Legea 161 din 19/04/2003 privind unele masuri pentru asigurarea transparentei în exercitarea demnitatilor publice, a functiilor publice si in mediul de afaceri, prevenirea si sanctionarea coruptiei

Publicat in Monitorul Oficial, Partea I nr. 279 din 21/04/2003

TITLUL III
Prevenirea şi combaterea criminalităţii informatice

CAPITOLUL I
Dispozitii generale

Art. 34. - Prezentul titlu reglementează prevenirea si combaterea criminalitãtii informatice, prin mãsuri specifice de prevenire, descoperire si sanctionare a infractiunilor sãvârsite prin intermediul sistemelor informatice, asigurându-se respectarea drepturilor omului si protectia datelor personale.
Art. 35. - (1) În prezentul titlu, termenii si expresiile de mai jos au urmãtorul înteles:
a) prin sistem informatic se întelege orice dispozitiv sau ansamblu de dispozitive interconectate sau aflate în relatie functionalã, dintre care unul sau mai multe asigurã prelucrarea automatã a datelor, cu ajutorul unui program informatic;
b) prin prelucrare automatã a datelor se întelege procesul prin care datele dintr-un sistem informatic sunt prelucrate prin intermediul unui program informatic;
c) prin program informatic se întelege un ansamblu de instructiuni care pot fi executate de un sistem informatic în vederea obtinerii unui rezultat determinat;
d) prin date informatice se întelege orice reprezentare a unor fapte, informatii sau concepte într-o formã care poate fi prelucratã printr-un sistem informatic. În aceastã categorie se include si orice program informatic care poate determina realizarea unei functii de cãtre un sistem informatic;
e) prin furnizor de servicii se întelege:
1. orice persoanã fizicã sau juridicã ce oferã utilizatorilor posibilitatea de a comunica prin intermediul sistemelor informatice;
2. orice altã persoanã fizicã sau juridicã ce prelucreazã sau stocheazã date informatice pentru persoanele prevãzute la pct. 1 si pentru utilizatorii serviciilor oferite de acestea;
f) prin date referitoare la traficul informational se întelege orice date informatice referitoare la o comunicare realizatã printr-un sistem informatic si produse de acesta, care reprezintã o parte din lantul de comunicare, indicând originea, destinatia, ruta, ora, data, mãrimea, volumul si durata comunicãrii, precum si tipul serviciului utilizat pentru comunicare;
g) prin date referitoare la utilizatori se întelege orice informatie care poate conduce la identificarea unui utilizator, incluzând tipul de comunicatie si serviciul folosit, adresa postalã, adresa geograficã, numere de telefon sau alte numere de acces si modalitatea de platã a serviciului respectiv, precum si orice alte date care pot conduce la identificarea utilizatorului;
h) prin mãsuri de securitate se întelege folosirea unor proceduri, dispozitive sau programe informatice specializate cu ajutorul cãrora accesul la un sistem informatic este restrictionat sau interzis pentru anumite categorii de utilizatori;
i) prin materiale pornografice cu minori se întelege orice material care prezintã un minor având un comportament sexual explicit sau o persoanã majorã care este prezentatã ca un minor având un comportament sexual explicit ori imagini care, desi nu prezintã o persoanã realã, simuleazã, în mod credibil, un minor având un comportament sexual explicit.
(2) În sensul prezentului titlu, actioneazã fãrã drept persoana care se aflã în una dintre urmãtoarele situatii:
a) nu este autorizatã, în temeiul legii sau al unui contract;
b) depãseste limitele autorizãrii;
c) nu are permisiunea, din partea persoanei fizice sau juridice competente, potrivit legii, sã o acorde, de a folosi, administra sau controla un sistem informatic ori de a desfãsura cercetãri stiintifice sau de a efectua orice altã operatiune într-un sistem informatic.

CAPITOLUL II
Prevenirea criminalitãtii informatice

Art. 36. - Pentru asigurarea securitãtii sistemelor informatice si a protectiei datelor personale, autoritãtile si institutiile publice cu competente în domeniu, furnizorii de servicii, organizatiile neguvernamentale si alti reprezentanti ai societãtii civile desfãsoarã activitãti comune si programe de prevenire a criminalitãtii informatice.
Art. 37. - Autoritãtile si institutiile publice cu competente în domeniu, în cooperare cu furnizorii de servicii, organizatiile neguvernamentale si alti reprezentanti ai societãtii civile promoveazã politici, practici, mãsuri, proceduri si standarde minime de securitate a sistemelor informatice.
Art. 38. - Autoritãtile si institutiile publice cu competente în domeniu, în cooperare cu furnizorii de servicii, organizatiile neguvernamentale si alti reprezentanti ai societãtii civile organizeazã campanii de informare privind criminalitatea informaticã si riscurile la care sunt expusi utilizatorii de sisteme informatice.
Art. 39. - (1) Ministerul Justitiei, Ministerul de Interne, Ministerul Comunicatiilor si Tehnologiei Informatiei, Serviciul Român de Informatii si Serviciul de Informatii Externe constituie si actualizeazã continuu baze de date privind criminalitatea informaticã.
(2) Institutul National de Criminologie din subordinea Ministerului Justitiei efectueazã studii periodice în scopul identificãrii cauzelor care determinã si a conditiilor ce favorizeazã criminalitatea informaticã.
Art. 40. - Ministerul Justitiei, Ministerul de Interne, Ministerul Comunicatiilor si Tehnologiei Informatiei, Serviciul Român de Informatii si Serviciul de Informatii Externe desfãsoarã programe speciale de pregãtire si perfectionare a personalului cu atributii în prevenirea si combaterea criminalitãtii informatice.
Art. 41. - Proprietarii sau administratorii de sisteme informatice la care accesul este interzis sau restrictionat pentru anumite categorii de utilizatori au obligatia de a avertiza utilizatorii cu privire la conditiile legale de acces si utilizare, precum si cu privire la consecintele juridice ale accesului fãrã drept la aceste sisteme informatice. Avertizarea trebuie sã fie accesibilã oricãrui utilizator.

CAPITOLUL III
Infractiuni si contraventii

SECTIUNEA 1
Infractiuni contra confidentialitãtii si integritãtii datelor si sistemelor informatice

Art. 42. - (1) Accesul, fãrã drept, la un sistem informatic constituie infractiune si se pedepseste cu închisoare de la 3 luni la 3 ani sau cu amendã.
(2) Fapta prevãzutã la alin. (1), sãvârsitã în scopul obtinerii de date informatice, se pedepseste cu închisoare de la 6 luni la 5 ani.
(3) Dacã fapta prevãzutã la alin. (1) sau (2) este sãvârsitã prin încãlcarea mãsurilor de securitate, pedeapsa este închisoarea de la 3 la 12 ani.
Art. 43. - (1) Interceptarea, fãrã drept, a unei transmisii de date informatice care nu este publicã si care este destinatã unui sistem informatic, provine dintr-un asemenea sistem sau se efectueazã în cadrul unui sistem informatic constituie infractiune si se pedepseste cu închisoare de la 2 la 7 ani.
(2) Cu aceeasi pedeapsã se sanctioneazã si interceptarea, fãrã drept, a unei emisii electromagnetice provenite dintr-un sistem informatic ce contine date informatice care nu sunt publice.
Art. 44. - (1) Fapta de a modifica, sterge sau deteriora date informatice ori de a restrictiona accesul la aceste date, fãrã drept, constituie infractiune si de pedepseste cu închisoare de la 2 la 7 ani.
(2) Transferul neautorizat de date dintr-un sistem informatic se pedepseste cu închisoare de la 3 la 12 ani.
(3) Cu pedeapsa prevãzutã la alin. (2) se sanctioneazã si transferul neautorizat de date dintr-un mijloc de stocare a datelor informatice.
Art. 45. - Fapta de a perturba grav, fãrã drept, functionarea unui sistem informatic, prin introducerea, transmiterea, modificarea, stergerea sau deteriorarea datelor informatice sau prin restrictionarea accesului la aceste date constituie infractiune si se pedepseste cu închisoare de la 3 la 15 ani.
Art. 46. - (1) Constituie infractiune si se pedepseste cu închisoare de la 1 la 6 ani:

a) fapta de a produce, vinde, de a importa, distribui sau de a pune la dispozitie, sub orice altã formã, fãrã drept, a unui dispozitiv sau program informatic conceput sau adaptat în scopul sãvârsirii uneia dintre infractiunile prevãzute la art. 42-45;
b) fapta de a produce, vinde, de a importa, distribui sau de a pune la dispozitie, sub orice altã formã, fãrã drept, a unei parole, cod de acces sau alte asemenea date informatice care permit accesul total sau partial la un sistem informatic în scopul sãvârsirii uneia dintre infractiunile prevãzute la art. 42-45.
(2) Cu aceeasi pedeapsã se sanctioneazã si detinerea, fãrã drept, a unui dispozitiv, program informatic, parolã, cod de acces sau datã informaticã dintre cele prevãzute la alin. (1) în scopul sãvârsirii uneia dintre infractiunile prevãzute la art. 42-45.
Art. 47. - Tentativa infractiunilor prevãzute la art. 42-46 se pedepseste.

SECTIUNEA a 2-a
Infractiuni informatice

Art. 48. - Fapta de a introduce, modifica sau sterge, fãrã drept, date informatice ori de a restrictiona, fãrã drept, accesul la aceste date, rezultând date necorespunzãtoare adevãrului, în scopul de a fi utilizate în vederea producerii unei consecinte juridice, constituie infractiune si se pedepseste cu închisoare de la 2 la 7 ani.
Art. 49. - Fapta de a cauza un prejudiciu patrimonial unei persoane prin introducerea, modificarea sau stergerea de date informatice, prin restrictionarea accesului la aceste date ori prin împiedicarea în orice mod a functionãrii unui sistem informatic, în scopul de a obtine un beneficiu material pentru sine sau pentru altul, constituie infractiune si se pedepseste cu închisoare de la 3 la 12 ani.
Art. 50. - Tentativa infractiunilor prevãzute la art. 48 si 49 se pedepseste.

SECTIUNEA a 3-a
Pornografia infantilã prin sisteme informatice

Art. 51. - (1) Constituie infractiune si se pedepseste cu închisoare de la 3 la 12 ani si interzicerea unor drepturi producerea în vederea rãspândirii, oferirea sau punerea la dispozitie, rãspândirea sau transmiterea, procurarea pentru sine sau pentru altul de materiale pornografice cu minori prin sisteme informatice ori detinerea, fãrã drept, de materiale pornografice cu minori într-un sistem informatic sau un mijloc de stocare a datelor informatice.
(2) Tentativa se pedepseste.

SECTIUNEA a 4-a
Contraventii

Art. 52. - Nerespectarea obligatiei prevãzute la art. 41 constituie contraventie si se sanctioneazã cu amendã de la 5.000.000 lei la 50.000.000 lei.
Art. 53. - (1) Constatarea contraventiei prevãzute la art. 52 si aplicarea sanctiunii se fac de cãtre personalul împuternicit în acest scop de cãtre ministrul comunicatiilor si tehnologiei informatiei, precum si de cãtre personalul special abilitat din cadrul Ministerului de Interne.
(2) Contraventiei prevãzute la art. 52 îi sunt aplicabile dispozitiile Ordonantei Guvernului nr. 2/2001 privind regimul juridic al contraventiilor, aprobatã cu modificãri si completãri prin Legea nr. 180/2002, cu modificãrile ulterioare.

CAPITOLUL IV
Dispozitii procedurale

Art. 54. - (1) În cazuri urgente si temeinic justificate, dacã existã date sau indicii temeinice cu privire la pregãtirea sau sãvârsirea unei infractiuni prin intermediul sistemelor informatice, în scopul strângerii de probe sau al identificãrii fãptuitorilor, se poate dispune conservarea imediatã a datelor informatice ori a datelor referitoare la traficul informational, fatã de care existã pericolul distrugerii ori alterãrii.
(2) În cursul urmãririi penale conservarea se dispune de procuror, prin ordonantã motivatã, la cererea organului de cercetare penalã sau din oficiu, iar în cursul judecãtii, de instantã prin încheiere.
(3) Mãsura prevãzutã la alin. (1) se dispune pe o duratã ce nu poate depãsi 90 de zile si poate fi prelungitã, o singurã datã, cu o perioadã ce nu poate depãsi 30 de zile.
(4) Ordonanta procurorului sau încheierea instantei se transmite, de îndatã, oricãrui furnizor de servicii sau oricãrei persoane în posesia cãreia se aflã datele prevãzute la alin. (1), aceasta fiind obligatã sã le conserve imediat, în conditii de confidentialitate.
(5) În cazul în care datele referitoare la traficul informational se aflã în posesia mai multor furnizori de servicii, furnizorul de servicii prevãzut la alin.(4) are obligatia de a pune, de îndatã, la dispozitia organului de urmãrire penalã sau a instantei informatiile necesare identificãrii celorlalti furnizori de servicii, în vederea cunoasterii tuturor elementelor din lantul de comunicare folosit.
(6) Pânã la terminarea urmãririi penale, procurorul este obligat sã încunostinteze, în scris, persoanele fatã de care se efectueazã urmãrirea penalã si ale cãror date au fost conservate.
Art. 55. - (1) În termenul prevãzut la art. 54 alin. (3) procurorul, pe baza autorizatiei motivate a procurorului anume desemnat de procurorul general al parchetului de pe lângã curtea de apel sau, dupã caz, de procurorul general al Parchetului de pe lângã Curtea Supremã de Justitie, ori instanta de judecatã dispune cu privire la ridicarea obiectelor care contin date informatice, date referitoare la traficul informational sau date referitoare la utilizatori, de la persoana sau furnizorul de servicii care le detine, în vederea efectuãrii de copii, care pot servi ca mijloc de probã.
(2) Dacã obiectele care contin datele informatice sau datele referitoare la traficul informational nu sunt puse de bunãvoie la dispozitia organelor judiciare pentru efectuarea de copii, procurorul prevãzut la alin. (1) sau instanta de judecatã dispune ridicarea silitã. În cursul judecãtii, dispozitia de ridicare silitã se comunicã procurorului, care ia mãsuri de aducere la îndeplinire, prin organul de cercetare penalã.
(3) Copiile prevãzute la alin. (1) se realizeazã cu mijloace tehnice si proceduri adecvate de naturã sã asigure integritatea informatiilor continute de acestea.
Art. 56. - (1) Ori de câte ori pentru descoperirea si strângerea probelor este necesarã cercetarea unui sistem informatic sau a unui suport de stocare a datelor informatice, organul competent prevãzut de lege poate dispune efectuarea unei perchezitii.
(2) Dacã organul de urmãrire penalã sau instanta de judecatã apreciazã cã ridicarea obiectelor care contin datele prevãzute la alin. (1) ar afecta grav desfãsurarea activitãtii persoanelor care detin aceste obiecte, poate dispune efectuarea de copii, care pot servi ca mijloc de probã si care se realizeazã potrivit art. 55 alin. (3).
(3) În cazul în care, cu ocazia cercetãrii unui sistem informatic sau a unui suport de stocare a datelor informatice, se constatã cã datele informatice cãutate sunt cuprinse într-un alt sistem informatic sau suport de stocare a datelor informatice si sunt accesibile din sistemul sau suportul initial, se poate dispune, de îndatã, autorizarea efectuãrii perchezitiei în vederea cercetãrii tuturor sistemelor informatice sau suporturilor de stocare a datelor informatice cãutate.
(4) Dispozitiile din Codul de procedurã penalã referitoare la efectuarea perchezitiei domiciliare se aplicã în mod corespunzãtor.
Art. 57. - (1) Accesul într-un sistem informatic, precum si interceptarea si înregistrarea comunicãrilor desfãsurate prin intermediul sistemelor informatice se efectueazã când sunt utile pentru aflarea adevãrului, iar stabilirea situatiei de fapt sau identificarea fãptuitorilor nu poate fi realizatã în baza altor probe.
(2) Mãsurile prevãzute la alin. (1) se realizeazã cu autorizarea motivatã a procurorului anume desemnat de procurorul general al parchetului de pe lângã curtea de apel sau, dupã caz, de procurorul general al Parchetului de pe lângã Curtea Supremã de Justitie ori de procurorul general al Parchetului National Anticoruptie, de cãtre organele de cercetare penalã, cu sprijinul unor persoane specializate, care sunt obligate sã pãstreze secretul operatiunii efectuate.

(3) Autorizatia prevãzutã la alin. (2) se dã pentru cel mult 30 de zile, cu posibilitatea prelungirii în aceleasi conditii, pentru motive temeinic justificate, fiecare prelungire neputând depãsi 30 de zile. Durata maximã a mãsurii autorizate nu poate depãsi 4 luni.
(4) Pânã la terminarea urmãririi penale, procurorul este obligat sã încunostinteze în scris persoanele fatã de care s-au dispus mãsurile prevãzute la alin. (1).
(5) Dispozitiile Codului de procedurã penalã referitoare la înregistrãrile audio sau video se aplicã în mod corespunzãtor.
Art. 58. - Dispozitiile prezentului capitol se aplicã în urmãrirea penalã sau judecarea cauzelor privind infractiunile prevãzute în prezentul titlu si a oricãror alte infractiuni sãvârsite prin intermediul sistemelor informatice.
Art. 59. - În cazul infractiunilor prevãzute în prezentul titlu si al oricãror alte infractiuni sãvârsite prin intermediul sistemelor informatice, pentru a garanta aducerea la îndeplinire a confiscãrii speciale prevãzute la art. 118 din Codul penal se pot lua mãsurile asigurãtorii prevãzute de Codul de procedurã penalã.

CAPITOLUL V
Cooperare internationalã

Art. 60. - (1) Autoritãtile judiciare române cooperează în mod direct, în conditiile legii si cu respectarea obligatiilor decurgând din instrumentele juridice internationale la care România este parte, cu institutiile având atributii similare din alte state, precum si cu organizatiile internationale specializate în domeniu.
(2) Cooperarea, care se organizează si se desfãsoarã potrivit alin. (1), poate avea ca obiect, dupã caz, asistenta judiciarã internationalã în materie penalã, extrãdarea, identificarea, blocarea, sechestrarea si confiscarea produselor si instrumentelor infractiunii, desfãsurarea anchetelor comune, schimbul de informatii, asistenta tehnicã sau de altã naturã pentru culegerea si analiza informatiilor, formarea personalului de specialitate, precum si alte asemenea activitãti.
Art. 61. - (1) La solicitarea autoritãtilor competente române sau ale altor state, pe teritoriul României se pot desfãsura anchete comune, în vederea prevenirii si combaterii criminalitãtii informatice.
(2) Anchetele comune prevãzute la alin. (1) se desfãsoarã în baza acordurilor bilaterale sau multilaterale încheiate de autoritãtile competente.
(3) Reprezentantii autoritãtilor competente române pot participa la anchete comune desfãsurate pe teritorii ale altor state, cu respectarea legislatiilor acestora.
Art. 62. - (1) Pentru asigurarea cooperãrii internationale imediate si permanente în domeniul combaterii criminalitãtii informatice se înfiinteazã, în cadrul Sectiei de Combatere a Criminalitãtii Organizate si Antidrog din Parchetul de pe lângã Curtea Supremã de Justitie, Serviciul de combatere a criminalitãtii informatice, ca punct de contact disponibil permanent.
(2) Serviciul de combatere a criminalitãtii informatice are urmãtoarele atributii:
a) acordã asistentã de specialitate si oferã date despre legislatia românã în materie punctelor de contact similare din alte state;
b) dispune conservarea imediatã a datelor, precum si ridicarea obiectelor care contin datele informatice sau datele referitoare la traficul informational solicitate de o autoritate strãinã competentã;
c) executã sau facilitează executarea, potrivit legii, a comisiilor rogatorii solicitate în cauze privind combaterea criminalitãtii informatice, cooperând cu toate autoritãtile române competente.
Art. 63. - (1) În cadrul cooperãrii internationale, autoritãtile strãine competente pot solicita Serviciului de combatere a criminalitãtii informatice conservarea imediatã a datelor informatice ori a datelor referitoare la traficul informational, existente într-un sistem informatic de pe teritoriul României, cu privire la care autoritatea strãinã urmează sã formuleze o cerere de asistentã judiciarã internationalã în materie penalã.
(2) Cererea de conservare imediatã prevãzutã la alin. (1) cuprinde urmãtoarele:
a) autoritatea care solicitã conservarea;
b) o scurtã prezentare a faptelor care fac obiectul urmãririi penale si încadrarea juridicã a acestora;
c) datele informatice care se solicitã a fi conservate;
d) orice informatie disponibilã, necesarã pentru identificarea detinãtorului de date informatice si a localizãrii sistemului informatic;
e) utilitatea datelor informatice si necesitatea conservãrii lor;

f) intentia autoritãtii strãine de a formula o cerere de asistentã judiciarã internationalã în materie penalã.
(3) Cererea de conservare se executã potrivit art. 54 pentru o perioadã care nu poate fi mai micã de 60 de zile si este valabilã pânã la luarea unei decizii de cãtre autoritãtile române competente cu privire la cererea de asistentã judiciarã internationalã în materie penalã.
Art. 64. - Dacã în executarea cererii formulate potrivit art. 63 alin. (1) se constatã cã un furnizor de servicii al altui stat este în posesia unor date referitoare la traficul informational, Serviciul de combatere a criminalitãtii informatice va informa de îndatã despre aceasta autoritatea strãinã solicitantã, comunicând totodatã informatiile necesare identificãrii respectivului furnizor de servicii.
Art. 65. - (1) O autoritate strãinã competentã poate avea acces la sursele publice române de date informatice publice, fãrã a fi necesarã formularea unei solicitãri în acest sens cãtre autoritãtile române.
(2) O autoritate strãinã competentã poate avea acces sau poate primi, prin intermediul unui sistem informatic existent pe teritoriul sãu, date informatice stocate în România, dacã are aprobarea persoanei autorizate, potrivit legii, sã le punã la dispozitie prin intermediul acelui sistem informatic, fãrã a fi necesarã formularea unei solicitãri în acest sens cãtre autoritãtile române.
Art. 66. - Autoritãtile române competente pot transmite, din oficiu, autoritãtilor strãine competente, cu respectarea prevederilor legale privind protectia datelor cu caracter personal, informatiile si datele detinute, necesare pentru descoperirea infractiunilor sãvârsite prin intermediul sistemelor informatice sau pentru solutionarea de cãtre autoritãtile strãine competente a cauzelor referitoare la aceste infractiuni.
Art. 67. -Art. 29 din Legea nr. 365/2002 privind comertul electronic, publicatã în Monitorul Oficial al României, Partea I, nr. 483 din 5 iulie 2002, se abrogã.