ACCESUL FĂRĂ DREPT LA UN SISTEM INFORMATIC
Art.42 alin.1, 2, 3 din Legea nr.161/2003

Procuror
Justina Condoiu

Accesul fără drept la un sistem informatic se realizează cu ocazia montării la ATM a dispozitivelor de citire a benzii magnetice a cardului autentic şi a codului PIN aferent acestuia sau **accesul fără drept la un sistem informatic, în scopul obţinerii de date informatice, prin încălcarea măsurilor de securitate, se produce abia prin folosirea la bancomat a cardului falsificat ori chiar a celui autentic, fără acordul titularului său.**

Examenul jurisprudenţei actuale evidenţiază mai multe orientări cu privire la aceste aspecte şi, prin urmare, caracterul neunitar al practicii judiciare, astfel :

***I. 1. Într-o primă opinie**, s-a apreciat că montarea dispozitivelor de citire a benzii magnetice a cardului autentic, a video-camerei sau a falsei tastaturi nu constituie acces fără drept la un sistem informatic, infracţiune prevăzută de art.42 alin.1 din Legea nr.161/2003.*

Instanţele au încadrat această faptă în dispoziţiile art.25 din Legea 365/2002, reţinându-se că inculpaţii „au deţinut echipamente electronice apte să citească şi să memoreze date din cărţile de credit, în scopul obţinerii acelor date care permit retragerea sumelor de bani din cărţile de credit".

Alte instanţe au apreciat că, „fapta inculpatului de a ataşa la un ATM un dispozitiv format dintr-un telefon mobil prevăzut cu cameră video şi card de memorie şi un suport menit a susţine şi disimula telefonul în plafonul bancomatului, în scopul de a înregistra codul PIN tastat de utilizatorii acestuia, întruneşte elementele constitutive ale infracţiunii prevăzute de art.46 alin. 2 din Legea nr.161/2003, adică deţinere fără drept a unui dispozitiv conceput sau adaptat în scopul săvârşirii uneia dintre infracţiunile prevăzute de art.42-45 din aceeaşi lege".

Cele mai multe instanţe însă, au menţinut încadrarea juridică din actul de sesizare, fără a pune în discuţie şi fără a se pronunţa în mod expres asupra problemei de drept supusă prezentului recurs.

Înalta Curte de Casaţie şi Justiţie a împărtăşit această primă orientare prin deciziile nr. 4009 din 4 decembrie 2008, nr. 251 din 26 ianuarie 201, nr. 2416 din 18 iunie 2010, nr. 3425 din 5 octombrie 2011 şi nr. 3354 din 3 octombrie 2011.

***2. a) Într-o a doua opinie**, s-a reţinut, dimpotrivă, că, prin montarea la bancomat a dispozitivelor de citire a informaţiilor înregistrate pe banda magnetică a cardului şi de captare a codului PIN tastat cu ocazia folosirii cardului de către titularul său, se realizează un acces fără drept la sistemul informatic, prin încălcarea măsurilor de securitate.*

În argumentarea acestei opinii, instanţele au apreciat că „ATM-ul este un mijloc de colectare, prelucrare şi transmitere a unor date informatice, reprezentate de numărul de cont al titularului, care este stocat pe nivelul 2 al benzii magnetice. Pe de altă parte, prin montarea skimmer-lui în fanta bancomatului, prin care se introduce cardul şi se realizează citirea benzii magnetice a fiecărui card în parte, stocându-se informaţia astfel obţinută, au fost încălcate măsurile de securitate care aveau drept scop asigurarea secretului numărului de cont şi a operaţiunilor efectuate şi apărarea împotriva folosirii de către o altă persoană a acestor carduri în vederea fraudării. În consecinţă, inculpaţii au accesat fără drept un sistem informatic încălcând astfel măsurile de securitate."

Cu aceeaşi motivare, unele instanţe au reţinut ca incidente, pentru această situaţie de fapt, dispoziţiile art.44 alin. 2, 3 şi art. 46 alin. 2 alături de cele ale art.42 alin. 2, 3 din Legea nr.161/2003.

În argumentarea acestei opinii, instanţele au apreciat că atât video-camera cât şi skimmer-ul au fost deţinute în scopul cerut de art.46 alin.2 din Legea nr.161/2003.

Înalta Curte de Casație și Justiție a împărtășit această orientare prin deciziile nr. 376 din 2 februarie 2010, nr. 5288 din 15 septembrie 2006 și nr. 2094 din 27 mai 2010.

b) La același punct de vedere au aderat și instanțele, inclusiv Înalta Curte de Casație și Justiție prin decizia nr. 2991 din 1 martie 2010, care, deși nu au reținut aplicarea art.42 alin.1 din Legea nr.161/2003, au considerat că acesta ar fi fost aplicabil „în situația în care ar fi fost montate dispozitive de citire a benzilor magnetice la ATM".

II. 1. Cât privește accesarea fără drept a unui sistem informatic, prin încălcarea măsurilor de securitate cu prilejul folosirii la ATM a cardului falsificat, *oricare ar fi fost modul în care s-au obținut datele informatice cu care a fost acesta inscripționat, unele instanțe au concluzionat în sensul că fapta întrunește elementele constitutive ale infracțiunii prevăzute de art.42 alin.1 și 3 din Legea nr.161/2003.*

Acest punct de vedere a fost argumentat pe dispozițiile art.35 din Legea nr.161/2003, ale cărui condiții sunt îndeplinite de bancomat, privit nu doar din punct de vedere fizic, ci și ca sistem informatic interconectat la rețeaua de bancomate a băncii din care face parte, fapt care permite un schimb de date informatice ce se realizează de îndată ce cardul falsificat prin inscripționarea datelor aflate pe cardul autentic este „recunoscut" de bancomatul la care este folosit.

Instanțele care au aderat la această opinie au încadrat fapta de folosire a cardului falsificat pentru retragere de numerar de la ATM-uri în dispozițiile art.42 alin.1 și 3 din Legea nr.161/2003 alături de cele ale art.24 alin.2 din Legea nr.365/2002, singur sau împreună cu art.27 alin.1 din aceeași lege.

Înalta Curte de Casație și Justiție a împărtășit această orientare prin deciziile nr. 1989 din 13 mai 2011, nr. 3354 din 3 octombrie 2011, nr. 2094 din 27 mai 2010, nr. 3503 din 7 octombrie 2010, nr. 1457 din 16 aprilie 2010 și nr. 3408 din 5 octombrie 2011.

2. a). Dimpotrivă, alte instanțe au apreciat că folosirea cardului falsificat pentru retragerea de numerar de la ATM nu constituie acces fără drept și prin încălcarea măsurilor de securitate la un sistem informatic.

Instanțele care au aderat la această opinie, au încadrat faptele inculpaților în sarcina cărora au reținut inscripționarea mai multor carduri blanc cu date informatice preluate de pe cardurile autentice și retragerea a diferite sume de bani din bancomate, în dispozițiile art.24 alin. 1 și 2, art.25 alin. 1 și art.27 alin. 1 din Legea nr. 365/2002.

Înalta Curte de Casație și Justiție a împărtășit această orientare prin deciziile nr. 251 din 26 ianuarie 2011, nr. 1090 din 25 martie 2008, nr. 2834 din 17 septembrie 2008, nr. 1350 din 9 aprilie 2010, nr. 2223 din 12 iunie 2009, nr. 2991 din 1 martie 2010, nr. 3942 din 26 noiembrie 2009, nr. 666 din 22 februarie 2011, nr. 3889 din 23 noiembrie 2009, nr. 4044 din 15 noiembrie 2011, nr. 591 din 16 februarie 2011 și nr. 1681 din 14 mai 2008.

b). În ipoteza folosirii cardului autentic, fără consimțământul titularului său, pentru retragerea de numerar de la A.T.M. fapta a fost încadrată, exclusiv, în dispozițiile art.27 alin. 1 din Legea nr. 365/2002.

*

* *

I. Considerăm că au aplicat corect legea instanțele care au apreciat că prin montarea la ATM a dispozitivului de citire a benzii magnetice a cardului și a video-camerei ori a dispozitivului modificat de tip tastatură, nu se realizează accesul fără drept la un sistem informatic, infracțiune prevăzută de art.42 alin. 1 din Legea nr.161/2003.

II. Pe de altă parte, folosirea la ATM a cardului inscripționat cu datele culese de pe cardul autentic, oricare ar fi fost modul de obținere a acestora, ori utilizarea cardului autentic, fără acordul titularului său, reprezintă acces fără drept la un sistem informatic, în scopul obținerii de date informatice, prin încălcarea măsurilor de securitate, faptă incriminată de art.42 alin. 1, 2 și 3 din Legea nr.161/2003.

Premisele legale ale practicii neunitare ce fac obiectul prezentului recurs în interesul legii sunt dispozițiile art.42 din Legea nr.161/2003 care incriminează fapta de acces ilegal la un sistem informatic într-o variantă tip, în alineatul 1 și în două variante agravate, în alineatele 2 și 3: accesul, fără drept, la un sistem informatic, săvârșit în scopul obținerii de date informatice, respectiv accesul la un sistem informatic, prin încălcarea măsurilor de securitate.

În privința conținutului constitutiv al infracțiunii, în doctrină[1] s-a arătat că elementul material al laturii obiective se realizează prin accesul, fără drept, într-un sistem informatic: stație de lucru, server ori rețea informatică. Accesul, în sensul legii, desemnează intrarea în tot sau numai într-o parte a sistemului informatic, metoda de comunicare neprezentând importanță. Accesul fără drept la un sistem informatic presupune o interacțiune a făptuitorului cu tehnica de calcul vizată prin intermediul echipamentelor sau diverselor componente ale sistemului (surse de alimentare, butoane de pornire, tastatură, mouse, joystick). Manipularea acestor dispozitive se transformă în solicitări către UCP (unitatea centrală de prelucrare) a sistemului, care va procesa date ori va rula programe de aplicații în beneficiul intrusului.

Din punct de vedere fizic, urmarea imediată este modificarea pe care acțiunea făptuitorului a produs-o în lumea externă[2]. Aceasta constă în trecerea într-o stare de nesiguranță a sistemului informatic şi/sau a resurselor sale. Dacă scopul accesului neautorizat a fost obținerea de date informatice, starea de nesiguranță a sistemului este dublată de starea de nesiguranță a datelor informatice stocate sau prelucrate de acesta. Încălcarea măsurilor de securitate va determina o transformare efectivă adusă obiectului material al infracțiunii[3], adică entităților materiale care compun sistemele informatice (calculatoare, rețele de calculatoare, elemente hardware – echipamente periferice, cabluri, plăci, servere etc. şi software – programe, aplicații, baze de date etc.) sau datelor informatice spre care se îndreaptă atenția făptuitorului. Sub aspectul consecințelor pe care acțiunea incriminată le are asupra valorii sociale ocrotite, urmarea este tocmai starea de pericol, de amenințare, la adresa „domiciliului informatic".

Cât priveşte legătura de cauzalitate între activitatea făptuitorului şi urmarea produsă, aceasta rezultă *ex re*, adică din materialitatea faptei, în cazul accesului neautorizat în formă simplă, respectiv trebuie demonstrată forțarea măsurilor de securitate (parole, coduri de acces etc.), în cazul formelor agravate.

Cardul emis de o instituție de credit reprezintă un instrument de plată electronică, respectiv un suport de informație standardizat, securizat şi individualizat, care permite deținătorului său să folosească disponibilitățile băneşti proprii dintr-un cont deschis pe numele lui la emitentul cardului şi/sau să utilizeze o linie de credit (în limita unui plafon stabilit în prealabil) deschisă de emitent în

---

[1] Maxim Dobrinoiu – Infracțiuni în domeniul informatic, Editura C.H.Beck, Bucureşti, 2006, pag.149

[2] Ibidem, pag.159.

[3] Ibidem, pag.148

favoarea deținătorului cardului, în vederea efectuării uneia sau a mai multora dintre următoarele operațiuni[4] :

- retragerea sau depunerea de numerar de la terminale precum ATM-le, ghișeele emitentului sau ale unei alte instituții obligată prin contract să accepte instrumentul de plată electronică;

- plata bunurilor achiziționate ori a serviciilor prestate de comercianții acceptanți sau de emitenți, precum și plata obligațiilor către autoritățile administrației publice (impozite, taxe, amenzi etc.);

- transferurile de fonduri.

Elementele de identificare dispuse pe spatele cardului bancar (cele care prezintă interes în prezenta cauză) sunt reprezentate de[5] :

- banda magnetică care conține date codificate stocate electronic referitoare la card (titularul cardului, numărul de cont, data expirării etc.) poziționate pe trei sau mai multe piste;

- zona pentru semnătură;

- CVV-ul (Card Verification Value) număr format din 3 cifre codat pe banda magnetică a cardurilor valide. Când un card este introdus într-un terminal, CVV se transmite băncii emitente odată cu celelalte informații despre cont, informația fiind apoi procesată împreună cu codul confidențial al emitentului pentru a verifica dacă valoarea transmisă se potrivește cu cea din înregistrare[6];

- codul CVV2 (pentru cardul VISA) și codul CVC2 (pentru cardul MASTERCARD) reprezintă un număr format din 3 cifre imprimate pe zona pentru semnătură și înclinate spre stânga. Pe aceeași zonă este imprimat tot înclinat invers și numărul de cont duplicat, care asigură corespondența cu numărul de cont care apare pa fața cardului, putând fi format din întreg acest număr sau din ultimele sale patru cifre.

I. **Skimming-ul** reprezintă activitatea de copiere a datelor valide de pe banda magnetică a unui card autentic prin intermediul unui dispozitiv de citire a cardurilor, fără cunoștința posesorului legitim, cu intenția de a fi folosite în scopuri frauduloase. Dispozitivele de skimming pot fi „de mână" - hand skimmers, ipoteză în care datele de pe banda magnetică sunt copiate în momentul când cardul este înmânat de către titular unei alte persoane (de regulă, un comerciant în timpul

---

[4] Art.2 pct.1 din Regulamentul Băncii Naționale a României nr.6 din 11 octombrie 2006 privind emiterea și utilizarea instrumentelor de plată electronică și relațiile dintre participanții la tranzacțiile cu aceste instrumente.

[5] Adrian Cristian Moise, Metodologia investigării criminalistice a infracțiunilor informatice, Universul Juridic, București, 2011, pag.289).

[6] Ioan Dascălu, Ion Tomescu, Diță Bondarici, Frauda în domeniul cardurilor, Editura Sfinx 2000, Târgoviște 2003., pag.31.

efectuării unei tranzacții) sau montate la ATM-uri sau POS-uri - ATM/POS skimmers, datele de pe banda magnetică fiind înregistrate în momentul când titularul cardului introduce cardul în bancomat, pentru a efectua o tranzacție. În acest din urmă caz skimmer-ul este poziționat pe latura externă a fantei de introducere a cardului și poate avea forma fantei pentru card, fiind lipit chiar deasupra acesteia, astfel încât **datele de pe banda magnetică sunt citite și captate înainte ca respectivul card să intre în fanta bancomatului și să se realizeze transmisia de date informatice între card și ATM.**

Dispozitivele de skimming sunt însoțite de mini video-camere sau de dispozitive modificate de tip tastatură (keypads) care înregistrează codul PIN aferent cardului, în momentul tastării acestuia.

Din cele anterior arătate rezultă că **obținerea datelor de pe banda magnetică a cadrului autentic se realizează în exteriorul bancomatului și fără ca dispozitivele menționate să intre în vreun fel de conexiune cu sistemul informatic al băncii**. În egală măsură, **captarea codului PIN se realizează în exteriorul ATM-ului și nu presupune acces la sistemul informatic**.

Dispozițiile art.42 din Legea nr.161/2003 incriminează accesul fără drept **la un sistem informatic**. Neîndoielnic că **bancomatul, folosit conform destinației sale, este un terminal în cadrul unui sistem informatic** din care mai fac parte toate celelalte terminale din rețeaua aceleiași bănci, serverul acesteia etc. Bancomatul **este folosit conform destinației sale atunci când, prin intermediul său, se face retragerea de numerar, plata furnizorilor de utilități, transferurile de fonduri, interogarea de sold**. În toate aceste situații **bancomatul condiționează accesul la baza de date a băncii**. Dacă este folosit însă ca **simplă entitate materială, suport fizic pentru dispozitivele prin care se realizează skimmingul, el nu se conectează la baza de date a băncii, neîndeplinindu-și rolul de parte a unui sistem informatic.**

De altfel, astfel cum arătam anterior, citirea benzii magnetice a cardului autentic nu este condiționată de atașarea skimmer-lui la bancomat, ea putându-se face și cu un dispozitiv de citire manual, neîndoienic lipsit de orice fel de conexiune cu sistemul bancar. Devine, astfel, evident că operațiunile prin care sunt citite datele de pe banda magnetică a cardului concomitent cu captarea codului PIN aferent lui, reprezintă doar acte pregătitoare ale infracțiunii de acces fără drept la un sistem informatic: cum citirea datelor de pe banda magnetică a cardului nu este condiționată de atașarea dispozitivului electronic de citire la bancomat, aceeași activitate de captare a datelor de pe banda magnetică ar primi consecințe juridice diferite datorită unei împrejurări extranee vreunei norme de incriminare – atașarea sau nu a skimmer-lui la bancomat.

Aşadar, operaţiunea de citire a datelor de pe banda magnetică a cardului, prin ataşarea skimmer-lui la bancomat, nu interacţionează în niciun fel cu soft-ul bancomatului, nu se realizează nici o solicitare către unitatea centrală de prelucrare a sistemului, care să proceseze date ori să ruleze programe de aplicaţii în beneficiul făptuitorului, astfel că, **infracţiunea de acces fără drept la sistemul informatic,** în ipoteza supusă prezentei analize, **este lipsită de însuşi elementul său material.**

II. Pentru aceleaşi argumente, privite *per a contrario*, în cazul folosirii la ATM a cardului falsificat sau a celui real, fără consimţământul titularului său, se realizează un acces fără drept la sistemul informatic. De această dată bancomatul este folosit conform destinaţiei sale: introducerea cardului şi tastarea codului PIN (prin aceasta din urmă operaţiune înlăturându-se măsura de securitate reprezentată de codul de acces), în posesia cărora făptuitorul se află în mod nelegal, determinând „recunoaşterea" de către bancomat a cardului falsificat ca fiind un card valid şi permiţând astfel un schimb de informaţii între posesorul cardului şi mediul de stocare al datelor privitoare la contul bancar, ataşat cardului „recunoscut". **Chiar dacă activitatea infracţională s-ar opri aici, nefiind solicitată nicio operaţiune financiară, infracţiunea de acces fără drept la un sistem informatic este consumată.**

Urmare operaţiunilor anterior arătate s-a realizat o interacţiune a făptuitorului cu tehnica de calcul vizată, prin intermediul componentelor sistemului (tastatura), manipularea acesteia transformându-se în solicitări către unitatea centrală de prelucrare a sistemului, care îi vor permite posesorului nelegitim al cardului accesul către date informatice din sistemul bancar. Prin aceasta, datele informatice stocate au devenit vulnerabile, integritatea lor fiind ameninţată. Cum legătura de cauzalitate dintre acţiunea făptuitorului şi urmarea produsă datelor informatice rezultă din însăşi materialitatea faptei, latura obiectivă a infracţiunii de acces fără drept la un sistem informatic este realizată.

Cât priveşte latura subiectivă, fapta este săvârşită cu intenţie.

În concluzie, prin folosirea la ATM a cardului falsificat sau a celui real, fără consimţământul titularului său, sunt întrunite elementele constitutive ale infracţiunii de acces fără drept la un sistem informatic. Folosit conform destinaţiei sale, bancomatul face parte din sistemul informatic bancar, datele transmise şi receptate de acest dispozitiv fiind protejate prin măsuri de securitate încorporate în sistemul de citire a cardurilor şi în codul PIN.

*

* *

Potrivit art.44 alin. 2, 3 din Legea nr.161/2003 constituie infracțiune transferul neautorizat de date dintr-un sistem informatic, respectiv dintr-un mijloc de stocare a datelor informatice, iar prin art.46 alin. 2 din acelaşi act normativ este incriminată **fapta de deținere, fără drept, a unui dispozitiv**, program informatic, parolă, **cod de acces sau dată informatică**, dintre cele care permit accesul total sau parțial la un sistem informatic, în scopul săvârşirii uneia dintre infracțiunile prevăzute la art.42-45. Skimmer-ul, video-camera şi falsa tastatură de bancomat sunt dispozitive deținute în scopul săvârşirii unui acces, fără drept la sistemul informatic, iar datele informatice şi codul de acces **obținute prin folosirea acestor dispozitive** permit accesul total sau parțial la un sistem informatic, putând fi utilizate fie pentru inscripționarea ulterioară a unor carduri clonate, fie pentru plata unor tranzacții on-line. Textele legale menționate devin în egală măsură incidente şi în cazul folosirii unui skimmer ataşat la bancomat, dar şi în cazul obținerii datelor de pe banda magnetică a cardului cu ajutorul unui hand-skimmer.

Pe de altă parte, este de observat că Legea nr.161/2003 cuprinde infracțiuni îndreptate contra confidențialității şi integrității datelor şi sistemelor informatice, în timp ce Legea nr. 365/2002 privind comerțul electronic prevede infracțiuni îndreptate împotriva securității şi integrității instrumentelor de plată electronice. Spre deosebire de primele infracțiuni, **cele din urmă sunt îndreptate efectiv spre integritatea fizică a instrumentului de plată care este clonat sau falsificat**.

Astfel, art.24 din Legea nr. 365/2002 incriminează, în alin. 1, falsificarea unui instrument de plată electronică, iar, în alin. 2, punerea în circulație sau deținerea în vederea punerii în circulație a unui astfel de instrument falsificat. Art.27 alin. 1 din aceeaşi lege sancționează efectuarea de operațiuni financiare prin utilizarea unui instrument de plată, fără consimțământul titularului său.

De altfel, art.25 din Legea nr. 365/2002 (reținut greşit de unele instanțe în cazul montării la ATM a dispozitivelor de citire a benzii magnetice a cardului autentic şi a codului PIN) incriminează fabricarea ori deținerea de echipamente, inclusiv hardware sau software, cu scopul de a servi la **falsificarea instrumentelor de plată electronică**. Sunt avute în vedere dispozitivele prin care se inscripționează cardurile (de tipul MSR-lui, spre pildă) cu datele culese prin skimmer. Scopul acestei infracțiuni este producerea unui alt card, cu existență fizică de sine-stătătoare, identic cu cel autentic, care să poată fi folosit întocmai ca acesta. Scopul skimming-lui este obținerea de date informatice, desigur lipsite de

existență materială, care pot fi ulterior folosite pentru inscripționarea unor carduri clonate, dar şi pentru plata on-line. În această din urmă situație nu există un card falsificat în materialitatea lui, ci datele informatice obținute în modalitatea anterior enunțată sunt folosite pentru accesul fără drept la sistemul informatic bancar. Pentru acest motiv nu dispozițiile art.25 din Legea nr. 365/2002, ci cele ale art. 46 alin. 2 din Legea nr.161/2003 sunt incidente în cazul montării la ATM a dispozitivelor de citire a benzii magnetice a cardului autentic şi a codului PIN aferent acestuia. Cât priveşte infracțiunea prevăzută de art.44 alin. 2, 3 din Legea nr.161/2003, reținută de unele instanțe în concurs cu cele prevăzute de art.46 alin. 2 şi art.42 alin. 2, 3 din aceeaşi lege, este de observat că prin copierea datelor de pe banda magnetică a cardului autentic nu se realizează un **transfer** de date informatice, acestea nedispărând din mediul de stocare, nepărăsind, prin copiere, banda magnetică de pe care au fost captate.

În concluzie, din analiza textelor legale anterior amintite, rezultă că, în vederea pregătirii săvârşirii infracțiunilor din Legea comerțului electronic, se pot săvârşi infracțiuni îndreptate împotriva securității datelor sau sistemelor informatice, cum este şi aceea de acces ilegal într-un sistem informatic. Aşadar, accesul ilegal în sistemul informatic se face, de regulă, în scopul săvârşirii uneia sau mai multora dintre infracțiunile prevăzute de Legea comerțului electronic, situație care justifică reținerea unui concurs de conexitate etiologică în care accesul ilegal reprezintă mijlocul prin care efectuarea de operațiuni financiare în mod fraudulos, adică scopul, se realizează.

Pentru argumentele arătate apreciem că:

I. **Încadrarea juridică** ce se impune a fi dată faptei de a monta la bancomat dispozitive de citire a benzii magnetice a cardului, mini-videocamere sau dispozitive tip tastatură **este aceea prevăzută de art.46 alin. 2 din Legea nr.161/2003.**

II. Cât priveşte **folosirea la bancomat**, pentru retrageri de numerar sau orice alte operațiuni financiare, **a unui card falsificat sau a unuia real, fără consimțământul titularului său,** fapta întruneşte elementele constitutive ale infracțiunii prevăzute de art.42 alin.1,2 şi 3 din Legea nr.161/2003, săvârşită în concurs ideal cu cea prevăzută art.24 alin.2 din Legea nr.365/2002 sau art.27 alin.1 din aceeaşi lege, după caz.