

## DREPT PUBLIC

CZU: 343.7:004.056

[https://doi.org/10.52277/1857-2405.2023.1\(64\).01](https://doi.org/10.52277/1857-2405.2023.1(64).01)

## CARACTERUL ILEGAL AL ACCESULUI LA INFORMAȚIA COMPUTERIZATĂ: CONDIȚIE DE APLICARE A ART. 259 DIN CODUL PENAL AL REPUBLICII MOLDOVA



**Alexandru STRÎMBEANU,**  
doctorand, USM  
<https://orcid.org/0000-0002-7746-6541>

### SUMAR

Accesul la informația computerizată are un caracter ilegal, dacă este realizat fie în lipsa autorizării în temeiul legii sau al unui contract, fie cu depășirea limitelor autorizării, fie fără permisiunea persoanei competente să folosească, să administreze sau să controleze un sistem informatic ori să desfășoare cercetări științifice sau să efectueze orice altă operațiune într-un sistem informatic. Pentru ca accesul la informația computerizată să fie considerat legal, este necesară prezența nu doar a unor scopuri legitime, ci și a tuturor celorlalte condiții care asigură respectarea legalității.

**Cuvinte-cheie:** acces, informație computerizată, sistem informatic, caracter ilegal, lipsă de autorizare, lipsa permisiunii.

După cum rezultă din dispoziția alin. (1) art. 259 CP, nu orice acces la informația computerizată intră sub incidența acestui articol. Condiția obligatorie este ca accesul la informația computerizată să aibă un caracter ilegal.

Termenul „illegal”, utilizat în art. 259 CP, în raport cu acțiunea de acces la informația computerizată, își găsește concretizarea în sintagma „al unei persoane care nu este autorizată în temeiul legii sau al unui contract, depășește limitele autorizării ori nu are permisiunea persoanei competente să folosească, să administreze sau să controleze un sistem informatic ori să desfășoare cercetări științifice sau să efectueze orice altă operațiune într-un sistem informatic”, folosită în dispoziția alin. (1) art. 259 CP. Din această sintagmă rezultă că accesul la informația computerizată este ilegal, dacă se realizează:

- 1) în lipsa autorizării în temeiul legii sau al unui contract;

### ILLEGAL CHARACTER OF ACCESS TO COMPUTERIZED INFORMATION: CONDITION FOR APPLICATION OF ART. 259 OF THE CRIMINAL CODE OF THE REPUBLIC OF MOLDOVA

#### SUMMARY

Access to computerized information is illegal, if it is carried out either without authorization by law or contract, or exceeding the limits of authorization, or without the permission from a competent person to use, administer, or control a data system or to conduct scientific research or to perform any other operation in a data system. In order for access to computerized information to be considered legal, the presence of not only legitimate purposes, but also all other conditions that ensure compliance with legality is necessary.

**Key-words:** access, computerized information, computer system, illegal character, lack of authorization, lack of permission.

- 2) cu depășirea limitelor autorizării;
- 3) fără permisiunea persoanei competente să folosească, să administreze sau să controleze un sistem informatic ori să desfășoare cercetări științifice sau să efectueze orice altă operațiune într-un sistem informatic.

Ca paradigmă pentru sintagma sus-menționată din alin. (1) art. 259 CP a servit formularea din alin. (2) art. 35 al Legii României nr. 161 din 19.04.2003 privind unele măsuri pentru asigurarea transparenței în exercitarea demnităților publice, a funcțiilor publice și în mediul de afaceri, prevenirea și sancționarea corupției (în continuare – Legea României nr. 161/2003): „În sensul prezentului titlu (se are în vedere Titlul III „Prevenirea și combaterea criminalității informatice” – *n.a.*), acționează fără drept persoana care se află în una dintre următoarele situații: a) nu este autorizată, în temeiul legii sau al unui contract; b) depășește limitele autorizării; c) nu are permisiunea, din partea persoanei fizice sau juridice

competente, potrivit legii, să o acorde, de a folosi, administra sau controla un sistem informatic ori de a desfășura cercetări științifice sau de a efectua orice altă operațiune într-un sistem informatic” [10]. Până la intrarea în vigoare la 01.02.2014 a Legii României nr. 187 din 24.10.2012 pentru punerea în aplicare a Legii nr. 286/2009 privind Codul penal [11], art. 42 al Legii României nr. 161/2003 (care a fost abrogat) avea următorul conținut: „Accesul, fără drept, la un sistem informatic constituie infracțiune și se pedepsește cu închisoare de la 3 luni la 3 ani sau cu amendă. (2) Fapta prevăzută la alin. (1), săvârșită în scopul obținerii de date informatice, se pedepsește cu închisoare de la 6 luni la 5 ani. (3) Dacă fapta prevăzută la alin. (1) sau (2) este săvârșită prin încălcarea măsurilor de securitate, pedeapsa este închisoarea de la 3 la 12 ani” [10].

În continuare, vor fi analizate cele trei ipoteze de ilegalitate, specificate în alin. (1) art. 259 CP RM.

Anumite indicii în ceea ce privește *prima dintre aceste ipoteze* – lipsa autorizării de a accesa informația computerizată – găsim în opinia exprimată de către L. Gîrla și Iu. Tabarcea: „Accesul va fi neautorizat atunci când subiectul nu are un temei legal pentru utilizarea resurselor informatice sau pentru deținerea acestora, precum și în cazurile în care o persoană, deși accesează informația computerizată legal, o face fără a respecta procedura stabilită de proprietarul informației sau de lege” [12, p. 16]. La aceeași ipoteză se referă M. Dobrinou: „În momentul în care un utilizator (funcționar) are stabilite anumite sarcini de serviciu, iar pentru îndeplinirea acestora este necesară accesarea conținuturilor create pentru interacțiunea cu informațiile înregistrate în respectivele baze de date, se admite *per se* că persoanele respective sunt autorizate legal să utilizeze respectivul mijloc de muncă. *Per a contrario*, din punct de vedere tehnic și procedural, lipsa autorizării poate fi înțeleasă drept situația în care utilizatorul i-au fost anulate credențialele de acces ori, după caz, acestuia i-au fost modificate anumite drepturi de prelucrare de date informatice sau, procedural, acestuia i-au fost interzise, prin dispoziție scrisă sau verbală, toate sau doar anumite operațiuni (logice) asupra datelor informatice respective” [5].

Așadar, lipsa autorizării de a accesa informația computerizată presupune lipsa împuternicirii de a o accesa, pe care o acordă proprietarul informației computerizate sau un alt posesor al acestei informații. Pentru aplicarea art. 259 CP, nu are importanță dacă autorizarea, care-i lipsește făptuitorului, are ca sursă o lege sau un contract. De asemenea, nu contează dacă:

- 1) făptuitorul nu a avut în genere autorizarea de a accesa informația computerizată;
- 2) făptuitorul a avut în trecut autorizarea de a accesa informația computerizată, însă, în momentul săvârșirii infracțiunii, nu o mai

avea, întrucât fie termenul autorizării expirase, fie autorizarea a fost suspendată ori revocată;

- 3) făptuitorului urma să-i fie acordată autorizarea de a accesa informația computerizată, însă, în momentul săvârșirii infracțiunii, acesta încă nu o avea, întrucât termenul autorizării nu începuse să curgă.

Astfel de circumstanțe pot fi luate în calcul, eventual, doar la individualizarea pedepsei.

La cea de-a doua ipoteză a ilegalității – depășirea limitelor autorizării de a accesa informația computerizată – se referă următoarea explicație din Decizia Înaltei Curți de Casație și Justiție a României nr. 68 din 29.09.2021 privind dispozițiile art. 360 alin. (1) din Codul penal: „Analiza depășirii limitelor autorizării implică, pe de o parte, stabilirea existenței autorizării legale sau contractuale, iar, pe de altă parte, determinarea conținutului acesteia, singurul în măsură să furnizeze criteriile obiective în raport cu care se poate concluziona asupra caracterului legal sau ilegal al accesului la sistemul informatic. În acest sens, în cadrul examenului realizat, organul judiciar verifică, în temeiul actelor normative care reglementează competențele și atribuțiile de serviciu într-un anumit domeniu de activitate, al regulamentelor de ordin intern sau al clauzelor specifice din contractele de muncă și al prevederilor din fișele postului, limitele autorizării, dar și conduita materială efectivă a agentului pe durata accesului la sistemul informatic, toate acestea constituind aspecte de natură strict factuală, ce diferă de la caz la caz, în funcție de particularitățile speței deduse judecării, și care urmează a fi stabilite de instanța investită pe baza materialului probator administrat în cauză, care va fundamenta concluzia depășirii sau a nedeptării respectivelor limite și, implicit, a caracterului legal ori ilegal al accesului” [4].

Așadar, depășirea limitelor autorizării de a accesa informația computerizată presupune că făptuitorul deține autorizarea de a accesa informația computerizată, însă acesta nu se conformează autorizării respective, arogându-și împuterniciri care nu i-au fost acordate. Analiza unor prevederi relevante dintr-un act normativ ne permite să înțelegem care pot fi împrejurările în care se depășesc limitele autorizării de a accesa informația computerizată. Depășind limitele autorizării de a accesa informația computerizată, făptuitorul își arogă împuterniciri de a accesa: un volum mai mare de informație decât cel autorizat pentru statutul pe care-l deține; informație calitativ diferită de cea autorizată pentru statutul pe care-l deține. Astfel de circumstanțe nu influențează asupra calificării faptei în baza art. 259 CP, însă pot fi luate în calcul la individualizarea pedepsei.

Ultima, a treia ipoteză a ilegalității presupune realizarea accesului la informația computerizată fără permisiunea persoanei competente să folo-



sească, să administreze sau să controleze un sistem informatic ori să desfășoare cercetări științifice sau să efectueze orice altă operațiune într-un sistem informatic.

Această ipoteză implică îndeplinirea următoarelor două condiții:

- 1) făptuitorul nu are permisiunea de a accesa informația computerizată;
- 2) o asemenea permisiune o acordă persoana competentă să folosească, să administreze sau să controleze un sistem informatic ori să desfășoare cercetări științifice, sau să efectueze orice altă operațiune într-un sistem informatic.

Cât privește prima dintre aceste condiții, nu are importanță dacă permisiunea de a accesa informația computerizată (pe care ar fi trebuit să o aibă făptuitorul, însă nu o are) are un caracter verbal sau scris. De asemenea, nu este relevant dacă:

- a) făptuitorul a solicitat permisiunea de a accesa informația computerizată, după care a ignorat refuzul de a da curs unei asemenea solicitări;
- b) făptuitorul nu a solicitat permisiunea de a accesa informația computerizată.

La fel, nu contează dacă:

- a) făptuitorul nu a avut în genere permisiunea de a accesa informația computerizată;
- b) făptuitorul a avut în trecut permisiunea de a accesa informația computerizată, însă, în momentul săvârșirii infracțiunii, nu o mai avea, întrucât fie termenul permisiunii expirase, fie permisiunea a fost suspendată ori revocată;
- c) făptuitorului urma să-i fie acordată permisiunea de a accesa informația computerizată, însă, în momentul săvârșirii infracțiunii, acesta încă nu o avea, întrucât termenul permisiunii nu începuse să curgă.

Astfel de circumstanțe pot fi luate în calcul, eventual, doar la individualizarea pedepsei.

Referitor la cea de-a doua condiție, la calificarea faptei urmează să fie stabilită, în baza prevederilor actelor normative, competența persoanei care a permis accesul făptuitorului la informația computerizată. Dacă o astfel de persoană nu are calitatea de victimă a infracțiunii și nu are competența de a permite accesul făptuitorului la informația computerizată, atunci, în baza art. 259 CP, va răspunde:

- a) doar ea – în cazul în care a acționat cu intenție, în timp ce persoana care a obținut permisiunea lovită de nulitate a acționat fără vinovăție sau din imprudență. În acest caz, persoana care a permis accesul făptuitorului la informația computerizată va răspunde ca autor al infracțiunii;
- b) atât ea, cât și persoana care a obținut permisiunea lovită de nulitate – în cazul în care ambele aceste persoane au acționat cu in-

tenție. În acest caz, persoana care a permis accesul făptuitorului la informația computerizată va răspunde ca instigator sau organizator al infracțiunii. Bineînțeles, persoana care a obținut permisiunea lovită de nulitate va răspunde ca autor al infracțiunii.

Până aici am analizat ilegalitatea accesului la informația computerizată, privită drept condiție de aplicare a art. 259 CP. În cele ce urmează vom examina contrateza – legalitatea accesului la informația computerizată – privită drept condiție de neaplicare a art. 259 CP.

Interpretarea *per a contrario* a sintagmei „al unei persoane care nu este autorizată în temeiul legii sau al unui contract, depășește limitele autorizării ori nu are permisiunea persoanei competente să folosească, să administreze sau să controleze un sistem informatic ori să desfășoare cercetări științifice, sau să efectueze orice altă operațiune într-un sistem informatic”, utilizată în dispoziția din alin. (1) art. 259 CP, ne determină să afirmăm că persoana care realizează accesul la informația computerizată nu este pasibilă de răspundere în baza acestui articol în oricare din următoarele cazuri:

- 1) este autorizată în temeiul legii sau al unui contract;
- 2) nu depășește limitele autorizării;
- 3) are permisiunea, din partea persoanei fizice sau juridice competente, potrivit legii, să acorde, de a folosi, administra sau controla un sistem informatic ori de a desfășura cercetări științifice, sau de a efectua orice altă operațiune într-un sistem informatic.

Fiind pe poziții apropiate, S. Brînza și V. Stati dezvăluie conținutul noțiunii „acces legal la informația computerizată”: „De exemplu, nu poate avea un caracter ilegal accesul care a fost autorizat de către proprietarul sau alt posesor al sistemului informatic vizat. [...] La fel, nu poate fi considerată infracțiune nici interacționarea cu un sistem informatic care permite accesul liber și gratuit al publicului (de exemplu, rețelele Wi-Fi neprotejate sau care oferă servicii de comunicații electronice „la liber” [1, p. 351]. L. Gîrla și Iu. Tabarcea prezintă exemple din aceeași categorie: „Accesul se consideră autorizat în următoarele cazuri: 1) accesul a fost autorizat de către proprietarul sau posesorul resurselor informaționale sau al sistemelor informatice, al tehnologiilor și mijloacelor de asigurare a acestora în vederea verificării sau protejării sistemelor informatice; 2) accesul la resursele informaționale ale sistemelor informatice publice și private este realizat de către organele statului abilitate de lege în vederea asigurării securității naționale, în cursul urmăririi penale sau în procesul de desfășurare a activităților speciale de investigații; 3) accesul în legătură cu activitățile uzuale și legale de proiectare a sistemelor informatice, cu activitățile de funcționare curentă a sistemelor informatice sau cu activitățile comercia-



le licite; 4) accesul pentru a obține informații despre propria persoană” [12, p. 16].

În legătură cu ultimele trei exemple prezentate de către L. Gîrla și Iu. Tabarcea, trebuie să precizăm că prezența unor scopuri legitime nu este suficientă, fiind necesare toate celelalte condiții care asigură respectarea legalității. Or, de exemplu, în conformitate cu alin. (3) art. 28 al Legii nr. 1069 din 22.06.2000 cu privire la informatică, „în scopul asigurării securității naționale, organele abilitate au drept de acces la resursele informaționale din sistemele informatice publice sau private. În procesele penale, organele menționate pot, în baza mandatului emis de procuror, intercepta rețelele informatice, utilizând aparatul tehnic al proprietarului sistemului informatic” [6]. Pentru a fi interpretată la justa valoare, această dispoziție trebuie coroborată cu alin. (1) art. 7 din Codul de procedură penală al Republicii Moldova: „Procesul penal se desfășoară în strictă conformitate cu principiile și normele unanim recunoscute ale dreptului internațional, cu tratatele internaționale la care Republica Moldova este parte, cu prevederile Constituției Republicii Moldova și ale prezentului cod” [2]. De asemenea, conform lit. a) art. 3 al Legii nr. 59 din 29.03.2012 privind activitatea specială de investigații, „activitatea specială de investigații se bazează pe [principiul] legalității” [9].

Prin prisma principiului legalității trebuie privite și alte reglementări care vizează accesul la informația computerizată:

- „În scopul descoperirii și ridicării urmelor infracțiunii, a mijloacelor materiale de probă pentru a stabili circumstanțele infracțiunii ori alte circumstanțe care au importanță pentru cauză, organul de urmărire penală efectuează cercetarea la fața locului a [...] sistemelor informatice sau suporturilor de stocare a datelor informatice [...]” [2] (alin. (1) art. 118 din Codul de procedură penală al Republicii Moldova);
- „Identificarea [...] unui punct de acces la un sistem informatic constă în solicitarea unui furnizor de servicii de a identifica [...] proprietarul sau utilizatorul [...] unui punct de acces la un sistem informatic sau de a oferi informații despre faptul că [...] un anumit punct de acces la un sistem informatic este folosit sau este activ ori a fost folosit sau a fost activ la o anumită dată” [9] (alin. (1) art. 28 al Legii nr. 59 din 29.03.2012 privind activitatea specială de investigații);
- „Culegerea informației despre persoane și fapte constă în dobândirea informației despre persoane fizice și juridice, despre faptele, evenimentele, circumstanțele care prezintă interes prin studierea nemijlocită a documentelor, a materialelor, a bazelor de date, prin întocmirea de solicitări adresate persoanelor fizice și juridice care posedă sau

care dispun de informația nominalizată” [9] (art. 35 al Legii nr. 59 din 29.03.2012 privind activitatea specială de investigații) etc.

Atunci când vorbim despre legalitatea accesului la informația computerizată, nu trebuie neglijate nici alte prevederi:

- „Exercitarea drepturilor prevăzute în alineatul (1) al prezentului articol poate fi supusă unor restricții pentru motive specifice, ce corespund principiilor dreptului internațional, inclusiv pentru apărarea securității naționale sau vieții private a persoanei” [2] (alin. (2) art. 4 al Legii nr. 982 din 11.05.2000 privind accesul la informație);
- „Datele cu caracter personal care fac obiectul prelucrării trebuie să fie [...] prelucrate în mod corect și conform prevederilor legii” [8] (lit. a) alin. (1) art. 4 al Legii nr. 133 din 08.07.2011 privind protecția datelor cu caracter personal);
- „Activitatea particulară de detectiv și de pază se întemeiază pe [principiul] legalității [...]” [7] (alin. (1) art. 4 al Legii nr. 283 din 04.07.2003 privind activitatea particulară de detectiv și de pază) etc.

Persoana care realizează accesul la informația computerizată se află în câmpul legalității nu doar atunci când este autorizată în temeiul legii sau al unui contract ori atunci când nu depășește limitele autorizării, ci și atunci când are permisiunea – expresă sau tacită – din partea persoanei fizice sau juridice competente, potrivit legii, să o acorde, de a folosi, administra sau controla un sistem informatic ori de a desfășura cercetări științifice, sau de a efectua orice altă operațiune într-un sistem informatic. La baza unei astfel de interpretări, care rezultă din alin. (1) art. 259 CP, este pusă poziția cu valoare de principiu din art. 55 al Constituției Republicii Moldova: „Orice persoană își exercită drepturile și libertățile constituționale cu bună-credință, fără să încalce drepturile și libertățile altora” [3].

Atunci când este vorba despre persoane între care există un anumit climat de încredere, poate fi suficientă permisiunea tacită de a accesa informația computerizată. În context, S. Brînza și V. Stati menționează: „Accesul la informația computerizată aparținând ambilor soți de către unul dintre aceștia nu poate fi considerat ilegal atât timp cât calculatorul, suportul material de informație, sistemul sau rețeaua informatică este în mod uzual folosită de către fiecare dintre aceștia, iar informația computerizată stocată nu este personalizată sau semnalizată prin criptare sau protejare împotriva deschiderii. [...] Dacă ne aflăm în cazul unui computer la care lucrează în mod curent două sau mai multe persoane, se admite faptul că acestea accesează respectivul sistem informatic legal, fiind beneficiarele unei aprobări prelabile sau ale unei înțelegeri. În aceste condiții, fapta uneia dintre persoane de a accesa in-



formația computerizată, stocată sau vehiculată de o alta în interiorul aceluiași computer, nu mai poate fi calificată în baza [...] art. 259 CP” [1, p. 351].

Concluzia este următoarea: este posibil ca două sau mai multe persoane să aibă drept de acces la informația computerizată care se află în același calculator, pe același suport material de informație, în același sistem informatic sau în aceeași rețea informatică. Într-un asemenea caz, se prezumă că toate aceste persoane:

- 1) sunt autorizate în temeiul legii sau al unui contract;
- 2) nu depășesc limitele autorizării;
- 3) au permisiunea, din partea persoanei fizice sau juridice competente, potrivit legii, să o acorde, de a folosi, administra sau controla un sistem informatic ori de a desfășura cercetări științifice, sau de a efectua orice altă operațiune într-un sistem informatic.

Această prezumție nu funcționează în ipoteza în care:

- a) pentru una sau mai multe dintre persoanele respective este restricționat dreptul de acces la o anumită informație computerizată care se află în același calculator, pe același suport material de informație, în același sistem informatic sau în aceeași rețea informatică;
- b) una sau unele dintre persoanele respective încalcă acea restricție, ceea ce echivalează cu accesarea ilegală a informației computerizate.

**Concluziile** acestui studiu sunt:

- 1) accesul la informația computerizată este ilegal, dacă se realizează:
  - a) în lipsa autorizării în temeiul legii sau al unui contract;
  - b) cu depășirea limitelor autorizării;
  - c) fără permisiunea persoanei competente să folosească, să administreze sau să controleze un sistem informatic ori să desfășoare cercetări științifice, sau să efectueze orice altă operațiune într-un sistem informatic;
- 2) lipsa autorizării de a accesa informația computerizată presupune lipsa împuternicirii de a o accesa, pe care o acordă proprietarul informației computerizate sau un alt posesor al acestei informații;
- 3) depășirea limitelor autorizării de a accesa informația computerizată presupune că făptuitorul deține autorizarea de a accesa informația computerizată, însă acesta nu se conformează autorizării respective, arogându-și împuterniciri care nu i-au fost acordate;
- 4) pentru a considera accesul la informația computerizată ilegal, nu este relevant dacă: a) făptuitorul a solicitat permisiunea de a accesa informația computerizată, după care a ignorat refuzul de a da curs unei asemenea solicitări; b)

făptuitorul nu a solicitat permisiunea de a accesa informația computerizată;

- 5) accesul legal la informația computerizată presupune prezența nu doar a unor scopuri legitime, ci și a tuturor celorlalte condiții care asigură respectarea legalității;
- 6) art. 259 CP se aplică în ipoteza în care: a) pentru una sau mai multe persoane – care au drept de acces la informația computerizată aflată în același calculator, pe același suport material de informație, în același sistem informatic sau în aceeași rețea informatică – este restricționat dreptul de acces la o anumită informație computerizată de acest gen și b) una sau unele dintre persoanele respective încalcă acea restricție.

### Referințe bibliografice

1. Brînză S., Stati V. *Tratat de drept penal. Partea Specială. Vol. II.* Chișinău: Tipografia Centrală, 2015. 1300 p.
2. Codul de procedură penală al Republicii Moldova. Nr. 122 din 14.03.2003. În: *Monitorul Oficial al Republicii Moldova*, 2003, nr. 104-110/447. În vigoare din 12 iunie 2003.
3. Constituția Republicii Moldova. În: *Monitorul Oficial al Republicii Moldova*, 1994, nr. 1. În vigoare din 27 august 1994.
4. Decizia Înaltei Curți de Casație și Justiție a României nr. 68 din 29.09.2021 privind dispozițiile art. 360 alin. (1) din Codul penal. În: *Monitorul Oficial al României*, 2022, nr. 56.
5. Dobrinou M. Considerații tehnice și juridice privind reținerea infracțiunii de acces ilegal la un sistem informatic în situația interogării unei baze de date prin depășirea limitelor autorizării. În: *Penalmente Relevant*, 2021, nr. 1, p. 70-78.
6. Legea Republicii Moldova cu privire la informatică. Nr. 1069 din 22.06.2000. În: *Monitorul Oficial al Republicii Moldova*, 2001, nr. 73-74/547. În vigoare din 5 iulie 2001.
7. Legea Republicii Moldova privind activitatea particulară de detectiv și de pază. Nr. 283 din 04.07.2003. În: *Monitorul Oficial al Republicii Moldova*, 2003, nr. 200-203/769. În vigoare din 19 septembrie 2003.
8. Legea Republicii Moldova privind protecția datelor cu caracter personal. Nr. 133 din 08.07.2011. În: *Monitorul Oficial al Republicii Moldova*, 2011, nr. 170-175/492. În vigoare din 14 aprilie 2012.
9. Legea Republicii Moldova privind activitatea specială de investigații. Nr. 59 din 29.03.2012. În: *Monitorul Oficial al Republicii Moldova*, 2012, nr. 113-118/373. În vigoare din 8 decembrie 2012.
10. Legea României privind unele măsuri pentru asigurarea transparenței în exercitarea demnităților publice, a funcțiilor publice și în mediul de afaceri, prevenirea și sancționarea corupției. Nr. 161 din 19.04.2003. În: *Monitorul Oficial al României*, 2003, nr. 279. În vigoare din 21 aprilie 2003.
11. Legea României pentru punerea în aplicare a Legii nr. 286/2009 privind Codul penal. Nr. 187 din 24.10.2012. În: *Monitorul Oficial al României*, 2012, nr. 757. În vigoare din 1 februarie 2014.
12. Гырла Л.Г., Табарча Ю.М. *Уголовное право Республики Молдова. Часть Особенная. Том 2.* Кишинэу: Cartdidact, 2010. 592 с.