme în sensul legii penale. În același sens, într-un articol de specialitate s-a menționat că nu are relevanță pentru stabilirea calificării juridice a unui obiect virtual, cum ar fi o armă virtuală, legalitatea deținerii sale în mediul fizic sau chiar posibilitatea existenței sale, importantă fiind posibilitatea existenței unei valori patrimoniale sau recreaționale a respectivului obiect virtual[48].

Există totuși anumite obiecte care să poată fi calificate ca arme în mediul online? În dreptul internațional s-a discutat în ce măsură un atac cibernetic poate fi considerat un atac armat, fiind agreat cu ocazia mai multor întâlniri ale organismelor internaționale că în anumite situații atacurile cibernetice pot fi calificate ca atacuri în forță sau atacuri armate, care să dea dreptul unui actor internațional la utilizarea forței pentru a se apăra, fără însă a fi stabilite criterii clare în acest sens[49]. Totuși, nu s-a discutat, cel puțin până la acest moment, calificarea a *armă* a unui sistem informatic, însă, spre exemplu, a fost amplu analizată în doctrină posibilitatea reținerii legitimei apărări în domeniul criminalității informatice[50].

Indiferent de dezbaterea menționată, *de lege lata* cu siguranță un sistem informatic nu ar putea fi calificat ca o armă în sensul legii penale[51]. Cu toate acestea, există o normă de incriminare care sancționează interacțiunea cu sisteme informatice malițioase, care pot fi folosite ca arme, respectiv art. 365 C.pen., operațiuni ilegale cu dispozitive sau programe informatice[52], o incriminare obstacol care sancționează inclusiv deținerea unui sistem informatic ce poate fi folosit în scopul comiterii unei infracțiuni informatice. Astfel, există o normă specială, o incriminare obstacol care sancționează deținerea a ceea ce am putea numi *„arme informatice”.*

---

[48] *L. Strikwerda*, Theft of virtual items in online multiplayer computer games: an ontological and moral analysis. *Ethics Inf Technol* 14, 89–97 (2012). https://doi.org/10.1007/s10676-011-9285-3.

[49] Pentru mai multe detalii, a se vedea *C. Moldovan,* Atacurile cibernetice și legitima apărare în dreptul internațional, Analele Științifice ale Universității Alexandru Ioan Cuza din Iași, seria Științe Juridice 2-bis, 2019, p. 175-186.

[50] *G. Zlati*, Legitima apărare şi starea de necesitate în domeniul criminalității informatice (I), în Revista Dreptul nr. 4/2015; *G. Zlati*, Legitima apărare şi starea de necesitate în domeniul criminalității informatice (II), în Revista Dreptul nr. 5/2015. Intenționăm să abordăm și noi acest subiect într-o lucrare viitoare.

[51] Desigur, dacă discutăm de un sistem de tipul unei arme dotate cu inteligență artificială (*i.e.* un sistem de apărare care poate lansa atacuri fizice în domeniul material), un astfel de sistem ar putea fi atât un sistem informatic, cât și o armă în sensul legii penale. Însă aici ne referim în general, la un sistem informatic ce nu este integrat într-o armă propriu-zisă.

[52] Art. 365 C.pen. *„(1) Fapta persoanei care, fără drept, produce, importă, distribuie sau pune la dispoziție sub orice formă:*
a) dispozitive sau programe informatice concepute sau adaptate în scopul comiterii uneia dintre infracțiunile prevăzute în art. 360-364;
b) parole, coduri de acces sau alte asemenea date informatice care permit accesul total sau parțial la un sistem informatic, în scopul săvârșirii uneia dintre infracțiunile prevăzute în art. 360-364, se pedepsește cu închisoare de la 6 luni la 3 ani sau cu amendă.
(2) Deținerea, fără drept, a unui dispozitiv, a unui program informatic, a unei parole, a unui cod de acces sau a altor date informatice dintre cele prevăzute în alin. (1), în scopul săvârșirii uneia dintre infracțiunile prevăzute în art. 360-364, se pedepsește cu închisoare de la 3 luni la 2 ani sau cu amendă.”

4. Exploatarea unei persoane (art. 182 C.pen.)

Deși poate surprinzătoare în contextul lucrării noastre, analiza expresiei exploatarea unei persoane poate să aibă relevanță inclusiv din perspectiva obligării la prestarea de muncă/servicii în mediul online. Conform art. 182 C.pen., prin exploatarea unei persoane se înțelege:

„a) supunerea la executarea unei munci sau îndeplinirea de servicii, în mod forțat;

b) ținerea în stare de sclavie sau alte procedee asemănătoare de lipsire de libertate ori de aservire;

c) obligarea la practicarea prostituției, la manifestări pornografice în vederea producerii și difuzării de materiale pornografice sau la alte forme de exploatare sexuală;

d) obligarea la practicarea cerșetoriei;

e) prelevarea de organe, țesuturi sau celule de origine umană, în mod ilegal".

Din aceste variante alternative, litera e) este exclusă de la aplicabilitate în mediul online, însă toate celelalte variante sunt posibile, litera c) fiind chiar creată special pentru mediul online – prin referire la producerea și difuzarea de materiale pornografice. Sunt multe modalități în care persoane pot fi obligate la muncă și exploatate în mediul online, de la activități sexuale, la implicarea în diferite forme de înșelătorii online[53] și până la constrângerea unor persoane să ajute la spălarea banilor[54] ori la comiterea altor infracțiuni online, sub diferite pretexte ori amenințări că vor fi divulgate informații sau fotografii sensibile cu acestea obținute de făptuitori[55].

Astfel, infracțiuni precum traficul de persoane sau traficul de minori pot fi comise în totalitate în mediul online, de la distanță, fără o interacțiune fizică între făptuitor și victimă, atât timp cât făptuitorul a dobândit un control psihic asupra victimei, prin șantaj sau alte forme de constrângere, control care îi permite să determine conduita victimelor și să le exploateze în una din formele prevăzute în art. 182 C.pen.

Interesantă în acest context ar mai putea fi discuția posibilității comiterii infracțiunii de exploatarea cerșetoriei[56] în mediul online. Observăm că textul de incriminare nu distinge, singurul reper fiind includerea noțiunii de *public* în conținutul infracțiunii[57]. Deși cerșetoria nu mai este o infracțiune în actuala lege[58], fiind reglementată drept o contravenție, în vechiul Cod

[53] De exemplu, cele denumite *pig-butchering scams:* https://www.investopedia.com/pig-butchering-scams-8605501 (accesat 15.11.2024). Pentru alte exemple, a se vedea https://news.un.org/en/story/2021/10/1104392 (accesat 15.11.2024).

[54] Victimele devenind astfel ceea ce poate fi denumit *money mule:* https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/money-mules (accesat 25.11.2024).

[55] Situație denumită *sextortion.* A se vedea, de exemplu, https://www.esafety.gov.au/key-topics/image-based-abuse/deal-with-sextortion (accesat 15.11.2024).

[56] Art. 214 C.pen.: *Fapta persoanei care determină un minor sau o persoană cu dizabilități fizice ori psihice să apeleze în mod repetat la mila publicului pentru a cere ajutor material sau beneficiază de foloase patrimoniale de pe urma acestei activități se pedepsește cu închisoare de la 6 luni la 3 ani sau cu amendă.*

[57] Într-o lucrare anterioară am abordat pe larg posibilitatea considerării infracțiunilor comise online ca fapte săvârșite în public. A se vedea *D. Herinean,* Infracțiunile comise în mediul online – infracțiuni comise în public? în AUBD – Forum juridic nr. 2/2024, disponibil online.

[58] Pentru o incursiune istorică în legătură cu cerșetoria în dreptul penal român, a se vedea *H.-Ș. Tiugan*, Vagabondajul și cerșetoria. Între politica penală a mizeriei și mizeria politicii penale, în Curierul Judiciar nr. 5/2020, p. 273-282.

penal aceasta era o infracțiune care aducea atingere unor relații de conviețuire socială, reglementată în art. 326 C.pen.1968[59].

Pentru a folosi termenii din art. 214 C.pen., cerșetoria, în sensul legii penale, pare să desemneze *fapta minorului sau a persoanei cu dizabilități fizice sau psihice de a apela în mod repetat la mila publicului pentru a cere ajutor material.* Astfel, orice persoană care determină un minor / o persoană cu dizabilități fizice ori psihice să apeleze în mod repetat la mila publicului pentru a obține bani ori beneficiază de pe urma unei astfel de activități ar putea fi considerată că exploatează cerșetoria și astfel săvârșește această faptă.

În acest context, trebuie analizată situația platformelor de *crowdfunding*[60] sau *fundraising* care facilitează solicitarea de finanțări în mediul online de la persoane necunoscute și nedeterminate (ceea ce denotă în mod cert că discutăm de o solicitare în public) pentru a fi folosite în diferite proiecte. Desigur, majoritatea acestor platforme percep la rândul lor un mic comision pentru fiecare tranzacție sau un comision din suma totală strânsă, ceea ce înseamnă că ele beneficiază patrimonial de pe urma acestei activități. Dacă luăm cazul unul minor care își face un cont pe o astfel de platformă pentru a solicita bani de la public, solicitând în mod repetat astfel de finanțări pentru diverse motive, ar putea fi deținătorii platformei (persoane fizice și/sau juridice) acuzați de infracțiunea de exploatarea cerșetoriei? De asemenea, dacă mutăm ipoteza în cazul unei persoane cu dizabilități fizice care solicită pe o astfel de platformă bani de la public pentru a finanța o intervenție medicală, iar apoi pentru a achiziționa un dispozitiv medical, platforma comisionând ambele finanțări, se comite în egală măsură fapta prevăzută în art. 214 C.pen.?

Răspunsul pare a veni în mod firesc că nu, însă dacă mutăm ipoteza într-un spațiu fizic, la o gură de metrou unde un copil / o persoană cu dizabilități stă și solicită bani în mod repetat, plătind unor persoane un mic comision pentru a-i număra banii obținuți, răspunsul firesc se mută la polul opus. În acest context, trebuie observat că deși în denumirea marginală se folosește cuvântul *exploatare*, din conținutul infracțiunii reiese că nu discutăm de o trimitere la art. 182 C.pen., mai ales că în cazul alin. (2) se vorbește de constrângere ca element circumstanțial agravant, constrângere care este o premisă a definiției menționate. Prin urmare, termenul *exploatare* din denumirea marginală nu ne ajută la rezolvarea acestei dileme.

În egală măsură, transpunând discuția la nivel contravențional, fapta unei persoane apte de muncă de a apela la mila publicului în mod repetat, pe stradă, pentru a-și astâmpăra foamea s-ar transpune fără probleme pe dispozițiile art. 2 pct. 3 din Legea nr. 61/1991[61], însă fapta unei persoane de a solicita public și în mod repetat, pe o rețea de socializare sau pe o platformă, donații pentru a-și susține traiul nu cunoaștem, din informațiile publice, să fi fost vreodată sancționată ca o contravenție.

Ce repere putem avea în acest sens? În primul rând, art. 1 din Legea nr. 61/1991 stabilește că „*Pentru asigurarea climatului de ordine și liniște publică necesar desfășurării*

[59] Art. 326 C.pen.1968: *Fapta persoanei care, având capacitatea de a munci, apelează în mod repetat la mila publicului, cerând ajutor material, se pedepseşte cu închisoare de la o lună la 3 ani.*

[60] Pentru explicarea acestei noțiuni, a se vedea https://www.investopedia.com/terms/c/crowdfunding.asp# (accesat 25.11.2024).

[61] Potrivit art. 2 pct. 3 din Legea nr. 61/1991, republicată (M.Of. nr. 125 din 18.02.2020) *Constituie contravenţie săvârşirea oricăreia dintre următoarele fapte, dacă nu sunt comise în astfel de condiţii încât, potrivit legii penale, să fie considerate infracţiuni: [...] apelarea, în mod repetat, la mila publicului, de către o persoană aptă de muncă, precum şi determinarea unei persoane la săvârşirea unor astfel de fapte.*

normale a activității economice și social-culturale și promovarea unor relații civilizate în viața cotidiană, cetățenii sunt obligați să aibă un comportament civic, moral și responsabil, în spiritul legilor țării și al normelor de conviețuire socială". Apoi, trebuie să acordăm atenție cuvântului milă, pe care DEX îl definește ca: „*Sentiment de înțelegere și de compasiune față de suferința sau de nenorocirea cuiva*", dar și ca „*bunătate, bunăvoință, indulgență, îngăduință, înțelegere*".

Să fie generată diferența doar de nuanță, doar de modalitatea în care se pune problema? Mai exact, să fie considerată cerșetorie fapta aceluia care cere de pomană pe stradă motivat de faptul că suferă, că îi e foame sau că se află într-o situație dificilă (ceea ce se înțelege de altfel în mod curent prin cerșetorie), dar să poată *ocoli* această încadrare dacă pur și simplu cere bani pentru a-și finanța o anumită dorință / un anumit plan – alta decât cea a-și astâmpăra foamea? Dacă o persoană care în mod recurent apelează la mila publicului pe stradă, ar fi determinată de cineva care o învață (o determină - și care astfel ar „*exploata*"-o în sensul art. 214 C.pen.) să-și creeze un cont de YouTube unde să expună problemele sale și să solicite banii sub formă de donații într-un cont bancar, își pierde calitatea de „*contravenient*" și „*cerșetor*"? Din perspectiva noastră, nu; însă răspunsul trebuie explicat.

Gândindu-ne la obiectul juridic – buna desfășurare a conviețuirii sociale *lato sensu* – și privind problema din perspectiva legii penale, unde este incriminată doar exploatarea cerșetoriei ca o infracțiune contra persoanei (mai exact, contra persoanelor vulnerabile), putem observa că diferența „de nuanță" prezentată mai sus poate fi validă: solicitarea de donații în vederea finanțării unor proiecte (indiferent dacă e realizată pe stradă sau online) nu pare să sugereze existența unei persoane vulnerabile și nici să fie justificată de sentimente de milă, astfel încât obținerea inclusiv de către alții a unui beneficiu ca urmare a acestei facilitări nu ar leza obiectul juridic, însă dacă se apelează la sentimentul de *milă* al publicului, bazat pe suferință, pe sentimente negative, acestea nu ar trebui să aibă o valoarea tranzacționabilă, mai ales pentru alte persoane decât cea care solicită ajutorul – aceasta este paradigma legii penale. Chiar în ipoteza în care se apelează la mila publicului pentru motive medicale (condiția *în mod repetat* fiind de asemenea importantă în context), legea penală împiedică obținerea de foloase patrimoniale de către alte persoane decât cea care este beneficiarul aparent al fondurilor.

Apoi, din perspectiva legii contravenționale, putem considera că solicitarea de finanțări pentru diverse proiecte nu ar fi în *detrimentul conviețuirii sociale, al activității economice și a promovării de relații civilizate în viața cotidiană* – astfel cum declară art. 1 din Legea nr. 61/1991 precitat – ci, din contră, le-ar facilita. Pe de altă parte, în raport cu scopul declarat al legii, scoaterea din sfera ilicitului contravențional a încercării de exploatare repetată a sentimentului de milă de către o persoană aptă de muncă poate fi justificată de un caracter reprobabil din punct de vedere social și moral al unei astfel de îndeletniciri.

La mijloc între acestea, s-ar afla conduitele în care nu discutăm nici de finanțarea unor proiecte de care ar beneficia chiar indirect și alții sau societatea, dar nici de generarea unui sentiment de milă: solicitarea repetată de finanțare pentru îndeplinirea unui scop egoist, de tipul îndeplinirii unei dorințe (care poate fi cumpărată) care are un caracter pur personal: de exemplu, o excursie la Disneyland, o mașină nouă, un tatuaj făcut de o celebritate, un salt cu parașuta, cumpărarea unui Bitcoin, un zbor pe lună ș.a. În aceste cazuri, ne vom limita la a spune că delimitarea se va face tot în funcție de cele prevăzute în art. 1 din Legea nr. 61/1991: fapta va fi o contravenție în măsura în care se consideră că este demnă de un „*comportament civic, moral și responsabil, în spiritul legilor țării și al normelor de conviețuire socială*", că prin

ea nu este încălcat *„climatul de ordine și liniște publică necesar desfășurării normale a activității economice și social-culturale*" sau că prin ea nu se lezează *„promovarea unor relații civilizate în viața cotidiană".*

Mai putem constata, empiric și cutumiar, că apelarea pe rețelele de socializare la mila publicului prin intermediul platformelor care solicită un comision inclusiv pentru finanțarea unor intervenții medicale este tolerată, ceea ce pare să sugereze că morala contemporană nu justifică aplicarea normelor contravenționale și/sau penale acestor conduite atunci când sunt realizate în mediul online.

II. TERMENI ȘI EXPRESII DIN PARTEA SPECIALĂ

În această parte ne propunem să analizăm, pe scurt, câțiva dintre termenii și câteva dintre expresiile utilizate în partea specială a Codului penal, indiferent dacă în cazul lor discutăm de autonomia conceptuală a dreptului penal. Vom analiza termenii în ordinea în care apar în Codul penal.

1. Urmărește și supraveghează locuința (art. 208 C.pen.)

Infracțiunea de hărțuire în varianta de bază are un element material alternativ, aceasta putând fi comisă atât prin urmărirea unei persoane, cât și prin supravegherea locuinței acesteia.

Prima observație ce trebuie făcută este legată de obiectul juridic al infracțiunii de hărțuire, care după cum vom vedea, limitează de o manieră importantă domeniul de aplicabilitate al infracțiunii. Obiectul juridic este libertatea psihică a unei persoane[62], urmarea imediată prevăzută în alin. (1) al incriminării fiind o stare de temere. Din obiectul juridic și mai ales din această urmare imediată apare o cerință implicită a infracțiunii: ca subiectul pasiv să cunoască activitatea infracțională a făptuitorului, fiind imposibilă crearea unei stări de temeri altfel. Desigur, este posibil ca starea de temere să apară ulterior unei ample activități de hărțuire, însă infracțiunea se va considera consumată doar la momentul apariției stării de temere, iar în lipsa urmării imediate fapta nu va avea o valență infracțională, tentativa nefiind pedepsită.

Trecând mai departe, prin urmărirea unei persoane ne vom referi întotdeauna la o urmărire fizică a unei persoane, urmărirea pe stradă[63] de exemplu, direct sau chiar prin intermediul unor mijloace tehnice (cum ar fi o dronă[64]), neputând discuta de accepțiunea acestui cuvânt din mediul online (*„follow*", când discutăm de un cont de social media). Așadar, chiar dacă o persoană ar urmări întreaga activitate din mediul online a unei alte persoane (ceea ce s-ar putea numi un *„stalker*") nu va putea fi reținută vreodată infracțiunea de hărțuire în această modalitate.

Dincolo de faptul că în mod cert elementul material constând în *urmărirea* nu se referă la urmărirea activității din mediul online, este greu de imaginat și crearea unei stări de temere în aceste ipoteze, astfel încât ar lipsi și urmarea imediată. De principiu, fiecare persoană are un anumit control asupra aspectelor pe care le postează și le postează tocmai pentru a fi

[62] Pentru o analiză extinsă, se vedea *D. Herinean*, Infracțiunea de hărțuire. Aspecte controversate. Exerciții teoretice și examen de jurisprudență, în Penalmente Relevant nr. 1/2020, disponibil online (accesat 25.11.2024).
[63] Cu toate că nu este exclusă nici urmărirea efectuată prin mi
[64] În același sens, a se vedea *T. Manea*, *C.-N. Constantinescu-Mărunțel, H.-Ș. Tiugan,* op. cit., p. 189.

urmărite, asupra persoanelor cărora le permite accesul la conturile de *social media* și astfel poate limita accesul persoanelor nedorite. Din această perspectivă, eventualele fapte comise în acest context, dacă se depășește o urmărire pasivă a activității și se trece la contactarea persoanei, vor putea fi analizate pe tărâmul variantei alternative de hărțuire – art. 208 alin. (2) C.pen. – sau, pot fi încadrate ca *cyberbullying*.

Când vine vorba despre supravegherea locuinței unei persoane, infracțiunea de hărțuire vizează, din nou, supravegherea fizică a locuinței persoanei, acele ipoteze în care starea de temere a victimei se realizează ca urmare a observării autorului faptei în repetate rânduri în preajma locuinței sale. Așadar, de principiu, în cazul hărțuirii nu discutăm de supravegherea locuinței într-o manieră online, de la distanță, o astfel de faptă putând fi, eventual, analizată pe tărâmul violării vieții private, conform art. 226 alin. (5)[65] C.pen. Totuși, dacă victima ar cunoaște că făptuitorul a plasat o cameră de supraveghere în apropierea locuinței sale și o urmărește mereu când vine acasă, nu este exclusă nici reținerea unei infracțiuni de hărțuire.

Desigur, când discutăm de mediul online, cea mai frecventă formă de hărțuire este cea prevăzută în art. 208 alin. (2) C.pen., deoarece aceasta se realizează prin efectuarea de apeluri sau comunicări prin mijloace de transmitere la distanță. Nu vom insista însă pe această variantă normativă de transmitere în cuprinsul acestui articol, discuțiile fiind mereu orientate în doctrină față de mediul online în cazul acesteia[66].

2. Domiciliu (art. 224 C.pen.) și Sediu profesional (art. 225 C.pen.)

Noțiunea de domiciliu este exemplul clasic de autonomie conceptuală a dreptului penal, întrucât este notoriu faptul că domiciliul din dreptul penal are o altă semnificație decât domiciliul din celelalte ramuri de drept, în dreptul penal domiciliul fiind definit, astfel cum ni se confirmă încă o dată prin decizia HP nr. 18/2024[67], ca fiind o „*locuință, încăpere, dependință sau loc împrejmuit ținând de acestea*". Așadar, atunci când discutăm de domiciliu din punct de vedere penal, discutăm întotdeauna de un loc fizic.

Prin urmare, infracțiunea de violare de domiciliu nu poate fi comisă *de lege lata* niciodată în mediul online, în lumile virtuale, în jocuri sau în orice alte „locuri" din *cyberspace*, chiar dacă ar exista, spre exemplu, elemente de viață privată stocate în mod digital în acele spații virtuale (fotografii, filmulețe sau informații sensibile).

Totuși, există alte infracțiuni care ar putea să fie aplicabile în anumite cazuri, cum ar fi accesul ilegal la un sistem informatic, dacă pentru accesarea acelor locații s-ar utiliza conturi la care autorul nu ar avea un drept de acces sau dacă s-ar realiza cu depășirea limitelor autorizării. Spre exemplu, dacă un utilizator care are acces într-o lume virtuală doar la anumite locații virtuale ar reuși să pătrundă, în varii moduri, în alte locații unde accesul său era restricționat.

Soluția este similară în cazul infracțiunii de violarea sediului profesional. La acest moment, nu putem discuta despre „*sediile unde o persoană juridică sau fizică își desfășoară activitatea profesională*" în mediul online, fiind clar că textul de lege se referă doar la spații

[65] *„Plasarea, fără drept, de mijloace tehnice de înregistrare audio sau video, în scopul săvârșirii faptelor prevăzute în alin. (1) și alin. (2), se pedepsește cu închisoarea de la unu la 5 ani."*

[66] În acest scop, facem trimitere la orice lucrare de Drept penal – Partea specială sau la articolul nostru, disponibil online, *D. Herinean*, Infracțiunea de hărțuire. Aspecte controversate. Exerciții teoretice și examen de jurisprudență, *cit. supra,* disponibil integral la următorul link.

[67] M. Of., Partea I nr. 446 din 15.05.2024.

fizice unde persoana juridică își desfășoară activitatea profesională. Desigur, activitatea profesională a unor persoane juridice poate fi considerată a fi gestionată în totalitate în mediul online, însă acest lucru nu transformă cyberspațiul într-un sediu al persoanei juridice. La fel ca în cazul de mai sus, în ipoteza accesului neautorizat la activitatea digitală a persoanei juridice discuția se va purta pe tărâmul infracțiunii de acces ilegal la un sistem informatic și/sau, după caz, a celorlalte infracțiuni contra siguranței și integrității sistemelor și datelor informatice (art. 360-365 C.pen.).

3. Viață privată (art. 226 C.pen.)

Când vine vorba de expresia „*viață privată*", aceasta ne duce automat cu gândul la o multitudine de aspecte, de la un drept fundamental al omului, la limitele inerente acestui drept și, desigur, la infracțiunea de violarea vieții private. Singura întrebare la care ne propunem să răspundem în contextul acestei infracțiuni este dacă, din punctul de vedere al legii penale, viața privată se regăsește doar în mediul fizic sau, din contră, aceasta există și în mediul online.

Analizând infracțiunea prevăzută în art. 226 C.pen, răspunsul pare a putea fi privit din două perspective distincte.

Pe de-o parte, dacă analizăm ceea ce am putea numi o *violare directă* a vieții private, pare că aceasta se realizează exclusiv în mediul fizic. Prin *violarea directă* a vieții private ne referim la conduitele prevăzute în art. 226 alin. (1) și (5) C.pen., care se realizează printr-o intervenție directă a autorului în viața privată a victimei, fie „*prin fotografierea, captarea sau înregistrarea de imagini, ascultarea cu mijloace tehnice sau înregistrarea audio a unei persoane aflate într-o locuință sau încăpere ori dependință ținând de aceasta sau a unei convorbiri private*", fie „*plasarea, fără drept, de mijloace tehnice de înregistrare audio sau video*". Așadar, față de aceste modalități de comitere, viața privată a persoanei este protejată exclusiv în mediul fizic, nefiind tipică fapta de a fotografia o persoană în mediul online.

Când vine vorba de conversațiile private din mediul online, trebuie atrasă atenția asupra art. 226 alin. (4)[68] C.pen., care prevede acele cauze justificative speciale în care o conduită descrisă *supra* nu ar constitui infracțiunea. Astfel, de principiu, dacă o conversație (fie ea în mediul online fie în mediul fizic) este înregistrată de una din persoanele participante la ea, atât timp cât justifică un interes legitim, fapta sa nu va constitui infracțiune. *Per a contrario,* în lipsa unui interes legitim, ar putea fi comisă o infracțiune. În acest context, trebuie atrasă atenția și asupra infracțiunii de violare a secretului corespondenței (art. 302 C.pen.), care se comite prin violarea unei corespondențe „***adresate altuia***" (s.n.), astfel încât, în cazul care s-ar divulga corespondența adresată sieși (*i.e. o conversație dintre autor și o altă persoană)*, nu am fi în prezența unei infracțiuni.

Pe de altă parte, dacă analizăm *violarea indirectă* a vieții private (prin *violare indirectă* ne referim la acele situații în care sunt „*divulgarea, difuzarea, prezentarea sau transmiterea,*

[68] *„(4) Nu constituie infracțiune fapta prevăzută la alin. (1) și (2) săvârșită:*
a) de către cel care a participat la întâlnirea cu persoana vătămată în cadrul căreia au fost surprinse sunetele, convorbirile sau imaginile, dacă justifică un interes legitim;
b) dacă persoana vătămată a acționat explicit cu intenția de a fi văzută ori auzită de făptuitor;
c) dacă făptuitorul surprinde săvârșirea unei infracțiunii sau contribuie la dovedirea săvârșirii unei infracțiuni;
d) dacă surprinde fapte de interes public, care au semnificație pentru viața comunității și a căror divulgare prezintă avantaje publice mai mari decât prejudiciul produs persoanei vătămate".

fără drept, a sunetelor, convorbirilor ori a imaginilor" care ating viața privată a unei persoane, conduite care vor fi calificate conform art. 226 alin. (2) și (2^1) C.pen.), aceasta se va face, de cele mai multe ori, în mediul online, fiind cea mai facilă și eficientă manieră de publicare a unor informații ori imagini. În egală măsură, având în vedere că textul nu condiționează ca imaginile/sunetele/convorbirile publicate să fie obținute în maniera prevăzută la art. 226 alin. (1) C.pen., astfel cum rezultă din Decizia RIL 51/2021[69], această *violare indirectă* a vieții private poate fi rezultatul obținerii tot din mediul online a unor imagini/sunete/convorbiri a căror publicare/comunicare apoi devine o activitate infracțională.

Din această perspectivă, trebuie subliniat faptul că atât în cazul art. 226 alin. (2), cât și în cazul art. 226 alin. (2^1) C.pen. nu este necesară publicarea, aceasta fiind doar un element alternativ al infracțiunii, ci este suficientă comunicarea strict față de o altă persoană a respectivelor imagini (atât timp cât nu ne aflăm în ipotezele de la art. 226 alin. (4) C.pen.).

Observăm așadar că protecția vieții private în mediul online se realizează în special prin incriminarea conduitelor de divulgare/publicare/difuzare/comunicare a imaginilor, sunetelor sau convorbirilor care au elemente de viață privată.

Un corolar al normelor analizate este că nu va fi considerată o violare a vieții private niciodată o conduită prin care se aduce la cunoștința publicului informații / imagini / înregistrări care au ieșit din sfera vieții private ca urmare a publicării lor tocmai de către persoana vizată, întrucât se consideră, în mod justificat, că s-a renunțat la confidențialitate odată cu publicarea lor.

Nu în ultimul rând, trebuie menționat că, de multe ori, obținerea unor informații / imagini / înregistrări din cyberspațiu sau mediul online este protejată și de infracțiunile contra siguranței și integrității sistemelor și datelor informatice (art. 360-365 C.pen.).

4. Bun mobil (art. 228, 238 C.pen.)

Discuțiile cu privire la noțiunea de *bun mobil* din cadrul infracțiunii de furt sunt deosebit de complexe, astfel încât nu vom intra într-o analiză amănunțită a noțiunii, ci ne vom limita doar la ceea ce servește scopului prezentului material: *„bunurile mobile"* din cyberspațiu și din mediul online.

Ca repere inițiale, trebuie reamintită autonomia conceptuală a dreptului penal, astfel încât definiția bunurilor mobile din dreptul civil[70] nu este aplicabilă automat în aceste cazuri[71], deși poate fi avută ca reper. În dreptul penal, remarcăm dispozițiile art. 228 alin. (3) C.pen., potrivit cărora *„se consideră bunuri mobile și înscrisurile, energia electrică, precum și orice alt fel de energie care are valoare economică*". Cea mai simplă definiție ce ar putea fi dată noțiunii de *bun mobil* ar porni de la sensul propriu al cuvântului *mobil*, adică cea de bun susceptibil de a fi mișcat, după cum sugerează chiar denumirea în engleză (*movable good),* putând totodată

[69] M. Of., Partea I nr. 1050 din 03.11.2021.

[70] Realizată în art. 539 C.civ. alin. (1) prin excludere, respectiv *„Bunurile pe care legea nu le consideră imobile sunt bunuri mobile*". Alte dispoziții relevante pentru subiectul nostru pot fi identificate în art. 539 alin. (2). C.civ., potrivit cărora *„Sunt bunuri mobile şi undele electromagnetice sau asimilate acestora, precum şi energia de orice fel produse, captate şi transmise, în condiţiile legii, de orice persoană şi puse în serviciul său, indiferent de natura mobiliară sau imobiliară a sursei acestora*".

[71] În același sens al neaplicării automate a regulilor din dreptul civil, a se vedea *V. Cioclei,* Drept penal. Partea specială I. Infracțiuni contra persoanei și infracțiuni contra patrimoniului, Ediția 8, Editura C.H. Beck, București, 2023, p. 267.

defini noțiunea și ca bun susceptibil de apropriere fizică. S-a mai arătat în doctrină că bunul mobil trebuie să fie corporal (să aibă o existență materială[72]) și că trebuie să aibă o minimă valoare economică[73], putând fi animat sau neanimat, fungibil sau nefungibil[74].

În acest sens, după cum am mai arătat *supra*, trebuie să fim foarte precauți la distincția dintre bunuri mobile și date informatice. Diferențierea este foarte importantă, întrucât *bunurile* vor fi obiectul material al infracțiunilor contra patrimoniului, în timp ce datele informatice vor fi, de cele mai multe ori, obiectul material în cazul infracțiunilor contra siguranței și integrității sistemelor și datelor informatice.

În literatura de specialitate s-a conturat și ideea de *dematerializare* a obiectului material[75], fiind tratată inclusiv infracțiunea de furt și obiectul său material. În acest context. definiția *bunului mobil* arătată mai sus a fost criticată de autorul citat ca fiind depășită din perspectiva evoluției tehnologice[76]. Propunerea de redefinire a bunului mobil a fost în sensul utilizării criteriului capacității unui bun de a fi apropriat de către o persoană, accentul fiind pus pe unicitatea posesiei mai degrabă decât pe tangibilitatea bunului[77]. Prin urmare, mergând pe această opinie, se pare că am putea discuta și despre bunuri mobile care au o corporalitate aparentă doar în cyberspațiu, deși ele sunt create și stocate pe baza unor date informatice.

Interpretarea evolutivă a textelor clasice a creat însă în alte state jurisprudență în care s-a ajuns la considerarea comiterii unei infracțiuni de furt din mediul virtual. Spre exemplu, în cauza *Runescape*, o instanță olandeză a constatat că a fost vorba de un furt de bunuri atunci când inculpații, după ce au constrâns victima să se autentifice în contul asociat jocului *Runescape*, au accesat contul acesteia și au transferat către un cont pe care îl controlau bunuri virtuale (o amuletă și o mască), instanța considerând că bunurile virtuale respective erau unice (în lumea virtuală – doar o persoană putea să le dețină la un anumit moment) și aveau o valoare economică[78]. Într-o altă speță din jurisprudența olandeză, prezentată de același autor[79], a fost vorba de piese de mobilier care au fost transferate din contul victimei din jocul *Habbo Hotel* de către inculcați către un cont pe care îl controlau, instanța reținând un concurs între infracțiunea de acces ilegal la un sistem informatic și furt calificat[80].

Din perspectiva noastră, atât timp cât energia electrică este considerată *de lege lata* un bun mobil (și orice alt fel de energie care are valoare economică), nu vedem o rațiune pentru

---

[72] *T. Manea*, *C.-N. Constantinescu-Mărunțel, H.-Ș. Tiugan,* Drept penal. Partea specială, Infracțiuni contra persoanei. Infracțiuni contra patrimoniului. Ediția a 2-a, Editura Hamangiu, București, 2024, p. 296.

[73] *S. Bogdan, D.A. Șerban*, Drept penal. Partea specială. Infracțiuni contra patrimoniului, contra autorității, de corupție, de serviciu, de fals și contra ordinii și liniștii publice, Editura Universul Juridic, București, 2020, pp. 19-25; *M. Udroiu*, Sinteze de Drept penal. Partea specială, Volumul I, Ediția 3, Ed. București, 2022, p. 417.

[74] *M. Udroiu*, op. cit., pp. 417-418.

[75] *G. Zlati,* Dematerializarea obiectului material al infracțiunii în contextul evoluției tehnologice și consecințele acesteia, în Dreptul, nr. 9/2013.

[76] *Idem,* p. 166. Trebuie subliniat că articolul citat a apărut în anul 2013!

[77] *Idem,* p. 167.

[78] *G. Zlati,* Dematerializarea obiectului material al infracțiunii în contextul evoluției tehnologice și consecințele acesteia, op. cit., p. 171.

[79] *Ibidem.*

[80] Un alt autor propune ca atunci când discutăm de bunuri virtuale create de utilizator, însușirea acestora îmn mediul virtual de arte persoane să fie sancționată potrivit normelor de incriminare care au ca obiect juridic dreptul de proprietate intelectuală. A se vedea *T. Gřivna,* Virtual Crimes, publicat în Masaryk University Journal of Law and Technology nr. 1/2008, p. 102, consultat pe ceeol.com.

care să excludem *de plano* posibilitatea adoptării unor soluții similare și în România[81]. Când am discuta de reprezentări de date informatice din mediul virtual care ar putea fi, la fel ca în speța prezentată mai sus, pe de-o parte, caracterizate de unicitate și de o minimă valoare economică și, pe de altă parte, de o corporalitate virtuală, astfel încât acestea să poată fi calificate drept bunuri virtuale mai degrabă decât drept simple date informatice.

Mai recent, discuțiile privind criptomonedele și NFT-urile sunt în mod evident cele mai importante. Criptoactivele pot fi reprezentarea digitală a unui bun mobil sau a oricărui drept, reprezentare care poate fi transferată și stocată în blockchain , în literatura de specialitate opinându-se în sensul că nu va putea fi niciodată considerată ca fiind un transfer de date informatice o tranzacție având ca obiect o monedă virtuală sau un alt criptoactiv, având în vedere că tranzacția aceasta nu are ca urmare o copiere sau relocare a unor date informatice, ceea ce exclude posibilitatea aplicării art. 364 C.pen., autorul citat considerând că mai degrabă am discuta de o introducere/modificare de date atunci când ar fi vorba de o infracțiune de fraudă informatică.

Spre exemplu, atunci când discutăm despre portofele digitale, sustragerea unui portofel digital – *i.e.* a stick-ului care permite accesul – nu echivalează cu sustragerea monedelor virtuale, acestea nefiind stocate în mod fizic în portofelul digital, cel din urmă fiind doar o cheie de acces[82]. Pe de altă parte, orice operațiune cu criptomonede – prin care acestea sunt transferate de exemplu – va face obiectul altor infracțiuni, fraudă informatică (art. 249 C.pen.) sau efectuarea de operațiuni financiare în mod fraudulos (250 C.pen.), acestea fiind *monede virtuale,* iar nu *bunuri mobile*. În egală, măsură, în doctrină se arată că sustragerea *seed phrase*-ului sau a datelor de identificare ale unui card, chiar dacă sunt notate pe o coală de hârtie, nu va putea fi încadrată ca o infracțiune de furt, lipsind minima valoare economică a acestor informații[83], o astfel de sustragere putând fi însă acte de pregătire în ceea ce privește comiterea infracțiunii reglementate în art. 250 C.pen. sau de art. 249 C.pen.

În ceea ce privește monedele virtuale, în literatura specialitate se menționează că nu pot fi calificate ca *bunuri,* neputând face astfel obiectul infracțiunii prevăzute în art. 243 – însușirea bunului găsit ori ajuns din eroare la făptuitor[84]. Deși înțelegem rațiunea tehnică pentru care autorul propune această soluție, aceasta ni se pare totuși injustă și credem că, în lipsa unei intervenții legislative, o interpretare evolutivă a noțiunii de *bun mobil,* cel puțin în contextul acestei infracțiuni, ar fi de dorit, dat fiind că transferul din eroare a unui bitcoin ar produce un prejudiciu mult mai mare victimei decât un bun găsit pe stradă. Desigur, o astfel de abordare nu este la adăpost de critici, putând fi acuzați de o depășire a limitelor interpretării evolutive și teleologice și de apelare la o analogie în defavoarea inculpatului.

Cu privire la NFT-uri, în doctrină s-a arătat că situația transferului neautorizat al unui NFT s-ar apropia din punct de vedere conceptual de o acțiune de a sustrage un bun mobil[85], în cazul acestora părând a se acorda o mai mare importanță aparenței virtuale decât datelor informatice pe baza cărora acestea funcționează, opinie cu care tindem să fim de acord.

În practica judiciară (fără să existe însă date statistice în acest sens la acest moment) am observat că majoritatea infracțiunilor în ceea ce privește criptomonedele sunt de înșelăciune,

[81] În același sens, considerându-se că nu se realizează o analogie în defavoarea inculpatului, a se vedea *Idem,* p. 172.
[82] *Idem*, p. 44 și urm.
[83] *Idem,* p. 45.
[84] *G. Zlati,* Tehnologia blockchain, monedele virtuale și dreptul penal, op. cit., p. 62-63.
[85] *Idem*, p. 59.

paguba fiind produsă persoanelor vătămate prin inducerea acestora în eroare să transfere voluntar criptomonedele făptuitorilor sub diferite pretexte, iar infracțiunile de înșelăciune nu au un specific în mediul online, altfel decât prin mijloacele de comunicare la distanță prin care sunt comise.

Tot în acest context, dorim să precizăm că în cazul noțiunii de *terminal de comunicații* utilizată în art. 230 C.pen., în cadrul formei asimilate a infracțiunii de furt de folosință, textul de incriminare pare să aibă în vedere doar interacțiunea fizică cu un astfel de terminal, iar nu utilizarea lui *remote,* prin obținerea controlului asupra sa prin mijloace de la distanță, când ar fi, de altfel, incidente alte infracțiuni, din nou cele contra siguranței și integrității sistemelor și datelor informatice (art. 360-365 C.pen.), în acele cazuri nefiind afectată posesia fizică asupra bunului (care este presupusă de specificul infracțiunii de furt). O altă mențiune ar fi că noțiunea de vehicul din art. 230 alin. (1) C.pen. nu poate fi interpretată că ar face referire inclusiv la un vehicul virtual *de lege lata*.

CONCLUZII

Cu titlu de succinte concluzii, observăm că din punct de vedere al termenilor și expresiilor definite, fie că se exercită autonomia conceptuală a dreptului penal sau nu în cazul lor, cadrul juridic stabilit de Codul penal pare a fi pregătit și adaptat, din punct de vedere terminologic, la un nivel satisfăcător analizei și luptei împotriva criminalității în cyberspațiu în actualul moment al dezvoltării tehnologice, chiar dacă, din perspectiva instrumentelor de plată fără numerar și mai ales în privința criptoactivelor, legislația noastră nu pare a fi la un nivel *state of the art*.