IDR
Romanian Diplomatic Institute

Ministerul Afacerilor Externe

# România în contextul guvernanței europene și internaționale privind divulgarea coordonată a vulnerabilităților și a cercetării în domeniul securității cibernetice

**Teodora Curelariu**


POLICY FORUM nr. 8/2026

# România în contextul guvernanței europene și internaționale privind divulgarea coordonată a vulnerabilităților și a cercetării în domeniul securității cibernetice [1] *

**Teodora Curelariu** [2]

*Doctorandă, Université Grenoble Alpes & Inria*

Policy Forum no. 8 / 2026

Published by: Romanian Diplomatic Institute

ISSN: 3119-8562

**Abstract**

Pe măsură ce amenințările cibernetice se intensifică, iar societățile devin tot mai dependente de infrastructurile digitale, vulnerabilitățile software nu mai pot fi înțelese exclusiv ca defecte tehnice. Acestea au devenit chestiuni juridice, instituționale, strategice și diplomatice. Acest articol examinează divulgarea coordonată a vulnerabilităților (CVD) și cercetarea de securitate la intersecția dintre dreptul românesc, dreptul Uniunii Europene și cooperarea internațională în domeniul securității cibernetice. Articolul situează România într-un cadru normativ în evoluție, modelat de Directiva NIS2, de mecanismele europene emergente de gestionare a vulnerabilităților și de Convenția de la Budapesta. În dreptul românesc, problema izvorăște din tensiunea dintre incriminarea accesului neautorizat și a infracțiunilor informatice conexe, prevăzute la articolele 360-366 din Codul penal, și noul cadru național de securitate cibernetică instituit prin Ordonanța de urgență nr. 155/2024, aprobată și modificată prin Legea nr. 124/2025. Deși ordonanța a lăsat inițial nesoluționată legalitatea cercetării tehnice premergătoare unei raportări, o lege adoptată de Parlament în iunie 2026 ar introduce o protecție penală condiționată pentru conduitele expres prevăzute, în măsura în care sunt îndeplinite cerințele privind cercetarea și raportarea. Articolul susține că CVD și cercetarea de securitate legitimă nu sunt simple practici tehnice, ci mecanisme de construire a încrederii între autorități, cercetători, sectorul privat și partenerii internaționali. Implementarea efectivă și clarificarea acestei protecții pentru cercetarea necesară, proporțională și nedistructivă ar consolida reziliența internă a României și ar susține o poziție românească coerentă în dezbaterile europene și internaționale privind guvernanța vulnerabilităților, protecția cercetătorilor și diplomația cibernetică.

**Cuvinte cheie**: România, divulgarea coordonată a vulnerabilităților, cercetare de securitate, Uniunea Europeană, Convenția de la Budapesta, exonerare legală de răspundere, diplomație cibernetică.

[1] Această publicație se bazează exclusiv pe surse deschise. Opiniile exprimate aparțin în întregime autoarei și nu reflectă neapărat poziția instituției.

* Acest material reprezintă traducerea în limba română a textului original publicat în limba engleză.

[2] tcurelariu@gmail.com

## INTRODUCERE

Să presupunem că un cercetător identifică o vulnerabilitate potențială într-un software utilizat de un spital, de o autoritate publică, de un serviciu esențial sau de o infrastructură critică. Pentru a elabora un raport credibil, cercetătorul poate avea nevoie să interacționeze cu sistemul respectiv și să verifice existența reală a vulnerabilității. Această verificare limitată poate contribui la prevenirea unui atac cibernetic, însă poate fi, în același timp, asimilată **accesului neautorizat** în sensul dreptului penal. Întrebarea centrală din perspectiva politicilor publice este dacă legislația română permite cercetătorilor responsabili să efectueze testările minime necesare pentru protejarea interesului public, înainte ca aceeași vulnerabilitate să fie exploatată de un atacator. Problema nu se limitează la modul în care organizațiile remediază vulnerabilitățile deja cunoscute. Aceasta privește, în egală măsură, existența unor canale legale și de încredere prin care statul permite descoperirea și semnalarea vulnerabilităților înainte ca acestea să fie exploatate.

**Cercetarea vulnerabilităților și divulgarea coordonată a vulnerabilităților (CVD) sunt, prin urmare, strâns legate între ele.** O vulnerabilitate nu poate fi, în mod normal, evaluată și remediată prin mecanismul CVD decât după ce a fost descoperită și validată suficient pentru a susține un raport credibil. Totuși, această validare poate presupune scanare, enumerare, testarea autentificării sau realizarea unui *proof of concept* limitat, exact acele acțiuni care riscă să fie calificate drept **acces neautorizat sau tentativă de acces neautorizat** în dreptul penal. Cercetătorii independenți pot identifica vulnerabilități care scapă testărilor interne, certificărilor și evaluărilor de rutină, în special după punerea în funcțiune a sistemelor și în cazul arhitecturilor care combină software, servicii cloud și componente furnizate de terți.

**Atunci când consecințele juridice ale unei testări proporționale sunt imprevizibile, cercetătorii pot fi descurajați să participe la procesul de CVD**, iar vulnerabilitățile rămân neraportate (Pupillo et al., 2018, 53-54). Un stat care protejează doar raportul final, lăsând însă cercetarea care îl precedă într-o zonă de incertitudine juridică, reglementează doar jumătate din procesul de CVD.

Această relație dintre cercetare și remediere explică **motivul pentru care CVD a devenit parte integrantă a cadrului european de securitate cibernetică**. Directiva NIS2

impune ca strategiile naționale să promoveze și să faciliteze CVD, precum și obligația statelor membre de a desemna un CSIRT drept coordonator național, care să acționeze ca intermediar de încredere (European Parliament and Council, 2022, art. 7 alin. (2) lit. c) și art. 12 alin. (1)). Regulamentul privind reziliența cibernetică (Cyber Resilience Act) impune producătorilor obligația de a institui procese de gestionare a vulnerabilităților și de a raporta vulnerabilitățile exploatate activ, în timp ce Legea privind securitatea cibernetică (Cybersecurity Act) integrează evaluarea și gestionarea vulnerabilităților în sistemul european de certificare (European Parliament and Council, 2024, art. 13 și art. 14 alin. (1), Anexa I, Partea a II-a; European Parliament and Council, 2019, art. 51 lit. d). Împreună, aceste instrumente tratează informația privind vulnerabilitățile drept o resursă pentru reziliența colectivă și consolidează primirea, coordonarea și remedierea acesteia. Ele reglementează ceea ce organizațiile trebuie să facă din momentul în care informația privind o vulnerabilitate există deja, fără a armoniza însă condițiile în care cercetătorii externi pot produce, în mod legal, această informație.

Consecințele vulnerabilităților neremediate sau slab coordonate pot depăși cu mult sistemul afectat inițial. În urma incidentului WannaCry, președintele Microsoft, Brad Smith, a comparat divulgarea instrumentului de exploatare cu situația în care armata americană ar fi avut „rachete Tomahawk furate", ilustrând astfel riscurile generate de păstrarea vulnerabilităților exploatabile și divulgarea lor ulterioară în afara unui proces controlat de remediere (Smith, 2017). Cazul WannaCry a arătat modul în care un instrument de exploatare dezvoltat inițial ca parte a unei capacități cibernetice statale poate provoca prejudicii extinse odată ajuns în domeniul public, în timp ce Log4Shell a arătat modul în care o vulnerabilitate dintr-o componentă software larg reutilizată poate expune produse, organizații și servicii critice în numeroase sectoare și jurisdicții. În România, preambulul Ordonanței de urgență nr. 155/2024 face referire la un incident produs în primul trimestru al anului 2024, care a afectat 26 de spitale printr-un furnizor de servicii gestionate și care a avut un impact direct asupra serviciilor vitale oferite populației (Romanian Government, 2024, preambul). **Guvernanța vulnerabilităților reprezintă, prin urmare, o componentă a rezilienței naționale, a securității lanțului de aprovizionare și a diplomației cibernetice**, nu o simplă funcție tehnică.

România are un interes deosebit în abordarea **acestui decalaj legislativ**. Administrația publică, economia și serviciile esențiale ale țării depind de produse, servicii și infrastructuri caracterizate prin lanțuri de aprovizionare și dependențe tehnice transfrontaliere. În calitate de

stat membru al UE și al NATO, parte la Convenția de la Budapesta și țară-gazdă atât pentru Oficiul Programului privind Criminalitatea Informatică al Consiliului Europei (C-PROC), cât și pentru Centrul european de competențe în materie de securitate cibernetică (ECCC), România are deopotrivă responsabilitatea de a-și perfecționa managementul intern al vulnerabilităților și o poziție favorabilă pentru a contribui la dezbaterile europene și internaționale privind dreptul penal al criminalității informatice, protecția cercetătorilor și comportamentul responsabil al statelor.

Cadrul normativ românesc a evoluat substanțial. Studiul comparativ realizat de ENISA în 2022 a clasificat România printre statele membre care nu dispuneau de o politică națională privind CVD. Ulterior, Ordonanța de urgență nr. 155/2024 a instituit un mecanism legal de coordonare și a desemnat Directoratul Național de Securitate Cibernetică (DNSC) drept coordonator național al CVD și intermediar de încredere. Ordonanța reglementează raportarea, transmiterea anonimă a informațiilor, comunicarea cu furnizorii afectați și coordonarea transfrontalieră. Cu toate acestea, ea păstrează aplicabilitatea Codului penal, lăsând inițial incert efectul juridic al conformării. În iunie 2026, Parlamentul a adoptat o lege prin care se introduce articolul 365[1] în Codul penal, excluzând caracterul infracțional al unor fapte determinate, în măsura în care sunt întrunite cumulativ condițiile prevăzute la art. 36 alin. (5) și (6). Sub rezerva promulgării și a intrării în vigoare, această reformă reprezintă un pas semnificativ, dar incomplet, către o protecție legală condiționată (Romanian Parliament, 2026).

Prezenta lucrare susține că România a creat un mecanism instituțional pentru primirea și coordonarea raportărilor de vulnerabilități și a început să asigure cadrul legal al procesului prin care acestea sunt produse, cu toate că protecția propusă rămâne condiționată și incompletă. Obiectivul nu este acela de a exonera cercetătorii de securitate de răspunderea penală sau de a autoriza testări nelimitate, ci de a distinge cercetarea necesară, proporțională și neconstitutivă de daune de intruziunea dăunătoare, extragerea de date, persistența în sistem și perturbarea funcționării acestuia. Întrebarea este, prin urmare, mai restrânsă decât aceea dacă hacking-ul etic ar trebui permis în general. Ea privește tratamentul juridic al unor acțiuni limitate, întreprinse pentru a stabili existența unei vulnerabilități, pentru a evalua relevanța acesteia din perspectiva securității și pentru a comunica suficiente dovezi în vederea remedierii. Legalitatea conduitei ar trebui, în consecință, să depindă de întinderea acesteia, de scopul urmărit, de efectele produse și de comportamentul ulterior al cercetătorului.

Analiza combină trei niveluri de examinare. **La nivel național**, sunt cercetate raporturile dintre articolele 360-366 din Codul penal, mecanismul instituit prin Ordonanța de urgență nr. 155/2024 și protecția condiționată propusă prin articolul 365[1]. **La nivel european**, sunt avute în vedere Directiva 2013/40/UE, Directiva NIS2, Regulamentul privind reziliența cibernetică și Legea privind securitatea cibernetică. **La nivel internațional**, este evaluat accesul „fără drept" la un sistem informatic în sensul Convenției de la Budapesta, precum și modul în care Convenția Națiunilor Unite împotriva Criminalității Informatice recunoaște cercetarea legitimă în materie de securitate. În continuare, lucrarea propune o agendă juridică și diplomatică pentru România.

## DE CE DIVULGAREA COORDONATĂ A VULNERABILITĂȚILOR DEPINDE DE CERCETAREA ÎN DOMENIUL SECURITĂȚII

### De la descoperirea vulnerabilității la remedierea coordonată

O vulnerabilitate reprezintă o deficiență care poate fi exploatată pentru a compromite un produs sau un sistem digital. Managementul vulnerabilităților acoperă răspunsul mai amplu la această problemă, de la identificarea și evaluarea deficienței până la remedierea acesteia, distribuirea corecției și monitorizarea rezultatului. CVD abordează o componentă esențială a acestui răspuns: modul în care persoana care descoperă deficiența comunică cu organizația care are capacitatea de a o remedia și modul în care părțile coordonează etapele următoare. Definiția propusă de ENISA este deosebit de relevantă în acest sens**: o politică națională de CVD ar trebui să permită și să încurajeze cercetarea, în condiții clar definite** (ENISA, 2022, p. 6). O simplă adresă de e-mail pentru raportare nu constituie, prin urmare, o politică completă, în măsura în care cercetătorii continuă să nu cunoască limitele testărilor pe care le pot efectua în mod legal.

În practică, procesul de CVD debutează în momentul în care o posibilă deficiență este descoperită și validată suficient pentru a susține un raport credibil. Furnizorul evaluează, în continuare, constatarea respectivă, elaborează o corecție și coordonează comunicarea cu cercetătorul și, atunci când este necesar, cu alți furnizori sau autorități. Obiectivul urmărit este acela de a evita, pe de o parte, publicarea prematură, care poate expune utilizatorii înainte de

existența unei corecții, și, pe de altă parte, păstrarea secretului pe termen indefinit, care lasă vulnerabilitatea nerezolvată.

Coordonarea are o importanță deosebită atunci când partea afectată este dificil de identificat sau atunci când o singură vulnerabilitate este integrată în mai multe produse. Procesul poate implica cel care descoperă vulnerabilitatea, autorul raportării, furnizorul afectat, organizațiile care utilizează produsul respectiv, precum și un CSIRT sau un alt intermediar de încredere. Un intermediar de încredere poate reduce asimetriile informaționale, poate asigura confidențialitatea și poate coordona comunicarea dincolo de limitele organizaționale și naționale. Delimitarea rolurilor respective clarifică cine poate autoriza testarea, cine poate remedia deficiența și cine poate coordona divulgarea acesteia. CVD nu privește, prin urmare, doar momentul publicării, ci și repartizarea responsabilităților între actorii care dețin, fiecare, părți diferite din informația necesară remedierii.

**Mecanisme și forme de autorizare distincte**

CVD, politicile de divulgare a vulnerabilităților, programele de recompensare a descoperirii vulnerabilităților (*bug bounty*) și testele de penetrare sunt adesea grupate laolaltă, însă acestea răspund unor întrebări juridice diferite. Distincția este relevantă întrucât sursa, întinderea și efectul juridic al autorizării nu sunt identice în fiecare caz.

- **O politică de divulgare a vulnerabilităților** indică cercetătorilor modalitatea în care trebuie raportată o vulnerabilitate și poate, de asemenea, preciza sistemele și tehnicile pe care organizația le autorizează.
- **Un proces mai amplu de CVD** poate implica mai mulți furnizori, CSIRT-uri sau autorități străine, în timp ce un program de tip *bug bounty* adaugă o recompensă politicii de divulgare a organizației respective.
- **Un test de penetrare**, în schimb, este comandat în temeiul unui contract care definește sistemele autorizate, metodele utilizate și perioada de testare.

Aceste mecanisme nu oferă un nivel echivalent de protecție juridică. Un expert în *pentesting* (i.e. test de penetrare extern, simularea unui atac) contractat se află în poziția cea mai clară, întrucât clientul autorizează, în mod expres, operațiuni determinate asupra unor sisteme determinate. Această protecție se limitează, însă, la sfera contractului. Testarea unui subdomeniu exclus, provocarea unei întreruperi neautorizate a serviciului (*denial of service*)

sau accesarea unui volum de date mai mare decât cel necesar pot excede întinderea autorizată. Un participant la un program de tip *bug bounty* se află într-o poziție similară, întemeiată pe regulile publice ale programului, care pot exclude anumite subdomenii, conturi de utilizator, servicii ale unor terți sau tehnici precum ingineria socială. O organizație nu poate autoriza testarea unei infrastructuri asupra căreia nu exercită control, chiar dacă aceasta este conectată, din punct de vedere tehnic, la programul respectiv.

**Cercetătorul independent se află în poziția cea mai incertă**, întrucât acesta nu beneficiază, în prealabil, de nicio autorizare. Delimitarea dintre interacțiunea publică obișnuită și accesul neautorizat trebuie, prin urmare, evaluată ulterior actului tehnic în sine. Consultarea unei pagini web publice sau a unui repozitoriu poate fi efectuată cu drept, în timp ce utilizarea unei credențiale expuse, executarea unei comenzi, accesarea unui punct final restricționat sau accesarea unor date care nu sunt publice pot constitui acces fără drept, chiar și în situația în care vulnerabilitatea a fost descoperită în mod accidental.

**Autorizarea poate rămâne dificil de delimitat în cazul sistemelor care se bazează pe servicii cloud, interfețe externe și componente provenite din lanțul de aprovizionare,** întrucât testarea unei aplicații autorizate poate afecta o infrastructură controlată de o altă entitate. Întinderea autorizării trebuie, așadar, să reflecte arhitectura reală a sistemului.

**Evaluarea trebuie să evite două extreme**. Accesibilitatea publică nu echivalează cu o permisiune nelimitată, însă o configurare nesecurizată nu ar trebui să transforme orice răspuns neașteptat al sistemului într-o faptă penală. Legalitatea cercetării nu depinde, prin urmare, de denumirea acesteia, ci de actul tehnic precis realizat, de sursa și limitele autorizării, de scopul urmărit de cercetător, de efectele produse și de împrejurarea dacă interacțiunea a excedat, în mod conștient, limitele accesului public obișnuit.

## Cercetarea în domeniul securității ca etapă prealabilă necesară a CVD

Cercetarea în domeniul securității nu constituie un act tehnic unitar. Consultarea documentației publice sau a unei fișe CVE presupune o interacțiune redusă sau inexistentă cu ținta vizată. Scanarea identifică serviciile expuse; *fingerprinting*-ul identifică software-ul sau configurația utilizată, iar enumerarea urmărește obținerea unor informații mai detaliate privind resursele accesibile. Testarea autentificării examinează posibilitatea eludării controalelor de acces, în timp ce *fuzzing*-ul sau realizarea unui *proof of concept* poate presupune executarea

unor comenzi, modificarea temporară a unei stări a sistemului sau întreruperea unui serviciu. Riscul juridic crește, în general, pe măsură ce cercetarea trece de la observația pasivă la interacțiunea cu resurse restricționate, la accesarea de date sau la producerea unor efecte asupra funcționării sistemului. Tratarea fiecărei etape drept echivalentă cu celelalte estompează atât realitatea tehnică, cât și conduita efectivă a cercetătorului.

Raportul explicativ al Convenției de la Budapesta oferă două limite utile în acest sens. Accesul presupune penetrarea integrală sau parțială a unui sistem astfel încât simpla transmitere a unui mesaj sau a unui fișier nu constituie, în sine, acces. Utilizarea unui instrument tehnic nu este, prin ea însăși, ilicită, iar interacțiunea cu un sistem liber accesibil publicului poate fi realizată cu drept (Council of Europe, 2001b, pct. 46-48). Îndrumările de la nivel românesc ar trebui construite pe baza acestei distincții. Ele ar trebui să separe interacțiunea publică obișnuită de testarea activă, de accesul la resurse restricționate, de accesul la date, precum și de persistența în sistem, modificarea și perturbarea acestuia. Un cercetător trebuie să întrerupă investigația de îndată ce dispune de suficiente dovezi, însă legea trebuie să permită un nivel de verificare suficient pentru a distinge o vulnerabilitate reală de o simplă suspiciune.

## MECANISMUL DE RAPORTARE AL ROMÂNIEI ȘI PROTECȚIA JURIDICĂ ÎN CURS DE FORMARE

### De la implicarea internațională timpurie la coordonarea națională

Implicarea României în procesul de CVD precedă ordonanța din 2024. Alături de Ungaria și Olanda, România a participat la o inițiativă dezvoltată în cadrul Global Forum on Cyber Expertise, având ca obiect schimbul de experiență privind divulgarea responsabilă și coordonată a vulnerabilităților. Această inițiativă a contribuit la un proiect regional care a implicat Cehia, Ungaria, Olanda și România și care a urmărit operaționalizarea unei măsuri de consolidare a încrederii adoptate în cadrul Organizației pentru Securitate și Cooperare în Europa, privind raportarea responsabilă a vulnerabilităților (ENISA, 2022, 28-33).

DNSC a operat, de asemenea, un mecanism intern de raportare și a acționat ca terț de încredere în anumite procese de divulgare. Cu toate acestea, ENISA a constatat că România nu implementase o politică națională de CVD la momentul colectării informațiilor relevante, în

2021 (ENISA, 2022, 32-33). România nu s-a aflat într-o situație izolată. ENISA a identificat un peisaj european fragmentat, în care doar un grup restrâns de state membre implementaseră cerințe de politică națională în această materie. Mai important, **șaptesprezece state membre consultate au identificat dreptul penal drept cel mai presant obstacol juridic în calea CVD, aspect care a determinat ENISA să recomande statelor „să definească rolul hackerilor etici în legislația națională relevantă”** (ENISA, 2022, 7, 62-63).

**Strategia de Securitate Cibernetică a României pentru perioada 2022-2027** a oferit fundamentul politic al reformei, punând accentul pe reziliență, cercetare, cooperare public-privat-mediul academic, schimbul de informații și diplomația cibernetică (Romanian Government, 2021, secț. 4.1-4.5). **Strategia a furnizat justificarea politică pentru CVD, fără a oferi, însă, claritatea juridică de care cercetătorii au nevoie în practică.** În plus, nu a precizat care anume acte tehnice pot fi efectuate anterior raportării unei vulnerabilități, nici ce protecție decurge dintr-o conduită responsabilă.

**Transpunerea Directivei NIS2 prin Ordonanța de urgență nr. 155/2024**

Ordonanța de urgență nr. 155/2024 a conferit CVD un loc statutar în cadrul guvernanței securității cibernetice românești și a fost ulterior aprobată și modificată prin Legea nr. 124/2025. Articolul 23 impune ca politica națională de securitate cibernetică să abordeze CVD, cercetarea și dezvoltarea, formarea de competențe, securitatea lanțului de aprovizionare și cooperarea dintre actorii publici, privați și mediul academic, în timp ce articolul 25 împuternicește DNSC să reglementeze și să administreze procesul național de CVD.

Articolul 36 desemnează DNSC drept CSIRT național responsabil de CVD și drept intermediar de încredere între autorul raportării vulnerabilității și producătorul sau furnizorul produsului ori serviciului TIC potențial vulnerabil. DNSC poate primi și evalua raportări, poate facilita raportarea anonimă, poate identifica entitățile afectate, poate pune în legătură părțile implicate și poate sprijini verificarea în colaborare cu furnizorul responsabil (Romanian Government, 2024, art. 36 alin. (1)-(2)). DNSC poate, de asemenea, negocia termenele de divulgare și de remediere atunci când sunt afectate mai multe entități, poate coopera cu ceilalți membri ai Rețelei CSIRT-urilor UE în cazurile cu impact transfrontalier semnificativ și poate emite proceduri, norme tehnice și îndrumări destinate autorilor raportărilor, entităților afectate și programelor private de divulgare a vulnerabilităților. Orice persoană fizică sau juridică poate

raporta o vulnerabilitate către DNSC, sub rezerva respectării legislației aplicabile (Guvernul României, 2024, art. 36 alin. (2)-(3)).

Legea adoptată în iunie 2026 ar impune, de asemenea, DNSC obligația de a consulta un comitet fără personalitate juridică, alcătuit din autoritățile responsabile în domeniul securității cibernetice, apărării, ordinii publice și activității de informații, în temeiul Legii nr. 58/2023. Chiar dacă această măsură ar putea consolida coordonarea interinstituțională, raportul acesteia cu mecanismele deja instituite prin articolul 39 din Ordonanța de urgență nr. 155/2024 ar trebui clarificat, astfel încât DNSC să își păstreze rolul de intermediar civil de încredere în materie de CVD (Romanian Parliament 2026; Romanian Legislative Council 2026, 2-4).

În temeiul Legii nr. 124/2025, producătorii și furnizorii care au calitatea de entități esențiale sau importante au obligația de a informa DNSC cu privire la vulnerabilitățile identificate de aceștia sau primite de la terți și de a le remedia într-un termen convenit cu DNSC (Parlamentul României, 2025). Astfel, cercetătorii nu mai trebuie să identifice și să convingă, în mod individual, fiecare actor afectat. Raportarea anonimă este posibilă, iar mecanismul recunoaște faptul că o singură componentă poate afecta mai mulți furnizori și mai multe jurisdicții. DNSC poate, prin urmare, reduce asimetriile informaționale și costurile de coordonare pe care cercetătorii, acționând individual, nu le-ar putea depăși. **Mecanismul nu determină, însă, legalitatea cercetării care a precedat raportarea.**

**Conduita responsabilă în temeiul articolului 36**

Pe lângă instituirea unui canal de raportare, articolul 36 prevede și condiții minime pentru cercetarea care precedă o raportare. **Cercetarea trebuie desfășurată cu bună-credință, exclusiv în scopul îmbunătățirii securității cibernetice și în conformitate cu legislația aplicabilă.** Aceasta nu poate implica accesul neautorizat la conținutul fișierelor sau copierea acestuia, ștergerea ori modificarea datelor, atacuri de tip *brute-force*, inginerie socială, întreruperea serviciilor, utilizarea de *malware* sau tehnici care afectează disponibilitatea sistemelor. Vulnerabilitatea trebuie raportată în termen de 48 de ore de la identificare și nu poate fi divulgată public fără acordul DNSC (Romanian Government, 2024, art. 36 alin. (5)-(6)).

Entitățile esențiale și importante trebuie să instituie procese pentru primirea, evaluarea și remedierea raportărilor privind vulnerabilități, să coopereze cu DNSC și să publice datele de

contact, precum și condițiile de raportare. Articolul 36 impune, astfel, obligații atât cercetătorilor, cât și entităților vizate: cercetătorii trebuie să reducă la minimum eventualele prejudicii, în timp ce entitățile vizate trebuie să fie în măsură să primească, să evalueze și să acționeze în urma raportărilor primite. **Aceste condiții sunt conforme cu principiile recunoscute ale cercetării responsabile, printre care proporționalitatea și minimizarea datelor colectate.** Totodată, acestea delimitează cercetarea de șantaj, de interferența distructivă și de exploatarea malițioasă (Romanian Government, 2024, art. 3 alin. (1) lit. b) și art. 36 alin. (5)-(6)).

Cu toate acestea, articolul 36 impune conformitatea cu legislația în vigoare și păstrează aplicabilitatea Codului penal, a GDPR și a altor regimuri juridice (Romanian Government, 2024, art. 2 alin. (5), astfel cum a fost modificat prin Legea adoptată de Parlamentul României, 2025, pct. 1). Articolul 36, în sine, nu prevede că respectarea acestor condiții exclude răspunderea penală sau civilă. Acest vid legislativ ar fi urmat să fie acoperit prin reforma legislativă adoptată de Parlament în iunie 2026, examinată în cele ce urmează.

## Sub rezerva promulgării: protecția legală condiționată a cercetării vulnerabilităților[3]

La momentul redactării prezentei lucrări, Parlamentul României a adoptat o lege de completare a articolului 36 din Ordonanța de urgență nr. 155/2024 și de introducere a unui nou articol 365¹ în Codul penal. Sub rezerva promulgării, publicării și intrării în vigoare, cadrul legal existent rămâne aplicabil. Dispoziția propusă prevede că faptele care se circumscriu articolelor 360 alin. (1) și (3), 361 și 364 nu ar constitui infracțiune atunci când o persoană fizică sau juridică întrunește, cumulativ, condițiile privind cercetarea vulnerabilităților și raportarea acestora, prevăzute la articolul 36 alin. (5) și (6) (Romanian Parliament, 2026).

**Întinderea limitată a articolului 365¹** reflectă istoricul legislativ al reformei. Propunerea inițială ar fi urmat să se aplice tuturor infracțiunilor reglementate de articolele 360-365 din Codul penal. Consiliul Legislativ a emis un aviz negativ, motivând că mai multe dintre aceste infracțiuni erau incompatibile cu condițiile cumulative prevăzute la articolul 36 alin. (5) și (6), care interzic modificarea datelor, perturbarea serviciilor și alte forme de conduită dăunătoare. Comisiile parlamentare au restrâns, ulterior, sfera de aplicare a dispoziției la

[3] Acest articol reflectă cadrul legislativ la data de 30 iunie 2026, data la care a fost finalizat manuscrisul.

articolele 360 alin. (1) și (3), 361 și 364. Raportul comisiilor a recunoscut, totuși, că cercetarea legitimă a vulnerabilităților poate presupune, în mod inevitabil, o formă de interacțiune cu un sistem informatic, primirea sau transferul incidental de date, precum și utilizarea unor instrumente specializate. Raportul nu este pe deplin consecvent în privința articolului 360 alin. (2): **motivarea sa arată că această infracțiune nu ar trebui exclusă în mod absolut de la protecție, însă textul modificat și adoptat nu o include.** Sfera finală de aplicare reprezintă, astfel, o încercare de a distinge consecințele tehnice incidentale ale unei testări legitime de conduitele a căror simplă realizare ar contraveni, prin ea însăși, condițiilor cercetării responsabile (Romanian Legislative Council, 2026, 4-6; Romanian Senate, 2026, 2-4 și anexă).

Reforma reprezintă o schimbare semnificativă în abordarea românească a acestei materii. Conformitatea cu articolul 36 nu ar mai funcționa exclusiv ca un ansamblu de cerințe privind conduita responsabilă, ci ar produce un efect substanțial expres în materia dreptului penal. Dispoziția ar proteja anumite forme de cercetare a vulnerabilităților fără a impune, în mod expres, o autorizare prealabilă din partea organizației afectate. România ar trece, astfel, dincolo de un mecanism de raportare susținut doar prin interpretare de la caz la caz și prin marja de apreciere a organelor de urmărire penală, către o protecție legală condiționată.

**Restrângerea sferei infracțiunilor incluse nu elimină, însă, toate problemele de legalitate.** În cursul procesului legislativ, Ministerul Afacerilor Interne a observat că protecția propusă nu era autonomă, întrucât depindea de conformitatea cu condiții prevăzute în Ordonanța de urgență nr. 155/2024, aspect care ar putea afecta previzibilitatea și stabilitatea impuse legii penale. Ministerul Justiției a considerat că formularea inițială risca o dezincriminare excesiv de largă a infracțiunilor informatice, în timp ce DNSC a susținut instituirea protecției, solicitând, în același timp, corectarea infracțiunilor cărora aceasta li s-ar aplica**. Aceste poziții explică atât formularea finală restrictivă, cât și necesitatea persistentă a unor îndrumări administrative și de urmărire penală detaliate** (Romanian Senate, 2026, 2-4).

Protecția ar rămâne, cu toate acestea, specifică anumitor infracțiuni, fără a constitui o exonerare de răspundere cu aplicabilitate generală. Aceasta nu ar cuprinde, în mod expres, accesul realizat în scopul obținerii de date informatice în sensul articolului 360 alin. (2), alterarea integrității datelor în sensul articolului 362, perturbarea funcționării sistemelor informatice în sensul articolului 363 sau operațiunile ilegale cu dispozitive ori programe

informatice în sensul articolului 365. De asemenea, aceasta nu ar clarifica, în mod expres, regimul tentativei prevăzute la articolul 366 și nu ar oferi protecție împotriva răspunderii civile. Eficacitatea sa practică ar depinde, la rândul său, de modul de interpretare a condițiilor cumulative prevăzute la articolul 36, în special de termenul de 48 de ore pentru raportare și de restricțiile privind actele tehnice necesare pentru verificarea unei vulnerabilități.

**Chestiunile nerezolvate din cuprinsul articolului 36**

Aceste ambiguități dobândesc, în prezent, o semnificație directă în materie de drept penal, întrucât protecția propusă prin articolul 365[1] ar depinde de conformitatea cumulativă cu articolul 36 alin. (5) și (6) (Romanian Parliament, 2026).

**În primul rând, se pune întrebarea când începe să curgă termenul de 48 de ore.** Identificarea unei vulnerabilități este, adesea, un proces gradual: cercetătorul poate observa, inițial, un comportament anormal al sistemului și poate confirma abia ulterior că deficiența este reproductibilă și relevantă din perspectiva securității. O interpretare rigidă, care ar face să curgă termenul de la prima anomalie observată, ar putea încuraja raportări premature și incomplete. Termenul ar trebui, mai degrabă, să se aplice unei notificări inițiale transmise după o confirmare rezonabilă, cu posibilitatea comunicării ulterioare a unor informații tehnice suplimentare.

**În al doilea rând, se impune stabilirea a ceea ce constituie eludarea unei bariere tehnice.** Atacurile de tip *brute-force*, *phishing*-ul și ingineria socială pot fi excluse fără dificultate, însă anumite vulnerabilități constau chiar în posibilitatea de a eluda un control de autentificare sau de autorizare. DNSC ar trebui să distingă între tentativa de a compromite o măsură de protecție funcțională și demonstrația minimă a faptului că respectiva măsură nu funcționează conform destinației sale.

**În al treilea rând, se pune problema duratei pentru care divulgarea poate fi amânată.** Confidențialitatea temporară este necesară pe perioada pregătirii unei corecții, însă articolul 36 nu prevede nicio limită exterioară a perioadei în care DNSC poate refuza autorizarea publicării informațiilor privind vulnerabilitatea. În absența unei proceduri de revizuire și a unor termene prezumate, coordonarea riscă să se transforme într-un embargo nedefinit, lăsând utilizatorii în imposibilitatea de a-și evalua propria expunere la risc.

**În sfârșit, articolul 2 exclude din sfera sa de aplicare instituțiile** din domeniul apărării, ordinii publice și securității naționale, Ministerul Afacerilor Externe, Oficiul Registrului Național al Informațiilor Secrete de Stat, entitățile cu atribuții de aplicare a legii, precum și sistemele care procesează informații clasificate. Aceste excluderi sunt de înțeles, având în vedere sensibilitatea sistemelor în cauză, însă ele împiedică articolul 36 să ofere o cale uniformă pentru întregul sector public. Sunt necesare proceduri speciale echivalente, astfel încât vulnerabilitățile care afectează instituțiile excluse să poată fi raportate în condiții de siguranță, fără expunerea unor informații operaționale sau clasificate.

| Instrument | Contribuția principală | Lacuna rămasă |
|---|---|---|
| Strategia de Securitate Cibernetică 2022-2027 | Stabilește reziliența, cercetarea, cooperarea public-privată și diplomația cibernetică drept priorități naționale. | Nu determină statutul juridic al cercetătorilor în domeniul securității. |
| Ordonanța de urgență nr. 155/2024 | Desemnează DNSC drept coordonator al CVD și reglementează raportarea, coordonarea și obligațiile entităților. | Condițiile privind cercetarea și raportarea rămân deschise interpretării și nu abordează răspunderea civilă. |
| Codul penal, articolele 360-366 și proiectul de articol 365 | Protejează sistemele și datele împotriva infracțiunilor informatice; articolul 365[1] propus ar exclude, condiționat, caracterul infracțional al unor fapte determinate, în conformitate cu articolul 36. | Ar exclude mai multe infracțiuni și nu ar aborda în mod expres tentativa sau răspunderea civilă. |
| Legea nr. 361/2022 | Protejează anumite raportări efectuate într-un context profesional. | Nu instituie un drept general la cercetarea independentă a vulnerabilităților. |
| NIS2, CRA și EUVD | Consolidează coordonarea națională, securitatea produselor și informațiile europene privind vulnerabilitățile. | Nu creează o protecție uniformă de drept penal la nivel european. |

Tabelul 1. Principalele contribuții și lacune rămase în cadrul juridic și instituțional al României privind CVD și cercetarea în domeniul securității.

## CÂND CERCETAREA ÎN DOMENIUL SECURITĂȚII SE ÎNTÂLNEȘTE CU DREPTUL PENAL ROMÂN

### Răspunderea de fond și reacția organelor de urmărire penală

Cercetarea vulnerabilităților ridică două întrebări distincte de drept penal. Prima este de natură **substanțială** și privește dacă actele tehnice îndeplinite de cercetător întrunesc elementele constitutive ale accesului ilegal sau ale unei alte infracțiuni informatice. A doua

este de natură **procedurală** și privește dacă urmărirea penală ar trebui să fie declanșată în situația în care cercetătorul a acționat cu scop defensiv, a limitat testarea la ceea ce era necesar și a raportat cu promptitudine vulnerabilitatea. O conduită poate să se circumscrie textului unei infracțiuni definite în termeni largi și, în același timp, să prezinte trăsături care pledează împotriva urmăririi penale (Pupillo et al., 2018, 43-46).

O decizie a organelor de urmărire penală de a nu declanșa urmărirea penală nu implică, în mod necesar, că fapta a fost legală, în timp ce o cauză justificativă prevăzută de lege modifică natura juridică substanțială a conduitei respective. În sens invers, existența unei infracțiuni definite în termeni largi nu impune autorităților să ignore scopul, proporționalitatea sau absența unui prejudiciu atunci când decid dacă o cauză justifică cercetarea și urmărirea penală. Reforma adoptată de România deplasează întrebarea de la aceea dacă ar trebui să existe o cauză justificativă legală, la aceea a modului în care condițiile, limitele și raportul acesteia cu marja de apreciere a organelor de urmărire penală ar trebui interpretate.

**„Accesul fără drept" în sensul Convenției de la Budapesta**

Convenția de la Budapesta constituie unul dintre principalele fundamente internaționale ale infracțiunilor informatice din dreptul român. Articolul 2 impune fiecărei părți obligația de a incrimina accesul intenționat, integral sau parțial, la un sistem informatic, realizat fără drept, permițând, în același timp, statelor să adauge condiții restrictive, precum încălcarea unor măsuri de securitate, intenția de a obține date, o altă intenție frauduloasă sau existența unei legături între sisteme informatice (Council of Europe, 2001a, art. 2).

Expresia „fără drept" delimitează accesul de natură penală de conduita autorizată, permisă de lege sau justificată în alt mod. Raportul explicativ precizează că accesul autorizat în vederea testării de securitate sau a protecției sistemului este realizat cu drept și că utilizarea unui instrument tehnic nu conferă un caracter ilicit accesului, atunci când sistemul este liber accesibil publicului (Council of Europe, 2001b, pct. 38, 47-48). Expresia respectivă lasă, prin urmare, loc autorizării legale și altor cauze justificative recunoscute.

**Autorii Convenției au recunoscut, totuși, existența unor controverse privind incriminarea simplului acces.** Unele state au considerat că pătrunderea neautorizată este, în sine, dăunătoare, în timp ce altele au susținut că simpla pătrundere nu produce, în mod necesar, un prejudiciu și poate, dimpotrivă, să evidențieze deficiențe de securitate. Articolul 2 permite,

astfel, părților să restrângă sfera infracțiunii, prin condiționarea acesteia de încălcarea unor măsuri de securitate sau de existența unei intenții determinate (Council of Europe, 2001b, pct. 49-50). În consecință, **Convenția instituie un standard minim de incriminare, lăsând, în același timp, o marjă substanțială de apreciere legislației interne.** Ea nu instituie nici un statut al cercetătorului etic, nici un mijloc de apărare direct în favoarea cercetătorilor de bună-credință, lăsând, în mare măsură, semnificația noțiunilor de autorizare, intenție, necesitate și justificare în sarcina dreptului național.

**Sfera largă a infracțiunii de „acces fără drept" în dreptul român**

**Articolul 360 alin. (1) din Codul penal român incriminează accesul fără drept, chiar și în situația în care nu sunt obținute date și nu se produce niciun prejudiciu.** Pedepsele sunt majorate atunci când scopul urmărit este obținerea de date sau atunci când sistemul este protejat prin măsuri speciale de restricționare a accesului (Romanian Parliament, 2009, art. 360). Infracțiunea este, prin urmare, centrată pe însăși pătrunderea neautorizată, și nu pe o consecință dăunătoare determinată.

Infracțiunea prevăzută de dreptul român nu impune eludarea unei măsuri de securitate. **Sfera sa de aplicare este, astfel, mai largă decât infracțiunea minimă** impusă de articolul 3 din Directiva 2013/40/UE, care condiționează răspunderea de încălcarea unei măsuri de securitate, cel puțin în cazurile care nu sunt minore. Comisia Europeană a identificat România printre statele membre ale căror dispoziții nu impuneau eludarea unei astfel de măsuri pentru stabilirea răspunderii (European Commission, 2017). Un cercetător poate face, astfel, obiectul unei anchete penale, chiar și atunci când nu a trecut de vreo barieră tehnică, control de securitate sau parolă.

Articolul 35 alin. (2) din Legea nr. 161/2003 definește accesul fără drept ca fiind accesul realizat fără o autorizare legală sau contractuală, dincolo de limitele unei autorizări existente sau fără permisiunea persoanei îndreptățite să controleze sistemul. Cu toate că definiția menționează **cercetarea științifică** printre operațiunile pentru care permisiunea poate fi relevantă, aceasta nu instituie un privilegiu general al cercetării. Ea confirmă, dimpotrivă, faptul că cercetarea desfășurată în interiorul unui sistem informatic necesită, în mod obișnuit, un temei legal, contractual sau consensual (Romanian Parliament, 2003, art. 35 alin. (2)). Un

scop defensiv poate susține constatarea bunei-credințe, fără a înlocui, în mod necesar, autorizarea.

**În termeni simpli, un scop benefic nu exclude, în mod necesar, intenția penală**. Un cercetător poate efectua, în mod deliberat, o testare pentru a îmbunătăți securitatea, cunoscând, în același timp, că autorizarea ar putea să nu existe. Până la intrarea în vigoare a articolului 365[1] propus, buna-credință poate influența evaluarea cauzei sau decizia de urmărire penală, fără a exclude, în mod necesar, existența infracțiunii.

În cursul procesului legislativ, Consiliul Superior al Magistraturii a făcut trimitere, de asemenea, la articolul 21 din Codul penal, potrivit căruia exercitarea unui drept sau îndeplinirea unei obligații poate justifica o conduită care ar fi, altfel, infracțională. Această cauză justificativă generală nu instituie, prin ea însăși, un drept al cercetătorului independent de a testa sistemul unui terț fără autorizare prealabilă; ea presupune, dimpotrivă, existența prealabilă a dreptului sau a obligației respective (Superior Council of Magistracy, 2026, 1-2).

**Infracțiuni care exced accesul ilegal**

Cercetarea poate interacționa, de asemenea, cu articolele 361-365 din Codul penal. Interceptarea unui trafic care nu este public se poate circumscrie articolului 361; modificarea sau ștergerea datelor se poate circumscrie articolului 362; blocarea unui serviciu prin *fuzzing* sau prin cereri automatizate se poate circumscrie articolului 363, iar copierea, chiar și a unui eșantion redus dintr-o bază de date, în scopul demonstrării deficienței, se poate circumscrie articolului 364. Articolul 365 privește instrumentele, parolele și programele deținute sau distribuite în scopul comiterii acestor infracțiuni.

O testare poate trece de la o infracțiune la alta de îndată ce afectează comunicațiile, datele, disponibilitatea sistemului sau credențialele de acces. Scanerele, depanatoarele (*debuggers*), platformele destinate exploatării vulnerabilităților și programele de audit al parolelor constituie instrumente cu dublă utilizare, a căror deținere și utilizare trebuie evaluată în funcție de scopul urmărit, de autorizare și de conduita efectivă.

Articolul 6 alin. (2) din Convenția de la Budapesta consacră, în mod expres, această distincție. Incriminarea utilizării abuzive a dispozitivelor nu ar trebui să se extindă asupra producerii, distribuirii sau deținerii acestora, atunci când acestea nu sunt destinate comiterii unei infracțiuni, inclusiv în cazul testării autorizate sau al protecției sistemului (Council of

Europe, 2001a, art. 6 alin. (2); Council of Europe, 2001b, pct. 76-77). **A trata simpla deținere a unui instrument de securitate ca fiind suspectă ar echivala cu incriminarea unei practici profesionale obișnuite.**

**Tentativa și incriminarea cercetării nereușite**

Dreptul român sancționează, de asemenea, tentativa de a comite infracțiunile informatice reglementate în Capitolul VI. Un cercetător se poate, prin urmare, expune unui risc juridic chiar și atunci când o testare eșuează și nu are loc niciun acces, nicio extragere de date și nicio perturbare a sistemului (Romanian Parliament, 2009, art. 366). Acest aspect este important deoarece activitățile de cercetare implică deseori încercarea de a determina dacă accesul este posibil. Noțiunea de tentativă privește trecerea în cadrul *iter criminis*[4] de la conduita pregătitoare la începerea executării unei infracțiuni. În temeiul articolului 32 din Codul penal, tentativa există atunci când executarea faptei intenționate a început, dar a fost întreruptă sau nu și-a produs efectul. Actele pregătitoare nu sunt, în mod automat, sancționabile, însă conduita orientată direct către finalizarea faptei poate fi.

Această distincție prezintă o importanță deosebită în materia cercetării vulnerabilităților. O scanare generală a porturilor sau o cerere obișnuită nu ar trebui să echivaleze, în mod automat, cu o tentativă de acces ilegal, întrucât o astfel de acțiune poate doar să evidențieze existența unui serviciu, fără a pătrunde în sistem. În schimb, o tentativă direcționată de a eluda autentificarea, de a exploata o vulnerabilitate determinată, de a accesa un punct final restricționat sau de a executa un *proof of concept* poate constitui începerea executării infracțiunii, chiar și în absența obținerii efective a accesului, în funcție de circumstanțele tehnice și de intenția cercetătorului. Raportul explicativ al Convenției de la Budapesta face, la fel, distincția dintre penetrarea efectivă și simpla transmitere a unui mesaj sau a unui fișier (Council of Europe, 2001b, pct. 46).

**Abordarea românească este mai strictă decât standardul minim impus de Convenția de la Budapesta,** al cărei articol 11 nu obligă statele să incrimineze tentativa de acces ilegal în sensul articolului 2 (Council of Europe 2001a, art. 11(2); Council of Europe 2001b, para. 120). Același *proof of concept* nereușit poate constitui, astfel, un act pregătitor

[4] *Iter criminis* se referă la etapele succesive prin care se poate dezvolta o infracțiune, de la pregătire până la începutul executării, consumare și, acolo unde este cazul, producerea rezultatului urmărit.

nepedepsit într-o jurisdicție și o tentativă pedepsită în alta, chiar dacă conduita tehnică este identică. Absența unei referiri expres la articolul 366 în cuprinsul articolului 365[1] propus poate lăsa, prin urmare, incert tratamentul juridic al cercetării vulnerabilităților care nu s-a finalizat cu succes, dar care respectă, în celelalte privințe, condițiile impuse (Romanian Parliament, 2026).

## De ce protecția avertizorilor de integritate nu este suficientă pentru cercetătorii de securitate

**Cercetătorii de securitate sunt, uneori, comparați cu avertizorii de integritate, întrucât amândoi pot divulga informații de interes public.** Legea română nr. 361/2022 reglementează încălcările privind securitatea rețelelor și a sistemelor informatice și protejează persoanele care obțin informații relevante într-un context profesional (Romanian Parliament, 2022, art. 2-3).

Articolul 21 poate proteja raportarea sau divulgarea informațiilor, precum și accesul la informații disponibile în exercitarea atribuțiilor profesionale, în măsura în care un astfel de acces este necesar pentru realizarea raportării, fără a proteja, însă, acte lipsite de legătură cu aceasta sau nenecesare (Romanian Parliament, 2022, art. 21). Un angajat care întâlnește o vulnerabilitate în cursul unei activități autorizate poate fi, astfel, protejat, în timp ce un cercetător extern, care nu se află într-o relație profesională cu entitatea vizată, nu beneficiază, în general, de această protecție. Legea nu justifică, de asemenea, în mod automat, etapele tehnice îndeplinite anterior momentului în care persoana dobândește calitatea de autor protejat al unei raportări.

Legislația privind protecția avertizorilor de integritate protejează, în principal, persoana care raportează informații dobândite în cursul activității profesionale. CVD trebuie, însă, să abordeze și situația persoanei care descoperă și validează, în mod independent, o deficiență. Cele două regimuri se pot suprapune parțial, însă niciunul nu îl poate substitui pe celălalt.

## Drepturile fundamentale ca garanții și nu ca imunități

Libertatea cercetării științifice protejează urmărirea cunoașterii, în timp ce libertatea de exprimare protejează comunicarea rezultatelor cercetării. Aceste interese prezintă o pondere

deosebită atunci când cercetarea evidențiază riscuri pentru siguranța publică (United Nations 1966, art. 15; European Union 2012, arts. 11 and 13; Council of Europe 1950, art. 10). Aceste drepturi consolidează securitatea juridică și proporționalitatea, fără a institui, însă, o prerogativă nelimitată de a accesa sisteme aparținând altor persoane. Restricțiile privind cercetarea și publicarea trebuie, cu toate acestea, să urmărească scopuri legitime, să fie previzibile și să rămână proporționale.

## GUVERNANȚA EUROPEANĂ ȘI INTERNAȚIONALĂ, ÎN ABSENȚA UNEI PROTECȚII COMUNE PENTRU CERCETĂTORI

### Expunerea cercetătorului în temeiul Directivei NIS2

Politicile publice europene a identificat problema din amonte încă înaintea Directivei NIS2. Îndrumările ENISA din 2016 au descris efectele neintenționate ale răspunderii penale și civile drept un obstacol major în calea divulgării vulnerabilităților. Comunicarea Comisiei din 2017 privind securitatea cibernetică a solicitat recunoașterea rolului cercetătorilor de securitate din partea terților, precum și instituirea unor condiții care să susțină CVD la nivelul statelor membre. Grupul de lucru CEPS a recomandat, ulterior, un cadru european, completat de legislația națională și fundamentat pe standardele ISO/IEC 29147 și ISO/IEC 30111, în vederea asigurării clarității juridice, atât pentru descoperire, cât și pentru divulgare (ENISA 2016; European Commission and High Representative 2017, 6; NIS Cooperation Group 2023; Pupillo et al. 2018).

Dreptul Uniunii Europene instituie un standard minim de drept penal, lăsând, însă, protecția cercetătorilor, în mare măsură, în sarcina statelor membre. Directiva 2013/40/UE exclude din noțiunea de „acces fără drept” accesul autorizat prin lege sau de titularul dreptului, însă infracțiunile naționale continuă să difere în privința tratamentului măsurilor de securitate, al intenției și al autorizării (European Parliament and Council, 2013; European Commission, 2017). Directiva NIS2 depășește simpla incriminare, impunând statelor membre obligația de a promova CVD prin strategii naționale și de a desemna un CSIRT în măsură să primească raportări, să păstreze anonimatul, să faciliteze comunicarea și să coopereze în cazurile transfrontaliere (European Parliament and Council, art. 7 și 12). Considerentul 60 recunoaște, în mod expres, faptul că cercetătorii se pot expune răspunderii penale și civile și încurajează

**„statele membre să adopte orientări privind neurmărirea penală a cercetătorilor în domeniul securității informatice”**. Un considerent nu constituie, însă, un mijloc de apărare executoriu, astfel încât Directiva NIS2 identifică problema fără a acoperi, în mod efectiv, vidul legislativ existent (European Parliament and Council, 2022, considerentul 60).

Directiva NIS2 constituie, de asemenea, temeiul juridic al **Bazei de Date Europene privind Vulnerabilitățile** (EUVD). Operațională din mai 2025, EUVD centralizează informații privind produsele afectate, gravitatea vulnerabilităților, stadiul exploatării acestora și măsurile de remediere disponibile, fiind accesibilă autorităților, furnizorilor, cercetătorilor și publicului. EUVD îmbunătățește informațiile disponibile privind vulnerabilitățile, fără a determina, însă, legalitatea cercetării care le-a produs. Europa dezvoltă, prin urmare, o hartă tot mai precisă a vulnerabilităților, fără a dispune, în aceeași măsură, de o hartă coerentă a protecției juridice de care beneficiază persoanele care le descoperă.

Dreptul european reglementează, prin urmare, într-o măsură tot mai extinsă, ceea ce autoritățile, bazele de date și producătorii trebuie să facă din momentul în care informația privind o vulnerabilitate există deja, în timp ce condițiile în care cercetătorii pot produce, în mod legal, această informație rămân fragmentate. Furnizorii aflați în jurisdicții cu un cadru legal incert pot primi, în consecință, mai puține raportări, o cooperare tehnică redusă și alerte întârziate privind deficiențele cu impact transfrontalier (ENISA, 2016; ENISA, 2022; NIS Cooperation Group, 2023).

## Responsabilitatea privind produsele în temeiul Regulamentului privind reziliența cibernetică

Regulamentul privind reziliența cibernetică (CRA – Cyber Resilience Act) instituie noi responsabilități în sarcina producătorilor de produse cu elemente digitale, impunându-le obligația de a concepe produsele având în vedere securitatea cibernetică, de a menține procese de gestionare a vulnerabilităților, de a asigura puncte de contact și de a emite actualizări de securitate pe durata perioadei de asistență. Începând cu 11 septembrie 2026, producătorii vor avea obligația de a raporta vulnerabilitățile exploatate activ și incidentele grave prin intermediul Platformei Unice de Raportare a ENISA, în general printr-o alertă inițială transmisă în termen de 24 de ore și printr-o notificare completă transmisă în termen de 72 de ore (European Parliament and Council, 2024, art. 14-16).

Aceste obligații conferă o importanță deosebită pentru produsele durabile și interconectate care se încadrează în domeniul de aplicare al Regulamentului, inclusiv sistemele industriale și dispozitivele destinate consumatorilor din domeniul internetului obiectelor (*Internet of Things*). Software-ul acestor produse poate rămâne în uz timp de mulți ani, în condițiile în care furnizorii, dependențele tehnice și amenințările evoluează. O gestionare eficientă a vulnerabilităților necesită, prin urmare, atât testarea internă anterioară introducerii pe piață, cât și capacitatea continuă de a primi și de a acționa în urma raportărilor primite de la cercetători externi, pe întreaga durată a perioadei de asistență (Parlamentul European și Consiliul, 2024; Pupillo et al., 2018). Regulamentul privind reziliența cibernetică consolidează obligațiile producătorilor în materia gestionării vulnerabilităților, fără a determina, însă, statutul de drept penal al cercetătorilor externi și fără a autoriza testarea de către terți.

Cadrul normativ rămâne, astfel, complementar, dar incomplet: CRA impune producătorilor obligația de a acționa, mecanismele naționale de CVD indică cercetătorilor unde trebuie să raporteze, iar dreptul național trebuie, în continuare, să determine momentul în care cercetarea care precedă raportarea beneficiază de protecție juridică.

**Legea privind securitatea cibernetică și certificarea**

Legea privind securitatea cibernetică (EU Cybersecurity Act) contribuie, în mod indirect, prin intermediul schemelor europene de certificare în materie de securitate cibernetică. Certificarea poate impune evaluarea vulnerabilităților, testarea de securitate și proceduri de gestionare a deficiențelor nou descoperite. Schema europeană Common Criteria, de exemplu, impune titularilor de certificate obligația de a menține procese de gestionare a vulnerabilităților și de a răspunde informațiilor relevante privind produsele certificate.

Certificarea poate susține procedurile de gestionare a vulnerabilităților, fără a garanta, însă, siguranța continuă a unui produs și fără a proteja cercetătorii independenți. Certificarea poate contribui la normalizarea procedurilor de divulgare, impunând titularilor de certificate obligația de a menține puncte de contact și proceduri destinate deficiențelor anterior necunoscute. Ea nu poate substitui, însă, descoperirea independentă, întrucât evaluează un produs într-o configurație determinată, la un moment dat. Cercetarea externă rămâne, astfel, un mecanism corectiv pentru premisele care se dovedesc, ulterior, incomplete.

## Convenția de la Budapesta și limitele armonizării

Convenția de la Budapesta rămâne principalul cadru internațional obligatoriu în materia infracțiunilor informatice și a cooperării privind probele electronice. Terminologia acesteia modelează legislațiile naționale referitoare la acces, interceptare, interferență și utilizare abuzivă a instrumentelor informatice. Cu toate acestea, Convenția a fost concepută, în principal, ca un tratat de incriminare și de cooperare. Aceasta protejează conduita legitimă prin intermediul expresiei „fără drept" și prin interpretările naționale ale noțiunilor de autorizare, intenție și justificare, fără a impune, însă, instituirea unor mecanisme de CVD sau a unor forme de protecție dedicate cercetătorilor.

**Caracterul transnațional al cercetării evidențiază această limitare.** Cercetătorul, sistemul afectat, furnizorul de tehnologie, utilizatorii și infrastructura de găzduire (*hosting*) se pot afla în state diferite, fiecare dintre acestea putându-și afirma competența pe baza conduitei teritoriale, a efectelor produse, a locului unde se află sistemul sau a cetățeniei persoanei implicate. O autorizare valabilă în temeiul unei politici naționale poate, astfel, să nu împiedice declanșarea unei proceduri într-un alt stat, iar o formă de protecție internă nu se aplică în mod automat cercetătorului dincolo de frontierele naționale (Pupillo et al., 2018, p. 46).

Flexibilitatea Convenției a facilitat o participare largă, permițând, în același timp, praguri diferite de incriminare. Tratamentul măsurilor de securitate, al tentativei, al bunei-credințe și al autorizării poate, astfel, varia de la o jurisdicție la alta.

## Cercetarea legitimă în domeniul securității în temeiul Convenției Națiunilor Unite împotriva Criminalității Informatice

Convenția Națiunilor Unite împotriva Criminalității Informatice, adoptată în 2024 (neintrată încă în vigoare), urmează modelul consacrat al incriminării accesului intenționat fără drept, permițând, în același timp, statelor să adauge condiții suplimentare (United Nations, 2024, art. 7). Principala inovație a Convenției, relevantă pentru prezenta lucrare, este articolul 53 alin. (3) lit. e), care recunoaște activitățile legitime de cercetare în domeniul securității, desfășurate exclusiv în scopul consolidării securității și în condițiile prevăzute de dreptul intern (United Nations, 2024, art. 53 alin. (3) lit. e)). **Acest aspect prezintă o importanță politică deosebită, întrucât un instrument global în materia criminalității informatice recunoaște,**

**în prezent, faptul că cercetarea în domeniul securității poate contribui la prevenirea infracțiunilor, iar nu la facilitarea acestora.**

Dispoziția rămâne, totuși, limitată, întrucât figurează printre măsurile preventive, și nu ca o excepție de la infracțiunile de fond, și trimite condițiile protecției către dreptul intern. Ea încurajează protecția, fără a determina, însă, care anume acte tehnice sunt licite. Cu toate acestea, dispoziția oferă României un temei diplomatic suplimentar pentru a susține adoptarea unor standarde naționale și internaționale mai clare.

**Divulgarea responsabilă a vulnerabilităților ca normă cibernetică internațională emergentă?**

Cadrul internațional de politică publică se extinde, de asemenea, dincolo de tratatele privind criminalitatea informatică. Grupul de Experți Guvernamentali al ONU (GGE) a afirmat, în raportul din 2015, că **statele ar trebui să încurajeze raportarea responsabilă a vulnerabilităților TIC și să facă schimb de informații privind soluțiile de remediere disponibile.** Raportul GGE din 2021 a invitat statele să analizeze instituirea unor cadre juridice și de politici publice imparțiale, destinate deciziei privind modul în care ar trebui gestionate vulnerabilitățile. Cu toate că nu au caracter obligatoriu, aceste formulări recunosc raportarea și remedierea vulnerabilităților drept aspecte ale comportamentului responsabil al statelor (United Nations 2015; United Nations 2021).

Statele sunt, prin urmare, chemate nu doar să susțină divulgarea responsabilă în cadrul forurilor diplomatice, ci și să instituie puncte de contact de încredere, proceduri funcționale, securitate juridică și canale pentru schimbul de informații privind măsurile de remediere. Norma respectivă nu instituie o imunitate, însă susține teza potrivit căreia dreptul penal intern nu ar trebui să contravină practicilor de raportare și remediere pe care statele le promovează la nivel internațional (Global Forum on Cyber Expertise 2016; United Nations 2015; United Nations 2021).

Întrucât dreptul european și internațional nu oferă o protecție comună de tip *safe harbour*, sistemele naționale rămân principalele laboratoare pentru protecția cercetătorilor. Belgia, Olanda și Lituania ilustrează, de exemplu, trei modele diferite, care ar putea contribui la evaluarea și rafinarea modelului românesc în curs de formare.

## MODELE COMPARATE DE PROTECȚIE A CERCETĂTORILOR

### Belgia și protecția legală condiționată

**Belgia a legalizat, în mod condiționat, sau, mai exact, a dezincriminat hacking-ul etic.** Începând cu 2023, o persoană fizică sau juridică poate investiga o potențială vulnerabilitate fără consimțământul prealabil al organizației afectate și poate beneficia de protecție, în măsura în care sunt întrunite condițiile prevăzute de lege. Articolele 22 și 23 din Legea belgiană NIS2 din 26 aprilie 2024 detaliază acest cadru normativ, care se aplică inclusiv atunci când organizația nu dispune de o politică de divulgare a vulnerabilităților. Belgia a instituit, astfel, o cauză justificativă legală pentru anumite fapte care ar constitui, altminteri, infracțiuni informatice. Cercetătorul trebuie să acționeze fără intenție frauduloasă sau vătămătoare și să limiteze investigația la ceea ce este necesar și proporțional pentru identificarea și raportarea vulnerabilității.

O notificare simplificată trebuie transmisă, în general, organizației afectate și Centrului Belgian pentru Securitate Cibernetică (CCB) în termen de 24 de ore de la descoperire, urmată de un raport complet în termen de 72 de ore. Divulgarea publică necesită acordul CCB, iar cercetarea privind anumite entități sensibile necesită o autorizare prealabilă suplimentară (CCB, 2025). Atunci când condițiile cumulative sunt întrunite, mecanismul poate proteja cercetătorul atât în temeiul dreptului penal, cât și al dreptului civil belgian.

Articolul 36 din legislația română conține condiții comparabile, printre care buna-credință, absența perturbării sistemului și raportarea promptă. Articolul 365[1] propus ar aduce România mai apropiată de modelul legal belgian, atașând o protecție de drept penal conformării cu aceste condiții. Protecția românească ar rămâne, totuși, mai restrânsă, întrucât s-ar aplica doar unor infracțiuni determinate și nu ar aborda, în mod expres, răspunderea civilă (Romanian Parliament, 2026).

### Modelul olandez, fundamentat pe marja de apreciere a procurorului

Olanda dispune de o politică națională de CVD începând cu anul 2013 și au fost unul dintre primele state europene care au instituționalizat divulgarea responsabilă. Cadrul olandez se bazează pe îndrumări naționale, pe politicile organizaționale de CVD și pe poziția

Ministerului Public, mai degrabă decât pe o protecție legală de tip *safe harbour*. Hacking-ul etic nu constituie o categorie autonomă în dreptul penal olandez; procurorul își păstrează marja de apreciere privind declanșarea urmăririi penale, luând în considerare conformitatea conduitei cu îndrumările privind CVD (Openbaar Ministerie, 2013; ENISA, 2022, 29-30, 64-65).

Evaluarea efectuată de procuror ține seama de interesul social urmărit prin cercetare, de scopul cercetătorului, de subsidiaritate, de proporționalitate și de conduita ulterioară descoperirii vulnerabilității. **Cercetătorii care limitează testarea la ceea ce este necesar, evită accesul sau copierea inutilă a datelor, raportează cu promptitudine și cooperează cu organizația afectată sunt delimitați de persoanele care instituie persistență în sistem, extrag baze de date, solicită plăți sau publică informațiile în mod iresponsabil.**

Îndrumările respective nu exclud, în mod automat, urmărirea penală, însă oferă Ministerului Public un cadru consacrat pentru a distinge cercetarea de securitate benefică din punct de vedere social de intruziunea de natură penală. Modelul oferă flexibilitate, întrucât procurorii pot lua în considerare conduita de ansamblu a cercetătorului, însă protecția rămâne discreționară și nu constituie o imunitate executorie. Acesta oferă, prin urmare, un grad de securitate juridică mai redus decât cauza justificativă legală instituită în dreptul belgian, în special în cauzele transnaționale, demonstrând, totodată, modul în care o practică stabilă a Ministerului Public și îndrumări naționale publicate pot reduce riscul de a trata cercetarea de securitate responsabilă în același mod ca intruziunea malițioasă.

**Lituania și un culoar legal restrictiv pentru cercetare**

Lituania a adoptat un cadru legislativ pentru cercetarea și divulgarea vulnerabilităților, în locul recurgerii, în principal, la marja de apreciere a organelor de urmărire penală. Modificările privind CVD au intrat în vigoare în iunie 2021, în urma consultărilor care au implicat Ministerul Justiției, Parchetul General și Departamentul de Poliție. Reforma a abordat atât dreptul de a căuta vulnerabilități, cât și condițiile care reglementează această activitate (ENISA, 2022, 25-26).

Articolul 25 din Legea lituaniană privind securitatea cibernetică prevede că cercetarea și divulgarea vulnerabilităților pot fi legale și nu pot atrage răspunderea, în măsura în care sunt întrunite condițiile prevăzute de lege. **Protecția vizează chiar activitatea de cercetare**. Cercetătorii trebuie să evite perturbarea funcționării sistemului, afectarea disponibilității

serviciului sau modificarea datelor, să întrerupă testarea inutilă de îndată ce vulnerabilitatea este confirmată, să raporteze prin procedura prevăzută și să limiteze accesul la ceea ce este necesar pentru identificarea și demonstrarea vulnerabilității (Lithuanian Parliament, 2014, art. 25, astfel cum a fost modificat în 2024).

Întrucât legislația reglementează cercetarea vulnerabilităților ca activitate în sine, aceasta poate proteja testările limitate sau nereușite, efectuate anterior obținerii cu succes a accesului. Protecția nu se extinde, însă, în mod automat, asupra oricărei tentative de acces. Conduita care excedează ceea ce este necesar, care afectează datele sau disponibilitatea sistemului sau care nu respectă procedura de raportare rămâne supusă infracțiunilor obișnuite prevăzute la articolele 196-198 din Codul penal lituanian.

Lituania oferă, prin urmare, o protecție legală condiționată de tip *safe harbour*, care asigură o securitate juridică mai puternică decât o politică bazată exclusiv pe toleranța organelor de urmărire penală. Punctul său slab constă în restrângerea sferei culoarului protejat. Cerințele stricte privind necesitatea, întreruperea testării și raportarea promptă pot genera incertitudine atunci când confirmarea impactului unei vulnerabilități necesită o examinare tehnică suplimentară.

Pentru România, învățătura principală este aceea că protecția ar trebui să acopere cercetarea care precedă raportarea, însă condițiile acesteia trebuie să rămână suficient de flexibile pentru a corespunde realităților tehnice ale procesului de validare a vulnerabilităților.

**Lecții comparative pentru România**

Experiența comparată avertizează asupra riscului de a face protecția atât de rigidă din punct de vedere procedural încât să devină inutilizabilă. Belgia și Lituania demonstrează că protecția legală poate fi extinsă asupra cercetării care precedă raportarea, în timp ce Olanda ilustrează valoarea continuă a îndrumărilor operaționale și de urmărire penală publicate. România nu se mai confruntă cu o alegere abstractă între aceste modele: Parlamentul a optat pentru o abordare legală condiționată, atașând protecția, în mod direct, conformității cu articolul 36 (NIS Cooperation Group 2023; Pupillo et al. 2018; Romanian Parliament 2026).

**Articolul 365¹ propus creează, totuși, un culoar mai restrâns decât o protecție cuprinzătoare de tip *safe harbour*.** Acesta ar acoperi doar articolele 360 alin. (1) și (3), 361 și 364, fără a aborda, în mod expres, răspunderea civilă, tentativa reglementată de articolul 366

sau conduitele care se circumscriu articolelor 360 alin. (2), 362, 363 și 365. Valoarea sa practică ar depinde, de asemenea, de interpretarea termenului de 48 de ore și de restricțiile tehnice prevăzute la articolul 36.

**România ar trebui, prin urmare, să adopte o abordare hibridă. Protecția legală ar trebui susținută prin îndrumări din partea DNSC și a organelor de urmărire penală**, în timp ce o revizuire ulterioară ar trebui să stabilească dacă infracțiunile excluse, cercetarea nereușită și răspunderea civilă necesită clarificări sau o protecție suplimentară.

## O FOAIE DE PARCURS STRATEGICĂ ȘI DIPLOMATICĂ PENTRU ROMÂNIA

Foaia de parcurs propusă combină îndrumări imediate, punerea în aplicare și clarificarea protecției legale condiționate, precum și măsuri instituționale și diplomatice pe termen mai lung.

### Clarificarea și operaționalizarea cadrului existent

#### *Clarificarea articolului 36*

Prioritatea imediată ar trebui să constea în adoptarea unor îndrumări detaliate din partea DNSC, în temeiul articolului 36 alin. (2) lit. i), care să delimiteze cercetarea pasivă, interacțiunea publică obișnuită, scanarea, enumerarea activă, validarea limitată, accesul la resurse restricționate, extragerea de date, persistența în sistem și interferența cu funcționarea sistemului. Aceste îndrumări ar trebui să clarifice momentul de la care începe să curgă termenul de raportare de 48 de ore, să confirme posibilitatea completării ulterioare a unui raport inițial și să definească nivelul minim de dovezi necesar pentru demonstrarea unei vulnerabilități, fără accesarea inutilă a datelor.

Îndrumările ar trebui, de asemenea, să stabilească așteptările față de organizații, inclusiv existența unor canale de raportare accesibile, confirmarea promptă a primirii raportării, comunicarea continuă cu cercetătorul, prioritizarea, remedierea și publicarea coordonată. Protecția legală, luată izolat, nu va încuraja raportarea, în situația în care organizațiile rămân tăcute sau nu dispun de capacitatea de a acționa în urma unei raportări (National Cyber Security

Centre of the Netherlands 2013; Householder et al. 2017; Schaffer et al. 2023; NIS Cooperation Group 2023).

Tratamentul barierelor tehnice necesită o atenție deosebită. Îndrumările ar trebui să precizeze în ce condiții o vulnerabilitate care afectează autentificarea sau autorizarea poate fi demonstrată printr-o testare minimă și care metode rămân interzise. Obiectivul urmărit ar trebui să fie acela de a permite dovedirea deficienței, fără a autoriza escaladarea dincolo de ceea ce este necesar. Ar trebui elaborate, de asemenea, termene clare de divulgare. Instituirea unei perioade prezumate de remediere, ajustabilă în funcție de gravitate și de complexitate, ar asigura previzibilitate. Un cercetător ar trebui să poată solicita o revizuire, în situația în care entitatea afectată nu cooperează sau DNSC nu autorizează divulgarea într-un termen rezonabil.

***Clarificarea răspunsului de drept penal***

În cazul în care articolul 365[1] intră în vigoare, DNSC, Ministerul Public, DIICOT și Poliția Română ar trebui să elaboreze îndrumări comune privind aplicarea acestuia în cauzele referitoare la cercetarea vulnerabilităților. Aceste îndrumări ar trebui să abordeze sfera protecției, scopul urmărit, proporționalitatea, minimizarea datelor, efectele produse, raportarea promptă, cooperarea ulterioară descoperirii vulnerabilității și distincția dintre cercetarea pregătitoare și tentativa de acces.

Astfel de îndrumări nu ar înlătura autoritatea judiciară și nici nu ar extinde protecția legală dincolo de sfera sa de aplicare. Ele ar putea, totuși, reduce inconsecvențele de tratament, ar putea clarifica conduitele care nu se circumscriu articolului 365[1] și ar putea conferi efect practic considerentului 60 din Directiva NIS2, referitor la neurmărirea penală a cercetătorilor în domeniul securității cibernetice.

***Adoptarea unei politici naționale-model de divulgare a vulnerabilităților***

DNSC ar trebui să publice o politică publică drept model destinată instituțiilor publice și organizațiilor private. Această politică ar trebui să definească:

- sistemele și serviciile incluse;
- tehnicile autorizate și interzise;

- abordarea privind datele întâlnite în mod accidental;
- canale sigure de raportare și termene de răspuns;
- proceduri de remediere și de divulgare coordonată;
- un angajament privind acțiunea în justiție, sub condiția respectării politicii de către cercetător.

Aceasta ar trebui să fie facil de identificat înaintea testării și ar trebui să explice, în termeni accesibili, consecințele juridice ale conformării cu aceasta. Ea ar trebui însoțită de un fișier security.txt conform standardului RFC 9116, care să permită cercetătorilor identificarea directă, pe baza domeniului unei organizații, a persoanei de contact corecte și a regulilor de raportare aplicabile (Schaffer et al., 2023; Foudil și Shafranovich, 2022).

Practica oficială demonstrează că astfel de politici pot fi puse în aplicare de autoritățile publice, fără a crea o permisiune generală de testare a oricărui sistem. CISA, JPCERT/CC, Direcția Națională Israeliană pentru Securitate Cibernetică și Armata Germană publică rute dedicate de divulgare, care identifică sistemele vizate, conduita așteptată și canalul prin care trebuie transmise constatările (CISA, n.d..; JPCERT/CC, 2019; Israel National Cyber Directorate, 2021; Bundeswehr, 2023).

Modelul-cadru ar trebui să stabilească termene-țintă pentru confirmarea primirii, actualizări de stadiu, căi de escaladare și criterii de închidere a raportărilor, în conformitate cu modelul de coordonare CERT/CC, cu îndrumările NIST și cu recomandările Grupului de Cooperare NIS (Householder et al., 2017; Schaffer et al., 2023; NIS Cooperation Group, 2023). Implementarea în sectorul public ar trebui să debuteze cu autoritățile și serviciile civile care fac obiectul Ordonanței de urgență nr. 155/2024, urmată de instituirea unor mecanisme specializate pentru instituțiile excluse în temeiul articolului 2. Organizațiile sensibile nu au, în mod necesar, nevoie să autorizeze o testare publică extinsă, dar ar trebui să pună la dispoziție canale sigure pentru descoperirile accidentale și să definească, în mod clar, formele de cercetare pe care sunt dispuse să le primească.

DNSC ar trebui să publice, anual, date anonimizate privind raportările primite, sectoarele afectate, termenele de confirmare și de remediere, cauzele transfrontaliere și motivele închiderii raportărilor. Acești indicatori ar permite evaluarea cadrului, fără divulgarea unor informații tehnice exploatabile.

**Punerea în aplicare și completarea protecției legale condiționate**

**Dacă va fi promulgată și va intra în vigoare, legea ar oferi o consecință expresă de drept penal, prin introducerea articolului 365¹.** Prioritatea imediată este, prin urmare, aceea de a asigura o interpretare obiectivă și consecventă a condițiilor sale. Protecția ar trebui să rămână legată de scopul îmbunătățirii securității, de un nivel rezonabil de necesitate și proporționalitate, de minimizarea datelor, de absența persistenței sau a perturbării intenționate, de întreruperea cercetării de îndată ce se obține o confirmare suficientă, de raportarea promptă și de absența unor cereri coercitive sau a utilizării abuzive a informațiilor.

O revizuire ulterioară ar trebui să evalueze dacă protecția ar trebui extinsă asupra articolului 360 alin. (2), a articolelor 362, 363 și 365, precum și asupra tentativei reglementate de articolul 366. Raportul dintre cercetarea conformă a vulnerabilităților și răspunderea civilă ar trebui, de asemenea, clarificat. Orice extindere a protecției ar trebui să păstreze garanțiile împotriva conduitelor dăunătoare, inutile sau disproporționate, asigurând, în același timp, că protecția acoperă atât raportarea, cât și cercetarea minimă prealabilă necesară pentru producerea acesteia (Romanian Parliament, 2026).

**Consolidarea capacității de implementare și a poziției de lider internațional**

***Construirea unui ecosistem național de cercetare***

Un cadru național de CVD necesită mai mult decât norme juridice. Furnizorii, în special întreprinderile mici și mijlocii, pot să nu dispună de expertiza necesară pentru a evalua raportările, a comunica cu cercetătorii și a implementa corecțiile de securitate. ENISA a avertizat că instituirea CVD, în absența unei capacități organizaționale și tehnice suficiente, poate genera un aflux de raportări pe care organizațiile nu le pot procesa în mod eficient (ENISA, 2022, 68-73). Programele de tip *bug bounty* pot completa, dar nu ar trebui să substituie, un canal general de divulgare.

DNSC ar putea asigura triajul tehnic, documentația-model și medierea pentru organizațiile care nu dispun de echipe specializate. Universitățile, institutele de cercetare și companiile din domeniul securității cibernetice ar trebui să contribuie la formare, la proceduri de evaluare etică și la elaborarea unor standarde comune de cercetare. Ar putea fi introduse

programe-pilot publice de tip *bug bounty*, destinate unor servicii publice selectate cu atenție, care nu prezintă un caracter sensibil. Scopul acestora nu ar fi doar identificarea vulnerabilităților, ci și testarea limbajului contractual, a proceselor de răspuns și a cooperării dintre instituții și cercetători.

***Valorificarea poziției instituționale a României în diplomația cibernetică***

Reforma internă ar putea susține o poziție internațională mai amplă. Strategia Națională de Securitate Cibernetică definește diplomația cibernetică drept acțiunea de promovare a unui spațiu cibernetic deschis, stabil și sigur, în care se aplică drepturile omului, libertățile fundamentale și statul de drept (Romanian Government, 2021, secț. 4.1-4.5 și 5).

C-PROC conectează România la implementarea globală a Convenției de la Budapesta și la consolidarea capacităților în materia criminalității informatice și a probelor electronice; ECCC conectează Bucureștiul la cercetarea europeană în domeniul securității cibernetice și la politica industrială din acest sector, iar DNSC participă la Rețeaua CSIRT-urilor UE și poate coordona divulgarea vulnerabilităților cu impact transfrontalier. Împreună, aceste instituții ar putea susține crearea unui director regional de persoane de contact de încredere, formarea comună pentru CSIRT-uri și autoritățile de justiție penală, precum și asistența în elaborarea politicilor naționale de CVD (United Nations, 2015; United Nations, 2021; Dominioni, 2023).

**La nivelul UE,** România ar putea pleda pentru o mai mare convergență privind protecția condiționată a cercetătorilor, inclusiv prin criterii comune privind necesitatea, proporționalitatea, minimizarea datelor și raportarea responsabilă. Aceasta ar putea susține o reevaluare viitoare a Directivei 2013/40/UE, a cărei armonizare minimă a generat praguri naționale divergente.

**În cadrul Consiliului Europei,** România ar putea promova un dialog structurat între autoritățile de justiție penală, CSIRT-uri, cercetători și furnizorii de tehnologie. Scopul nu ar fi slăbirea incriminărilor din Convenția de la Budapesta, ci clarificarea modului în care noțiunile de acces fără drept, intenție și tentativă se aplică cercetării legitime în domeniul securității.

**La nivel regional,** România ar putea oferi expertiză Republicii Moldova, Ucrainei și statelor din Balcanii de Vest cu privire la mecanismele naționale de CVD, îndrumările pentru organele de urmărire penală, coordonarea instituțională și politicile din sectorul public. Aceasta

ar conecta consolidarea capacităților cibernetice cu prioritățile mai largi de politică externă ale României.

Obiectivul diplomatic ar trebui să fie mai degrabă unul practic, și nu declarativ. Cercetătorii nu ar trebui să se expună unor riscuri radical diferite doar pentru că un serviciu cloud, un furnizor sau un utilizator se află dincolo de o frontieră. Existenta unor criterii minime comune ar reduce fragmentarea și ar sprijini piața unică digitală a UE. Grupul de lucru CEPS a identificat deja normele divergente privind accesul ilegal drept o sursă de incertitudine substanțială pentru cercetarea transfrontalieră și a recomandat o coordonare mai strânsă, precum și luarea în considerare a unei armonizări la nivelul UE (Pupillo et al., 2018, 40-53).

## CONCLUZII

România se află într-o poziție favorabilă pentru a conecta reforma internă cu cooperarea europeană și internațională. Prevenirea criminalității informatice și protecția cercetătorilor nu constituie obiective concurente, ci elemente complementare ale rezilienței. România a creat ușa instituțională prin care vulnerabilitățile pot fi raportate, iar Parlamentul a făcut, în prezent, un pas semnificativ către asigurarea, pentru cercetătorii responsabili, a unei căi legale de a ajunge la aceasta.

Sarcina care rămâne este aceea de a asigura că, în cazul intrării în vigoare a articolului 365[1], condițiile acestuia sunt funcționale și că sfera sa limitată de aplicare nu lasă neprotejate forme importante de cercetare legitimă. În absența unei puneri în aplicare eficiente, alertele pot ajunge, în continuare, cu întârziere, prin canale informale sau nesigure, sau pot să nu ajungă deloc, în timp ce incertitudinea juridică reziduală descurajează cercetătorii responsabili, fără a descuraja, în același timp, actorii malițioși.

## BIBLIOGRAFIE

Bundeswehr. 2023. Vulnerability Disclosure Policy. 5 June 2023. https://www.bundeswehr.de/de/security-policy

Centre for Cybersecurity Belgium (CCB). 2020a. *Guide to Coordinated Vulnerability Disclosure Policies. Part I: Good Practices*.

Centre for Cybersecurity Belgium (CCB). 2020b. *Guide to Coordinated Vulnerability Disclosure Policies. Part II: Legal Aspects*.

Centre for Cybersecurity Belgium (CCB). 2025. *Coordinated Vulnerability Disclosure*. https://ccb.belgium.be/regulation/cvdp

Council of Europe. 1950. *Convention for the Protection of Human Rights and Fundamental Freedoms*. European Treaty Series No. 5.

Council of Europe. 2001a. *Convention on Cybercrime*. European Treaty Series No. 185. Budapest, 23 November 2001.

Council of Europe. 2001b. *Explanatory Report to the Convention on Cybercrime*. European Treaty Series No. 185.

Council of the European Union. 2017. *Council Conclusions on the Joint Communication to the European Parliament and the Council, Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU*. 20 November 2017.

Cybersecurity and Infrastructure Security Agency (CISA). n.d. Coordinated Vulnerability Disclosure Program.

Dominioni, S. 2023. *Operationalizing a directory of points of contact for cyber confidence-building measures.* United Nations Institute for Disarmament Research. https://unidir.org/files/2023-05/UNIDIR_Operationalizing_Directory_Points_of_Contact_Cyber_Confidence_Building_V4.pdf

European Commission. 2017. *Report Assessing the Extent to Which the Member States Have Taken the Necessary Measures in Order to Comply with Directive 2013/40/EU on Attacks against Information Systems*. COM(2017) 474 final.

European Commission and High Representative of the Union for Foreign Affairs and Security Policy. 2017. *Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU*. JOIN(2017) 450 final.

European Parliament and Council. 2013. Directive 2013/40/EU of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA. *Official Journal of the European Union, L 218*, 8-14.

European Parliament and Council. 2019. Regulation (EU) 2019/881 on ENISA and on information and communications technology cybersecurity certification. *Official Journal of the European Union, L 151*, 15-69.

European Parliament and Council. 2021. Regulation (EU) 2021/887 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres. *Official Journal of the European Union, L 202*, 1-31.

European Parliament and Council. 2022. Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union. *Official Journal of the European Union, L 333*, 80-152.

European Parliament and Council. 2024. Regulation (EU) 2024/2847 on horizontal cybersecurity requirements for products with digital elements. *Official Journal of the European Union.*

European Union. 2012. Charter of Fundamental Rights of the European Union. *Official Journal of the European Union, C 326*, 391-407.

European Union Agency for Cybersecurity (ENISA). 2016. *Good practice guide on vulnerability disclosure: From challenges to recommendations.* https://www.enisa.europa.eu/publications/vulnerability-disclosure

European Union Agency for Cybersecurity (ENISA). 2022. *Coordinated vulnerability disclosure policies in the EU.* https://doi.org/10.2824/983447

European Union Agency for Cybersecurity (ENISA). 2025. Consult the European Vulnerability Database to enhance your digital security. 13 May 2025. https://www.enisa.europa.eu/news/consult-the-european-vulnerability-database-to-enhance-your-digital-security

Foudil, E., & Shafranovich, Y. 2022. *RFC 9116: A file format to aid in security vulnerability disclosure.* Internet Engineering Task Force. https://doi.org/10.17487/RFC9116

Global Forum on Cyber Expertise. 2016. *Coordinated vulnerability disclosure.* https://thegfce.org/wp-content/uploads/CoordinatedVulnerabilityDisclosure-1-1.pdf

Householder, A. D., Wassermann, G., Manion, A., & King, C. 2017. *The CERT guide to coordinated vulnerability disclosure.* Special Report CMU/SEI-2017-SR-022. Software Engineering Institute, Carnegie Mellon University. https://www.sei.cmu.edu/documents/1945/2017_003_001_503340.pdf

International Organization for Standardization. 2018. *ISO/IEC 29147:2018 Information Technology, Security Techniques, Vulnerability Disclosure*. Geneva: ISO.

International Organization for Standardization. 2019. *ISO/IEC 30111:2019 Information Technology, Security Techniques, Vulnerability Handling Processes*. Geneva: ISO.

Israel National Cyber Directorate. 2021. Vulnerabilities Disclosure Program - CVE. Gov.il, 8 April 2021. https://www.gov.il/en/pages/cve_cyber_israel

JPCERT/CC. 2019. *Vulnerability coordination and disclosure policy.* 8 July 2019. https://www.jpcert.or.jp/english/vh/vul-coordination-disclosure-policy_2019.pdf

Lithuanian Parliament. 2014. *Law of the Republic of Lithuania on Cyber Security No. XII-1428 of 11 December 2014, as amended in 2024*.

National Cyber Security Centre of the Netherlands. 2013. *Guideline for Responsible Disclosure of IT Vulnerabilities*. Ministry of Security and Justice.

National Cyber Security Directorate. Coordinated Vulnerability Disclosure - CVD. https://www.dnsc.ro/pages/CVD

NIS Cooperation Group. 2023. *Guidelines on implementing national coordinated vulnerability disclosure policies.*

Openbaar Ministerie. 2013. *Beleidsbrief Responsible Disclosure*. College van procureurs-generaal, 18 March 2013.

Pupillo, L., Ferreira, A., & Varisco, G. 2018. *Software vulnerability disclosure in Europe: Technology, policies and legal challenges.* CEPS Task Force Report. Centre for European Policy Studies.

Romanian Government. 2021. *Romania's Cybersecurity Strategy for the Period 2022-2027*. Approved by Government Decision No. 1321 of 30 December 2021. Official Gazette of Romania No. 2 bis of 3 January 2022.

Romanian Government. 2024. *Emergency Ordinance No. 155/2024 on Establishing a Framework for the Cybersecurity of Networks and Information Systems in the National Civil Cyberspace*. Official Gazette of Romania No. 1332 of 31 December 2024.

Romanian Legislative Council. 2026. *Opinion No. 152 of 23 February 2026 on the Legislative Proposal Amending and Supplementing Emergency Ordinance No. 155/2024 and Supplementing Law No. 286/2009 on the Criminal Code* (b53/11.02.2026; L133/2026).

Romanian Parliament. 2003. *Law No. 161/2003 on Certain Measures for Ensuring Transparency in the Exercise of Public Dignities, Public Functions and the Business Environment and for Preventing and Sanctioning Corruption*. Official Gazette of Romania No. 279 of 21 April 2003.

Romanian Parliament. 2004. *Law No. 64/2004 for the Ratification of the Council of Europe Convention on Cybercrime*. Official Gazette of Romania No. 343 of 20 April 2004.

Romanian Parliament. 2009. *Law No. 286/2009 on the Criminal Code*. Official Gazette of Romania No. 510 of 24 July 2009.

Romanian Parliament. 2022. *Law No. 361/2022 on the Protection of Whistleblowers in the Public Interest*. Official Gazette of Romania No. 1218 of 19 December 2022.

Romanian Parliament. 2025. *Law No. 124/2025 Approving Emergency Ordinance No. 155/2024*. Official Gazette of Romania No. 638 of 7 July 2025.

Romanian Parliament. 2026. *Law Supplementing Article 36 of Emergency Ordinance No. 155/2024 and Law No. 286/2009 on the Criminal Code*. Legislative file L133/2026, registered at the Chamber of Deputies as PL-x 350/2026. Form sent to the President of Romania for promulgation on 22 June 2026.

Romanian Senate. 2026. *Joint Report No. XIX/75 and No. LXIX/109 of 20 April 2026 on Legislative Proposal L133/2026, including the admitted amendments*.

Schaffer, K., Mell, P., Trinh, H., & Van Wyk, I. 2023. *Recommendations for federal vulnerability disclosure guidelines.* NIST Special Publication 800-216. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-216

Smith, B. 2017. The need for urgent collective action to keep people safe online: Lessons from last week's cyberattack. Microsoft On the Issues, 14 May 2017. https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack/

Superior Council of Magistracy. 2026. *Letter No. 3/2807 of 24 March 2026 concerning Legislative Proposal b53/11.02.2026 on the amendment of Emergency Ordinance No. 155/2024 and the Criminal Code*.

United Nations. 1966. International Covenant on Economic, Social and Cultural Rights. General Assembly Resolution 2200A (XXI), 16 December 1966. https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-economic-social-and-cultural-rights

United Nations. 2015. *Report of the Group of Governmental Experts on developments in the field of information and telecommunications in the context of international security.* A/70/174, 22 July 2015.

United Nations. 2021. *Group of Governmental Experts on advancing responsible State behaviour in cyberspace in the context of international security.* A/76/135, 14 July 2021.

United Nations. 2024. *United Nations Convention against Cybercrime: Strengthening international cooperation for combating certain crimes committed by means of information and communications technology*

*systems and for the sharing of evidence in electronic form of serious crimes.* United Nations General Assembly Resolution 79/243 of 24 December 2024.

**Misiune.** Institutul Diplomatic Român (IDR) își asumă misiunea de a contribui substanțial la creșterea calității diplomației românești prin formare, educare continuă, cercetare, prin dezvoltarea gândirii critice și strategice, prin conectare internațională. O politică externă bună servește unei politici interne benefice.

**Principii**: valorizarea resurselor umane, profesionalismul, respectul și dialogul, responsabilitatea pentru comunitate.

Pornind de la atribuțiile legale fondatoare ale IDR, dezvoltarea în continuare a institutului se realizează, în funcție de nevoile identificate în MAE, pe următoarele patru direcții:

- Formarea și educarea continuă a diplomaților și a altor categorii de cursanți;
- Aprofundarea dimensiunii de cercetare și expertiză pe spații regionale și problematici funcționale;
- Funcționarea IDR ca *think-tank* al MAE;
- Integrarea IDR în cadrul unei rețele internaționale de institute relevante similare.

**Autor**: Teodora Curelariu este doctorandă în drept internațional și securitate cibernetică la Université Grenoble Alpes din Franța, în colaborare cu Inria, institutul național francez pentru cercetare în științe și tehnologii digitale.

**Seria *IDR Policy Forum*** cuprinde materiale elaborate de experte și experți din afara IDR.

Seria IDR Policy Forum
ISSN 3119-8562
ISSN-L 3119-8562

Editor, formatare și grafică: Claudiu Codreanu

Imagine copertă: https://unsplash.com/photos/a-laptop-computer-sitting-on-top-of-a-desk-nBXwqxjDa5c

Institutul Diplomatic Român - IDR
https://www.idr.ro/en/ | secretariat@idr.ro
Primăverii 17, sector 1, București, 011972