



MONITORUL OFICIAL

AL

ROMÂNIEI

Anul 181 (XXV) — Nr. 760

PARTEA I
LEGI, DECRETE, HOTĂRĂRI ȘI ALTE ACTE

Vineri, 6 decembrie 2013

SUMAR

<u>Nr.</u>	<u>Pagina</u>
ACTE ALE ORGANELOR DE SPECIALITATE ALE ADMINISTRAȚIEI PUBLICE CENTRALE	
170. — Ordin al ministrului afacerilor interne privind organizarea și desfășurarea activității de identificare, desemnare și protecție a infrastructurilor critice în Ministerul Afacerilor Interne.....	2–5
1.348. — Ordin al ministrului agriculturii și dezvoltării rurale pentru modificarea și completarea anexei la Ordinul ministrului agriculturii, pădurilor și dezvoltării rurale nr. 392/2009 privind aprobarea listei cu cheltuieli eligibile pentru proiectele finanțate în cadrul Programului Operațional pentru Pescuit 2007–2013	6
1.446. — Ordin al ministrului sănătății pentru modificarea Ordinului ministrului sănătății nr. 1.091/2013 privind stabilirea cuantumului taxei și modalitatea de plată a acesteia pentru participarea la examenul de grad principal pentru asistenții medicali generaliști, moașe și asistenți medicali — sesiunea 2013	7
ACTE ALE ÎNALTEI CURȚI DE CASAȚIE ȘI JUSTIȚIE	
Decizia nr. 15 din 14 octombrie 2013	8–32

ACTE ALE ORGANELOR DE SPECIALITATE ALE ADMINISTRAȚIEI PUBLICE CENTRALE

MINISTERUL AFACERILOR INTERNE

ORDIN

privind organizarea și desfășurarea activității de identificare, desemnare și protecție a infrastructurilor critice în Ministerul Afacerilor Interne

Având în vedere prevederile Hotărârii Guvernului nr. 1.110/2010 privind componența, atribuțiile și modul de organizare ale Grupului de lucru interinstituțional pentru protecția infrastructurilor critice, cu modificările ulterioare, ale Hotărârii Guvernului nr. 1.154/2011 pentru aprobarea pragurilor critice aferente criteriilor intersectoriale ce stau la baza identificării potențialelor infrastructuri critice naționale și privind aprobarea Metodologiei pentru aplicarea pragurilor critice aferente criteriilor intersectoriale și stabilirea nivelului de criticitate, ale Hotărârii Guvernului nr. 718/2011 pentru aprobarea Strategiei naționale privind protecția infrastructurilor critice, ale Hotărârii Guvernului nr. 1.198/2012 privind desemnarea infrastructurilor critice naționale, ale Deciziei prim-ministrului nr. 43/2012 privind aprobarea Planului de acțiune pentru implementarea, monitorizarea și evaluarea obiectivelor Strategiei naționale privind protecția infrastructurilor critice și ale Deciziei prim-ministrului nr. 166/2013 privind aprobarea Normelor metodologice pentru realizarea/echivalarea/revizuirea planurilor de securitate ale proprietarilor/ operatorilor/ administratorilor de infrastructură critică națională/europeană, a structurii-cadru a planului de securitate al proprietarului/operatorului/administratorului deținător de infrastructură critică națională/europeană și a atribuțiilor ofițerului de legătură pentru securitate din cadrul compartimentului specializat desemnat la nivelul autorităților publice responsabile și la nivelul proprietarului/operatorului/ administratorului de infrastructură critică națională/europeană,

în conformitate cu prevederile Ordonanței de urgență a Guvernului nr. 98/2010 privind identificarea, desemnarea și protecția infrastructurilor critice, aprobată cu modificări prin Legea nr. 18/2011,

în temeiul art. 7 alin. (5) din Ordonanța de urgență a Guvernului nr. 30/2007 privind organizarea și funcționarea Ministerului Afacerilor Interne, aprobată cu modificări prin Legea nr. 15/2008, cu modificările și completările ulterioare,

ministrul afacerilor interne emite prezentul ordin.

CAPITOLUL I

Dispoziții generale

Art. 1. — Prezentul ordin stabilește cadrul general de organizare și desfășurare a activităților specifice domeniului protecției infrastructurilor critice naționale (ICN)/infrastructurilor critice europene (ICE) în unitățile Ministerului Afacerilor Interne, denumit în continuare *M.A.I.*, având ca scop asigurarea unei concepții coerente și unitare de acțiune, și instituie, la nivelul *M.A.I.*, normele referitoare la:

a) modul de organizare și desfășurare a activităților necesare identificării, desemnării și protecției ICN/ICE;

b) rolul și responsabilitățile structurilor *M.A.I.* în procesul de identificare și desemnare a ICN/ICE.

Art. 2. — Prevederile prezentului ordin se aplică tuturor structurilor *M.A.I.* angrenate în procesul de identificare, desemnare și protecție a ICN/ICE, precum și personalului nominalizat să desfășoare activități în domeniul de referință.

Art. 3. — (1) Termenii și expresiile din domeniul protecției infrastructurilor critice, utilizate în prezentul ordin, au înțelesul definit în legislația națională.

(2) În sensul prezentului ordin, „structura *M.A.I.* competentă” este structura care are în responsabilitate ICN/ICE.

CAPITOLUL II

Activitatea de identificare, desemnare și protecție a ICN/ICE

SECȚIUNEA 1

Organizarea și coordonarea activității

Art. 4. — (1) Organizarea și coordonarea activității în domeniul identificării, desemnării și protecției ICN/ICE în *M.A.I.*

se realizează de Centrul de coordonare a protecției infrastructurilor critice, denumit în continuare *Centrul*.

(2) Activitățile prevăzute la alin. (1) se realizează conform Planului anual de acțiune al *M.A.I.* în domeniul protecției ICN/ICE, elaborat în baza Planului de acțiune pentru implementarea, monitorizarea și evaluarea obiectivelor Strategiei naționale privind protecția infrastructurilor critice și Calendarului principalelor activități ale Grupului de lucru interinstituțional pentru protecția infrastructurilor critice, aprobate prin decizii ale prim-ministrului.

Art. 5. — Centrul are competență teritorială generală în domeniul de activitate reglementat de prezentul ordin și pe linie de specialitate coordonează, îndrumă și controlează compartimentele de profil constituite la nivelul instituțiilor și structurilor aflate în subordinea/coordonarea *M.A.I.*

Art. 6. — (1) În executarea atribuțiilor ce îi revin potrivit legii, Centrul îndeplinește următoarele funcții:

a) de reglementare, prin care asigură elaborarea proiectelor de acte normative și a standardelor/procedurilor operaționale în domeniul protecției ICN/ICE;

b) de planificare, prin care asigură elaborarea documentelor de planificare strategică și a planurilor de implementare a acestora;

c) de coordonare, prin care se asigură caracterul unitar și integrat al acțiunilor și măsurilor necesare îmbunătățirii nivelului de protecție a ICN/ICE aflate în responsabilitate;

d) de management al informațiilor, prin care se asigură diseminarea datelor privind evoluțiile înregistrate în plan internațional și intern, precum și cele referitoare la tipurile de riscuri și amenințări ce pot afecta ICN/ICE;

e) de reprezentare, prin care asigură punctul național de contact în relația cu CE, statele membre, NATO, alte organisme internaționale și reprezintă M.A.I. în Grupul de lucru interinstituțional pentru protecția infrastructurilor critice, denumit în continuare *G.L.I.P.I.C.*;

f) de comunicare, prin care se asigură notificarea/înștiințarea în cadrul mecanismului de comunicare și avertizare timpurie;

g) de control, prin care se asigură testarea/verificarea viabilității planurilor de securitate ale proprietarilor/operatorilor/administratorilor de ICN/ICE, denumite în continuare *PSO*;

h) de cooperare, prin care planifică, organizează și desfășoară acțiuni în comun, în conformitate cu angajamentele asumate de M.A.I., pe plan intern și internațional, în domeniul protecției infrastructurilor critice.

(2) În vederea îndeplinirii atribuțiilor stabilite prin lege, Centrul organizează și menține cooperarea cu reprezentanții autorităților publice responsabile în domeniul protecției ICN/ICE, ai mediului academic și ai organizațiilor nonguvernamentale cu preocupări în domeniul specificat.

Art. 7. — (1) După consultarea reprezentanților autorităților publice responsabile în *G.L.I.P.I.C.*, constituit potrivit Hotărârii Guvernului nr. 1.110/2010 privind componența, atribuțiile și modul de organizare ale Grupului de lucru interinstituțional pentru protecția infrastructurilor critice, cu modificările ulterioare, Centrul elaborează și propune, după caz, spre semnare, aprobare sau avizare, ministrului afacerilor interne:

a) proiectele de acte normative de nivel superior pentru modificarea/completarea prevederilor legale în domeniul protecției ICN/ICE;

b) proiectele strategiilor naționale/sectoriale în domeniu;

c) criteriile/cerințele minime necesare în procesul de formare a personalului în domeniul protecției ICN/ICE;

d) măsurile pentru asigurarea pregătirii personalului desemnat să îndeplinească funcția de ofițer de legătură pentru securitatea ICN/ICE;

e) raportul de evaluare a riscurilor, amenințărilor și punctelor vulnerabile ale ICN/ICE și propunerile cu privire la necesitatea îmbunătățirii protecției acestora.

(2) Centrul elaborează/propune spre aprobare/avizare ministrului afacerilor interne:

a) componența nominală a Comisiei de evaluare a *PSO* din M.A.I.;

b) *PSO* elaborate la nivelul proprietarilor/operatorilor/administratorilor de ICN/ICE din M.A.I.;

c) raportul trimestrial privind evoluțiile în domeniul protecției ICN/ICE destinat informării prim-ministrului;

d) planul anual de acțiune al M.A.I. în domeniul protecției ICN/ICE;

e) planul anual de verificare a viabilității *PSO* din M.A.I.;

f) planul anual de pregătire de specialitate a personalului cu atribuții în domeniul protecției ICN/ICE;

g) planul anual de relații internaționale al Centrului;

h) măsurile cu caracter imediat în situația producerii unor riscuri la nivelul ICN/ICE din responsabilitatea M.A.I.

Art. 8. — (1) Șeful Centrului îndeplinește funcția de ofițer de legătură pentru securitatea ICN/ICE al M.A.I., în sensul prevederilor art. 8 alin. (2) din Ordonanța de urgență a Guvernului nr. 98/2010 privind identificarea, desemnarea și protecția infrastructurilor critice, aprobată cu modificări prin Legea nr. 18/2011, denumită în continuare *O.U.G. nr. 98/2010*.

(2) Șeful Centrului reprezintă M.A.I. în *G.L.I.P.I.C.*

Art. 9. — (1) În vederea eficientizării comunicării în domeniul protecției ICN/ICE la nivelul M.A.I., Centrul stabilește modalitățile de realizare a cooperării cu ofițerii de legătură desemnați pentru securitatea ICN/ICE.

(2) În scopul asigurării coordonării unitare a măsurilor pentru protecția ICN/ICE, precum și pentru realizarea cu celeritate a schimbului de date și informații între operatorii/prorietarii/administratorii de ICN/ICE, Centrul operaționalizează și administrează mecanismul de comunicare și avertizare timpurie în sensul art. 8 alin. (4) din *O.U.G. nr. 98/2010*.

SECȚIUNEA a 2-a

Atribuțiile și competențele unităților din aparatul central și ale structurilor și instituțiilor aflate în subordinea/coordonarea M.A.I. care au în responsabilitate ICN/ICE

Art. 10. — (1) Unitățile din aparatul central, structurile și instituțiile aflate în subordinea/coordonarea M.A.I., precum și structurile aflate în subordinea acestora care au calitatea de proprietari/operatori/administratori de ICN/ICE au obligația de desemna un compartiment specializat în domeniul ICN/ICE, în condițiile prevăzute de art. 8 din *O.U.G. nr. 98/2010*.

(2) În cazul în care nu este posibilă constituirea unor astfel de compartimente, atribuțiile, competențele și responsabilitățile respective vor fi repartizate unei structuri existente sau unor persoane desemnate în acest scop de conducerea structurii respective.

Art. 11. — Numirea în funcție a ofițerilor de legătură pentru securitatea ICN/ICE în cadrul unităților, structurilor și instituțiilor prevăzute la art. 10 alin. (1) se realizează cu avizul Centrului.

Art. 12. — Unitățile, structurile și instituțiile prevăzute la art. 10 alin. (1) dispun măsuri pentru elaborarea *PSO*, în condițiile prevăzute de art. 8 alin. (3) din *O.U.G. nr. 98/2010*.

SECȚIUNEA a 3-a

Identificarea, desemnarea și protecția ICN/ICE în M.A.I.

Art. 13. — (1) Procesul de identificare, desemnare și protecție a ICN/ICE este o activitate ciclică, reluată, în mod obligatoriu, anual, de către toate structurile aflate în subordinea/coordonarea M.A.I.

(2) Unitățile din aparatul central, structurile și instituțiile aflate în subordinea/coordonarea M.A.I., precum și structurile aflate în subordinea acestora care, la data reluării procesului menționat la alin. (1), nu au calitatea de proprietari/operatori/administratori de ICN/ICE vor desemna reprezentanți, la nivel șef serviciu/birou pentru a participa la activități conform procedurilor stabilite de Centru.

Art. 14. — (1) Procesul de identificare a potențialelor ICN/ICE din responsabilitatea M.A.I. se organizează sub coordonarea Centrului, conform prevederilor art. 10 și anexei nr. 2 la *O.U.G. nr. 98/2010*.

(2) După parcurgerea etapelor obligatorii prevăzute de legislația în vigoare pentru identificarea ICN/ICE din responsabilitate, structurile M.A.I. transmit la Centru, sub semnătura conducătorului structurii, lista cu propunerile de ICN/ICE.

Art. 15. — (1) Centrul acordă asistență de specialitate structurilor M.A.I. care au în responsabilitate ICN/ICE desemnate, conform prevederilor legale în vigoare și asigură accesul acestora la informații cu privire la cele mai bune practici și metode disponibile în domeniu.

(2) Centrul poate solicita structurilor M.A.I. să asigure participarea personalului care își desfășoară activitatea în compartimentele specializate în domeniul protecției infrastructurilor critice la activități de formare și schimb de informații privind noi evoluții tehnice în materie.

Art. 16. — (1) În termen de un an de la desemnarea unei ICN/ICE în responsabilitatea unei structuri a M.A.I., aceasta elaborează un raport conținând evaluarea riscurilor, amenințărilor și punctelor vulnerabile ale acestei ICN/ICE și propune măsuri cu privire la necesitatea îmbunătățirii protecției acesteia.

(2) După finalizarea procesului de desemnare a ICN/ICE, activitățile prevăzute la alin. (1) se realizează anual.

(3) Raportul prevăzut la alin. (1) se transmite Centrului, anual, până la data de 15 decembrie sau la solicitarea acestuia.

Art. 17. — Conducătorii structurilor M.A.I. competente au obligația de a informa Centrul despre orice modificare survenită la nivelul ICN/ICE deținute care poate influența negativ nivelul de securitate al acesteia.

Art. 18. — Structurile M.A.I. competente realizează monitorizarea și evaluarea permanentă a nivelului de vulnerabilitate al ICN/ICE și desfășoară activități pentru identificarea măsurilor necesare diminuării acestuia.

Art. 19. — (1) Centrul realizează monitorizarea permanentă și evaluarea trimestrială a stadiului îndeplinirii obiectivelor Planului de acțiune pentru implementarea, monitorizarea și evaluarea obiectivelor Strategiei naționale privind protecția infrastructurilor critice, aprobat prin decizie a prim-ministrului.

(2) Pentru realizarea evaluării prevăzute la alin. (1), structurile M.A.I. competente transmit datele și informațiile de interes pentru trimestrul încheiat, până la data de 10 a primei luni din trimestrul următor sau la solicitarea Centrului.

SECȚIUNEA a 4-a

Planul de securitate al

proprietarului/operatorului/administratorului de ICN/ICE

Art. 20. — (1) PSO este documentul de planificare, cu caracter operativ, destinat identificării și punerii în aplicare a soluțiilor de securitate pentru îmbunătățirea nivelului de protecție și reziliență a infrastructurilor critice naționale/europene.

(2) Structura-cadru a PSO este prevăzută în Decizia prim-ministrului nr. 166/2013 privind aprobarea Normelor metodologice pentru realizarea/echivalarea/revizuirea planurilor de securitate ale proprietarilor/operatorilor/administratorilor de infrastructură critică națională/europeană, a structurii-cadru a planului de securitate al proprietarului/operatorului/administratorului deținător de infrastructură critică națională/europeană și a atribuțiilor ofițerului de legătură pentru securitate din cadrul compartimentului specializat desemnat la nivelul autorităților publice responsabile și la nivelul proprietarului/operatorului/administratorului de ICN/ICE.

Art. 21. — În scopul creșterii gradului de protecție a ICN/ICE din responsabilitate, structura M.A.I. competentă desfășoară activități pentru:

- a) identificarea amenințărilor;
- b) elaborarea scenariilor de amenințări;
- c) identificarea punctelor vulnerabile;
- d) realizarea evaluărilor de risc;
- e) elaborarea și testarea viabilității PSO;
- f) actualizarea periodică a PSO.

Art. 22. — (1) PSO sau, după caz, identificarea echivalentului acestuia se realizează de către structurile M.A.I. competente în termen de 9 luni de la desemnarea ICN/ICE.

(2) În cazul în care este identificat un echivalent al PSO, proprietarii/operatorii/administratorii de ICN/ICE transmit Centrului 2 (două) exemplare originale ale documentelor pentru a fi echivalate, prezentând într-un memoriu sau notă justificativă elementele de echivalență și analiza de suficiență, din care să reiasă satisfacerea necesităților de protecție a ICN/ICE fără elaborarea unui document distinct în acest sens.

Art. 23. — (1) PSO și documentele echivalente acestuia se evaluează de către o Comisie de evaluare compusă din: ofițerul de legătură pentru securitate al M.A.I., ofițerul de legătură pentru securitate al unității aparatului central al M.A.I. competente și 2 ofițeri din cadrul Centrului.

(2) Pentru analizarea conținutului capitolelor de specialitate din cuprinsul PSO sau al documentelor echivalente acestuia care necesită un înalt nivel de expertiză tehnico-științifică ori cunoștințe detaliate despre natura proceselor analizate, Comisia de evaluare poate coopta și reprezentanți ai altor structuri specializate din M.A.I., cu rol consultativ, fără ca aceștia să facă parte din Comisia de evaluare prevăzută la alin. (1).

Art. 24. — (1) Procesul de evaluare se încheie prin întocmirea unui raport de evaluare semnat de toți membrii Comisiei, în condițiile prevăzute de Decizia prim-ministrului nr. 166/2013.

(2) Raportul se finalizează în maximum 30 de zile de la primirea de la proprietar/operator/administrator de ICN/ICE a PSO sau a documentelor echivalente acestuia. În acest sens:

a) Comisia de evaluare realizează, după caz, una dintre acțiunile prevăzute la art. 17 alin. (1) din anexa la Decizia prim-ministrului nr. 166/2013;

b) Proprietarii/operatorii/administratorii de ICN/ICE transmit Centrului raportul-sinteză în condițiile art. 17 alin. (2) din anexa nr. 1 la Decizia prim-ministrului nr. 166/2013.

(3) După evaluarea conținutului documentelor prevăzute la alin. (1) și (2), Comisia de evaluare le înaintează spre avizare ministrului afacerilor interne.

Art. 25. — (1) La elaborarea PSO se iau în considerare scenariile de amenințări elaborate de către proprietarii/operatorii/administratorii de ICN/ICE.

(2) La elaborarea scenariilor de amenințări vor fi avute în vedere, după caz, amenințări de tipul:

- a) fenomene meteorologice periculoase;
- b) fenomene distructive de origine geologică;
- c) accidente, avarii, explozii, incendii;
- d) poluări de ape;
- e) prăbușiri de construcții, instalații, amenajări;
- f) accident nuclear major sau urgență radiologică cu efect transfrontalier;
- g) accident major în care sunt implicate substanțe periculoase;
- h) boli transmisibile care pot afecta sănătatea publică (epidemii/pandemii);
- i) amenințări teroriste;
- j) grave tulburări sociale;
- k) alte amenințări cu specific sectorial, conform criteriilor aprobate în sectorul respectiv;
- l) evenimente internaționale și/sau cu caracter geopolitic sau de natura amenințărilor militare, dacă acestea pot genera amenințări suplimentare la nivelul ICN.

Art. 26. — (1) Pentru efectuarea evaluărilor de risc, proprietarii/operatorii/administratorii de ICN/ICE pot utiliza orice metodă sau tehnică de analiză acceptată, astfel:

a) una dintre metodele sau tehnicile descrise de standardele internaționale în materie;

b) o metodă de evaluare standardizată pe plan internațional, cu indicarea standardului public aplicabil;

c) o metodă sau tehnică nestandardizată de analiză sau un procedeu nestandardizat de estimare a consecințelor, în măsura în care proprietarul/operatorul/administratorul de ICN/ICE poate să ofere documentație detaliată cu privire la modul de aplicare a acesteia/acestui, să justifice necesitatea și avantajele alegerii acestei abordări.

(2) În cuprinsul evaluărilor de risc se precizează, în mod obligatoriu, denumirea/tipul metodei utilizate, presupunerile inițiale avute în vedere, valorile parametrilor inițiali sau intermediari introduși în algoritmi și aproximările realizate, astfel încât, exclusiv pe baza informațiilor disponibile, o terță parte să poată expertiza, în cazul în care se consideră necesar, nivelul de conformitate.

Art. 27. — În scopul asigurării unui cadru unitar de realizare a PSO, Centrul organizează ședințe, ateliere de lucru și seminare.

Art. 28. — (1) PSO și planurile sau documentele echivalente acestuia se testează prin exerciții interne organizate și desfășurate la nivel național cu o periodicitate de minimum un exercițiu pe an.

(2) PSO sau documentele echivalente acestuia se pot testa și prin exerciții parțiale (în teren, exerciții simulate, exerciții tematice cu forțe și mijloace etc.), cât și prin exerciții de alertare, desfășurate în mod periodic și astfel încât să acopere, în timp, o gamă variată de condiții: anunțate/neanunțate, cu scenariul cunoscut/parțial cunoscut/necunoscut, ziua/noaptea, iarna/vara, în timpul/afara programului, în weekend/în timpul săptămânii etc.

(3) Normele de organizare, desfășurare și evaluare a exercițiilor se elaborează de către Centru.

(4) Exercițiile organizate și desfășurate în conformitate cu prevederile alin. (1) și (2) se finalizează prin întocmirea unui raport de evaluare a fiecărui exercițiu, elaborat conform normelor prevăzute la alin. (3).

Art. 29. — Pentru identificarea soluțiilor optime de realizare a protecției elementelor de ICN/ICE și stabilirea modalităților de intervenție preventivă, structurile M.A.I. colaborează cu autorități sau persoane juridice în condițiile în care ICN/ICE ar putea genera efecte în domeniul de responsabilitate al acestora.

SECȚIUNEA a 5-a

Colaborarea și cooperarea internă și internațională

Art. 30. — În exercitarea atribuțiilor sale, Centrul:

a) colaborează în domeniile de activitate specifice cu unitățile aparatului central al M.A.I., precum și cu instituțiile și structurile aflate în subordinea/coordonarea M.A.I.;

b) cooperează nemijlocit cu consilierul desemnat al prim-ministrului pentru probleme de securitate națională,

precum și cu structurile similare ale autorităților publice responsabile în domeniul protecției ICN/ICE;

c) menține contacte de lucru active cu instituțiile specializate ale UE, NATO, statelor membre ale UE, precum și cu alte organisme internaționale în domeniul de referință.

Art. 31. — În vederea participării la misiuni internaționale, Centrul stabilește oportunitatea participării la misiune și elaborează proiectul de mandat pe care îl supune avizării G.L.I.P.I.C. și ulterior aprobării prim-ministrului.

Art. 32. — Schimbul de date și informații cu partenerii externi se realizează prin intermediul punctului național de contact cu informarea ulterioară a direcției de specialitate a M.A.I.

Art. 33. — (1) Participarea reprezentanților structurilor M.A.I. la activități în domeniul protecției ICN/ICE se realizează exclusiv pe baza unui mandat avizat de Centru.

(2) Reprezentanții structurilor M.A.I. care participă la activități în cadrul cărora sunt abordate aspecte specifice domeniului protecției infrastructurilor critice sunt obligați să informeze Centrul cu privire la aspectele discutate și concluziile rezultate.

CAPITOLUL III Dispoziții finale

Art. 34. — (1) Personalul Centrului este abilitat să constate și să propună ministrului afacerilor interne aplicarea de sancțiuni contravenționale personalului structurilor M.A.I., în conformitate cu prevederile art. 12 și 13 din O.U.G. nr. 98/2010.

(2) Organizarea și desfășurarea controalelor pe linia protecției ICN/ICE se realizează conform procedurilor proprii elaborate de Centru/structura M.A.I. competentă.

Art. 35. — Documentele transmise de proprietarii/operatorii/administratorii de ICN/ICE către Comisia de evaluare constituită la nivelul Centrului în conformitate cu prevederile art. 23 alin. (1), se clasifică în raport cu conținutul acestora, conform prevederilor legale.

Art. 36. — Structurile M.A.I. competente realizează diseminarea/accesul la datele și informațiile referitoare la protecția ICN/ICE din responsabilitate către alte structuri ale M.A.I. sau instituții cu atribuții în domeniul de referință, cu excepția Centrului, numai cu aprobarea ministrului afacerilor interne și respectarea principiului „necesității de a cunoaște” și dispun măsurile din competență pentru aplicarea legislației în vigoare în domeniul protecției informațiilor clasificate.

Art. 37. — În vederea desfășurării activităților în domeniul protecției infrastructurilor critice, în mod unitar, Centrul elaborează proceduri de sistem/interne de lucru.

Art. 38. — Documentele de colaborare/cooperare încheiate de structurile M.A.I. care vizează domeniul protecției infrastructurilor critice se avizează de Centru înaintea semnării de către șeful structurii care le-a întocmit.

Art. 39. — Tematica cursurilor/programelor de formare profesională continuă a personalului în domeniul protecției ICN/ICE, organizate în instituțiile de învățământ ale M.A.I., se avizează de Centru.

Art. 40. — Prezentul ordin se publică în Monitorul Oficial al României, Partea I.

Ministrul afacerilor interne,
Radu Stroe

MINISTERUL AGRICULTURII ȘI DEZVOLTĂRII RURALE

ORDIN**pentru modificarea și completarea anexei la Ordinul ministrului agriculturii, pădurilor și dezvoltării rurale nr. 392/2009 privind aprobarea listei cu cheltuieli eligibile pentru proiectele finanțate în cadrul Programului Operațional pentru Pescuit 2007—2013**

Având în vedere Referatul de aprobare al Direcției generale pescuit — Autoritate de management pentru POP nr. 253.022 din 20 noiembrie 2013,

în baza prevederilor:

— Regulamentului (CE) nr. 1.198/2006 al Consiliului din 27 iulie 2006 privind Fondul European pentru Pescuit, cu modificările și completările ulterioare;

— Regulamentului (CE) nr. 498/2007 al Comisiei din 26 martie 2007 de stabilire a unor norme detaliate pentru punerea în aplicare a Regulamentului (CE) nr. 1.198/2006 al Consiliului privind Fondul European pentru Pescuit, cu modificările și completările ulterioare;

— Ordonanței de urgență a Guvernului nr. 74/2009 privind gestionarea fondurilor comunitare nerambursabile provenite din Fondul european de garantare agricolă, Fondul european agricol de dezvoltare rurală și Fondul european pentru pescuit și a fondurilor alocate de la bugetul de stat, privind gestionarea fondurilor nerambursabile alocate de la Comunitatea Europeană și a fondurilor alocate de la bugetul de stat aferente programului de colectare și gestionare a datelor necesare desfășurării politicii comune în domeniul pescuitului și a programului de control, inspecție și supraveghere în domeniul pescuitului și pentru modificarea art. 10 din Legea nr. 218/2005 privind stimularea absorbției fondurilor SAPARD, Fondul european agricol pentru dezvoltare rurală, Fondul european pentru pescuit, Fondul european de garantare agricolă, prin preluarea riscului de creditare de către fondurile de garantare, aprobată cu modificări prin Legea nr. 371/2009, cu modificările și completările ulterioare;

— Hotărârii Guvernului nr. 442/2009 privind stabilirea cadrului general de implementare a măsurilor cofinanțate din Fondul European pentru Pescuit prin Programul Operațional pentru Pescuit 2007—2013, cu modificările și completările ulterioare;

— art. 7 alin. (5) din Hotărârea Guvernului nr. 725/2010 privind reorganizarea și funcționarea Ministerului Agriculturii și Dezvoltării Rurale, precum și a unor structuri aflate în subordinea acestuia, cu modificările și completările ulterioare,

ministrul agriculturii și dezvoltării rurale emite prezentul ordin.

Art. I. — Anexa la Ordinul ministrului agriculturii, pădurilor și dezvoltării rurale nr. 392/2009 privind aprobarea listei cu cheltuieli eligibile pentru proiectele finanțate în cadrul Programului Operațional pentru Pescuit 2007—2013, publicat în Monitorul Oficial al României, Partea I, nr. 467 din 7 iulie 2009, cu modificările și completările ulterioare, se modifică și se completează după cum urmează:

1. La punctul II, litera J) Măsura 2.2 „Pescuit în apele interioare”, după punctul 14 se introduce un nou punct, punctul 15, cu următorul cuprins:

„15. prime pentru schimbarea destinației ambarcațiunilor de pescuit în apele interioare către alte activități”.

2. La punctul II, litera S, măsura 5.1. „Asistența tehnică” Acțiunea 3, secțiunea „Alte activități de asistență tehnică” punctul 2.5 se modifică și va avea următorul cuprins:

„2.5. alte costuri aferente transportului (taxă înmatriculare, taxă mediu, taxă certificat înmatriculare, taxă plăcuțe numere înmatriculare, RCA, CASCO, rovinieta, taxe de pod și altele asimilate);”.

Art. II. — Prezentul ordin se publică în Monitorul Oficial al României, Partea I.

p. Ministrul agriculturii și dezvoltării rurale,

Achim Irimescu,
secretar de stat

București, 27 noiembrie 2013.

Nr. 1.348.

MINISTERUL SĂNĂTĂȚII

ORDIN**pentru modificarea Ordinului ministrului sănătății nr. 1.091/2013
privind stabilirea cuantumului taxei și modalitatea de plată a acesteia
pentru participarea la examenul de grad principal pentru asistenții medicali generaliști,
moașe și asistenți medicali — sesiunea 2013**

Având în vedere Referatul de aprobare al Direcției generale resurse umane și certificare nr. E.N. 12.100/2013 și prevederile Hotărârii Guvernului nr. 144/2010 privind organizarea și funcționarea Ministerului Sănătății, cu modificările și completările ulterioare, în temeiul dispozițiilor Ordonanței de urgență a Guvernului nr. 144/2008 privind exercitarea profesiei de asistent medical generalist, a profesiei de moașă și a profesiei de asistent medical, precum și organizarea și funcționarea Ordinului Asistenților Medicali Generaliști, Moașelor și Asistenților Medicali din România,

ministrul sănătății emite prezentul ordin.

Art. I. — Ordinul ministrului sănătății nr. 1.091/2013 privind stabilirea cuantumului taxei și modalitatea de plată a acesteia pentru participarea la examenul de grad principal pentru asistenții medicali generaliști, moașe și asistenți medicali — sesiunea 2013, publicat în Monitorul Oficial al României, Partea I, nr. 596 din 24 septembrie 2013, se modifică după cum urmează:

1. Articolul 1 va avea următorul cuprins:

„Art. 1. — (1) Se desemnează Ordinul Asistenților Medicali Generaliști, Moașelor și Asistenților Medicali din România (OAMGMAMR) să organizeze examenul de grad principal pentru asistenții medicali generaliști, moașe și asistenți medicali — sesiunea 2013.

(2) Cuantumul taxei de participare la examenul de grad principal pentru asistenții medicali generaliști, moașe și asistenți medicali — sesiunea 2013 se stabilește în sumă de 120 lei/participant. Taxa se va plăti după cum urmează:

a) 30%, respectiv suma de 36 lei, în contul IBAN nr. RO85TREZ7005003XXX000092, CUI — 4266456, Direcția de Trezorerie a Municipiului București (DTMB), beneficiar Ministerul Sănătății, str. Cristian Popișteanu nr. 1—3, sectorul 1, București, cod 010024;

b) 70%, respectiv suma de 84 lei, în contul RO49UGBI0000362008983RON, Garanti Bank, beneficiar Ordinul Asistenților Medicali Generaliști, Moașelor și Asistenților Medicali din România (OAMGMAMR), CIF 15346984, str. Ing. Zabłowski nr. 76, cod poștal 011312.

(3) La finalizarea perioadei de înscriere, OAMGMAMR virează Ministerului Sănătății în contul sus menționat contravaloarea sumei de 84 lei, virată de participant în contul OAMGMAMR sus-menționat.

(4) Pentru sumele prevăzute la alin. (3), OAMGMAMR transmite Ministerului Sănătății borderoul nominal cu datele de identificare ale plătitorilor.”

2. Articolul 3 va avea următorul cuprins:

„Art. 3. — (1) Ministerul Sănătății, din sumele achitate de către participanți, repartizează către OAMGMAMR, pe bază de contract civil de prestări servicii, o cotă de 70%, pentru plata cheltuielilor de personal pe bază de contract civil (cu excepția funcționarilor publici), plata membrilor comisiei centrale și comisiilor județene de examen, a comisiei de elaborare a subiectelor, a colectivelor tehnice (cu excepția funcționarilor publici), a cheltuielilor materiale efectuate de către comisia centrală și comisiile județene de examen, închiriere săli, în baza documentelor justificative.

(2) Modelul contractului civil de prestări servicii prevăzut la alin. (1) se aprobă prin ordin al ministrului sănătății.

(3) În termen de 30 de zile de la finalizarea examenului de grad principal pentru asistenții medicali generaliști, moașe și asistenți medicali — sesiunea 2013, OAMGMAMR are obligația de a prezenta Ministerului Sănătății atât decontul de cheltuieli, cât și documentele justificative. Decontul de cheltuieli reprezintă anexa la contractul civil de prestări servicii.

(4) Suma rămasă neutilizată de OAMGMAMR, după prezentarea decontului prevăzut la alin. (3), se restituie Ministerului Sănătății.”

3. Articolul 4 va avea următorul cuprins:

„Art. 4. — Repartizarea sumelor pe filialele județene și, respectiv, a municipiului București ale OAMGMAMR se va face în baza bugetelor stabilite de către OAMGMAMR, iar decontarea cheltuielilor se va face pe baza documentelor justificative privind cheltuielile ocazionate de organizarea examenului de grad principal pentru asistenții medicali generaliști, moașe și asistenți medicali — sesiunea 2013, însușită sub semnătură de președintele filialei județene/a municipiului București a OAMGMAMR.”

Art. II. — Prezentul ordin se publică în Monitorul Oficial al României, Partea I.

Ministrul sănătății,
Gheorghe-Eugen Nicolăescu

București, 28 noiembrie 2013.
Nr. 1.446.

ACTE ALE ÎNALTEI CURȚI DE CASAȚIE ȘI JUSTIȚIE

ÎNALTA CURTE DE CASAȚIE ȘI JUSTIȚIE

COMPLETUL COMPETENT SĂ JUDECE RECURSUL ÎN INTERESUL LEGII

DECIZIA Nr. 15**din 14 octombrie 2013**

Dosar nr. 12/2013

Livia Doina Stanciu	— președintele Înaltei Curți de Casație și Justiție, președintele completului
Lavinia Curelea	— președintele Secției I civile
Roxana Popa	— președintele delegat al Secției a II-a civile
Ionel Barbă	— președintele Secției de contencios administrativ și fiscal
Corina Michaela Jîiie	— președintele Secției penale
Simona Cristina Neniță	— judecător Secția penală
Ioana Bogdan	— judecător Secția penală
Ionuț Mihai Matei	— judecător Secția penală
Leontina Șerban	— judecător Secția penală
Ștefan Pistol	— judecător Secția penală
Mirela Sorina Popescu	— judecător Secția penală
Florentina Dragomir	— judecător Secția penală
Sofica Dumitrașcu	— judecător Secția penală
Mariana Ghena	— judecător Secția penală
Săndel Lucian Macavei	— judecător Secția penală
Alina Ioana Ilie	— judecător Secția penală
Lavinia Valeria Lefterache	— judecător Secția penală, judecător raportor
Maricela Cobzariu	— judecător Secția penală
Ana Maria Dascălu	— judecător Secția penală
Dragu Crețu	— judecător Secția I civilă
Alina Iuliana Țuca	— judecător Secția I civilă
Mariana Cîrstocea	— judecător Secția a II-a civilă
Mirela Polițeanu	— judecător Secția a II-a civilă
Carmen Sîrbu	— judecător Secția de contencios administrativ și fiscal
Carmen Maria Ilie	— judecător Secția de contencios administrativ și fiscal

Completul competent să judece recursul în interesul legii ce formează obiectul Dosarului nr. 12/2013 este constituit conform dispozițiilor art. 414⁴ alin. 3 din Codul de procedură penală, modificat și completat prin Legea nr. 202/2010, raportat la dispozițiile art. 27² din Regulamentul privind organizarea și funcționarea administrativă a Înaltei Curți de Casație și Justiție, republicat, cu modificările și completările ulterioare.

Ședința completului este prezidată de doamna Livia Doina Stanciu, președintele Înaltei Curți de Casație și Justiție.

La ședința de judecată participă procurorul general al Parchetului de pe lângă Înalta Curte de Casație și Justiție, domnul procuror Tiberiu Nițu.

La ședința de judecată participă magistratul-asistent din cadrul Secțiilor Unite, doamna Monica Eugenia Ungureanu, desemnat în conformitate cu dispozițiile art. 27³ din Regulamentul privind organizarea și funcționarea administrativă a Înaltei Curți de Casație și Justiție, republicat, cu modificările și completările ulterioare.

Înalta Curte de Casație și Justiție — Completul competent să judece recursul în interesul legii a luat în examinare recursul în interesul legii formulat de către procurorul general al Parchetului de pe lângă Înalta Curte de Casație și Justiție prin Sesizarea nr. 11.874/2670/III-5/2011, pentru a se stabili, în

vederea interpretării și aplicării unitare a dispozițiilor art. 42 alin. (1), (2) și (3) din Legea nr. 161/2003, respectiv pentru interpretarea unitară a noțiunii de acces fără drept la un sistem informatic, determinat de diferențierea practică între:

— accesul prin intermediul montării la ATM a dispozitivelor de citire a benzii magnetice a cardului autentic și a codului PIN aferent acestuia; sau

— accesul produs prin folosirea la bancomat a cardului falsificat ori chiar a celui autentic, fără acordul titularului său.

Procurorul general al Parchetului de pe lângă Înalta Curte de Casație și Justiție a susținut recursul în interesul legii învederând că examenul jurisprudenței penale actuale a evidențiat mai multe orientări cu privire la acest aspecte și, prin urmare, caracterul neunitar al practicii judiciare:

I. Într-o primă orientare a practicii, unele instanțe au considerat că montarea dispozitivelor de citire a benzii magnetice a cardului autentic, a videocamerei sau a falsei tastaturi nu constituie acces fără drept la un sistem informatic, infracțiune prevăzută de art. 42 alin. (1) din Legea nr. 161/2003 (anexele nr. 1, 3, 43—45, 55).

Instanțele au încadrat această faptă în dispozițiile art. 25 din Legea nr. 365/2002, reținându-se că inculpații „au deținut echipamente electronice apte să citească și să memoreze date din cărțile de credit, în scopul obținerii acelor date care permit retragerea sumelor de bani din cărțile de credit” (anexa nr. 44).

Alte instanțe au apreciat că „fapta inculpatului de a atașa la un ATM un dispozitiv format dintr-un telefon mobil prevăzut cu cameră video și card de memorie și un suport menit a susține și disimula telefonul în plafonul bancomatului, în scopul de a înregistra codul PIN tastat de utilizatorul acestuia, întrunește elementele constitutive ale infracțiunii prevăzute de art. 46 alin. (2) din Legea nr. 161/2003, adică deținere fără drept a unui dispozitiv conceput sau adaptat în scopul săvârșirii uneia dintre infracțiunile prevăzute de art. 42—45 din aceeași lege” (anexa nr. 55).

Cele mai multe instanțe însă au menținut încadrarea juridică din actul de sesizare, fără a pune în discuție și fără a se pronunța în mod expres asupra problemei de drept supusă prezentului recurs.

Înalta Curte de Casație și Justiție a împărțit această primă orientare prin deciziile nr. 4.009 din 4 decembrie 2008 (anexa nr. 1), nr. 251 din 26 ianuarie 2011 (anexa nr. 3), nr. 2.416 din 18 iunie 2010 (anexa nr. 43), nr. 3.425 din 5 octombrie 2011 (anexa nr. 44) și nr. 3.354 din 3 octombrie 2011 (anexa nr. 45).

Într-o a doua orientare a practicii s-a reținut, dimpotrivă, că prin montarea la bancomat a dispozitivelor de citire a informațiilor înregistrate pe banda magnetică a cardului și de capture 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 (anexele nr. 39—41, 46—47).

În argumentarea acestei opinii, instanțele au apreciat că „ATM-ul este un mijloc de colectare, prelucrare și 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 skimmerului în fanta bancomatului, prin care se introduce cardul și se realizează citirea benzii magnetice a fiecărui card în parte, stocându-se informația astfel obținută, au fost încălcate măsurile de securitate care aveau drept scop asigurarea secretului numărului de cont și a operațiunilor efectuate și apărarea împotriva folosirii de către o altă persoană a acestor carduri în vederea fraudării. În consecință, inculpații au accesat fără drept un sistem informatic încălcând astfel măsurile de securitate.” (anexa nr. 46).

Cu aceeași motivare, unele instanțe au reținut ca incidente, pentru această situație de fapt, dispozițiile art. 44 alin. (2), (3) și art. 46 alin. (2) alături de cele ale art. 42 alin. (2), (3) din Legea nr. 161/2003 (anexa nr. 41).

În argumentarea acestei opinii, instanțele au apreciat că atât videocamera, cât și skimmerul au fost deținute în scopul cerut de art. 46 alin. (2) din Legea nr. 161/2003.

Înalta Curte de Casație și Justiție a împărțit această orientare prin deciziile nr. 376 din 2 februarie 2010 (anexa nr. 39), nr. 5.288 din 15 septembrie 2006 (anexa nr. 46) și nr. 2.094 din 27 mai 2010 (anexa nr. 47).

La același punct de vedere au aderat și instanțele, inclusiv Înalta Curte de Casație și Justiție prin Decizia nr. 2.991 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” (anexa nr. 16).

II. 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 (anexele nr. 42, 45, 47—53).

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 (anexa nr. 42) sau împreună cu art. 27 alin. (1) din aceeași lege (anexele nr. 45, 47—53).

Înalta Curte de Casație și Justiție a împărțit această orientare prin deciziile nr. 1.989 din 13 mai 2011 (anexa nr. 42), nr. 3.354 din 3 octombrie 2011 (anexa nr. 45), nr. 2.094 din 27 mai 2010 (anexa nr. 47), nr. 3.503 din 7 octombrie 2010 (anexa nr. 50), nr. 1.457 din 16 aprilie 2010 (anexa nr. 51) și nr. 3.408 din 5 octombrie 2011 (anexa nr. 53).

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 (anexele nr. 2—30, 54).

Instanțele care au împărțit 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 și art. 27 alin. (1) din Legea nr. 365/2002.

Înalta Curte de Casație și Justiție a împărțit această orientare prin deciziile nr. 251 din 26 ianuarie 2011 (anexa nr. 3), nr. 1.090 din 25 martie 2008 (anexa nr. 4), nr. 2.834 din 17 septembrie 2008 (anexa nr. 12), nr. 1.350 din 9 aprilie 2010

(anexa nr. 13), nr. 2.223 din 12 iunie 2009 (anexa nr. 15), nr. 2.991 din 1 martie 2010 (anexa nr. 16), nr. 3.942 din 26 noiembrie 2009 (anexa nr. 17), nr. 666 din 22 februarie 2011 (anexa nr. 22), nr. 3.889 din 23 noiembrie 2009 (anexa nr. 23), nr. 4.044 din 15 noiembrie 2011 (anexa nr. 25), nr. 591 din 16 februarie 2011 (anexa nr. 27) și nr. 1.681 din 14 mai 2008 (anexa nr. 29).

În ipoteza folosirii cardului autentic, fără consimțământul titularului său, pentru retragerea de numerar de la ATM fapta a fost încadrată, exclusiv, în dispozițiile art. 27 alin. (1) din Legea nr. 365/2002 (anexele nr. 31—38).

A fost arătată opinia procurorului general al Parchetului de pe lângă Înalta Curte de Casație și Justiție, în sensul orientării jurisprudențiale potrivit căreia 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.

Cât privește folosirea la bancomat, pentru retrageri de numerar sau orice alte operațiuni financiare, a unui card falsificat sau a unui real, fără consimțământul titularului său, fapta întrunește elementele constitutive ale infracțiunii prevăzute de art. 42 alin. (1), (2) și (3) din Legea nr. 161/2003, săvârșită în concurs ideal cu cea prevăzută la art. 24 alin. (2) din Legea nr. 365/2002 sau art. 27 alin. (1) din aceeași lege, după caz.

Președintele Înaltei Curți de Casație și Justiție, doamna judecătoarea Livia Doina Stanciu, a declarat debaterile închise, iar completul de judecată a rămas în pronunțare asupra recursului în interesul legii.

ÎNALTA CURTE,

deliberând asupra recursului în interesul legii, cu privire la interpretarea și aplicarea art. 42 alin. (1), (2) și (3) din Legea nr. 161/2003 (acces fără drept la un sistem informatic), determinat de diferențierea practică între:

- montarea la ATM a dispozitivelor de citire a benzii magnetice a cardului autentic și a codului PIN aferent acestuia;
 - folosirea la bancomat a cardului falsificat ori chiar a celui autentic, fără acordul titularului său,
- constată următoarele:

1. Problema de drept care a generat practica neunitară

Prin recursul în interesul legii formulat de procurorul general al Parchetului de pe lângă Înalta Curte de Casație și Justiție s-a arătat că în practica judiciară națională nu există un punct de vedere unitar cu privire la înțelesul noțiunii de acces fără drept la un sistem informatic și, în consecință, au fost formulate soluții divergente cu privire la încadrarea juridică dată faptelor atunci când se montează la ATM dispozitivele de citire a benzii magnetice a cardului autentic și a codului PIN aferent acestuia, precum și atunci când se folosește la bancomat cardul falsificat ori cel autentic, fără acordul titularului său.

2. Examenul jurisprudențial

Prin recursul în interesul legii se arată că în urma verificării jurisprudenței la nivel național a fost relevată o practică neunitară în interpretarea și aplicarea art. 42 alin. (1), (2) și (3) din Legea nr. 161/2003 cu privire la înțelesul noțiunii de acces fără drept la un sistem informatic. Procurorul general a menționat în sesizarea scrisă faptul că cele mai multe instanțe au menținut încadrarea juridică din actul de sesizare, fără a pune în discuție și fără a se pronunța în mod expres asupra problemei de drept supuse prezentului recurs în interesul legii.

2.1. *Soluțiile pronunțate de instanțele judecătorești cu privire la montarea la ATM a dispozitivelor de citire a benzii magnetice a cardului autentic și a codului PIN aferent acestuia*

2.1.1. *Jurisprudență în sensul lipsei accesului la un sistem informatic și incidenței art. 25 din Legea nr. 365/2002.* Opinia trimisă de procurorul general arată că, într-o primă orientare a

practicii, unele instanțe au considerat că montarea dispozitivelor de citire a benzii magnetice a cardului autentic, a videocamerei sau a falsei tastaturi nu constituie acces fără drept la un sistem informatic, infracțiune prevăzută de art. 42 alin. (1) din Legea nr. 161/2003 (anexele nr. 1, 3, 43—45, 55).

Instanțele au încadrat fapta în art. 25 din Legea nr. 365/2002, reținându-se că inculpații „au deținut echipamente electronice apte să citească și să memoreze date din cărțile de credit, în scopul obținerii acelor date care permit retragerea sumelor de bani din cărțile de credit” (anexa nr. 44).

2.1.2. Jurisprudență în sensul deținerii fără drept a unui dispozitiv conceput sau adaptat în scopul săvârșirii uneia dintre infracțiunile prevăzute de art. 42—45 din Legea nr. 161/2003. De asemenea, procurorul general arată că într-o a doua orientare s-a apreciat că „fapta inculpatului de a atașa la un ATM un dispozitiv format dintr-un telefon mobil prevăzut cu cameră video și card de memorie cu un suport menit a susține și disimula telefonul în plafonul bancomatului, în scopul de a înregistra codul PIN tastat de utilizatorii acestuia, întrunește elementele constitutive ale infracțiunii prevăzute de art. 46 alin. (2) din Legea nr. 161/2003, reprezentând deținerea fără drept a unui dispozitiv conceput sau adaptat în scopul săvârșirii uneia dintre infracțiunile prevăzute de art. 42—45 din aceeași lege” (anexa nr. 55).

În opinia transmisă de către procurorul general se arată că cele mai multe instanțe au menținut încadrarea juridică din actul de sesizare fără a pune în discuție și fără a se pronunța în mod expres asupra problemei de drept supuse prezentului recurs.

2.1.3. Jurisprudență în sensul existenței accesului la un sistem informatic. Într-o a treia orientare a practicii, s-a reținut că prin montarea la bancomat a dispozitivelor de citire a informațiilor înregistrate pe banda magnetică a cardului și 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 (anexele nr. 39—41, 46—47).

În argumentarea acestei opinii, instanțele au apreciat că „ATM-ul este un mijloc de colectare, prelucrare și transmitere a unor date informatice, reprezentate de numărul de cont al titularului, care este stocat pe nivelul doi al benzii magnetice. Pe de altă parte, prin montarea skimmerului în fanta bancomatului, prin care se introduce cardul și se realizează citirea benzii magnetice a fiecărui card în parte, stocându-se informația astfel obținută, au fost încălcate măsurile de securitate care aveau drept scop asigurarea secretului numărului de cont și a operațiunilor efectuate și apărarea împotriva folosirii de către o altă persoană a acestor carduri în vederea fraudării. În consecință, inculpații au accesat fără drept un sistem informatic, încălcând astfel măsurile de securitate”, astfel că sunt întrunite elementele constitutive ale infracțiunii prevăzute de art. 42 alin. (1) și (3) din Legea nr. 161/2003 (anexa nr. 46).

2.1.4. Cu aceeași motivare, alte instanțe au reținut ca incidente, pentru această situație de fapt, dispozițiile art. 44 alin. (2), (3) și art. 46 alin. (2), alături de cele ale art. 42 alin. (2) și (3) din Legea nr. 161/2003 (anexele nr. 39, 41, 46, 47).

În argumentarea acestei opinii, instanțele au apreciat că atât videocamera, cât și skimmerul au fost deținute în scopul menționat de art. 46 alin. (2) din Legea nr. 161/2003.

La același punct de vedere au aderat și instanțele, 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” (anexa nr. 16).

2.2. Soluțiile pronunțate de instanțele judecătorești cu privire la folosirea la bancomat a cardului falsificat ori chiar a celui autentic, fără acordul titularului său

2.2.1. Jurisprudență în sensul reținerii accesului la un sistem informatic. Într-o primă orientare jurisprudențială unele instanțe au ajuns la concluzia că fapta întrunește elementele constitutive ale infracțiunii prevăzute de art. 42 alin. (1) și (3) din Legea nr. 161/2003 (anexele nr. 42, 45, 47—53).

Acest punct de vedere a fost argumentat pe dispozițiile art. 35 din Legea nr. 161/2003. Bancomatul este un 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 art. 42 alin. (1) și (3) din Legea nr. 161/2003 în concurs cu art. 24 alin. (2) din Legea nr. 365/2002 (anexa nr. 42) sau în concurs cu art. 24 alin. (2) și art. 27 alin. (1) din Legea nr. 365/2002 (anexele nr. 45, 47—53).

2.2.2. Jurisprudență în sensul lipsei accesului la un sistem informatic. 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 (anexele nr. 2—30, 54).

Instanțele care au împărțit 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 art. 24 alin. (1) și (2), art. 25 și art. 27 alin. (1) din Legea nr. 365/2002 (anexele nr. 3, 4, 12, 13, 15, 16, 17, 22, 23, 25, 27, 29).

2.2.3. Jurisprudență în sensul reținerii art. 27 alin. (1) din Legea nr. 365/2002. În ipoteza folosirii cardului autentic, fără consimțământul titularului său, pentru retragerea de numerar de la ATM fapta a fost încadrată, exclusiv, în dispozițiile art. 27 alin. (1) din Legea nr. 365/2002 (anexele nr. 31—38).

3. Opinia procurorului general

3.1. Soluția problemei de drept

Soluția propusă de către procurorul general al Parchetului de pe lângă Înalta Curte de Casație și Justiție este în sensul că:

— încadrarea juridică pentru fapta de a monta la bancomat dispozitive de citire a benzii magnetice a cardului, minivideocamere sau dispozitive tip tastatură este aceea prevăzută de art. 46 alin. (2) din Legea nr. 161/2003;

— încadrarea juridică pentru fapta de a folosi la bancomat pentru retrageri de numerar sau orice alte operațiuni financiare un card falsificat sau un card real, fără consimțământul titularului său, este aceea prevăzută de art. 42 alin. (1), (2) și (3) din Legea nr. 161/2003, în concurs ideal cu art. 24 alin. (2) din Legea nr. 365/2002 (falsificarea instrumentelor de plată electronică) sau art. 27 alin. (1) din Legea nr. 365/2002 (efectuarea de operațiuni financiare în mod fraudulos).

3.2. Înțelesul unor termeni

În opinia transmisă de către procurorul general sunt definite noțiunile de *acces la un sistem informatic*, *skimming* și *card*.

Accesul la un sistem informatic este definit ca intrarea în tot sau numai într-o parte a sistemului informatic, metoda de comunicare fiind fără 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.

Cardul emis de o instituție de credit reprezintă un instrument de plată electronică, respectiv un suport de informație standardizat, securizat și individualizat, care permite

deținătorului său să folosească disponibilitățile bănești proprii dintr-un cont deschis pe numele lui la emitentul cardului și/sau să utilizeze o linie de credit (în limita unui plafon stabilit în prealabil) deschisă de emitent în favoarea deținătorului cardului, în vederea efectuării uneia sau a mai multora dintre următoarele operațiuni: retragerea sau depunerea de numerar de la terminale precum ATM-uri, ghișeele emitentului sau ale unei alte instituții obligate 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: banda magnetică ce 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 trei 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; codul CVV2 (pentru cardul VISA) și codul CVC2 (pentru cardul MASTERCARD) reprezintă un număr format din trei 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 pe fața cardului, putând fi format din întreg acest număr sau din ultimele sale patru cifre.

Skimmingul 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 înmănat de către titular unei alte persoane (de regulă, un comerciant în timpul 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 *skimmerul* 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-videocamere și/sau de dispozitive modificate de tip tastatură (*keypads*) care înregistrează codul PIN aferent cardului, în momentul tastării acestuia.

3.3. *Cu privire la montarea la bancomat a dispozitivelor de citire a benzii magnetice a cardului autentic și a codului PIN aferent acestuia (mini-videocamere sau dispozitive tip tastatură), procurorul general apreciază că sunt întrunite elementele constitutive ale infracțiunii prevăzute de art. 46 alin. (2) din Legea nr. 161/2003.*

În opinia înaintată Înaltei Curți se arată 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 videocamerei 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.

Articolul 42 din Legea nr. 161/2003 incriminează fapta de acces ilegal la un sistem informatic într-o variantă-tip, în alin. (1)

și în două variante agravate, în alin. (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.

Elementul material al laturii obiective se realizează prin accesul fără drept într-un sistem informatic: stație de lucru, server ori rețea informatică.

Accesul fără drept la un sistem informatic presupune o interacțiune a făptuitorului cu tehnica de calcul. Prin intermediul echipamentelor agentul trimite solicitări către UCP (unitatea centrală de prelucrare) a sistemului, care va procesa date ori va rula programe de aplicații în beneficiul intrusului. Urmarea imediată constă într-o stare de pericol cu privire la siguranța sistemului informatic și/sau a resurselor sale. Dacă scopul accesului neautorizat a fost obținerea de date informatice, starea de pericol este dublată de atingerea adusă protecției datelor informatice stocate sau prelucrate de acesta. Încălcarea măsurilor de securitate determină o transformare efectivă adusă obiectului material al infracțiunii, și anume entităților materiale care compun sistemele informatice (calculatoare, rețele de calculatoare, elemente hardware — echipamente periferice, cabluri, plăci, servere etc. și software — programe, aplicații, baze de date etc.) sau datelor informatice vizate. 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”. Legătura de cauzalitate între activitatea făptuitorului și urmarea produsă rezultă *ex re*, în cazul accesului neautorizat în formă simplă, respectiv trebuie demonstrată forțarea măsurilor de securitate (parole, coduri de acces etc.), în cazul formelor agravate.

Obținerea datelor de pe banda magnetică a cardului 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.

Articolul 42 din Legea nr. 161/2003 incriminează accesul fără drept la un sistem informatic. 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 fac 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 și nu își îndeplinește rolul de parte a unui sistem informatic.

Citirea benzii magnetice a cardului autentic nu este condiționată de atașarea *skimmerului* la bancomat. Citirea benzii magnetice se face și printr-un dispozitiv de citire manual, 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 din cauza unei împrejurări extranece vreunei norme de incriminare — atașarea sau neatașarea *skimmerului* la bancomat.

Așadar, operațiunea de citire a datelor de pe banda magnetică a cardului, prin atașarea *skimmerului* la bancomat, nu interacționează în niciun fel cu softul bancomatului, nu se realizează nicio solicitare către unitatea centrală de prelucrare

a sistemului, care să proceseze date ori să ruleze programe de aplicații în beneficiul făptuitorului, astfel că infracțiunea de acces fără drept la sistemul informatic este lipsită de însuși elementul său material.

3.4. *Cu privire la folosirea la bancomat, pentru retrageri de numerar sau orice alte operațiuni financiare, a cardului falsificat ori chiar a celui autentic fără acordul titularului său, procurorul general apreciază că sunt întrunite elementele constitutive ale infracțiunii prevăzute de art. 42 alin. (1), (2) și (3) din Legea nr. 161/2003, în concurs ideal cu art. 24 alin. (2) din Legea nr. 365/2002 (dacă este un card falsificat) sau art. 27 alin. (1) din Legea nr. 365/2002 (dacă este un card real folosit fără acordul proprietarului său), după caz.*

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. Folosit conform destinației sale, bancomatul face parte din sistemul informatic bancar, datele transmise și receptate de acest dispozitiv fiind protejate prin măsuri de securitate încorporate în sistemul de citire a cardurilor și în codul PIN. În cazul folosirii la ATM a cardului falsificat sau a celui real fără consimțământul titularului său se realizează un acces fără drept la sistemul informatic. De această dată bancomatul este folosit conform destinației sale: introducerea cardului și tastarea codului PIN (prin această din urmă operațiune înlăturându-se măsura de securitate reprezentată de codul de acces), în posesia cărora făptuitorul se află în mod nelegal, determinând „recunoașterea” de către bancomat a cardului falsificat ca fiind un card valid și permițând astfel un schimb de informații între posesorul cardului și mediul de stocare a datelor privitoare la contul bancar, atașat cardului „recunoscut”. Chiar dacă activitatea infracțională s-ar opri aici, nefiind solicitată nicio operațiune financiară, infracțiunea de acces fără drept la un sistem informatic este consumată.

Făptuitorul transmite prin intermediul componentelor sistemului (tastatură) 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 amenințată. Legătura de cauzalitate dintre acțiunea făptuitorului și urmarea produsă datelor informatice rezultă din însăși materialitatea faptei. Cât privește latura subiectivă, fapta este săvârșită cu intenție.

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 același 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 săvârșirii uneia dintre infracțiunile prevăzute la art. 42—45. Skimmerul, videocamera și falsa tastatură de bancomat sunt dispozitive deținute în scopul săvârșirii unui acces fără drept la sistemul informatic, iar datele informatice și 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 și în cazul folosirii unui skimmer atașat la bancomat, dar și în cazul obținerii datelor de pe banda magnetică a cardului cu ajutorul unui hand-skimmer.

Legea nr. 161/2003 sancționează infracțiuni îndreptate contra confidențialității și integrității datelor și sistemelor informatice, în timp ce Legea nr. 365/2002 privind comerțul

electronic prevede infracțiuni îndreptate împotriva securității și 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 aceeași lege sancționează efectuarea de operațiuni financiare prin utilizarea unui instrument de plată, fără consimțământul titularului său.

Pe de altă parte, art. 25 din Legea nr. 365/2002 (reținut greșit de unele instanțe în cazul montării la ATM a dispozitivelor de citire a benzii magnetice a cardului autentic și 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, de 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 skimmingului este obținerea de date informatice, desigur lipsite de existență materială, care pot fi ulterior folosite pentru inscripționarea unor carduri clonate, dar și 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 este incident, în cazul montării la ATM a dispozitivelor de citire a benzii magnetice a cardului autentic și a codului PIN aferent acestuia, art. 46 alin. (2) din Legea nr. 161/2003, și nu art. 25 din Legea nr. 365/2002. Cât privește 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) și art. 42 alin. (2) și (3) din aceeași lege, prin copierea datelor de pe banda magnetică a cardului autentic nu se realizează un transfer de date informatice, acestea nu dispar din mediul de stocare, nu părăsesc, prin copiere, banda magnetică de pe care au fost captate.

În concluzie, din analiza textelor legale anterior amintite, rezultă că, în vederea pregătirii săvârșirii infracțiunilor din Legea nr. 365/2002 privind comerțul electronic, se pot săvârși infracțiuni îndreptate împotriva securității datelor sau sistemelor informatice, cum este și aceea de acces ilegal într-un sistem informatic. Așadar, accesul ilegal în sistemul informatic se face, de regulă, în scopul săvârșirii uneia sau mai multora dintre infracțiunile prevăzute de Legea nr. 365/2002 privind comerțul electronic, situație care justifică reținerea unui concurs cu conexitate etiologică în care accesul ilegal reprezintă mijlocul prin care se realizează scopul și anume efectuarea de operațiuni financiare în mod fraudulos.

4. Puncte de vedere solicitate conform art. 414^d din Codul de procedură penală

Au fost solicitate și transmise puncte de vedere cu privire la aspectele tehnice referitoare la situația de fapt, precum și, după caz, cu privire la încadrarea juridică dată faptelor care au suscit o practică neunitară de la Institutul pentru Tehnologii Avansate, Institutul de Cercetări Juridice din cadrul Academiei Române, Departamentul de drept penal din cadrul Facultății de Drept a Universității București, Departamentul de drept public din cadrul Facultății de Drept a Universității „Babeș-Bolyai”, Catedra de drept penal din cadrul Facultății de Drept și Științe Administrative a Universității din Craiova, Facultatea de Drept a Universității „Lucian Blaga” din Sibiu, Departamentul de drept public din cadrul Facultății de Drept a Universității de Vest din Timișoara.

4.1 *Punctul de vedere al Institutului pentru Tehnologii Avansate cu privire la aspectele tehnice din care decurge situația de fapt*

4.1.1. *Înțelesul unor termeni cu privire la montarea la ATM a dispozitivelor de citire a benzii magnetice a cardului autentic și a codului PIN aferent acestuia*

În segmentul terminal, destinat utilizatorilor, activitatea de fraudare presupune instalarea unui sistem de supraveghere format din două componente: un dispozitiv de *skimming*, destinat interceptării și memorării/transmiterii la distanță a datelor înscrise pe banda magnetică a cardurilor bancare, realizat în diferite forme constructive (un montaj electronic disimulat în diverse componente mecanice, potrivite ca formă, dimensiuni și culoare cu echipamentul original cu interfață pentru card bancar pe care se instalează ca, de exemplu, ATM, automat de plată a parcării sau combustibilului, un montaj electronic introdus în interiorul unui echipament tip POS; un dispozitiv artizanal sau comercial, de sine stătător), folosit în mod fraudulos de persoana căreia i-a fost înmănat cardul de către titular, în vederea unei tranzacții (de exemplu, de către recepționar, ospătar etc.); un dispozitiv de achiziție a codului PIN (cuprinde un dispozitiv electronic dotat cu cameră video, de exemplu, telefon mobil, mp4 player cu înregistrare, înregistrator video miniatural, dispozitiv video spion), disimulat în ornamente aflate în apropierea tastaturii la care utilizatorul introduce codul de siguranță și care înregistrează aceste momente sau un ansamblu format dintr-o tastatură falsă, care se montează deasupra tastaturii originale, și un montaj electronic care preia și memorează codul tastat de utilizator.

Montajul electronic din interiorul dispozitivelor tip *skimmer* are o arhitectură alcătuită din: bloc de achiziție a datelor înscrise pe banda magnetică a cardurilor, reprezentat în general de un cap magnetic de citire cu una, două sau trei piste; bloc de conversie a semnalului analogic provenit de la capul magnetic în semnal digital, reprezentat în general de un circuit integrat de interfață de cap magnetic; bloc de prelucrare a datelor, reprezentat în general de un microcontroler de uz general; bloc de memorare a datelor, reprezentat în general de un circuit integrat de memorie nevolatilă, care își păstrează conținutul informațional și după întreruperea alimentării; bloc de comunicație, care realizează legătura și conversia datelor între interfața serială tip UART a microcontrolerului și interfața serială tip RS232 sau tip USB, specifice porturilor seriale ale unui sistem de calcul tip PC (uneori acest bloc este format doar dintr-o interfață hardware tip conector liniar artizanal, la care se leagă un cablu adaptor în care se află circuitul integrat cu funcția de conversie); bloc de alimentare.

Montajul electronic poate fi de tip industrial, provenind dintr-un echipament comercial tip MSR, destinat citirii benzii magnetice a cardurilor, sau poate fi artizanal, realizat după o schemă proprie. În acest ultim caz, proiectantul poate folosi o modalitate de criptare a datelor la stocarea în circuitul de memorie, algoritm implementat prin programul rulat de microcontroler. De asemenea, acesta poate utiliza facilitatea de blocare la citire a programului ce rulează în microcontrolerul dispozitivului și, totodată, implementează o funcție proprie de descărcare a datelor în calculator, care decodifică datele transferate. Astfel, datele din memoria *skimmer*-ului pot fi accesate doar prin cunoașterea algoritmului de criptare din microcontroler și a aplicației ce rulează pe PC.

Cardurile bancare conțin o bandă magnetică structurată, din punct de vedere al organizării datelor, pe 3 piste. Caracteristicile fizice ale cardurilor, dimensiunile, poziția pistelor și modul de înscriere a datelor sunt stabilite în mod unic de standardele ISO 7810, 7811, 7813, precizând densitățile de înregistrare, codarea caracterului și un conținut informațional. Datele informatice înscrise pe primele două piste (împreună cu codul PIN)

reprezintă tot ceea ce este necesar pentru accesarea sistemului informatic al băncii, prin intermediul unor echipamente de tip bancomat sau POS, în vederea efectuării de operațiuni financiare.

În fapt, prin montarea dispozitivelor tip *skimmer* peste fanta de introducere a cardului la un echipament cu interfață de card bancar, se realizează transferul neautorizat de date informatice din mijloacele de stocare a datelor informatice, reprezentate de toate cardurile bancare utilizate de titulari, în perioada în care sunt montate dispozitivele frauduloase.

În limbaj informatic, copierea datelor dintr-un mijloc de stocare a datelor informatice reprezintă un transfer de date, fără a fi necesară ștergerea respectivelor date din mijlocul de stocare.

Dispozitivele electronice dotate cu cameră video și utilizate pentru achiziția codurilor PIN provin, în marea majoritate a cazurilor analizate, din echipamente comerciale de uz general (telefoane mobile, mp4 playere cu înregistrare, înregistratoare video miniaturale, dispozitive video spion etc.), cărora le sunt îndepărtate carcusele, pentru reducerea dimensiunilor, iar acumulatorii originali sunt înlocuiți cu ansambluri de acumulatori cu durată de funcționare mărită.

Poziționarea camerelor video permite vizualizarea, prin intermediul obiectivelor optice, a tastaturii echipamentelor cu interfață de card bancar. Dispozitivele în care se stochează înregistrările video ale momentelor în care utilizatorii introduc codul PIN sunt dotate cu memorie nevolatilă (circuite integrate sau carduri de memorie tip microSD), iar cele care transmit la distanță imaginile vizate sunt dotate cu emițătoare radio. Toate dispozitivele comerciale sunt dotate cu interfață serială, în general USB, accesibilă pe un conector standard tip USB, mini USB sau micro USB. Cu ajutorul unui cablu adaptor uzual, înregistrările sunt descărcate ulterior într-un sistem de calcul, iar rezoluția obiectivelor optice permite extragerea informației referitoare la codul PIN.

În cazul montării unei tastaturi false deasupra tastaturii originale a unui echipament dotat cu interfață de card bancar, se urmărește preluarea și memorarea codului PIN tastat de utilizator. Dispozitivul artizanal conține un montaj electronic, a cărui arhitectură este alcătuită din: un bloc de prelucrare a datelor provenite de la tastatura falsă, tip microcontroler; un bloc de memorare; un bloc de comunicație, pentru interfațarea montajului cu un sistem de calcul în vederea descărcării informațiilor; un bloc de alimentare.

Atât dispozitivul dotat cu cameră video, cât și dispozitivul ce încorporează o tastatură falsă permit interceptarea, fără drept, a transmisiei de date informatice care nu este publică și este destinată sistemului informatic al băncii, și anume codul PIN, un cod de securitate introdus de bancă pentru restricționarea accesului utilizatorilor neautorizați la sistemul informatic al băncii.

Există numeroase variante de scheme electrice pentru dispozitivele electronice de fraudare a echipamentelor dotate cu interfață de card bancar. Toate montajele artizanale sau comerciale de citire a benzii magnetice a cardurilor au implementat un modul de ceas real (circuit integrat independent sau funcție internă a microcontrolerului) și introduc o etichetă temporală la fiecare înregistrare corespunzătoare citirii unui card. Dispozitivele comerciale de înregistrare video au, de asemenea, modul de ceas real. Corelarea temporală între înregistrările din memoria dispozitivului de citire a benzii magnetice și momentele de timp la care utilizatorii tastează codul PIN asigură asocierea între informațiile confidențiale corespunzătoare unui card: date informatice înscrise pe banda magnetică și date referitoare la codul de siguranță.

În prezent, se constată tendința de exploatare la distanță atât a dispozitivelor frauduloase pentru interceptarea datelor

memorate pe banda magnetică, cât și a celor pentru codul PIN. În cazul exploatării la distanță, blocurile de memorare și comunicație din schema electrică sunt înlocuite cu un emițător în infraroșu sau radio, care transmite în timp real datele interceptate către un receptor infraroșu/radio, aflat în proximitate și care include o componentă hardware de memorare a datelor. Pentru canalul de comunicație radio pot fi folosite emițătoare artistanale sau comerciale tip bluetooth.

Oricare ar fi modul de realizare a fraudării echipamentelor dotate cu interfață de card bancar, dispozitivele descrise sunt concepute sau adaptate în scopul săvârșirii infracțiunii de acces, fără drept, la un sistem informatic, prin intermediul unor instrumente de plată electronică falsificate sau prin utilizarea, în același scop, a informațiilor obținute prin intermediul acestor dispozitive.

4.1.2. Înțelesul unor termeni cu privire la folosirea la bancomat a cardului falsificat ori chiar a celui autentic, fără acordul titularului său

Falsificarea instrumentelor de plată electronică presupune:

— obținerea, în prealabil, a datelor informatice corespunzătoare unor carduri bancare valide, în orice mod: montare de dispozitive tip skimmer sau furt de baze de date din sistemul informatic al băncii sau ale furnizorilor de servicii;

— înscrierea datelor informatice pe banda magnetică a unor carduri de tip blank, carduri de fidelizare emise de diferite firme, carduri expirate sau sustrase de la titulari etc., cu ajutorul unor echipamente comerciale dedicate înscrierii cartelelor magnetice.

Introducerea unui card bancar falsificat sau a unuia autentic, fără consimțământul titularului său, la un echipament dotat cu interfață de card bancar, realizează accesul, fără drept, la sistemul informatic al băncii, în scopul obținerii de date informatice și cu încălcarea măsurilor de securitate introduse de bancă, indiferent de tipul operațiunii efectuate: interogare, autentificare, retrageri de numerar, transferuri sau orice alte operațiuni financiare. În cazul folosirii datelor de identificare ale cardurilor bancare pentru efectuarea unor tranzacții on-line, se accesează, fără drept, sistemul informatic al băncii, cu încălcarea măsurilor de securitate introduse de bancă.

4.1.3. Soluția tehnică

Montarea la un echipament dotat cu interfață de card bancar a dispozitivelor de citire a benzii magnetice a cardurilor are ca rezultat transferul neautorizat de date informatice din mijloacele de stocare a datelor informatice, reprezentate de cardurile bancare utilizate de titulari, în perioada cât sunt montate dispozitivele frauduloase; scopul final este accesul, fără drept, la sistemul informatic al băncii, pentru obținerea de date informatice și cu încălcarea măsurilor de securitate introduse de bancă.

Montarea dispozitivelor dotate cu cameră video sau tastatură falsă permit interceptarea, fără drept, a transmisiei de date informatice care nu este publică și este destinată sistemului informatic al băncii, și anume codul PIN, un cod de securitate introdus de bancă pentru restricționarea accesului utilizatorilor neautorizați la sistemul informatic al băncii.

Folosirea la un echipament dotat cu interfață de card bancar, a unui card bancar falsificat sau a unuia autentic, fără consimțământul titularului său, precum și folosirea datelor de identificare ale cardurilor bancare pentru efectuarea unor tranzacții on-line realizează accesul, fără drept, la sistemul informatic al băncii, în scopul obținerii de date informatice și cu încălcarea măsurilor de securitate introduse de bancă.

4.2. Punctul de vedere al Institutului de Cercetări Juridice din cadrul Academiei Române cu privire la încadrarea juridică dată faptelor care au suscitată o practică neunitară

4.2.1. Soluția problemei de drept

Punctul de vedere este în sensul soluției propuse pe Parchetul de pe lângă Înalta Curte de Casație și Justiție. Prin

operațiunile de montare a dispozitivelor de citire a benzii magnetice a cardului concomitent cu captarea codului PIN aferent cardului nu se realizează elementul material al laturii obiective a infracțiunii de acces, fără drept, la un sistem informatic prevăzută de art. 42 alin. (1) din Legea nr. 161/2003 care presupune un acces fraudulos, respectiv o intrare fără drept într-un sistem informatic, așa cum s-a arătat și argumentat în cuprinsul motivelor de recurs în interesul legii.

4.2.2. Cu privire la montarea la bancomat a dispozitivelor de citire a benzii magnetice a cardului autentic și a codului PIN aferent acestuia (minivideocamere sau dispozitive tip tastatură)

Deținerea și procurarea instrumentelor, dispozitivelor și mijloacelor prin care urmează să se realizeze latura obiectivă a infracțiunii, precum și activitățile preparatorii întreprinse de viitorul autor al infracțiunii reprezintă acte de pregătire în vederea săvârșirii infracțiunii. Actele de pregătire nu sunt incriminate în legislația penală română, decât prin excepție, atunci când legiuitorul consideră că instrumentele, dispozitivele, mijloacele sau activitățile pregătitoare prezintă, prin ele însele, gradul de pericol social care justifică incriminarea.

În considerarea importanței deosebite a valorii sociale pe care o reprezintă în economia vieții economico-sociale, necesitatea de a se apăra inviolabilitatea sistemului informatic, legiuitorul român a incriminat prin art. 46 alin. (2) deținerea, fără drept, a unui dispozitiv, program informatic, parolă, cod de acces sau dată informatică dintre cele prevăzute la alin. (1) din același text, în scopul săvârșirii uneia dintre infracțiunile prevăzute la art. 42—45 din Legea nr. 161/2003.

Deținerea dispozitivelor de citire a benzii magnetice a cardului, minivideocamerelor sau dispozitivelor tip tastatură și, implicit, montarea acestora pentru citirea benzii magnetice a cardului concomitent cu captarea codului PIN aferent cardului constituie acte pregătitoare în vederea săvârșirii infracțiunii de acces fără drept la un sistem informatic, prevăzute de art. 42 din Legea nr. 161/2003, care, în considerarea gradului mare de pericol social pe care îl prezintă, prin ele însele, au determinat în mod justificat incriminarea lor în textul art. 46 alin. (2) din aceeași lege.

4.3. Punctul de vedere al Departamentului de drept public din cadrul Facultății de Drept a Universității „Babeș Bolyai” cu privire la încadrarea juridică dată faptelor care au suscitată o practică neunitară

4.3.1. Soluția problemei de drept

Cu privire la montarea la bancomat a dispozitivelor de citire a benzii magnetice a cardului autentic și a codului PIN aferent acestuia (minivideocamere sau dispozitive tip tastatură)

a) Montarea dispozitivelor nu implică un acces la bancomat nici măcar în situația în care peste acțiunea agentului de montare a respectivelor dispozitive se suprapune și acțiunea victimei de introducere a cardului bancar în bancomat, moment în care se inițiază procesul de copiere a datelor înscrise pe banda magnetică.

b) Strictea montare a dispozitivelor supuse discuției nu poate oferi aplicabilitate art. 46 alin. (2) din Legea nr. 161/2003 prin raportare la art. 42 alin. (2) și (3) din aceeași lege sau a art. 25 din Legea nr. 365/2002 în baza unei analize *in abstracto*. Aceste încadrări necesită a fi analizate *in concreto*, ținându-se seama de starea de fapt prezentă în fiecare speță în parte. Montarea dispozitivelor implică o deținere a acestora, ce reprezintă în sensul legii un act preparator care poate viza comiterea unei multitudini de infracțiuni. Din acest considerent nu se poate analiza *in abstracto* comportamentul agentului, deoarece o asemenea analiză ar evidenția echivocitatea actului preparator, respectiv nu s-ar putea identifica cu certitudine care a fost scopul deținerii respectivelor dispozitive.

Singura încadrare juridică care ar putea fi reținută *de plano*, în baza unei analize *in abstracto*, este cea prevăzută de art. 46

alin. (2) din Legea nr. 161/2003 prin raportare la art. 44 alin. (3) din aceeași lege (deținerea skimmerului în vederea transferului de date de pe banda magnetică a instrumentului de plată electronică, privit ca mijloc de stocare).

c) Montarea dispozitivelor, urmată de acțiunea victimei de introducere a cardului în bancomat, atrage un concurs real între infracțiunea prevăzută de art. 46 alin. (2) din Legea nr. 161/2003 și art. 44 alin. (3) din aceeași lege.

Cu privire la folosirea la bancomat, pentru retrageri de numerar sau orice alte operațiuni financiare a cardului falsificat ori chiar a celui autentic, fără acordul titularului său

a) Retragerea de numerar fără drept de la bancomat determină un concurs real între infracțiunea prevăzută de art. 42 alin. (2) și (3) din Legea nr. 161/2003 și cea prevăzută de art. 27 alin. (1) din Legea nr. 365/2002. În situația în care cel care clonează cardul, îl utilizează în vederea retragerii de numerar, se va afla sub incidența art. 27 alin. (1) din Legea nr. 365/2002.

b) În măsura în care cel care clonează cardul nu utilizează cardul personal, ci îl înmânează unei terțe persoane, ori doar îl deține în acest scop, complicitatea materială (dacă respectivul card este folosit) va fi sancționată printr-un text distinct, respectiv art. 24 alin. (2) din Legea nr. 365/2002.

4.3.2. Înțelesul unor termeni

În opinia transmisă este definit accesul la un sistem informatic, deoarece soluțiile contradictorii întâlnite în practica judiciară referitoare la încadrarea faptei de *montare la ATM a dispozitivelor de citire a benzii magnetice a cardului autentic și a codului PIN aferent acestuia* sunt determinate în principal de modul în care a fost interpretată noțiunea.

Accesul la un sistem informatic a fost definit ca intrarea în tot sau numai într-o parte a sistemului informatic. Această descriere nu poate fi acceptată ca fiind o definiție susceptibilă să clarifice conținutul noțiunii. Nu se poate afirma că accesul, în sensul legii, desemnează intrarea în tot sau numai într-o parte a sistemului informatic, deoarece Legea nr. 161/2003 nu definește noțiunea. Definirea accesului prin intrarea în tot sau în parte nu clarifică în nicio măsură conținutul termenului având în vedere că ne raportăm la un mediu virtual și la interacțiuni logice, intrarea în sistemul informatic nefiind realizată la nivel fizic.

Sintagma *intrarea în tot sau în parte* este utilizată de Convenția privind criminalitatea informatică fără să fie definită însă noțiunea de acces. Sintagma în cauză (într-o formă similară) este utilizată la art. 2 din Convenție, *accesarea ilegală*, pentru a se sublinia faptul că întinderea accesului este irelevantă sub aspectul încadrării juridice. De exemplu, se poate discuta despre un veritabil acces chiar dacă agentul rămâne restricționat într-o anumită parte a sistemului informatic, acesta putând utiliza doar anumite aplicații ori fișiere stocate pe acesta, restul necesitănd o autorizare specială (sunt parolate, pot fi accesate doar de un anumit utilizator etc.).

În doctrină pot fi întâlnite două puncte de vedere cu privire la definirea noțiunii de acces la un sistem informatic:

a) O primă definiție ar putea fi cea de inspirație americană, întâlnită și în doctrina din România, unde accesul este văzut ca reprezentând capacitatea de a da comenzi, de a cauza introducerea, obținerea, afișarea, stocarea ori diseminarea de date informatice sau folosirea în orice alt mod a resurselor unui calculator, sistem ori rețea informatică sau comunicarea cu unitățile sale aritmetice, logice ori de memorie (I. Vasii, L. Vasii, Contaminanții informatici ca vector ai accesului ilegal, în Revista de drept penal, nr. 2/2006, p. 37).

Definiția nu este totuși lipsită de critică, deoarece înșiruirea de acte materiale susceptibile să ofere contur unui acces la un sistem informatic oferă un conținut mult prea larg acestei noțiuni. Capacitatea de a da comenzi ar acoperi și ipoteze care au fost excluse în mod expres prin Raportul explicativ al Convenției privind criminalitatea informatică din sfera infracțiunii de acces

la un sistem informatic (paragraful 46 din Raportul explicativ), ca, de exemplu, *trimiterea unui e-mail nesolicitat*, care din punct de vedere tehnic semnifică o interacțiune la nivel logic între sistemul informatic utilizat de agent și sistemul informatic ce găzduiește serviciul de poștă electronică utilizat de persoana care recepționează respectivul e-mail. Mai mult, această interacțiune logică implică inclusiv darea unei comenzi (în momentul în care acel e-mail urmează să fie salvat pe sistemul informatic ce găzduiește serviciul de poștă electronică a destinatarului).

Prin urmare, ne-am afla în situația evidentă în care o definiție mult prea generoasă s-ar afla în contradicție cu intenția legiuitorului european, intenție care a fost transpusă în dreptul intern în mod fidel în urma adoptării Legii nr. 161/2003.

b) O a doua definiție privește accesul ca fiind o interacțiune logică (deci nu orice fel de interacțiune) ce se manifestă prin aceea că agentul poate beneficia de resursele ori/și funcțiile sistemului informatic (a se vedea G. Zlati, Unele aspecte în legătură cu infracțiunile informatice din perspectiva legislației în vigoare, precum și a Noului Cod penal, în Dreptul, nr. 10/2012, p. 221).

Atunci când se discută despre un acces local (de exemplu, agentul interacționează în mod direct cu un laptop) și nu unul de la distanță (de exemplu, agentul utilizează o rețea wireless ori internetul pentru a obține un acces fără drept la un laptop conectat la respectiva rețea wireless ori la internet), se interacționează și la nivel fizic cu sistemul informatic. Practic, agentul, prin interacțiunea fizică cu sistemul informatic (pornirea acestuia, transmiterea unor comenzi prin utilizarea tastaturii etc.), oferă contur și unei interacțiuni la nivel logic. Cu titlu de exemplu, interacțiunea fizică a agentului cu tastatura inițiază o interacțiune logică, sistemul informatic vizat ajungând să recepționeze informația transmisă de agent prin intermediul tastaturii, să o interpreteze cu ajutorul unui program informatic și să returneze un răspuns. O interacțiune logică poate avea la bază și o interacțiune fizică, dar o interacțiune fizică nu implică în mod necesar și o interacțiune logică.

Este posibil ca interpretarea eronată a noțiunii de acces să aibă drept premisă exemplele oferite de Raportul explicativ la care s-a făcut trimitere mai sus. Paragraful 46 din Raportul explicativ descrie accesul la un sistem informatic ca fiind o formă de intrare, exemplele oferite în acest sens plasând acțiunea de intrare în legătură cu elemente precum componente hardware, date informatice, directoare etc. Cu toate acestea, nu s-ar putea susține că un acces la un sistem informatic se conturează atunci când agentul realizează o acțiune de intrare vizavi de o componentă hardware. O asemenea abordare denotă mai degrabă o incongruență logică, deoarece nu se poate imagina o ipoteză în care agentul să intre într-o componentă hardware. Prin urmare, singura interpretare adecvată a noțiunii de acces trebuie să aibă drept premisă o interacțiune strict la nivel logic cu respectivul sistem informatic. Trimiterea la componentele hardware este relevantă doar în contextul în care interacțiunea logică se realizează prin intermediul interacțiunii cu o componentă hardware (interacțiunea agentului cu tastatura, cu butonul de pornire al sistemului informatic etc.).

4.3.3. *Cu privire la montarea la bancomat a dispozitivelor de citire a benzii magnetice a cardului autentic și a codului PIN aferent acestuia (minivideocamere sau dispozitive tip tastatură)*

Montarea dispozitivelor de citire a benzii magnetice (skimmer) și a videocamerei ori a falsei tastaturi nu constituie un acces la un sistem informatic.

a) Atunci când agentul doar montează respectivele dispozitive fără ca victima să introducă în skimmer cardul autentic și să tasteze codul PIN ce urmează a fi înregistrat fie de videocamera plasată de agent, fie de falsa tastatură poziționată de acesta peste tastatura legitimă a bancomatului. În această

ipoteză este exclusă posibilitatea unui acces la sistemul informatic, deoarece agentul nu face decât să mascheze aceste dispozitive în așa fel încât victima să nu realizeze că urmează să interacționeze cu alte dispozitive decât cele legitime, ale bancomatului. Între aceste dispozitive și bancomat nu există absolut nicio interacțiune la nivel logic. Toate dispozitivele funcționează în mod independent (sunt dispozitive stand alone, fiind alimentate din surse proprii).

b) O a doua ipoteză este aceea în care peste acțiunea agentului de a monta skimmerul se suprapune și acțiunea victimei de introducere a instrumentului de plată electronică în fanta bancomatului. Din punct de vedere tehnic, în această fază skimmerul interacționează cu banda magnetică a cardului introdus de victimă, realizându-se o copie a datelor înscrise pe banda magnetică în memoria internă a skimmerului. Este posibil și ca skimmerul să transmită la distanță datele obținute de pe banda magnetică fie prin wireless, fie prin bluetooth. În acest caz, stocarea datelor de pe banda magnetică se realizează pe un terț mediu de stocare și nu în memoria internă a skimmerului.

La fel ca și în prima ipoteză analizată, este exclusă identificarea unui acces la sistemul informatic, deoarece lipsește o interacțiune la nivel logic între dispozitivele montate de agent și dispozitivele bancomatului. Dispozitivele montate de agent obțin datele înscrise pe banda magnetică și codul PIN utilizând funcții proprii, iar bancomatul nu are niciun rol în acest proces de copiere/captare a datelor. Atât obținerea datelor de pe banda magnetică, cât și captarea codului PIN se realizează în exteriorul bancomatului. Un skimmer poate să copieze datele înscrise pe banda magnetică chiar dacă nu este atașat unui bancomat ori bancomatul unde a fost plasat skimmerul are o defecțiune tehnică și nu funcționează.

Analiza elementelor constitutive ale infracțiunii prevăzute de art. 42 din Legea nr. 161/2003 relevă așadar lipsa unui element esențial din structura laturii obiective, respectiv accesul. În cadrul mai general al operațiunii de skimming se realizează un acces la bancomat, însă acesta este realizat de victimă, după ce copierea datelor de pe banda magnetică s-a realizat. Astfel, victima, în momentul în care introduce cardul în fanta bancomatului interacționează cu skimmerul agentului, moment în care se inițiază procesul de copiere a datelor. Imediat după acest moment, cardul ajunge să interacționeze cu dispozitivul legitim de citire al bancomatului moment în care victima ajunge să interacționeze cu bancomatul prin intermediul tastaturii ori tastelor acestuia. Acesta este momentul în care putem discuta despre un acces la un sistem informatic.

În acest caz, accesul este realizat de victimă în mod licit, aceasta având dreptul de a interacționa cu bancomatul. Accesul se realizează după ce datele au fost deja copiate de skimmer, moment în care acesta și-a încetat orice fel de interacțiune cu cardul victimei și implicit cu aceasta. Punctul de vedere conform căruia nu discutăm despre un acces la un sistem informatic se regăsește în doctrină (G. Zlati, Unele aspecte în legătură cu infracțiunile informatice din perspectiva legislației în vigoare, precum și a Noului Cod penal, în Dreptul, nr. 10/2012, p. 218—221). În doctrină s-a exprimat și punctul de vedere contrar (C. Duvac, Accesul ilegal la un sistem informatic în reglementarea Noului Cod penal, în RRDP1, nr. 1/2012, p. 96), în sensul existenței unui acces fără drept la un sistem informatic, autorul achiesând la soluțiile instanțelor de judecată ce au statuat în acest sens.

Plasarea unor asemenea dispozitive nu poate în nicio ipoteză să atragă tipicitatea infracțiunii prevăzute de art. 42 din Legea nr. 161/2003. În acest sens, unele instanțe au considerat că ne aflăm sub incidența prevăzută de art. 25 din Legea nr. 365/2002, în timp ce altele au plasat acest comportament sub incidența art. 46 alin. (2) din Legea nr. 161/2003. Ambele

infracțiuni reprezintă incriminarea unor acte preparatorii. Astfel, dacă în cazul art. 25 din Legea nr. 365/2002 discutăm despre deținerea unor echipamente în vederea comiterii infracțiunii prevăzute de art. 24 (falsificarea instrumentelor de plată electronică), în cazul art. 46 alin. (2) din Legea nr. 161/2003 discutăm despre deținerea de echipamente în scopul comiterii infracțiunilor prevăzute de art. 42—45 din aceeași lege.

Punctul de vedere transmis de către procurorul general are în vedere că este incident art. 46 alin. (2) din Legea nr. 161/2003 și nu art. 25 din Legea nr. 365/2002. Argumentul pentru care s-a considerat că nu poate primi aplicabilitate art. 25 din Legea nr. 365/2002 a fost acela că prin acesta se incriminează deținerea de dispozitive în scopul clonării unui instrument de plată electronică. Or, este evident că intenția agentului poate fi nu doar aceea de a clona instrumentul de plată electronică, ci și de a utiliza datele obținute de pe banda magnetică în vederea efectuării unor plăți on-line. Încadrarea juridică nu poate fi reținută însă *de plano și in abstracto ca fiind cea prevăzută de art. 46 alin. (2) din Legea nr. 161/2003*. Practic, analiza trebuie făcută *in concreto*, în funcție de starea de fapt a fiecărei spețe în parte. Este așadar posibil ca întreaga activitate a agentului să contureze intenția acestuia de a utiliza datele obținute prin utilizarea skimmerului în vederea clonării instrumentului de plată electronică, astfel încât reținerea art. 25 din Legea nr. 365/2002 nu este exclusă, ci doar necesită a fi analizată în funcție de circumstanțele speței supuse discuției.

În consecință:

a) montarea dispozitivelor supuse discuției nu implică un acces la bancomat nici atunci când peste acțiunea agentului de montare a respectivelor dispozitive se suprapune și acțiunea victimei de introducere a cardului bancar în bancomat, moment în care se inițiază procesul de copiere a datelor înscrise pe banda magnetică;

b) încadrarea juridică care ar putea fi reținută *de plano*, în baza unei analize *in abstracto*, este cea prevăzută de art. 46 alin. (2) din Legea nr. 161/2003 prin raportare la art. 44 alin. (3) din aceeași lege (deținerea skimmerului în vederea transferului de date de pe banda magnetică a instrumentului de plată electronică, privit ca mijloc de stocare);

c) montarea dispozitivelor, urmată de acțiunea victimei de introducere a cardului în bancomat dă naștere unui concurs real între infracțiunea prevăzută de art. 46 alin. (2) din Legea nr. 161/2003 și art. 44 alin. (3) din aceeași lege. Transferul de date dintr-un sistem informatic are drept premisă accesarea acestuia, iar un acces la bancomat este exclus în baza argumentelor deja menționate, astfel încât nu poate fi reținută și infracțiunea prevăzută de art. 44 alin. (2) din Legea nr. 161/2003.

Opinia conform căreia nu putem discuta despre un transfer dintr-un mediu de stocare [art. 44 alin. (3) din Legea nr. 161/2003], deoarece copierea nu face ca respectivele date înscrise pe banda magnetică să dispară, este nefondată, fiind interpretată în mod eronat noțiunea de transfer, care nu are la bază în mod obligatoriu ștergerea datelor de pe mediul de stocare prin relocarea acestora într-un alt mediu de stocare pe un sistem informatic terț. Este posibil ca această confuzie să aibă drept izvor o analiză doctrinară (a se vedea M.A. Hotca, M. Dobrinioiu, Infracțiuni prevăzute în legi speciale. Comentarii și explicații, ediția a 2-a, Ed. C.H. Beck, București, 2010, p. 590—591), unde transferul a fost definit ca fiind mutarea fără drept a reprezentării binare dintr-o locație în altă locație, considerându-se în acest sens că urmarea imediată în cazul transferului de date este ștergerea datelor din locația inițială și crearea concomitentă a unei replici în altă locație. Același autor a revenit recent asupra acestui punct de vedere (a se vedea M. Dobrinioiu, Comentariu, în V. Dobrinioiu ș.a., Noul Cod penal comentat, Partea specială, vol. II, Ed. Universul Juridic, București, 2012, p. 910).

Astfel, s-a considerat că transferul implică o „mutare” a datelor, însă aceasta poate viza două ipoteze: datele vizate sunt fie copiate, fie sunt supuse unui proces de relocare. Se observă așadar o reinterpretare doctrinară a noțiunii de transfer, care nu mai este privită ca implicând o ștergere a datelor din locația inițială (o relocare a acestora), ci și o simplă copiere a datelor fără a mai discuta despre vreo ștergere simultană procesului de duplicare. Această din urmă opinie reflectă intenția legiuitorului, deoarece acesta nu a vizat doar integritatea datelor informatice, ci și confidențialitatea acestora. Mai mult, în momentul în care autorul analizează infracțiunea de transfer neautorizat de date de pe un mijloc de stocare (art. 364 din Noul Cod penal), apreciază că această infracțiune acoperă și situațiile în care discutăm despre copierea datelor înscrise pe banda magnetică a instrumentului de plată electronică prin intermediul skimmerului (M. Dobrinou, Comentariu, în V. Dobrinou ș.a., Noul Cod penal comentat, p. 911—912).

4.3.4. *Cu privire la folosirea la bancomat, pentru retrageri de numerar sau orice alte operațiuni financiare, a cardului falsificat ori chiar a celui autentic, fără acordul titularului său*

Infracțiunea prevăzută de art. 24 alin. (2) din Legea nr. 365/2002 se consumă în momentul introducerii cardului clonat în bancomat, moment în care se poate discuta cel puțin despre o tentativă de acces la un sistem informatic, astfel încât s-ar putea identifica un concurs ideal cu infracțiunea prevăzută de art. 42 alin. (1), (2) și (3) din Legea nr. 161/2003.

În cazul art. 27 alin. (1) din Legea nr. 365/2002 concursul ideal este exclus. Aceasta întrucât, textul de incriminare vizează, în contextul dat, retragerea de numerar de la bancomat. Accesul la bancomat s-ar consuma înainte de a putea discuta despre o tentativă de retragere de numerar. După accesarea bancomatului, agentul trebuie să facă o solicitare de retragere de numerar și să introducă suma ce urmează a fi retrasă. Tentativa prevăzută de art. 27 alin. (5) din Legea nr. 365/2002 ar putea fi reținută însă doar în momentul în care agentul face solicitarea de retragere de numerar, până în acel moment scopul agentului fiind echivoc. Acesta ar putea dori fie schimbarea PIN-ului, fie doar consultarea soldului și nu doar retragerea de numerar. În consecință, agentul realizează două acțiuni: o primă acțiune vizând accesul la bancomat, iar cea de-a doua acțiune retragerea de numerar prin solicitările trimise bancomatului.

Utilizarea bancomatului nu implică o punere în circulație a instrumentului de plată electronică [art. 24 alin. (2) din Legea nr. 365/2002]. Punerea în circulație a unei entități materiale implică prin natura ei pierderea posesiei asupra acelei entități de către titularul inițial al acesteia. În intervalul scurt în care instrumentul de plată electronică se află în bancomat, agentul nu pierde posesia asupra acestuia. Pe de altă parte, nu se poate conchide că intenția legiuitorului prin incriminarea punerii în circulație ori deținerii în vederea punerii în circulație a avut în vedere ipoteza în care instrumentul de plată electronică este folosit la bancomat. Pentru această utilizare, avem o infracțiune distinctă și anume cea prevăzută de art. 27 alin. (1) din Legea nr. 365/2002. În situația în care cel care clonează cardul, îl utilizează în vederea retragerii de numerar, se află sub incidența art. 27 alin. (1) din Legea nr. 365/2002. În măsura în care acesta nu utilizează cardul personal, ci îl înmânează unei terțe persoane ori doar îl deține în acest scop, complicitatea materială (dacă respectivul card este folosit) este sancționată printr-un text distinct, respectiv art. 24 alin. (2) din Legea nr. 365/2002.

Retragerea de numerar fără drept de la bancomat se concretizează într-un concurs real între infracțiunea prevăzută de art. 42 alin. (2) și (3) din Legea nr. 161/2003 și cea prevăzută de art. 27 alin. (1) din Legea nr. 365/2002.

4.4. *Punctul de vedere al Departamentului de drept penal din cadrul Facultății de Drept a Universității București cu privire la încadrarea juridică dată faptelor care au suscitată o practică neunitară*

4.4.1. *Soluția problemei de drept*

a) Deținerea unui dispozitiv de skimming pentru a fi folosit la accesarea sistemului informatic al băncii și obținerea datelor informatice stocate pe cardul bancar constituie infracțiune prevăzută de art. 46 alin. (2) din Legea nr. 161/2003, prin raportare la art. 42 și art. 44 alin. (3) din aceeași lege.

b) Utilizarea dispozitivului de skimming prin montarea la ATM sau POS pentru accesarea sistemului informatic bancar și obținerea datelor informatice stocate pe cardul bancar realizează conținutul constitutiv al infracțiunilor de acces, fără drept, la un sistem informatic săvârșit în scopul obținerii de date informatice și prin încălcarea măsurilor de securitate [art. 42 alin. (1), (2) și (3) din Legea nr. 161/2003] și transfer neautorizat de date dintr-un mijloc de stocare a datelor informatice [art. 44 alin. (3) din Legea nr. 161/2003].

c) În cazul în care dispozitivul de skimming este folosit în mod independent de ATM sau POS pentru a copia informațiile de pe banda magnetică a cardului bancar, fapta reprezintă transfer neautorizat de date dintr-un mijloc de stocare a datelor informatice [art. 44 alin. (3) din Legea nr. 161/2003].

d) Deținerea unor dispozitive optice sau optoelectronice de filmare a introducerilor de coduri PIN pentru efectuarea de autentificări la operațiuni cu cardul la ATM sau POS constituie infracțiune [art. 46 alin. (2), raportat la art. 42—45 din Legea nr. 161/2003].

e) În cazul în care se probează că dispozitivele optice sau optoelectronice de filmare a introducerilor de coduri PIN pentru efectuarea de autentificări la operațiuni cu cardul bancar la ATM sau POS s-au folosit pentru a produce, fără drept, o parolă, un cod de acces sau alte asemenea date informatice care permit accesul total ori parțial la un sistem informatic în scopul săvârșirii uneia dintre infracțiunile prevăzute la art. 42—45, fapta va constitui infracțiunea prevăzută de art. 46 alin. (1) litera b) din Legea nr. 161/2003.

f) Amplasarea unei tastaturi false deasupra tastaturii originale de la ATM sau POS în scopul obținerii codului PIN întrunește elementele constitutive ale infracțiunii de acces fără drept la un sistem informatic în scopul obținerii de date informatice [art. 42 alin. (1) și (2) din Legea nr. 161/2003], în concurs cu interceptarea fără drept a unei transmisii de date informatice (transmiterea codului PIN către bancă) care nu este publică și care este destinată unui sistem informatic [art. 43 alin. (1) din Legea nr. 161/2003].

g) În cazul în care se probează că tastatura falsă de înregistrare a codurilor PIN pentru efectuarea de autentificări la operațiuni cu cardul bancar la ATM sau POS s-a folosit pentru a produce, fără drept, o parolă, un cod de acces sau alte asemenea date informatice care permit accesul total ori parțial la un sistem informatic în scopul săvârșirii uneia dintre infracțiunile prevăzute la art. 42—45, fapta va constitui infracțiunea prevăzută de art. 46 alin. (1) litera b) din Legea nr. 161/2003.

h) Deținerea unei tastaturi false pentru înregistrarea introducerilor de coduri PIN la efectuarea de autentificări pentru operațiuni cu cardul la ATM sau POS constituie infracțiune [art. 46 alin. (2), raportat la art. 42—45 din Legea nr. 161/2003].

i) Folosirea la ATM sau POS a unui card bancar falsificat pentru efectuarea de transferuri de fonduri, altele decât cele ordonate și executate de către instituții financiare, respectiv retrageri de numerar, precum și încărcarea și descărcarea unui instrument de monedă electronică constituie infracțiunea de efectuare de operațiuni financiare în mod fraudulos prin utilizarea unui instrument de plată electronică, inclusiv a datelor

de identificare care permit utilizarea acestuia [art. 27 alin. (2) din Legea nr. 365/2002], în concurs ideal cu infracțiunea de acces, fără drept, la un sistem informatic comisă în scopul obținerii de date informatice prin încălcarea măsurilor de securitate [art. 42 alin. (1), (2) și (3) din Legea nr. 161/2003] și în concurs real cu infracțiunea de falsificare a instrumentelor de plată electronică [art. 24 alin. (1) sau (2) din Legea nr. 365/2002].

j) Folosirea la ATM sau POS a cardului bancar autentic, însă fără acordul titularului său, în scopul efectuării unor transferuri de fonduri, respectiv retrageri de numerar, precum și încărcarea/descărcarea unui instrument de monedă electronică constituie infracțiunea de efectuare de operațiuni financiare în mod fraudulos prin utilizarea unui instrument de plată electronică, inclusiv a datelor de identificare care permit utilizarea acestuia [art. 27 alin. (1) din Legea nr. 365/2002], săvârșită în concurs ideal cu infracțiunea de acces, fără drept, la un sistem informatic comisă în scopul obținerii de date informatice prin încălcarea măsurilor de securitate [art. 42 alin. (1), (2) și (3) din Legea nr. 161/2003].

k) Folosirea informațiilor obținute de pe cardul bancar autentic prin transferarea datelor de pe banda magnetică a acestuia la efectuarea unor transferuri de fonduri prin internet constituie infracțiunea de efectuare de operațiuni financiare în mod fraudulos prin utilizarea neautorizată a oricăror date de identificare sau prin utilizarea de date de identificare fictive [art. 27 alin. (2) din Legea nr. 365/2002].

Soluțiile recomandate pentru interpretarea situațiilor de fapt și realizarea încadrărilor juridice își mențin valabilitatea și după intrarea în vigoare a Noului Cod penal (1 februarie 2014) și abrogarea prevederilor speciale din Legea nr. 161/2003 și Legea nr. 365/2002, urmând a fi aplicabile articolele corespunzătoare din Noul Cod penal.

4.4.2. Înțelesul unor termeni

Situația de fapt (accesul prin intermediul montării la ATM a dispozitivelor de citire a benzii magnetice a cardului autentic și a codului PIN aferent acestuia, respectiv accesul produs prin folosirea la bancomat a cardului falsificat ori chiar a celui autentic, însă fără acordul titularului său) necesită clarificarea unor aspecte de natură tehnică, dar și precizarea terminologiei de specialitate folosite.

Astfel, în art. 35 din Legea nr. 161/2003 sunt prevăzuți termenii și expresiile utilizate în reglementarea titlului din lege privind prevenirea și combaterea criminalității informatice, pentru a defini noțiunile tehnice utilizate și relevante în speță: a) prin *sistem informatic* se înțelege orice dispozitiv sau ansamblu de dispozitive interconectate ori aflate în relație funcțională, dintre care unul sau mai multe asigură prelucrarea automată a datelor, cu ajutorul unui program informatic; b) prin *prelucrare automată a datelor* se înțelege procesul prin care datele dintr-un sistem informatic sunt prelucrate prin intermediul unui program informatic; c) prin *program informatic* se înțelege un ansamblu de instrucțiuni care pot fi executate de un sistem informatic în vederea obținerii unui rezultat determinat; d) prin *date informatice* se înțelege orice reprezentare a unor fapte, informații sau concepte într-o formă care poate fi prelucrată printr-un sistem informatic. În această categorie se include și orice program informatic care poate determina realizarea unei funcții de către un sistem informatic; e) (...); f) prin *date referitoare la traficul informațional* se înțelege orice date informatice referitoare la o comunicare realizată printr-un sistem informatic și produse de acesta, care reprezintă o parte din lanțul de comunicare, indicând originea, destinația, ruta, ora, data, mărimea, volumul și durata comunicării, precum și tipul serviciului utilizat pentru comunicare; g) prin *date referitoare la utilizatori* se înțelege orice informație care poate conduce la identificarea unui utilizator, incluzând tipul de comunicație și serviciul folosit, adresa poștală, adresa geografică, numere de

telefon sau alte numere de acces și modalitatea de plată a serviciului respectiv, precum și orice alte date care pot conduce la identificarea utilizatorului; h) prin *măsuri de securitate* se înțelege folosirea unor proceduri, dispozitive sau programe informatice specializate cu ajutorul cărora accesul la un sistem informatic este restricționat sau interzis pentru anumite categorii de utilizatori; (...).

Dispozitivele de citire a benzii magnetice a cardurilor bancare. Dispozitivele de citire a datelor înscrise pe banda magnetică a cardurilor bancare (dispozitiv de skimming, termen din limba engleză însemnând reutilizare frauduloasă a informațiilor electronice de pe un card bancar) pot consta, conform punctului de vedere tehnic avut în vedere, formulat de Institutul pentru Tehnologii Avansate, într-un montaj electronic ce se instalează pe un ATM (*automatic teller machine*, mașină automată de distribuit bani), pe un automat de plată a parcării sau a combustibilului, ori poate fi un montaj electronic ce se introduce într-un echipament tip POS (*point of sale*, punct de vânzare) sau, în fine, poate fi un dispozitiv artizanal sau comercial de sine stătător. Din informațiile cuprinse în schema privind arhitectura montajului electronic dintr-un skimmer și cele privind funcționarea acestor dispozitive, coroborate cu prevederile art. 35 alin. (1) lit. a) din Legea nr. 161/2003 privind definiția sistemului informatic, rezultă că dispozitivul de skimming este un sistem informatic, chiar dacă este unul mai „primitiv” în ceea ce privește capacitatea de prelucrare a datelor. Dispozitivul de skimming poate fi folosit pentru accesarea sistemului informatic al băncii și obținerea datelor informatice stocate pe cardul bancar în vederea întrebuirii lor doar în mod direct (de exemplu, pentru cumpărături on-line întrebuirând datele de identificare de pe card) sau pentru „clonarea cardurilor” (falsificarea unor instrumente de plată electronică pe baza informațiilor obținute de pe cardul autentic).

ATM-urile și POS-urile sunt terminale și/sau periferice ale sistemului informatic bancar, prin intermediul lor realizându-se mai multe funcții: identificarea clientului (titular al contului bancar), identificarea contului bancar al clientului, accesarea sistemului bancar al clientului (prin intermediul sistemului informatic al băncii căreia îi aparține ATM-ul sau POS-ul), utilizându-se drept cod de acces codul PIN (*Personal Identification Number*, numărul personal de identificare) al clientului, transmiterea de date privind sumele transferate/eliberate prin operațiunea de plată cerută, contul bancar creditor (la plățile prin ATM sau POS) și confirmarea soldului suficient al contului bancar debitor al clientului, precum și tipărirea operațiunilor realizate și înregistrate în sistemele informatice ale băncilor implicate.

Cardurile bancare (de credit sau de debit) stochează pe banda lor magnetică informații privind numărul contului bancar, numele titularului cardului, date adiționale privind data expirării cardului, precum și alte date discreționare, la latitudinea băncii emitente a cardului. Potrivit art. 35 alin. (1) lit. d) din Legea 161/2003 rezultă că informațiile din banda magnetică a cardurilor bancare sunt date informatice în sensul legii penale, iar cardul bancar este mijloc de stocare a datelor informatice, copierea datelor de pe card reprezentând transfer de date informatice. În același timp, datele informatice conținute pe banda magnetică a cardului bancar autentic sunt absolut necesare în cazul falsificării unui card bancar, precum și pentru efectuarea unor operațiuni financiare în mod fraudulos.

Orice folosire a unui ATM sau POS reprezintă o accesare a unui sistem informatic, fie pentru a obține date informatice din sistem, fie pentru a transmite date informatice în sistem, fie pentru a transfera date de pe un mijloc de stocare a datelor informatice.

ATM-ul sau POS-ul împreună cu cardul bancar (care reprezintă unitate de stocare a datelor informatice) formează un

singur sistem informatic (ce cuprinde și serverele băncilor implicate) în care făptuitorul interpune un dispozitiv de skimming (montat la ATM sau POS), ce reprezintă o extindere frauduloasă a sistemului informatic bancar cu sistemul informatic al skimmerului, având ca unic scop copierea datelor informatice de pe cardul bancar; în această modalitate reprezintă atât un acces fără drept la un sistem informatic (prin montarea skimmerului în sistemul informatic bancar), în scopul obținerii de date informatice, prin încălcarea măsurilor de securitate existente pe benzile magnetice ale cardului bancar, cât și transfer neautorizat de date dintr-un mijloc de stocare a datelor informatice (cardul bancar).

În cazul în care dispozitivul de skimming este folosit în mod independent de ATM sau POS, pentru a copia informațiile de pe banda magnetică a cardului bancar, fapta reprezintă transfer neautorizat de date dintr-un mijloc de stocare a datelor informatice (cardul bancar).

În toate ipotezele, simpla deținere a dispozitivului de skimming este incriminată distinct atât în cazul în care se urmărește exclusiv obținerea unor date informatice prin accesarea fără drept a sistemului informatic și transferarea datelor informatice din cardul bancar, cât și în cazul în care aceste operațiuni sunt premergătoare, dar indispensabile, falsificării unui instrument de plată electronică (card bancar clonat). Trebuie menționat că, în sens informatic, transferarea unor date informatice reprezintă o operațiune de copiere a unor fișiere sau programe informatice, fără ștergerea lor de pe suportul-sursă (mediul de stocare). Transferarea unor date nu este o mutare fizică a datelor pe noul suport informatic, afirmația în sens contrar făcută în recursul în interesul legii promovat de Parchetul de pe lângă Înalta Curte de Casație și Justiție fiind eronată.

Dispozitive de aflare a codului PIN prin utilizarea cardurilor bancare

Dispozitivele optice sau optoelectronice de filmare a introducerilor de coduri PIN permit aflarea acestuia atunci când clientul utilizează propriul card bancar pentru efectuarea de operațiuni la ATM sau POS. Fapta, considerată distinct de transferarea datelor de pe banda magnetică a cardului bancar, are relevanță penală întrucât este un act preparator incriminat expres în art. 46, raportat la art. 42—45, din Legea nr. 161/2003, prin care se urmărește de către făptuitor obținerea pe cale vizuală a codului de acces la sistemul informatic al băncii titularului cardului bancar folosit pentru autentificarea operațiunilor cu cardul. În același timp însă aceeași faptă este act preparator în cazul falsificării unor instrumente de plată electronică sau săvârșirii infracțiunii de efectuare de operațiuni financiare în mod fraudulos.

Cu totul alta este situația amplasării unei tastaturi false deasupra tastaturii originale de la ATM sau POS, întrucât tastatura originală face parte din sistemul informatic bancar, iar prin intermediul său se transmite codul de acces la sistemul informatic, astfel încât tastatura falsă (care prezintă la rândul ei trăsăturile specifice unui sistem informatic) ajunge să fie integrată în sistemul informatic al băncii și să acceseze astfel, fără drept, sistemul informatic în scopul obținerii de date informatice, să fie folosită la interceptarea fără drept a unei transmisii de date informatice (transmiterea codului PIN către bancă) care nu este publică și care este destinată unui sistem informatic.

4.4.3. *Cu privire la montarea la bancomat a dispozitivelor de citire a benzii magnetice a cardului autentic și a codului PIN aferent acestuia (minivideocamere sau dispozitive tip tastatură)*

Faptele în legătură cu încălcarea relațiilor sociale privind protejarea integrității fizice și funcționale a sistemelor și datelor informatice sunt incriminate în art. 42—50 din titlul III (Prevenirea și combaterea criminalității informatice) din Legea

nr. 161/2003 privind unele măsuri pentru asigurarea transparenței în exercitarea demnităților publice, a funcțiilor publice și în mediul de afaceri, prevenirea și sancționarea corupției. Faptele privind operațiunile ilicite în legătură cu instrumentele de plată electronică sunt incriminate în art. 24—28 din Legea nr. 365/2002 privind comerțul electronic.

Incrimările din Legea nr. 365/2002 (art. 24—28) vor fi abrogate la 1 februarie 2014 (prin art. 107 pct. 2, coroborat cu art. 247 din Legea nr. 187/2012 pentru punerea în aplicare a Legii nr. 286/2009 privind Codul penal), iar incrimările din Legea nr. 161/2003 (art. 42—50) vor fi abrogate prin art. 130 pct. 1 și 2, coroborate cu art. 247 din Legea nr. 187/2012, de la acea dată cadrul incrimărilor urmând a fi reprezentat de art. 249—252 (Fraude comise prin sisteme informatice și mijloace de plată electronice), art. 311 (Falsificarea de titluri de credit sau instrumente de plată), art. 313 (Punerea în circulație de valori falsificate), art. 314 (Deținerea de instrumente în vederea falsificării de valori), art. 325 (Falsul informatic), art. 360 (Accesul ilegal la un sistem informatic), art. 361 (Interceptarea ilegală a unei transmisii de date informatice), art. 362 (Alterarea integrității datelor informatice), art. 363 (Perturbarea funcționării sistemelor informatice) și art. 365 (Operațiuni ilegale cu dispozitive sau programe informatice) din Noul Cod penal (Legea nr. 286/2009).

Obiectul juridic generic al infracțiunilor din Legea nr. 161/2003 este reprezentat de relațiile sociale a căror formare și dezvoltare normală impun respectarea necondiționată a confidențialității și integrității datelor și sistemelor informatice, viața contemporană fiind dominată de tehnologizarea și informatizarea accentuate în cadrul tuturor domeniilor de activitate.

Obiectul juridic generic al infracțiunilor din Legea nr. 365/2002 este reprezentat de relațiile sociale în legătură cu emiterea și utilizarea instrumentelor de plată electronică și cu utilizarea datelor de identificare în vederea efectuării de operațiuni financiare a căror formare și dezvoltare normală impun respectarea încrederii publice în mijloacele de plată electronice, precum și protejarea patrimoniului persoanelor fizice sau juridice împotriva utilizării frauduloase a instrumentelor de plată electronică ori a datelor de identificare a acestora.

a) Deținerea unui dispozitiv de skimming pentru a fi folosit la accesarea sistemului informatic al băncii și obținerea datelor informatice stocate pe cardul bancar constituie infracțiune prevăzută de art. 46 alin. (2) din Legea nr. 161/2003, prin raportare la art. 42 și art. 44 alin. (3) din aceeași lege.

b) Utilizarea dispozitivului de skimming prin montarea la ATM sau POS pentru accesarea sistemului informatic bancar și obținerea datelor informatice stocate pe cardul bancar realizează conținutul constitutiv al infracțiunilor de acces, fără drept, la un sistem informatic săvârșit în scopul obținerii de date informatice și prin încălcarea măsurilor de securitate [art. 42 alin. (1), (2) și (3) din Legea nr. 161/2003] și transfer neautorizat de date dintr-un mijloc de stocare a datelor informatice [art. 44 alin. (3) din Legea nr. 161/2003].

c) În cazul în care dispozitivul de skimming este folosit în mod independent de ATM sau POS pentru a copia informațiile de pe banda magnetică a cardului bancar, fapta reprezintă transfer neautorizat de date dintr-un mijloc de stocare a datelor informatice [art. 44 alin. (3) din Legea nr. 161/2003].

d) Deținerea unor dispozitive optice sau optoelectronice de filmare a introducerilor de coduri PIN pentru efectuarea de autentificări la operațiuni cu cardul la ATM sau POS constituie infracțiune [art. 46 alin. (2), raportat la art. 42—45 din Legea nr. 161/2003].

e) În cazul în care se probează că dispozitivele optice sau optoelectronice de filmare a introducerilor de coduri PIN pentru efectuarea de autentificări la operațiuni cu cardul bancar la ATM

sau POS s-au folosit pentru a produce, fără drept, o parolă, un cod de acces ori alte asemenea date informatice care permit accesul total sau parțial la un sistem informatic în scopul săvârșirii uneia dintre infracțiunile prevăzute la art. 42—45, fapta va constitui infracțiunea prevăzută de art. 46 alin. (1) lit. b) din Legea nr. 161/2003.

f) Amplasarea unei tastaturi false deasupra tastaturii originale de la ATM sau POS în scopul obținerii codului PIN întrunește elementele constitutive ale infracțiunii de acces fără drept la un sistem informatic în scopul obținerii de date informatice [art. 42 alin. (1) și (2) din Legea nr. 161/2003], în concurs cu interceptarea fără drept a unei transmisii de date informatice (transmiterea codului PIN către bancă) care nu este publică și care este destinată unui sistem informatic [art. 43 alin. (1) din Legea nr. 161/2003].

g) În cazul în care se probează că tastatura falsă de înregistrare a codurilor PIN pentru efectuarea de autentificări la operațiuni cu cardul bancar la ATM sau POS s-a folosit pentru a produce, fără drept, o parolă, un cod de acces ori alte asemenea date informatice care permit accesul total sau parțial la un sistem informatic în scopul săvârșirii uneia dintre infracțiunile prevăzute la art. 42—45, fapta va constitui infracțiunea prevăzută de art. 46 alin. (1) litera (b) din Legea nr. 161/2003.

h) Deținerea unei tastaturi false pentru înregistrarea introducerilor de coduri PIN la efectuarea de autentificări pentru operațiuni cu cardul la ATM sau POS constituie infracțiune [art. 46 alin. (2), raportat la art. 42—45 din Legea nr. 161/2003].

4.4.4. Cu privire la folosirea la bancomat a cardului falsificat ori chiar a celui autentic, fără acordul titularului său

Folosirea la ATM sau POS a cardului falsificat ori chiar a celui autentic, însă fără acordul titularului său, în scopul efectuării unor transferuri de fonduri, respectiv retrageri de numerar, precum și încărcarea/descărcarea unui instrument de monedă electronică constituie infracțiunea de efectuare de operațiuni financiare în mod fraudulos prin utilizarea unui instrument de plată electronică, inclusiv a datelor de identificare care permit utilizarea acestuia. Specificul instrumentelor de plată electronică este acela că sunt create și pot fi folosite preponderent, dar nu exclusiv, în cadrul unui sistem informatic pentru efectuarea unor operațiuni financiar-bancare determinate: transferuri de fonduri (prin ATM, POS sau internet), retrageri de numerar (prin ATM), depuneri de numerar (prin ATM), încărcarea/descărcarea unui instrument de monedă electronică (prin ATM, POS sau internet), dar cardurile de credit pot fi folosite și în afara unui sistem informatic, de exemplu, pentru garantarea stingerii unor eventuale obligații suplimentare de plată. Astfel, accesarea fără drept a sistemului informatic al băncii, prin încălcarea măsurilor de securitate, nu este absorbită în mod natural în elementul material al infracțiunii de efectuare de operațiuni financiare în mod fraudulos prin utilizarea unui instrument de plată electronică autentic sau falsificat, săvârșirea acestei infracțiuni neimplicând, ca o condiție esențială de existență, accesarea unui sistem informatic bancar prin intermediul căruia infracțiunea să fie comisă. Din acest motiv se impune reținerea în concurs ideal, atunci când este cazul, a infracțiunii de acces fără drept la sistemul informatic al băncii în scopul obținerii de date informatice prin încălcarea măsurilor de securitate.

Falsificarea unui instrument de plata electronică, în sensul alin. (1) al art. 24 din Legea nr. 365/2002, implică operațiuni de inscripționare/transferare a datelor informatice privind cardul real, autentic, asupra cardurilor contrafăcute, acestea din urmă fiind adevărate „clone” ale unor carduri reale, valabile și operaționale. Din acest motiv, acțiunile de obținere a datelor informatice de pe un card bancar autentic, în orice mod, în afara cadrului legal și în scopul falsificării unui instrument de plată electronică, nu vor constitui tentativă de falsificare a

instrumentelor de plată electronică, ci un simplu act preparator, neincriminat de Legea nr. 365/2002.

În cazul în care instrumentul de plată electronică folosit la efectuarea de operațiuni financiare în mod fraudulos este falsificat, se va reține în concurs real și infracțiunea de falsificare a instrumentelor de plată electronică.

4.5. Punctul de vedere al Catedrei de Drept Penal din cadrul Facultății de Drept și Științe Administrative a Universității din Craiova cu privire la încadrarea juridică dată faptelor care au suscit o practică neunitară

4.5.1. Soluția problemei de drept

a) Încadrarea juridică a faptei de a monta la un bancomat dispozitive de citire a benzii magnetice a cardului, minivideocamere sau dispozitive tip tastatură este aceea prevăzută de art. 46 alin. (2) din Legea nr. 161/2003.

b) În cazul folosirii la bancomat, pentru retrageri de numerar sau alte operațiuni financiare a unui card falsificat ori a unuia real, fără consimțământul titularului său, sunt întrunite elementele constitutive ale infracțiunii prevăzute de art. 42 alin. (1), (2) și (3) din Legea nr. 161/2003, săvârșită în concurs ideal cu cea prevăzută de art. 24 alin. (2) sau, după caz, art. 27 alin. (1) din Legea nr. 365/2002.

4.5.2. Cu privire la montarea la bancomat a dispozitivelor de citire a benzii magnetice a cardului autentic și a codului PIN aferent acestuia (minivideocamere sau dispozitive tip tastatură)

Accesul presupune intrarea, în tot sau în parte, într-un sistem informatic, conectarea la un sistem informatic, astfel încât să poată fi citite, cunoscute, accesate informațiile din sistem. Prin montarea unui skimmer nu are loc o interacțiune cu bancomatul, privit ca sistem informatic, ci doar cu instrumentul de plată electronic, cu banda magnetică a cardului, ale cărui informații sunt copiate, stocate în memoria skimmerului.

Prin montarea la ATM a dispozitivului de citire a benzii magnetice a cardului și a videocamerei ori a dispozitivului modificat de tip tastatură nu putem vorbi de infracțiunea de acces fără drept la un sistem informatic prevăzută și sancționată de art. 42 alin. (1) din Legea nr. 161/2003. Într-o astfel de situație nu este realizat elementul material al infracțiunii, respectiv accesul, neexistând vreo interacțiune, comunicare cu datele conținute în sistemul informatic.

Un alt argument privind lipsa elementului material al infracțiunii rezultă din faptul că datele de pe banda magnetică a cardului sunt citite și captate înainte ca respectivul card să intre în fanta bancomatului și înainte să se realizeze vreo transmisie de date informatice între card și ATM. Într-o astfel de situație, ATM-ul este folosit doar ca un suport fizic, ca un camuflaj pentru skimmer, și nu ca o componentă a unui sistem informatic prin intermediul căreia are loc accesarea datelor din respectivul sistem.

În mod evident nu sunt întrunite elementele constitutive ale infracțiunii prevăzute de art. 42 alin. (1) din Legea nr. 161/2003, însă o astfel de faptă se încadrează drept deținere, fără drept, a unui dispozitiv în vederea săvârșirii uneia dintre infracțiunile prevăzute în art. 42—45 din Legea nr. 161/2003.

Prin urmare, încadrarea juridică a faptei de a monta la un bancomat dispozitive de citire a benzii magnetice a cardului, minivideocamere sau dispozitive tip tastatură este aceea prevăzută de art. 46 alin. (2) din Legea nr. 161/2003.

4.5.3. Cu privire la folosirea la bancomat, pentru retrageri de numerar sau orice alte operațiuni financiare, a cardului falsificat ori chiar a celui autentic, fără acordul titularului său

În cazul în care, după obținerea cardului falsificat, acesta este folosit în scopul retragerii de numerar are loc o accesare a datelor din bancomat. Bancomatul nu mai este întrebuințat doar ca un suport, ci potrivit destinației sale, ca o componentă a unui sistem informatic ce permite conectarea în sistem și cunoașterea datelor conținute de acest sistem. Într-o astfel de

situație, există un schimb de informații între cel care utilizează cardul și datele din sistemul informatic, bancar în acest caz, ceea ce înseamnă că în momentul tastării codului PIN se poate vorbi de acces, ca element material al infracțiunii prevăzute și sancționate de art. 42 alin. (1) din Legea nr. 161/2003. Infracțiunea există și s-a consumat din acest moment, indiferent dacă s-a solicitat sau nu vreo operațiune financiară. O astfel de solicitare nu este necesară pentru existența infracțiunii în discuție ale cărei elemente constitutive s-au unit în momentul în care a avut loc schimbul de informații, ceea ce înseamnă acces ca element material al infracțiunii.

În cazul folosirii la bancomat, pentru retrageri de numerar sau alte operațiuni financiare, a unui card falsificat ori a unui real, fără consimțământul titularului său, sunt întrunite elementele constitutive ale infracțiunii prevăzute de art. 42 alin. (1), (2) și (3) din Legea nr. 161/2003, săvârșită în concurs ideal cu cea prevăzută de art. 24 alin. (2) sau, după caz, art. 27 alin. (1) din Legea nr. 365/2002.

4.6. *Punctul de vedere al Facultății de Drept a Universității „Lucian Blaga” din Sibiu cu privire la încadrarea juridică dată faptelor care au suscitat o practică neunitară*

4.6.1. *Soluția problemei de drept*

a) Un simplu telefon mobil, o cameră video sau chiar un dispozitiv modificat tip tastatură nu pot fi considerate ca fiind dispozitive deținute fără drept și, prin urmare, nu sunt întrunite elementele constitutive ale infracțiunii prevăzute de art. 46 alin. (2) din Legea nr. 161/2003.

b) Deținerea telefonului mobil sau a camerei video nu se încadrează nici în prevederile art. 25 din Legea nr. 365/2002, care incriminează fabricarea ori deținerea de echipamente, inclusiv hardware sau software, cu scopul de a servi la falsificarea instrumentelor de plată electronică.

c) Ținând cont de prevederile legale enunțate se impune a se analiza în concret operațiunile efectuate de făptuitor, deoarece este posibil ca făptuitorul care efectuează doar retrageri de numerar sau plăți cu acel card (real ori falsificat), fără să facă interogări de sold, să nu urmărească să obțină date informatice, în astfel de situații lipsind scopul special cerut expres de prevederile art. 42 alin. (2) din Legea nr. 161/2003. Acestea nu pot fi reținute în sarcina sa, urmând a fi incidente doar cele ale alin. (1) și (3) ale aceluiași articol (operațiunea fiind efectuată în mod clar prin încălcarea măsurilor de securitate).

d) În situația în care făptuitorul utilizează cardul real sau falsificat pentru interogarea soldului ori pentru alte operațiuni care i-ar pune la dispoziție date informatice (urmate sau nu de retrageri de numerar, transferuri ori plăți), încadrarea juridică este cea prevăzută de art. 42 alin. (1), (2) și (3) din Legea nr. 161/2003.

În ipoteza efectuării de retrageri de numerar, plăți sau transferuri de bani, infracțiunea de acces fără drept la un sistem informatic intră în concurs cu infracțiunile prevăzute de Legea nr. 365/2002 referitoare la comerțul electronic. Dacă vorbim de cardul falsificat, infracțiunea va fi cea prevăzută de art. 24 alin. (2) din lege (punerea în circulație a unui instrument de plată electronică falsificat), iar dacă avem în vedere un card real, folosit fără consimțământul titularului său, fapta se va încadra în prevederile art. 27 alin. (1) din legea menționată.

4.6.2. *Cu privire la montarea la bancomat a dispozitivelor de citire a benzii magnetice a cardului autentic și a codului PIN aferent acestuia (minivideocamere sau dispozitive tip tastatură)*

Montarea la ATM a dispozitivului de citire a benzii magnetice a cardului și a videocamerei ori a dispozitivului modificat de tip tastatură nu realizează accesul fără drept la un sistem informatic, infracțiune prevăzută de art. 42 alin. (1) din Legea nr. 161/2003.

Fără a mai relua ampla argumentare adusă în sprijinul acestei opinii de către procurorul general al Parchetului de pe

lângă Înalta Curte de Casație și Justiție, punctul de vedere subliniază faptul că, deși ATM-ul reprezintă un terminal în cadrul unui sistem informatic, în ipoteza utilizării de către o persoană a dispozitivului de citire a benzii magnetice a cardului și a videocamerei ori a dispozitivului modificat de tip tastatură, bancomatul nu este folosit pentru a se realiza vreun acces la datele informatice, ci constituie doar un suport fizic pentru dispozitivele menționate. Nu există deci în această situație nicio interacțiune a făptuitorului cu tehnica de calcul prin intermediul echipamentelor utilizate. O astfel de faptă reprezintă practic un act preparator al infracțiunii de acces fără drept la un sistem informatic, care însă nu este incriminat.

În opinia procurorului general se arată că deținerea, fără drept, a unui dispozitiv, program informatic, parolă, cod de acces sau dată informatică în scopul săvârșirii uneia dintre infracțiunile prevăzute la art. 42—45 din Legea nr. 161/2003 constituie infracțiunea prevăzută de art. 46 alin. (2) din aceeași lege. Trebuie însă analizat în concret dacă dispozitivul utilizat de făptuitor este deținut fără drept sau nu. Telefonul mobil, camera video sau chiar un dispozitiv modificat tip tastatură nu pot fi considerate ca fiind dispozitive deținute fără drept și, prin urmare, nu sunt întrunite elementele constitutive ale infracțiunii prevăzute de art. 46 alin. (2) din Legea nr. 161/2003. Deținerea telefonului mobil sau a camerei video nu se încadrează nici în prevederile art. 25 din Legea nr. 365/2002, care incriminează fabricarea ori deținerea de echipamente, inclusiv hardware sau software, cu scopul de a servi la falsificarea instrumentelor de plată electronică (deși au existat și soluții în acest sens).

4.6.3. *Cu privire la folosirea la bancomat, pentru retrageri de numerar sau orice alte operațiuni financiare, a cardului falsificat ori chiar a celui autentic, fără acordul titularului său*

În astfel de cazuri există întotdeauna un acces fără drept la un sistem informatic, dar este necesar a fi făcute unele precizări în ceea ce privește încadrarea juridică a unor astfel de fapte.

În opinia exprimată de procurorul general se arată că fapta întrunește elementele constitutive ale infracțiunii prevăzute de art. 42 alin. (1), (2) și (3) din Legea nr. 161/2003. Norma de incriminare are următorul cuprins: (1) *Accesul, fără drept, la un sistem informatic constituie infracțiune și se pedepsește cu închisoare de la 3 luni la 3 ani sau cu amendă.* (2) *Fapta prevăzută la alin. (1), săvârșită în scopul obținerii de date informatice, se pedepsește cu închisoare de la 6 luni la 5 ani.* (3) *Dacă fapta prevăzută la alin. (1) sau (2) este săvârșită prin încălcarea măsurilor de securitate, pedeapsa este închisoare de la 3 la 12 ani.*”

Ținând cont de prevederile legale enunțate se impune a se analiza în concret operațiunile efectuate de făptuitor, deoarece este posibil ca făptuitorul care efectuează doar retrageri de numerar sau plăți cu acel card (real ori falsificat), fără să facă interogări de sold, să nu urmărească să obțină date informatice. În astfel de situații lipsește scopul special cerut expres de prevederile alin. (2) ale art. 42 din Legea nr. 161/2003. Acestea nu pot fi reținute în sarcina sa, urmând a fi incidente doar cele ale alin. (1) și (3) ale aceluiași articol (operațiunea fiind efectuată în mod clar prin încălcarea măsurilor de securitate).

În situația în care făptuitorul utilizează cardul real sau falsificat pentru interogarea soldului ori pentru alte operațiuni care i-ar pune la dispoziție date informatice (urmate sau nu de retrageri de numerar, transferuri ori plăți), încadrarea juridică este cea prevăzută de art. 42 alin. (1), (2) și (3) din Legea nr. 161/2003.

În ipoteza efectuării de retrageri de numerar, plăți sau transferuri de bani, infracțiunea de acces fără drept la un sistem informatic intră în concurs cu infracțiunile prevăzute de Legea nr. 365/2002 referitoare la comerțul electronic. Dacă vorbim de cardul falsificat, infracțiunea va fi cea prevăzută de art. 24 alin. (2) din lege (punerea în circulație a unui instrument de plată

electronică falsificat), iar dacă se are în vedere un card real, folosit fără consimțământul titularului său, fapta se va încadra în prevederile art. 27 alin. (1) din Legea nr. 365/2002.

4.7. Punctul de vedere al Departamentului de Drept Public din cadrul Facultății de Drept a Universității de Vest din Timișoara cu privire la încadrarea juridică dată faptelor care au suscitat o practică neunitară

4.7.1. Înțelesul unor termeni

Bancomatul (ATM) constituie un sistem informatic, în sensul art. 35 alin. (1) lit. a) din Legea nr. 161/2003, deoarece asigură prelucrarea automată a datelor, cu ajutorul unui program informatic.

Dispozitivele de skimming nu au caracteristicile unui sistem informatic, indiferent dacă este vorba de camere video, dispozitive de citire a benzii magnetice a cardului sau tastatură falsă. Ele nu au caracteristicile sistemului informatic deoarece nu asigură prelucrarea automată a datelor, cu ajutorul unui program informatic, permițând doar copierea codurilor înscrise pe cardul care asigură accesarea sistemului informatic.

Prin **transfer neautorizat** se înțelege mutarea fără drept a reprezentării binare a informațiilor din mediul de stocare curent (autorizat) pe un alt suport de stocare extern sau chiar în interiorul aceluiași sistem, informatic, dar în altă locație.

4.7.2. Soluția problemei de drept

a) Deținerea dispozitivelor de skimming, dacă au fost concepute sau adaptate în scopul săvârșirii uneia dintre infracțiunile prevăzute la art. 42—45, constituie infracțiunea prevăzută de art. 46 alin. (2) din Legea nr. 161/2003, nefiind necesară atașarea lor la bancomat.

b) Deținerea dispozitivelor de skimming nu poate realiza însă și conținutul infracțiunilor prevăzute de art. 44 alin. (2) și (3), deoarece nu are loc un transfer de date din sistemul informatic ATM și mutarea lor în alt loc, ci doar o copie a datelor înscrise pe card.

c) După ce se clonează un card și prin intermediul acestuia se accesează bancomatul, chiar fără a se efectua nicio operațiune bancară, se săvârșește infracțiunea prevăzută de art. 42 din Legea nr. 161/2003, aflată în concurs etiologic cu infracțiunea prevăzută de art. 46 alin. (2) din Legea nr. 161/2003.

d) Nu se poate reține infracțiunea prevăzută de art. 25 din Legea nr. 365/2002, constând în fabricarea ori deținerea de echipamente, inclusiv hardware sau software, cu scopul de a servi la falsificarea instrumentelor de plată electronică, deoarece dispozitivele de skimming nu permit ele însele fabricarea sau producerea unui card nou, pe care să se inscripționeze datele copiate.

4.7.3. Cu privire la montarea la bancomat a dispozitivelor de citire a benzii magnetice a cardului autentic și a codului PIN aferent acestuia (minivideocamere sau dispozitive tip tastatură)

Deținerea dispozitivelor de skimming, dacă au fost concepute sau adaptate în scopul săvârșirii uneia dintre infracțiunile prevăzute la art. 42—45, constituie infracțiunea prevăzută de art. 46 alin. (2) din Legea nr. 161/2003, nefiind necesară atașarea lor la bancomat.

Atașarea lor la bancomat și citirea benzii magnetice a cardului nu realizează însă accesarea sistemului informatic al bancomatului, permițând doar fabricarea (clonarea) ulterioară a unui card, cu care să se acceseze sistemul informatic. Citirea datelor cardului se realizează înainte ca acesta să interacționeze cu ATM-ul. Simpla amplasare a unui dispozitiv electronic în imediata apropiere a sistemului sau chiar în contact fizic cu respectivul sistem, fără ca cele două componente (sistemul informatic și dispozitivul electronic) să interacționeze, nu poate fi apreciată ca fiind un acces neautorizat. Montarea unui echipament de skimming la un ATM, în vederea obținerii datelor cardurilor utilizate la respectivul terminal, constituie doar infracțiunea prevăzută de art. 46 alin. (2) din Legea nr. 161/2003.

Această infracțiune reprezintă o infracțiune mijloc pentru săvârșirea infracțiunilor prevăzute de art. 42—45, deci inclusiv pentru săvârșirea infracțiunii de acces fără drept la un sistem informatic.

Deținerea dispozitivelor de skimming nu poate realiza însă și conținutul infracțiunilor prevăzute de art. 44 alin. (2) și (3), deoarece nu are loc un transfer de date din sistemul informatic ATM și mutarea lor în alt loc, ci doar o copie a datelor înscrise pe card.

În cazul transferului de date informatice, urmarea o constituie, pe de o parte, ștergerea datelor informatice din locația inițială, astfel că acestea nu mai există pentru utilizatorul de drept, și crearea concomitentă a unei replici a datelor informatice, pe același suport de stocare sau pe un altul, extern, în posesia făptuitorului. Abia după ce cu ajutorul datelor captate prin skimming se clonează un card și prin intermediul acestuia se accesează bancomatul, chiar fără a se efectua nicio operațiune bancară, se săvârșește infracțiunea prevăzută de art. 42 din Legea nr. 161/2003, aflată în concurs etiologic cu infracțiunea prevăzută de art. 46 alin. (2) din Legea nr. 161/2003.

Nu se poate reține infracțiunea prevăzută de art. 25 din Legea nr. 365/2002, constând în fabricarea ori deținerea de echipamente, inclusiv hardware sau software, cu scopul de a servi la falsificarea instrumentelor de plată electronică, deoarece dispozitivele de skimming nu permit ele însele fabricarea sau producerea unui card nou, pe care să se inscripționeze datele copiate.

Doar deținerea de echipamente hardware sau software care permit falsificarea instrumentelor de plată electronică realizează conținutul infracțiunii prevăzute de art. 25 din Legea nr. 365/2002, iar falsificarea efectivă a cardului realizează conținutul infracțiunii de falsificare a instrumentelor de plată electronică prevăzută de art. 24 din Legea nr. 365/2002.

4.7.4. Cu privire la folosirea la bancomat, pentru retrageri de numerar sau orice alte operațiuni financiare, a cardului falsificat ori chiar a celui autentic, fără acordul titularului său

Utilizarea unui card falsificat sau a unui card valid (fără acordul titularului) la un ATM conduce la realizarea unui acces neautorizat într-un sistem informatic, art. 42 alin. (1), (2) sau (3), după caz, din Legea nr. 161/2003.

Această încadrare este valabilă doar pentru activitatea de interogare a ATM-ului, iar dacă autorul va efectua și operațiuni financiare (retrageri de sume, plăți, transferuri etc.) infracțiunea de acces neautorizat va veni în concurs cu infracțiunea prevăzută de art. 27 alin. (1) sau (2) din Legea nr. 365/2002, constând în efectuarea de operațiuni financiare în mod fraudulos, infracțiuni aflate în concurs ideal.

ATM-ul are caracteristicile unui sistem informatic, iar prin utilizarea unui card falsificat sau a unui card valid, dar fără acordul titularului, autorul infracțiunii va obține accesul la datele de cont, sistemul percependu-l ca fiind persoana autorizată.

Infracțiunea prevăzută de art. 42 din Legea nr. 161/2003 are ca obiect juridic protejarea datelor informatice, pe când prin incriminarea faptelor descrise în art. 27 din Legea nr. 365/2002 se urmărește protejarea operațiunilor financiare. Cele două infracțiuni diferă și prin faptul că accesul neautorizat constituie infracțiune de pericol, fără a fi nevoie să se producă un prejudiciu, pe când infracțiunea de efectuare a unor operațiuni financiare în mod fraudulos reprezintă o infracțiune de rezultat.

5. Raportul asupra recursului în interesul legii

5.1. Legislația relevantă

5.1.1. Legea nr. 161/2003 privind unele măsuri pentru asigurarea transparenței în exercitarea demnităților publice, a funcțiilor publice și în mediul de afaceri, prevenirea și sancționarea corupției

Faptele în legătură cu încălcarea relațiilor sociale privind protejarea integrității fizice și funcționale a sistemelor și datelor

informatice sunt incriminate în art. 42—50, cartea 1, titlul III („Prevenirea și combaterea criminalității informatice”) din Legea nr. 161/2003 privind unele măsuri pentru asigurarea transparenței în exercitarea demnităților publice, a funcțiilor publice și în mediul de afaceri, prevenirea și sancționarea corupției, iar art. 35 din Legea nr. 161/2003 prevede înțelesul termenilor și expresiilor utilizate în reglementarea titlului respectiv:

„L E G E
privind unele măsuri pentru asigurarea
transparenței în exercitarea demnităților publice,
a funcțiilor publice și în mediul de afaceri,
prevenirea și sancționarea corupției

CARTEA I

Reglementări generale pentru prevenirea și combaterea corupției

TITLUL III

Prevenirea și combaterea criminalității informatice

CAPITOLUL I
Dispoziții generale

Art. 34. — Prezentul titlu reglementează prevenirea și combaterea criminalității informatice, prin măsuri specifice de prevenire, descoperire și sancționare a infracțiunilor săvârșite prin intermediul sistemelor informatice, asigurându-se respectarea drepturilor omului și protecția datelor personale.

Art. 35. — (1) În prezentul titlu, termenii și expresiile de mai jos au următorul înțeles:

a) prin *sistem informatic* se înțelege 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;

b) prin *prelucrare automată a datelor* se înțelege procesul prin care datele dintr-un sistem informatic sunt prelucrate prin intermediul unui program informatic;

c) prin *program informatic* se înțelege un ansamblu de instrucțiuni care pot fi executate de un sistem informatic în vederea obținerii unui rezultat determinat;

d) prin *date informatice* se înțelege orice reprezentare a unor fapte, informații sau concepte într-o formă care poate fi prelucrată printr-un sistem informatic. În această categorie se include și orice program informatic care poate determina realizarea unei funcții de către un sistem informatic;

e) prin *furnizor de servicii* se înțelege:

1. orice persoană fizică sau juridică ce oferă utilizatorilor posibilitatea de a comunica prin intermediul sistemelor informatice;

2. orice altă persoană fizică sau juridică ce prelucrează sau stochează date informatice pentru persoanele prevăzute la pct. 1 și pentru utilizatorii serviciilor oferite de acestea;

f) prin *date referitoare la trafic informational* se înțelege orice date informatice referitoare la o comunicare realizată printr-un sistem informatic și produse de acesta, care reprezintă o parte din lanțul de comunicare, indicând originea, destinația, ruta, ora, data, mărimea, volumul și durata comunicării, precum și tipul serviciului utilizat pentru comunicare;

g) prin *date referitoare la utilizatori* se înțelege orice informație care poate conduce la identificarea unui utilizator, incluzând tipul de comunicație și serviciul folosit, adresa poștală, adresa geografică, numere de telefon sau alte numere de acces și modalitatea de plată a serviciului respectiv, precum și orice alte date care pot conduce la identificarea utilizatorului;

h) prin *măsuri de securitate* se înțelege folosirea unor proceduri, dispozitive sau programe informatice specializate cu ajutorul cărora accesul la un sistem informatic este restricționat sau interzis pentru anumite categorii de utilizatori;

i) (...)

(2) În sensul prezentului titlu, acționează fără drept persoana care se află în una dintre următoarele situații:

a) nu este autorizată, în temeiul legii sau al unui contract;

b) depășește limitele autorizării;

c) nu are permisiunea, din partea persoanei fizice sau juridice competente, potrivit legii, să o acorde, de a folosi, administra sau controla un sistem informatic ori de a desfășura cercetări științifice sau de a efectua orice altă operațiune într-un sistem informatic.

CAPITOLUL III
Infrațiuni și contravenții

SECȚIUNEA 1

Infrațiuni contra confidențialității și integrității datelor și sistemelor informatice

Art. 42. — (1) Accesul, fără drept, la un sistem informatic constituie infracțiune și se pedepsește cu închisoare de la 3 luni la 3 ani sau cu amendă.

(2) Fapta prevăzută la alin. (1), săvârșită în scopul obținerii de date informatice, se pedepsește cu închisoare de la 6 luni la 5 ani.

(3) Dacă fapta prevăzută la alin. (1) sau (2) este săvârșită prin încălcarea măsurilor de securitate, pedeapsa este închisoarea de la 3 la 12 ani.

Art. 43. — (1) Interceptarea, fără drept, a unei transmisii de date informatice care nu este publică și care este destinată unui sistem informatic, provine dintr-un asemenea sistem sau se efectuează în cadrul unui sistem informatic constituie infracțiune și se pedepsește cu închisoare de la 2 la 7 ani.

(2) Cu aceeași pedeapsă se sancționează și interceptarea, fără drept, a unei emisii electromagnetice provenite dintr-un sistem informatic ce conține date informatice care nu sunt publice.

Art. 44. — (1) Fapta de a modifica, șterge sau deteriora date informatice ori de a restricționa accesul la aceste date, fără drept, constituie infracțiune și se pedepsește cu închisoare de la 2 la 7 ani.

(2) Transferul neautorizat de date dintr-un sistem informatic se pedepsește cu închisoare de la 3 la 12 ani.

(3) Cu pedeapsa prevăzută la alin. (2) se sancționează și transferul neautorizat de date dintr-un mijloc de stocare a datelor informatice.

Art. 45. — Fapta de a perturba grav, fără drept, funcționarea unui sistem informatic, prin introducerea, transmiterea, modificarea, ștergerea sau deteriorarea datelor informatice sau prin restricționarea accesului la aceste date constituie infracțiune și se pedepsește cu închisoare de la 3 la 15 ani.

Art. 46. — (1) Constituie infracțiune și se pedepsește cu închisoare de la 1 la 6 ani:

a) fapta de a produce, vinde, de a importa, distribui sau de a pune la dispoziție, sub orice altă formă, fără drept, a unui dispozitiv sau program informatic conceput sau adaptat în scopul săvârșirii uneia dintre infracțiunile prevăzute la art. 42—45;

b) fapta de a produce, vinde, de a importa, distribui sau de a pune la dispoziție, sub orice altă formă, fără drept, a unei parole, cod de acces sau alte asemenea date informatice care permit accesul total sau parțial la un sistem informatic în scopul săvârșirii uneia dintre infracțiunile prevăzute la art. 42—45.

(2) Cu aceeași pedeapsă se sancționează și deținerea, fără drept, a unui dispozitiv, program informatic, parolă, cod de acces sau dată informatică dintre cele prevăzute la alin. (1) în scopul săvârșirii uneia dintre infracțiunile prevăzute la art. 42—45.

Art. 47. — Tentativa infracțiunilor prevăzute la art. 42—46 se pedepsește.”

5.1.2. *Legea nr. 365/2002 privind comerțul electronic.* Faptele privind operațiunile ilicite în legătură cu instrumentele de plată electronică sunt incriminate în art. 24—28 din Legea nr. 365/2002 privind comerțul electronic.

„L E G E
privind comerțul electronic

CAPITOLUL I
Dispoziții generale

ARTICOLUL 1

Definiții

În înțelesul prezentei legi, următorii termeni se definesc astfel: (...)

11. *instrument de plată electronică* — un instrument care permite titularului său să efectueze următoarele tipuri de operațiuni:

a) transferuri de fonduri, altele decât cele ordonate și executate de către instituții financiare;

b) retrageri de numerar, precum și încărcarea și descărcarea unui instrument de monedă electronică;

12. *instrument de plată cu acces la distanță* — instrument de plată electronică prin intermediul căruia titularul său poate să își acceseze fondurile deținute într-un cont la o instituție financiară și să autorizeze efectuarea unei plăți, utilizând un cod personal de identificare sau un alt mijloc de identificare similar;

13. *instrument de monedă electronică* — instrument de plată electronică reîncărcabil, altul decât instrumentul de plată cu acces la distanță, pe care unitățile de valoare sunt stocate electronic și care permite titularului său să efectueze tipurile de operațiuni menționate la pct. 11;

14. *titular* — persoană care deține un instrument de plată electronică pe baza unui contract încheiat cu un emitent, în condițiile prevăzute de lege;

15. *date de identificare* — orice informații care pot permite sau facilita efectuarea tipurilor de operațiuni menționate la pct. 11, precum un cod de identificare, numele sau denumirea, domiciliul ori sediul, numărul de telefon, fax, adresa de poștă electronică, numărul de înmatriculare sau alte mijloace similare de identificare, codul de înregistrare fiscală, codul numeric personal și altele asemenea;

16. (...)

ARTICOLUL 2

Scop și domeniu de aplicare

(1) Prezenta lege are ca scop stabilirea condițiilor de furnizare a serviciilor societății informaționale, precum și prevederea ca infracțiuni a unor fapte săvârșite în legătură cu securitatea domeniilor utilizate în comerțul electronic, emiterea și utilizarea instrumentelor de plată electronică și cu utilizarea datelor de identificare în vederea efectuării de operațiuni financiare, pentru asigurarea unui cadru favorabil liberei circulații și dezvoltării în condiții de securitate a acestor servicii. (...)

CAPITOLUL VIII

Infracțiuni săvârșite în legătură cu emiterea și utilizarea instrumentelor de plată electronică și cu utilizarea datelor de identificare în vederea efectuării de operațiuni financiare

ARTICOLUL 24

Falsificarea instrumentelor de plată electronică

(1) Falsificarea unui instrument de plată electronică se pedepsește cu închisoare de la 3 la 12 ani și interzicerea unor drepturi.

(2) Cu aceeași pedeapsă se sancționează punerea în circulație, în orice mod, a instrumentelor de plată electronică falsificate sau deținerea lor în vederea punerii în circulație.

(3) Pedeapsa este închisoarea de la 5 la 15 ani și interzicerea unor drepturi, dacă faptele prevăzute la alin. (1) și (2) sunt săvârșite de o persoană care, în virtutea atribuțiilor sale de serviciu:

a) realizează operații tehnice necesare emiterii instrumentelor de plată electronică ori efectuării tipurilor de operațiuni prevăzute la art. 1 pct. 11; sau

b) are acces la mecanismele de securitate implicate în emiterea sau utilizarea instrumentelor de plată electronică; sau

c) are acces la datele de identificare sau la mecanismele de securitate implicate în efectuarea tipurilor de operațiuni prevăzute la art. 1 pct. 11.

(4) Tentativa se pedepsește.

ARTICOLUL 25

Deținerea de echipamente în vederea falsificării instrumentelor de plată electronică

Fabricarea ori deținerea de echipamente, inclusiv hardware sau software, cu scopul de a servi la falsificarea instrumentelor de plată electronică se pedepsește cu închisoare de la 6 luni la 5 ani.

ARTICOLUL 26

Falsul în declarații în vederea emiterii sau utilizării instrumentelor de plată electronică

Declararea necorespunzătoare adevărului, făcută unei instituții bancare, de credit sau financiare ori oricărei alte persoane juridice autorizate în condițiile legii să emită instrumente de plată electronică sau să accepte tipurile de operațiuni prevăzute la art. 1 pct. 11, în vederea emiterii sau utilizării unui instrument de plată electronică, pentru sine sau pentru altul, atunci când, potrivit legii ori împrejurărilor, declarația făcută servește pentru emiterea sau utilizarea aceluși instrument, se pedepsește cu închisoare de la 3 luni la 2 ani sau cu amendă.

ARTICOLUL 27

Efectuarea de operațiuni financiare în mod fraudulos

(1) Efectuarea uneia dintre operațiunile prevăzute la art. 1 pct. 11, prin utilizarea unui instrument de plată electronică, inclusiv a datelor de identificare care permit utilizarea acestuia, fără consimțământul titularului instrumentului respectiv, se pedepsește cu închisoare de la 1 la 12 ani.

(2) Cu aceeași pedeapsă se sancționează efectuarea uneia dintre operațiunile prevăzute la art. 1 pct. 11, prin utilizarea neautorizată a oricăror date de identificare sau prin utilizarea de date de identificare fictive.

(3) Cu aceeași pedeapsă se sancționează transmiterea neautorizată către altă persoană a oricăror date de identificare, în vederea efectuării uneia dintre operațiunile prevăzute la art. 1 pct. 11.

(4) Pedeapsa este închisoarea de la 3 la 15 ani și interzicerea unor drepturi, dacă faptele prevăzute la alin. (1)—(3) sunt săvârșite de o persoană care, în virtutea atribuțiilor sale de serviciu:

a) realizează operații tehnice necesare emiterii instrumentelor de plată electronică ori efectuării tipurilor de operațiuni prevăzute la art. 1 pct. 11; sau

b) are acces la mecanismele de securitate implicate în emiterea sau utilizarea instrumentelor de plată electronică; sau

c) are acces la datele de identificare sau la mecanismele de securitate implicate în efectuarea tipurilor de operațiuni prevăzute la art. 1 pct. 11.

(5) Tentativa se pedepsește.

ARTICOLUL 28

Acceptarea operațiunilor financiare efectuate în mod fraudulos

(1) Acceptarea uneia dintre operațiunile prevăzute la art. 1 pct. 11, cunoscând că este efectuată prin folosirea unui instrument de plată electronică falsificat sau utilizat fără consimțământul titularului său, se pedepsește cu închisoare de la 1 la 12 ani.

(2) Cu aceeași pedeapsă se sancționează acceptarea uneia dintre operațiunile prevăzute la art. 1 pct. 11, cunoscând că este efectuată prin utilizarea neautorizată a oricăror date de identificare sau prin utilizarea de date de identificare fictive.

(3) Tentativa se pedepsește.”

5.1.3. Noul Cod penal

Incrimările din Legea nr. 365/2002 (art. 24—28) vor fi abrogate la 1 februarie 2014 (prin art. 107 pct. 2, coroborat cu art. 247 din Legea nr. 187/2012 pentru punerea în aplicare a Legii nr. 286/2009 privind Codul penal), iar incriminările din Legea nr. 161/2003 (art. 42—50) vor fi abrogate prin art. 130 pct. 1 și 2, coroborate cu art. 247 din Legea nr. 187/2012, de la acea dată cadrul incriminărilor urmând a fi reprezentat de art. 249—252 (Fraude comise prin sisteme informatice și mijloace de plată electronice), art. 311 (Falsificarea de titluri de credit sau instrumente de plată), art. 313 (Punerea în circulație de valori falsificate), art. 314 (Deținerea de instrumente în vederea falsificării de valori), art. 325 (Falsul informatic), art. 360 (Accesul ilegal la un sistem informatic), art. 361 (Interceptarea ilegală a unei transmisii de date informatice), art. 362 (Alterarea integrității datelor informatice), art. 363 (Perturbarea funcționării sistemelor informatice) și art. 365 (Operațiuni ilegale cu dispozitive sau programe informatice) din noul Cod penal (Legea nr. 286/2009).

5.2. Soluția preconizată

Recursul în interesul legii solicită, conform sesizării, clarificarea noțiunii de acces fără drept la un sistem informatic, iar în anexele cuprinzând jurisprudența în divergență se fac referiri la încadrarea juridică dată faptelor conform Legii nr. 161/2003 [art. 42 în anexele nr. 1, 3, 43—45, 55, art. 46 în anexa nr. 55, art. 44 alin. (2), (3) și art. 46 alin. (2) în anexa nr. 41, art. 46 alin. (2) în anexele nr. 39, 46, 47] și Legii nr. 365/2002 [art. 24 alin. (2) în anexa nr. 42, art. 25 în anexa nr. 44, art. 27 alin. (1) în anexele nr. 42, 45, 47—53, art. 24, alin. (1) și (2), art. 25 și art. 27 alin. (1) în concurs în anexele nr. 2—30, 54, art. 27 alin. (1) în anexele nr. 31—38].

Sintetizând situațiile de fapt descrise de considerentele recursului în interesul legii și de anexele cuprinzând jurisprudența, raportul constată că sunt avute în vedere mai multe ipoteze, respectiv: montarea la bancomat a dispozitivelor de citire a benzii magnetice a cardului autentic și a codului PIN aferent acestuia (minivideocamere sau dispozitive tip tastatură) urmată de descoperirea faptei înainte ca victima să folosească un card; montarea la bancomat a dispozitivelor de citire a benzii magnetice a cardului autentic și a codului PIN aferent acestuia (minivideocamere sau dispozitive tip tastatură) urmată de folosirea bancomatului de către victimă realizează un transfer de date de pe card; montarea la bancomat a dispozitivelor de citire a benzii magnetice a cardului autentic și a codului PIN aferent acestuia (minivideocamere sau dispozitive tip tastatură) urmată de utilizarea bancomatului de către victimă și transmiterea datelor de pe card și de utilizare a datelor de către persoana acuzată.

Raportul a analizat fiecare dintre ipotezele de fapt descrise în jurisprudența anexată, fără a se pronunța exclusiv asupra existenței sau absenței accesului la un sistem informatic, deoarece chiar soluția propusă de procurorul general (secțiunea 3.1 din prezenta decizie) face referire la montarea dispozitivelor de citire a cardurilor la bancomat, precum și la retrageri de numerar

prin folosirea unui card falsificat sau prin folosirea cardului fără consimțământul titularului său.

În ceea ce privește referirea în considerentele opiniei procurorului general la faptul că instanțele de judecată nu au pus în discuție schimbarea încadrării juridice și au condamnat persoanele acuzate pe baza faptelor din rechizitorii, pronunțând astfel soluții divergente cu privire la semnificația dată faptelor cu care au fost investite (secțiunea 2.1.2 din prezenta decizie), raportul arată că schimbarea încadrării juridice de către instanța de fond este limitată de obiectul judecății, astfel că nu se pot reține fapte noi care nu au făcut obiectul acuzației (vezi Completul de 9 judecători, Decizia nr. 74 din 8 octombrie 2001), iar schimbarea încadrării juridice de către instanțele de control este, în plus, limitată de principiul neagrării situației în propria cale de atac (art. 372, art. 385⁸ din Codul de procedură penală). În consecință, chiar pentru soluțiile pronunțate după publicarea deciziei în interesul legii, principiile anterioare limitează posibilitatea schimbării încadrării juridice pentru faptele care au făcut deja obiectul investirii instanțelor.

5.3. Analiza consecințelor cu privire la încadrarea juridică decurgând din:

— scopul urmărit prin montarea dispozitivelor;

— modul în care dispozitivele de citire a benzii magnetice a cardului autentic și a codului PIN aferent interacționează cu sistemul informatic al băncii;

— modul în care cardul interacționează cu sistemul băncii și consecințele produse în cazul în care cardul este falsificat sau cardul este autentic, dar este folosit fără acordul titularului său.

Montarea la bancomat a dispozitivelor de citire a benzii magnetice a cardului autentic și a codului PIN aferent acestuia (minivideocamere sau dispozitive tip tastatură) urmată de descoperirea faptei înainte ca victima să folosească un card la bancomatul respectiv, prima dintre ipotezele analizate presupune distincția dintre legea generală, Legea nr. 161/2003 și legea specială, Legea nr. 365/2002. Rezolvarea problemei de drept determinată de ipoteza menționată anterior are în vedere opinia Departamentului de drept penal al Facultății de Drept a Universității din București (secțiunea 4.4.3 din prezenta decizie) și opinia Departamentului de drept public al Universității „Babeș-Bolyai” (secțiunea 4.3.3 din prezenta decizie), cu privire la distincția dintre art. 25 din Legea nr. 365/2002 și art. 46 alin. (2) din Legea nr. 161/2003, opiniile trimise de Institutul de Cercetări Juridice al Academiei Române (secțiunea 4.2.1 din prezenta decizie), Catedra de drept penal din cadrul Facultății de Drept și Științe Administrative a Universității din Craiova (secțiunea 4.5.2 din prezenta decizie), Departamentul de drept public din cadrul Facultății de Drept a Universității de Vest din Timișoara (secțiunea 4.7.2 din prezenta decizie), cu privire la încadrarea juridică, precum și punctul de vedere trimis de Universitatea „Lucian Blaga” din Sibiu (secțiunea 4.6.1 din prezenta decizie) cu privire la administrarea probelor pentru clarificarea scopului deținerii echipamentelor.

În ambele ipoteze reglementate de Legea nr. 161/2003 și Legea nr. 365/2002, legiuitorul a incriminat actele de pregătire: deținerea, fără drept, a unui dispozitiv, program informatic, parolă, cod de acces sau dată informatică în scopul săvârșirii uneia dintre infracțiunile contra confidențialității și integrității datelor și sistemelor informatice [art. 46 alin. (2) din Legea nr. 161/2003], respectiv fabricarea ori deținerea de echipamente, inclusiv hardware sau software, cu scopul de a servi la falsificarea instrumentelor de plată electronică (art. 25 din Legea nr. 355/2002). În ambele ipoteze legiuitorul a incriminat o faptă similară celei prevăzute de art. 285 din Codul penal (deținerea de instrumente în vederea falsificării de valori), apreciind că și în materia infracțiunilor informatice actele de pregătire au un pericol social generic semnificativ, astfel că trebuie asimilate faptului consumat și incluse în ilicitul penal.

Includerea actelor de pregătire în ilicitul penal este consecința scopului pentru care acestea s-au produs: săvârșirea uneia dintre infracțiunile contra confidențialității și integrității datelor și sistemelor informatice, respectiv falsificarea instrumentelor de plată electronică. Dovedirea scopului deținerii echipamentelor este în consecință de esența reținerii vinovăției persoanei acuzate și stabilirii încadrării juridice corecte.

Elementul material comun celor două infracțiuni, respectiv deținerea de echipamente, inclusiv hardware sau software, face necesară analiza criteriilor de diferențiere a faptelor. Încadrarea juridică dată faptelor de deținere a respectivelor dispozitive este diferită în raport cu scopul urmărit de persoana acuzată prin montarea acestora:

a) dacă probele administrate conduc la concluzia că prin montarea dispozitivelor se urmărește scopul prevăzut de art. 42—45 din Legea nr. 161/2003 sunt întrunite elementele constitutive ale infracțiunii prevăzute de art. 46 alin. (2) din Legea nr. 161/2003;

b) dacă probele administrate conduc la concluzia că prin montarea dispozitivelor se urmărește falsificarea instrumentelor de plată electronice sunt întrunite elementele constitutive ale infracțiunii prevăzute de art. 25 din Legea nr. 365/2002.

Montarea la bancomat a dispozitivelor de citire a benzii magnetice a cardului autentic și a codului PIN aferent reprezintă acte de pregătire a infracțiunilor săvârșite prin intermediul sistemelor informatice, incriminate ca infracțiune distinctă indiferent dacă datele au fost transferate sau de modul în care urmează să fie folosite datele transferate.

Deși montarea dispozitivelor de citire a benzii magnetice a cardului autentic și a codului PIN aferent este infracțiune independent de realizarea transferului neautorizat de date, odată ce transferul datelor operează, ia naștere un concurs de infracțiuni între deținerea dispozitivelor și utilizarea lor. Scopul în care datele urmează să fie folosite ulterior face însă și diferența între infracțiunea prevăzută de art. 46 alin. (2) din Legea nr. 161/2003 și art. 25 din Legea nr. 365/2002. Montarea dispozitivelor de citire a benzii magnetice a cardului autentic și a codului PIN aferent la bancomat probează scopul săvârșirii unor infracțiuni informatice care au ca premisă captarea datelor pentru care dispozitivele au fost create. În lipsa altor probe care să dovedească faptul că scopul este circumscris doar săvârșirii infracțiunii de falsificare a instrumentelor de plată, încadrarea juridică va fi cea prevăzută de art. 46 alin. (2) din Legea nr. 161/2003.

Legea nr. 161/2003 sancționează infracțiuni îndreptate contra confidențialității și integrității datelor și sistemelor informatice, în timp ce Legea nr. 365/2002 privind comerțul electronic incriminează infracțiuni îndreptate împotriva securității și integrității instrumentelor de plată electronice. Spre deosebire de infracțiunile din Legea nr. 161/2003, cele prevăzute de Legea nr. 365/2002 sunt îndreptate efectiv spre integritatea fizică a instrumentului de plată, care este clonat sau falsificat. Datele informatice conținute pe banda magnetică a cardului bancar autentic sunt absolut necesare atât pentru efectuarea unor operațiuni financiare în mod fraudulos, cât și pentru falsificarea unui card bancar. În consecință este incident art. 46 alin. (2) din Legea nr. 161/2003 atunci când dispozitivele de citire a benzii magnetice a cardului autentic și a codului PIN aferent au fost deținute în scopul săvârșirii uneia dintre infracțiunile prevăzute la art. 42—45 din Legea nr. 161/2003. Este incident art. 25 din Legea nr. 365/2002 atunci când se probează că dispozitivele de citire a benzii magnetice a cardului autentic și a codului PIN aferent au fost deținute în scopul de a servi la falsificarea instrumentelor de plată electronică.

Obținerea datelor de pe card, prin dispozitivele de citire a benzii magnetice a cardului autentic și a codului PIN aferent, chiar dacă nu este suficientă prin ea însăși pentru falsificarea

instrumentelor de plată, deoarece ulterior datele trebuie să fie inscripționate pe un alt mediu de stocare, realizează elementul material al infracțiunii prevăzute de art. 25 din Legea nr. 365/2002. Legea nr. 365/2002 cere ca echipamentele să fie deținute cu scopul de a servi la falsificarea instrumentelor de plată electronică. Legea nu incriminează fapta doar dacă sunt deținute toate echipamentele care conduc la falsificarea instrumentelor de plată, fiind suficient ca, în ipoteza avută în vedere de recursul în interesul legii, montarea la bancomat a dispozitivelor, să se probeze că datele urmau să fie folosite pentru clonarea cardurilor.

În cazul în care se probează că dispozitivele s-au folosit pentru a produce, fără drept, o parolă, un cod de acces sau alte asemenea date informatice care permit accesul total sau parțial la un sistem informatic în scopul săvârșirii uneia dintre infracțiunile prevăzute la art. 42—45, fapta va constitui infracțiunea prevăzută de art. 46 alin. (1) lit. b) din Legea nr. 161/2003.

c) *Montarea la bancomat a dispozitivelor de citire a benzii magnetice a cardului autentic și a codului PIN aferent acestuia (minivideocamera sau dispozitive tip tastatură) urmată de folosirea bancomatului de către victimă realizează un transfer de date de pe card.*

Rezolvarea problemei de drept determinată de ipoteza menționată anterior are în vedere opinia Institutului pentru Tehnologii Avansate, conform căreia nu se realizează un acces la sistemul informatic al băncii, dar se realizează un transfer de date din mijlocul de stocare a datelor informatice reprezentat de card (secțiunea 4.1.1. din prezenta decizie), opinia Departamentului de drept penal a Facultății de Drept a Universității din București (secțiunea 4.4.1. din prezenta decizie).

De asemenea, conform art. 2 din Regulamentul Băncii Naționale a României nr. 6/2006 privind emiterea și utilizarea instrumentelor de plată electronică și relațiile dintre participanții la tranzacțiile cu aceste instrumente, publicat în Monitorul Oficial al României, Partea I, nr. 927 din 15 noiembrie 2006, se prevede că în înțelesul regulamentului, termenii și expresiile de mai jos au următoarele semnificații:

„1. *Cardul emis de o instituție de credit* este un instrument de plată electronică, respectiv un suport de informație standardizat, securizat și individualizat, care permite deținătorului său să folosească disponibilitățile bănești proprii dintr-un cont deschis pe numele său la emitentul cardului și/sau să utilizeze o linie de credit, în limita unui plafon stabilit în prealabil, deschisă de emitent în favoarea deținătorului cardului, în vederea efectuării uneia sau mai multora dintre următoarele operațiuni:

a) retragerea sau depunerea de numerar de la terminale precum distribuitoarele de numerar și/sau ATM, de la ghișeele emitentului/instituției acceptante sau de la sediul unei instituții, obligată prin contract să accepte instrumentul de plată electronică, respectiv încărcarea și descărcarea unităților valorice în cazul monedei electronice;

b) plata bunurilor achiziționate și/sau serviciilor prestate de comercianții acceptanți și/sau emitenți (de exemplu, plata serviciilor prestate de companii în domeniul telefoniei mobile, fixe, transmisii de date, servicii de televiziune și internet sau de către alți furnizori de utilități), precum și plata obligațiilor către autoritățile administrației publice, reprezentând impozite, taxe, amenzi, penalități etc., prin intermediul imprinterelor, terminalelor POS, ATM sau prin alte medii electronice.”

În consecință prin montarea dispozitivelor tip skimmer peste fanta de introducere a cardului la un echipament cu interfață de card bancar se realizează, dacă victima folosește bancomatul, transferul neautorizat de date informatice din mijloacele de stocare a datelor informatice. În acest caz mijlocul de stocare a

datelor informatice este reprezentat de cardul bancar utilizat de titular, în perioada în care sunt montate dispozitivele frauduloase.

Utilizarea dispozitivelor de citire a benzii magnetice a cardului autentic și a codului PIN aferent, de către persoana acuzată, pentru a copia informațiile de pe banda magnetică a cardului bancar, reprezintă infracțiunea de transfer neautorizat de date dintr-un mijloc de stocare a datelor informatice, reprezentat de cardul bancar, prevăzută de art. 44 alin. (3) din Legea nr. 161/2003.

d) Montarea la bancomat a dispozitivelor de citire a benzii magnetice a cardului autentic și a codului PIN aferent acestuia (minivideocamere sau dispozitive tip tastatură) urmată de utilizarea bancomatului de către victimă și transmiterea datelor de pe card și de utilizare a datelor de către persoana acuzată

Rezolvarea problemei de drept determinată de ipoteza menționată anterior are în vedere opinia Institutului de Cercetări Juridice al Academiei Române (secțiunea 4.2.2. din prezenta decizie), Departamentului de drept penal a Facultății de Drept a Universității din București (secțiunea 4.4.3. din prezenta decizie), Departamentului de drept public al Universității „Babeș-Bolyai” (secțiunea 4.3.2 și 4.3.3 din prezenta decizie), Catedrei de drept penal din cadrul Facultății de Drept și Științe Administrative a Universității din Craiova (secțiunea 4.5.2 din prezenta decizie), Universității Lucian Blaga din Sibiu (secțiunea 4.6.3 din prezenta decizie), Departamentului de drept public din cadrul Facultății de Drept a Universității de Vest din Timișoara (secțiunea 4.7.2 din prezenta decizie).

În acest caz probele administrate trebuie să clarifice dacă intenția aceluia care captează datele de pe card este de a clona instrumentul de plată electronică sau dacă intenția sa este de a utiliza datele obținute de pe banda magnetică în vederea efectuării unor plăți on-line. Încadrarea juridică dată faptelor este diferită în raport cu scopul urmărit de persoana acuzată.

În cazul în care se probează că dispozitivele s-au folosit pentru a produce, fără drept, o parolă, un cod de acces sau alte asemenea date informatice care permit accesul total sau parțial la un sistem informatic în scopul săvârșirii uneia dintre infracțiunile prevăzute la art. 42—45, sunt întrunite elementele constitutive ale infracțiunii prevăzute de art. 46 alin. (1) lit. (b) din Legea nr. 161/2003. Introducerea unui card bancar falsificat sau a unui autentic, fără consimțământul titularului său, la un echipament dotat cu interfață de card bancar, realizează accesul, fără drept, la sistemul informatic al băncii, în scopul obținerii de date informatice și cu încălcarea măsurilor de securitate introduse de bancă, indiferent de tipul operațiunii efectuate: interogare, autentificare, retrageri de numerar, transferuri sau orice alte operațiuni financiare. În cazul folosirii datelor de identificare ale cardurilor bancare pentru efectuarea unor tranzacții on-line, se accesează, fără drept, sistemul informatic al băncii, cu încălcarea măsurilor de securitate introduse de bancă.

Atunci când dispozitivul amplasat ilegal are o existență autonomă și captează informațiile de pe card înainte ca acestea să ajungă în sistemul băncii, accesul la sistemul informatic al băncii nu există, chiar dacă se captează informațiile de pe card. Accesul la un sistem informatic reprezintă o interacțiune logică între dispozitivul montat și sistemul informatic. Interacțiunea logică apare atunci când prin intermediul dispozitivului se beneficiază de resursele ori/și funcțiile sistemului informatic. Doar în acest caz, prin interacțiunea fizică cu sistemul informatic (pornirea acestuia, transmiterea unor comenzi prin utilizarea tastaturii etc.) se creează și o interacțiune la nivel logic. Interacțiunea cu tastatura (apăsarea tastelor) inițiază o interacțiune logică doar dacă sistemul informatic vizat ajunge să recepționeze informația transmisă prin intermediul tastaturii, să

o interpreteze cu ajutorul unui program informatic și să returneze un răspuns.

Simpla amplasare a unui dispozitiv electronic în imediata apropiere a bancomatului sau chiar în contact fizic cu respectivul sistem, fără ca cele două componente (sistemul informatic și dispozitivul electronic) să comunice, nu poate fi apreciată ca fiind un acces neautorizat. Montarea dispozitivelor de citire a benzii magnetice a cardurilor la un echipament dotat cu interfață de card bancar are însă ca rezultat transferul neautorizat de date informatice din mijloacele de stocare a datelor informatice, reprezentate de cardurile bancare utilizate de titulari, în perioada în care sunt montate dispozitivele frauduloase. Montarea dispozitivelor dotate cu cameră video sau tastatură falsă permite interceptarea, fără drept, a transmisiei de date informatice care nu este publică și este destinată sistemului informatic al băncii, și anume codul PIN, un cod de securitate introdus de bancă pentru restricționarea accesului utilizatorilor neautorizați la sistemul informatic al băncii.

În ceea ce privește sistemul informatic al băncii, chiar și în situația amplasării unei tastaturi false deasupra tastaturii originale de la ATM sau POS, doar tastatura originală face parte din sistemul informatic bancar și doar prin intermediul său se transmite codul de acces la sistemul informatic, astfel că tastatura falsă (care prezintă, la rândul ei, trăsăturile specifice unui sistem informatic) nu ajunge să fie integrată în sistemul informatic al băncii și să acceseze astfel, fără drept, sistemul informatic al băncii în scopul obținerii de date informatice. O interacțiune logică poate avea la bază și o interacțiune fizică, dar o interacțiune fizică nu implică în mod necesar și o interacțiune logică.

În cazul utilizării la bancomat a dispozitivelor de citire a benzii magnetice a cardului autentic și a codului PIN aferent acestuia are loc un transfer neautorizat de date dintr-un mijloc de stocare a datelor informatice, reprezentat de cardul bancar. Cardul conține informații într-o formă care poate fi prelucrată prin sistemul informatic al băncii, astfel că din perspectiva art. 35 alin. (1) lit. d) din Legea nr. 161/2003 reprezintă un mediu de stocare a datelor informatice, a cărui protecție se realizează inclusiv prin mijloace de drept penal.

Transferul neautorizat de date are loc fără ca dispozitivul de citire să interacționeze cu sistemul informatic al băncii. Odată ce cardul a fost introdus în bancomat și codul tastat, datele de pe cardul introdus în bancomat și codul PIN pot fi transferate chiar dacă respectivul bancomat nu este funcțional sau este în revizie.

e) Folosirea unui card bancar autentic, însă fără acordul titularului său, în scopul efectuării unor retrageri de numerar la bancomat

Rezolvarea problemei de drept determinate de ipoteza menționată anterior are în vedere opinia Institutului de Cercetări Juridice al Academiei Române (secțiunea 4.2.2 din prezenta decizie), Departamentului de drept penal al Facultății de Drept a Universității din București (secțiunea 4.4.4 din prezenta decizie), Departamentului de drept public al Universității „Babeș-Bolyai” (secțiunea 4.3.4 din prezenta decizie), Catedrei de drept penal din cadrul Facultății de Drept și Științe Administrative a Universității din Craiova (secțiunea 4.5.3 din prezenta decizie), Universității „Lucian Blaga” din Sibiu (secțiunea 4.6.3 din prezenta decizie), Departamentului de drept public din cadrul Facultății de Drept a Universității de Vest din Timișoara (secțiunea 4.7.3 din prezenta decizie).

Folosirea unui card bancar autentic, însă fără acordul titularului său, în scopul efectuării unor retrageri de numerar la bancomat, întrunește elementele constitutive ale infracțiunii de efectuare de operațiuni financiare în mod fraudulos prin utilizarea unui instrument de plată electronică, inclusiv a datelor de identificare care permit utilizarea acestuia — art. 27 alin. (1)

din Legea nr. 365/2002, săvârșită în concurs cu infracțiunea de acces, fără drept, la un sistem informatic comisă în scopul obținerii de date informatice prin încălcarea măsurilor de securitate — art. 42 alin. (1), (2) și (3) din Legea nr. 161/2003.

Folosirea cardului inscripționat cu datele culese de pe cardul autentic, oricare ar fi fost modul de obținere a acestora, ori folosirea cardului autentic, fără acordul titularului său, la ATM 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. Bancomatul face parte din sistemul informatic bancar, datele transmise și receptate fiind protejate prin măsuri de securitate încorporate în sistemul de citire a cardurilor și în codul PIN.

În cazul folosirii la ATM atât a cardului falsificat, cât și a celui real, fără consimțământul titularului său, se realizează un acces fără drept la sistemul informatic:

— în cazul cardului real, prin introducerea cardului și tastarea codului PIN care înlătură măsura de securitate reprezentată de codul de acces;

— în cazul cardului falsificat, prin recunoașterea cardului ca fiind un card valid și prin schimbul de informații între posesorul cardului și mediul de stocare a datelor privitoare la contul bancar atașat cardului.

Infracțiunea de acces fără drept la un sistem informatic este consumată prin folosirea codului PIN, chiar dacă nu se solicită nicio operațiune financiară. Această ipoteză nu exclude însă concursul ideal pentru cazul în care cardul autentic este folosit pentru retrageri de numerar, având în vedere că în acest caz accesul la sistemul informatic inițiat prin folosirea codului PIN se menține pe durata tranzacției și se epuizează prin retragerea de numerar.

f) *Folosirea unui card bancar falsificat, la bancomat, pentru retrageri de numerar*

Rezolvarea problemei de drept determinate de ipoteza menționată anterior are în vedere opinia Departamentului de drept penal al Facultății de Drept a Universității din București (secțiunea 4.4.4 din prezenta decizie), Departamentului de drept public al Universității „Babeș-Bolyai” (secțiunea 4.3.4 din prezenta decizie), Catedrei de drept penal din cadrul Facultății de Drept și Științe Administrative a Universității din Craiova (secțiunea 4.5.3 din prezenta decizie), Universității „Lucian Blaga” din Sibiu (secțiunea 4.6.3 din prezenta decizie), Departamentului de drept public din cadrul Facultății de Drept a Universității de Vest din Timișoara (secțiunea 4.7.3 din prezenta decizie).

Folosirea unui card bancar falsificat, la bancomat, pentru retrageri de numerar întrunește elementele constitutive ale infracțiunii prevăzute de art. 27 alin. (1) din Legea nr. 365/2002, în concurs cu infracțiunea de acces, fără drept, la un sistem informatic comisă în scopul obținerii de date informatice prin încălcarea măsurilor de securitate — art. 42 alin. (1), (2) și (3) din Legea nr. 161/2003 și în concurs cu infracțiunea de falsificare a instrumentelor de plată electronică — art. 24 alin. (2) din Legea nr. 365/2002.

Introducerea unui card bancar falsificat realizează accesul, fără drept, la sistemul informatic al băncii, în scopul obținerii de date informatice și cu încălcarea măsurilor de securitate introduse de bancă, indiferent de tipul operațiunii efectuate. În raport cu tipul operațiunii efectuate prin intermediul cardului falsificat (interogare, autentificare, retrageri de numerar, transferuri plăți on-line sau orice alte operațiuni financiare) se realizează elementul material al laturii obiective din conținutul altor infracțiuni. Astfel, de exemplu, folosirea unui card bancar falsificat, la bancomat, pentru retrageri de numerar constituie infracțiunea prevăzută de art. 27 alin. (1) din Legea nr. 365/2002, în concurs cu infracțiunea de acces, fără drept, la

un sistem informatic comisă în scopul obținerii de date informatice prin încălcarea măsurilor de securitate — art. 42 alin. (1), (2) și (3) din Legea nr. 161/2003 și în concurs cu infracțiunea de falsificare a instrumentelor de plată electronică — art. 24 alin. (2) din Legea nr. 365/2002.

O faptă care întrunește elementele constitutive ale infracțiunii prevăzute în art. 24 alin. (2) din Legea nr. 365/2002, în modalitatea punerii în circulație a instrumentelor de plată electronică falsificate, nu întrunește, întotdeauna, și elementele constitutive ale infracțiunii prevăzute în art. 27 alin. (1) din Legea nr. 365/2002. Nici situația contrară nu este întotdeauna posibilă. Astfel, infracțiunea prevăzută în art. 24 alin. (2) din Legea nr. 365/2002, în modalitatea punerii în circulație a instrumentelor de plată electronică falsificate, nu se realizează, în mod obligatoriu, prin retrageri de numerar, ci se poate realiza, de exemplu, prin vânzarea instrumentelor de plată electronică falsificate.

În ceea ce privește distincția dintre alineatele art. 27 din Legea nr. 365/2002, raportul arată că Secția penală a adoptat anterior și a transmis instanțelor de judecată punctul de vedere conform căruia alin. (1) nu precizează că efectuarea operațiunii financiare se realizează numai prin utilizarea instrumentului de plată electronică original, fără consimțământul titularului instrumentului respectiv, ci, dimpotrivă, include în sfera de aplicare a normei de incriminare efectuarea de operațiuni financiare prin utilizarea datelor de identificare ce permit folosirea instrumentului de plată electronică, fără consimțământul titularului instrumentului respectiv. În concluzie, conform practicii Secției penale a Înaltei Curți de Casație și Justiție, art. 27 alin. (1) din Legea nr. 365/2002 incriminează atât efectuarea de operațiuni financiare prin utilizarea instrumentului de plată electronică original, fără consimțământul titularului instrumentului respectiv, cât și efectuarea de operațiuni financiare prin utilizarea unui instrument de plată electronică falsificat care permite folosirea datelor de identificare ale instrumentului de plată electronică original, fără consimțământul titularului instrumentului respectiv.

Soluția propusă în secțiunea de față decurge și din Decizia nr. 5.288 din 15 septembrie 2006 a Secției penale a Înaltei Curți de Casație și Justiție prin care a fost soluționată problema de drept privind existența concursului între infracțiunea prevăzută în art. 24 alin. (1) din Legea nr. 365/2002 și infracțiunea prevăzută în art. 24 alin. (2) din aceeași lege. Decizia menționată prevede că punerea în circulație a instrumentelor de plată electronică falsificate se poate realiza prin retragerea sumelor de bani în numerar, nefiind necesară transmiterea posesiei instrumentelor de plată electronică falsificate către alte persoane. Decizia are în vedere faptul că punerea în circulație a instrumentelor tip card nu este strict legată de transmiterea materială a acestora, fiind în acord cu modul în care Banca Națională a României (BNR) a clasificat tranzacțiile efectuate prin card. Astfel, Regulamentul BNR nr. 6 din 11 octombrie 2006, privind emiterea și utilizarea instrumentelor de plată electronică și relațiile dintre participanții la tranzacțiile cu aceste instrumente prevede că, în raport cu prezența fizică a cardului, tranzacțiile prin card pot fi clasificate astfel: (i) tranzacții unde cardul este prezent — locații comerciale tradiționale, ATM și ghișee de bancă — reprezintă acele tranzacții unde banda magnetică a cardului sau cipul cardului este citită/citit electronic sau unde se obține amprenta elementelor confecționate în relief a cardului pe chitanță cu ajutorul imprimantului mecanic; (ii) tranzacții unde cardul nu este prezent reprezintă tranzacțiile ordonate prin telefon, poștă, internet, unde nu există dovada participării fizice a cardului, însă deținătorul trebuie să furnizeze parole sau coduri, de exemplu, Card Verification Value (CVV2), parola e-commerce etc.

Infracțiunea prevăzută în art. 27 alin. (1) din Legea nr. 365/2002, în modalitatea efectuării unei operațiuni financiare prin utilizarea datelor de identificare ce permit folosirea unui instrument de plată electronică, fără consimțământul titularului instrumentului respectiv, nu presupune, în mod obligatoriu, falsificarea instrumentului de plată electronică original. Infracțiunea se poate realiza fără falsificarea acestuia, de exemplu, prin efectuarea unui transfer de fonduri, prin internet, prin utilizarea datelor de identificare ce permit folosirea instrumentului de plată electronică, fără consimțământul titularului său.

Faptul că fiecare dintre infracțiunile prevăzute în art. 24 alin. (2) și în art. 27 alin. (1) din Legea nr. 365/2002 poate fi săvârșită prin acțiuni distincte nu exclude însă posibilitatea ca printr-o singură acțiune, săvârșită în anumite împrejurări, să fie întrunite atât elementele constitutive ale infracțiunii prevăzute în art. 24 alin. (2) din Legea nr. 365/2002, cât și elementele constitutive ale infracțiunii prevăzute în art. 27 alin. (1) din aceeași lege, cum este ipoteza retragerii de numerar prin utilizarea unui instrument de plată electronică falsificat, pe care sunt imprimate datele de identificare ale instrumentului de plată electronică original. De exemplu, concursul ideal există în cazul în care cardul falsificat este folosit pentru retrageri de numerar, având în vedere că accesul la sistemul informatic inițiat prin folosirea codului PIN se menține pe durata tranzacției și se epuizează abia prin retragerea de numerar.

g) *Încredințarea cardului falsificat pentru a fi folosit la bancomat pentru retrageri de numerar*

Rezolvarea problemei de drept determinate de ipoteza menționată anterior are în vedere opinia Departamentului de drept penal al Facultății de Drept a Universității din București (secțiunea 4.4.3 din prezenta decizie) și opinia Departamentului de drept public al Universității „Babeș-Bolyai” (secțiunile 4.3.2 și 4.3.3. din prezenta decizie).

Înmânarea cardului falsificat unei terțe persoane ori deținerea cardului falsificat în acest scop constituie infracțiunea prevăzută de art. 24 alin. (2) din Legea nr. 365/2002.

Soluțiile preconizate în ipotezele de mai sus au în vedere faptul că montarea la bancomat a dispozitivelor de citire a benzii magnetice a cardului autentic și a codului PIN aferent presupune, în cazul dispozitivelor autonome, doar captarea datelor (conținute pe card) pentru care dispozitivele au fost create, nu și accesul la sistemul informatic al băncii. Scopul transferării datelor constituie un element esențial al infracțiunii și face diferența între actele preparatorii incriminate de Legea nr. 161/2003 și Legea nr. 365/2002. Folosirea la bancomat pentru retragerea de numerar a cardului falsificat ori a celui autentic, fără acordul titularului său, presupune însă accesul la sistemul informatic al băncii. În acest caz accesul la sistemul informatic inițiat prin folosirea codului PIN se menține pe durata tranzacției și se epuizează prin retragerea de numerar, astfel că infracțiunile care iau naștere ca urmare a folosirii codului PIN și retragerii de numerar sunt în concurs ideal.

6. Înalta Curte de Casație și Justiție

6.1. Obiectul recursului în interesul legii

Pentru soluționarea prezentului recurs în interesul legii s-a stabilit termen de judecată la 16 septembrie 2013, dată la care completul competent să judece recursul a constatat, analizând considerentele scrise, că, deși obiectul sesizării, astfel cum este precizat la pagina 1 din opinia procurorului general, este limitat la corecta interpretare a dispozițiilor art. 42 alin. (1), (2) și (3) din Legea nr. 161/2003, în cuprinsul acestora se face referire la mai multe texte de lege care ar avea incidență în situațiile de fapt reținute de instanțe, respectiv dispozițiile art. 25, art. 24 alin. (1) și (2), art. 27 alin. (1) din Legea nr. 365/2002, ultimele două texte de lege fiind incluse și în soluția propusă de procurorul general în argumentele finale.

În raport cu aceste referiri, precum și cu multiplele situații care rezultă din raportul întocmit la dosar și punctele de vedere exprimate în scris, Completul competent să judece recursul în interesul legii a apreciat că se impune repunerea cauzei pe rol, în vederea lămuririi obiectului sesizării, atât în raport cu concluziile scrise din preambulul recursului în interesul legii, cât și în raport cu cele din finalul sesizării, în care se face referire la mai multe texte de lege.

Pentru aceste motive, cu respectarea dispozițiilor art. 4144 alin. 9 din Codul de procedură penală, în urma deliberărilor, cu unanimitate de voturi, Completul competent să judece recursul în interesul legii a dispus repunerea cauzei pe rol și a stabilit termen de judecată la data de 14 octombrie 2013.

La data de 10 octombrie 2013, ca urmare a solicitării de precizare a obiectului recursului, dispusă de instanță prin încheierea din 16 septembrie 2013, procurorul general al Parchetului de pe lângă Înalta Curte de Casație și Justiție a înaintat concluzii privind obiectul sesizării, menționând că problema de drept a cărei dezlegare o solicită se referă la stabilirea modului unitar de interpretare și aplicare a dispozițiilor art. 42 alin. (1), (2) și (3) din Legea nr. 161/2003, în ceea ce privește înțelesul sintagmei *acces fără drept la un sistem informatic*. S-a mai precizat că nu formează obiect al sesizării prin prezentul recurs în interesul legii situațiile de fapt descrise la pct. 7 lit. b, c, d și g din Raportul întocmit de judecătorul-raportor (secțiunea 5.3 din prezenta decizie) prin care se propune și proiectul de minută.

Completul competent să judece recursul în interesul legii, investit în limitele precizate de procurorul general al Parchetului de pe lângă Înalta Curte de Casație și Justiție în concluziile scrise, susținute oral, a reținut dosarul în pronunțare asupra recursului în interesul legii, stabilind următoarele:

6.2. *Montarea la bancomat a dispozitivelor autonome de citire a benzii magnetice a cardului autentic și a codului PIN aferent acestuia (skimmere, minivideocamere sau dispozitive tip tastatură falsă) constituie infracțiunea prevăzută de art. 46 alin. (2) din Legea nr. 161/2003.*

Montarea la bancomat a dispozitivelor autonome de citire a benzii magnetice a cardului autentic și a codului PIN aferent acestuia (skimmere, minivideocamere sau dispozitive tip tastatură falsă) nu reprezintă un acces la sistemul informatic al băncii, singura conduită ce intră în ilicitul penal fiind deținerea respectivelor dispozitive.

Legea nr. 161/2003 incriminează în art. 42 fapta de acces ilegal la un sistem informatic într-o variantă tip, în alin. (1) și în două variante agravante, în alin. (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.

Prin montarea la ATM a dispozitivului de citire a benzii magnetice a cardului și a videocamerei ori a dispozitivului modificat de tip tastatură nu se realizează accesul fără drept la sistemul informatic al băncii, deoarece lipsește interacțiunea făptuitorului cu tehnica de calcul. Obținerea datelor de pe banda magnetică a cardului autentic se realizează în exteriorul bancomatului și fără ca dispozitivele menționate să intre în conexiune cu sistemul informatic al băncii. Dispozitivele de skimming nu au caracteristicile unui sistem informatic, indiferent dacă este vorba de camere video, dispozitive de citire a benzii magnetice a cardului sau tastatură falsă, deoarece nu asigură prelucrarea automată a datelor, cu ajutorul unui program informatic, permițând doar copierea codurilor înscrise pe cardul care asigură accesarea sistemului informatic.

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. 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 din cauza unei împrejurări extranece vreunei norme de incriminare — atașarea sau nu a skimmerului la bancomat. Citirea datelor de pe banda magnetică a cardului, prin atașarea skimmerului la bancomat, nu interacționează cu softul bancomatului, nu se realizează o solicitare către unitatea centrală de prelucrare a sistemului, care să proceseze date ori să ruleze programe de aplicații în beneficiul făptuitorului, astfel că infracțiunea de acces fără drept la sistemul informatic ar fi lipsită de însuși elementul său material.

Conform legii, art. 46 alin. (2) din Legea nr. 161/2003, este incriminată deținerea, fără drept, a unui dispozitiv, program informatic, parolă, cod de acces sau dată informatică dintre cele prevăzute la art. 46 alin. (1) din Legea nr. 161/2003, în scopul săvârșirii uneia dintre infracțiunile prevăzute la art. 42—45 din aceeași lege.

Deținerea dispozitivelor de citire a benzii magnetice a cardului, minivideocamerelor sau dispozitivelor tip tastatură și, implicit, montarea acestora pentru citirea benzii magnetice a cardului concomitent cu captarea codului PIN aferent cardului constituie acte pregătitoare în vederea săvârșirii infracțiunii de acces fără drept la un sistem informatic, prevăzute de art. 42 din Legea nr. 161/2003, care în considerarea gradului mare de pericol social pe care îl prezintă, prin ele însele, au determinat incriminarea din art. 46 alin. (2) din aceeași lege.

6.3. Folosirea la bancomat a unui card bancar autentic, fără acordul titularului său, în scopul efectuării unor retrageri de numerar, constituie infracțiunea de efectuare de operațiuni financiare în mod fraudulos prin utilizarea unui instrument de plată electronică, inclusiv a datelor de identificare care permit utilizarea acestuia, prevăzută de art. 27 alin. (1) din Legea nr. 365/2002, în concurs ideal cu infracțiunea de acces, fără drept, la un sistem informatic comisă în scopul obținerii de date informatice prin încălcarea măsurilor de securitate, prevăzută de art. 42 alin. (1), (2) și (3) din Legea nr. 161/2003.

6.3.1. Dispoziții legale privind falsificarea instrumentelor de plată electronică și efectuarea de operațiuni financiare în mod fraudulos cuprinse în Legea nr. 365/2002 privind comerțul electronic

Legea nr. 365/2002 privind comerțul electronic incriminează falsificarea instrumentelor de plată electronică în art. 24, iar efectuarea de operațiuni financiare în mod fraudulos, în art. 27 din aceeași lege.

Art. 24 din Legea nr. 365/2002

Falsificarea instrumentelor de plată electronică

(1) Falsificarea unui instrument de plată electronică se pedepsește cu închisoare de la 3 la 12 ani și interzicerea unor drepturi.

(2) Cu aceeași pedeapsă se sancționează punerea în circulație, în orice mod, a instrumentelor de plată electronică falsificate sau deținerea lor în vederea punerii în circulație.

[...]

Art. 27 alin. (1) din Legea nr. 365/2002

Efectuarea de operațiuni financiare în mod fraudulos

(1) Efectuarea uneia dintre operațiunile prevăzute la art. 1 pct. 11, prin utilizarea unui instrument de plată electronică, inclusiv a datelor de identificare care permit utilizarea acestuia, fără consimțământul titularului instrumentului respectiv, se pedepsește cu închisoare de la 1 la 12 ani.

Operațiunile prevăzute la art. 1 pct. 11 din Legea nr. 365/2002 sunt: a) transferuri de fonduri, altele decât cele ordonate și executate de către instituții financiare; b) retrageri de numerar, precum și încărcarea și descărcarea unui instrument de monedă electronică.

6.3.2. Decizia-cadru a Consiliului Uniunii Europene din 28 mai 2001 de combatere a fraudei și a falsificării mijloacelor de plată, altele decât numerarul (2001/413/JAI)

Decizia este transpusă în dreptul intern și prin prevederile Legii nr. 365/2002, iar în art. 2 (Infracțiuni în legătură cu instrumentele de plată) se menționează că fiecare stat membru ia măsurile necesare pentru a garanta că următoarele comportamente constituie infracțiune atunci când sunt săvârșite cu intenție, cel puțin în ceea ce privește cârțile de credit, cardurile de tip eurocec, alte carduri emise de instituții financiare, cecurile de călătorie, eurocecurile, alte cecuri și cambii: (a) furtul sau o altă însușire ilegală a unui instrument de plată; (b) contrafacerea sau falsificarea unui instrument de plată în scopul utilizării frauduloase a acestuia; (c) primirea, obținerea, transportul, vânzarea sau transferul către o altă persoană sau posedarea unui instrument de plată furat sau însușit ilegal ori a unui instrument de plată contrafăcut sau falsificat pentru a fi folosit în mod fraudulos; (d) utilizarea frauduloasă a unui instrument de plată furat sau însușit ilegal ori a unui instrument de plată contrafăcut sau falsificat.

6.3.3. Efectuarea de operațiuni financiare în mod fraudulos

Dispozițiile art. 27 alin. (1) din Legea nr. 365/2002 incriminează efectuarea uneia dintre operațiunile prevăzute la art. 1 pct. 11 din aceeași lege, operațiuni care includ retragerile de numerar, prin utilizarea unui instrument de plată electronică, inclusiv a datelor de identificare care permit utilizarea acestuia, fără consimțământul titularului instrumentului respectiv.

Art. 27 alin. (1) din Legea nr. 365/2002 nu precizează că efectuarea operațiunii financiare se realizează numai prin utilizarea instrumentului de plată electronică original, fără consimțământul titularului instrumentului respectiv, ci, dimpotrivă, include în sfera de aplicare a normei de incriminare efectuarea de operațiuni financiare prin utilizarea datelor de identificare care permit folosirea instrumentului de plată electronică, fără consimțământul titularului instrumentului respectiv.

În multe cazuri, retragerile de numerar prin utilizarea datelor de identificare care permit folosirea unui instrument de plată electronică original se realizează prin falsificarea acestuia/prin imprimarea datelor de identificare ale instrumentului de plată electronică original, obținute în mod fraudulos, pe un alt suport, rezultând un instrument de plată electronică falsificat.

În consecință, art. 27 alin. (1) din Legea nr. 365/2002 incriminează atât efectuarea de operațiuni financiare prin utilizarea instrumentului de plată electronică original, fără consimțământul titularului instrumentului respectiv, cât și efectuarea de operațiuni financiare prin utilizarea unui instrument de plată electronică falsificat care permite folosirea datelor de identificare ale instrumentului de plată electronică original, fără consimțământul titularului instrumentului respectiv.

Așadar, art. 27 alin. (1) din Legea nr. 365/2002 constituie atât temeiul legal pentru sancționarea făptuitorului care reține numerar prin utilizarea instrumentului de plată electronică original, fără consimțământul titularului instrumentului respectiv, cât și temeiul legal pentru pedepsirea făptuitorului care reține numerar prin utilizarea unui instrument de plată electronică falsificat, pe care sunt imprimate datele de identificare ale instrumentului de plată electronică original. A admite că art. 27 alin. (1) din Legea nr. 365/2002 constituie temeiul legal numai pentru pedepsirea făptuitorului care reține numerar prin utilizarea instrumentului de plată electronică original înseamnă a conferi impunitate făptuitorului care reține numerar prin utilizarea unui instrument de plată electronică falsificat, pe care sunt imprimate datele de identificare ale instrumentului de plată electronică original, deși textul art. 27 alin. (1) din Legea nr. 365/2002 se referă explicit la folosirea datelor de identificare care permit utilizarea instrumentului de plată electronică.

Noul Cod penal separă, cu mai multă claritate, ipoteza utilizării instrumentului de plată electronică și ipoteza utilizării datelor de identificare, stabilind, în art. 250 alin. (1), *efectuarea de operațiuni financiare în mod fraudulos, că: efectuarea unei operațiuni de retragere de numerar, încărcare sau descărcare a unui instrument de monedă electronică ori de transfer de fonduri, prin utilizarea, fără consimțământul titularului, a unui instrument de plată electronică sau a datelor de identificare care permit utilizarea acestuia, se pedepsește cu închisoare de la 2 la 7 ani.*

De asemenea, Decizia-cadru a Consiliului Uniunii Europene din 28 mai 2001 (2001/413/JAI) se referă, în art. 2 lit. (d), atât la utilizarea frauduloasă a unui instrument de plată furat sau însușit ilegal (instrument de plată original), cât și la utilizarea frauduloasă a unui instrument de plată contrafăcut sau falsificat.

Nu în ultimul rând, art. 28 alin. (1) din Legea nr. 365/2002, referitor la *acceptarea operațiunilor financiare efectuate în mod fraudulos, incriminează „acceptarea uneia dintre operațiunile prevăzute la art. 1 pct. 11, cunoscând că este efectuată prin folosirea unui instrument de plată electronică falsificat sau utilizat fără consimțământul titularului său”. Or, este dificil de admis că legiuitorul a incriminat acceptarea unei operațiuni financiare atât în cazul în care este efectuată prin folosirea unui instrument de plată electronică falsificat, cât și în cazul în care este efectuată prin folosirea instrumentului de plată electronică original utilizat fără consimțământul titularului său, dar a incriminat numai efectuarea unei operațiuni financiare prin utilizarea instrumentului de plată electronică original fără consimțământul titularului său, iar nu și efectuarea unei operațiuni financiare prin utilizarea unui instrument de plată electronică falsificat.*

Prin folosirea la ATM a cardului autentic, fără acordul titularului său, se accesează fără drept un sistem informatic, în scopul obținerii de date informatice, prin încălcarea măsurilor de securitate, fapta incriminată de art. 42 alin. (1), (2) și (3) din Legea nr. 161/2003.

În cazul în care cardul este folosit pentru retrageri de numerar, având în vedere că accesul la sistemul informatic inițiat prin folosirea codului PIN se epuizează prin retragerea de numerar, ia naștere un concurs ideal cu infracțiunea prevăzută de art. 27 alin. (1) din Legea nr. 365/2002. Astfel dacă ulterior accesului fără drept la un sistem informatic, în scopul obținerii de date informatice, prin încălcarea măsurilor de securitate, se vor efectua și operațiuni financiare (retrageri de sume, plăți, transferuri etc.), infracțiunea de acces neautorizat va veni în concurs cu infracțiunea prevăzută de art. 27 alin. (1) din Legea nr. 365/2002, constând în efectuarea de operațiuni financiare în mod fraudulos, infracțiuni aflate în concurs ideal.

Făptuitorul transmite prin intermediul componentelor sistemului (tastatură) 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 amenințată. Legătura de cauzalitate dintre acțiunea făptuitorului și urmarea produsă datelor informatice rezultă din însăși materialitatea faptei.

6.4. Folosirea la bancomat a unui card bancar falsificat, pentru retrageri de numerar, constituie infracțiunea de efectuare de operațiuni financiare în mod fraudulos prin utilizarea unui instrument de plată electronică, inclusiv a datelor de identificare care permit utilizarea acestuia, prevăzută de art. 27 alin. (1) din Legea nr. 365/2002, în concurs ideal cu infracțiunea de acces, fără drept, la un sistem informatic comisă în scopul obținerii de date informatice prin încălcarea măsurilor de securitate, prevăzută de art. 42 alin. (1), (2) și (3) din Legea nr. 161/2003, și cu infracțiunea de falsificare a instrumentelor de plată electronică, prevăzută de art. 24 alin. (2) din Legea nr. 365/2002.

Punerea în circulație a instrumentelor de plată electronică falsificate și efectuarea de operațiuni financiare în mod fraudulos

Dispozițiile art. 24 alin. (2) din Legea nr. 365/2002 incriminează punerea în circulație, în orice mod, a instrumentelor de plată electronică falsificate sau deținerea lor în vederea punerii în circulație.

În accepțiunea art. 24 alin. (2) din Legea nr. 365/2002, *retragerea de numerar prin utilizarea unui instrument de plată electronică falsificat constituie un mod de punere în circulație a unui instrument de plată electronică falsificat.* Soluția decurge din Decizia nr. 5.288 din 15 septembrie 2006 a Secției penale a Înaltei Curți de Casație și Justiție, conform căreia punerea în circulație a instrumentelor de plată electronică falsificate se poate realiza prin retragerea sumelor de bani în numerar, nefiind necesară transmiterea posesiei instrumentelor de plată electronică falsificate către alte persoane. Soluția decurge și din funcțiile cardului astfel cum sunt precizate în Regulamentul BNR nr. 6 din 11 octombrie 2006, publicat în Monitorul Oficial al României, Partea I, nr. 927 din 15 noiembrie 2006, privind emiterea și utilizarea instrumentelor de plată electronică și relațiile dintre participanții la tranzacțiile cu aceste instrumente. În raport cu prezența fizică a cardului, tranzacțiile prin card pot fi clasificate astfel: (i) tranzacții unde cardul este prezent — locații comerciale tradiționale, ATM și ghișee de bancă — reprezintă acele tranzacții unde banda magnetică a cardului sau cipul cardului este citită/citit electronic sau unde se obține amprenta elementelor confecționate în relief a cardului pe chitanță cu ajutorul imprimantului mecanic; (ii) tranzacții unde cardul nu este prezent reprezintă tranzacțiile ordonate prin telefon, poștă, internet, unde nu există dovada participării fizice a cardului, însă deținătorul trebuie să furnizeze parole sau coduri, de exemplu, Card Verification Value (CVV2), parola e-commerce etc.

În cazul în care făptuitorul efectuează retrageri de numerar prin utilizarea unui instrument de plată electronică falsificat, pe care sunt imprimate datele de identificare ale instrumentului de plată electronică original, sunt întrunite atât elementele constitutive ale infracțiunii prevăzute în art. 24 alin. (2) din Legea nr. 365/2002, cât și elementele constitutive ale infracțiunii prevăzute în art. 27 alin. (1) din Legea nr. 365/2002, aflate în concurs ideal de infracțiuni, conform art. 33 lit. b) din Codul penal. Concursul ideal decurge din faptul că, în cazul în care cardul este folosit pentru retrageri de numerar, accesul la sistemul informatic inițiat prin folosirea codului PIN se epuizează prin retragerea de numerar.

Astfel, acțiunea de a retrage numerar prin utilizarea unui instrument de plată electronică falsificat, pe care sunt imprimate datele de identificare ale instrumentului de plată electronică original:

— realizează elementele constitutive ale infracțiunii prevăzute în art. 24 alin. (2) din Legea nr. 365/2002, întrucât acțiunea de a retrage numerar prin utilizarea unui instrument de plată electronică falsificat reprezintă o punere în circulație, în orice mod, a unui instrument de plată electronică falsificat;

— realizează elementele constitutive ale infracțiunii prevăzute în art. 27 alin. (1) din Legea nr. 365/2002, întrucât acțiunea de a retrage numerar prin utilizarea unui instrument de plată electronică falsificat, pe care sunt imprimate datele de identificare ale instrumentului de plată electronică original, reprezintă efectuarea operațiunii prevăzute la art. 1 pct. 11 lit. b) din Legea nr. 365/2002, prin utilizarea datelor de identificare care permit folosirea unui instrument de plată electronică, fără consimțământul titularului instrumentului respectiv.

În acest context, se impune precizarea că o faptă care întrunește elementele constitutive ale infracțiunii prevăzute în art. 24 alin. (2) din Legea nr. 365/2002, în modalitatea punerii în circulație a instrumentelor de plată electronică falsificate, nu întrunește, întotdeauna, și elementele constitutive ale infracțiunii

prevăzute în art. 27 alin. (1) din Legea nr. 365/2002 și, invers, o faptă care întrunește elementele constitutive ale infracțiunii prevăzute în art. 27 alin. (1) din Legea nr. 365/2002 nu întrunește, întotdeauna, și elementele constitutive ale infracțiunii prevăzute în art. 24 alin. (2) din Legea nr. 365/2002, în modalitatea punerii în circulație a instrumentelor de plată electronică falsificate.

Infracțiunea prevăzută în art. 24 alin. (2) din Legea nr. 365/2002, în modalitatea punerii în circulație a instrumentelor de plată electronică falsificate, nu se realizează, în mod obligatoriu, prin retrageri de numerar, ci se poate realiza, de exemplu, prin vânzarea instrumentelor de plată electronică falsificate.

Infracțiunea prevăzută în art. 27 alin. (1) din Legea nr. 365/2002, în modalitatea efectuării unei operațiuni financiare prin utilizarea datelor de identificare care permit folosirea unui instrument de plată electronică, fără consimțământul titularului instrumentului respectiv, nu presupune, în mod obligatoriu, falsificarea instrumentului de plată electronică original, ci se poate realiza fără falsificarea acestuia, de exemplu, prin

efectuarea unui transfer de fonduri, prin internet, prin utilizarea datelor de identificare care permit folosirea instrumentului de plată electronică, fără consimțământul titularului său.

Faptul că fiecare dintre infracțiunile prevăzute în art. 24 alin. (2) și în art. 27 alin. (1) din Legea nr. 365/2002 poate fi săvârșită prin acțiuni distincte nu exclude însă posibilitatea ca printr-o singură acțiune, săvârșită în anumite împrejurări, să fie întrunite atât elementele constitutive ale infracțiunii prevăzute în art. 24 alin. (2) din Legea nr. 365/2002, cât și elementele constitutive ale infracțiunii prevăzute în art. 27 alin. (1) din aceeași lege, cum este ipoteza retragerii de numerar prin utilizarea unui instrument de plată electronică falsificat, pe care sunt imprimate datele de identificare ale instrumentului de plată electronică original.

Prin folosirea la ATM a cardului inscripționat cu datele culese de pe cardul autentic, oricare ar fi fost modul de obținere a acestora, se accesează de asemenea fără drept 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.

Pentru considerentele arătate, în temeiul art. 414⁴ și 414⁵ din Codul de procedură penală, astfel cum a fost modificat și completat prin Legea nr. 202/2010,

ÎNALTA CURTE DE CASAȚIE ȘI JUSTIȚIE

În numele legii

DECIDE:

Admite recursul în interesul legii formulat de procurorul general al Parchetului de pe lângă Înalta Curte de Casație și Justiție și, în consecință, stabilește că:

1. Montarea la bancomat a dispozitivelor autonome de citire a benzii magnetice a cardului autentic și a codului PIN aferent acestuia (skimmere, minivideocamere sau dispozitive tip tastatură falsă) constituie infracțiunea prevăzută de art. 46 alin. (2) din Legea nr. 161/2003.

2. Folosirea la bancomat a unui card bancar autentic, fără acordul titularului său, în scopul efectuării unor retrageri de numerar, constituie infracțiunea de efectuare de operațiuni financiare în mod fraudulos prin utilizarea unui instrument de plată electronică, inclusiv a datelor de identificare care permit utilizarea acestuia, prevăzută de art. 27 alin. (1) din Legea nr. 365/2002, în concurs ideal cu infracțiunea de acces, fără drept, la un sistem informatic comisă în scopul obținerii de date informatice prin încălcarea măsurilor de securitate, prevăzută de art. 42 alin. (1), (2) și (3) din Legea nr. 161/2003.

3. Folosirea la bancomat a unui card bancar falsificat, pentru retrageri de numerar, constituie infracțiunea de efectuare de operațiuni financiare în mod fraudulos prin utilizarea unui instrument de plată electronică, inclusiv a datelor de identificare care permit utilizarea acestuia, prevăzută de art. 27 alin. (1) din Legea nr. 365/2002, în concurs ideal cu infracțiunea de acces, fără drept, la un sistem informatic comisă în scopul obținerii de date informatice prin încălcarea măsurilor de securitate, prevăzută de art. 42 alin. (1), (2) și (3) din Legea nr. 161/2003, și cu infracțiunea de falsificare a instrumentelor de plată electronică, prevăzută de art. 24 alin. (2) din Legea nr. 365/2002.

Obligatorie, potrivit art. 414⁵ alin. 4 din Codul de procedură penală.

Pronunțată, în ședință publică, astăzi, 14 octombrie 2013.

PREȘEDINTELE ÎNALTEI CURȚI DE CASAȚIE ȘI JUSTIȚIE

LIVIA DOINA STANCIU

Magistrat-asistent
Monica Eugenia Ungureanu

EDITOR: GUVERNUL ROMÂNIEI



„Monitorul Oficial” R.A., Str. Parcului nr. 65, sectorul 1, București; C.I.F. RO427282,
IBAN: RO55RNCB0082006711100001 Banca Comercială Română — S.A. — Sucursala „Unirea” București
și IBAN: RO12TREZ70050699XXX000531 Direcția de Trezorerie și Contabilitate Publică a Municipiului București
(alocat numai persoanelor juridice bugetare)

Tel. 021.318.51.29/150, fax 021.318.51.15, e-mail: marketing@ramo.ro, internet: www.monitoruloficial.ro

Adresa pentru publicitate: Centrul pentru relații cu publicul, București, șos. Panduri nr. 1,
bloc P33, parter, sectorul 5, tel. 021.401.00.70, fax 021.401.00.71 și 021.401.00.72

Tiparul: „Monitorul Oficial” R.A.

