MINISTERUL CERCETĂRII, INOVĂRII ȘI DIGITALIZĂRII

Drept la replică

În temeiul art. 49 și art. 50 din Decizia Consiliului Național al Audiovizualului nr. 220/2011 privind Codul de reglementare a conţinutului audiovizual, publicată în Monitorul Oficial, Partea I nr. 174 din 11 martie 2011, Partea I, Ministerul Cercetării, Inovării și Digitalizării (MCID) formulează prezentul drept la replică cu privire la articolul de presă apărut în data de 22.12.2022 pe pagina de internet a unei publicații de știri[1].

MCID, în calitate de autoritate de stat în domeniul securității cibernetice și coordonator de reformă în Planul Național de Redresare și Reziliență (PNRR) - Domeniul Transformare Digitală a preluat coordonarea și elaborarea Legii privind securitatea și apărarea cibernetică a României.

Legea securității și apărării cibernetice a fost asumată de România ca jalon în PNRR în urma nevoii semnalate de autoritățile publice, mediul privat și cetățeni de a exista un cadru legal unitar care să permită prevenirea și combaterea eficientă a riscurilor cibernetice de la nivelul rețelelor și infrastructurilor informatice.

Legea securității și apărării cibernetice este o lege civilă construită în jurul ideii de efort colectiv, cooperare și colaborare loială între autorități, pe de-o parte, și între autorități și mediu privat, pe de altă parte, în scopul prevenirii și combaterii riscurilor, precum și al limitării impactului negativ al incidentelor cibernetice.

MCID a promovat o lege care să răspundă atât necesității de consolidare a rezilienței cibernetice a statului român, cât și nevoii cetățenilor României de a beneficia de servicii publice, rețele și sisteme informatice sigure, în condiții de confidențialitate, integritate și disponibilitate a datelor. În contextul interdependenței și interoperabilității tot mai mari a tehnologiilor, infrastructurilor, soluțiilor și serviciilor, precum și în condițiile emergenței tehnologiilor avansate pervazive, asigurarea securității cibernetice are nevoie de implementarea unor mecanisme și norme robuste care să asigure coordonarea între instituțiile statului, mediul privat și utilizatori, servind nevoii de protecție a ecosistemului ce susține infrastructurile cibernetice cu valențe critice, dar și a cetățeanului, în egală măsură.

Legea a urmat toată procedura constituțională de inițiere și promovare a actelor normative. Legea securității și apărării cibernetice a stat în perioadă de consultare publică, a fost transmisă în consultare interinstituțională către toate autoritățile și instituțiile publice implicate, a fost organizată dezbatere publică la solicitarea societății civile. De asemenea, a fost respectată întru totul procedura de avizare interministerială prevăzută de HG nr. 561/2009, s-a răspuns fiecărei propuneri și observații trimise de instituții, mediul privat și

[1] Diana Meseșan, ”La 33 de ani de la mitingul lui Ceaușescu, legea privind securitatea și apărarea cibernetică adoptată în Senat va naște, conform unui expert, „informatorii 2.0” Citeşte întreaga ştire: La 33 de ani de la mitingul lui Ceaușescu, legea privind securitatea și apărarea cibernetică adoptată în Senat va naște, conform unui expert, „informatorii 2.0””, Libertatea.ro, Joi, 22 decembrie 2022, disponibil la: https://www.libertatea.ro/stiri/la-33-de-ani-de-la-mitingul-lui-ceausescu-legea-privind-securitatea-si-apararea-cibernetica-adoptata-azi-in-senat-va-naste-conform-unui-expert-informatorii-2-0-4388825; accesat la data de 23.12.2022.

Str. D.I. Mendeleev 21-25, Sector 1, 010362, București
Tel: +40 021 303 21 20
E-mail: office@research.gov.ro
www.research.gov.ro

societate civilă și s-au însușit propuneri substanțiale din partea societății civile și a mediului privat (ex. dilatarea termenelor de notificare a incidentelor, diminuarea sancțiunilor contravenționale, prevederea unor mecanisme transparente și predictibile de notificare a incidentelor cibernetice de către mediul privat etc).

În ceea ce privește dezbaterea și votarea proiectului de lege în Parlament, MCID a solicitat, în temeiul art. 76 alin. (3) din Constituția României, republicată, dezbaterea în procedură de urgență, solicitare aprobată de Birourile Permanente ale celor două Camere ale Parlamentului. Chiar și în procedura de urgență, deputații, senatorii, ministerele și alte autorități administrative autonome au formulat amendamente care s-au supus dezbaterii și votului deputaților și senatorilor. Procedura parlamentară de urgență este o instituție constituțională și uzitată în dreptul parlamentar atunci când nevoia de reglementare este urgentă, situație în care s-a aflat și prezenta lege. Procedura parlamentară de urgență nu a înfrânat sub nicio formă dezbaterea, contradictorialitatea, autonomia regulamentară a Parlamentului. Singura diferență între procedura ordinară parlamentară și procedura de urgență parlamentară este termenul care curge între sesizarea comisiilor, respectiv între sesizarea comisiilor și votul în plen. Cu toate acestea menționăm că proiectul de lege a fost în dezbaterea Guvernului și a Parlamentului timp de 2 luni, perioadă în care orice persoană fizică și juridică a putut formula amendamente, acestea fiind toate procesate și dezbătute de Guvern și Parlament.

Legea securității și apărării cibernetice nu militarizează internetul, cum în mod fals afirmă autorul, ci dimpotrivă, asigură o coordonare civilă transparentă la nivel național privind raportarea responsabilă a incidentelor și managementul alertelor de securitate cibernetică, la nivelul Directoratului Național de Securitate Cibernetică (DNSC), autoritate națională civilă în domeniul securității cibernetice (art. 20 alin. (1) din Lege).

Mai mult, MCID s-a asigurat că nicio autoritate militară nu primește mai multe atribuții prin prezenta lege, altele decât cele care se circumscriu deja competenței lor. Spre exemplu, Ministerul Apărării Naționale devine autoritate națională în domeniul apărării cibernetice, aspect care consacră angajamentele României în cadrul NATO și conferă suport legislativ activității de excelență pe care Comandamentul Apărării Cibernetice de la nivelul Armatei îl desfășoară. Un alt exemplu este Serviciul Român de Informații care este desemnat autoritate națională în domeniul cyberintelligence, cyberintelligence-ul fiind o parte componentă a activității de informații, competență pe care SRI deja o are în temeiul art. 1 din Legea nr. 14/1992 și a art. 6 din Legea nr. 51/1991. Un al treilea exemplu este Serviciul de Telecomunicații Speciale care, pentru rețelele și sistemele informatice proprii prin intermediul cărora asigură telecomunicațiile speciale pentru statul român conform Legii nr. 92/1996, sunt desemnați să asigure și securitatea cibernetică. Un al patrulea exemplu este Serviciul de Protecție și Pază care, în deplină concordanță cu prevederile art. 14 alin. (1), lit. g) din Legea nr. 191/1998, coordonează măsurile de securitate cibernetică pentru demnitarii cărora le asigură protecție.

Str. D.I. Mendeleev 21-25, Sector 1, 010362, București
Tel: +40 021 303 21 20
E-mail: office@research.gov.ro
www.research.gov.ro

Readucem aminte opiniei publice că întreaga activitate a serviciilor și instituțiilor militare din România este controlată direct de Parlament, astfel: (1) pentru SRI și SIE, prin comisie parlamentară permanentă specială; (2) pentru MAPN, MAI, SPP, STS, prin comisiile parlamentare permanente comune de apărare, ordine publică și securitate națională. MCID s-a asigurat că legea nu permite niciunei autorități militare să-și atribuie competențe specifice unei alte autorități militare sau civile.

Legea securității și apărării cibernetice are două mecanisme majore de notificare a incidentelor de securitate cibernetică.

Primul mecanism este cel creat prin Platforma națională pentru raportarea incidentelor de securitate cibernetică, denumită în continuare PNRISC. Această Platformă este gestionată de o autoritate civilă, respectiv de către DNSC, și este constituită conform prevederilor Legii nr. 362/2018 și a OUG nr. 104/2021. Există două termene de notificare în PNRISC: primul este în primele 48 de ore de la apariția incidentului de securitate cibernetică, iar al doilea, în 5 zile de la notificarea inițială, pentru situațiile în care nu pot fi furnizate deodată toate informațiile despre incident. Astfel, legiuitorul a înțeles să acorde termene permisive celor care au obligația notificării incidentelor de securitate, scopul fiind identificarea completă și corectă a incidentelor, atacurilor și amenințărilor, nu parcurgerea unei operațiuni administrative formale. Scopul final al acestui demers de notificare este acela ca autoritățile responsabile de securitate cibernetică să poată acorda sprijin, la cerere, proprietarilor, administratorilor, posesorilor și/sau utilizatorilor de rețele și sisteme informatice aflate în domeniul lor de competență, activitate sau responsabilitate, spre adoptarea de măsuri reactive de primă urgență pentru remedierea efectelor incidentelor de securitate cibernetică deja întâmplate (conform art. 23).

Al doilea mecanism de notificare a incidentelor de securitate cibernetică are ca premisă asigurarea rezilienței în spațiul cibernetic național, astfel cum este înțeleasă de legiuitor la art. 24 din Lege. Acest mecanism de notificare se face la cererea autorităților de la art. 10 din Lege, responsabile de securitatea cibernetică, trebuie să fie motivată și să se încadreze în limitele date de lege noțiunilor de incidente, amenințări, riscuri sau vulnerabilități. Solicitarea referă date primare, necesare reacției rapide la eventuale situații avute în atenție la nivelul autorităților competente menționate de prezenta Lege, situații care - în urma validării încadrării lor în categoria incidentelor cibernetice - intră sub incidența necesității de raportare conform art. 21. Și în acest caz de notificare există două termene, unul de 48 de ore de la solicitare, în care se furnizează doar existența incidentului și un al doilea termen, de 5 zile de la solicitare, în care se notifică amenințări, riscuri, vulnerabilități sau atacuri care, prin natura lor, necesită timp de procesare și analizare.

Care sunt rețelele și sistemele care intră sub incidența obligației de notificare a incidentelor?

- rețelele și sistemele informatice deținute, organizate, administrate, utilizate sau aflate în competența autorităților și instituțiilor publice din domeniul apărării, ordinii publice, securității naționale, justiției, situațiilor de urgență, Oficiului Registrului Național al Informațiilor Secrete de Stat.

- rețelele și sistemele informatice deținute de persoanele fizice și juridice de drept privat și utilizate în vederea furnizării de servicii de comunicații electronice către autoritățile și instituțiile administrației publice centrale și locale.
- rețelele și sistemele informatice deținute, organizate, administrate sau utilizate de autorități și instituții ale administrației publice centrale și locale, altele decât cele prevăzute la lit. a), precum și de persoane fizice și juridice care furnizează servicii publice ori de interes public, altele decât cele de la lit. b).

În ceea ce privește obligația de notificare de către persoanele care furnizează servicii publice ori de interes public, acestea se referă la acele persoane care, potrivit legii, prin activitatea lor, satisfac o nevoie publică, cum ar fi operatorii de apă, canalizare, curent electric sau companii naționale precum Poșta Română sau Radiocom, care desfășoară servicii esențiale pentru cetățeni și care, atacate cibernetic, ar crea disfuncționalități majore în bună funcționare a statului, a administrației publice și a serviciilor pentru cetățeni.

Este foarte important de precizat că legiuitorul a prevăzut expres că, prin intermediul celor două mecanisme de notificare nu se transferă date de conținut, ci numai metadate care contribuie strict la identificarea incidentului și combaterea amenințării. Aceste mecanisme de notificare privind incidentele de securitate cibernetică sunt bazate pe standarde internaționale (ex. STIX și TAXII) ce au fost dezvoltate și sunt utilizate curent în efortul de a îmbunătăți prevenirea și atenuarea atacurilor cibernetice. Ele includ strict date tehnice privind incidentele cibernetice, cum ar fi: data și ora incidentului, tehnica de atac cibernetic folosită de atacator, tehnologiile utilizate de acesta, indicatorii tehnici de compromitere a infrastructurilor afectate, sursa raportării incidentului, incidente conexe, etc. Astfel, spre exemplu, date privind identitatea unei persoane nu sunt utile notificării decât dacă, prin natura lor, pot identifica autorul atacului cibernetic. Pe de altă parte, date precum cele medicale, date privind cazierul fiscal al persoanei sau judiciar, sau oricare alte date similare, nu sunt în niciun caz utile prevenirii unui atac ciberentic și nu sunt prevăzute a fi comunicate în cadrul acțiunilor de raportare a incidentelor.

De asemenea, este important de menționat că, prin cele două mecanisme de notificare a incidentelor, autoritățile nu au niciun drept de a accesa un sistem sau rețea informatică. Cooperarea se realizează pe bază de cereri formulate, respectiv pe bază de proceduri ce vor fi stabilite prin hotărâre a Guvernului României și a directorului DNSC. Astfel, în nicio situație nu se poate vorbi de violarea unor drepturi privind viața privată, secretul profesional, libertatea de exprimare ori alte asemenea.

Legea securității și apărării cibernetice, prin sistemele de notificare a incidentelor cibernetice, urmărește să prevină și să combată atacuri cibernetice care duc la disfuncționalitatea unor rețele și sisteme informatice, la furtul de date, la operațiuni financiare ilegale etc. Astfel, scopul măsurilor este de a asigura un climat de siguranță în spațiul cibernetic, de a asigura respectarea legii, drepturilor și libertăților cetățenilor, de a asigura protejarea exercitării unor drepturi și executarea unor obligații licite și morale. Or, eventuale clauze contractuale de confidențialitate între cei care au obligația de notificare și terți (clienți)

nu pot ascunde sub imperiul acelor clauze protejarea unor fapte ilicite și imorale, acest lucru reieșind și din prevederile art. 11, art. 14 alin. (1) și art. 1169 din Codul civil.

Astfel, MCID deplânge discursul public care promovează ideea că prin contracte se pot ascunde fapte ilicite de tipul atacurilor cibernetice, furtului de date sau infracțiuni financiare în spațiul virtual, pe care statul să nu poată să le identifice și să le combată. Clauzele contractuale de confidențialitate nu pot și nu trebuie să prevină obligativitatea raportării unor incidente cibernetice ce, în numeroase cazuri, intră inclusiv sub incidența Codului Penal, spre exemplu raportarea de incidente cibernetice privind accesul ilegal la un sistem informatic (Art 360 Cod Penal), alterarea integrităţii datelor informatice (Art 362 Cod Penal) sau perturbarea funcţionării sistemelor informatice (Art. 363 Cod penal). Este de esența funcționării statului să asigure un climat de ordine publică și de respectare a legii, iar această Lege a securității și apărării cibernetice, prin mecanismele de notificare, nu urmărește decât prezervarea acestui climat.

Mai mult, reamintim că există deja, la nivelul legislației românești în domeniul securității și rețelelor informatice, mecanisme de notificare a incidentelor de securitate cibernetică. Mecanismul de notificare a incidentelor de securitate cibernetică, precum și condițiile funcționării platformei PNRISC, sunt reglementate în Legea nr. 362/2018 (care transpune Directiva europeană NIS1) și în OUG nr. 104/2021, și se află sub coordonarea și responsabilitatea DNSC. Legea securității și apărării cibernetice consolidează și menține integrat acest cadru de raportare a incidentelor, sub autoritatea unică a DNSC, urmărind în același timp eficientizarea procesuală, evitarea dublării eforturilor, evitarea suprapunerii de competențe și economia utilizării resurselor, pentru acest scop.

Cele două sisteme de notificare a incidentelor de securitate cibernetică, prevăzute la art. 21 și art. 25, nu au nicio legătură cu completarea Legii nr. 51/1991 privind securitatea națională a României. Completarea Legii nr. 51/1991 vizează trei noi amenințări care se realizează în spațiul cibernetic și care devin amenințări la adresa securității naționale a României. Pentru a da relevanță practică conceptelor de cyber intelligence și counter-cyberintellicence, dar și pentru ca autoritățile cu atribuții în domeniul securității naționale prevăzute la art. 6 din Legea nr. 51/1991 să-și poată exercita atribuțiile în domeniul securității cibernetice potrivit propriilor competențe, prin Legea securității și apărării cibernetice se completează art. 3 din Legea nr. 51/1991 privind securitatea națională a României cu următoarele tipuri de amenințări:

1. *Amenințări cibernetice sau atacuri cibernetice asupra infrastructurilor informatice și de comunicații de interes național;*

Conceptul de amenințare cibernetică este definit la art. 2, lit. b) din Legea securității și apărării cibernetice, cu trimitere la art. 2 lit. f) din Ordonanța de Urgență a Guvernului nr. 104/2021;

Conceptul de atac cibernetic este definit la art.2, lit. c) din Legea securității și apărării cibernetice ca fiind ”acțiune ostilă (de rea-credință) desfășurată în spațiul cibernetic de natură să afecteze securitatea cibernetică”.

Conceptul de infrastructură informatică și de comunicații de interes național este definită de art. 2, lit.d) din Legea nr. 163/2021 privind adoptarea unor măsuri referitoare la infrastructuri informatice și de comunicații de interes național și condițiile implementării rețelelor 5G.

Astfel, apreciem că acest tip de amenințare prezintă toate garanțiile de calitate, claritate și previzibilitate a legii impuse de prevederile art. 1, alin. (5) din Constituția României, republicată.

2. *Acțiuni, inacțiuni sau stări de fapt cu consecințe la nivel național, regional sau global care afectează reziliența statului român în raport cu riscurile și amenințările de tip hibrid;*

Conceptul de reziliență este amplu definit în mai multe acte normative la nivelul statului român, plecând de la definiția rezilienței în spațiul cibernetic, prevăzută la art. 2 lit.v) din Legea securității și apărării cibernetice, până la dezvoltarea conceptului în Hotărârea Parlamentului nr. 22/2020 privind aprobarea Strategiei Naţionale de Apărare a Ţării pentru perioada 2020-2024, în Hotărârea Guvernului nr. 1321/2021 privind aprobarea Strategiei de securitate cibernetică a României, pentru perioada 2022-2027, precum și a Planului de acțiune pentru implementarea Strategiei de securitate cibernetică a României, pentru perioada 2022-2027, în Ordonanţa de Urgenţă a Guvernului nr. 155/2020 privind unele măsuri pentru elaborarea Planului naţional de redresare şi rezilienţă necesar României pentru accesarea de fonduri externe rambursabile şi nerambursabile în cadrul Mecanismului de redresare şi rezilienţă, precum și în Ordonanţa de Urgenţă a Guvernului nr. 124/2021 privind stabilirea cadrului instituţional şi financiar pentru gestionarea fondurilor europene alocate României prin Mecanismul de redresare şi rezilienţă, precum şi pentru modificarea şi completarea Ordonanţei de urgenţă a Guvernului nr. 155/2020 privind unele măsuri pentru elaborarea Planului naţional de redresare şi rezilienţă necesar României pentru accesarea de fonduri externe rambursabile şi nerambursabile în cadrul Mecanismului de redresare şi rezilienţă.

Riscurile și amenințările de tip hibrid la adresa securității cibernetice sunt acele amenințări și riscuri cibernetice, astfel cum sunt definite în art. 2, lit. b) și w) din Legea securității și apărării cibernetice, care se manifestă sub formă hibridă. Forma hibridă a amenințărilor și riscurilor de securitate cibernetică este conceptualizată prin Hotărârea Parlamentului nr. 22/2020 privind aprobarea Strategiei Naţionale de Apărare a Ţării pentru perioada 2020-2024.

Astfel, apreciem că acest tip de amenințare prezintă toate garanțiile de calitate, claritate și previzibilitate a legii impuse de prevederile art. 1, alin. (5) din Constituția României, republicată.

3. *Acțiuni derulate de către o entitate statală sau nonstatală, prin realizarea, în spațiul cibernetic, a unor campanii de propagandă sau dezinformare, de natură a afecta ordinea constituțională.*

Prin Hotărârea Parlamentului nr. 22/2020 privind aprobarea Strategiei Naţionale de Apărare a Ţării pentru perioada 2020-2024 s-a stabilit ca obiectiv strategic ”prevenirea şi contracararea riscurilor de natură teroristă asociate activităţilor unor organizaţii de profil, prezenţei pe teritoriul naţional a membrilor sau adepţilor unor astfel de entităţi, intensificării

propagandei extremist-jihadiste, în special în mediul online, şi a proceselor de radicalizare în România."

Acţiunile informative ostile continuă să vizeze dezvoltarea unor puncte de sprijin, utilizate în scop de influenţă, obţinerea de informaţii cu privire la evoluţiile interne, necesare susţinerii proceselor decizionale din statele de provenienţă, dar şi pentru rafinarea şi dezvoltarea bazelor de sprijin şi a canalelor de propagandă, cu potenţial de obstrucţionare a proiectelor strategice ale României şi a deciziilor în stat. Parteneriatele strategice ale României şi politicile promovate în acord cu statutul de membru al UE şi NATO menţin ţara noastră în atenţia spionajului străin, nivelul de intruziune şi ofensivitate oscilând în funcţie de interesele statelor agresoare în raport cu Bucureştiul şi alianţele sau parteneriatele noastre.

Prin aceeași strategie de apărare a țării s-a constatat, ca vulnerabilitate, "persistenţa unor lacune legislative în domeniul securităţii naţionale sau în ceea ce priveşte contracararea agresiunilor informaţionale, respectiv pe palierul reglementării instrumentelor necesare prevenirii şi contracarării propagandei cu scop destabilizator, inclusiv în eventualitatea unor campanii de tip hibrid".

Direcțiile de acțiune pe linia de informații, contrainformații și de securitate, conform SNAp 2020-2024, vizează și "Prevenirea şi contracararea riscurilor asociate activităţilor unor entităţi teroriste, prezenţei pe teritoriul naţional a membrilor sau simpatizanţilor unor asemenea entităţi, intensificării propagandei extremist-teroriste, în special a celei jihadiste în ascensiune în mediul online, şi a proceselor de radicalizare în România".

Ținând cont de cele anterioare, apreciem necesară instituirea, la nivelul legii, a unor noi tipuri de amenințări care să răspundă nevoilor de securitate cibernetică și securitate națională a României, astfel încât să se asigure cu succes protejarea cetățenilor și a statului român.

Acțiunile de propagandă și dezinformare vizate sunt doar cele care afectează ordinea constituțională, adică setul de principii fundamentale pe care este constituit statul român, regimul constituțional de drepturi și libertăți fundamentale, regimul constituțional al funcționării autorităților publice de rang constituțional, protejarea garanțiilor prevăzute de Constituție.

Menționăm că aceste amenințări instituite au relevanță doar pentru activitatea de informații și contrainformații, activitate desfășurată doar de autoritățile competente potrivit art. 6 din Legea nr. 51/1991. Prin prezenta lege nu se pot desfășura activități de natură a restrânge exercițiul unor drepturi și libertăți fundamentale și nici activități specifice culegerii de informații, precum nici activități de contrainformații. Prezenta lege reglementează activitatea de cyberintelligence și counter cyber intelligence doar la nivel conceptual, urmând ca definițiile să se completeze corespunzător cu dreptul material prevăzut în Legea nr. 51/1991 și alte legi speciale din domeniul securității naționale.

Relevanța practică a acestor amenințări se materializează doar în activitatea de informații și contrainformații care, atunci când se realizează prin metode care presupun restrângerea exercițiului unor drepturi și libertăți fundamentale, se poate face numai pe baza unui mandat emis de un judecător de la Înalta Curte de Casație și Justiție, conform art. 14 și urm. din Legea nr. 51/1991. Astfel, pentru orice utilizare a acestor amenințări ca temei al activității de informații, este necesar mandatul prealabil al judecătorului ICCJ, constituind cea mai înaltă formă de protecție împotriva unor eventuale abuzuri de orice fel.

Completarea Legii nr. 51/1991 cu trei noi amenințări la adresa securității naționale, și care au legătură cu domeniul securității cibernetice, nu vizează mecanismul de notificare prin PNRISC și nici cel reglementat de art. 21 și art. 25 din Lege. Implicit, completarea Legii nr. 51/1991 nu are nicio legătură cu sancțiunile contravenționale pentru nenotificarea în PNRISC, respectiv pentru nenotificarea în temeiul art. 21 și art. 25. De altfel, Legea nr. 51/1991 nu prevede sancțiuni contravenționale și nici penale pentru necomunicarea de informații, indiferent dacă sunt sau nu de interes pentru securitatea națională. În concluzie, acuzațiile publice conform cărora în temeiul prezentei legi s-ar putea aplica sancțiuni contravenționale pentru fapte ce constituie amenințări la adresa securității naționale sunt afirmații mincinoase, formulate cu rea-credință și superficialitate juridică, în scopul deturnării misiunii legii de a proteja cetățenii și instituțiile statului român.

Str. D.I. Mendeleev 21-25, Sector 1, 010362, București
Tel: +40 021 303 21 20
E-mail: office@research.gov.ro
www.research.gov.ro