DECIZIE nr. 15 din 14 octombrie 2013 referitoare la recursul în interesul legii formulat de către procurorul general al Parchetului de pe lângă Înalta Curte de Casaţie şi Justiţie prin Sesizarea nr. 11.874/2670/III-5/2011, pentru a se stabili, în vederea interpretării şi aplicării unitare a dispoziţiilor art. 42 alin. (1), (2) şi (3) din Legea nr. 161/2003, respectiv pentru interpretarea unitară a noţiunii de acces fără drept la un sistem informatic

ÎNALTA CURTE DE CASAŢIE ŞI JUSTIŢIE

COMPLETUL COMPETENT SĂ JUDECE RECURSUL ÎN INTERESUL LEGII

Dosar nr. 12/2013

Livia Doina Stanciu	- preşedintele Înaltei Curţi de Casaţie şi Justiţie, preşedintele completului
Lavinia Curelea	- preşedintele Secţiei I civile
Roxana Popa	- preşedintele delegat al Secţiei a II-a civile
Ionel Barbă	- preşedintele Secţiei de contencios administrativ şi fiscal
Corina Michaela Jîjîie	- preşedintele Secţiei penale
Simona Cristina Neniţă	- judecător Secţia penală
Ioana Bogdan	- judecător Secţia penală
Ionuţ Mihai Matei	- judecător Secţia penală
Leontina Şerban	- judecător Secţia penală
Ştefan Pistol	- judecător Secţia penală
Mirela Sorina Popescu	- judecător Secţia penală
Florentina Dragomir	- judecător Secţia penală
Sofica Dumitraşcu	- judecător Secţia penală
Mariana Ghena	- judecător Secţia penală
Săndel Lucian Macavei	- judecător Secţia penală
Alina Ioana Ilie	- judecător Secţia penală
Lavinia Valeria Lefterache	- judecător Secţia penală, judecător raportor
Maricela Cobzariu	- judecător Secţia penală
Ana Maria Dascălu	- judecător Secţia penală
Dragu Creţu	- judecător Secţia I civilă
Alina Iuliana Ţuca	- judecător Secţia I civilă
Mariana Cîrstocea	- judecător Secţia a II-a civilă
Mirela Poliţeanu	- judecător Secţia a II-a civilă
Carmen Sîrbu	- judecător Secţia de contencios administrativ şi fiscal
Carmen Maria Ilie	- judecător Secţia de contencios administrativ şi fiscal

Completul competent să judece recursul în interesul legii ce formează obiectul Dosarului nr. 12/2013 este constituit conform dispoziţiilor art. 414^4 alin. 3 din Codul de procedură penală, modificat şi completat prin Legea nr. 202/2010, raportat la dispoziţiile art. 27^2 din Regulamentul privind organizarea şi funcţionarea administrativă a Înaltei Curţi de Casaţie şi Justiţie, republicat, cu modificările şi completările ulterioare.

Şedinţa completului este prezidată de doamna Livia Doina Stanciu, preşedintele Înaltei Curţi de Casaţie şi Justiţie.

La şedinţa de judecată participă procurorul general al Parchetului de pe lângă Înalta Curte de Casaţie şi Justiţie, domnul procuror Tiberiu Niţu.

La şedinţa de judecată participă magistratul-asistent din cadrul Secţiilor Unite, doamna Monica Eugenia Ungureanu, desemnat în conformitate cu dispoziţiile art. 27^3 din Regulamentul privind organizarea şi funcţionarea administrativă a Înaltei Curţi de Casaţie şi Justiţie, republicat, cu modificările şi completările ulterioare.

Înalta Curte de Casaţie şi Justiţie - 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 Casaţie şi Justiţie prin Sesizarea nr. 11.874/2670/III-5/2011, pentru a se stabili, în vederea interpretării şi aplicării unitare a dispoziţiilor art. 42 alin. (1), (2) şi (3) din Legea nr. 161/2003, respectiv pentru interpretarea unitară a noţiunii de acces fără drept la un sistem informatic, determinat de diferenţierea practică între:

- accesul prin intermediul montării la ATM a dispozitivelor de citire a benzii magnetice a cardului autentic şi 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 Casaţie şi Justiţie a susţinut recursul în interesul legii învederând că examenul jurisprudenţei penale actuale a evidenţiat mai multe orientări cu privire la acest aspecte şi, prin urmare, caracterul neunitar al practicii judiciare:

I. Într-o primă orientare a practicii, unele instanţe 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, infracţiune prevăzută de art. 42 alin. (1) din Legea nr. 161/2003 (anexele nr. 1, 3, 43-45, 55).

Instanţele au încadrat această faptă în dispoziţiile art. 25 din Legea nr. 365/2002, reţinându-se că inculpaţii "au deţinut echipamente electronice apte să citească şi să memoreze date din cărţile de credit, în scopul obţinerii acelor date care permit retragerea sumelor de bani din cărţile de credit" (anexa nr. 44).

Alte instanţe au apreciat că "fapta inculpatului de a ataşa la un ATM un dispozitiv format dintr-un telefon mobil prevăzut cu cameră video şi card de memorie şi un suport menit a susţine şi disimula telefonul în plafonul bancomatului, în scopul de a înregistra codul PIN tastat de utilizatorii acestuia, întruneşte elementele constitutive ale infracţiunii prevăzute de art. 46 alin. (2) din Legea nr. 161/2003, adică deţinere fără drept a unui dispozitiv conceput sau adaptat în scopul săvârşirii uneia dintre infracţiunile prevăzute de art. 42-45 din aceeaşi lege" (anexa nr. 55).

Cele mai multe instanţe însă au menţinut încadrarea juridică din actul de sesizare, fără a pune în discuţie şi fără a se pronunţa în mod expres asupra problemei de drept supusă prezentului recurs. Înalta Curte de Casaţie şi Justiţie a împărtăşit această primă orientare prin deciziile nr. 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) şi nr. 3.354 din 3 octombrie 2011 (anexa nr. 45).

Într-o a doua orientare a practicii s-a reţinut, dimpotrivă, că prin montarea la bancomat a dispozitivelor de citire a informaţiilor înregistrate pe banda magnetică a cardului şi de captare a codului PIN tastat cu ocazia folosirii cardului de către titularul său se realizează un acces fără drept la sistemul informatic, prin încălcarea măsurilor de securitate (anexele nr. 39-41, 46-47).

În argumentarea acestei opinii, instanţele au apreciat că "ATM-ul este un mijloc de colectare, prelucrare şi transmitere

a unor date informatice, reprezentate de numărul de cont al titularului, care este stocat pe nivelul 2 al benzii magnetice. Pe de altă parte, prin montarea skimmerului în fanta bancomatului, prin care se introduce cardul şi se realizează citirea benzii magnetice a fiecărui card în parte, stocându-se informaţia astfel obţinută, au fost încălcate măsurile de securitate care aveau drept scop asigurarea secretului numărului de cont şi a operaţiunilor efectuate şi apărarea împotriva folosirii de către o altă persoană a acestor carduri în vederea fraudării. În consecinţă, inculpaţii au accesat fără drept un sistem informatic încălcând astfel măsurile de securitate." (anexa nr. 46).

Cu aceeaşi motivare, unele instanţe au reţinut ca incidente, pentru această situaţie de fapt, dispoziţiile art. 44 alin. (2), (3) şi art. 46 alin. (2) alături de cele ale art. 42 alin. (2), (3) din Legea nr. 161/2003 (anexa nr. 41).

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

Înalta Curte de Casaţie şi Justiţie a împărtăşit această orientare prin deciziile nr. 376 din 2 februarie 2010 (anexa nr. 39), nr. 5.288 din 15 septembrie 2006 (anexa nr. 46) şi nr. 2.094 din 27 mai 2010 (anexa nr. 47).

La acelaşi punct de vedere au aderat şi instanţele, inclusiv Înalta Curte de Casaţie şi Justiţie prin Decizia nr. 2.991 din 1 martie 2010, care, deşi nu au reţinut aplicarea art. 42 alin. (1) din Legea nr. 161/2003, au considerat că acesta ar fi fost aplicabil "în situaţia în care ar fi fost montate dispozitive de citire a benzilor magnetice la ATM" (anexa nr. 16).

II. Cât priveşte 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 obţinut datele informatice cu care a fost acesta inscripţionat, unele instanţe au concluzionat în sensul că fapta întruneşte elementele constitutive ale infracţiunii prevăzute de art. 42 alin. (1) şi (3) din Legea nr. 161/2003 (anexele nr. 42, 45, 47-53).

Acest punct de vedere a fost argumentat pe dispoziţiile art. 35 din Legea nr. 161/2003, ale cărui condiţii sunt îndeplinite de bancomat, privit nu doar din punct de vedere fizic, ci şi ca sistem informatic interconectat la reţeaua 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 inscripţionarea datelor aflate pe cardul autentic este "recunoscut" de bancomatul la care este folosit.

Instanţele care au aderat la această opinie au încadrat fapta de folosire a cardului falsificat pentru retragere de numerar de la ATM-uri în dispoziţiile art. 42 alin. (1) şi (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 aceeaşi lege (anexele nr. 45, 47-53).

Înalta Curte de Casaţie şi Justiţie a împărtăşit 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) şi nr. 3.408 din 5 octombrie 2011 (anexa nr. 53).

Dimpotrivă, alte instanţe au apreciat că folosirea cardului falsificat pentru retragerea de numerar de la ATM nu constituie acces fără drept şi prin încălcarea măsurilor de securitate la un sistem informatic (anexele nr. 2-30, 54).

Instanţele care au împărtăşit această opinie au încadrat faptele inculpaţilor, în sarcina cărora au reţinut inscripţionarea mai multor carduri blanc cu date informatice preluate de pe cardurile autentice şi retragerea a diferite sume de bani din bancomate, în dispoziţiile art. 24 alin. (1) şi (2), art. 25 şi art. 27 alin. (1) din Legea nr. 365/2002.

Înalta Curte de Casaţie şi Justiţie a împărtăşit 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) şi nr. 1.681 din 14 mai 2008 (anexa nr. 29).

În ipoteza folosirii cardului autentic, fără consimţământul titularului său, pentru retragerea de numerar de la ATM fapta a fost încadrată, exclusiv, în dispoziţiile 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 Casaţie şi Justiţie, în sensul orientării jurisprudenţiale 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 priveşte folosirea la bancomat, pentru retrageri de numerar sau orice alte operaţiuni financiare, a unui card falsificat sau a unuia real, fără consimţământul titularului său, fapta întruneşte elementele constitutive ale infracţiunii prevăzute de art. 42 alin. (1), (2) şi (3) din Legea nr. 161/2003, săvârşită în concurs ideal cu cea prevăzută la art. 24 alin. (2) din Legea nr. 365/2002 sau art. 27 alin. (1) din aceeaşi lege, după caz.

Preşedintele Înaltei Curţi de Casaţie şi Justiţie, doamna judecător Livia Doina Stanciu, a declarat dezbaterile închise, iar completul de judecată a rămas în pronunţare asupra recursului în interesul legii.

ÎNALTA CURTE,

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

- montarea la ATM a dispozitivelor de citire a benzii magnetice a cardului autentic şi 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 Casaţie şi Justiţie sa arătat că în practica judiciară naţională nu există un punct de vedere unitar cu privire la înţelesul noţiunii de acces fără drept la un sistem informatic şi, în consecinţă, au fost formulate soluţii divergente cu privire la încadrarea juridică dată faptelor atunci când se montează la ATM dispozitivele de citire a benzii magnetice a cardului autentic şi a codului PIN aferent acestuia, precum şi atunci când se foloseşte la bancomat cardul falsificat ori cel autentic, fără acordul titularului său.

2. Examenul jurisprudenţial

Prin recursul în interesul legii se arată că în urma verificării jurisprudenţei la nivel naţional a fost relevată o practică neunitară în interpretarea şi aplicarea art. 42 alin. (1), (2) şi (3) din Legea nr. 161/2003 cu privire la înţelesul noţiunii de acces fără drept la un sistem informatic. Procurorul general a menţionat în sesizarea scrisă faptul că cele mai multe instanţe au menţinut încadrarea juridică din actul de sesizare, fără a pune în discuţie şi fără a se pronunţa în mod

expres asupra problemei de drept supuse prezentului recurs în interesul legii.
2.1. Soluţiile pronunţate de instanţele judecătoreşti cu privire la montarea la ATM a dispozitivelor de citire a benzii magnetice a cardului autentic şi a codului PIN aferent acestuia
2.1.1. Jurisprudenţă în sensul lipsei accesului la un sistem informatic şi incidenţei art. 25 din Legea nr. 365/2002. Opinia trimisă de procurorul general arată că, într-o primă orientare a practicii, unele instanţe 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, infracţiune prevăzută de art. 42 alin. (1) din Legea nr. 161/2003 (anexele nr. 1, 3, 43-45, 55).
Instanţele au încadrat fapta în art. 25 din Legea nr. 365/2002, reţinându-se că inculpaţii "au deţinut echipamente electronice apte să citească şi să memoreze date din cărţile de credit, în scopul obţinerii acelor date care permit retragerea sumelor de bani din cărţile de credit" (anexa nr. 44).
2.1.2. Jurisprudenţă în sensul deţinerii fără drept a unui dispozitiv conceput sau adaptat în scopul săvârşirii uneia dintre infracţiunile 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 ataşa la un ATM un dispozitiv format dintr-un telefon mobil prevăzut cu cameră video şi card de memorie cu un suport menit a susţine şi disimula telefonul în plafonul bancomatului, în scopul de a înregistra codul PIN tastat de utilizatorii acestuia, întruneşte elementele constitutive ale infracţiunii prevăzute de art. 46 alin. (2) din Legea nr. 161/2003, reprezentând deţinerea fără drept a unui dispozitiv conceput sau adaptat în scopul săvârşirii uneia dintre infracţiunile prevăzute de art. 42-45 din aceeaşi lege" (anexa nr. 55).
În opinia transmisă de către procurorul general se arată că cele mai multe instanţe au menţinut încadrarea juridică din actul de sesizare fără a pune în discuţie şi fără a se pronunţa în mod expres asupra problemei de drept supuse prezentului recurs.
2.1.3. Jurisprudenţă în sensul existenţei accesului la un sistem informatic. Într-o a treia orientare a practicii, s-a reţinut că prin montarea la bancomat a dispozitivelor de citire a informaţiilor înregistrate pe banda magnetică a cardului şi de captare a codului PIN tastat cu ocazia folosirii cardului de către titularul său se realizează un acces fără drept la sistemul informatic, prin încălcarea măsurilor de securitate (anexele nr. 39-41, 46-47).
În argumentarea acestei opinii, instanţele au apreciat că "ATM-ul este un mijloc de colectare, prelucrare şi transmitere a unor date informatice, reprezentate de numărul de cont al titularului, care este stocat pe nivelul doi al benzii magnetice. Pe de altă parte, prin montarea skimmerului în fanta bancomatului, prin care se introduce cardul şi se realizează citirea benzii magnetice a fiecărui card în parte, stocându-se informaţia astfel obţinută, au fost încălcate măsurile de securitate care aveau drept scop asigurarea secretului numărului de cont şi a operaţiunilor efectuate şi apărarea împotriva folosirii de către o altă persoană a acestor carduri în vederea fraudării. În consecinţă, inculpaţii au accesat fără drept un sistem informatic, încălcând astfel măsurile de securitate", astfel că sunt întrunite elementele constitutive ale infracţiunii prevăzute de art. 42 alin. (1) şi (3) din Legea nr. 161/2003 (anexa nr. 46).
2.1.4. Cu aceeaşi motivare, alte instanţe au reţinut ca incidente, pentru această situaţie de fapt, dispoziţiile art. 44 alin. (2), (3) şi art. 46 alin. (2), alături de cele ale art. 42 alin. (2) şi (3) din Legea nr. 161/2003 (anexele nr. 39, 41, 46, 47).
În argumentarea acestei opinii, instanţele au apreciat că atât videocamera, cât şi skimmerul au fost deţinute în scopul menţionat de art. 46 alin. (2) din Legea nr. 161/2003.
La acelaşi punct de vedere au aderat şi instanţele, care, deşi nu au reţinut aplicarea art. 42 alin. (1) din Legea nr. 161/2003, au considerat că acesta ar fi fost aplicabil "în situaţia în care ar fi fost montate dispozitive de citire a benzilor magnetice la ATM" (anexa nr. 16).
2.2. Soluţiile pronunţate de instanţele judecătoreşti cu privire la folosirea la bancomat a cardului falsificat ori chiar a celui autentic, fără acordul titularului său
2.2.1. Jurisprudenţă în sensul reţinerii accesului la un sistem informatic. Într-o primă orientare jurisprudenţială unele instanţe au ajuns la concluzia că fapta întruneşte elementele constitutive ale infracţiunii prevăzute de art. 42 alin. (1) şi (3) din Legea nr. 161/2003 (anexele nr. 42, 45, 47-53).
Acest punct de vedere a fost argumentat pe dispoziţiile art. 35 din Legea nr. 161/2003. Bancomatul este un sistem informatic interconectat la reţeaua 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 inscripţionarea datelor aflate pe cardul autentic este recunoscut de bancomatul la care este folosit.
Instanţele 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) şi (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) şi art. 27 alin. (1) din Legea nr. 365/2002 (anexele nr. 45, 47-53).
2.2.2. Jurisprudenţă în sensul lipsei accesului la un sistem informatic. Dimpotrivă, alte instanţe au apreciat că folosirea cardului falsificat pentru retragerea de numerar de la ATM nu constituie acces fără drept şi prin încălcarea măsurilor de securitate la un sistem informatic (anexele nr. 2-30, 54).
Instanţele care au împărtăşit această opinie au încadrat faptele inculpaţilor, în sarcina cărora au reţinut inscripţionarea mai multor carduri blanc cu date informatice preluate de pe cardurile autentice şi retragerea a diferite sume de bani din bancomate, în art. 24 alin. (1) şi (2), art. 25 şi 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. Jurisprudenţă în sensul reţinerii art. 27 alin. (1) din Legea nr. 365/2002. În ipoteza folosirii cardului autentic, fără consimţământul titularului său, pentru retragerea de numerar de la ATM fapta a fost încadrată, exclusiv, în dispoziţiile art. 27 alin. (1) din Legea nr. 365/2002 (anexele nr. 31-38).
3. Opinia procurorului general
3.1. Soluţia problemei de drept
Soluţia propusă de către procurorul general al Parchetului de pe lângă Înalta Curte de Casaţie şi Justiţie 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 operaţiuni financiare un card falsificat sau un card real, fără consimţământul titularului său, este aceea prevăzută de art. 42 alin. (1), (2) şi (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 operaţiuni financiare în mod fraudulos).

3.2. Înţelesul unor termeni

În opinia transmisă de către procurorul general sunt definite noţiunile de acces la un sistem informatic, skimming şi 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 importanţă. Accesul fără drept la un sistem informatic presupune o interacţiune 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 aplicaţii în beneficiul intrusului.

Cardul emis de o instituţie de credit reprezintă un instrument de plată electronică, respectiv un suport de informaţie standardizat, securizat şi individualizat, care permite deţinătorului său să folosească disponibilităţile băneşti proprii dintr-un cont deschis pe numele lui la emitentul cardului şi/sau să utilizeze o linie de credit (în limita unui plafon stabilit în prealabil) deschisă de emitent în favoarea deţinătorului cardului, în vederea efectuării uneia sau a mai multora dintre următoarele operaţiuni: retragerea sau depunerea de numerar de la terminale precum ATM-uri, ghişeele emitentului sau ale unei alte instituţii obligate prin contract să accepte instrumentul de plată electronică; plata bunurilor achiziţionate ori a serviciilor prestate de comercianţii acceptanţi sau de emitenţi, precum şi plata obligaţiilor către autorităţile administraţiei 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 conţine date codificate stocate electronic referitoare la card (titularul cardului, numărul de cont, data expirării etc.) poziţionate 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 informaţii despre cont, informaţia fiind apoi procesată împreună cu codul confidenţial al emitentului pentru a verifica dacă valoarea transmisă se potriveşte cu cea din înregistrare; codul CVV2 (pentru cardul VISA) şi codul CVC2 (pentru cardul MASTERCARD) reprezintă un număr format din trei cifre imprimate pe zona pentru semnătură şi înclinate spre stânga. Pe aceeaşi zonă este imprimat tot înclinat invers şi numărul de cont duplicat, care asigură corespondenţa cu numărul de cont care apare pe faţa 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 cunoştinţa posesorului legitim, cu intenţia de a fi folosite în scopuri frauduloase. Dispozitivele de skimming pot fi "de mână" - hand skimmers, ipoteză în care datele de pe banda magnetică sunt copiate în momentul când cardul este înmânat de către titular unei alte persoane (de regulă, un comerciant în timpul efectuării unei tranzacţii) 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 tranzacţie. În acest din urmă caz skimmerul este poziţionat pe latura externă a fantei de introducere a cardului şi poate avea forma fantei pentru card, fiind lipit chiar deasupra acesteia, astfel încât datele de pe banda magnetică sunt citite şi captate înainte ca respectivul card să intre în fanta bancomatului şi să se realizeze transmisia de date informatice între card şi ATM.

Dispozitivele de skimming sunt însoţite de mini-videocamere şi/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 şi a codului PIN aferent acestuia (mini-videocamere sau dispozitive tip tastatură), procurorul general apreciază că sunt întrunite elementele constitutive ale infracţiunii prevăzute de art. 46 alin. (2) din Legea nr. 161/2003.

În opinia înaintată Înaltei Curţi se arată că au aplicat corect legea instanţele care au apreciat că prin montarea la ATM a dispozitivului de citire a benzii magnetice a cardului şi a videocamerei ori a dispozitivului modificat de tip tastatură nu se realizează accesul fără drept la un sistem informatic, infracţiune 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) şi în două variante agravate, în alin. (2) şi (3): accesul fără drept la un sistem informatic, săvârşit în scopul obţinerii 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: staţie de lucru, server ori reţea informatică.

Accesul fără drept la un sistem informatic presupune o interacţiune 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 aplicaţii în beneficiul intrusului. Urmarea imediată constă într-o stare de pericol cu privire la siguranţa sistemului informatic şi/sau a resurselor sale. Dacă scopul accesului neautorizat a fost obţinerea de date informatice, starea de pericol este dublată de atingerea adusă protecţiei datelor informatice stocate sau prelucrate de acesta. Încălcarea măsurilor de securitate determină o transformare efectivă adusă obiectului material al infracţiunii, şi anume entităţilor materiale care compun sistemele informatice (calculatoare, reţele de calculatoare, elemente hardware - echipamente periferice, cabluri, plăci, servere etc. şi software - programe, aplicaţii, baze de date etc.) sau datelor informatice vizate. Sub aspectul consecinţelor pe care acţiunea incriminată le are asupra valorii sociale ocrotite, urmarea este tocmai starea de pericol, de ameninţare, la adresa "domiciliului informatic". Legătura de cauzalitate între activitatea făptuitorului şi urmarea produsă rezultă ex re, în cazul accesului neautorizat în formă simplă, respectiv trebuie demonstrată forţarea măsurilor de securitate (parole, coduri de acces etc.), în cazul formelor agravate.

Obţinerea datelor de pe banda magnetică a cadrului autentic se realizează în exteriorul bancomatului şi fără ca dispozitivele menţionate să intre în vreun fel de conexiune cu sistemul informatic al băncii. În egală măsură, captarea codului PIN se realizează în exteriorul ATM-ului şi nu presupune acces la sistemul informatic.

- Articolul 42 din Legea nr. 161/2003 incriminează accesul fără drept la un sistem informatic. Bancomatul, folosit conform destinaţiei sale, este un terminal în cadrul unui sistem informatic din care mai fac parte toate celelalte terminale din reţeaua aceleiaşi bănci, serverul acesteia etc. Bancomatul este folosit conform destinaţiei sale atunci când, prin intermediul său, se fac retragerea de numerar, plata furnizorilor de utilităţi, transferurile de fonduri, interogarea de sold. În toate aceste situaţii bancomatul condiţionează 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 şi nu îşi îndeplineşte rolul de parte a unui sistem informatic.

Citirea benzii magnetice a cardului autentic nu este condiţionată de ataşarea skimmerului la bancomat. Citirea benzii magnetice se face şi printr-un dispozitiv de citire manual, lipsit de orice fel de conexiune cu sistemul bancar. Devine astfel evident că operaţiunile prin care sunt citite datele de pe banda magnetică a cardului, concomitent cu captarea codului PIN aferent lui, reprezintă doar acte pregătitoare ale infracţiunii de acces fără drept la un sistem informatic: cum citirea datelor de pe banda magnetică a cardului nu este condiţionată de ataşarea dispozitivului electronic de citire la bancomat, aceeaşi activitate de captare a datelor de pe banda magnetică ar primi consecinţe juridice diferite din cauza unei împrejurări extranee vreunei norme de incriminare - ataşarea sau neataşarea skimmerului la bancomat.

Aşadar, operaţiunea de citire a datelor de pe banda magnetică a cardului, prin ataşarea skimmerului la bancomat, nu interacţionează 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 aplicaţii în beneficiul făptuitorului, astfel că infracţiunea de acces fără drept la sistemul informatic este lipsită de însuşi elementul său material.

3.4. Cu privire la folosirea la bancomat, pentru retrageri de numerar sau orice alte operaţiuni financiare, a cardului falsificat ori chiar a celui autentic fără acordul titularului său, procurorul general apreciază că sunt întrunite elementele constitutive ale infracţiunii prevăzute de art. 42 alin. (1), (2) şi (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 inscripţionat cu datele culese de pe cardul autentic, oricare ar fi fost modul de obţinere a acestora, ori utilizarea cardului autentic fără acordul titularului său reprezintă acces fără drept la un sistem informatic, în scopul obţinerii de date informatice, prin încălcarea măsurilor de securitate, faptă incriminată de art. 42 alin. (1), (2) şi (3) din Legea nr. 161/2003. Folosit conform destinaţiei sale, bancomatul face parte din sistemul informatic bancar, datele transmise şi receptate de acest dispozitiv fiind protejate prin măsuri de securitate încorporate în sistemul de citire a cardurilor şi în codul PIN. În cazul folosirii la ATM a cardului falsificat sau a celui real fără consimţământul titularului său se realizează un acces fără drept la sistemul informatic. De această dată bancomatul este folosit conform destinaţiei sale: introducerea cardului şi tastarea codului PIN (prin această din urmă operaţiune înlăturându-se măsura de securitate reprezentată de codul de acces), în posesia cărora făptuitorul se află în mod nelegal, determinând "recunoaşterea" de către bancomat a cardului falsificat ca fiind un card valid şi permiţând astfel un schimb de informaţii între posesorul cardului şi mediul de stocare a datelor privitoare la contul bancar, ataşat cardului "recunoscut". Chiar dacă activitatea infracţională s-ar opri aici, nefiind solicitată nicio operaţiune financiară, infracţiunea de acces fără drept la un sistem informatic este consumată.

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 ameninţată. Legătura de cauzalitate dintre acţiunea făptuitorului şi urmarea produsă datelor informatice rezultă din însăşi materialitatea faptei. Cât priveşte latura subiectivă, fapta este săvârşită cu intenţie.

Potrivit art. 44 alin. (2), (3) din Legea nr. 161/2003, constituie infracţiune transferul neautorizat de date dintr-un sistem informatic, respectiv dintr-un mijloc de stocare a datelor informatice, iar prin art. 46 alin. (2) din acelaşi act normativ este incriminată fapta de deţinere, fără drept, a unui dispozitiv, program informatic, parolă, cod de acces sau dată informatică, dintre cele care permit accesul total sau parţial la un sistem informatic, în scopul săvârşirii uneia dintre infracţiunile prevăzute la art. 42-45. Skimmerul, videocamera şi falsa tastatură de bancomat sunt dispozitive deţinute în scopul săvârşirii unui acces fără drept la sistemul informatic, iar datele informatice şi codul de acces obţinute prin folosirea acestor dispozitive permit accesul total sau parţial la un sistem informatic, putând fi utilizate fie pentru inscripţionarea ulterioară a unor carduri clonate, fie pentru plata unor tranzacţii on-line. Textele legale menţionate devin în egală măsură incidente şi în cazul folosirii unui skimmer ataşat la bancomat, dar şi în cazul obţinerii datelor de pe banda magnetică a cardului cu ajutorul unui hand-skimmer.

Legea nr. 161/2003 sancţionează infracţiuni îndreptate contra confidenţialităţii şi integrităţii datelor şi sistemelor informatice, în timp ce Legea nr. 365/2002 privind comerţul electronic prevede infracţiuni îndreptate împotriva securităţii şi integrităţii instrumentelor de plată electronice. Spre deosebire de primele infracţiuni, 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 circulaţie sau deţinerea în vederea punerii în circulaţie a unui astfel de instrument falsificat. Art. 27 alin. (1) din aceeaşi lege sancţionează efectuarea de operaţiuni financiare prin utilizarea unui instrument de plată, fără consimţământul titularului său.

Pe de altă parte, art. 25 din Legea nr. 365/2002 (reţinut greşit de unele instanţe în cazul montării la ATM a dispozitivelor de citire a benzii magnetice a cardului autentic şi a codului PIN) incriminează fabricarea ori deţinerea 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 inscripţionează cardurile (de tipul MSR-lui, de pildă) cu datele culese prin skimmer.

Scopul acestei infracţiuni este producerea unui alt card, cu existenţă fizică de sine stătătoare, identic cu cel autentic, care să poată fi folosit întocmai ca acesta. Scopul skimmingului este obţinerea de date informatice, desigur lipsite de existenţă materială, care pot fi ulterior folosite pentru inscripţionarea unor carduri clonate, dar şi pentru plata on-line. În această din urmă situaţie nu există un card falsificat în materialitatea lui, ci datele informatice obţinute în modalitatea anterior enunţată 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 şi a codului PIN aferent acestuia, art. 46 alin. (2) din Legea nr. 161/2003, şi nu art. 25 din Legea nr. 365/2002. Cât priveşte infracţiunea prevăzută de art. 44 alin. (2), (3) din Legea nr. 161/2003, reţinută de unele instanţe în concurs cu cele prevăzute de art. 46 alin. (2) şi art. 42 alin. (2) şi (3) din aceeaşi 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 săvârşirii infracţiunilor din Legea nr. 365/2002 privind comerţul electronic, se pot săvârşi infracţiuni îndreptate împotriva securităţii datelor sau sistemelor informatice, cum este şi aceea de acces ilegal într-un sistem informatic. Aşadar, accesul ilegal în sistemul informatic se face, de regulă, în scopul săvârşirii uneia sau mai multora dintre infracţiunile prevăzute de Legea nr.

365/2002 privind comerţul electronic, situaţie care justifică reţinerea unui concurs cu conexitate etiologică în care accesul ilegal reprezintă mijlocul prin care se realizează scopul şi anume efectuarea de operaţiuni financiare în mod fraudulos.

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

Au fost solicitate şi transmise puncte de vedere cu privire la aspectele tehnice referitoare la situaţia de fapt, precum şi, după caz, cu privire la încadrarea juridică dată faptelor care au suscitat o practică neunitară de la Institutul pentru Tehnologii Avansate, Institutul de Cercetări Juridice din cadrul Academiei Române, Departamentul de drept penal din cadrul Facultăţii de Drept a Universităţii Bucureşti, Departamentul de drept public din cadrul Facultăţii de Drept a Universităţii "Babeş-Bolyai", Catedra de drept penal din cadrul Facultăţii de Drept şi Ştiinţe Administrative a Universităţii din Craiova, Facultatea de Drept a Universităţii "Lucian Blaga" din Sibiu, Departamentul de drept public din cadrul Facultăţii de Drept a Universităţii de Vest din Timişoara.

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

4.1.1. Înţelesul unor termeni cu privire la montarea la ATM a dispozitivelor de citire a benzii magnetice a cardului autentic şi 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 şi memorării/transmiterii la distanţă 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 şi culoare cu echipamentul original cu interfaţă 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 înmânat cardul de către titular, în vederea unei tranzacţii (de exemplu, de către recepţioner, ospătar etc.); un dispozitiv de achiziţie 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 siguranţă şi care înregistrează aceste momente sau un ansamblu format dintr-o tastatură falsă, care se montează deasupra tastaturii originale, şi un montaj electronic care preia şi memorează codul tastat de utilizator.

Montajul electronic din interiorul dispozitivelor tip skimmer are o arhitectură alcătuită din: bloc de achiziţie 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 interfaţă 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 îşi păstrează conţinutul informaţional şi după întreruperea alimentării; bloc de comunicaţie, care realizează legătura şi conversia datelor între interfaţa serială tip UART a microcontrolerului şi interfaţa serială tip RS232 sau tip USB, specifice porturilor seriale ale unui sistem de calcul tip PC (uneori acest bloc este format doar dintro interfaţă hardware tip conector liniar artizanal, la care se leagă un cablu adaptor în care se află circuitul integrat cu funcţia 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 şi, totodată, implementează o funcţie proprie de descărcare a datelor în calculator, care decodifică datele transferate. Astfel, datele din memoria skimmer-ului pot fi accesate doar prin cunoaşterea algoritmului de criptare din microcontroler şi a aplicaţiei ce rulează pe PC.

Cardurile bancare conţin o bandă magnetică structurată, din punct de vedere al organizării datelor, pe 3 piste. Caracteristicile fizice ale cardurilor, dimensiunile, poziţia pistelor şi modul de înscriere a datelor sunt stabilite în mod unic de standardele ISO 7810, 7811, 7813, precizând densităţile de înregistrare, codarea caracterului şi un conţinut informaţional. 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 operaţiuni financiare.

În fapt, prin montarea dispozitivelor tip skimmer peste fanta de introducere a cardului la un echipament cu interfaţă 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 ştergerea respectivelor date din mijlocul de stocare.

Dispozitivele electronice dotate cu cameră video şi utilizate pentru achiziţia 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 carcasele, pentru reducerea dimensiunilor, iar acumulatorii originali sunt înlocuiţi cu ansambluri de acumulatori cu durata de funcţionare mărită.

Poziţionarea camerelor video permite vizualizarea, prin intermediul obiectivelor optice, a tastaturii echipamentelor cu interfaţă 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 distanţă imaginile vizate sunt dotate cu emiţătoare radio. Toate dispozitivele comerciale sunt dotate cu interfaţă 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 rezoluţia obiectivelor optice permite extragerea informaţiei referitoare la codul PIN.

În cazul montării unei tastaturi false deasupra tastaturii originale a unui echipament dotat cu interfaţă de card bancar, se urmăreşte preluarea şi memorarea codului PIN tastat de utilizator. Dispozitivul artizanal conţine 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 comunicaţie, pentru interfaţarea montajului cu un sistem de calcul în vederea descărcării informaţiilor; un bloc de alimentare.

Atât dispozitivul dotat cu cameră video, cât şi dispozitivul ce încorporează o tastatură falsă permit interceptarea, fără

drept, a transmisiei de date informatice care nu este publică şi este destinată sistemului informatic al băncii, şi anume codul PIN, un cod de securitate introdus de bancă pentru restricţionarea accesului utilizatorilor neautorizaţi la sistemul informatic al băncii.

Există numeroase variante de scheme electrice pentru dispozitivele electronice de fraudare a echipamentelor dotate cu interfaţă 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 funcţie internă a microcontrolerului) şi 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 şi momentele de timp la care utilizatorii tastează codul PIN asigură asocierea între informaţiile confidenţiale corespunzătoare unui card: date informatice înscrise pe banda magnetică şi date referitoare la codul de siguranţă.

În prezent, se constată tendinţa de exploatare la distanţă atât a dispozitivelor frauduloase pentru interceptarea datelor memorate pe banda magnetică, cât şi a celor pentru codul PIN. În cazul exploatării la distanţă, blocurile de memorare şi comunicaţie din schema electrică sunt înlocuite cu un emiţător în infraroşu sau radio, care transmite în timp real datele interceptate către un receptor infraroşu/radio, aflat în proximitate şi care include o componentă hardware de memorare a datelor. Pentru canalul de comunicaţie radio pot fi folosite emiţătoare artizanale sau comerciale tip bluetooth.

Oricare ar fi modul de realizare a fraudării echipamentelor dotate cu interfaţă de card bancar, dispozitivele descrise sunt concepute sau adaptate în scopul săvârşirii infracţiunii de acces, fără drept, la un sistem informatic, prin intermediul unor instrumente de plată electronică falsificate sau prin utilizarea, în acelaşi scop, a informaţiilor obţinute prin intermediul acestor dispozitive.

4.1.2. Înţelesul 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:

- obţinerea, 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 consimţământul titularului său, la un echipament dotat cu interfaţă de card bancar, realizează accesul, fără drept, la sistemul informatic al băncii, în scopul obţinerii de date informatice şi cu încălcarea măsurilor de securitate introduse de bancă, indiferent de tipul operaţiunii efectuate: interogare, autentificare, retrageri de numerar, transferuri sau orice alte operaţiuni financiare. În cazul folosirii datelor de identificare ale cardurilor bancare pentru efectuarea unor tranzacţii on-line, se accesează, fără drept, sistemul informatic al băncii, cu încălcarea măsurilor de securitate introduse de bancă.

4.1.3. Soluţia tehnică

Montarea la un echipament dotat cu interfaţă 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 obţinerea de date informatice şi 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 şi este destinată sistemului informatic al băncii, şi anume codul PIN, un cod de securitate introdus de bancă pentru restricţionarea accesului utilizatorilor neautorizaţi la sistemul informatic al băncii.

Folosirea la un echipament dotat cu interfaţă de card bancar, a unui card bancar falsificat sau a unuia autentic, fără consimţământul titularului său, precum şi folosirea datelor de identificare ale cardurilor bancare pentru efectuarea unor tranzacţii on-line realizează accesul, fără drept, la sistemul informatic al băncii, în scopul obţinerii de date informatice şi 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 suscitat o practică neunitară

4.2.1. Soluţia problemei de drept

Punctul de vedere este în sensul soluţiei propuse pe Parchetul de pe lângă Înalta Curte de Casaţie şi Justiţie. Prin operaţiunile 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 infracţiunii 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, aşa cum s-a arătat şi 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 şi a codului PIN aferent acestuia (minivideocamere sau dispozitive tip tastatură)

Deţinerea şi procurarea instrumentelor, dispozitivelor şi mijloacelor prin care urmează să se realizeze latura obiectivă a infracţiunii, precum şi activităţile preparatorii întreprinse de viitorul autor al infracţiunii reprezintă acte de pregătire în vederea săvârşirii infracţiunii. Actele de pregătire nu sunt incriminate în legislaţia penală română, decât prin excepţie, atunci când legiuitorul consideră că instrumentele, dispozitivele, mijloacele sau activităţile pregătitoare prezintă, prin ele însele, gradul de pericol social care justifică incriminarea.

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

Deţinerea dispozitivelor de citire a benzii magnetice a cardului, minivideocamerelor sau dispozitivelor tip tastatură şi, implicit, montarea acestora pentru citirea benzii magnetice a cardului concomitent cu captarea codului PIN aferent cardului constituie acte pregătitoare în vederea săvârşirii infracţiunii 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 aceeaşi lege.

4.3. Punctul de vedere al Departamentului de drept public din cadrul Facultăţii de Drept a Universităţii "Babeş Bolyai" cu privire la încadrarea juridică dată faptelor care au suscitat o practică neunitară
4.3.1. Soluţia problemei de drept
Cu privire la montarea la bancomat a dispozitivelor de citire a benzii magnetice a cardului autentic şi a codului PIN aferent acestuia (minivideocamere sau dispozitive tip tastatură)
a) Montarea dispozitivelor nu implică un acces la bancomat nici măcar în situaţia în care peste acţiunea agentului de montare a respectivelor dispozitive se suprapune şi acţiunea victimei de introducere a cardului bancar în bancomat, moment în care se iniţiază procesul de copiere a datelor înscrise pe banda magnetică.
b) Stricta montare a dispozitivelor supuse discuţiei nu poate oferi aplicabilitate art. 46 alin. (2) din Legea nr. 161/2003 prin raportare la art. 42 alin. (2) şi (3) din aceeaşi lege sau a art. 25 din Legea nr. 365/2002 în baza unei analize in abstracto. Aceste încadrări necesită a fi analizate in concreto, ţinându-se seama de starea de fapt prezentă în fiecare speţă în parte. Montarea dispozitivelor implică o deţinere a acestora, ce reprezintă în sensul legii un act preparator care poate viza comiterea unei multitudini de infracţiuni. Din acest considerent nu se poate analiza in abstracto comportamentul agentului, deoarece o asemenea analiză ar evidenţia echivocitatea actului preparator, respectiv nu s-ar putea identifica cu certitudine care a fost scopul deţinerii respectivelor dispozitive.
Singura încadrare juridică care ar putea fi reţinută 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 aceeaşi lege (deţinerea 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 acţiunea victimei de introducere a cardului în bancomat, atrage un concurs real între infracţiunea prevăzută de art. 46 alin. (2) din Legea nr. 161/2003 şi art. 44 alin. (3) din aceeaşi lege.
Cu privire la folosirea la bancomat, pentru retrageri de numerar sau orice alte operaţiuni 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 infracţiunea prevăzută de art. 42 alin. (2) şi (3) din Legea nr. 161/2003 şi cea prevăzută de art. 27 alin. (1) din Legea nr. 365/2002. În situaţia în care cel care clonează cardul, îl utilizează în vederea retragerii de numerar, se va afla sub incidenţa 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 terţe persoane, ori doar îl deţine în acest scop, complicitatea materială (dacă respectivul card este folosit) va fi sancţionată printr-un text distinct, respectiv art. 24 alin. (2) din Legea nr. 365/2002.
4.3.2. Înţelesul unor termeni
În opinia transmisă este definit accesul la un sistem informatic, deoarece soluţiile contradictorii întâlnite în practica judiciară referitoare la încadrarea faptei de montare la ATM a dispozitivelor de citire a benzii magnetice a cardului autentic şi a codului PIN aferent acestuia sunt determinate în principal de modul în care a fost interpretată noţiunea.
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 definiţie susceptibilă să clarifice conţinutul noţiunii. 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 defineşte noţiunea. Definirea accesului prin intrarea în tot sau în parte nu clarifică în nicio măsură conţinutul termenului având în vedere că ne raportăm la un mediu virtual şi la interacţiuni logice, intrarea în sistemul informatic nefiind realizată la nivel fizic.
Sintagma intrarea în tot sau în parte este utilizată de Convenţia privind criminalitatea informatică fără să fie definită însă noţiunea de acces. Sintagma în cauză (într-o formă similară) este utilizată la art. 2 din Convenţie, 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 restricţionat într-o anumită parte a sistemului informatic, acesta putând utiliza doar anumite aplicaţii ori fişiere stocate pe acesta, restul necesitând 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 noţiunii de acces la un sistem informatic:
a) O primă definiţie ar putea fi cea de inspiraţie americană, întâlnită şi în doctrina din România, unde accesul este văzut ca reprezentând capacitatea de a da comenzi, de a cauza introducerea, obţinerea, afişarea, stocarea ori diseminarea de date informatice sau folosirea în orice alt mod a resurselor unui calculator, sistem ori reţea informatică sau comunicarea cu unităţile sale aritmetice, logice ori de memorie (I. Vasiu, L. Vasiu, Contaminanţii informatici ca vector ai accesului ilegal, în Revista de drept penal, nr. 2/2006, p. 37).
Definiţia nu este totuşi lipsită de critică, deoarece înşiruirea de acte materiale susceptibile să ofere contur unui acces la un sistem informatic oferă un conţinut mult prea larg acestei noţiuni. Capacitatea de a da comenzi ar acoperi şi ipoteze care au fost excluse în mod expres prin Raportul explicativ al Convenţiei privind criminalitatea informatică din sfera infracţiunii 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 interacţiune la nivel logic între sistemul informatic utilizat de agent şi sistemul informatic ce găzduieşte serviciul de poştă electronică utilizat de persoana care recepţionează respectivul e-mail. Mai mult, această interacţiune logică implică inclusiv darea unei comenzi (în momentul în care acel e-mail urmează să fie salvat pe sistemul informatic ce găzduieşte serviciul de poştă electronică a destinatarului).
Prin urmare, ne-am afla în situaţia evidentă în care o definiţie mult prea generoasă s-ar afla în contradicţie cu intenţia legiuitorului european, intenţie care a fost transpusă în dreptul intern în mod fidel în urma adoptării Legii nr. 161/2003.
b) O a doua definiţie priveşte accesul ca fiind o interacţiune logică (deci nu orice fel de interacţiune) ce se manifestă prin aceea că agentul poate beneficia de resursele ori/şi funcţiile sistemului informatic (a se vedea G. Zlati, Unele aspecte în legătură cu infracţiunile informatice din perspectiva legislaţiei în vigoare, precum şi a Noului Cod penal, în Dreptul, nr. 10/2012, p. 221).
Atunci când se discută despre un acces local (de exemplu, agentul interacţionează în mod direct cu un laptop) şi nu unul de la distanţă (de exemplu, agentul utilizează o reţea wireless ori internetul pentru a obţine un acces fără drept la un laptop conectat la respectiva reţea wireless ori la internet), se interacţionează şi la nivel fizic cu sistemul informatic. Practic, agentul, prin interacţiunea fizică cu sistemul informatic (pornirea acestuia, transmiterea unor comenzi prin utilizarea tastaturii etc.), oferă contur şi unei interacţiuni la nivel logic. Cu titlu de exemplu, interacţiunea fizică a agentului cu tastatura iniţiază o interacţiune logică, sistemul informatic vizat ajungând să recepţioneze informaţia transmisă de agent prin intermediul tastaturii, să o interpreteze cu ajutorul unui program informatic şi să returneze un răspuns. O interacţiune logică poate avea la bază şi o interacţiune fizică, dar o interacţiune fizică nu implică în mod

necesar şi o interacţiune logică.
Este posibil ca interpretarea eronată a noţiunii 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 acţiunea de intrare în legătură cu elemente precum componente hardware, date informatice, directoare etc. Cu toate acestea, nu s-ar putea susţine că un acces la un sistem informatic se conturează atunci când agentul realizează o acţiune de intrare vizavi de o componentă hardware. O asemenea abordare denotă mai degrabă o incongruenţă logică, deoarece nu se poate imagina o ipoteză în care agentul să intre într-o componentă hardware. Prin urmare, singura interpretare adecvată a noţiunii de acces trebuie să aibă drept premisă o interacţiune strict la nivel logic cu respectivul sistem informatic. Trimiterea la componentele hardware este relevantă doar în contextul în care interacţiunea logică se realizează prin intermediul interacţiunii cu o componentă hardware (interacţiunea 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 şi a codului PIN aferent acestuia (minivideocamere sau dispozitive tip tastatură)
Montarea dispozitivelor de citire a benzii magnetice (skimmer) şi 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 şi să tasteze codul PIN ce urmează a fi înregistrat fie de videocamera plasată de agent, fie de falsa tastatură poziţionată 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 aşa fel încât victima să nu realizeze că urmează să interacţioneze cu alte dispozitive decât cele legitime, ale bancomatului. Între aceste dispozitive şi bancomat nu există absolut nicio interacţiune la nivel logic. Toate dispozitivele funcţionează în mod independent (sunt dispozitive stand alone, fiind alimentate din surse proprii).
b) O a doua ipoteză este aceea în care peste acţiunea agentului de a monta skimmerul se suprapune şi acţiunea victimei de introducere a instrumentului de plată electronică în fanta bancomatului. Din punct de vedere tehnic, în această fază skimmerul interacţionează cu banda magnetică a cardului introdus de victimă, realizându-se o copiere a datelor înscrise pe banda magnetică în memoria internă a skimmerului. Este posibil şi ca skimmerul să transmită la distanţă datele obţinute de pe banda magnetică fie prin wireless, fie prin bluetooth. În acest caz, stocarea datelor de pe banda magnetică se realizează pe un terţ mediu de stocare şi nu în memoria internă a skimmerului.
La fel ca şi în prima ipoteză analizată, este exclusă identificarea unui acces la sistemul informatic, deoarece lipseşte o interacţiune la nivel logic între dispozitivele montate de agent şi dispozitivele bancomatului. Dispozitivele montate de agent obţin datele înscrise pe banda magnetică şi codul PIN utilizând funcţii proprii, iar bancomatul nu are niciun rol în acest proces de copiere/captare a datelor. Atât obţinerea datelor de pe banda magnetică, cât şi captarea codului PIN se realizează în exteriorul bancomatului. Un skimmer poate să copieze datele înscrise pe banda magnetică chiar dacă nu este ataşat unui bancomat ori bancomatul unde a fost plasat skimmerul are o defecţiune tehnică şi nu funcţionează.
Analiza elementelor constitutive ale infracţiunii prevăzute de art. 42 din Legea nr. 161/2003 relevă aşadar lipsa unui element esenţial din structura laturii obiective, respectiv accesul. În cadrul mai general al operaţiunii 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 interacţionează cu skimmerul agentului, moment în care se iniţiază procesul de copiere a datelor. Imediat după acest moment, cardul ajunge să interacţioneze cu dispozitivul legitim de citire al bancomatului moment în care victima ajunge să interacţioneze 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 interacţiona cu bancomatul. Accesul se realizează după ce datele au fost deja copiate de skimmer, moment în care acesta şi-a încetat orice fel de interacţiune cu cardul victimei şi implicit cu aceasta. Punctul de vedere conform căruia nu discutăm despre un acces la un sistem informatic se regăseşte în doctrină (G. Zlati, Unele aspecte în legătură cu infracţiunile informatice din perspectiva legislaţiei în vigoare, precum şi a Noului Cod penal, în Dreptul, nr. 10/2012, p. 218-221). În doctrină s-a exprimat şi 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 existenţei unui acces fără drept la un sistem informatic, autorul achiesând la soluţiile instanţelor de judecată ce au statuat în acest sens.
Plasarea unor asemenea dispozitive nu poate în nicio ipoteză să atragă tipicitatea infracţiunii prevăzute de art. 42 din Legea nr. 161/2003. În acest sens, unele instanţe au considerat că ne aflăm sub incidenţa prevăzută de art. 25 din Legea nr. 365/2002, în timp ce altele au plasat acest comportament sub incidenţa art. 46 alin. (2) din Legea nr. 161/2003. Ambele infracţiuni reprezintă incriminarea unor acte preparatorii. Astfel, dacă în cazul art. 25 din Legea nr. 365/2002 discutăm despre deţinerea unor echipamente în vederea comiterii infracţiunii prevăzute de art. 24 (falsificarea instrumentelor de plată electronică), în cazul art. 46 alin. (2) din Legea nr. 161/2003 discutăm despre deţinerea de echipamente în scopul comiterii infracţiunilor prevăzute de art. 42-45 din aceeaşi lege.
Punctul de vedere transmis de către procurorul general are în vedere că este incident art. 46 alin. (2) din Legea nr. 161/2003 şi nu art. 25 din Legea nr. 365/2002. Argumentul pentru care sa considerat că nu poate primi aplicabilitate art. 25 din Legea nr. 365/2002 a fost acela că prin acesta se incriminează deţinerea de dispozitive în scopul clonării unui instrument de plată electronică. Or, este evident că intenţia agentului poate fi nu doar aceea de a clona instrumentul de plată electronică, ci şi de a utiliza datele obţinute de pe banda magnetică în vederea efectuării unor plăţi on-line. Încadrarea juridică nu poate fi reţinută însă de plano şi in abstracto ca fiind cea prevăzută de art. 46 alin. (2) din Legea nr. 161/2003. Practic, analiza trebuie făcută in concreto, în funcţie de starea de fapt a fiecărei speţe în parte. Este aşadar posibil ca întreaga activitate a agentului să contureze intenţia acestuia de a utiliza datele obţinute prin utilizarea skimmerului în vederea clonării instrumentului de plată electronică, astfel încât reţinerea art. 25 din Legea nr. 365/2002 nu este exclusă, ci doar necesită a fi analizată în funcţie de circumstanţele speţei supuse discuţiei.
În consecinţă:
a) montarea dispozitivelor supuse discuţiei nu implică un acces la bancomat nici atunci când peste acţiunea agentului de montare a respectivelor dispozitive se suprapune şi acţiunea victimei de introducere a cardului bancar în bancomat, moment în care se iniţiază procesul de copiere a datelor înscrise pe banda magnetică;
b) încadrarea juridică care ar putea fi reţinută 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 aceeaşi lege (deţinerea 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 acţiunea victimei de introducere a cardului în bancomat dă naştere unui concurs real între infracţiunea prevăzută de art. 46 alin. (2) din Legea nr. 161/2003 şi art. 44 alin. (3) din aceeaşi lege. Transferul de date dintr-un sistem informatic are drept premisă accesarea acestuia, iar un acces la bancomat este exclus în baza argumentelor deja menţionate, astfel încât nu poate fi reţinută şi infracţiunea 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 noţiunea de transfer, care nu are la bază în mod obligatoriu ştergerea datelor de pe mediul de stocare prin relocarea acestora într-un alt mediu de stocare pe un sistem informatic terţ. Este posibil ca această confuzie să aibă drept izvor o analiză doctrinară (a se vedea M.A. Hotca, M. Dobrinoiu, Infracţiuni prevăzute în legi speciale. Comentarii şi explicaţii, ediţia a 2-a, Ed. C.H. Beck, Bucureşti, 2010, p. 590-591), unde transferul a fost definit ca fiind mutarea fără drept a reprezentării binare dintr-o locaţie în altă locaţie, considerându-se în acest sens că urmarea imediată în cazul transferului de date este ştergerea datelor din locaţia iniţială şi crearea concomitentă a unei replici în altă locaţie. Acelaşi autor a revenit recent asupra acestui punct de vedere (a se vedea M. Dobrinoiu, Comentariu, în V. Dobrinoiu ş.a., Noul Cod penal comentat, Partea specială, vol. II, Ed. Universul Juridic, Bucureşti, 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 aşadar o reinterpretare doctrinară a noţiunii de transfer, care nu mai este privită ca implicând o ştergere a datelor din locaţia iniţială (o relocare a acestora), ci şi o simplă copiere a datelor fără a mai discuta despre vreo ştergere simultană procesului de duplicare. Această din urmă opinie reflectă intenţia legiuitorului, deoarece acesta nu a vizat doar integritatea datelor informatice, ci şi confidenţialitatea acestora. Mai mult, în momentul în care autorul analizează infracţiunea de transfer neautorizat de date de pe un mijloc de stocare (art. 364 din Noul Cod penal), apreciază că această infracţiune acoperă şi situaţiile în care discutăm despre copierea datelor înscrise pe banda magnetică a instrumentului de plată electronică prin intermediul skimmerului (M. Dobrinoiu, Comentariu, în V. Dobrinoiu ş.a., Noul Cod penal comentat, p. 911-912).
4.3.4. Cu privire la folosirea la bancomat, pentru retrageri de numerar sau orice alte operaţiuni financiare, a cardului falsificat ori chiar a celui autentic, fără acordul titularului său
Infracţiunea 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 puţin despre o tentativă de acces la un sistem informatic, astfel încât s-ar putea identifica un concurs ideal cu infracţiunea prevăzută de art. 42 alin. (1), (2) şi (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 şi să introducă suma ce urmează a fi retrasă. Tentativa prevăzută de art. 27 alin. (5) din Legea nr. 365/2002 ar putea fi reţinută 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 PINului, fie doar consultarea soldului şi nu doar retragerea de numerar. În consecinţă, agentul realizează două acţiuni: o primă acţiune vizând accesul la bancomat, iar cea de-a doua acţiune retragerea de numerar prin solicitările trimise bancomatului.
Utilizarea bancomatului nu implică o punere în circulaţie a instrumentului de plată electronică [art. 24 alin. (2) din Legea nr. 365/2002]. Punerea în circulaţie a unei entităţi materiale implică prin natura ei pierderea posesiei asupra acelei entităţi de către titularul iniţial 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 intenţia legiuitorului prin incriminarea punerii în circulaţie ori deţinerii în vederea punerii în circulaţie a avut în vedere ipoteza în care instrumentul de plată electronică este folosit la bancomat. Pentru această utilizare, avem o infracţiune distinctă şi anume cea prevăzută de art. 27 alin. (1) din Legea nr. 365/2002. În situaţia în care cel care clonează cardul, îl utilizează în vederea retragerii de numerar, se află sub incidenţa art. 27 alin. (1) din Legea nr. 365/2002. În măsura în care acesta nu utilizează cardul personal, ci îl înmânează unei terţe persoane ori doar îl deţine în acest scop, complicitatea materială (dacă respectivul card este folosit) este sancţionată 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 infracţiunea prevăzută de art. 42 alin. (2) şi (3) din Legea nr. 161/2003 şi cea prevăzută de art. 27 alin. (1) din Legea nr. 365/2002.
4.4. Punctul de vedere al Departamentului de drept penal din cadrul Facultăţii de Drept a Universităţii Bucureşti cu privire la încadrarea juridică dată faptelor care au suscitat o practică neunitară
4.4.1. Soluţia problemei de drept
a) Deţinerea unui dispozitiv de skimming pentru a fi folosit la accesarea sistemului informatic al băncii şi obţinerea datelor informatice stocate pe cardul bancar constituie infracţiune prevăzută de art. 46 alin. (2) din Legea nr. 161/2003, prin raportare la art. 42 şi art. 44 alin. (3) din aceeaşi lege.
b) Utilizarea dispozitivului de skimming prin montarea la ATM sau POS pentru accesarea sistemului informatic bancar şi obţinerea datelor informatice stocate pe cardul bancar realizează conţinutul constitutiv al infracţiunilor de acces, fără drept, la un sistem informatic săvârşit în scopul obţinerii de date informatice şi prin încălcarea măsurilor de securitate [art. 42 alin. (1), (2) şi (3) din Legea nr. 161/2003] şi 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 informaţiile 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) Deţinerea unor dispozitive optice sau optoelectronice de filmare a introducerilor de coduri PIN pentru efectuarea de autentificări la operaţiuni cu cardul la ATM sau POS constituie infracţiune [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 operaţiuni 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 parţial la un sistem informatic în scopul săvârşirii uneia dintre infracţiunile prevăzute la art. 42-45, fapta va constitui infracţiunea 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 obţinerii codului PIN întruneşte elementele constitutive ale infracţiunii de acces fără drept la un sistem informatic în scopul obţinerii de date informatice [art. 42 alin. (1) şi (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 şi 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 operaţiuni 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 parţial la un sistem informatic în scopul săvârşirii uneia dintre infracţiunile prevăzute la art. 42-45, fapta va constitui infracţiunea prevăzută de art. 46 alin. (1) litera b) din Legea nr. 161/2003.
h) Deţinerea unei tastaturi false pentru înregistrarea introducerilor de coduri PIN la efectuarea de autentificări pentru operaţiuni cu cardul la ATM sau POS constituie infracţiune [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 şi executate de către instituţii financiare, respectiv retrageri de numerar, precum şi încărcarea şi descărcarea unui instrument de monedă electronică constituie infracţiunea de efectuare de operaţiuni 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 infracţiunea de acces, fără drept, la un sistem informatic comisă în scopul obţinerii de date informatice prin încălcarea măsurilor de securitate [art. 42 alin. (1), (2) şi (3) din Legea nr. 161/2003] şi în concurs real cu infracţiunea 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 şi încărcarea/descărcarea unui instrument de monedă electronică constituie infracţiunea de efectuare de operaţiuni 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], săvârşită în concurs ideal cu infracţiunea de acces, fără drept, la un sistem informatic comisă în scopul obţinerii de date informatice prin încălcarea măsurilor de securitate [art. 42 alin. (1), (2) şi (3) din Legea nr. 161/2003].
k) Folosirea informaţiilor obţinute de pe cardul bancar autentic prin transferarea datelor de pe banda magnetică a acestuia la efectuarea unor transferuri de fonduri prin internet constituie infracţiune de efectuare de operaţiuni 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].
Soluţiile recomandate pentru interpretarea situaţiilor de fapt şi realizarea încadrărilor juridice îşi menţin valabilitatea şi după intrarea în vigoare a Noului Cod penal (1 februarie 2014) şi abrogarea prevederilor speciale din Legea nr. 161/2003 şi Legea nr. 365/2002, urmând a fi aplicabile articolele corespunzătoare din Noul Cod penal.
4.4.2. Înţelesul unor termeni
Situaţia de fapt (accesul prin intermediul montării la ATM a dispozitivelor de citire a benzii magnetice a cardului autentic şi 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 şi precizarea terminologiei de specialitate folosite.
Astfel, în art. 35 din Legea nr. 161/2003 sunt prevăzuţi termenii şi expresiile utilizate în reglementarea titlului din lege privind prevenirea şi combaterea criminalităţii informatice, pentru a defini noţiunile tehnice utilizate şi relevante în speţă: a) prin sistem informatic se înţelege orice dispozitiv sau ansamblu de dispozitive interconectate ori aflate în relaţie funcţională, dintre care unul sau mai multe asigură prelucrarea automată a datelor, cu ajutorul unui program informatic; b) prin prelucrare automată a datelor se înţelege procesul prin care datele dintr-un sistem informatic sunt prelucrate prin intermediul unui program informatic; c) prin program informatic se înţelege un ansamblu de instrucţiuni care pot fi executate de un sistem informatic în vederea obţinerii unui rezultat determinat; d) prin date informatice se înţelege orice reprezentare a unor fapte, informaţii sau concepte într-o formă care poate fi prelucrată printr-un sistem informatic. În această categorie se include şi orice program informatic care poate determina realizarea unei funcţii de către un sistem informatic; e) (...); f) prin date referitoare la traficul informaţional se înţelege orice date informatice referitoare la o comunicare realizată printr-un sistem informatic şi produse de acesta, care reprezintă o parte din lanţul de comunicare, indicând originea, destinaţia, ruta, ora, data, mărimea, volumul şi durata comunicării, precum şi tipul serviciului utilizat pentru comunicare; g) prin date referitoare la utilizatori se înţelege orice informaţie care poate conduce la identificarea unui utilizator, incluzând tipul de comunicaţie şi serviciul folosit, adresa poştală, adresa geografică, numere de telefon sau alte numere de acces şi modalitatea de plată a serviciului respectiv, precum şi orice alte date care pot conduce la identificarea utilizatorului; h) prin măsuri de securitate se înţelege folosirea unor proceduri, dispozitive sau programe informatice specializate cu ajutorul cărora accesul la un sistem informatic este restricţionat 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 informaţiilor 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, maşină 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 informaţiile cuprinse în schema privind arhitectura montajului electronic dintr-un skimmer şi cele privind funcţionarea acestor dispozitive, coroborate cu prevederile art. 35 alin. (1) lit. a) din Legea nr. 161/2003 privind definiţia sistemului informatic, rezultă că dispozitivul de skimming este un sistem informatic, chiar dacă este unul mai "primitiv" în ceea ce priveşte capacitatea de prelucrare a datelor. Dispozitivul de skimming poate fi folosit pentru accesarea sistemului informatic al băncii şi obţinerea datelor informatice stocate pe cardul bancar în vederea întrebuinţării lor doar în mod direct (de exemplu, pentru cumpărături on-line întrebuinţând datele de identificare de pe card) sau pentru "clonarea cardurilor" (falsificarea unor instrumente de plată electronică pe baza informaţiilor obţinute de pe cardul autentic).

ATM-urile şi POS-urile sunt terminale şi/sau periferice ale sistemului informatic bancar, prin intermediul lor realizându-se mai multe funcţii: identificarea clientului (titular al contului bancar), identificarea contului bancar al clientului, accesarea sistemului bancar al clientului (prin intermediul sistemului informatic al băncii căreia îi aparţine 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 operaţiunea de plată cerută, contul bancar creditor (la plăţile prin ATM sau POS) şi confirmarea soldului suficient al contului bancar debitor al clientului, precum şi tipărirea operaţiunilor realizate şi înregistrate în sistemele informatice ale băncilor implicate.

Cardurile bancare (de credit sau de debit) stochează pe banda lor magnetică informaţii privind numărul contului bancar, numele titularului cardului, date adiţionale privind data expirării cardului, precum şi alte date discreţionare, la latitudinea băncii emitente a cardului. Potrivit art. 35 alin. (1) lit. d) din Legea 161/2003 rezultă că informaţiile 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 acelaşi timp, datele informatice conţinute pe banda magnetică a cardului bancar autentic sunt absolut necesare în cazul falsificării unui card bancar, precum şi pentru efectuarea unor operaţiuni financiare în mod fraudulos.

Orice folosire a unui ATM sau POS reprezintă o accesare a unui sistem informatic, fie pentru a obţine 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 şi 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 obţinerii de date informatice, prin încălcarea măsurilor de securitate existente pe benzile magnetice ale cardului bancar, cât şi 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 informaţiile 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 deţinere a dispozitivului de skimming este incriminată distinct atât în cazul în care se urmăreşte exclusiv obţinerea unor date informatice prin accesarea fără drept a sistemului informatic şi transferarea datelor informatice din cardul bancar, cât şi în cazul în care aceste operaţiuni sunt premergătoare, dar indispensabile, falsificării unui instrument de plată electronică (card bancar clonat). Trebuie menţionat că, în sens informatic, transferarea unor date informatice reprezintă o operaţiune de copiere a unor fişiere sau programe informatice, fără ştergerea lor de pe suportul-sursă (mediul de stocare). Transferarea unor date nu este o mutare fizică a datelor pe noul suport informatic, afirmaţia în sens contrar făcută în recursul în interesul legii promovat de Parchetul de pe lângă Înalta Curte de Casaţie şi Justiţie 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 operaţiuni la ATM sau POS. Fapta, considerată distinct de transferarea datelor de pe banda magnetică a cardului bancar, are relevanţă penală întrucât este un act preparator incriminat expres în art. 46, raportat la art. 42-45, din Legea nr. 161/2003, prin care se urmăreşte de către făptuitor obţinerea pe cale vizuală a codului de acces la sistemu[informatic al băncii titularului cardului bancar folosit pentru autentificarea operaţiunilor cu cardul. În acelaşi timp însă aceeaşi faptă este act preparator în cazul falsificării unor instrumente de plată electronică sau săvârşirii infracţiunii de efectuare de operaţiuni financiare în mod fraudulos.

Cu totul alta este situaţia 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 şi să acceseze astfel, fără drept, sistemul informatic în scopul obţinerii 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 şi 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 şi a codului PIN aferent acestuia (minivideocamere sau dispozitive tip tastatură)

Faptele în legătură cu încălcarea relaţiilor sociale privind protejarea integrităţii fizice şi funcţionale a sistemelor şi datelor informatice sunt incriminate în art. 42-50 din titlul III (Prevenirea şi combaterea criminalităţii informatice) din Legea nr. 161/2003 privind unele măsuri pentru asigurarea transparenţei în exercitarea demnităţilor publice, a funcţiilor publice şi în mediul de afaceri, prevenirea şi sancţionarea corupţiei. Faptele privind operaţiunile ilicite în legătură cu instrumentele de plată electronică sunt incriminate în art. 24-28 din Legea nr. 365/2002 privind comerţul electronic.

Incriminările 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 şi 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 şi mijloace de plată electronice), art. 311 (Falsificarea de titluri de credit sau instrumente de plată), art. 313 (Punerea în circulaţie de valori falsificate), art. 314 (Deţinerea 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 integrităţii datelor informatice), art. 363 (Perturbarea funcţionării sistemelor informatice) şi art. 365 (Operaţiuni ilegale cu dispozitive sau programe informatice) din Noul Cod penal (Legea nr. 286/2009).

Obiectul juridic generic al infracţiunilor din Legea nr. 161/2003 este reprezentat de relaţiile sociale a căror formare şi dezvoltare normală impun respectarea necondiţionată a confidenţialităţii şi integrităţii datelor şi sistemelor informatice, viaţa contemporană fiind dominată de tehnologizarea şi informatizarea accentuate în cadrul tuturor domeniilor de activitate.

Obiectul juridic generic al infracţiunilor din Legea nr. 365/2002 este reprezentat de relaţiile sociale în legătură cu emiterea şi utilizarea instrumentelor de plată electronică şi cu utilizarea datelor de identificare în vederea efectuării de operaţiuni financiare a căror formare şi dezvoltare normală impun respectarea încrederii publice în mijloacele de plată

electronice, precum şi protejarea patrimoniului persoanelor fizice sau juridice împotriva utilizării frauduloase a instrumentelor de plată electronică ori a datelor de identificare a acestora.

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

b) Utilizarea dispozitivului de skimming prin montarea la ATM sau POS pentru accesarea sistemului informatic bancar şi obţinerea datelor informatice stocate pe cardul bancar realizează conţinutul constitutiv al infracţiunilor de acces, fără drept, la un sistem informatic săvârşit în scopul obţinerii de date informatice şi prin încălcarea măsurilor de securitate [art. 42 alin. (1), (2) şi (3) din Legea nr. 161/2003] şi 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 informaţiile 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) Deţinerea unor dispozitive optice sau optoelectronice de filmare a introducerilor de coduri PIN pentru efectuarea de autentificări la operaţiuni cu cardul la ATM sau POS constituie infracţiune [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 operaţiuni 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 parţial la un sistem informatic în scopul săvârşirii uneia dintre infracţiunile prevăzute la art. 42-45, fapta va constitui infracţiunea prevăzută de art. 46 alin. f1) lit. b) din Legea nr. 161/2003.

f) Amplasarea unei tastaturi false deasupra tastaturii originale de la ATM sau POS în scopul obţinerii codului PIN întruneşte elementele constitutive ale infracţiunii de acces fără drept la un sistem informatic în scopul obţinerii de date informatice [art. 42 alin. (1) şi (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 şi 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 operaţiuni 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 parţial la un sistem informatic în scopul săvârşirii uneia dintre infracţiunile prevăzute la art. 42-45, fapta va constitui infracţiunea prevăzută de art. 46 alin. (1) litera (b) din Legea nr. 161/2003.

h) Deţinerea unei tastaturi false pentru înregistrarea introducerilor de coduri PIN la efectuarea de autentificări pentru operaţiuni cu cardul la ATM sau POS constituie infracţiune [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 şi încărcarea/descărcarea unui instrument de monedă electronică constituie infracţiunea de efectuare de operaţiuni 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 şi pot fi folosite preponderent, dar nu exclusiv, în cadrul unui sistem informatic pentru efectuarea unor operaţiuni 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 şi în afara unui sistem informatic, de exemplu, pentru garantarea stingerii unor eventuale obligaţii 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 infracţiunii de efectuare de operaţiuni financiare în mod fraudulos prin utilizarea unui instrument de plată electronică autentic sau falsificat, săvârşirea acestei infracţiuni neimplicând, ca o condiţie esenţială de existenţă, accesarea unui sistem informatic bancar prin intermediul căruia infracţiunea să fie comisă. Din acest motiv se impune reţinerea în concurs ideal, atunci când este cazul, a infracţiunii de acces fără drept la sistemul informatic al băncii în scopul obţinerii 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 operaţiuni de inscripţionare/transferare a datelor informatice privind cardul real, autentic, asupra cardurilor contrafăcute, acestea din urmă fiind adevărate "clone" ale unor carduri reale, valabile şi operaţionale. Din acest motiv, acţiunile de obţinere a datelor informatice de pe un card bancar autentic, în orice mod, în afara cadrului legal şi 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 operaţiuni financiare în mod fraudulos este falsificat, se va reţine în concurs real şi infracţiunea de falsificare a instrumentelor de plată electronică.

4.5. Punctul de vedere al Catedrei de Drept Penal din cadrul Facultăţii de Drept şi Ştiinţe Administrative a Universităţii din Craiova cu privire la încadrarea juridică dată faptelor care au suscitat o practică neunitară

4.5.1. Soluţia 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 operaţiuni financiare a unui card falsificat ori a unuia real, fără consimţământul titularului său, sunt întrunite elementele constitutive ale infracţiunii prevăzute de art. 42 alin. (1), (2) şi (3) din Legea nr. 161/2003, săvârşită 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 şi 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 informaţiile din sistem. Prin montarea unui skimmer nu are loc o interacţiune cu bancomatul, privit ca sistem informatic, ci doar cu instrumentul de plată electronic, cu banda magnetică a cardului, ale cărui informaţii sunt copiate, stocate în memoria skimmerului.

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

Un alt argument privind lipsa elementului material al infracţiunii rezultă din faptul că datele de pe banda magnetică a cardului sunt citite şi captate înainte ca respectivul card să intre în fanta bancomatului şi înainte să se realizeze vreo transmisie de date informatice între card şi ATM. Într-o astfel de situaţie, ATM-ul este folosit doar ca un suport fizic, ca un camuflaj pentru skimmer, şi 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 infracţiunii prevăzute de art. 42 alin. (1) din Legea nr. 161/2003, însă o astfel de faptă se încadrează drept deţinere, fără drept, a unui dispozitiv în vederea săvârşirii uneia dintre infracţiunile 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 operaţiuni financiare, a cardului falsificat ori chiar a celui autentic, fără acordul titularului său

În cazul în care, după obţinerea cardului falsificat, acesta este folosit în scopul retragerii de numerar are loc o accesare a datelor din bancomat. Bancomatul nu mai este întrebuinţat doar ca un suport, ci potrivit destinaţiei sale, ca o componentă a unui sistem informatic ce permite conectarea în sistem şi cunoaşterea datelor conţinute de acest sistem. Într-o astfel de situaţie, există un schimb de informaţii între cel care utilizează cardul şi 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 infracţiunii prevăzute şi sancţionate de art. 42 alin. (1) din Legea nr. 161/2003. Infracţiunea există şi s-a consumat din acest moment, indiferent dacă s-a solicitat sau nu vreo operaţiune financiară. O astfel de solicitare nu este necesară pentru existenţa infracţiunii în discuţie ale cărei elemente constitutive s-au unit în momentul în care a avut loc schimbul de informaţii, ceea ce înseamnă acces ca element material al infracţiunii.

În cazul folosirii la bancomat, pentru retrageri de numerar sau alte operaţiuni financiare, a unui card falsificat ori a unuia real, fără consimţământul titularului său, sunt întrunite elementele constitutive ale infracţiunii prevăzute de art. 42 alin. (1), (2) şi (3) din Legea nr. 161/2003, săvârşită 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 Facultăţii de Drept a Universităţii "Lucian Blaga" din Sibiu cu privire la încadrarea juridică dată faptelor care au suscitat o practică neunitară

4.6.1. Soluţia 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 deţinute fără drept şi, prin urmare, nu sunt întrunite elementele constitutive ale infracţiunii prevăzute de art. 46 alin. (2) din Legea nr. 161/2003.

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

c) Ţinând cont de prevederile legale enunţate se impune a se analiza în concret operaţiunile efectuate de făptuitor, deoarece este posibil ca făptuitorul care efectuează doar retrageri de numerar sau plăţi cu acel card (real ori falsificat), fără să facă interogări de sold, să nu urmărească să obţină date informatice, în astfel de situaţii lipsind scopul special cerut expres de prevederile art. 42 alin. (2) din Legea nr. 161/2003. Acestea nu pot fi reţinute în sarcina sa, urmând a fi incidente doar cele ale alin. (1) şi (3) ale aceluiaşi articol (operaţiunea fiind efectuată în mod clar prin încălcarea măsurilor de securitate).

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

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

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

Montarea la ATM a dispozitivului de citire a benzii magnetice a cardului şi a videocamerei ori a dispozitivului modificat de tip tastatură nu realizează accesul fără drept la un sistem informatic, infracţiune 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 Casaţie şi Justiţie, punctul de vedere subliniază faptul că, deşi 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 şi a video-camerei 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 menţionate. Nu există deci în această situaţie nicio interacţiune a făptuitorului cu tehnica de calcul prin intermediul echipamentelor utilizate. O astfel de faptă reprezintă practic un act preparator al infracţiunii de acces fără drept la un sistem informatic, care însă nu este incriminat.

În opinia procurorului general se arată că deţinerea, fără drept, a unui dispozitiv, program informatic, parolă, cod de acces sau dată informatică în scopul săvârşirii uneia dintre infracţiunile prevăzute la art. 42-45 din Legea nr. 161/2003 constituie infracţiunea prevăzută de art. 46 alin. (2) din aceeaşi lege. Trebuie însă analizat în concret dacă dispozitivul utilizat de făptuitor este deţinut fără drept sau nu. Telefonul mobil, camera video sau chiar un dispozitiv modificat tip tastatură nu pot fi considerate ca fiind dispozitive deţinute fără drept şi, prin urmare, nu sunt întrunite elementele constitutive ale infracţiunii prevăzute de art. 46 alin. (2) din Legea nr. 161/2003. Deţinerea telefonului mobil sau a camerei video nu se încadrează nici în prevederile art. 25 din Legea nr. 365/2002, care incriminează fabricarea ori deţinerea de echipamente, inclusiv hardware sau software, cu scopul de a servi la falsificarea instrumentelor de plată

electronică (deşi au existat şi soluţii în acest sens).
4.6.3. Cu privire la folosirea la bancomat, pentru retrageri de numerar sau orice alte operaţiuni 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 priveşte încadrarea juridică a unor astfel de fapte.
În opinia exprimată de procurorul general se arată că fapta întruneşte elementele constitutive ale infracţiunii prevăzute de art. 42 alin. (1), (2) şi (3) din Legea nr. 161/2003. Norma de incriminare are următorul cuprins: (1) Accesul, fără drept, la un sistem informatic constituie infracţiune şi se pedepseşte cu închisoare de la 3 luni la 3 ani sau cu amendă. (2) Fapta prevăzută la alin. (1), săvârşită în scopul obţinerii de date informatice, se pedepseşte cu închisoare de la 6 luni la 5 ani. (3) Dacă fapta prevăzută la alin. (1) sau (2) este săvârşită prin încălcarea măsurilor de securitate, pedeapsa este închisoarea de la 3 la 12 ani."
Ţinând cont de prevederile legale enunţate se impune a se analiza în concret operaţiunile efectuate de făptuitor, deoarece este posibil ca făptuitorul care efectuează doar retrageri de numerar sau plăţi cu acel card (real ori falsificat), fără să facă interogări de sold, să nu urmărească să obţină date informatice. În astfel de situaţii lipseşte scopul special cerut expres de prevederile alin. (2) ale art. 42 din Legea nr. 161/2003. Acestea nu pot fi reţinute în sarcina sa, urmând a fi incidente doar cele ale alin. (1) şi (3) ale aceluiaşi articol (operaţiunea fiind efectuată în mod clar prin încălcarea măsurilor de securitate).
În situaţia în care făptuitorul utilizează cardul real sau falsificat pentru interogarea soldului ori pentru alte operaţiuni care i-ar pune la dispoziţie date informatice (urmate sau nu de retrageri de numerar, transferuri ori plăţi), încadrarea juridică este cea prevăzută de art. 42 alin. (1), (2) şi (3) din Legea nr. 161/2003.
În ipoteza efectuării de retrageri de numerar, plăţi sau transferuri de bani, infracţiunea de acces fără drept la un sistem informatic intră în concurs cu infracţiunile prevăzute de Legea nr. 365/2002 referitoare la comerţul electronic. Dacă vorbim de cardul falsificat, infracţiunea va fi cea prevăzută de art. 24 alin. (2) din lege (punerea în circulaţie a unui instrument de plată electronică falsificat), iar dacă se are în vedere un card real, folosit fără consimţământul 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 Facultăţii de Drept a Universităţii de Vest din Timişoara cu privire la încadrarea juridică dată faptelor care au suscitat o practică neunitară
4.7.1. Înţelesul 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, permiţând doar copierea codurilor înscrise pe cardul care asigură accesarea sistemului informatic.
Prin transfer neautorizat se înţelege mutarea fără drept a reprezentării binare a informaţiilor din mediul de stocare curent (autorizat) pe un alt suport de stocare extern sau chiar în interiorul aceluiaşi sistem, informatic, dar în altă locaţie.
4.7.2. Soluţia problemei de drept
a) Deţinerea dispozitivelor de skimming, dacă au fost concepute sau adaptate în scopul săvârşirii uneia dintre infracţiunile prevăzute la art. 42-45, constituie infracţiunea prevăzută de art. 46 alin. (2) din Legea nr. 161/2003, nefiind necesară ataşarea lor la bancomat.
b) Deţinerea dispozitivelor de skimming nu poate realiza însă şi conţinutul infracţiunilor prevăzute de art. 44 alin. (2) şi (3), deoarece nu are loc un transfer de date din sistemul informatic ATM şi mutarea lor în alt loc, ci doar o copiere a datelor înscrise pe card.
c) După ce se clonează un card şi prin intermediul acestuia se accesează bancomatul, chiar fără a se efectua nicio operaţiune bancară, se săvârşeşte infracţiunea prevăzută de art. 42 din Legea nr. 161/2003, aflată în concurs etiologic cu infracţiunea prevăzută de art. 46 alin. (2) din Legea nr. 161/2003.
d) Nu se poate reţine infracţiunea prevăzută de art. 25 din Legea nr. 365/2002, constând în fabricarea ori deţinerea 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 inscripţioneze datele copiate.
4.7.3. Cu privire la montarea la bancomat a dispozitivelor de citire a benzii magnetice a cardului autentic şi a codului PIN aferent acestuia (minivideocamere sau dispozitive tip tastatură)
Deţinerea dispozitivelor de skimming, dacă au fost concepute sau adaptate în scopul săvârşirii uneia dintre infracţiunile prevăzute la art. 42-45, constituie infracţiunea prevăzută de art. 46 alin. (2) din Legea nr. 161/2003, nefiind necesară ataşarea lor la bancomat.
Ataşarea lor la bancomat şi citirea benzii magnetice a cardului nu realizează însă accesarea sistemului informatic al bancomatului, permiţând doar fabricarea (clonarea) ulterioară a unui card, cu care să se acceseze sistemul informatic. Citirea datelor cardului se realizează înainte ca acesta să interacţioneze 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 şi dispozitivul electronic) să interacţioneze, nu poate fi apreciată ca fiind un acces neautorizat. Montarea unui echipament de skimming la un ATM, în vederea obţinerii datelor cardurilor utilizate la respectivul terminal, constituie doar infracţiunea prevăzută de art. 46 alin. (2) din Legea nr. 161/2003.
Această infracţiune reprezintă o infracţiune mijloc pentru săvârşirea infracţiunilor prevăzute de art. 42-45, deci inclusiv pentru săvârşirea infracţiunii de acces fără drept la un sistem informatic.
Deţinerea dispozitivelor de skimming nu poate realiza însă şi conţinutul infracţiunilor prevăzute de art. 44 alin. (2) şi (3), deoarece nu are loc un transfer de date din sistemul informatic ATM şi mutarea lor în alt loc, ci doar o copiere a datelor înscrise pe card.
În cazul transferului de date informatice, urmarea o constituie, pe de o parte, ştergerea datelor informatice din locaţia iniţială, astfel că acestea nu mai există pentru utilizatorul de drept, şi crearea concomitentă a unei replici a datelor informatice, pe acelaşi suport de stocare sau pe un altul, extern, în posesia făptuitorului. Abia după ce cu ajutorul datelor captate prin skimming se clonează un card şi prin intermediul acestuia se accesează bancomatul, chiar fără a se efectua nicio operaţiune bancară, se săvârşeşte infracţiunea prevăzută de art. 42 din Legea nr. 161/2003, aflată în

concurs etiologic cu infracţiunea prevăzută de art. 46 alin. (2) din Legea nr. 161/2003.
Nu se poate reţine infracţiunea prevăzută de art. 25 din Legea nr. 365/2002, constând în fabricarea ori deţinerea 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 inscripţioneze datele copiate.
Doar deţinerea de echipamente hardware sau software care permit falsificarea instrumentelor de plată electronică realizează conţinutul infracţiunii prevăzute de art. 25 din Legea nr. 365/2002, iar falsificarea efectivă a cardului realizează conţinutul infracţiunii 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 operaţiuni 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 şi operaţiuni financiare (retrageri de sume, plăţi, transferuri etc.) infracţiunea de acces neautorizat va veni în concurs cu infracţiunea prevăzută de art. 27 alin. (1) sau (2) din Legea nr. 365/2002, constând în efectuarea de operaţiuni financiare în mod fraudulos, infracţiuni 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 infracţiunii va obţine accesul la datele de cont, sistemul percepându-l ca fiind persoana autorizată.
Infracţiunea 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 urmăreşte protejarea operaţiunilor financiare. Cele două infracţiuni diferă şi prin faptul că accesul neautorizat constituie infracţiune de pericol, fără a fi nevoie să se producă un prejudiciu, pe când infracţiunea de efectuare a unor operaţiuni financiare în mod fraudulos reprezintă o infracţiune de rezultat.
5. Raportul asupra recursului în interesul legii
5.1. Legislaţia relevantă
5.1.1. Legea nr. 161/2003 privind unele măsuri pentru asigurarea transparenţei în exercitarea demnităţilor publice, a funcţiilor publice şi în mediul de afaceri, prevenirea şi sancţionarea corupţiei
Faptele în legătură cu încălcarea relaţiilor sociale privind protejarea integrităţii fizice şi funcţionale a sistemelor şi datelor informatice sunt incriminate în art. 42-50, cartea 1, titlul III ("Prevenirea şi combaterea criminalităţii informatice") din Legea nr. 161/2003 privind unele măsuri pentru asigurarea transparenţei în exercitarea demnităţilor publice, a funcţiilor publice şi în mediul de afaceri, prevenirea şi sancţionarea corupţiei, iar art. 35 din Legea nr. 161/2003 prevede înţelesul termenilor şi expresiilor utilizate în reglementarea titlului respectiv:
"LEGE privind unele măsuri pentru asigurarea transparenţei în exercitarea demnităţilor publice, a funcţiilor publice şi în mediul de afaceri, prevenirea şi sancţionarea corupţiei
CARTEA I: Reglementări generale pentru prevenirea şi combaterea corupţiei
.....
Titlul III: Prevenirea şi combaterea criminalităţii informatice
CAPITOLUL I: Dispoziţii generale
Art. 34
Prezentul titlu reglementează prevenirea şi combaterea criminalităţii informatice, prin măsuri specifice de prevenire, descoperire şi sancţionare a infracţiunilor săvârşite prin intermediul sistemelor informatice, asigurându-se respectarea drepturilor omului şi protecţia datelor personale.
Art. 35
(1) În prezentul titlu, termenii şi expresiile de mai jos au următorul înţeles:
a) prin sistem informatic se înţelege orice dispozitiv sau ansamblu de dispozitive interconectate sau aflate în relaţie funcţională, dintre care unul sau mai multe asigură prelucrarea automată a datelor, cu ajutorul unui program informatic;
b) prin prelucrare automată a datelor se înţelege procesul prin care datele dintr-un sistem informatic sunt prelucrate prin intermediul unui program informatic;
c) prin program informatic se înţelege un ansamblu de instrucţiuni care pot fi executate de un sistem informatic în vederea obţinerii unui rezultat determinat;
d) prin date informatice se înţelege orice reprezentare a unor fapte, informaţii sau concepte într-o formă care poate fi prelucrată printr-un sistem informatic. În această categorie se include şi orice program informatic care poate determina realizarea unei funcţii de către un sistem informatic;
e) prin furnizor de servicii se înţelege:
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 şi pentru utilizatorii serviciilor oferite de acestea;
f) prin date referitoare la traficul informaţional se înţelege orice date informatice referitoare la o comunicare realizată printr-un sistem informatic şi produse de acesta, care reprezintă o parte din lanţul de comunicare, indicând originea, destinaţia, ruta, ora, data, mărimea, volumul şi durata comunicării, precum şi tipul serviciului utilizat pentru comunicare;
g) prin date referitoare la utilizatori se înţelege orice informaţie care poate conduce la identificarea unui utilizator, incluzând tipul de comunicaţie şi serviciul folosit, adresa poştală, adresa geografică, numere de telefon sau alte numere de acces şi modalitatea de plată a serviciului respectiv, precum şi orice alte date care pot conduce la identificarea utilizatorului;
h) prin măsuri de securitate se înţelege folosirea unor proceduri, dispozitive sau programe informatice specializate cu ajutorul cărora accesul la un sistem informatic este restricţionat sau interzis pentru anumite categorii de utilizatori;
i) (...)
(2) În sensul prezentului titlu, acţionează fără drept persoana care se află în una dintre următoarele situaţii:

a) nu este autorizată, în temeiul legii sau al unui contract;
b) depăşeşte 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 desfăşura cercetări ştiinţifice sau de a efectua orice altă operaţiune într-un sistem informatic.
.....
CAPITOLUL III: Infracţiuni şi contravenţii
SECŢIUNEA 1: Infracţiuni contra confidenţialităţii şi integrităţii datelor şi sistemelor informatice
Art. 42
(1) Accesul, fără drept, la un sistem informatic constituie infracţiune şi se pedepseşte cu închisoare de la 3 luni la 3 ani sau cu amendă.
(2) Fapta prevăzută la alin. (1), săvârşită în scopul obţinerii de date informatice, se pedepseşte cu închisoare de la 6 luni la 5 ani.
(3) Dacă fapta prevăzută la alin. (1) sau (2) este săvârşită 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 şi care este destinată unui sistem informatic, provine dintr-un asemenea sistem sau se efectuează în cadrul unui sistem informatic constituie infracţiune şi se pedepseşte cu închisoare de la 2 la 7 ani.
(2) Cu aceeaşi pedeapsă se sancţionează şi interceptarea, fără drept, a unei emisii electromagnetice provenite dintr-un sistem informatic ce conţine date informatice care nu sunt publice.
Art. 44
(1) Fapta de a modifica, şterge sau deteriora date informatice ori de a restricţiona accesul la aceste date, fără drept, constituie infracţiune şi se pedepseşte cu închisoare de la 2 la 7 ani.
(2) Transferul neautorizat de date dintr-un sistem informatic se pedepseşte cu închisoare de la 3 la 12 ani.
(3) Cu pedeapsa prevăzută la alin. (2) se sancţionează şi transferul neautorizat de date dintr-un mijloc de stocare a datelor informatice.
Art. 45
Fapta de a perturba grav, fără drept, funcţionarea unui sistem informatic, prin introducerea, transmiterea, modificarea, ştergerea sau deteriorarea datelor informatice sau prin restricţionarea accesului la aceste date constituie infracţiune şi se pedepseşte cu închisoare de la 3 la 15 ani.
Art. 46
(1) Constituie infracţiune şi se pedepseşte cu închisoare de la 1 la 6 ani:
a) fapta de a produce, vinde, de a importa, distribui sau de a pune la dispoziţie, sub orice altă formă, fără drept, a unui dispozitiv sau program informatic conceput sau adaptat în scopul săvârşirii uneia dintre infracţiunile prevăzute la art. 42-45;
b) fapta de a produce, vinde, de a importa, distribui sau de a pune la dispoziţie, sub orice altă formă, fără drept, a unei parole, cod de acces sau alte asemenea date informatice care permit accesul total sau parţial la un sistem informatic în scopul săvârşirii uneia dintre infracţiunile prevăzute la art. 42-45.
(2) Cu aceeaşi pedeapsă se sancţionează şi deţinerea, fără drept, a unui dispozitiv, program informatic, parolă, cod de acces sau dată informatică dintre cele prevăzute la alin. (1) în scopul săvârşirii uneia dintre infracţiunile prevăzute la art. 42-45.
Art. 47
Tentativa infracţiunilor prevăzute la art. 42-46 se pedepseşte."
5.1.2. Legea nr. 365/2002 privind comerţul electronic. Faptele privind operaţiunile ilicite în legătură cu instrumentele de plată electronică sunt incriminate în art. 24-28 din Legea nr. 365/2002 privind comerţul electronic.
"LEGE privind comerţul electronic
CAPITOLUL I: Dispoziţii generale
Art. 1: Definiţii
În înţelesul prezentei legi, următorii termeni se definesc astfel: (...)
11. instrument de plată electronică - un instrument care permite titularului său să efectueze următoarele tipuri de operaţiuni:
a) transferuri de fonduri, altele decât cele ordonate şi executate de către instituţii financiare;
b) retrageri de numerar, precum şi încărcarea şi descărcarea unui instrument de monedă electronică;
12. instrument de plată cu acces la distanţă - instrument de plată electronică prin intermediul căruia titularul său poate să îşi acceseze fondurile deţinute într-un cont la o instituţie financiară şi să autorizeze efectuarea unei plăţi, 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 distanţă, pe care unităţile de valoare sunt stocate electronic şi care permite titularului său să efectueze tipurile de operaţiuni menţionate la pct. 11;
14. titular - persoană care deţine un instrument de plată electronică pe baza unui contract încheiat cu un emitent, în condiţiile prevăzute de lege;
15. date de identificare - orice informaţii care pot permite sau facilita efectuarea tipurilor de operaţiuni menţionate la pct. 11, precum un cod de identificare, numele sau denumirea, domiciliul ori sediul, numărul de telefon, fax, adresa de poştă electronică, numărul de înmatriculare sau alte mijloace similare de identificare, codul de înregistrare fiscală, codul numeric personal şi altele asemenea;
16. (...)
Art. 2: Scop şi domeniu de aplicare
(1) Prezenta lege are ca scop stabilirea condiţiilor de furnizare a serviciilor societăţii informaţionale, precum şi prevederea ca infracţiuni a unor fapte săvârşite în legătură cu securitatea domeniilor utilizate în comerţul electronic, emiterea şi utilizarea instrumentelor de plată electronică şi cu utilizarea datelor de identificare în vederea efectuării de operaţiuni financiare, pentru asigurarea unui cadru favorabil liberei circulaţii şi dezvoltării în condiţii de securitate a acestor servicii. (...)

.....

CAPITOLUL VIII: Infracţiuni săvârşite în legătură cu emiterea şi utilizarea instrumentelor de plată electronică şi cu utilizarea datelor de identificare în vederea efectuării de operaţiuni financiare

Art. 24: Falsificarea instrumentelor de plată electronică

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

(2) Cu aceeaşi pedeapsă se sancţionează punerea în circulaţie, în orice mod, a instrumentelor de plată electronică falsificate sau deţinerea lor în vederea punerii în circulaţie.

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

a) realizează operaţii tehnice necesare emiterii instrumentelor de plată electronică ori efectuării tipurilor de operaţiuni 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 operaţiuni prevăzute la art. 1 pct. 11.

(4) Tentativa se pedepseşte.

Art. 25: Deţinerea de echipamente în vederea falsificării instrumentelor de plată electronică

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

Art. 26: Falsul în declaraţii în vederea emiterii sau utilizării instrumentelor de plată electronică

Declararea necorespunzătoare adevărului, făcută unei instituţii bancare, de credit sau financiare ori oricărei alte persoane juridice autorizate în condiţiile legii să emită instrumente de plată electronică sau să accepte tipurile de operaţiuni 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, declaraţia făcută serveşte pentru emiterea sau utilizarea acelui instrument, se pedepseşte cu închisoare de la 3 luni la 2 ani sau cu amendă.

Art. 27: Efectuarea de operaţiuni financiare în mod fraudulos

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

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

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

(4) Pedeapsa este închisoarea de la 3 la 15 ani şi interzicerea unor drepturi, dacă faptele prevăzute la alin. (1)-(3) sunt săvârşite de o persoană care, în virtutea atribuţiilor sale de serviciu:

a) realizează operaţii tehnice necesare emiterii instrumentelor de plată electronică ori efectuării tipurilor de operaţiuni 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 operaţiuni prevăzute la art. 1 pct. 11.

(5) Tentativa se pedepseşte.

Art. 28: Acceptarea operaţiunilor financiare efectuate în mod fraudulos

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

(2) Cu aceeaşi pedeapsă se sancţionează acceptarea uneia dintre operaţiunile 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 pedepseşte."

5.1.3. Noul Cod penal

Incriminările 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 şi 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 şi mijloace de plată electronice), art. 311 (Falsificarea de titluri de credit sau instrumente de plată), art. 313 (Punerea în circulaţie de valori falsificate), art. 314 (Deţinerea 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 integrităţii datelor informatice), art. 363 (Perturbarea funcţionării sistemelor informatice) şi art. 365 (Operaţiuni ilegale cu dispozitive sau programe informatice) din noul Cod penal (Legea nr. 286/2009).

5.2. Soluţia preconizată

Recursul în interesul legii solicită, conform sesizării, clarificarea noţiunii de acces fără drept la un sistem informatic, iar în anexele cuprinzând jurisprudenţa în divergenţă 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) şi art. 46 alin. (2) în anexa nr. 41, art. 46 alin. (2) în anexele nr. 39, 46, 47] şi 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) şi (2), art. 25 şi art. 27 alin. (1) în concurs în anexele nr. 2-30, 54, art. 27 alin. (1) în anexele nr. 31-38].

Sintetizând situaţiile de fapt descrise de considerentele recursului în interesul legii şi de anexele cuprinzând jurisprudenţa, raportul constată că sunt avute în vedere mai multe ipoteze, respectiv: montarea la bancomat a dispozitivelor de citire a benzii magnetice a cardului autentic şi 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 şi 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 şi a codului PIN aferent acestuia (minivideocamere sau dispozitive tip tastatură) urmată de utilizarea bancomatului de către victimă şi transmiterea datelor de pe card şi de utilizare a datelor de către persoana acuzată.

Raportul a analizat fiecare dintre ipotezele de fapt descrise în jurisprudenţa anexată, fără a se pronunţa exclusiv asupra existenţei sau absenţei accesului la un sistem informatic, deoarece chiar soluţia propusă de procurorul general (secţiunea 3.1 din prezenta decizie) face referire la montarea dispozitivelor de citire a cardurilor la bancomat, precum şi la retrageri de numerar prin folosirea unui card falsificat sau prin folosirea cardului fără consimţământul titularului său.

În ceea ce priveşte referirea în considerentele opiniei procurorului general la faptul că instanţele de judecată nu au pus în discuţie schimbarea încadrării juridice şi au condamnat persoanele acuzate pe baza faptelor din rechizitorii, pronunţând astfel soluţii divergente cu privire la semnificaţia dată faptelor cu care au fost învestite (secţiunea 2.1.2 din prezenta decizie), raportul arată că schimbarea încadrării juridice de către instanţa de fond este limitată de obiectul judecăţii, astfel că nu se pot reţine fapte noi care nu au făcut obiectul acuzaţiei (vezi Completul de 9 judecători, Decizia nr. 74 din 8 octombrie 2001), iar schimbarea încadrării juridice de către instanţele de control este, în plus, limitată de principiul neagravării situaţiei în propria cale de atac (art. 372, art. 385^8 din Codul de procedură penală). În consecinţă, chiar pentru soluţiile pronunţate după publicarea deciziei în interesul legii, principiile anterioare limitează posibilitatea schimbării încadrării juridice pentru faptele care au făcut deja obiectul învestirii instanţelor.

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

- scopul urmărit prin montarea dispozitivelor;
- modul în care dispozitivele de citire a benzii magnetice a cardului autentic şi a codului PIN aferent interacţionează cu sistemul informatic al băncii;
- modul în care cardul interacţionează cu sistemul băncii şi consecinţele 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 şi 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 distincţia dintre legea generală, Legea nr. 161/2003 şi legea specială, Legea nr. 365/2002. Rezolvarea problemei de drept determinată de ipoteza menţionată anterior are în vedere opinia Departamentului de drept penal al Facultăţii de Drept a Universităţii din Bucureşti (secţiunea 4.4.3 din prezenta decizie) şi opinia Departamentului de drept public al Universităţii "Babeş-Bolyai" (secţiunea 4.3.3 din prezenta decizie), cu privire la distincţia dintre art. 25 din Legea nr. 365/2002 şi art. 46 alin. (2) din Legea nr. 161/2003, opiniile trimise de Institutul de Cercetări Juridice al Academiei Române (secţiunea 4.2.1 din prezenta decizie), Catedra de drept penal din cadrul Facultăţii de Drept şi Ştiinţe Administrative a Universităţii din Craiova (secţiunea 4.5.2 din prezenta decizie), Departamentul de drept public din cadrul Facultăţii de Drept a Universităţii de Vest din Timişoara (secţiunea 4.7.2 din prezenta decizie), cu privire la încadrarea juridică, precum şi punctul de vedere trimis de Universitatea "Lucian Blaga" din Sibiu (secţiunea 4.6.1 din prezenta decizie) cu privire la administrarea probelor pentru clarificarea scopului deţinerii echipamentelor.

În ambele ipoteze reglementate de Legea nr. 161/2003 şi Legea nr. 365/2002, legiuitorul a incriminat actele de pregătire: deţinerea, fără drept, a unui dispozitiv, program informatic, parolă, cod de acces sau dată informatică în scopul săvârşirii uneia dintre infracţiunile contra confidenţialităţii şi integrităţii datelor şi sistemelor informatice [art. 46 alin (2) din Legea nr. 161/2003], respectiv fabricarea ori deţinerea 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 (deţinerea de instrumente în vederea falsificării de valori), apreciind că şi în materia infracţiunilor informatice actele de pregătire au un pericol social generic semnificativ, astfel că trebuie asimilate faptului consumat şi incluse în ilicitul penal. Includerea actelor de pregătire în ilicitul penal este consecinţa scopului pentru care acestea s-au produs: săvârşirea uneia dintre infracţiunile contra confidenţialităţii şi integrităţii datelor şi sistemelor informatice, respectiv falsificarea instrumentelor de plată electronică. Dovedirea scopului deţinerii echipamentelor este în consecinţă de esenţa reţinerii vinovăţiei persoanei acuzate şi stabilirii încadrării juridice corecte.

Elementul material comun celor două infracţiuni, respectiv deţinerea de echipamente, inclusiv hardware sau software, face necesară analiza criteriilor de diferenţiere a faptelor. Încadrarea juridică dată faptelor de deţinere 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 urmăreşte scopul prevăzut de art. 42-45 din Legea nr. 161/2003 sunt întrunite elementele constitutive ale infracţiunii prevăzute de art. 46 alin. (2) din Legea nr. 161/2003;

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

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

Deşi montarea dispozitivelor de citire a benzii magnetice a cardului autentic şi a codului PIN aferent este infracţiune independent de realizarea transferului neautorizat de date, odată ce transferul datelor operează, ia naştere un concurs de infracţiuni între deţinerea dispozitivelor şi utilizarea lor. Scopul în care datele urmează să fie folosite ulterior face însă şi diferenţa între infracţiunea prevăzută de art. 46 alin. (2) din Legea nr. 161/2003 şi art. 25 din Legea nr. 365/2002. Montarea dispozitivelor de citire a benzii magnetice a cardului autentic şi a codului PIN aferent la bancomat probează scopul săvârşirii unor infracţiuni 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 săvârşirii infracţiunii 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 sancţionează infracţiuni îndreptate contra confidenţialităţii şi integrităţii datelor şi sistemelor informatice, în timp ce Legea nr. 365/2002 privind comerţul electronic incriminează infracţiuni îndreptate împotriva securităţii şi integrităţii instrumentelor de plată electronice. Spre deosebire de infracţiunile 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 conţinute pe banda magnetică a cardului bancar autentic sunt absolut necesare atât pentru efectuarea unor operaţiuni financiare în mod fraudulos, cât şi pentru falsificarea unui card bancar. În

consecinţă este incident art. 46 alin. (2) din Legea nr. 161/2003 atunci când dispozitivele de citire a benzii magnetice a cardului autentic şi a codului PIN aferent au fost deţinute în scopul săvârşirii uneia dintre infracţiunile 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 şi a codului PIN aferent au fost deţinute în scopul de a servi la falsificarea instrumentelor de plată electronică.

Obţinerea datelor de pe card, prin dispozitivele de citire a benzii magnetice a cardului autentic şi a codului PIN aferent, chiar dacă nu este suficientă prin ea însăşi pentru falsificarea instrumentelor de plată, deoarece ulterior datele trebuie să fie inscripţionate pe un alt mediu de stocare, realizează elementul material al infracţiunii prevăzute de art. 25 din Legea nr. 365/2002. Legea nr. 365/2002 cere ca echipamentele să fie deţinute cu scopul de a servi la falsificarea instrumentelor de plată electronică. Legea nu incriminează fapta doar dacă sunt deţinute 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 parţial la un sistem informatic în scopul săvârşirii uneia dintre infracţiunile prevăzute la art. 42-45, fapta va constitui infracţiunea 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 şi 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.

Rezolvarea problemei de drept determinată de ipoteza menţionată 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 (secţiunea 4.1.1. din prezenta decizie), opinia Departamentului de drept penal a Facultăţii de Drept a Universităţii din Bucureşti (secţiunea 4.4.1. din prezenta decizie).

De asemenea, conform art. 2 din Regulamentul Băncii Naţionale a României nr. 6/2006 privind emiterea şi utilizarea instrumentelor de plată electronică şi relaţiile dintre participanţii la tranzacţiile cu aceste instrumente, publicat în Monitorul Oficial al României, Partea I, nr. 927 din 15 noiembrie 2006, se prevede că în înţelesul regulamentului, termenii şi expresiile de mai jos au următoarele semnificaţii:

"1. Cardul emis de o instituţie de credit este un instrument de plată electronică, respectiv un suport de informaţie standardizat, securizat şi individualizat, care permite deţinătorului său să folosească disponibilităţile băneşti proprii dintr-un cont deschis pe numele său la emitentul cardului şi/sau să utilizeze o linie de credit, în limita unui plafon stabilit în prealabil, deschisă de emitent în favoarea deţinătorului cardului, în vederea efectuării uneia sau mai multora dintre următoarele operaţiuni:

a) retragerea sau depunerea de numerar de la terminale precum distribuitoarele de numerar şi/sau ATM, de la ghişeele emitentului/instituţiei acceptante sau de la sediul unei instituţii, obligată prin contract să accepte instrumentul de plată electronică, respectiv încărcarea şi descărcarea unităţilor valorice în cazul monedei electronice;

b) plata bunurilor achiziţionate şi/sau serviciilor prestate de comercianţii acceptanţi şi/sau emitenţi (de exemplu, plata serviciilor prestate de companii în domeniul telefoniei mobile, fixe, transmisii de date, servicii de televiziune şi internet sau de către alţi furnizori de utilităţi), precum şi plata obligaţiilor către autorităţile administraţiei publice, reprezentând impozite, taxe, amenzi, penalităţi etc., prin intermediul imprinterelor, terminalelor POS, ATM sau prin alte medii electronice."

În consecinţă prin montarea dispozitivelor tip skimmer peste fanta de introducere a cardului la un echipament cu interfaţă de card bancar se realizează, dacă victima foloseşte 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 şi a codului PIN aferent, de către persoana acuzată, pentru a copia informaţiile de pe banda magnetică a cardului bancar, reprezintă infracţiunea 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 şi a codului PIN aferent acestuia (minivideocamere sau dispozitive tip tastatură) urmată de utilizarea bancomatului de către victimă şi transmiterea datelor de pe card şi de utilizare a datelor de către persoana acuzată

Rezolvarea problemei de drept determinată de ipoteza menţionată anterior are în vedere opinia Institutului de Cercetări Juridice al Academiei Române (secţiunea 4.2.2. din prezenta decizie), Departamentului de drept penal a Facultăţii de Drept a Universităţii din Bucureşti (secţiunea 4.4.3. din prezenta decizie), Departamentului de drept public al Universităţii "Babeş-Bolyai" (secţiunea 4.3.2 şi 4.3.3 din prezenta decizie), Catedrei de drept penal din cadrul Facultăţii de Drept şi Ştiinţe Administrative a Universităţii din Craiova (secţiunea 4.5.2 din prezenta decizie), Universităţii Lucian Blaga din Sibiu (secţiunea 4.6.3 din prezenta decizie), Departamentului de drept public din cadrul Facultăţii de Drept a Universităţii de Vest din Timişoara (secţiunea 4.7.2 din prezenta decizie).

În acest caz probele administrate trebuie să clarifice dacă intenţia aceluia care captează datele de pe card este de a clona instrumentul de plată electronică sau dacă intenţia sa este de a utiliza datele obţinute de pe banda magnetică în vederea efectuării unor plăţi 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 parţial la un sistem informatic în scopul săvârşirii uneia dintre infracţiunile prevăzute la art. 42-45, sunt întrunite elementele constitutive ale infracţiunii prevăzute de art. 46 alin. (1) lit. (b) din Legea nr. 161/2003. Introducerea unui card bancar falsificat sau a unuia autentic, fără consimţământul titularului său, la un echipament dotat cu interfaţă de card bancar, realizează accesul, fără drept, la sistemul informatic al băncii, în scopul obţinerii de date informatice şi cu încălcarea măsurilor de securitate introduse de bancă, indiferent de tipul operaţiunii efectuate: interogare, autentificare, retrageri de numerar, transferuri sau orice alte operaţiuni financiare. În cazul folosirii datelor de identificare ale cardurilor bancare pentru efectuarea unor tranzacţii 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 existenţă autonomă şi captează informaţiile de pe card înainte ca acestea

să ajungă în sistemul băncii, accesul la sistemul informatic al băncii nu există, chiar dacă se captează informaţiile de pe card. Accesul la un sistem informatic reprezintă o interacţiune logică între dispozitivul montat şi sistemul informatic. Interacţiunea logică apare atunci când prin intermediul dispozitivului se beneficiază de resursele ori/şi funcţiile sistemului informatic. Doar în acest caz, prin interacţiunea fizică cu sistemul informatic (pornirea acestuia, transmiterea unor comenzi prin utilizarea tastaturii etc.) se creează şi o interacţiune la nivel logic. Interacţiunea cu tastatura (apăsarea tastelor) iniţiază o interacţiune logică doar dacă sistemul informatic vizat ajunge să recepţioneze informaţia transmisă prin intermediul tastaturii, să o interpreteze cu ajutorul unui program informatic şi 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 şi 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 interfaţă 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 şi este destinată sistemului informatic al băncii, şi anume codul PIN, un cod de securitate introdus de bancă pentru restricţionarea accesului utilizatorilor neautorizaţi la sistemul informatic al băncii.

În ceea ce priveşte sistemul informatic al băncii, chiar şi în situaţia amplasării unei tastaturi false deasupra tastaturii originale de la ATM sau POS, doar tastatura originală face parte din sistemul informatic bancar şi 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 şi să acceseze astfel, fără drept, sistemul informatic al băncii în scopul obţinerii de date informatice. O interacţiune logică poate avea la bază şi o interacţiune fizică, dar o interacţiune fizică nu implică în mod necesar şi o interacţiune logică.

În cazul utilizării la bancomat a dispozitivelor de citire a benzii magnetice a cardului autentic şi 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 conţine informaţii 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 protecţie se realizează inclusiv prin mijloace de drept penal.

Transferul neautorizat de date are loc fără ca dispozitivul de citire să interacţioneze cu sistemul informatic al băncii. Odată ce cardul a fost introdus în bancomat şi codul tastat, datele de pe cardul introdus în bancomat şi codul PIN pot fi transferate chiar dacă respectivul bancomat nu este funcţional 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 menţionată anterior are în vedere opinia Institutului de Cercetări Juridice al Academiei Române (secţiunea 4.2.2 din prezenta decizie), Departamentului de drept penal al Facultăţii de Drept a Universităţii din Bucureşti (secţiunea 4.4.4 din prezenta decizie), Departamentului de drept public al Universităţii "Babeş-Bolyai" (secţiunea 4.3.4 din prezenta decizie), Catedrei de drept penal din cadrul Facultăţii de Drept şi Ştiinţe Administrative a Universităţii din Craiova (secţiunea 4.5.3 din prezenta decizie), Universităţii "Lucian Blaga" din Sibiu (secţiunea 4.6.3 din prezenta decizie), Departamentului de drept public din cadrul Facultăţii de Drept a Universităţii de Vest din Timişoara (secţiunea 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, întruneşte elementele constitutive ale infracţiunii de efectuare de operaţiuni 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, săvârşită în concurs cu infracţiunea de acces, fără drept, la un sistem informatic comisă în scopul obţinerii de date informatice prin încălcarea măsurilor de securitate - art. 42 alin. (1), (2) şi (3) din Legea nr. 161/2003.

Folosirea cardului inscripţionat cu datele culese de pe cardul autentic, oricare ar fi fost modul de obţinere a acestora, ori folosirea cardului autentic, fără acordul titularului său, la ATM reprezintă acces fără drept la un sistem informatic, în scopul obţinerii de date informatice, prin încălcarea măsurilor de securitate, faptă incriminată de art. 42 alin. (1), (2) şi (3) din Legea nr. 161/2003. Bancomatul face parte din sistemul informatic bancar, datele transmise şi receptate fiind protejate prin măsuri de securitate încorporate în sistemul de citire a cardurilor şi în codul PIN.

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

- în cazul cardului real, prin introducerea cardului şi tastarea codului PIN care înlătură măsura de securitate reprezentată de codul de acces;
- în cazul cardului falsificat, prin recunoaşterea cardului ca fiind un card valid şi prin schimbul de informaţii între posesorul cardului şi mediul de stocare a datelor privitoare la contul bancar ataşat cardului.

Infracţiunea de acces fără drept la un sistem informatic este consumată prin folosirea codului PIN, chiar dacă nu se solicită nicio operaţiune 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 iniţiat prin folosirea codului PIN se menţine pe durata tranzacţiei şi 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 menţionată anterior are în vedere opinia Departamentului de drept penal al Facultăţii de Drept a Universităţii din Bucureşti (secţiunea 4.4.4 din prezenta decizie), Departamentului de drept public al Universităţii "Babeş-Bolyai" (secţiunea 4.3.4 din prezenta decizie), Catedrei de drept penal din cadrul Facultăţii de Drept şi Ştiinţe Administrative a Universităţii din Craiova (secţiunea 4.5.3 din prezenta decizie), Universităţii "Lucian Blaga" din Sibiu (secţiunea 4.6.3 din prezenta decizie), Departamentului de drept public din cadrul Facultăţii de Drept a Universităţii de Vest din Timişoara (secţiunea 4.7.3 din prezenta decizie).

Folosirea unui card bancar falsificat, la bancomat, pentru retrageri de numerar întruneşte elementele constitutive ale infracţiunii prevăzute de art. 27 alin. (1) din Legea nr. 365/2002, în concurs cu infracţiunea de acces, fără drept, la un sistem informatic comisă în scopul obţinerii de date informatice prin încălcarea măsurilor de securitate - art. 42 alin. (1), (2) şi (3) din Legea nr. 161/2003 şi în concurs cu infracţiunea 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 obţinerii

de date informatice şi cu încălcarea măsurilor de securitate introduse de bancă, indiferent de tipul operaţiunii efectuate. În raport cu tipul operaţiunii efectuate prin intermediul cardului falsificat (interogare, autentificare, retrageri de numerar, transferuri plăţi on-line sau orice alte operaţiuni financiare) se realizează elementul material al laturii obiective din conţinutul altor infracţiuni. Astfel, de exemplu, folosirea unui card bancar falsificat, la bancomat, pentru retrageri de numerar constituie infracţiunea prevăzută de art. 27 alin. (1) din Legea nr. 365/2002, în concurs cu infracţiunea de acces, fără drept, la un sistem informatic comisă în scopul obţinerii de date informatice prin încălcarea măsurilor de securitate - art. 42 alin. (1), (2) şi (3) din Legea nr. 161/2003 şi în concurs cu infracţiunea de falsificare a instrumentelor de plată electronică - art. 24 alin. (2) din Legea nr. 365/2002.

O faptă care întruneşte elementele constitutive ale infracţiunii prevăzute în art. 24 alin. (2) din Legea nr. 365/2002, în modalitatea punerii în circulaţie a instrumentelor de plată electronică falsificate, nu întruneşte, întotdeauna, şi elementele constitutive ale infracţiunii prevăzute în art. 27 alin. (1) din Legea nr. 365/2002. Nici situaţia contrară nu este întotdeauna posibilă. Astfel, infracţiunea prevăzută în art. 24 alin. (2) din Legea nr. 365/2002, în modalitatea punerii în circulaţie 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 priveşte distincţia dintre alineatele art. 27 din Legea nr. 365/2002, raportul arată că Secţia penală a adoptat anterior şi a transmis instanţelor de judecată punctul de vedere conform căruia alin. (1) nu precizează că efectuarea operaţiunii financiare se realizează numai prin utilizarea instrumentului de plată electronică original, fără consimţământul titularului instrumentului respectiv, ci, dimpotrivă, include în sfera de aplicare a normei de incriminare efectuarea de operaţiuni financiare prin utilizarea datelor de identificare ce permit folosirea instrumentului de plată electronică, fără consimţământul titularului instrumentului respectiv. În concluzie, conform practicii Secţiei penale a Înaltei Curţi de Casaţie şi Justiţie, art. 27 alin. (1) din Legea nr. 365/2002 incriminează atât efectuarea de operaţiuni financiare prin utilizarea instrumentului de plată electronică original, fără consimţământul titularului instrumentului respectiv, cât şi efectuarea de operaţiuni financiare prin utilizarea unui instrument de plată electronică falsificat care permite folosirea datelor de identificare ale instrumentului de plată electronică original, fără consimţământul titularului instrumentului respectiv.

Soluţia propusă în secţiunea de faţă decurge şi din Decizia nr. 5.288 din 15 septembrie 2006 a Secţiei penale a Înaltei Curţi de Casaţie şi Justiţie prin care a fost soluţionată problema de drept privind existenţa concursului între infracţiunea prevăzută în art. 24 alin. (1) din Legea nr. 365/2002 şi infracţiunea prevăzută în art. 24 alin. (2) din aceeaşi lege. Decizia menţionată prevede că punerea în circulaţie 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 circulaţie a instrumentelor tip card nu este strict legată de transmiterea materială a acestora, fiind în acord cu modul în care Banca Naţională a României (BNR) a clasificat tranzacţiile efectuate prin card. Astfel, Regulamentul BNR nr. 6 din 11 octombrie 2006, privind emiterea şi utilizarea instrumentelor de plată electronică şi relaţiile dintre participanţii la tranzacţiile cu aceste instrumente prevede că, în raport cu prezenţa fizică a cardului, tranzacţiile prin card pot fi clasificate astfel: (i) tranzacţii unde cardul este prezent - locaţii comerciale tradiţionale, ATM şi ghişee de bancă - reprezintă acele tranzacţii unde banda magnetică a cardului sau cipul cardului este citită/citit electronic sau unde se obţine amprenta elementelor confecţionate în relief a cardului pe chitanţă cu ajutorul imprinterului mecanic; (ii) tranzacţii unde cardul nu este prezent reprezintă tranzacţiile ordonate prin telefon, poştă, internet, unde nu există dovada participării fizice a cardului, însă deţinătorul trebuie să furnizeze parole sau coduri, de exemplu, Card Verification Value (CVV2), parola ecommerce etc.

Infracţiunea prevăzută în art. 27 alin. (1) din Legea nr. 365/2002, în modalitatea efectuării unei operaţiuni financiare prin utilizarea datelor de identificare ce permit folosirea unui instrument de plată electronică, fără consimţământul titularului instrumentului respectiv, nu presupune, în mod obligatoriu, falsificarea instrumentului de plată electronică original. Infracţiunea 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 consimţământul titularului său.

Faptul că fiecare dintre infracţiunile prevăzute în art. 24 alin. (2) şi în art. 27 alin. (1) din Legea nr. 365/2002 poate fi săvârşită prin acţiuni distincte nu exclude însă posibilitatea ca printr-o singură acţiune, săvârşită în anumite împrejurări, să fie întrunite atât elementele constitutive ale infracţiunii prevăzute în art. 24 alin. (2) din Legea nr. 365/2002, cât şi elementele constitutive ale infracţiunii prevăzute în art. 27 alin. (1) din aceeaşi 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 iniţiat prin folosirea codului PIN se menţine pe durata tranzacţiei şi se epuizează abia prin retragerea de numerar.

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

Rezolvarea problemei de drept determinate de ipoteza menţionată anterior are în vedere opinia Departamentului de drept penal al Facultăţii de Drept a Universităţii din Bucureşti (secţiunea 4.4.3 din prezenta decizie) şi opinia Departamentului de drept public al Universităţii "Babeş-Bolyai" (secţiunile 4.3.2 şi 4.3.3. din prezenta decizie).

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

Soluţiile preconizate în ipotezele de mai sus au în vedere faptul că montarea la bancomat a dispozitivelor de citire a benzii magnetice a cardului autentic şi a codului PIN aferent presupune, în cazul dispozitivelor autonome, doar captarea datelor (conţinute pe card) pentru care dispozitivele au fost create, nu şi accesul la sistemul informatic al băncii. Scopul transferării datelor constituie un element esenţial al infracţiunii şi face diferenţa între actele preparatorii incriminate de Legea nr. 161/2003 şi 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 iniţiat prin folosirea codului PIN se menţine pe durata tranzacţiei şi se epuizează prin retragerea de numerar, astfel că infracţiunile care iau naştere ca urmare a folosirii codului PIN şi retragerii de numerar sunt în concurs ideal.

6. Înalta Curte de Casaţie şi Justiţie

6.1. Obiectul recursului în interesul legii

Pentru soluţionarea 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, deşi obiectul sesizării,

astfel cum este precizat la pagina 1 din opinia procurorului general, este limitat la corecta interpretare a dispoziţiilor art. 42 alin. (1), (2) şi (3) din Legea nr. 161/2003, în cuprinsul acestora se face referire la mai multe texte de lege care ar avea incidenţă în situaţiile de fapt reţinute de instanţe, respectiv dispoziţiile art. 25, art. 24 alin. (1) şi (2), art. 27 alin. (1) din Legea nr. 365/2002, ultimele două texte de lege fiind incluse şi în soluţia propusă de procurorul general în argumentele finale.

În raport cu aceste referiri, precum şi cu multiplele situaţii care rezultă din raportul întocmit la dosar şi 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 şi în raport cu cele din finalul sesizării, în care se face referire la mai multe texte de lege.

Pentru aceste motive, cu respectarea dispoziţiilor art. 414^4 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 şi 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 instanţă prin încheierea din 16 septembrie 2013, procurorul general al Parchetului de pe lângă Înalta Curte de Casaţie şi Justiţie a înaintat concluzii privind obiectul sesizării, menţionând că problema de drept a cărei dezlegare o solicită se referă la stabilirea modului unitar de interpretare şi aplicare a dispoziţiilor art. 42 alin (1), (2) şi (3) din Legea nr. 161/2003, în ceea ce priveşte înţelesul sintagmei acces fără drept la un sistem informatic. S-a mai precizat că nu formează obiect al sesizării prin prezentul recurs în interesul legii situaţiile de fapt descrise la pct. 7 lit. b, c, d şi g din Raportul întocmit de judecătorul-raportor (secţiunea 5.3 din prezenta decizie) prin care se propune şi proiectul de minută.

Completul competent să judece recursul în interesul legii, învestit în limitele precizate de procurorul general al Parchetului de pe lângă Înalta Curte de Casaţie şi Justiţie în concluziile scrise, susţinute oral, a reţinut dosarul în pronunţare asupra recursului în interesul legii, stabilind următoarele:

6.2. Montarea la bancomat a dispozitivelor autonome de citire a benzii magnetice a cardului autentic şi a codului PIN aferent acestuia (skimmere, minivideocamere sau dispozitive tip tastatură falsă) constituie infracţiunea 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 şi 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 deţinerea 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) şi în două variante agravante, în alin. (2) şi (3): accesul, fără drept, la un sistem informatic, săvârşit în scopul obţinerii 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 şi a videocamerei ori a dispozitivului modificat de tip tastatură nu se realizează accesul fără drept la sistemul informatic al băncii, deoarece lipseşte interacţiunea făptuitorului cu tehnica de calcul. Obţinerea datelor de pe banda magnetică a cardului autentic se realizează în exteriorul bancomatului şi fără ca dispozitivele menţionate 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, permiţând doar copierea codurilor înscrise pe cardul care asigură accesarea sistemului informatic.

Operaţiunile prin care sunt citite datele de pe banda magnetică a cardului, concomitent cu captarea codului PIN aferent lui, reprezintă doar acte pregătitoare ale infracţiunii de acces fără drept la un sistem informatic. Citirea datelor de pe banda magnetică a cardului nu este condiţionată de ataşarea dispozitivului electronic de citire la bancomat; aceeaşi activitate de captare a datelor de pe banda magnetică ar primi consecinţe juridice diferite din cauza unei împrejurări extranee vreunei norme de incriminare - ataşarea sau nu a skimmerului la bancomat. Citirea datelor de pe banda magnetică a cardului, prin ataşarea skimmerului la bancomat, nu interacţionează cu softul bancomatului, nu se realizează o solicitare către unitatea centrală de prelucrare a sistemului, care să proceseze date ori să ruleze programe de aplicaţii în beneficiul făptuitorului, astfel că infracţiunea de acces fără drept la sistemul informatic ar fi lipsită de însuşi elementul său material.

Conform legii, art. 46 alin. (2) din Legea nr. 161/2003, este incriminată deţinerea, 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 săvârşirii uneia dintre infracţiunile prevăzute la art. 42-45 din aceeaşi lege.

Deţinerea dispozitivelor de citire a benzii magnetice a cardului, minivideocamerelor sau dispozitivelor tip tastatură şi, implicit, montarea acestora pentru citirea benzii magnetice a cardului concomitent cu captarea codului PIN aferent cardului constituie acte pregătitoare în vederea săvârşirii infracţiunii 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 aceeaşi lege.

6.3. Folosirea la bancomat a unui card bancar autentic, fără acordul titularului său, în scopul efectuării unor retrageri de numerar, constituie infracţiunea de efectuare de operaţiuni 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 infracţiunea de acces, fără drept, la un sistem informatic comisă în scopul obţinerii de date informatice prin încălcarea măsurilor de securitate, prevăzută de art. 42 alin. (1), (2) şi (3) din Legea nr. 161/2003.

6.3.1. Dispoziţii legale privind falsificarea instrumentelor de plată electronică şi efectuarea de operaţiuni financiare în mod fraudulos cuprinse în Legea nr. 365/2002 privind comerţul electronic

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

Art. 24 din Legea nr. 365/2002

Falsificarea instrumentelor de plată electronică

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

(2) Cu aceeaşi pedeapsă se sancţionează punerea în circulaţie, în orice mod, a instrumentelor de plată electronică falsificate sau deţinerea lor în vederea punerii în circulaţie.

[...]

Art. 27 alin. (1) din Legea nr. 365/2002
Efectuarea de operaţiuni financiare în mod fraudulos
(1) Efectuarea uneia dintre operaţiunile prevăzute la art. 1 pct. 11, prin utilizarea unui instrument de plată electronică, inclusiv a datelor de identificare care permit utilizarea acestuia, fără consimţământul titularului instrumentului respectiv, se pedepseşte cu închisoare de la 1 la 12 ani.
Operaţiunile prevăzute la art. 1 pct. 11 din Legea nr. 365/2002 sunt: a) transferuri de fonduri, altele decât cele ordonate şi executate de către instituţii financiare; b) retrageri de numerar, precum şi încărcarea şi descărcarea unui instrument de monedă electronică.
6.3.2. Decizia-cadru a Consiliului Uniunii Europene din 28 mai 2001 de combatere a fraudei şi a falsificării mijloacelor de plată, altele decât numerarul (2001/413/JAI)
Decizia este transpusă în dreptul intern şi prin prevederile Legii nr. 365/2002, iar în art. 2 (Infracţiuni în legătură cu instrumentele de plată) se menţionează că fiecare stat membru ia măsurile necesare pentru a garanta că următoarele comportamente constituie infracţiune atunci când sunt săvârşite cu intenţie, cel puţin în ceea ce priveşte cărţile de credit, cardurile de tip eurocec, alte carduri emise de instituţii financiare, cecurile de călătorie, eurocecurile, alte cecuri şi cambii: (a) furtul sau o altă însuşire ilegală a unui instrument de plată; (b) contrafacerea sau falsificarea unui instrument de plată în scopul utilizării frauduloase a acestuia; (c) primirea, obţinerea, transportul, vânzarea sau transferul către o altă persoană sau posedarea unui instrument de plată furat sau însuşit 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 însuşit ilegal ori a unui instrument de plată contrafăcut sau falsificat.
6.3.3. Efectuarea de operaţiuni financiare în mod fraudulos
Dispoziţiile art. 27 alin. (1) din Legea nr. 365/2002 incriminează efectuarea uneia dintre operaţiunile prevăzute la art. 1 pct. 11 din aceeaşi lege, operaţiuni care includ retragerile de numerar, prin utilizarea unui instrument de plată electronică, inclusiv a datelor de identificare care permit utilizarea acestuia, fără consimţământul titularului instrumentului respectiv.
Art. 27 alin. (1) din Legea nr. 365/2002 nu precizează că efectuarea operaţiunii financiare se realizează numai prin utilizarea instrumentului de plată electronică original, fără consimţământul titularului instrumentului respectiv, ci, dimpotrivă, include în sfera de aplicare a normei de incriminare efectuarea de operaţiuni financiare prin utilizarea datelor de identificare care permit folosirea instrumentului de plată electronică, fără consimţământul 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, obţinute în mod fraudulos, pe un alt suport, rezultând un instrument de plată electronică falsificat.
În consecinţă, art. 27 alin. (1) din Legea nr. 365/2002 incriminează atât efectuarea de operaţiuni financiare prin utilizarea instrumentului de plată electronică original, fără consimţământul titularului instrumentului respectiv, cât şi efectuarea de operaţiuni financiare prin utilizarea unui instrument de plată electronică falsificat care permite folosirea datelor de identificare ale instrumentului de plată electronică original, fără consimţământul titularului instrumentului respectiv.
Aşadar, art. 27 alin. (1) din Legea nr. 365/2002 constituie atât temeiul legal pentru sancţionarea făptuitorului care retrage numerar prin utilizarea instrumentului de plată electronică original, fără consimţământul titularului instrumentului respectiv, cât şi temeiul legal pentru pedepsirea făptuitorului care retrage 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 retrage numerar prin utilizarea instrumentului de plată electronică original înseamnă a conferi impunitate făptuitorului care retrage numerar prin utilizarea unui instrument de plată electronică falsificat, pe care sunt imprimate datele de identificare ale instrumentului de plată electronică original, deşi 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 şi ipoteza utilizării datelor de identificare, stabilind, în art. 250 alin. (1), efectuarea de operaţiuni financiare în mod fraudulos, că: efectuarea unei operaţiuni de retragere de numerar, încărcare sau descărcare a unui instrument de monedă electronică ori de transfer de fonduri, prin utilizarea, fără consimţământul titularului, a unui instrument de plată electronică sau a datelor de identificare care permit utilizarea acestuia, se pedepseşte 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 însuşit ilegal (instrument de plată original), cât şi 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 operaţiunilor financiare efectuate în mod fraudulos, incriminează "acceptarea uneia dintre operaţiunile prevăzute la art. 1 pct. 11, cunoscând că este efectuată prin folosirea unui instrument de plată electronică falsificat sau utilizat fără consimţământul titularului său". Or, este dificil de admis că legiuitorul a incriminat acceptarea unei operaţiuni financiare atât în cazul în care este efectuată prin folosirea unui instrument de plată electronică falsificat, cât şi în cazul în care este efectuată prin folosirea instrumentului de plată electronică original utilizat fără consimţământul titularului său, dar a incriminat numai efectuarea unei operaţiuni financiare prin utilizarea instrumentului de plată electronică original fără consimţământul titularului său, iar nu şi efectuarea unei operaţiuni 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 obţinerii de date informatice, prin încălcarea măsurilor de securitate, fapta incriminată de art. 42 alin. (1), (2) şi (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 iniţiat prin folosirea codului PIN se epuizează prin retragerea de numerar, ia naştere un concurs ideal cu infracţiunea prevăzută de art. 27 alin. (1) din Legea nr. 365/2002. Astfel dacă ulterior accesului fără drept la un sistem informatic, în scopul obţinerii de date informatice, prin încălcarea măsurilor de securitate, se vor efectua şi operaţiuni financiare (retrageri de sume, plăţi, transferuri etc.), infracţiunea de acces neautorizat va veni în concurs cu infracţiunea prevăzută de art. 27 alin. (1) din Legea nr. 356/2002, constând în efectuarea de operaţiuni financiare în mod fraudulos, infracţiuni 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 ameninţată. Legătura de cauzalitate dintre acţiunea făptuitorului şi urmarea produsă datelor informatice rezultă din însăşi materialitatea faptei.

6.4. Folosirea la bancomat a unui card bancar falsificat, pentru retrageri de numerar, constituie infracţiunea de efectuare de operaţiuni 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 infracţiunea de acces, fără drept, la un sistem informatic comisă în scopul obţinerii de date informatice prin încălcarea măsurilor de securitate, prevăzută de art. 42 alin. (1), (2) şi (3) din Legea nr. 161/2003, şi cu infracţiunea de falsificare a instrumentelor de plată electronică, prevăzută de art. 24 alin. (2) din Legea nr. 365/2002.

Punerea în circulaţie a instrumentelor de plată electronică falsificate şi efectuarea de operaţiuni financiare în mod fraudulos

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

În accepţiunea 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 circulaţie a unui instrument de plată electronică falsificat. Soluţia decurge din Decizia nr. 5.288 din 15 septembrie 2006 a Secţiei penale a Înaltei Curţi de Casaţie şi Justiţie, conform căreia punerea în circulaţie 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. Soluţia decurge şi din funcţiile 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 şi utilizarea instrumentelor de plată electronică şi relaţiile dintre participanţii la tranzacţiile cu aceste instrumente. În raport cu prezenţa fizică a cardului, tranzacţiile prin card pot fi clasificate astfel: (i) tranzacţii unde cardul este prezent - locaţii comerciale tradiţionale, ATM şi ghişee de bancă - reprezintă acele tranzacţii unde banda magnetică a cardului sau cipul cardului este citită/citit electronic sau unde se obţine amprenta elementelor confecţionate în relief a cardului pe chitanţă cu ajutorul imprinterului mecanic; (ii) tranzacţii unde cardul nu este prezent reprezintă tranzacţiile ordonate prin telefon, poştă, internet, unde nu există dovada participării fizice a cardului, însă deţinătorul 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 infracţiunii prevăzute în art. 24 alin. (2) din Legea nr. 365/2002, cât şi elementele constitutive ale infracţiunii prevăzute în art. 27 alin. (1) din Legea nr. 365/2002, aflate în concurs ideal de infracţiuni, 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 iniţiat prin folosirea codului PIN se epuizează prin retragerea de numerar.

Astfel, acţiunea 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 infracţiunii prevăzute în art. 24 alin. (2) din Legea nr. 365/2002, întrucât acţiunea de a retrage numerar prin utilizarea unui instrument de plată electronică falsificat reprezintă o punere în circulaţie, în orice mod, a unui instrument de plată electronică falsificat;
- realizează elementele constitutive ale infracţiunii prevăzute în art. 27 alin. (1) din Legea nr. 365/2002, întrucât acţiunea 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 operaţiunii 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 consimţământul titularului instrumentului respectiv.

În acest context, se impune precizarea că o faptă care întruneşte elementele constitutive ale infracţiunii prevăzute în art. 24 alin. (2) din Legea nr. 365/2002, în modalitatea punerii în circulaţie a instrumentelor de plată electronică falsificate, nu întruneşte, întotdeauna, şi elementele constitutive ale infracţiunii prevăzute în art. 27 alin. (1) din Legea nr. 365/2002 şi, invers, o faptă care întruneşte elementele constitutive ale infracţiunii prevăzute în art. 27 alin. (1) din Legea nr. 365/2002 nu întruneşte, întotdeauna, şi elementele constitutive ale infracţiunii prevăzute în art. 24 alin. (2) din Legea nr. 365/2002, în modalitatea punerii în circulaţie a instrumentelor de plată electronică falsificate. Infracţiunea prevăzută în art. 24 alin. (2) din Legea nr. 365/2002, în modalitatea punerii în circulaţie 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.

Infracţiunea prevăzută în art. 27 alin. (1) din Legea nr. 365/2002, în modalitatea efectuării unei operaţiuni financiare prin utilizarea datelor de identificare care permit folosirea unui instrument de plată electronică, fără consimţământul 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 consimţământul titularului său.

Faptul că fiecare dintre infracţiunile prevăzute în art. 24 alin. (2) şi în art. 27 alin. (1) din Legea nr. 365/2002 poate fi săvârşită prin acţiuni distincte nu exclude însă posibilitatea ca printr-o singură acţiune, săvârşită în anumite împrejurări, să fie întrunite atât elementele constitutive ale infracţiunii prevăzute în art. 24 alin. (2) din Legea nr. 365/2002, cât şi elementele constitutive ale infracţiunii prevăzute în art. 27 alin. (1) din aceeaşi 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 inscripţionat cu datele culese de pe cardul autentic, oricare ar fi fost modul de obţinere a acestora, se accesează de asemenea fără drept un sistem informatic, în scopul obţinerii de date informatice, prin încălcarea măsurilor de securitate, faptă incriminată de art. 42 alin. (1), (2) şi (3) din Legea nr. 161/2003.

Pentru considerentele arătate, în temeiul art. 414^4 şi 414^5 din Codul de procedură penală, astfel cum a fost modificat şi completat prin Legea nr. 202/2010,

ÎNALTA CURTE DE CASAŢIE ŞI JUSTIŢIE

În numele legii

DECIDE:

Admite recursul în interesul legii formulat de procurorul general al Parchetului de pe lângă Înalta Curte de Casaţie şi Justiţie şi, în consecinţă, stabileşte că:

1. Montarea la bancomat a dispozitivelor autonome de citire a benzii magnetice a cardului autentic şi a codului PIN aferent acestuia (skimmere, minivideocamere sau dispozitive tip tastatură falsă) constituie infracţiunea 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 infracţiunea de efectuare de operaţiuni 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 infracţiunea de acces, fără drept, la un sistem informatic comisă în scopul obţinerii de date informatice prin încălcarea măsurilor de securitate, prevăzută de art. 42 alin. (1), (2) şi (3) din Legea nr. 161/2003.

3. Folosirea la bancomat a unui card bancar falsificat, pentru retrageri de numerar, constituie infracţiunea de efectuare de operaţiuni 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 infracţiunea de acces, fără drept, la un sistem informatic comisă în scopul obţinerii de date informatice prin încălcarea măsurilor de securitate, prevăzută de art. 42 alin. (1), (2) şi (3) din Legea nr. 161/2003, şi cu infracţiunea de falsificare a instrumentelor de plată electronică, prevăzută de art. 24 alin. (2) din Legea nr. 365/2002.

Obligatorie, potrivit art. 414^5 alin. 4 din Codul de procedură penală.

Pronunţată, în şedinţă publică, astăzi, 14 octombrie 2013.

-****-

PREŞEDINTELE ÎNALTEI CURŢI DE CASAŢIE ŞI JUSTIŢIE
LIVIA DOINA STANCIU
Magistrat-asistent
Monica Eugenia Ungureanu

Publicat în Monitorul Oficial cu numărul 760 din data de 6 decembrie 2013