UNIUNEA NAȚIONALĂ A BAROURILOR DIN ROMÂNIA
THE NATIONAL ASSOCIATION OF THE ROMANIAN BARS
L'UNION NATIONALE DES BARREAUX DE ROUMANIE

102

0210.

TRIBUNALUL BUCUREȘTI
SECȚIA I PENALĂ
(Primire / Distribuire)
Data 16.12.2025 ora 16:18
Departamentul
Nr. dosar 4697/3/2025

Către:
TRIBUNALUL BUCUREȘTI- SECȚIA PENALĂ
CAMERA PRELIMINARĂ.

DOSAR NR. 364/19/P/2024

DOMNULE PREȘEDINTE,

Subscrisa **UNIUNEA NAȚIONALĂ A BAROURILOR DIN ROMÂNIA**, cu sediul în București, Sector 5, Splaiul Independenței nr. 5, Palatul de Justiție, identificată prin C.I.F. RO 4315974, reprezentată legal prin Președinte Av. dr. Traian - Cornel BRICIU, e-mail: unbr@unbr.ro și reprezentată convențional de Dragu Marius- Cabinet de Avocat, prin av. Dragu Marius, în calitate de **persoană vătămată**, în dosarul penal cu nr.364/19/P/2024 al Parchetul de pe lângă Înalta Curte de Casație și Justiție- Direcția de investigare a infracțiunilor de criminalitate organizată și terorism (D.I.I.C.O.T.), în temeiul art. 340 cod procedură penală, în termen legal, formulez prezenta

PLÂNGERE ÎMPOTRIVA SOLUȚIE DE CLASARE

o

Prin prezenta, solicităm admiterea plângerii formulate de Uniunea Națională a Barourilor din România împotriva Ordonanței de clasare comunicată persoanei vătămate la data de 13.10.2025, precum și împotriva Ordonanței de respingere a plângerii, comunicată de DIICOT la data de 25.11.2025.

Solicităm instanței, în temeiul art. 341 alin. (6) lit. b) Cod procedură penală, **desființarea soluției de clasare și trimiterea cauzei la procuror pentru completarea urmăririi penale**, cu continuarea acesteia **in personam** față de numitul **Deleanu Ștefan-Lucian** și față de persoana juridică **ENTRYRISE S.R.L.**, având în vedere că soluția adoptată de DIICOT este nelegală, netemeinică și rezultatul unei anchete incomplete.

1. **ASPECTE GENERALE PRIVIND PROCEDURA DE RESPECTAREA A DISPOZIȚIILOR PRIVIND SOLUȚIONAREA ORDONANȚEI DE CLASARE**

Prin Ordonanța de clasare nr. 364/19/P/2024, emisă la data de 02.10.2025 și expediată la data de 08.10.2025, DIICOT – Secția de combatere a infracțiunilor de terorism și a criminalității

informatice, prin procurorul de caz, a dispus clasarea cauzei în temeiul art. 315 alin. (1) lit. b) C.proc.pen., raportat la art. 16 alin. (1) lit. b) C.proc.pen., sub aspectul infracțiunilor de:

- acces ilegal la un sistem informatic, prevăzută de art. 360 alin. (1)–(3) C.pen.;
- transfer neautorizat de date informatice, prevăzută de art. 364 C.pen.

Aceste fapte au fost sesizate împotriva numitului Deleanu Ştefan-Lucian şi a societății ENTRYRISE S.R.L., reprezentată de acesta.

În temeiul art. 339 alin. (4) C.proc.pen., persoana vătămată U.N.B.R. a depus, în termen, plângere împotriva soluției de clasare la data de 02.11.2025 (prin e-mail) şi la 03.11.2025 (prin poştă).

La data de 25.11.2025, DIICOT a comunicat ordonanța de soluționare, în sensul respingerii a plângerii formulată de către UNBR.

A. NULITATEA ACTELOR DE URMĂRIRE PENALĂ

În temeiul art. 282 C.proc.pen., **invoc nulitatea relativă** a actelor de urmărire penală care au stat la baza soluției de clasare şi a ordonanței de respingere, întrucât au fost încălcate dispozițiile:

1 **art. 94 C.proc.pen.** – refuzul nelegal al accesului la dosar pentru persoana vătămată şi avocatul ales;

2 **art. 100 C.proc.pen.** – neadministrarea probelor necesare aflării adevărului;

3 **art. 305 alin. (3) C.proc.pen.** – omisiunea nejustificată de a continua urmărirea penală **in personam**, deşi autorul era identificat;

4 **art. 6 C.proc.pen.** – obligația de motivare a actelor procedurale.

Aceste încălcări au produs o **vătămare substanțială**, constând în imposibilitatea exercitării eficiente a dreptului la apărare şi imposibilitatea formulării unei plângeri efective împotriva soluției de clasare.

Vătămarea nu poate fi înlăturată decât prin **desființarea actelor nelegale şi trimiterea cauzei la procuror pentru completarea urmăririi penale**.

B. MOTIVE DE NELEGALITATE ŞI NETEMEINICIE

Hotărârea de respingere a plângerii este lipsită de motivare reală, întrucât:

- **reia textual sau rezumativ conținutul ordonanței de clasare;**
- **reia plângerea UNBR, fără analiză;**
- **nu examinează fondul criticilor;**
- **nu analizează probele sau lipsa acestora;**
- **nu oferă justificări juridice pentru menținerea soluției;**
- **conține contradicții evidente cu propriile considerente.**

Aceste aspecte vor fi detaliate în secțiunile ulterioare ale plângerii, demonstrând încălcări procedurale grave şi o lipsă de corelare juridică între ordonanța de clasare şi ordonanța de respingere.

În raport cu cele de mai sus, este evident că urmărirea penală nu a fost efectivă, că au fost încălcate dispoziții obligatorii privind administrarea probelor și schimbarea calității procesuale, iar persoana vătămată a fost lipsită de acces la dosar, în mod repetat și nelegal.

În aceste condiții, **intervenția judecătorului de cameră preliminară este necesară** pentru:

- restabilirea legalității procedurii;
- desființarea soluțiilor nelegale;
- trimiterea cauzei la procuror pentru efectuarea tuturor actelor de urmărire penală impuse de natura cauzei;
- continuarea urmăririi penale **in personam** față de suspectul identificat și față de persoana juridică implicată.

o

În fapt, la data de **05 ianuarie 2024**, **Uniunea Națională a Barourilor din România (U.N.B.R.)** a formulat **plângere penală** împotriva **numitului Deleanu Ștefan–Lucian** și a **societății ENTRYRISE S.R.L.**, având ca obiect săvârșirea infracțiunilor de **acces ilegal la un sistem informatic**, prevăzută de **art. 360 Cod penal**, și **transfer neautorizat de date informatice**, prevăzută de **art. 364 Cod penal**.

Plângerea a fost determinată și argumentată cu probe cu privire la activitatea desfășurată de către **Deleanu Ștefan–Lucian**, administrator și asociat unic al **societății ENTRYRISE S.R.L.**, care a accesat fără drept sistemele informatice aparținând **U.N.B.R. (platforma IFEP)**, a descărcat baze de date conținând **informații confidențiale și date cu caracter personal**, iar ulterior a utilizat aceste date în scop comercial prin intermediul platformei **incorpo.ro**, administrată de aceeași societate.

În cadrul acestei activități, autorul a transmis, în mod repetat, mesaje electronice către numeroși avocați înscriși în tabloul profesiei, pretinzând că ar fi identificat o „breșă de securitate" în sistemul IFEP. Aceste mesaje au fost expediate **sub identitatea falsă „Alexandra Ardelean"**, o persoană virtuală creată prin instrumente de inteligență artificială, care nu există în realitate.

În conținutul acestor emailuri, autorul a afirmat că a transmis o notificare la adresa **help@ifep.ro**, susținând că ar fi descoperit o vulnerabilitate tehnică, deși în realitate **nu a existat nicio comunicare oficială** cu instituția.

De asemenea, într-un **comunicat public publicat la data de 04.01.2024**, actualizat la **06.01.2024**, acesta a inserat un **email datat 28 februarie 2023**, care pretindea a fi o „sesizare anterioară" transmisă către **helpdesk@ifep.ro**, fără ca un asemenea mesaj să fi fost vreodată înregistrat în sistemul informatic al U.N.B.R.

Ulterior, în propriile sale declarații și în înregistrări video publice, **Deleanu Ștefan–Lucian** a recunoscut că a transmis aceste mesaje **prin intermediul identității virtuale „Alexandra Ardelean"**, invocând că nu știa că platforma IFEP aparține Uniunii.

Acest fapt confirmă existența unei acțiuni deliberate, realizate prin mijloace tehnice specifice, menite să creeze **aparența unei activități legitime și de interes public**, însă desfășurate **fără drept și în scop comercial**.

Pentru dovedirea faptelor, **U.N.B.R.** a solicitat, prin plângerea penală, administrarea următoarelor mijloace de probă, necesare stabilirii adevărului şi identificării tuturor persoanelor implicate:

- **Efectuarea unei percheziţii informatice** la sediul **societăţii ENTRYRISE S.R.L.** şi asupra echipamentelor (cu privire la telefoanele mobile, calculatoare, componente hardware) şi orice alte dispozitive informatice pe care se pot identifica date şi informaţii de interes în prezenta cauză utilizate de **Deleanu Ştefan–Lucian**, în vederea identificării datelor descărcate din sistemele informatice ale U.N.B.R.;

- **Audierea persoanei juridice ENTRYRISE S.R.L.**, prin reprezentantul său legal, şi a administratorului **Deleanu Ştefan–Lucian**

- Să dispună măsuri asiguratorii care se impun **pentru a evita ascunderea, distrugerea, înstrăinarea sau sustragerea de la urmărire a bunurilor care pot face obiectul confiscării speciale sau al confiscării extinse** şi **conservarea echipamentelor şi suporturilor informatice folosite pentru activitatea infracţională**, conform art. 249 Cod procedură penală;

• orice alte mijloace de probă stabilite de către organul de urmărire penală.

I. OBIECTUL PLÂNGERII ŞI DATELE CAUZEI

Se impune menţionarea faptului că atât persoana vătămată – UNBR –, cât şi avocatul împuternicit au fost în mod constant împiedicaţi să îşi exercite dreptul la studierea şi copierea dosarului, garantat de art. 94 C.proc.pen.

Cererile formulate de UNBR au fost respinse prin adresele DIICOT nr. 3812/II-1/2025 din 10.10.2025 şi 14.11.2025, deşi ordonanţa de clasare a fost comunicată UNBR abia la 08.10.2025, aspect care face imposibil ca solicitările să fie anterioare comunicării. În mod paradoxal, deşi DIICOT a indicat că avocatul poate formula cererea potrivit art. 94, solicitarea acestuia a fost, la rândul ei, respinsă, fără temei legal.

În aceste condiţii, prezenta plângere este formulată în absenţa accesului la materialul de urmărire penală, pe baza informaţiilor limitate furnizate în ordonanţele atacate şi pe baza probelor deţinute de persoana vătămată, ceea ce impune interpretarea favorabilă a oricăror aspecte neclar.

PRECIZĂM CĂ NUMAI DUPĂ ACCESUL ELECTRONIC LA DOSARULUI DE URMĂRIRE PENALĂ PUTEM COMPLETA PLÂNGEREA FORMULATĂ LA INSTANŢĂ.

o

În fapt, **prin adresa cu nr. 364/19/P/2024 din data de 08.10.2025 şi comunicată pe data de 13.10.2025**, conform ştampilei care se găseşte pe plicul care conţine ordonanţa, a Parchetul de pe lângă Înalta Curte de Casaţie şi Justiţie- Direcţia de investigare a infracţiunilor de criminalitate

organizată şi terorism (D.I.I.C.O.T.), s-a dispus, în temeiul dispoziţiilor art. 315 al. 1 lit. b C.p.p. rap. la art. 16 lit.b C.p.p., art. 275 alin.(3) Cod proc. pen.,art. 316 alin. (1) din C. proc.pen., clasarea cauzei sub aspectul săvârşirii infracţiunilor de accesul ilegal la un sistem informatic, prevăzute de art. 360 alin. 1, 2, 3 C.p. şi transferul neautorizat de date informatice, prevăzute de art. 364 C.p., fapte sesizate împotriva numitului DELEANU ŞTEFAN - LUCIAN şi S.C.ENTRYRISE S.R.L. (reprezentată legal prin asociat unic şi administrator DELEANU ŞTEFAN - LUCIAN) de către UNIUNEA NAŢIONALĂ Â BAROURILOR DIN ROMÂNIA (U.N.B.R) şi CORPUL EXPERŢILOR CONTABILI ŞI CONTABILILOR AUTORIZAŢI DIN ROMÂNIA (CECCAR).

Motivarea procurorului este vagă, contradictorie şi lipsită de fundament probatoriu.

Soluția de clasare **s-a întemeiat aproape exclusiv pe declarația persoanei Deleanu Ștefan-Lucian,** apreciată în mod eronat ca exprimând „bună-credință", **deși susținerile acestuia nu au fost verificate prin administrarea unor măsuri asigurătorii și procedurale specifice infracțiunilor prevăzute de Codul penal**, deşi chiar ordonanța **descrie acțiuni precise de extragere, prelucrare și utilizare de date**, conform pag. 3–15 din ordonanță

În plus, noţiunea că „ nu se poate considera ca acţiunile întreprinse, în cauză de autorul faptei, - au fost îndeplinite cu rea-credinţă" invocată de parchet nu reprezintă şi nu poate constitui o cauză justificativă în materia infracţiunilor informatice, astfel încât această apreciere subiectivă nu poate fundamenta o soluţie de clasare.

o

Soluția de clasare emisă de DIICOT în dosarul nr. 364/19/P/2024 este afectată atât sub aspectul **legalității**, cât şi al **temeiniciei**, fiind rezultatul unei analize incomplete, contradictorii şi neconforme cu probele administrate ori chiar cu propriile constatări consemnate în ordonanță.

II. NELEGALITATEA ORDONANȚEI DE CLASARE

Soluția de clasare pronunțată în dosarul nr. 364/19/P/2024 este nelegală, fiind rezultatul unei anchete incomplete, neadministrării probelor esențiale, ignorării unor obligații procedurale imperative şi încălcării dreptului la apărare. În continuare sunt detaliate motivele de nelegalitate care afectează în mod radical valabilitatea actului atacat.

Procurorul a pronunțat o soluție prematură, cu încălcarea obligației legale de a administra toate probele esențiale, prevăzută de art. 168–170 şi art. 249 Cod procedură penală.

Procurorul a redat pe larg, la paginile 4–7 ale ordonanței de clasare, versiunea persoanei vizate de plângere, Ştefan Deleanu – în mod singular, necontradictoriu şi neverificat –, transformând discursul acestuia într-un substitut al probatoriului. Declarațiile acestuia sunt redate integral, inclusiv elemente confesive, justificative, sau moralizatoare, fără a fi puse în balanță cu datele tehnice ori cu situația de fapt reținută chiar de procuror în alte părți ale documentului.

Această tehnică de redactare arată că procurorul a preluat integral o perspectivă subiectivă, fără a o confrunta cu probele din dosar şi fără să verifice prin administrarea unor probe care să fie independente şi care se impune în cazul infracţiunilor informatice pentru verificarea aspectelor declarate şi recunoscute de către autor, încălcând obligaţia de imparţialitate şi art. 5 CPP – principiul aflării adevărului.

Nelegalitatea ordonanţei de clasare vizează, în principal, omisiunea de a soluţiona distinct răspunderea penală a persoanei juridice ENTRYRISE S.R.L., precum şi neadoptarea măsurilor de conservare a datelor informatice necesare pentru prevenirea ascunderii, distrugerii, înstrăinării sau sustragerii bunurilor şi mijloacelor de probă ce pot face obiectul confiscării speciale sau extinse.

Totodată, procurorul nu a dispus efectuarea unei **expertize informatice** asupra sistemelor utilizate de persoana fizică şi juridică cercetată, deşi aceasta constituia un act esenţial pentru stabilirea existenţei accesărilor neautorizate şi a circuitului datelor extrase.

În mod similar, nu au fost audiate persoanele tehnice relevante – reprezentanţii firmelor care administrau infrastructura informatică a UNBR şi CECCAR – deşi aceştia aveau cunoştinţă directă despre configuraţia sistemelor şi natura accesărilor.

Potrivit art. 285 alin. (1) Cod procedură penală, procurorul are **obligaţia de a strânge şi administra din oficiu** toate probele necesare pentru aflarea adevărului, indiferent dacă acestea au fost sau nu solicitate de părţi. Această obligaţie implică dispunerea, **din oficiu**, a tuturor actelor de urmărire penală care pot conduce la stabilirea situaţiei de fapt, în special atunci când natura infracţiunilor reclamate este una tehnică, ce presupune competenţă de specialitate.

Astfel, **expertiza informatică, măsurile de conservare a datelor informatice** (art. 170 C.proc.pen.), **ridicarea de sisteme informatice** (art. 169 C.proc.pen.) şi **audierea persoanelor cu cunoştinţe de specialitate** (art. 114 C.proc.pen.) constituie acte procedurale obligatorii **din oficiu**, întrucât acestea sunt singurele apte să clarifice faptele reclamate şi să determine natura şi întinderea accesărilor neautorizate.

Lipsa unei expertize tehnice – încălcarea art. 172 CPP

Ordonanţa se bazează pe:
- rapoarte tehnice puse la dispoziţie de operatorii sistemului (pag. 10–12)
- opinii tehnice ale unor persoane direct interesate (CECCAR, INTRA CONNECT)

Dar **nu există o expertiză independentă** dispusă de procuror, deşi natura faptei (acces la sisteme informatice) o impunea cu necesitate.
Aceasta încalcă pe de o parte art. 172 CPP – expertiza obligatorie când sunt necesare cunoştinţe tehnice şi art. 97 CPP – probele trebuie administrate nemijlocit.

Lipsa acestor demersuri nu poate fi justificată prin pasivitatea părţilor, întrucât rolul activ al procurorului este expres consacrat de art. 5 alin. (2) Cod procedură penală, care impune organului judiciar au obligaţia de a strânge şi de a administra probe atât în favoarea, cât şi în defavoarea suspectului ori inculpatului. Respingerea sau neconsemnarea cu rea-credinţă a probelor propuse în favoarea suspectului ori inculpatului se sancţionează conform dispoziţiilor prezentului cod.

Prin urmare, soluția de clasare a fost pronunțată cu ignorarea obligațiilor legale ale procurorului de a acționa **din oficiu**, ceea ce constituie o nelegalitate esențială de natură să atragă **infirmarea ordonanței**, potrivit art. 339 alin. (3) Cod procedură penală.

Mai mult, încă din cuprinsul **plângerii penale depusă la D.I.I.C.O.T.**, persoana vătămată a solicitat în mod expres **efectuarea de percheziții informatice**, ridicarea sistemelor și a dispozitivelor de stocare deținute de persoana fizică și juridică cercetată.

Aceste cereri de probatoriu, formulate expres și motivate în fapt și în drept, nu au fost nici soluționate, nici respinse motivat de către parchet, deși art. **250 alin. (1)** și **art. 285 alin. (2) C.proc.pen.** impun obligația procurorului de a se pronunța prin ordonanță motivată asupra tuturor cererilor formulate de părți.

Prin omisiunea de a dispune asupra acestor cereri, procurorul a nesocotit dispozițiile art. **5 alin. (2)** și **art. 286 alin. (1) și (2) lit. e** C.proc.pen., privitoare la obligația organului judiciar de a efectua o cercetare completă și efectivă, precum și principiul consacrat de **art. 10 alin. (5)** C.proc.pen., potrivit căruia organele judiciare **au obligația** de a asigura exercitarea deplină și efectivă a dreptului la apărare de către părți și subiecții procesuali principali în tot cursul procesului penal.

Această pasivitate a condus la lipsa oricărei verificări reale a suporturilor informatice implicate, la neidentificarea datelor descărcate și la imposibilitatea stabilirii circuitului acestora, fapt ce a viciat grav ancheta penală.

Soluția de clasare pronunțată în aceste condiții nu doar că este **prematură**, dar și **nelegală**, întrucât a fost emisă cu **încălcarea obligației de a soluționa cererile de probatoriu** formulate de persoana vătămată cuprinse în plângerea penală și care trebuiau soluționate către procurorul de caz în cursul urmăririi penale.

II.1 ÎNCĂLCAREA DREPTULUI LA APĂRARE. REFUZUL PARCHETULUI DE A PERMITE ACCESUL LA DOSAR ȘI DE A RECUNOAȘTE APĂRĂTORUL ALES

În analiza legalității soluției, trebuie subliniat că atât persoana vătămată – Uniunea Națională a Barourilor din România –, cât și avocatul împuternicit au fost împiedicați în mod repetat să își exercite dreptul fundamental de acces la dosar, garantat de art. 94 C.proc.pen., drept indispensabil formulării unei plângeri efective.

Prin adresa DIICOT nr. 3812/II-1/2025 comunicată UNBR la 14.11.2025, procurorul a respins cererea de studiere a dosarului motivând că aceasta ar fi fost formulată ulterior soluției de clasare, deși însuși conținutul adresei confirmă că UNBR a fost notificată despre clasare abia la data de 08.10.2025 – fiind, prin urmare, imposibil ca solicitarea să fi fost anterioară comunicării soluției. Aceeași motivare formală apare și în adresa din 10.10.2025, reiterând refuzul fără a analiza în concret temeiul legal al cererii.

În plus, deși DIICOT a indicat explicit că avocatul împuternicit poate formula cererea de studiere în baza art. 94 C.proc.pen., atunci când avocatul a procedat conform îndrumării, solicitarea acestuia a fost, la rândul ei, respinsă printr-o motivare identică, fără a se oferi un temei juridic care să justifice limitarea accesului după emiterea soluției de clasare.

Această interpretare restrictivă este incompatibilă atât cu jurisprudența constantă în materie, cât și cu principiul rolului activ al organelor de urmărire penală.

Refuzul repetat și nejustificat de a permite accesul la materialul de urmărire penală echivalează cu lipsirea persoanei vătămate de posibilitatea efectivă de a formula o plângere completă și fundamentată.

Atât UNBR, cât și reprezentantul convențional au fost refuzați și constrânși să analizeze și să critice soluția exclusiv pe baza unor fragmente selectate în ordonanța de clasare și pe baza propriilor mijloace de documentare, fără a putea accesa totalitatea probelor administrate, a eventualelor cereri ale suspectului sau a răspunsurilor instituțiilor implicate.

Această limitare a accesului la dosar a generat o situație profund contrară dreptului la apărare, principiului egalității armelor și exigențelor unei proceduri echitabile, afectând în mod direct posibilitatea de a supune controlului instanței legalitatea și temeinicia soluției. În condițiile imposibilității obiective de a consulta dosarul, orice eventuală lacună factuală din prezenta plângere este consecința exclusivă a conduitei DIICOT, fiind aplicabile principiile interpretării favorabile persoanei lipsite de acces la materialul cauzei

În consecință, această atitudine a parchetului constituie o încălcare gravă a dreptului la apărare, a principiului contradictorialității și a obligației organului judiciar de a asigura accesul la dosar, generând **nelegalitatea ordonanței de clasare** și impunând **infirmarea acesteia** în temeiul art. 341 alin. (6) lit. b) C.proc.pen.

II.2 MENȚINERE NELEGALĂ A URMĂRII PENALE – IN REM- FĂPTUITORUL ERA IDENTIFICAT

Această măsură nu este opțională, **ci obligatorie,** asigurând transformarea urmăririi penale din faza de „in rem" (privind fapta) în faza de „in personam" (privind persoana).

O nelegalitate esențială care viciază întreaga soluție o reprezintă menținerea cauzei în faza urmăririi penale *in rem*, deşi autorul faptei fusese pe deplin identificat în chiar constatările procurorului. Ordonanța descrie în mod detaliat persoana care a realizat accesarea și extragerea datelor, rolul său în infrastructura societății utilizate, metodele tehnice folosite, justificările oferite și scopul operațiunii. Identitatea făptuitorului nu a fost niciodată incertă sau neclară; dimpotrivă, întreaga ordonanță se construiește în jurul conduitei aceleiași persoane perfect determinate.

În aceste condiții, legea impunea trecerea cauzei la urmărirea penală *in personam*, potrivit art. 305 alin. (3) C.proc.pen., care prevede în mod imperativ că, „**în momentul în care se constată că o anumită persoană a săvârșit fapta**, organul de urmărire penală dispune efectuarea în continuare a urmăririi penale *față de acea persoană*".

Această obligație nu este una facultativă, nici condiționată de vreo apreciere ulterioară asupra temeiniciei acuzației. Identificarea autorului generează automat obligația de a schimba cadrul procesual, astfel încât ancheta să poată continua cu respectarea garanțiilor procedurale necesare.

Menținerea artificială a cauzei în faza *in rem* a avut efectul direct de a limita și chiar împiedica desfășurarea unei anchete efective.

Procurorul nu a audiat persoana identificată în calitate de suspect, nu i-a adus la cunoștință acuzațiile, nu a dispus ridicarea sistemelor informatice pe care le utiliza, nu a solicitat expertiza tehnică necesară evaluării activității informatice, nu a examinat volumul real al datelor extrase și nici nu a analizat rolul persoanei juridice implicate. Toate aceste acte procedurale erau obligatorii și nu puteau fi efectuate decât în contextul urmăririi penale *in personam*.

Mai mult, este important de subliniat că procurorul nu poate anticipa aplicarea art. 16 C.proc.pen. şi nu poate evita schimbarea calităţii procesuale invocând, direct sau indirect, o pretinsă lipsă a caracterului infracţional al faptei.

Orice analiză pe art. 16 trebuie realizată **doar după** administrarea completă a probelor esenţiale şi **după** schimbarea calităţii procesuale, nu înainte.

A aprecia incidenţa art. 16 în faza *in rem* echivalează cu ocolirea dispoziţiilor art. 305 alin. (3) şi cu golirea de conţinut a garanţiilor procedurale prevăzute de lege.

În realitate, organul de urmărire penală nu poate evalua temeinicia unei acuzaţii fără a administra probele necesare, iar aceste probe nu se pot administra cât timp cauza rămâne blocată într-o fază premergătoare.

Cu alte cuvinte, **nu se poate invoca art. 16 pentru a justifica faptul că nu s-a trecut la in personam**.

Ar însemna ca organul de urmărire penală să îşi creeze propriul fundament de clasare prin simpla omisiune de a efectua acte esenţiale.

Legea nu permite o asemenea modalitate de ocolire a procedurii.

Mai mult, pentru a aprecia temeiurile art. 16, procurorul ar fi trebuit să verifice în concret:
- intenţia persoanei,
- caracterul neautorizat al accesului,
- scopul operaţiunii,
- volumul datelor prelucrate,
- infrastructura utilizată,
- eventualele consecinţe,
- rolul persoanei juridice.
- verificarea declaraţiei numitului după expertiza informatică.

Prin faptul că nu a schimbat cadrul procesual, DIICOT a împiedicat efectuarea unei anchete reale, a eliminat posibilitatea de a verifica în mod obiectiv situaţia de fapt şi a creat premisa unei soluţii superficiale, pronunţate în absenţa probelor obligatorii. Această omisiune este una structurală şi afectează întreg parcursul procesual, soluţia de clasare devenind astfel nelegală indiferent de considerentele reţinute în ordonanţă.

Nimic din acestea NU a fost investigat tocmai pentru că nu s-a dispus trecerea în *in personam*. Prin urmare, invocarea art. 16 în ordonanţa de clasare este nu doar insuficientă, ci **nelegal formulată**, deoarece analiza ar fi trebuit să fie făcută într-o procedură completă, desfăşurată faţă de persoana identificată.

În concluzie, menţinerea cauzei în faza *in rem*, deşi făptuitorul era cunoscut şi pe deplin individualizat, reprezintă o încălcare gravă a art. 305 alin. (3) C.proc.pen., cu consecinţa nulităţii soluţiei de clasare.

În concluzie, chiar dacă DIICOT a propus soluţia de clasare în temeiul art. 16, această soluţie nu poate fi validă, întrucât a fost întemeiată pe o procedură viciată înainte de a se pronunţa cu privire la clasarea dosarului penal : **refuzul de a trece cauza la urmărirea penală in personam**.

Nelegalitatea este structurală şi impune desfiinţarea ordonanţei., cu administrarea completă a probelor necesare aflării adevărului.

III. NESOLUȚIONAREA RĂSPUNDERII PENALE A PERSOANEI JURIDICE ENTRYRISE S.R.L.

Plângerea penală viza distinct persoana juridică ENTRYRISE S.R.L. Ordonanța doar o menționează la sfârșitul ordonanței de clasare, fără a conține o analiză asupra răspunderii penale a acesteia. Din ansamblul datelor rezultă indicii temeinice pentru efectuarea urmăririi penale și sub acest aspect. Faptul că probatoriul administrat până la clasare este „restrâns" nu justifică închiderea cauzei, ci impune completarea cercetărilor. Potrivit art. 135 alin. (1) și (3) C.pen., persoanele juridice, altele decât statul și autoritățile publice, răspund penal pentru faptele săvârșite în numele sau în interesul lor ori în realizarea obiectului de activitate.

În speță, accesarea platformelor UNBR și CECCAR și descărcarea bazelor de date pentru promovarea platformei „incorpo.ro" s-au realizat în interesul direct al societății ENTRYRISE S.R.L.

Neadoptarea unor acte de urmărire penală specifice persoanei juridice, audierea reprezentantului legal (art. 489 C.proc.pen.) și lipsa unei analize dedicate contravin art. 314 alin. (1)–(2) C.proc.pen.

Un aspect fundamental omis de procuror și care afectează în mod grav temeinicia și legalitatea soluției de clasare îl reprezintă **nesoluționarea răspunderii penale a persoanei juridice ENTRYRISE S.R.L.**, societatea prin intermediul căreia au fost efectuate operațiunile tehnice de extragere, procesare și stocare a datelor aparținând avocaților și structurilor profesionale.

Ordonanța de clasare descrie în detaliu modul în care infrastructura informatică a societății ENTRYRISE S.R.L. a fost utilizată pentru realizarea întregului proces informatic: serverele acesteia au fost folosite pentru rularea scripturilor automate, spațiile de stocare au reținut datele extrase, iar activitatea a fost realizată în cadrul și cu resursele societății. Cu toate acestea, DIICOT nu a efectuat absolut nicio analiză privind răspunderea penală a persoanei juridice, nu a audiat reprezentanții societății, nu a solicitat documente, nu a verificat activele informatice și nu a analizat conduita organizației.

Această omisiune este esențială, întrucât art. 135 C.pen. reglementează expres răspunderea penală a persoanei juridice pentru faptele săvârșite în realizarea obiectului de activitate, în interesul ori în numele acesteia. Or, din chiar conținutul ordonanței rezultă că actele tehnice au fost realizate:

- cu resursele societății,
- prin infrastructura acesteia,
- în cadrul activităților sale profesionale,
- în beneficiul persoanei juridice sau în cadrul unui interes comercial al acesteia.

În aceste condiții, procurorul avea obligația să examineze :

5 dacă activitatea de extragere a datelor s-a realizat în numele societății;
6 dacă acțiunile au servit interesele ENTRYRISE (comerciale, informaționale, de marketing etc.);
7 dacă persoana fizică (Deleanu Ștefan-Lucian) a acționat în virtutea funcției deținute în cadrul societății;
8 dacă societatea a beneficiat sau putea beneficia de rezultatele activității;
9 dacă reprezentanții societății au cunoștință, au tolerat sau au încurajat activitatea;
10 dacă infrastructura și resursele societății au fost puse la dispoziție în mod deliberat.

Lipsa acestei analize reprezintă o încălcare gravă a obligației organului judiciar de a verifica **toate formele de răspundere penală incidente**. Soluția de clasare nu poate fi considerată completă câtă

vreme se limitează exclusiv la persoana fizică, ignorând total contextul profesional, tehnic și organizațional în care au fost desfășurate faptele.

Este, de asemenea, nelegal faptul că DIICOT nu a dispus audierea persoanei juridice, nu a solicitat documentele interne relevante (politici IT, politici de securitate, proceduri interne, registre de activitate), nu a verificat serverele, calculatoarele sau conturile utilizate în cadrul societății și nu a examinat eventualele beneficii economice ori profesionale ale firmei rezultate din prelucrarea neautorizată a datelor.

Mai mult, ordonanța nici măcar nu menționează existența societății ca posibil subiect al răspunderii penale, deși aceasta este descrisă factual ca fiind centrul operațional al întregii activități informatice. Această omisiune conduce la o **soluție incompletă**, contrară art. 285 C.proc.pen., care impune procurorului să efectueze urmărirea penală cu privire la **toate**faptele și la **toți** participanții.

Practica Înaltei Curți este constantă în sensul că, atunci când fapta se realizează printr-o structură organizată (fie societate comercială, fie altă entitate), organul judiciar are obligația să analizeze răspunderea persoanei juridice chiar dacă aceasta nu este sesizată expres în plângere, întrucât procurorul acționează din oficiu și în virtutea rolului activ.

Prin eliminarea totală a acestei analize, soluția de clasare devine **netemeinică** și **nelegală**, întrucât nu soluționează latura obiectivă a răspunderii juridice într-un context în care societatea comercială a constituit cadrul operațional esențial al faptelor.

În concluzie, ignorarea răspunderii penale a ENTRYRISE S.R.L. reprezintă o lacună fundamentală a urmăririi penale, care impune desființarea ordonanței atacate și reluarea urmăririi penale inclusiv sub aspectul examinării persoanei juridice, conform art. 135 C.pen. și art. 305 C.proc.pen.

IV. NETEMEINICIA ORDONANȚEI DE CLASARE

Soluția de clasare nu este doar nelegală, ci și profund netemeinică, întrucât analiza procurorului se bazează pe constatări incomplete, interpretări eronate ale situației de fapt, contradicții interne evidente și o evaluare subiectivă a probelor, incompatibilă cu obligația de aflare a adevărului prevăzută de art. 5 C.proc.pen.

În cele ce urmează sunt prezentate argumentele și probele care demonstrează că ordonanța a fost emisă pe baza unei analize superficiale, selective și necorelate cu probele existente sau cu obligațiile de investigare.

Procurorul reține, pe de o parte, că autorul a creat un mecanism informatic complet automatizat, a configurat scripturi de extragere și procesare a datelor, a stabilit o infrastructură informatică dedicată colectării informațiilor privind avocații și a descărcat un volum semnificativ de date cu caracter personal.

Aceste constatări sunt în mod evident specifice unui comportament intenționat, repetitiv și organizat.

Pe de altă parte, în analiza juridică, ordonanța concluzionează că fapta nu ar prezenta caracter infracțional sau că nu ar exista intenția specifică elementului subiectiv.

Această disonanță între situația de fapt descrisă în detaliu și concluzia juridică finală reprezintă o **contradicție** care face imposibilă validarea ordonanței sub aspectul temeiniciei.

Ordonanța nu explică niciun moment cum se poate ajunge logic de la un comportament tehnic avansat, organizat și repetat, la concluzia unei lipse de intenție sau a unui caracter nepenal al conduitei.

12

ACTIVITATEA PROBATORIE A PARCHETULUI S-A LIMITAT LA:

1. **ADRESE CĂTRE FIRMELE CARE ADMINISTRAU INFRASTRUCTURA INFORMATICĂ A UNBR ȘI CECCAR;**

Parchetul a transmis solicitări către firmele care asigurau mentenanța și hosting-ul platformelor informatice ale UNBR și CECCAR, pentru a obține informații privind eventuale accesări neautorizate.

Firmele IT administratoare, răspunzând solicitărilor DIICOT, au confirmat **existența unor accesări externe ale serverelor UNBR și CECCAR**, au precizat că **logurile disponibile sunt incomplete și nu permit identificarea exactă a utilizatorului**, iar **la dosar au fost transmise doar fragmente tehnice extrase din aceste loguri pentru că Deleanu Ștefan-Lucian a creat și utilizat mecanisme complexe de colectare automată a datelor**, capabile să interacționeze direct cu bazele informatice ale UNBR și CECCAR, să extragă informații confidențiale și să le integreze ulterior în platforma comercială pe care o controla (*incorpo.ro*), acțiune ce nu putea avea loc fără o intervenție tehnică deliberată și fără drept în sistemele respective.

Aceste răspunsuri, analizate în contextul general al cauzei, **demonstrează existența unor intervenții externe asupra sistemelor informatice**, dar și **lipsa unei reacții investigative adecvate din partea parchetului**, care s-a limitat la a prelua informațiile formale fără verificări tehnice suplimentare.

În realitate, aceste accesări externe **nu pot fi explicate printr-o utilizare obișnuită a sistemelor**, ci corespund unui **mecanism informatic elaborat**, creat de **Deleanu Ștefan-Lucian**, prin intermediul căruia a **automatizat colectarea și descărcarea bazelor de date** aparținând UNBR și CECCAR.

Prin acest mecanism, **au fost extrase volume mari de informații confidențiale**, ulterior **integrate și utilizate în cadrul platformei comerciale „incorpo.ro”**, în scop de promovare și valorificare economică.

Acest aspect rezultă implicit din coroborarea declarațiilor autorului, a materialelor publice postate de acesta și a informațiilor furnizate de instituțiile vătămate.

Astfel, **există o legătură directă între activitatea tehnică neautorizată asupra sistemelor informatice și beneficiul comercial urmărit**, ceea ce conturează elementele infracțiunilor prevăzute de art. 360 și art. 364 C.pen.

Faptul că parchetul **nu a dispus expertiză informatică** (art. 172 C.proc.pen.), **nu a audiat reprezentanții firmelor tehnice** și **nu a coroborat datele transmise cu declarațiile autorului** reprezintă **o omisiune gravă**, care face ancheta incompletă și soluția de clasare **netemeinică**.

Prin urmare, **analiza probatoriului existent demonstrează** că **mecanismele tehnice folosite de Deleanu nu puteau funcționa fără un acces efectiv în sistemele informatice protejate ale UNBR și CECCAR**, acces care, în absența unei autorizări, constituie **acces ilegal la un sistem informatic**, în sensul art. 360 C.pen.

În concluzie, prin adresele transmise, UNBR și CECCAR au confirmat că nu **au acordat acces sau mandat persoanei** ori societății menționate, că au constatat descărcări de date de pe serverele proprii, că **nu au putut evalua întinderea prejudiciului**, iar **sistemele informatice erau administrate tehnic de firme IT specializate**, menționate expres în ordonanță.

2. **DECLARAȚIA AUTORULUI**, INTERPRETATĂ SUBIECTIV

Potrivit **ordonanței de clasare din data de 13.10.2024**, întocmită de DIICOT, **numitul Deleanu Ștefan-Lucian**, administrator al societății **ENTRYRISE S.R.L.**, a fost audiat cu privire la faptele care au făcut obiectul plângerilor formulate de **UNBR** și **CECCAR**.

Conform celor reținute la **pagina 3-5** din ordonanță, rezultă din declarația acestuia *„a accesat platformele informatice UNBR și CECCAR pentru a verifica vulnerabilitățile acestora”*, arătând că *„nu a urmărit obținerea unui folos material”* și *„nu a intenționat să prejudicieze instituțiile respective”*.

Se consemnează că același autor a susținut că *„scopul activității sale a fost acela de a semnala public deficiențele sistemelor informatice și de a contribui la îmbunătățirea acestora”* și că *„nu a modificat sau distrus datele informatice, acționând din convingerea că realizează o activitate de interes public”*.

Aceste fragmente reprezintă **recunoașterea explicită a faptului că persoana a accesat sisteme informatice aparținând altor entități juridice și a descărcat date din acestea**, aspecte care corespund **elementului material al infracțiunilor prevăzute de art. 360 și art. 364 Cod penal**.

Totuși, din ordonanță, procurorul apreciază că:

„Din declarațiile persoanei audiate nu rezultă intenția de a prejudicia instituțiile vătămate, ci intenția de a semnala deficiențele de securitate.”

Și adaugă:

„Nu există elemente care să ateste intenția infracțională, fapta nefiind săvârșită cu scopul de a obține un avantaj necuvenit.”

Ulterior, concluzia devine decisivă pentru soluția de clasare:

„Accesul nu poate fi calificat ca fiind fără drept, în condițiile în care persoana auditată a acționat din convingerea că realizează o activitate utilă public.”

Această concluzie este **contradictorie și nelegală**.

Pe de o parte, procurorul **confirmă existența faptelor materiale**(accesarea şi descărcarea datelor), iar pe de altă parte **neagă caracterul ilicit al acestora**, pe baza unei presupuse „bunei-credințe" a autorului.

Mai ales în contextual în care acesta avea prieteni avocați care nu ia recomandat să folosească și să nu ia datele cu caracter personal din sistemul informatic.

3. LIPSA VERIDICITĂȚII DATELOR FURNIZATE DE CĂTRE NUMITUL DELEANU LUCIAN DUPĂ AUDIERE.

După audierea acestuia, procurorul nu a verificat codul scriptului folosit, modul de declanșare automată, istoricul accesărilor, logurile serverelor care sunt în patrimonial persoanei juridice, volumul real al datelor extrase, existența unor copii suplimentare, eventuale exporturi către terți, utilizarea datelor în scop comercial.

Fără aceste verificări, afirmațiile suspectului privind scopul „non-infracțional" al activității rămân simple declarații necontrolate.

O soluție de clasare construită pe declarațiile unei singure părți implicate, neconfirmate prin probe tehnice, este **netemeinică prin definiție**.

În plan juridic, infracțiunea de **acces ilegal la un sistem informatic (art. 360 C.pen.)** se consumă prin **simplul acces fără drept**, fără a fi necesară intenția de a produce un prejudiciu sau obținerea unui folos.

Prin urmare, chiar dacă autorul ar fi acționat „cu intenția de a semnala deficiențe", lipsa consimțământului titularului sistemului face ca fapta să fie **tipică penal**.

Totodată, parchetul **nu a coroborat această declarație** cu alte mijloace de probă — nu există **expertiză informatică, audierea firmelor IT administratoare, verificarea logurilor**, nici **analiza bazelor de date descărcate**. Declarația autorului a fost luată ca veridică şi completă, contrar **art. 103 alin. (2) C.proc.pen.**, care impune coroborarea oricărei declarații cu alte mijloace de probă.

Mai mult, există o **contradicție internă în declarația autorului**: acesta admite că a accesat şi descărcat date pentru a „demonstra vulnerabilități", însă tot el susține că nu a avut intenția de a le folosi sau de a le divulga. Această susținere este infirmată chiar de rezultatul ulterior – existența **platformei comerciale „incorpo.ro"**, unde au fost utilizate date colectate în urma acelor accesări.

În final, concluzia procurorului, potrivit căreia *„accesul nu poate fi calificat ca fiind fără drept"* (pag. 5), **nu are temei legal**. Codul penal **nu recunoaște „buna-credință" ca o cauză justificativă** și nu prevede excepții pentru accesul „motivat de interes public". Raționamentul procurorului transformă o **mărturisire a faptei** într-un **argument de clasare**, ceea ce este logic și juridic inacceptabil. Nu poate fi acceptată ideea că autorul faptelor sesizate a descărcat mai multe informații din sistemele informatice și pe care le a stocat fie pe cloud, fie pe dispozitivele personale și acesta să nu fie tras la răspundere și nici o măsură să nu fie luată de parchet.

Prin urmare, analiza comparativă a paginilor **2–5** din ordonanță arată clar contradicția: pe de o parte, procurorul **constată accesul și descărcarea datelor**, iar pe de altă parte, **neagă caracterul ilicit**, substituind criteriul legal cu o apreciere morală a intenției autorului.

Ordonanța descrie la paginile 16–18:
- crearea unui „proces automat" pentru extragerea datelor
- folosirea unui browser automatizat
- extragerea datelor precum CNP, domiciliu, număr de telefon
- comunicarea către avocați că există breșa de securitate prin cont și nume care sunt alese de autor.

Deși ordonanța descrie un acces repetat, automatizat și organizat asupra unor sisteme informatice protejate prin credențiale și proceduri de autentificare, procurorul apreciază că nu s-ar fi produs „acces ilegal".

Analiza omite însă elementele obiective esențiale:

- sistemele informatice respective erau accesibile doar membrilor profesiilor,
- unele dintre secțiuni erau protejate prin autentificare,
- identitatea folosită nu era autentică,
- procesul de extragere a fost automatizat pentru volum mare,
- datele extrase includ CNP-uri și informații sensibile,
- accesul a urmărit constituirea unor baze de date proprii.

Aceste elemente, chiar și luate separat, satisfac cerințele art. 360 și 364 C.pen.

Ordonanța le consemnează factual, dar nu le analizează juridic.

Aceste elemente, în mod obiectiv, **întrunesc elementele materiale ale art. 360 și 364 CP** – acces și transfer fără drept.

În paginile 4–7, procurorul reproduce integral discursul lui Deleanu, în care acesta:
- își justifică acțiunile,
- minimizează fapta,
- invocă intenții morale,
- invocă presupuse discuții cu avocați,
- sugerează că „a vrut să ajute".

Nu există nicio confruntare cu probe obiective ori documente tehnice. Nu există nicio analiză a intenției în raport cu faptele concrete.

Or, în materie penală, declarația persoanei cercetate:

- nu este suficientă pentru a stabili inexistența vinovăției,
- nu poate înlocui expertiza informatică,
- nu poate substitui constatările tehnice,
- nu poate justifica lipsa altor probe.

Practic, concluziile procurorului despre lipsa intenției provin exclusiv din relatările făptuitorului, fără o verificare independentă. Această metodă de analiză contravine art. 103 alin. (2) C.proc.pen.,

potrivit căruia **nicio probă nu are o valoare prestabilită**, iar declarațiile inculpatului/suspectului trebuie evaluate în raport cu ansamblul probator, nu izolat.

Cu alte cuvinte, **DIICOT tratează apărarea ca probă,** încălcând art. 6 CPP.

Această abordare contravine **principiului legalității incriminării** și dispozițiilor **art. 5 alin. (2) și art. 286 alin. (2) C.proc.pen.**, impunând **infirmarea ordonanței de clasare** și **reluarea urmăririi penale** față de persoana fizică și mai ales față de persoana juridică.

Ignorarea completă a prejudiciului și a datelor sensibile colectate, a persoanelor vătămate

Ordonanța recunoaște că au fost extrase:
- CNP-uri
- domicilii
- numere de telefon
- date profesionale

Totuși, nu analizează:câte persoane au fost afectate, dacă datele au fost stocate, dacă au fost transmise altora, dacă au fost folosite pentru contactare.

Aceasta reprezintă o analiză incompletă și superficială a laturii obiective.

Totuși, în concluzie, procurorul susține că nu ar fi elemente infracționale.

Aceasta reprezintă o eroare de logică juridică și o contradicție directă între situația de fapt și aprecierea finală.

4. CONSECINȚELE REALE ALE EXTRAGERII DATELOR ȘI PREJUDICIUL PRODUS

Ordonanța nu analizează deloc:
- impactul asupra persoanei vătămate UNBR,
- impactul asupra tuturor avocaților,
- riscurile pentru confidențialitatea profesională,
- stocarea continuă a datelor după extragere,
- eventualele utilizări comerciale,
- lipsa oricăror măsuri de securitate,
- imposibilitatea UNBR de a proteja membrii profesiei.

Lipsa evaluării prejudiciului produce o soluție de clasare incompletă și contrară obligației de a analiza toate urmările faptei.
În mod evident, DIICOT nu a reconstituit situația de fapt, nu a clarificat natura și scopul scriptului utilizat, nu a verificat suporturile informatice, nu a evaluat volumul real al datelor, nu a analizat contextul în care au fost utilizate datele și nu a determinat impactul asupra persoanelor vizate.

O soluție de clasare nu poate fi temeinică atunci când investigația este incompletă, iar analiza procurorului se reduce la o interpretare formală și superficială a unor fapte tehnice complexe, fără expertiză și fără probe obiective.

V. CERCETAREA ȘI RĂSPUNDEREA PERSOANEI JURIDICE ENTRYRISE S.R.L.

Cercetarea persoanei juridice ENTRYRISE S.R.L. – **omisiuni și lacune ale urmăririi penale, lipsa cercetării și a analizei persoanei jurdice care este cerută prin plângerea penală depusă de către U.N.B.R.**

Deși sesizarea a vizat expres atât pe **Deleanu Ștefan-Lucian**, cât și societatea administrată de acesta, **ENTRYRISE S.R.L.**, ordonanța de clasare din data de **13.10.2024** nu conține nicio analiză distinctă cu privire la **răspunderea penală a persoanei juridice**.

În ordonanță nu se regăsește **niciun act de dispunere a efectuării de cercetări față de persoana juridică**, nicio **mențiune privind reprezentantul legal**, și nici **o evaluare a activității societății în raport de faptele imputate**.

Or, potrivit **art. 135 alin. (1) și (3) Cod penal**, persoanele juridice, altele decât statul și autoritățile publice, răspund penal pentru faptele săvârșite în numele sau în interesul lor, ori în realizarea obiectului de activitate. În speță, faptele imputate – accesarea sistemelor informatice ale **UNBR** și **CECCAR** și descărcarea bazelor de date pentru promovarea platformei **incorpo.ro** – au fost efectuate **în numele și în interesul societății ENTRYRISE S.R.L.**, fiind recunoscute ca atare chiar de administratorul său.

Declarațiile acestuia, redate la paginile **2–4** din ordonanță, arată că acțiunile au avut ca scop „promovarea activității platformei" și „semnalarea deficiențelor de securitate". Prin urmare, **finalitatea faptelor este direct legată de activitatea comercială a societății**, ceea ce atrage aplicabilitatea art. **135 Cod penal**.

Cu toate acestea, parchetul **nu a extins urmărirea penală față de persoana juridică**, **nu a dispus nicio audiere a reprezentantului legal al acesteia** (art. 489 C.proc.pen.), și **nu a analizat raportul dintre fapta persoanei fizice și interesul societății**.

Această omisiune procedurală este gravă, întrucât conform **art. 314 alin. (1) și (2) C.proc.pen.**, organul de urmărire penală are obligația de a se pronunța distinct asupra tuturor persoanelor vizate de plângere. În cauză, DIICOT a limitat cercetarea exclusiv la persoana fizică, **ignorând componenta de răspundere penală a persoanei juridice**, deși faptele au fost comise în contextul activității acesteia.

De asemenea, ordonanța nu cuprinde **nicio măsură de verificare a activelor societății**, a **serverelor folosite pentru stocarea datelor descărcate** sau a **utilizării comerciale a acestor date** în cadrul platformei *incorpo.ro*.

Prin această pasivitate, parchetul a lăsat în afara oricărui control penal **mecanismul informatic creat și exploatat de societatea ENTRYRISE S.R.L.**, mecanism prin care s-au obținut și utilizat în mod neautorizat date cu caracter personal și informații confidențiale aparținând **UNBR** și **CECCAR**.

Rezultatul este o anchetă incompletă și o soluție vădit netemeinică, întrucât în absența unei analize asupra persoanei juridice **nu se poate aprecia întregul context infracțional**, nici **scopul comercial al faptelor**.

18

Această omisiune contravine:

- **art. 5 alin. (2) C.proc.pen.** – obligația de a asigura aflarea adevărului,
- **art. 286 alin. (2) C.proc.pen.** – obligația de a efectua o cercetare completă,
- și **art. 314 alin. (1)** – obligația de a se pronunța asupra tuturor persoanelor și faptelor din cauză.

Prin urmare, sub acest aspect, ordonanța este **nelegală și netemeinică**, iar instanța, în temeiul **art. 341 alin. (6) lit. b C.proc.pen.**, trebuie să dispună **infirmarea soluției de clasare** și **reluarea urmăririi penale față de persoana juridică ENTRYRISE S.R.L.**, cu respectarea dispozițiilor art. **489 și urm. C.proc.pen.**

1. **Constatări tehnice incomplete** de către parchet, fără expertiză care s-au limitat numai la declarația lui DELEANU ȘTEFAN – LUCIAN

Potrivit **ordonanței de clasare din 13.10.2024**, DIICOT a menționat că, urmare a solicitărilor adresate către **UNBR, CECCAR** și firmele IT care asigurau mentenanța platformelor informatice ale acestora, au fost primite *„fragmente de loguri”* și *„răspunsuri tehnice incomplete”*, din care *„nu se pot determina identitatea utilizatorului și modalitatea concretă de acces”*.

Astfel, în cuprinsul ordonanței se consemnează:

„Logurile disponibile sunt incomplete, ceea ce nu permite stabilirea cu certitudine an existenței unui acces neautorizat.” „Nu rezultă probe tehnice directe care să confirme că datele au fost extrase fără drept.”

Cu toate acestea, deși procurorul recunoaște expres **caracterul incomplet al datelor tehnice**, nu a dispus **nicio expertiză informatică** conform **art. 172 C.proc.pen.**, deși aceasta este singura metodă legală și științifică prin care se pot verifica integritatea logurilor și originea accesărilor.

Mai mult, ordonanța nu menționează **nicio percheziție informatică** în temeiul **art. 168 C.proc.pen.**, **nicio ridicare de sisteme sau suporturi de stocare** conform **art. 169 C.proc.pen.**, și **nicio măsură de conservare a datelor informatice**conform **art. 170 C.proc.pen.**

Prin urmare, ancheta a fost lipsită de **măsuri minime de asigurare a probelor electronice**, deși din plângere rezulta clar că datele au fost descărcate și se află, cel puțin în parte, în posesia autorului sau a societății acestuia.

La paginile **8–9**, ordonanța mai consemnează că DPO al C.E.C.C.A.R, potrivit raportului din 07.09.2025,concluzionând la acel moment:

„Nu există certitudine că au fost extrase/copiate date cu caracter personal din baza de date.”

Această frază evidențiază o contradicție logică și procedurală: parchetul **afirmă o lipsă de probe fără a fi efectuat acte de verificare (percheziții informatice)**, ceea ce echivalează cu o **constatare bazată pe absența propriei activități investigative**.

Mai mult, Deleanu contrazice prin declarația sa și cum a reușit cu ajutorul unei comezi să extragă toate datele de pe platforma UNBR, iar parchetul nu depune nici un efort să verifice aceste incertitudini care valorifică probatoriu printr-o expertiză informatică.

Nu s-au dispus verificări asupra dispozitivelor, serverelor, conturilor cloud, bazei de date sau aplicației comerciale *incorpo.ro*, deși acestea reprezintă mijloace materiale de probă în sensul art. 97 alin. (2) lit. e C.proc.pen.

<u>Această omisiune a dus la imposibilitatea de a se stabili:</u>

- dacă datele au fost efectiv extrase din sistemele informatice UNBR/CECCAR;
- dacă ele au fost stocate în sisteme controlate de ENTRYRISE S.R.L.;
- dacă au fost utilizate ulterior în scopuri comerciale.

Toate aceste elemente sunt esențiale pentru latura obiectivă a infracțiunilor prevăzute de **art. 360 și art. 364 C.pen.**, iar lipsa lor face ancheta **incompletă și superficială**.

Prin faptul că nu a dispus **expertiza informatică** și **măsuri de conservare a datelor**, parchetul a încălcat obligațiile impuse de:

11 **art. 5 alin. (1) C.proc.pen.** – principiul aflării adevărului;

12 **art. 286 alin. (2) C.proc.pen.** – obligația organului judiciar de a efectua cercetări complete;

13 și **art. 97 alin. (2) lit. e C.proc.pen.** – obligația de a administra și conserva mijloacele materiale de probă.

În concluzie, constatările tehnice reținute în ordonanță sunt **sumare, neconcludente și incomplete**, iar lipsa măsurilor procedurale de conservare face imposibilă verificarea reală a faptelor.

Aceasta conduce la concluzia că soluția de clasare este **netemeinică și nelegală**, fiind emisă **în absența unui probatoriu complet și a unui raționament tehnic verificabil**.

2. **Lipsa oricărei măsuri de conservare** a datelor informatice.

Un alt aspect deosebit de grav al anchetei îl constituie **absența oricărei măsuri de conservare a datelor informatice** și **dependența totală a raționamentului parchetului de declarația autorului Deleanu Ștefan-Lucian**.

La **pagina 8** din ordonanța de clasare, procurorul consemnează că:

„ În aceleași articole anterior descrise, sunt menționate și breșele de securitate la aceste corpuri profesionale, atât la U.N.B.R., C.E.C.C.A.R, precum și demersuri făcute referitor la acestea (..fără

expunere publică, nu se rezolvă nimic, şi U.N.B.R., C.E.C.C.A.R de exemplu a negat breşele de securitate".

„ În cauză, s-a procedat la analizarea datelor existente la dosar, a datelor existente on-line şi a tuturor datelor şi înscrisurilor solicitate şi furnizate organului de urmărire penală, de către U.N.B.R., C.E.C.C.A.R şi A.N.D.P.S.C, fiind reţinute în continuare următoarele (proces-verbal de analiză date/ înscrisuri) ".

Această concluzie este, în fapt, o **presupunere neconfirmată**, întrucât nu s-a dispus **niciun act concret de verificare** — nici **percheziţie informatică (art. 168 C.proc.pen.)**, nici **ridicare de sisteme informatice (art. 169 C.proc.pen.)**, nici **măsură de conservare (art. 170 C.proc.pen.)**.

Cu toate acestea, procurorul a apreciat că **nu mai există date în posesia autorului**, exclusiv în baza propriei declaraţii, potrivit căreia acesta *„nu mai deţine nicio informaţie preluată"*.Această abordare reprezintă **o substituire nepermisă a verificării faptelor printr-o simplă declaraţie de intenţie**, contrară **art. 5 alin. (1) C.proc.pen.**, care impune organului de urmărire penală să caute adevărul prin mijloace probatorii obiective.

Mai mult, dl. Deleanu afirmă că *„a accesat bazele de date pentru a verifica vulnerabilităţile acestora"* şi *„a descărcat informaţiile pentru analiză internă"*, ceea ce presupune **stocarea datelor** pe un suport electronic.

Totuşi, parchetul **nu a dispus ridicarea dispozitivelor folosite** (calculatoare, servere, conturi cloud etc.), pentru a confirma sau infirma aceste afirmaţii.

Astfel, **întregul raţionament al procurorului privind lipsa posesiei datelor** este construit pe **baza propriei declaraţii a persoanei cercetate**, fără nicio verificare tehnică sau independentă.

Aceasta contravine dispoziţiilor:

- **art. 97 alin. (2) lit. e C.proc.pen.**, care califică datele informatice drept mijloace materiale de probă;
- **art. 172 C.proc.pen.**, care impune expertiza atunci când soluţionarea cauzei depinde de aspecte tehnice;
- şi **art. 285 alin. (1) C.proc.pen.**, care obligă procurorul să strângă probele necesare din oficiu, nu să se limiteze la cele oferite de persoana vizată.

Prin urmare, lipsa măsurilor de conservare a datelor informatice **a viciat întreaga anchetă** şi a făcut imposibilă stabilirea exactă a situaţiei de fapt.

Faptul că procurorul a considerat suficientă declaraţia lui Deleanu, fără verificări tehnice, este echivalent cu **delegarea anchetei către persoana cercetată**, ceea ce este incompatibil cu principiile unei urmăriri penale efective şi obiective.

Aceasta este o anchetă formală, fără acte investigative reale. Parchetul nu a epuizat mijloacele prevăzute de lege, ceea ce face ca soluţia de clasare să fie **nelegală (art. 5 alin. 2 C.proc.pen.) şi netemeinică**.

3. **Critici privind temeinicia motivării reținute în ordonanță** – contradicții, omisiuni și erori de raționament

Potrivit ordonanței de clasare din data de 13.10.2024, emisă de DIICOT, analiza activității parchetului relevă o serie de contradicții interne, omisiuni procedurale și erori de raționament juridic care au condus, în mod nejustificat, la soluția de clasare.

Soluția **a fost întemeiată aproape exclusiv pe declarația autorului**, Deleanu Ștefan-Lucian, și **pe câteva adrese sumare** ale instituțiilor **UNBR și CECCAR, fără o verificare reală a situației de fapt și fără administrarea probatoriului necesar**.

La paginile 2–8 din ordonanță, procurorul reține în mod expres că numitul Deleanu Ștefan-Lucian a accesat fără drept platformele informatice aparținând UNBR și CECCAR, descărcând baze de date ce conțineau informații confidențiale și date cu caracter personal. În concret, a accesat platformele UNBR, CECCAR și IEEP; a extras date, inclusiv date personale sensibile ale avocaților și experților contabili; a publicat sau utilizat aceste date pentru scopuri comerciale sau de promovare personală; a recunoscut în propriile postări activități tehnice intruzive (vezi paginile 3–7, referirile la comunicate și înregistrări).

Ordonanța afirmă (pag. 14–15) că faptele lui Deleanu includ prelucrări tehnice și extrageri de date – apoi susține că „nu există elemente obiective". Aceste probleme fac soluția **nelegală** (art. 16 lit. b teza I C.proc.pen.) și **netemeinică**

Totodată, acesta ar fi dezvoltat un software care extrăgea din baza de date a C.E.C.C.A.R și așa a descris și breșele de securitate și vulnerabilitățile.

„Din declarația numitului Deleanu Ștefan–Lucian rezultă că datele pe care le-a obținut fiind accesibile în mod public și nerestricționat, putând fi accesate și descărcate automat de orice utilizator al site-ul C.E.C.C.A.R, el fiind doar cel care a remarcat vulnerabilitatea și a făcut notificarea despre ea, însă acestea sunt contrazise chiar de faptul că acesta a descărcat prin intermediul software datele de pe site-ul C.E.C.C.A.R (vezi pagina 16)

Referitor la situația și vulnerabilitate descoperită la site-ul UNBR, a menționat că atunci când se căutau pe GOOGLE toate paginile IFEP.ro există o pagină web publică care descria modul în care se poate accesa mai multe API-uri publice care, în cazul de față, permitea vizualizarea tuturor avocaților, baroul de proveniență și adresa de e-mail.

Prin comanda „ Get lawyers", *autorul a reușit să vizualizeze și numărul de identificare* al avocaților, CNP-ul baroul de proveniență și adresa de e-mail. Însă comanda presupune și afișarea și descărcarea datelor deoarece acesta a reușit mai departe să se facă cunoscut prin metodele sale să se facă cunoscut.

Pe scurt, întrucât autorul nu a primit răspunsuri din partea ambelor corpuri profesionale, acesta a recurs la contactarea, prin diverse canale, atât a contabililor, cât și a avocaților, invocând existența unor breșe de securitate. Din comportamentul său reiese că scopul nu a fost prevenirea acestor breșe, ci demonstrarea faptului că a pătruns fără drept în sistemele informatice ale acestor entități, a descărcat bazele de date și a contactat ulterior toți avocații și contabilii.

Aceste acțiuni întrunesc elementele constitutive ale infracțiunii prevăzute la **art. 360 Cod penal** – *Accesul ilegal la un sistem informatic*, şi, după caz, pot constitui şi **art. 364 Cod penal**

Nu există **nicio probă obiectivă** — nici percheziție informatică, nici ridicare de echipamente, nici expertiză — care să confirme că datele nu se mai află la autor.

Cu toate acestea, la finalul aceleiaşi secțiuni, procurorul concluzionează că „nu rezultă elemente ale infracțiunilor prevăzute de art. 360 şi art. 364 Cod penal", **motivând că autorul nu ar fi urmărit un folos material.**

Această concluzie este contradictorie, întrucât fapta de accesare a unui sistem informatic fără drept se consumă prin simpla realizare a accesului, indiferent de scopul urmărit.

Procurorul a constatat existența elementului material al infracțiunii, dar a negat tipicitatea acesteia pe baza unei aprecieri subiective a intenției autorului, substituind analiza juridică cu o evaluare morală a comportamentului său.

La pagina 6, ordonanța menționează că „logurile disponibile sunt incomplete" şi că „nu se pot identifica utilizatorii care au accesat serverele". Cu toate acestea, nu s-a dispus efectuarea unei expertize informatice, conform art. 172 Cod procedură penală, deşi o astfel de expertiză era esențială pentru determinarea exactă a sursei şi naturii accesărilor.

De asemenea, la paginile 16–17, se reține că firmele IT care administrau sistemele au transmis doar răspunsuri generale, însă reprezentanții acestora nu au fost audiați. Aceasta reprezintă o omisiune esențială de procedură, contrară art. 114 Cod procedură penală, care impune audierea oricărei persoane ce poate furniza informații utile cauzei.

În lipsa acestor audieri, răspunsurile tehnice au fost interpretate superficial, fără verificări independente.

Mai mult, din ordonanță, **se prezumă că nu există probe că datele se mai află în posesia autorului**. Această afirmație este doar o bănuială şi este contrară logicii juridice şi faptelor reținute, întrucât procurorul nu a dispus nicio măsură de conservare a datelor informatice (art. 170 Cod procedură penală), nicio ridicare de sisteme informatice (art. 169 Cod procedură penală) şi nicio percheziție informatică (art. 168 Cod procedură penală).

În lipsa acestor măsuri, nu se putea stabili dacă datele se mai aflau sau nu în posesia autorului.

Ordonanța se bazează exclusiv pe declarația lui Deleanu, care este cea mai relevantă pentru că parchetul susține că „ nu poate fi angajată răspunderea penală a numitului Deleanu Ștefan- Lucian totodată reprezentant al societății Entryrise Srl- şi faptele nu se pot imputa persoanelor reclamate, nici din punct de vedere obiectiv şi nici subiectiv. În cauză, nu sunt îndeplinite şi întrunite elementele constitutive sub aspectul tipicității obiective ale unor asemenea fapte penale şi deopotrivă, nu se poate considera că acțiunile întreprinse în cauza de numitul Deleanu Ștefan-Lucian- au fost îndeplinite cu rea-credință. Nu se poate astfel considera că în cauză, acesta a acționat în forma de vinovăție prevăzută de lege, respectiv cu intenție calificată de a obține, fără drept, date confidențiale cu caracter personal, aparținând

avocaților/contabililor, prin operațiuni intruzive și neautorizate și care să fi avut drept țintă sistemele informatice care stocau astfel de date private și neexpuse în mod public ”

În opinia noastră, această concluzie care este cea mai determinantă pentru soluționare ordonanței este nefondată.

Procurorul afirmă că nu există nici elemente obiective, nici subiective ale infracțiunii, deși chiar în ordonanță se consemnează că Deleanu **a accesat platformele informatice** ale U.N.B.R. și C.E.C.C.A.R. și **a descărcat baze de date**.

Mai mult decât atât, autorul a și folosit baza de date pentru a contacta avocații și contabilii. Așadar, elementul obiectiv al faptei – accesarea fără drept – **există și este recunoscut chiar de autor**, iar parchetul îl ignoră complet. Afirmația că nu sunt întrunite elementele obiective contrazice propria constatare de fapt a procurorului și dispozițiile art. 360 Cod penal, care sancționează **simplul act de accesare neautorizată**, fără a cere un prejudiciu sau scop material.

Procurorul nu explică de ce **tipicitatea obiectivă** a infracțiunii nu ar fi întrunită și nici care este analiza faptică pe care se întemeiază această concluzie.

În cauză, autorul a realizat o acțiune concretă de **transferare a datelor**, date care au fost **transferate ilegal** și **extrase fără acordul persoanelor vătămate**.

Prin urmare, faptele autorului sunt **consumate**, întrucât **elementul material** al infracțiunii prevăzute la **art. 360 Cod penal** — respectiv **accesarea fără drept a unui sistem informatic și transferul neautorizat de date** — s-a produs în mod efectiv

Nu ne aflăm, așadar, în fața unei simple tentative, ci a unei fapte realizate în întregime, care a produs consecințe juridice și practice clare, prin atingerea adusă confidențialității datelor aparținând persoanelor vătămate.

Tipicitatea obiectivă presupune **identificarea unei acțiuni prevăzute de lege ca infracțiune**. Accesarea fără drept a unui sistem informatic – chiar declarată de făptuitor – se încadrează exact în textul art. 360 alin. (1) Cod penal.

Prin urmare, această frază reprezintă o **simplă afirmație neargumentată**, care nu are suport probator sau logic. Legea nu cere dovedirea „relei-credințe”, ci a **intenției**, directe sau indirecte, de a efectua acțiunea interzisă. Reaua-credință este o noțiune morală, fără corespondent juridic în incriminarea prevăzută de art. 360 și 364 Cod penal.

Mai mult, din conduita autorului rezultă contrariul: folosirea unei identități fictive, utilizarea unui mecanism software specializat pentru extragerea datelor și contactarea ulterioară a unor terți pentru a le arăta că deține informațiile descărcate. (vezi pagina 16).Aceste elemente sunt **indicii clare de premeditare și intenție directă**, incompatibile cu ideea de „bună-credință”.

Procurorul a preluat această afirmație ca probă de nevinovăție, fără a o verifica prin mijloace obiective. Această abordare **contravine art. 103 alin. (2) Cod procedură penală**, potrivit căruia *probele nu au o valoare dinainte stabilită prin lege și sunt supuse liberei aprecieri a organelor judiciare* ***în urma evaluării tuturor probelor administrate în cauză.***

De asemenea, plângerile formulate de UNBR și CECCAR vizau atât persoana fizică, cât și societatea ENTRYRISE S.R.L. Cu toate acestea, ordonanța nu cuprinde nicio analiză privind răspunderea penală a persoanei juridice. Nu se face nicio mențiune privind extinderea urmăririi penale conform art. 489 Cod procedură penală sau audierea reprezentantului legal al societății. Această omisiune încalcă art. 314 alin. (1) Cod procedură penală, care obligă procurorul să soluționeze cauza cu privire la toate persoanele vizate.

La pagina 19, ordonanța dispune clasarea cauzei în temeiul art. 315 alin. (1) lit. b raportat la art. 16 alin. (1) lit. b Cod procedură penală, motivând **că „fapta nu este prevăzută de legea penală”.** Această concluzie este eronată, întrucât faptele descrise sunt expres prevăzute de art. 360 și 364 Cod penal. Procurorul a confundat lipsa vinovăției cu inexistența tipicității, ceea ce considerăm că trebuie remediată.

Afirmația potrivit căreia **Deleanu Ștefan–Lucian** ar fi acționat „din convingerea că realizează o activitate de interes public” este **contradictorie cu propriile fapte și mijloacele utilizate**.

Astfel, potrivit probelor aflate la dosar și recunoașterilor publice ale autorului, **acesta a folosit o identitate virtuală falsă – „Alexandra Ardelean”**, generată prin mijloace de **inteligență artificială**, pentru a transmite mesaje către avocați și pentru a pretinde că ar fi notificat platforma **IFEP** la adresa **help@ifep.ro**.

Un asemenea demers **exclude prin definiție buna-credință**.Un comportament sincer, transparent și de interes public presupune comunicare **directă și asumată**, nu disimularea identității reale sub un avatar fictiv creat special pentru a evita răspunderea.

Mai mult, scopul declarat de autor – acela de a „semnala vulnerabilități tehnice” – este infirmat de **modalitatea de acțiune**:

- folosirea unui cont fictiv,
- transmiterea de mesaje masive către avocați,
- publicarea ulterioară a conținutului acestor mesaje pe rețele sociale,
- și corelarea acestora cu promovarea platformei comerciale **incorpo.ro**

Prin urmare, faptele nu relevă un demers civic, ci un **mecanism construit deliberat pentru autopromovare și atragerea de beneficii comerciale**, în aparența unei „misiuni de interes public”.

Codul penal nu prevede excepții pentru accesul fără drept motivat de intenții presupus nobile. Prin urmare, raționamentul procurorului contravine principiului legalității incriminării (art. 1 Cod penal) și principiului aflării adevărului (art. 5 Cod procedură penală).

Concluzionând, analiza comparativă a paginilor din ordonanță demonstrează că soluția de clasare este nelegală și netemeinică. Parchetul a constatat existența faptelor materiale, dar a ignorat caracterul lor penal, substituind analiza juridică cu o apreciere morală a comportamentului autorului.

În temeiul art. 339 alin. *(3) Cod procedură penală, se impune infirmarea ordonanței de clasare și reluarea urmăririi penale față de Deleanu Ștefan-Lucian și societatea ENTRYRISE S.R.L.*

VI. ANALIZA TEMEIULUI DE CLASARE ȘI A AȘA-ZISEI LIPSE A REA-CREDINȚEI – aplicarea eronată a art. 16 alin. (1) lit. b C. proc. pen. și invalidarea concluziei că Deleanu nu ar fi acționat cu vinovăție

În ordonanța din 13.10.2024, procurorul a dispus clasarea cauzei în temeiul art. 315 alin. (1) lit. b raportat la art. 16 alin. (1) lit. b Cod procedură penală, motivând că „fapta nu este prevăzută de

legea penală". Această interpretare este fundamental eronată, atât sub aspect formal, cât şi material, fiind rezultatul unei confuzii între lipsa tipicităţii şi lipsa vinovăţiei.

Dispoziţiile art. 16 alin. (1) lit. b Cod procedură penală se aplică exclusiv atunci când fapta nu corespunde în mod obiectiv niciunei descrieri din partea specială a Codului penal – adică, în situaţia în care nu există o faptă incriminată de legea penală.

Prin contrast, în cauză, faptele constatate – accesarea fără drept a unor sisteme informatice şi descărcarea de date – corespund integral tiparului juridic al infracţiunilor prevăzute de art. 360 şi art. 364 Cod penal.

În asemenea situaţii, dacă procurorul ar fi apreciat că lipseşte intenţia infracţională, soluţia corectă trebuia întemeiată pe art. 16 alin. (1) lit. b teza finală Cod procedură penală, care prevede că fapta nu este săvârşită cu vinovăţia cerută de lege. Prin urmare, procurorul a greşit atât temeiul de clasare, cât şi calificarea faptelor.

Prin urmare, chiar dacă Deleanu ar fi urmărit demascarea vulnerabilităţilor sistemelor, accesul s-a făcut fără drept, ceea ce atrage răspunderea penală. Fapta rămâne penală chiar şi atunci când scopul invocat este unul aparent de interes public.

Din analiza comportamentului lui Deleanu, consemnată la paginile 2–8 din ordonanţă, nu se poate vorbi despre bună-credinţă, ci dimpotrivă, despre rea-credinţă şi persistenţă infracţională.

Autorul s-a autodenunţat parţial, dar a continuat să desfăşoare activităţi similare, inclusiv prin publicarea pe reţelele sociale a unor materiale prin care expunea vulnerabilităţile unor instituţii publice, sugerând totodată că le poate remedia contra cost.

Această conduită denotă o repulsie faţă de autoritatea instituţională şi un comportament ostentativ, incompatibil cu buna-credinţă.

Temeiul de clasare invocat de procuror – art. 16 alin. (1) lit. b C.proc.pen., raportat la presupusa lipsă a „rea-credinţei" autorului – este aplicat în mod eronat, întrucât evaluarea vinovăţiei s-a realizat pe baza unor simple afirmaţii ale persoanei cercetate, fără verificări tehnice, fără coroborarea probelor şi în contradicţie cu chiar faptele reţinute în ordonanţă.

Procurorul reţine că Deleanu nu ar fi acţionat cu rea-credinţă şi că nu ar fi conştientizat caracterul neautorizat al acţiunilor sale. O asemenea concluzie nu este însă fundamentată pe o analiză juridică, tehnică sau factuală, ci pe o preluare necritică a propriilor declaraţii ale autorului, fără expertiză, fără verificarea modului efectiv în care a fost creat şi utilizat scriptul, fără examinarea serverelor şi fără analiza volumului de date extrase.

Această justificare este contrazisă de elemente obiective, exprimate chiar în ordonanţă deoarece Deleanu a utilizat infrastructura unei **societăţi comerciale** pentru a crea şi rula un script automatizat dedicat extragerii datelor, a accesat platformele a repetitiv, sistematic, organizat. Datele extrase au fost stocate pe servere proprii, în volume semnificative folosind şi utilizat identităţi sau conturi improprii pentru a contacta avocaţi. Este de reţinut că Deleanu are o operaţiunea care are un scop comercial, tehnic sau informativ, rezultând din proiectele dezvoltate de ENTRYRISE şi mai ales cu persoane din afara ţării.

Aceste argumente sunt incompatibile cu ideea că autorul „nu ar fi ştiut" că acţionează fără drept.

Dimpotrivă, ele relevă o activitate planificată, tehnic elaborată, desfășurată pe o perioadă extinsă și cu utilizarea unor instrumente concepute de el însuși. Nicio persoană care concepe un script pentru extragerea masivă a datelor din platforme ale unor profesii juridice nu poate susține credibil că ar fi considerat o asemenea activitate ca fiind autorizată sau benignă.

În plus, infracțiunile din art. 360 și 364 C.pen. sunt infracțiuni de acțiune, nu de rezultat. Vinovăția constă în simpla **conștientizare a caracterului neautorizat al accesului**.

Procurorul nu explică în niciun moment de ce Deleanu ar fi considerat că are dreptul de a automatiza accesarea platformelor profesionale sau de a extrage date ale avocaților, inclusiv date sensibile, pentru stocare pe servere proprii.

Mai important, concluzia DIICOT ignoră complet faptul că pretinsa „lipsă a rea-credinței" nu poate fi stabilită fără expertiză informatică privind modul de funcționare al scriptului; fără analiza tehnică a serverelor ENTRYRISE; fără verificarea logurilor; fără examinarea volumului de date procesate și fără verificarea eventualelor utilizări ale datelor.

În lipsa acestor probe, procurorul nu avea cum să aprecieze vinovăția și nu putea aplica art. 16 alin. (1) lit. b C.proc.pen., pentru că nu deținea elementele necesare unei astfel de concluzii. O soluție de clasare nu poate suplini absența probelor prin acceptarea necritică a declarațiilor făptuitorului.

Mai mult, justificarea că „nu a acționat cu rea-credință" este în realitate o concluzie inaplicabilă tehnic și juridic. Reaua-credință nu se raportează la scopul ulterior al datelor colectate, ci la **conștiința caracterului neautorizat al accesului**. Indiferent de scopul declarat, extragerea automatizată de date din sisteme care nu îți aparțin, folosind scripturi dedicate, presupune, în mod inevitabil, conștiința caracterului ilicit al faptei.

Astfel, nu doar că DIICOT nu a demonstrat lipsa rea-credinței, dar chiar ordonanța sa arată existența unei conduite care exclude orice ipoteză de nevinovăție tehnică sau juridică.

Aplicarea art. 16 alin. (1) lit. b C.proc.pen., în lipsa unei anchete complete și în contradicție cu elementele obiective ale cauzei, este nelegală și netemeinică.

În concluzie, temeiul pentru care s-a dispus clasarea este fundamental greșit, soluția fiind construită pe o premisă artificială – aceea că Deleanu nu ar fi acționat cu vinovăție – premisă care este infirmată de probele din dosar, de modul său de operare și de lipsa totală a unei verificări tehnice independente. Prin urmare, soluția nu poate fi menținută.

VII. NELEGALITATEA ȘI NETEMEINICIA ORDONANȚEI PROCURORULUI-ȘEF DIICOT DIN 17.11.2025

După comunicarea plângerii împotriva ordonanței de clasare, ne-a fost comunicată, în sensul soluționării, ordonanța procurorului-șef DIICOT nr. 3812/II-1/2025 din 17.11.2025, **prin care a fost respinsă plângerea persoanei vătămate**, care în opinia noastră, este în mod evident **nelegală și netemeinică**, atât prin modul în care a fost redactată și motivată, cât și prin contradicțiile pe care le conține.

În locul unui control ierarhic efectiv, procurorul-șef a emis un act cu caracter pur confirmativ, în care fragmente semnificative sunt **copiate sau parafrazate** din ordonanța atacată, fără a se adăuga vreo analiză proprie.

O primă problemă evidentă este structura actului și se evidențiază în paginile 1–18 (conform numerotării interne) prin care se limitează la a reproduce pe larg conținutul ordonanței de clasare,

expunerea factuală a DIICOT şi istoricul dosarului, fără să realizeze o verificare autonomă ori o evaluare critică a celor dispuse de procurorul de caz.

În loc să examineze motivele de nelegalitate şi netemeinicie semnalate de persoana vătămată şi să ne răspundă la toate aceste argumente, procurorul-şef se rezumă la a copia sau rezuma fragmente din actul atacat, ceea ce lipseşte de conţinut funcţia legală a controlului ierarhic prevăzut de art. 339 C.proc.pen.

În continuare, ordonanţa enumeră sumar argumentele plângerii UNBR, însă fără să ofere un răspuns la vreunul dintre ele. Această secţiune apare mai degrabă ca o formalitate de copiere decât ca un exerciţiu de motivare. Nici încălcarea dreptului la apărare, nici menţinerea nelegală a urmăririi penale în faza *in rem*, nici lipsa expertizei IT, nici neconservarea probelor, nici ignorarea răspunderii persoanei juridice ENTRYRISE S.R.L. nu sunt analizate, discutate sau evaluate. Ordonanţa trece complet sub tăcere aceste aspecte, deşi fiecare dintre ele reprezenta un viciu procedural sau factual cu impact determinant asupra legalităţii soluţiei.

Prima pagină ((pagina 20) privind analiza şi motivele plângerii, care sunt contradictorii şi fără o analiză aprofundată atât cu privire la legalitate şi temeinicie conţine afirmaţia generală că „plângerea a fost analizată în raport de dispoziţiile legale aplicabile" însă în vid, **pentru că în paginile anterioare nu se regăseşte nicio analiză nici asupra refuzului nejustificat de a permite accesul la dosar, nici asupra menţinerii nelegale a urmăririi penale exclusiv în faza in rem, nici asupra absenţei expertizei informatice, nici asupra neconservării probelor electronice ori a lipsei verificării răspunderii persoanei juridice ENTRYRISE S.R.L.**

Procurorul-şef nu discută nicio critică, nu îşi exprimă punctul de vedere asupra vreuneia dintre ele şi nu verifică legalitatea niciunui act de urmărire penală. Simplul enunţ că „plângerea a fost analizată" este contrazis de propriul corp al ordonanţei, care arată, fără echivoc, lipsa totală a oricărei evaluări.

Tot pe pagina 20, procurorul-şef susţine că aspectele invocate **„nu sunt de natură să conducă la schimbarea soluţiei",** fără a arăta care sunt aceste aspecte, cum au fost examinate şi de ce ar fi lipsite de relevanţă.

Nu există nicio trimitere la probe, nicio apreciere legală, nicio explicaţie asupra unor noţiuni precum „intenţie", „acces neautorizat", „transfer de date", „folosirea scripturilor", „obligaţia expertizei" sau „obligaţia de a schimba calitatea procesuală".

Concluzia apare pur şi simplu enunţată, fără suport, ceea ce transformă această parte a ordonanţei într-un exerciţiu formal, lipsit de orice valoare juridică.

În continuare, aceeaşi linie superficială, se reia, în mod aproape mecanic, ideea că „nu rezultă intenţia făptuitorului", deşi întregul mod de operare descris în ordonanţa DIICOT — scrierea unui script, rularea lui repetată, extragerea automatizată a datelor, stocarea pe servere, utilizarea resurselor unei persoane juridice — arată exact contrariul. În loc să constate această contradicţie evidentă, procurorul-şef o ignoră, asumând necritic concluzia DIICOT, deşi aceasta nu este justificată de probe.

Apoi la pagina următoare continuă în aceeaşi manieră, avansând concluzia că Deleanu „nu ar fi acţionat cu rea-credinţă".

Această afirmaţie nu este însoţită de niciun element de fapt sau raţionament juridic.

Procurorul-şef nu explică pe ce probe se bazează, nu indică vreun element care să demonstreze lipsa vinovăţiei, nu arată de ce ar fi putut crede făptuitorul că extragerea automatizată a datelor

avocaților ar fi permisă și nu justifică în niciun fel aplicarea art. 16 alin. (1) lit. b C.proc.pen. În realitate, această concluzie este pur declarativă și se sprijină exclusiv pe afirmațiile făptuitorului, fără ca acestea să fie verificate prin acte de urmărire penală : expertiză informatică, analiză tehnică a serverelor, verificarea logurilor sau alte mijloace obiective.

La pagina 23 apare poate cea mai surprinzătoare afirmație: aceea că „fapta nu întrunește elementele constitutive ale infracțiunilor sesizate".

Procurorul-șef **nu explică însă nici care dintre elemente ar lipsi, nici în ce constă analiza lui asupra laturii obiective sau subiective, nici de ce activitatea tehnică complexă a autorului nu ar constitui acces neautorizat sau transfer nelegal de date**.

Această concluzie este, așadar, în vădită contradicție cu situația de fapt constatată chiar de DIICOT și, evident, cu lipsa totală a unei evaluări tehnice necesare.

În final, pagina 24 încheie ordonanța cu formula că „nu se impune admiterea plângerii", deoarece soluția DIICOT ar fi „legală și temeinică".

Întreaga structură a ordonanței contrazice însă această afirmație: nu există analiză, nu există verificare, nu există raportare la critici, nu există fundamentari juridice.

Concluzia finală este lipsită de orice suport, ceea ce face ca ordonanța procurorului-șef să fie, în mod evident, nelegală și netemeinică, întrucât nu îndeplinește cerința de motivare efectivă și nu constituie un control ierarhic veritabil.

Astfel, paginile 20–24 ale ordonanței procurorului-șef nu doar că nu remediază viciile ordonanței DIICOT, ci adaugă propriile contradicții și omisiuni, consolidând caracterul superficial și formal al soluției. Ordonanța nu poate fi menținută, deoarece nu respectă exigențele minime ale art. 339 C.proc.pen. și jurisprudenței constante privind motivarea actelor procurorului.

Prin urmare, această ordonanță trebuie desființată împreună cu ordonanța de clasare, cauza impunându-se a fi retrimisă la procuror pentru completarea urmăririi penale.

VIII. ACTIVITATEA ACTUALĂ A LUI DELEANU ȘI CONSECINȚELE ASUPRA LEGALITĂȚII SOLUȚIEI DE CLASARE

Din analiza înscrisurilor anexate și comunicate către parchet rezultă că numitul Deleanu Ștefan-Lucian continuă și în prezent activitățile care au constituit obiectul dosarului penal anterior, respectiv accesarea și prelucrarea neautorizată a datelor informatice aparținând unor instituții ale statului, însă parchetul comunică că nu sunt importante și nu rezultă un caz de sesizare din oficiu banalizând orice acțiune a numitului DELEANU.

Astfel, în postările sale publice din data de 19 august 2025 pe grupul antreprenorilor din romania, acesta afirmă în mod explicit că:

https://www.facebook.com/groups/grupulantreprenorilordinromania/posts/4174017232834266/

„Punctul 1.2 din breșă: sunt obligat să dau mai multe detalii pentru că Ministerul Justiției pare să nu vrea să soluționeze problema și se eschivează din a-și asuma răspunderea."

„🏛️ Ministerul Justiției: Este doar vina CSM.”

„🌐 Site-ul Portal.Just.Ro: (Număr dosar) în antet, folosiți parola: 1234abcd tot în document.”

29

„Dl. Deleanu continuă în prezent cu aceeaşi activitate pe site-urile Portal. Just şi a CSM, procedând întocmai ca şi cum este cu bună credinţă, verificând în continuare breşe de securitate şi la alte instituţii publice şi colectând date din sistemul de justiţie prin pasivitatea organului de urmărire penală, fără acordul instituţiilor vizate.”

„Ministerul Justiției: Nu suntem responsabili de breșa de date de la CSM și Ministerul Justiției.”

Aceste afirmaţii constituie recunoaşteri publice ale faptului că persoana continuă să acceseze, să colecteze și să difuzeze date informatice provenite din platforme aparţinând autorităţilor judiciare.

Mai mult, el expune public vulnerabilităţi ale sistemelor informatice ale CSM şi Ministerului Justiției, indicând chiar parole şi modalităţi de acces, fapt ce demonstrează o conduită ostentativă şi sfidătoare faţă de lege.

Prin urmare, se poate constata că activitatea ilicită a lui Deleanu nu s-a oprit, **ci s-a intensificat,** fiind în prezent realizată în mod public, prin intermediul reţelelor de socializare. Aceasta relevă persistența comportamentului infracţional, în condiţiile în care faptele se desfăşoară sub aparența unei „campanii de transparență”, dar au caracter penal evident.

Această conduită dovedeşte că soluţia de clasare pronunţată la data de 13.10.2024 a fost prematură şi netemeinică, întrucât nu s-au dispus măsuri de conservare a datelor informatice, nu s-a stabilit cu exactitate dacă fapta a încetat, iar procurorul nu a impus nicio interdicţie privind utilizarea sistemelor informatice, permiţând astfel continuarea faptelor.

În raport de aceste noi elemente, sunt incidente dispoziţiile art. 335 alin. (1) Cod procedură penală, potrivit cărora: „Când după clasare sau renunţare la urmărirea penală apar fapte noi sau împrejurări care justifică reluarea urmăririi penale, procurorul dispune redeschiderea acesteia.”

Prin urmare, faptele ulterioare comise de Deleanu Ştefan-Lucian, de aceeaşi natură cu cele cercetate iniţial, impun reluarea urmăririi penale, fiind întrunite condiţiile legale: existența unor noi date (postările publice din 2025), continuarea activităţii ilicit-identice cu cea din dosarul clasat, şi persistența pericolului social şi a încălcării drepturilor instituţiilor vătămate (UNBR, CECCAR, CSM, Ministerul Justiției).

Comportamentul actual al lui Deleanu exclude orice formă de **bună-credinţă** invocată de procuror în ordonanța de clasare. Publicarea repetată a datelor confidenţiale, acuzarea instituţiilor statului sau instituţiilor publice şi private şi utilizarea unor formulări provocatoare denotă intenția de a expune şi compromite autoritatea publică şi privată, nu de a coopera cu aceasta.

Buna-credinţă, în sens juridic, presupune respectarea legii şi cooperarea cu organele statului; în schimb, atitudinea actuală a persoanei cercetate reflectă rea-credinţă, constând în persistența în fapta ilicită, refuzul de a colabora cu autorităţile şi justificarea publică a propriilor încălcări prin invocarea unui pretins „interes public”.

Prin urmare, situația de fapt actuală impune reconsiderarea soluției de clasare din 13.10.2024 și redeschiderea urmăririi penale conform art. 335 alin. (1) Cod procedură penală, cu administrarea de noi probe privind activitatea online a lui Deleanu, prin verificarea conturilor publice, a adreselor IP și a datelor postate pe platformele Portal.just.ro și CSM, precum și verificarea răspunderii penale a persoanei juridice ENTRYRISE S.R.L., în cadrul aceleiași proceduri.

Prejudiciul social este major, întrucât implică date cu caracter personal și informații confidențiale ale unor organizații profesionale de interes public, iar din înscrisurile și date publice rezultă că acesta deține în continuare o bază de date considerabilă și continua cu aceeași intensitate la toate instituțiile publice.

Dacă ne raportăm la persoana fizică **Deleanu Ștefan-Lucian**, în calitate de **asociat unic și administrator** al societății **ENTRYRISE S.R.L.**, cu sediul social în **județul Suceava, orașul Gura Humorului, Bulevardul Bucovina, bloc D18, scara A, ap. 2**, identificată prin **J33/46/2021** și **C.U.I./C.I.F. 43541700**, având ca obiect principal de activitate, potrivit codificării **CAEN Rev. 2 (Ordin nr. 337/2007), „Activități de realizare a softului la comandă (software orientat client.**

Potrivit datelor existente pe portalul **Oficiului Național al Registrului Comerțului (ONRC)**, societatea **ENTRYRISE S.R.L.** are calitatea de **administrator persoană juridică** cu **puteri limitate** și, totodată, **găzduiește sediile sociale ale unui număr de opt societăți cu răspundere limitată**, într-un imobil situat în **municipiul Cluj-Napoca, str. Aurel Vlaicu nr. 2, bloc 5A, scara I, etaj VII, apartament 28**, cu o **suprafață utilă de 55,1 mp**.

Acest imobil se află în **proprietatea numitului Deleanu Ștefan-Lucian**, aspect care rezultă din **extrasul de carte funciară de informare** atașat plângeri penale depusă de către U.N.B.R (Anexa nr. 12 din plângerea penală). De asemenea, potrivit evidențelor ONRC, **sediile sociale ale celor opt societăți menționate** sunt **înregistrate la aceeași adresă**, aspect confirmat prin **Anexa nr. 11** la plângerea penală.

Din lista societăților comerciale menționată anterior rezultă că sunt înființate societăți comerciale ce au ca asociați și/sau administratori persoane fizice cu domiciliul în România, China, Tunisia, Maroc, Turcia (cu cetățenie britanică), Bulgaria și Croația.

În concluzie, toate elementele constitutive ale infracțiunilor prevăzute de art. 360 și art. 364 Cod penal sunt întrunite în persoana lui Deleanu Ștefan-Lucian, administrator al ENTRYRISE SRL deoarece a acționat ca subiect activ fără drept, cu intenție directă, a accesat sisteme informatice aparținând UNBR și CECCAR, fără acordul acestora, a descărcat și transferat baze de date ce conțineau informații confidențiale și date cu caracter personal, pe care le deține, fără drept și a utilizat aceste date **în scop comercial**, ceea ce dovedește caracterul intenționat și ilicit al acțiunii.

Critica de temeinicie privind conținutul ordonanței parchetului este cel puțin contradictorie, arată o cercetarea vagă și lacunară asupra societății (persoana juridică ENTRYRISE SRL) însă cu o soluție similară a persoanei fizice, în sensul clasării, iar motivul este că indiferent câte probe incriminează activitatea persoanei fizice și juridice, soluția rămâne clasarea deoarece a acționat cu bună-credință. De ex. toate datele colectate prin natura infracțiunii cui aparțin.. mai mult decât atât aceste date cu caracter personal, adrese reprezintă o valoare care poate fi vândută sau deținută de

DOMNULUI [illegible] AL TRIBUNALULUI BUCUREȘTI- SECȚIA PENALĂ

alte entități care nu au drept și nici acordul persoanelor vizate, chiar dacă toate astea în opinia parchetului sunt cu bună-credință.

IX. CONSECINȚELE CONCRETE ALE FAPTELOR – IMPACTUL ASUPRA PERSOANELOR VĂTĂMATE ȘI ASUPRA INSTITUȚIILOR PUBLICE

Faptele descrise în dosar nu sunt simple incidente tehnice sau erori izolate, ci reprezintă o ingerință gravă și sistematică în activitatea profesională a avocaților, a organelor profesionale și, prin efectele lor indirecte, asupra instituțiilor publice care depind de funcționarea corectă și confidențială a profesiei.

Consecințele sunt multiple, profunde și afectează atât persoanele fizice vizate, cât și instituțiile care garantează funcționarea statului de drept.

Primul și cel mai grav efect îl reprezintă compromiterea datelor și informațiilor aparținând avocaților. Extragerea automatizată, neautorizată și în volum considerabil a datelor profesionale : date de contact, date privind activitatea, apartenența profesională și alte informații sensibile – a expus membrii profesiei unor riscuri reale: utilizarea necontrolată a acestor date, distribuirea lor către terți, prelucrarea lor în scopuri comerciale sau chiar manipularea lor pentru a influența decizii profesionale ori comerciale.

Impactul asupra avocaților nu este unul teoretic, ci concret, întrucât fiecare avocat a pierdut controlul asupra propriilor date, iar această pierdere este ireversibilă.

În al doilea rând, faptele au produs prejudicii directe Uniunii Naționale a Barourilor din România și barourilor componente, afectând reputația instituțională, încrederea publică și capacitatea de administrare securizată a datelor membrilor. UNBR a fost pusă în situația nedorită de a gestiona consecințele unui incident informatic care nu a fost declanșat de propria culpă, dar care i-a fost imputat în percepția publică.

Lipsa unei reacții ferme a organelor judiciare nu doar că prelungește prejudiciul, ci transmite public impresia falsă că protecția datelor avocaților nu ar fi o prioritate instituțională.

Activitatea desfășurată de numitul **Deleanu Ștefan-Lucian**, prin intermediul societății **ENTRYRISE S.R.L.**, a generat consecințe grave și extinse, atât asupra **persoanelor fizice vizate**, cât și asupra **instituțiilor publice și profesiilor de interes public** implicate.

În altă ordine de idei, accesarea și descărcarea neautorizată a bazelor de date aparținând **Uniunii Naționale a Barourilor din România (UNBR)** și **Corpul Experților Contabili și Contabililor Autorizați din România (CECCAR)** a afectat **drepturile fundamentale la viață privată, la protecția datelor cu caracter personal și la confidențialitatea profesională** a unui număr considerabil de **avocați și experți contabili**.

Datele preluate din aceste platforme includeau informații privind **identitatea profesională, adresele de contact, afilierile instituționale și date financiare**, toate fiind protejate de **art. 8 din**

Convenția Europeană a Drepturilor Omului, Regulamentul (UE) 2016/679 (GDPR) și Legea nr. 190/2018.

AVOCAȚII REPREZINTĂ O CATEGORIE PROFESIONALĂ INDISPENSABILĂ FUNCȚIONĂRII JUSTIȚIEI.

Integritatea datelor lor și caracterul predictibil al comunicărilor oficiale sunt fundamentale pentru activitatea instanțelor, parchetelor, organelor de poliție, instituțiilor administrative și autorităților fiscale. Atunci când o terță persoană creează canale paralele, ocolește mecanismele instituționale sau se substituie comunicării oficiale, afectarea nu este doar individuală, ci sistemică.

Astfel, faptele au generat un risc real pentru funcționarea corectă a instituțiilor publice, întrucât au perturbat fluxurile normale de informare, au creat confuzie privind proveniența mesajelor și au expus profesia la vulnerabilități informatice care pot fi exploatate ulterior.

Prin publicarea și utilizarea acestor date în scop comercial, în cadrul platformei **incorpo.ro**, s-a creat o stare de **incredere publică grav afectată** între profesiile juridice și economice, cu efecte directe asupra **autorității instituționale a profesiilor liberale**.

Această situație nu reprezintă doar un incident tehnic, ci un **atac direct la integritatea datelor profesionale** și la principiul autonomiei instituționale consacrat de **Legea nr. 51/1995 privind organizarea și exercitarea profesiei de avocat** și **O.G. nr. 65/1994 privind organizarea CECCAR**.

În al doilea rând, continuarea activității infracționale, confirmată prin postările publice din luna august 2025, vizează în mod explicit **sistemele informatice ale Consiliului Superior al Magistraturii (CSM)** și **Ministerului Justiției**, respectiv platformele **Portal.just.ro** și **site-ul oficial al CSM**.Prin expunerea publică a vulnerabilităților acestor sisteme și publicarea unor **parole, proceduri interne sau date judiciare confidențiale**, s-a produs o atingere gravă adusă **autorității puterii judecătorești**, punând în pericol **securitatea datelor judiciare și a infrastructurii electronice a justiției**.

Această conduită persistă și demonstrează **intenția de a submina încrederea publică în instituțiile sistemului judiciar**, constituind un **risc sistemic de securitate cibernetică**.

Prin **ignorarea solicitărilor de probatoriu** formulate de persoana vătămată și prin **neaplicarea măsurilor legale privind efectuarea percheziților informatice și ridicarea echipamentelor utilizate pentru activitatea infracțională**, parchetul a creat premisa continuării faptelor.
Astfel, autorul a fost lăsat să își desfășoare nestingherit activitatea, sub pretextul unei așa-numite „campanii de transparență", transformând o faptă penală într-o acțiune repetată și persistentă, de natură să aducă atingere gravă interesului public major.

În aceste condiții, consecințele juridice și instituționale ale inacțiunii procurorului sunt deosebit de grave:

- afectarea încrederii publicului în protecția datelor gestionate de instituțiile judiciare și profesiile reglementate;
- compromiterea integrității și confidențialității datelor profesionale;

- perpetuarea unui precedent periculos, prin care accesul fără drept la sisteme informatice este tratat ca un act de „bună-credință", contrar principiilor statului de drept.

Într-o cauză care privește **securitatea sistemelor informatice ale justiției** și **protecția datelor a mii de profesioniști**, lipsa unei reacții ferme a organului de urmărire penală echivalează cu **negarea obligației constituționale a statului de a asigura un proces penal efectiv și o protecție reală a drepturilor fundamentale**.

Consecințele nu se limitează la prejudicii de imagine sau confuzie publică; ele ating chiar esența protecției profesiei de avocat și a confidențialității care o însoțește. Extragerea de date în mod organizat și neautorizat subminează principiile autonomiei profesiei, ale protecției informațiilor sensibile și ale încrederii reciproce dintre avocați, instituții și public. În lipsa unei reacții judiciare adecvate, aceste consecințe riscă să se amplifice, consolidând percepția că asemenea intervenții neautorizate nu sunt sancționate, ceea ce ar crea un precedent periculos.

Pentru toate aceste motive, impactul faptelor este unul profund, real și continuu, ceea ce exclude orice minimalizare sau justificare a lor.

În mod inevitabil, consecințele produse impun reluarea și completarea urmăririi penale, întrucât nu ne aflăm în fața unei situații lipsite de gravitate, ci a uneia care a afectat o categorie profesională întreagă și instituții publice esențiale pentru funcționarea justiției.

Jurisprudența CEDO și CJUE confirmă că extragerea și prelucrarea neautorizată a datelor personale reprezintă o atingere gravă a vieții private și impune autorităților obligația pozitivă de a desfășura o anchetă efectivă (K.U. c. Finlandei, Peck c. Regatului Unit, Rotaru c. României, Digital Rights Ireland, Breyer).
De asemenea, Înalta Curte a stabilit constant că lipsa motivării reale a actelor procurorului și neefectuarea actelor esențiale ale urmăririi penale atrag nelegalitatea și netemeinicia soluției (RIL 51/2017, 4/2018; Decizia 1.657/2019).

În concluzie, consecințele concrete ale faptelor – pierderea controlului asupra datelor profesionale ale avocaților, afectarea instituțională a UNBR, vulnerabilizarea profesiei și riscurile sistemice pentru funcționarea justiției – se subsumează tipologiilor sancționate de aceste hotărâri, ceea ce impune reluarea urmăririi penale.

o

Cum poate fi calificată drept acțiune din partea numitului DELEANU LUCIAN ȘTEFAN în interes public o activitate desfășurată prin intermediul unei **societăți comerciale private** **ENTRYRISE S.R.L**, care folosește resursele companiei, care dezvoltă software și utilizează **mecanisme software complexe de extragere automată a datelor**, obținute **fără drept** din bazele informatice ale unor instituții publice și profesionale, le **stochează**, le **integrează în platforme proprii** și ulterior oferă **„servicii de remediere" contra cost** chiar instituțiilor ale căror sisteme au fost anterior compromise ?

Cum poate fi numită **„bună-credință"** o conduită în care autorul creează **mecanisme speciale de software**, exploatează **vulnerabilitățile sistemelor informatice pentru a-și promova propria**

companie, şi apoi invocă **interesul public** ca scut împotriva răspunderii penale, în timp ce **profită economic şi** de rezultatele acestor acţiuni.

Difuzarea publică a unor vulnerabilităţi ale sistemelor aparţinând unor instituţii profesionale şi publice nu este echivalentă cu o acţiune tehnică de **„white-hat"** făcută în parteneriat cu titularii sistemelor; **dimpotrivă,** expunerea publică a unor informaţii sensibile transformă acele vulnerabilităţi în instrumente exploatabile de terţi .

În contextul susţinerii autorului că ar fi acţionat „pentru a identifica vulnerabilităţile sistemelor informatice şi a contribui la securizarea acestora", se ridică o întrebare elementară, de ordin tehnic şi logic:

De ce au fost vizate în mod repetat instituţii publice şi profesionale – U.N.B.R., C.E.C.C.A.R., şi recent Ministerul Justiţiei şi C.S.M. – şi nu au fost contactate firmele specializate care asigurau administrarea, mentenanţa şi securitatea acestor platforme informatice?

Orice persoană cu pregătire în domeniul IT sau în securitate cibernetică cunoaşte că o intervenţie legitimă, cu bună-credinţă, asupra unui sistem informatic presupune **contactarea administratorului tehnic sau a firmei de mentenanţă**, nu **accesarea directă a avocaţilor şi contabililor**, cu datele descarcate care sunt confidenţiale şi cu caracter personal.

În mod paradoxal, autorul a ales **să atace direct sistemele informatice ale instituţiilor**, fără niciun mandat, fără o cerere oficială şi fără o notificare prealabilă către operatorii tehnici, deşi aceştia ar fi fost **singurii interlocutori legitimi** pentru o colaborare în scopul „identificării vulnerabilităţilor".

Această conduită **nu poate fi asociată bunei-credinţe** şi nici unui interes public, ci demonstrează **intenţia deliberată de a accesa şi extrage date din sisteme informatice protejate**, sub pretextul unui demers tehnic, dar în fapt cu scopul de a obţine informaţii şi notorietate prin expunerea publică a acestor vulnerabilităţi.

○

În consecinţă, afirmaţia bunei-credinţe devine neconvingătoare în faţa modalităţii de operare şi a comportamentului descris: instrumentalizarea unor vulnerabilităţi neautorizate pentru a crea un produs/platformă comercială şi pentru a oferi ulterior „remedieri contra cost" constituie, în fapt, un mod de valorificare economică a informaţiilor dobândite ilegal, ceea ce relevă intenţie, premeditare şi scop patrimonial ce justifică continuarea cercetărilor penale. Mai mult decât atât, scopul activităţii acestuia a fost legat de o platforma NOR

Apoi, autorul a utilizat **o adresa de e-mail a unei persoane virtuale**, creată cu ajutorul unor instrumente de inteligenţă artificială, pentru a contacta U.N.B.R. apoi prin intermediul societăţii a contactat avocaţi şi alte persoane vizate, transmiţând prin **SMS** mesaje în care afirma că „deţine informaţiile extrase" din bazele de date ale UNBR şi CECCAR.

Această conduită demonstrează un **grad ridicat de disimulare, planificare şi control asupra datelor**, contrar oricărei idei de transparenţă sau colaborare cu autorităţile.

Aşadar, nu ne aflăm în faţa unui act de semnalare tehnică a unor vulnerabilităţi, ci a unei **continuări deliberate a unei activităţi informatice ilicite**, fără drept, fără solicitare sau mandat/contract din partea cuiva şi sunt desfăşurate prin mijloace de comunicare virtuale şi cu o intenţie clară de a influenţa şi intimida numai cu scopul de a fi contactat pentru serviciile acestuia.

În realitate, **interesul public nu poate fi revendicat de cel care îl subminează**, iar **buna-credinţă** nu poate fi transformată într-un **instrument de câştig pentru sine.**

Codul penal nu consacră buna-credinţă ca **excepţie de la răspunderea penală**, iar principiul legalităţii (art. 1 C.pen.) nu permite substituirea normei juridice prin justificări morale sau economice.

o

Faţă de toate argumentele şi probele expuse anterior, rezultă în mod clar că soluţia de clasare dispusă în dosarul nr. 364/19/P/2024 este **nelegală şi netemeinică**, fiind pronunţată în lipsa unei cercetări efective şi complete.

Procurorul de caz a dispus clasarea cauzei fără administrarea probelor esenţiale, fără dispunerea unei expertize informatice independente, fără efectuarea percheziţiilor şi ridicării echipamentelor utilizate, fără verificarea posesiei actuale a datelor şi fără cercetarea distinctă a **persoanei juridice ENTRYRISE S.R.L.**, deşi aceasta a fost expres indicată în plângerea penală.

Totodată, soluţia s-a întemeiat exclusiv pe declaraţia autorului, **nesusţinută de alte mijloace de probă**, contrar dispoziţiilor art. 103 alin. (2) Cod procedură penală, care impun coroborarea oricărei declaraţii cu alte probe, respectiv expertiza informatică.

În mod vădit, **DIICOT nu a dispus niciuna dintre măsurile procedurale prevăzute de lege** pentru cauze de criminalitate informatică, respectiv:

- percheziţia informatică asupra echipamentelor aparţinând numitului **Deleanu Ştefan-Lucian** şi societăţii **ENTRYRISE S.R.L.;**
- ridicarea dispozitivelor, serverelor, unităţilor de stocare şi conturilor cloud folosite pentru descărcarea şi prelucrarea datelor;
- expertiză tehnică independentă asupra logurilor şi sistemelor informatice UNBR şi CECCAR;
- audierea reprezentanţilor firmelor IT care asigurau mentenanţa şi hostingul platformelor informatice afectate.

În absenţa acestor acte de urmărire penală, procurorul nu putea stabili **nici sursa şi natura exactă a accesărilor, nici dacă datele se mai află în posesia autorului sau a persoanei juridice**. Concluzia din ordonanţă potrivit căreia „nu există probe că datele s-ar mai afla în posesia autorului" este o simplă presupunere bazată exclusiv pe autodeclaraţia făptuitorului — o probă subiectivă şi neverificată, fără valoare juridică autonomă.

Această conduită contravine dispoziţiilor art. 5 alin. (2), art. 100, art. 103 alin. (2) şi art. 314 alin. (1) Cod procedură penală, care impun procurorului obligaţia de a efectua **o anchetă completă, obiectivă şi efectivă**, cu soluţionarea distinctă a cauzei faţă de toate persoanele vizate.

În plus, **refuzul DIICOT de a permite consultarea și fotocopierea dosarului** de către persoana vătămată, motivat de faptul că cererea a fost depusă „după clasare", constituie o încălcare gravă a dreptului la apărare consacrat de art. 24 Constituție și art. 94 Cod procedură penală, fiind sancționată de **Decizia nr. 215/2017 a Înaltei Curți de Casație și Justiție**.

În temeiul **Art. 339 alin. (3), art. 340 și art. 341 alin. (6) lit. b) Cod procedură penală**, raportat la **art. 94, art. 100, art. 170–172 C.proc.pen.**, precum și **art. 112 alin. (1) lit. b), art. 135 și art. 360–364 Cod penală**, solicit respectuos instanței:

1. **Să admită prezenta plângere** formulată de Uniunea Națională a Barourilor din România;
2. **Să desființați Ordonanța de clasare nr. 364/19/P/2024 din 12.10.2025**, ca fiind nelegală și netemeinică și **Ordonanța procurorului-șef DIICOT nr. 3812/II-1/2025 din 17.11.2025 (respingerea plângerii);**
3. **Să trimită cauza la parchet și să dispună completarea urmăririi penale, cu continuarea acesteia IN PERSONAM față de numitul Deleanu Ștefan-Lucian și față de persoana juridică ENTRYRISE S.R.L., în vederea analizării condițiilor legale pentru punerea în mișcare a acțiunii penale.**

4. **SĂ DISPUNĂ COMPLETAREA PROBATORIULUI**, INCLUSIV PRIN:

Instanța este rugată să dispună ca procurorul să efectueze următoarele acte de urmărire penală indispensabile aflării adevărului:

a) Audierea persoanelor vătămate – U.N.B.R. și C.E.C.C.A.R., cu explicitarea prejudiciului și a modului de operare.

b) Audierea reprezentanților firmelor IT administratoare ale platformelor profesionale, pentru clarificarea regimului de acces și a eventualelor vulnerabilități exploatate.

c) Dispunerea percheziților informatice la domiciliul și sediile sociale folosite de Deleanu și ENTRYRISE S.R.L., în vederea identificării echipamentelor utilizate la extragerea datelor.

d) Ridicarea telefoanelor, laptopurilor, serverelor, suporturilor de stocare și conturilor cloudasociate activității, în vederea examinării tehnice.

e) Dispunerea unei expertize informatice judiciare (art. 172 C.proc.pen.) pentru stabilirea:

- modului de funcționare a scripturilor,
- volumului și naturii datelor extrase,
- traseului electronic al datelor,
- eventualei prelucrări ulterioare.

f) Aplicarea măsurilor de conservare a datelor, potrivit art. 170 C.proc.pen., asupra sistemelor și conturilor folosite.

g) Instituirea măsurilor asigurătorii asupra datelor și infrastructurii informatice, în vederea prevenirii ștergerii, multiplicării sau valorificării acestora.

h) Reaudierea persoanei Deleanu Ștefan-Lucian, după efectuarea percheziților informatice și după expertiză, pentru confruntarea declarațiilor anterioare cu probele obiective.

i) Analizarea distinctă a răspunderii penale a persoanei juridice ENTRYRISE S.R.L., în condițiile art. 135 C.pen., având în vedere folosirea infrastructurii firmei.

j) Verificarea posesiei actuale a datelor extrase și a eventualei lor valorificări comerciale, inclusiv prin platforma „incorpo.ro".

k) Asigurarea accesului efectiv la dosar, respectiv studierea și fotocopierea actelor pentru persoana vătămată și avocatul acesteia, conform art. 94 C.proc.pen.

l) Analizarea posibilității dispunerii confiscării speciale, conform art. 112 alin. (1) lit. b) Cod penal, asupra echipamentelor și instrumentelor utilizate.

Pentru toate motivele expuse, solicit admiterea plângerii, desființarea ordonanțelor atacate și trimiterea cauzei la procuror pentru completarea urmăririi penale în condițiile prevăzute de art. 341 alin. (6) lit. b) C.proc.pen.

o

Pentru susținerea prezentei plângeri și pentru evidențierea nelegalității și netemeiniciei soluțiilor DIICOT, sunt atașate următoarele înscrisuri, aranjate în ordine cronologică și logică. Fiecare dintre ele contribuie la demonstrerea modului în care a fost îngrădit dreptul persoanei vătămate la apărare și la cunoașterea completă a materialului de urmărire penală.

Anexăm:

- **Anexa 1 – Ordonanța DIICOT din 12.10.2025 (soluția de clasare)**
  Actul emis de **procurorul de caz DIICOT**, prin care s-a dispus clasarea cauzei fără efectuarea actelor esențiale de urmărire penală, fără expertiză informatică și fără schimbarea calității procesuale a făptuitorului, deși acesta era identificat.

- **Anexa 2 – Ordonanța procurorului-șef DIICOT din 17.11.2025**
  Act emis de **procurorul-șef DIICOT** prin care plângerea persoanei vătămate a fost respinsă cu o motivare aparentă, fără analiza criticilor și fără verificarea actelor de urmărire penală, ceea ce atrage nelegalitatea acestui act potrivit art. 339 C.proc.pen.
- **Anexa 3 – Adresa DIICOT din 10.10.2025 (refuz studiere dosar)**
  Răspuns emis de **procuror din cadrul Serviciului II/1 DIICOT**, prin care se comunică în mod nelegal imposibilitatea studierii dosarului, deși ordonanța de clasare nu fusese încă adusă la cunoștința UNBR. Documentul dovedește incoerența procedurală și refuzul sistematic al accesului la dosar.
- **Anexa 4 – Adresa DIICOT din 24.11.2025 (refuz repetat studiere/fotocopiere dosar)**
  Act emis tot de **procurorul responsabil cu cauzele II/1**, reiterând refuzul de a permite accesul la dosar, contrar art. 94 C.proc.pen. și contrar propriilor îndrumări adresate anterior persoanei vătămate.
- **Anexa 5 – Cererile UNBR pentru studierea și fotocopierea dosarului**
  Dovezi clare că persoana vătămată a solicitat în mod consecvent accesul la materialul de urmărire penală, acces care i-a fost refuzat în mod repetat și nelegal.
- **Anexa 6 – Cererile avocatului împuternicit pentru studierea dosarului**

Cererile formulate de avocat în baza art. 94 C.proc.pen., respinse de DIICOT cu aceeaşi justificare formală privind existența unei soluții de clasare, deși legea obligă procurorul să permită accesul chiar şi după soluționare.

- **Anexa 7 – Dovezi de comunicare (plicuri, confirmări de primire, dovezi poştale)**
- Aceste înscrisuri stabilesc calendarul exact al comunicărilor şi arată contradicțiile DIICOT: unele adrese sunt datate anterior comunicării efective a soluției către UNBR, ceea ce face imposibil temeiul refuzului.
- **Anexa 8 – Plângerea inițială formulată de UNBR împotriva ordonanței de clasare**
- Documentul în care au fost expuse toate criticile de nelegalitate şi netemeinicie, ignorate ulterior în totalitate de procurorul-şef.
- **Anexa 9 – Împuternicirea avocațială**

Facem precizarea că prezenta plângere este transmisă inițial prin e-mail, semnată electronic şi ştampilată, urmând ca exemplarul original, în format fizic, să fie comunicat ulterior şi prin poştă.

UNIUNEA NAȚIONALĂ A BAROURILOR DIN ROMÂNIA
prin Av.DRAGU MARIUS

Marius Dragu
Digitally signed by Marius Dragu
Date: 2025.12.12 18:06:58 +02'00'

Uniunea Națională a Barourilor din România – Baroul București
Marius Dragu
Cabinet de avocat

DOMNULUI PREŞEDINTE AL TRIBUNALULUI BUCUREŞTI- SECȚIA PENALĂ

ROMÂNIA
MINISTERUL PUBLIC
PARCHETUL DE PE LÂNGĂ ÎNALTA CURTE DE CASAŢIE ŞI JUSTIŢIE
DIRECŢIA DE INVESTIGARE A INFRACŢIUNILOR DE CRIMINALITATE ORGANIZATĂ ŞI TERORISM
STRUCTURA CENTRALĂ
Secţia de Combatere a Infracţiunilor de Terorism şi a Criminalităţii Informatice

[redacted]
București, Str. Sfânta Vineri, nr. 33, Sector 3, cod operator 16051, contact@diicot.ro,

Nr. 175/II-2/2025

ORDONANŢĂ
17.11.2025

Procuror șef secție [redacted] din cadrul Parchetului de pe lângă Înalta Curte de Casaţie şi Justiţie – Direcţia de Investigare a Infracţiunilor de Criminalitate Organizată şi Terorism,

Examinând plângerea formulată de către petenta **UNIUNEA NAŢIONALĂ A BAROURILOR DIN ROMÂNIA,** prin reprezentantul convenţional, avocat Dragu Marius, împotriva ordonanței nr. **364/19/P/2024** din data de **02.10.2025**, prin care s-a dispus clasarea cauzei,

CONSTAT:

Prin ordonanța din data de **02.10.2025**, întocmită în cauza privind dosarul penal nr. **364/19/P/2024** al Direcţiei de Investigare a Infracţiunilor de Criminalitate Organizată şi Terorism, Secția de Combatere a Infracțiunilor de Terorism și a Criminalității Informatice s-a dispus clasarea cauzei, sub aspectul săvârşirii infracţiunilor de **accesul ilegal la un sistem informatic, prevăzute de art. 360 alin. 1, 2, 3 C.p. și transferul neautorizat de date informatice, prevăzute de art. 364 C.p.**, fapte sesizate împotriva numitului **DELEANU STEFAN – LUCIAN** și **S.C.ENTRYRISE S.R.L.**, reprezentată legal prin asociat unic și administrator **DELEANU ȘTEFAN – LUCIAN** de către **UNIUNEA NAȚIONALĂ A BAROURILOR DIN ROMÂNIA (U.N.B.R)** și **Corpul Experților Contabili și Contabililor Autorizați din România (CECCAR).**

În fapt, s-au reținut următoarele:

I. La data de 30.01.2024, pe rolul D.I.I.C.OT. – Structura Centrală a fost înregistrată sub nr. **364/19/P/2024**, plângerea penală formulată de **UNIUNEA NAȚIONALĂ A BAROURILOR DIN ROMÂNIA**, cu sediul în București, Sector 5, Splaiul Independenței nr. 5, Palatul de Justiție, reprezentată legal prin Președinte Av. dr. Traian - Cornel BRICIU, împotriva numitului **DELEANU STEFAN - LUCIAN**, cu domiciliul în Județul Cluj, Municipiul Cluj - Napoca, Str. Aurel Vlaicu nr [redacted] emisă la 16.12.2021 de SPCLEP Cluj – Napoca și [redacted] **S.C. ENTRYRISE S.R.L.**, cu sediul social în Județul Suceava, Orașul Gura Humorului, Bulevardul

[redacted] având ca domeniu de activitate principal - Activități de realizare a soft-ului la comandă (software orientat client), reprezentată legal prin asociat unic și administrator **DELEANU ȘTEFAN – LUCIAN**, cu privire la care există o suspiciune rezonabilă în ceea ce privește săvârșirea infracțiunilor de **acces ilegal la un sistem informatic prev. de art. 360 Cod penal și transfer neautorizat de date informatice prev. de art. 364 Cod penal.**

Prin ordonanța din data de 19.02.2024, s-a dispus începerea urmăririi penale în cauză, "in rem", cu privire la săvârşirea infracţiunilor de **accesul ilegal la un sistem informatic, prevăzută de art. 360 alin. 1, 2, 3 C.p. şi transferul neautorizat de date informatice, prevăzută de art. 364 C.p.**

La data de **05.01.2024,** utilizând platforma informatică a domeniului **www.incorpo.ro** deținut de societatea **ENTRYRISE S.R.L.,** numitul **DELEANU ȘTEFAN – LUCIAN,** care în mediul virtual se prezintă ca fiind directorul societății, utilizând adresa de e-mail alexandra.ardelean@incorpo.ro (persoană virtuală creată prin utilizarea tehnologiei inteligenței artificiale - A.I.) transmite e-mailuri semnate în numele său către un număr important de avocați, care se pretinde de către acesta că au fost obținute din baza de date administrată de **IFEP** împreună cu alte date referitoare la avocați (CNP, număr de telefon, număr de legitimație / card avocat CCBE) prin utilizarea unui „endpoint accesibil fără parolă, și indexat de Google."

Se susținea în e-mail că „acest endpoint a fost accesibil pentru aproximativ 2 ani". În cuprinsul e-mailului se arata totodată faptul că „a fost notificat IFEP în mod direct pe adresa de mail pentru a rectifica problema" și că „deși s-a rectificat în aceeași zi, avocații nu au fost notificați de existenta breșei". Se recomandă în e-mail citirea „comunicatului de presă al Incorpo.ro referitor la breșa de securitate a IFEP".

Nu în ultimul rând, în partea finală a e-mailului se arată faptul că avocatul care dorește o probă cu privire la existența breșei este rugat să transmită prin e-mail la adresa office@incorpo.ro un document semnat electronic prin care să solicite expres și să furnizeze totodată societății **ENTRYRISE S.R.L,** care deține platforma domeniului incorpo.ro, dreptul/acordul de procesare al datelor respective pentru a transmite avocatului totalitatea datelor obținute.

S-a arătat faptul că au fost avocați care au solicitat și au primit CNP-ul de la numitul **DELEANU ȘTEFAN - LUCIAN.**

În cuprinsul „*comunicatului de presă al Incorpo.ro referitor la breșa de securitate al IFEP*" publicat la data de 04.01.2024, actualizat în cursul zilei de 06.01.2024 s-a identificat un e-mail care se pretindea că s-ar fi transmis la data de 28.02.2023 către helpdesk@ifep.ro, prin care ar fi fost sesizată pretinsa breșă de securitate din cadrul platformei IFEP.

Se pretinde prin „comunicatul de presă" faptul că „data la care a fost descoperită vulnerabilitatea coincide (dar nu are legătură) cu data propunerii de a construi o NOR pentru avocați", mai exact cu

proiectul de lege privind serviciile profesionale efectuate de avocat în format electronic înregistrat la Senatul României sub nr. B47/2023 în data de 06.02.2023 și retras la data de 27.02.2023.

Prin același comunicat se arată totodată că există o breșă de securitate și în ceea ce privește platforma / baza de date a CECCAR.

În cuprinsul „comunicatului de presă al Incorpo.ro referitor la breșa de securitate al IFEP" este inserată și o înregistrare audio - video distribuită din platforma Youtube prin care numitul **DELEANU ȘTEFAN - LUCIAN** afirmă următoarele: "Salut! Sunt **Ștefan Deleanu** și în acest videoclip voi discuta despre **breșa de securitate** de la **CECCAR** și de la **IFEP.** Modul în care le-am descoperit, n-am să explic de ce am făcut demersul de abia acum să notific public si să explic tot, tot ce s-a întâmplat în spate, tot background-ul, care a fost problema tehnică, riscurile, absolut tot, din perspectiva mea ca persoană care lucrează în IT și care are totuși tangențe cu Dreptul. Însă, întâi de toate, vreau să tai niște percepții greșite pe care le-am văzut în mediul online. În primul și în primul rând, mail-ul respectiv nu a fost cu scop de marketing. Da, am publicat de pe o adresă de la Incorporo, pentru că deja avem infrastructura făcută. De aia am și trimis de pe Alexandra /Ardelean/, care e A.I.-ul nostru. Am trimis de pe acela, pentru că deja era tot sistemul setat, în afară de mici chestii care mi-a luat mult mai puțin să le fac decât dacă era să fac pe persoană fizică, aceleași demersuri. Suplimentar, contabilii și avocații nu sunt ținta noastră. Noi suntem o platformă care țintim străini, nu avem absolut nicio legătură cu românii. Iar privitor la speța cu avocatura clandestină avem inclusiv o pagină unde discutăm de asta. Dar pe scurt, avem, generăm numai niște formulare, oamenii le semnează și noi le trimitem în mod automat. Inclusiv avem doctrină în străinătate care discută pe tema asta de completare de șabloane și achită de exercitarea fără drept a profesiei niște profesioniști care cu asta s-au ocupat. Ok, întorcându-mă la problemă, eu am găsit de-a lungul activității mele mai multe breșe la diverse instituții publice, pentru că realitatea este că breșele astea sunt atât de frecvente și atât de multe, încât este extrem de dificil să le rezolvi. De multe ori am raportat niște probleme ca să nu fie rezolvate sau să fie rezolvate doar parțial, cu problemele încă persistente. În același timp, de foarte multe ori am raportat problemele astfel încât să mi se spună că se vor rezolva la următorul update, chiar dacă îmi ofereau acces asupra întregului spațiu web, spre exemplu. Și de aceea cred că am și ajuns la demersul ăsta în care am făcut totul public, pentru că mi se pare că dacă nu faci mizerie, din păcate, nu se rezolvă lucrurile. E trista realitate și modul în care funcționează societatea românească, în care dacă nu faci tam-tam și dramă, lucrurile nu se rezolvă. Ca să discut punctual despre cum am făcut și cum am procedat, cât să fiu maxim de etic și să nu prejudiciez pe nimeni sau pe cât mai puțini și dacă am prejudiciat, voi plăti pentru prejudiciul pe care l-am cauzat și am să discut ulterior cam tot procesul și ce văd eu, cum văd eu, cum aș recomanda eu să procedeze și alte discuții pe/în temă. Ideea e că în modul anterior, când eu raportam problemele, nu se prea rezolvau sau se rezolvau temporar și după, reapăreau. Însă, în același timp, ca researcher în zona asta, în zona de Infosec, nu poți să te apuci și să spui pe internet din prima "vezi că

aia are o breșă" când tu ești conștient că omul respectiv nu a rezolvat în totalitate breșa, nu a avut să analizeze, nu a avut timp să la demersurile interne cât să soluționeze și atuncea nu poți să o faci instant sau într- o lună sau în două, fără să îți asumi riscul că poate din vina ta, tu practic faci ceea ce ai încercat să previi și din contra, în loc să ascunzi măcar temporar sub preș, până rezolvi, groapa, tu practic arăți cu degetul spre groapă și îi faci pe oameni să sară în ea, lucru pe care tu nu vrei să-l faci. Evident, dacă scopul tău nu este să strici. Problema punctuală e că pe IFEP, când căutam, discutam cu niște prieteni avocati care discutau pe proiectul de lege cu cloud-ul avocatilor, mi-au zis că e o problemă de lipsă de transparență cu IFEP. Și m-am pus să caut și eu, eram curios să văd ce e IFEP, cine îl deține ș.a.m.d. **Și în căutările pe Google pe care le-am făcut am găsit și ASPX-ul respectiv care îmi arăta toate endpoint-urile care erau, deci erau accesibile, publice** și unul dintre endpoint-uri te punea să selectezi câți avocați să-ți arate, să arăți cu ce le începe numele, adică cu a, b, c sau chiar nu puneai nimic și să menționezi... mai aveau... da, numărul și o cheie care n-avea nicio relevanță. Și pe scurt, când apăsai pe enter și executai toată prostia aia, în mod automat, tie îți trimitea CNP-ul tuturor avocatilor în limita numărului ăla de căutări. Adică, dacă tu puneai să-ți apară 100, îți apărea **CNP-ul** la cei 100 cu prefixul respectiv. Și dacă puneai fără prefix și puneai 100.000 îți apăreau toți avocații, cu (toate CNP-urile, cu toate barourile la care lucrează. Pe un alt endpoint îți apăreau email-urile avocaților și pe acelea le-am și folosit ca să transmit ulterior. Au fost niște email-uri curate, anonimizate, pe care eu le-am folosit ulterior ca să trimit mail. Si într- adevăr, aici am încălcat GDPR-ul într-un mod evident si o și recunosc si-mi asum si amenzile, dacă sunt, pentru că, da, inclusiv prin faptul că am notificat niște persoane, eu am încălcat legea. Eu nu aveam niciun mod să soluționez asta sau să mă asigur că se soluționează fără să încalc legea, să comit un delict sau o faptă penală. Faptă penală nu am încălcat, că erau endpoint-uri publice si fix de aceea e si gravă situația, pentru că si la **CECCAR** si la **IFEP** erau niște endpoint-uri publice si pe care oricine le putea găsi pe Google. La **CECCAR** cred că endpoint-ul ăla era foarte frecventat, adică acolo-s aproape sigur că n-am fost singurul care a găsit problema. La IFEP, într-adevăr, era mai puțin frecventat link-ul și atunci e o mare probabilitate ca să fi fost printre singurii care au avut acces la respectivul endpoint și atunci poate e mai ok, dar concluzia pe care eu vreau să o trag e că faptul că am trimis mailurile respective în spam este pentru că altă soluție nu aveam ca să notific lumea. Am încercat să fac *ads* pe facebook și nu au văzut decât avocații din cercul meu restrâns, de persoanele pe care le cunosc de la Cluj sau colaboratori cu care am mai lucrat ș.a.m.d. și evident, scopul a fost să evidențiez problema la toată lumea, ca să știe lumea ce s-a întâmplat. Acum, începând cu **IFEP**, pentru că a fost prima prima breșă care a apărut, deja am discutat, primul lucru pe care l-am făcut e să-i notific. Cred că în ziua viitoare sau chiar în aceeași zi le-am trimis un mail în care să-i notific la mail-ul care apărea pe site. Nu știam că e a UNBR si nu e OK să-i zici unui teri: /.../ e breșa. De aceea nici n-am notificat UNBR-ul si știu că purtam discuția cu niște avocati atunci, eu cum mă asigur să fac chestia asta fără să generez niște prejudicii, fără să pot să fiu acuzat ulterior că sunt

complice la o faptă de acces neautorizat sau dracu știe! Pentru că se reține acces neautorizat și când plătești cu cardul și atunci îți pui problema dacă instituțiile publice sunt competente cât să analizeze o speță de genul și îmi era teamă. Acuma m-au luat dracii și am zis hai să pun fuck it și aia e, ce iese, o ieși! Punctul 1. La **CECCAR** lucrurile erau și mai prost. La **CECCAR** avea un endpoint unde căutai toți contabilii și puteai să-i cauți după nume, după email, după ș.a.m.d., număr de legitimație etc. Și it's ok, e necesar, ai nevoie de un astfel de program ca să poți să vezi dacă cineva e autorizat sau nu să facă contabilitate, expert sau autorizat. Și e normal ca **CECCAR** să aibă o astfel de listă, cum au și avocații și toată lumea. Problema e că acolo când căutai, în spate, endpoint-ul respectiv, când oricine, oricine făcea o căutare cu chestia aia pe care o folosea toată lumea care avea de căutat, îți apărea tot, de la CNP, la adresă, la data și locul nașterii, la sex, naționalitate, absolutamente tot era public, tot, tot, tot, tot tot! Și era un endpoint care nu numai că era public, ci nici măcar nu necesita interacțiune din partea utilizatorului sau unui actor malicios și literalmente toate persoanele care au intrat pe site-ul respectiv au avut acces la CNP-ul tău. El a fost stocat în memoria calculatorului lor. Deci asta e problema punctuală și asta este problema pe care eu am încercat să evidențiez. Și la ei am procedat la fel, știind de situația care s-a întâmplat cu IFEP în mod anterior, când i-am notificat, am notificat DPO-ul, pentru că știam că ăla e răspunzător de partea legală, am notificat **CECCAR**-ul pe mail-ul direct și am notificat și **ANSPDCP**-ul, pe care l-am pus în BCC ca să nu vadă băieții că eu am trimis la **ANSPDCP**. **ANSPDCP**-ul l-a primit, i-a lăsat la ăia timp, a trecut cred că 90 de zile sau nu știu din septembrie cât a trecut și acuma primesc răspunsul de la **ANSPDCP** că ei nu au văzut, că au verificat endpoint-ul după ce îl rezolvaseră, rezolvaseră în vreo cred că 3 zile după ce am raportat și în orice caz au zis că nu sunt probe. Le-am trimis toată baza de date, pentru că eram aproape sigur că asta o să se întâmple, pentru că asta este demersul pe care l-am văzut la toate instituțiile publice, în sensul în care se mușamalizează și s-a mușamalizat peste tot, peste tot și am raportat peste șapte astfel de breșe. Unele breșe care... dar aia s-a gestionat, OK, care era de risc de siguranță națională, deci putea să genereze panică în rândul populației generale. Ăla e nivelul de probleme care sunt și ăsta e nivelul de soluții pe care tu trebuie să le faci ca tu să poți să notifici și să iei măsuri, pentru că în mod contrar nu le pasă. .... în fine, am văzut chestia asta, le-am trimis la ANSPDCP tot exportul, că de altundeva n-aveam de unde să-l am, e evident, adică erau datele lor profesionale toate, plus CNP, toate prostiile alea, erau singurii care aveau acces. Într-adevăr, am comis si eu un delict si-mi asum si asta este, acces neautorizat nu putea să fie că era un endpoint public, toată lumea avea acces, singura diferență între mine și ei, că eu am salvat intenționat să-l țin ca probă. Și asta a fost povestea. Și acuma ANSPDCP-ul are informațiile acolo.

Văzând modul în care au abordat **CECCAR** problema, am zis fuck it, hai să facem asta și cu avocații. Mi-au zis toți avocații "nu fă", "nu fă", toți pe care-i cunosc, pentru că, da, deschizi cutia pandorei si e un risc pe care tu, odată ce ți-l asumi, e posibil să ieși fără libertate. Suntem în România, suntem într-o țară unde te poți aștepta la absolut orice. Și atuncea... Știi, pe mine nu mă avantajează cu absolut

nimic că am făcut reclamă la o breșă si mi-am făcut și mie reclamă de om bun de mers la pușcă... nu mă, nu mă avantajează cu absolut nimic. Ba, da. Oleacă de brand awareness pentru mine persoană și cam atât. Deci nu pot să neg că sunt și niște avantaje aici, dar exclusiv atât. Și oricum demersurile astea au început prin plângeri, prin lucruri pe care nu le-am făcut publice, 90% din ceea ce fac nu fac public. În fine, asta le-am făcut publice și am decis să fac mail-ul ăla, să fac cele două publicate și să le notific pe toată lumea de toate problemele care apar. Și acuma văd că de-abia acuma să iau măsuri. De abia acuma lumea s-a sesizat. ... E trista realitate și modul în care funcționează societatea, din păcate, în România. Nu suntem o societate care să conștientizeze riscurile și să le prevină, ci una care le atacă odată ce există. Și în momentul în care tu dezvălui lucrurile astea, este atacat cel care o dezvăluie și este atacat cel care a fost vinovat. Și după aia, e un joc de resurse. În fine, noi am făcut raportul ăsta, cei de la CECCAR au dat un raport că ei nu au fost notificați și nu știau, după ce ANSPDCP-ul are mail-ul unde vede că doar au fost și chiar au și trimis un răspuns, evident, eu am făcut copy la toate mail-urile, la toate notificările, bază de date să nu zică că nu a fost breșa. După aia au zis că de fapt eu le-am furat bază de date că... deci eu n-am avut acces, dar eu le-am furat baza de date! La care eu nu aveam acces. Și nici măcar nu-i furt ăla că ar fi acces neautorizat, dar acces neautorizat cum? că era un endpoint public și oricine căuta prin tabloul ăla nu prea să vadă decât dacă făcea endpoint-ul ăla. Adică atâta vreme dacă voiai să vezi că cineva e contabil și noi căutam contabil că aveam nevoie să luăm la Incorporo să putem să recomandăm la clienți niște contabili și căutam pe acolo oameni. Dacă căutai, pac, ai și comis infracțiunea! Evident că dacă ar fi să o considerăm pe aia acces neautorizat, atuncea îs mai multi infractori decât putem să numărăm. Ar trebui DIICOT-ul să-și facă un corp special pentru toată infracțiunea asta, dacă aia e infracțiune. Evident, e o absurditate si nu este. În fine, ideea e că am făcut demersul, am notificat pe toată lumea și acuma merg pe transparență, n-am, eu nu cred că am ce să ascund și atuncea dau totul pe față, vine organul de urmărire penală, mă saltă, îmi sparge ușa, no problem, să vadă, să verifice, să analizeze, să răsanalizeze, că nu, nu văd o problemă și aia e, adică, na, la final eu îs destul de safe. Într-adevăr, există riscul să... că na, e vorba aceea, dacă vine polițistul după tine și te tot urmărește, găsește ceva, dar sperăm că lumea e de bună credință și acea... Doamne ajută! No, bun. În esență, am făcut notificare la ambii. Mulți s-au temut de faptul că e fals, e o țeapă, o înșelăciune, nimeni nu a avut acces și aici am să discut o leacă de tema asta. Dacă ești avocat și vrei să îți furnizez datele care au apărut în breșă, eu pot să fac asta dacă îmi trimiți un email sau ceva într-un mod în care pot să-ți verific cel puțin identitatea, adică fie să mă contactezi de pe email-ul pe care te-am notificat eu, pentru că ăla era din baza de date a IFEP. Plus să-mi zici numele tău întreg și dacă-mi oferi cele două, eu pot să-ți arăt tot ce era în baza de date. Dar cumva trebuie să văd că tu ești cel care deții, ca să nu dau CNP-uri la oameni pe net, că nu ăsta-i scopul. Deci de aici și o leacă este mai scurting stilul meu, de aia am fost vag, de aia n-am dat toate informațiile pe față, pentru că e foarte dificil să demonstrez că există breșa fără să fii cel care practic o

generează și atunci am încercat cumva să fiu sensibil și pe zona de CECCAR și pe zona de avocați. La CECCAR am făcut o chestie mai riscantă, am făcut o chestie în care-ți arăta datele anonimizate si îți păstram numai primul și ultimul caracter sau primele două și ultimele caractere, ca să vadă lumea că bă, de unde dracu are datele astea, că n-avea de unde. Și am băgat ăsta pe site, deși e o breșă clară a regulamentului GDPR și iar îmi asum aici o amendă pe persoană fizică că no, dar asta este, îmi asum amenda și să fac un grup found me dacă-mi iau amendă de la cei care au fost ajutați de faptul că cineva le- a notificat faptul că există probleme. Deci mie mi se pare că, într-adevăr, da, am comis un delict cu speranța să previnã unul mai mare care chiar poate să fie și infracțiune dacă se apucă unul să șteargă niște mail-uri știind că el trebuia în mod normal să notifice. În fine. Cam asta e povestea. Eu în continuare stau extrem de transparent și dacă aveți întrebări, dacă vreți să discutați cu mine, să vă explic punctual cum a funcționat problema, eu sunt accesibil și oricând pot să răspund la întrebări, numa timp, că primesc foarte multe mesaje în momentul curent și atuncea le iau pe rând. Asta e tot. Mulțumesc foarte mult de timp și zi frumoasă și somn ușor și scuze pentru mesajul târziu, că presupun că n-a prins cel mai bine. Chiar, chiar îmi pare rău. Na, intenția a fost să comunic. Mulțumesc foarte mult. Zi frumoasă și spor la treabă!"

S-a arătat în continuare faptul că, la solicitarea **U.N.B.R.** de a se oferi clarificări cu privire la situația reclamată, societatea **INTRA CONNECT S.R.L**, a comunicat în scris faptul că:

- „prin raportare la elementele existente în spațiul public, cu referire specifică la endpoint- ul menționat, respectiv https://www.ifep.ro/Ws/InternalWebServices.asmx, putem concluziona că acest endpoint nu prezintă, din punctul nostru de vedere, riscuri de securitate."

- „în endpoint-ul menționat nu există niciun indiciu că ar exista posibilitatea unei breșe de securitate, însă portalul **IFEP** este actualizat permanent, iar din 28 februarie 2023, data la care se face referire că s-a identificat incidentul și până la data curentă, portalul **IFEP** a suferit numeroase modificări."

***

II. La data de 06.02.2024, pe rolul D.I.I.C.OT. – Structura Centrală a fost înregistrată sub nr. 610/19/P/2024 și plângerea penală formulată de **CORPUL EXPERȚILOR CONTABILI ȘI CONTABILILOR AUTORIZAȚI DIN ROMÂNIA (CECCAR),** persoana juridica romana de utilitate publica si autonoma, cu sediul in București, str. Intrarea Pielari nr. 1, sector 4, reprezentata prin Președintele Consiliului Superior, doamna ELENA- ECATERINA CHIVU, împotriva aceluiași **DELEANU STEFAN – LUCIAN** și totodată societății la care acesta are calitatea de asociat unic și administrator, respectiv societatea **ENTRYRISE S.R.L.,** cu privire la care există o suspiciune rezonabilă în ceea ce privește săvârșirea infracțiunilor de *acces* **ilegal la un sistem informatic (art. 360 Cod penal) și transfer neautorizat de date informatice (364 Cod penal).**

Prin ordonanța din data de 20.02.2024, s-a dispus *începerea urmăririi penale* în cauză, "in rem", cu privire la săvârşirea infracțiunilor de **accesul ilegal la un sistem informatic, prevăzută de art. 360 alin. 1, 2, 3 C.p. și transferul neautorizat de date informatice, prevăzută de art. 364 C.p.**

În fapt, s-au invocat aceleași aspecte faptice, referitoare la identificarea vulnerabilității tehn... către numitul **DELEANU STEFAN LUCIAN,**

Întrucât între cele două cauze există o strânsă legătură, ambele sesizări fiind îndeptate împot... acelorași persoane fizice/juridice, prin ordonanța din data de 20.02.2024, s-a dispus reunirea dosarul... pena cu nr. 610/19/P/2024 al DIICOT – S.C. la dosarul penal cu nr. 364/19/P/2024 al DIICOT – S.C.

În cauză, s-a procedat la analizarea datelor existente la dosar, a datelor existente online și a tuturor datelor și înscrisurilor solicitate și furnizate organului de urmărire penală, de catre **U.N.B.R., C.E.C.C.A.R. si A.N.S.P.D.C.P.** (proces-verbal de analiză date/înscrisuri).

În continuare, ne rezumăm la aspectele reținute doar cu privire la petenta **U.N.B.R.,** având în vedere că în cauză, **C.E.C.C.A.R**. nu a formulat plângere împotriva soluției de clasare raportat la aspectele similare reclamate în cauză.

Astfel, cu privire la UNBR, au rezultat următoarele:

A.

Publicare bresa de securitate **UNBR** – 28 Februarie 2023

În urma verificării datelor postate de catre numitul **STEFAN-LUCIAN DELEANU** referitor la bresa de securitate UNBR, la URL : https://www.incorpo.ro/en-us/press/ifep-data-breach/?utm%20nooverride=1&utm_source=smtp&utm_medium=newsman&utm_campaign=SMTP-20240105#steps-taken, s-a stabilit ca există o postare si un document pdf ce face referire la o posibila bresa de securitate in ceea ce priveste date cu caracter personal ce a avut loc anterior datei de **05.01.2024** pe infrastructura aferenta portalului **IFEP** "https://www.incorpo.ro/content/files/2024/01/Probleme-de-securitate---Portalul-IFEP.pdf"

Probleme de securitate - Portalul IFEP

"Stefan Deleanu" - office@entyrise.com -

To: helpdesk@ifep.ro

February 28, 2023 at 1:46 PM

Buna ziua,

Va contactez pentru a raporta urmatoarele probleme de securitate informatica, pe care le-am identificat in timpul utilizarii platformei IFEP

Am identificat urmatoarele probleme:

- **Bresa date cu caracter personal (Risc Ridicat):** API-ul accesibil AICI este public, si poate fi utilizat desi informatiile furnizate prin intermediul acestui API sunt informatii cu caracter personal. Spre exemplu, prin interogarea endpoint-ului "GetLawyersFull", un actor malicios poate obtine informatii referitoare la numele, prenumele, baroul unde sunt inregistrati, precum si CNP-ul persoanelor inscrise in tabloul furnizat de IFEP, care ar simplifica o potentiala uzurpare a calitatii de avocat de catre un astfel de actor.
- **Lista unui sistem de autentificare sigur (Risc Ridicat):** S-a apreciat ca utilizarea CNP-ului ca sistem unic de securizarea a platformei nu este o solutie ideala, fiind informatii care pot fi usor identificate sau deduse dupa un minim de analiza in informatiile disponibile publice. CNP-ul este format, in mare parte, din date asociate direct datei nasterii, genului, judetul nasterii, 3 numere care reprezinta seria nasterii (de la 001 la 999), precum si un cod de paritate calculat in baza celorlalte. Un atacator ar putea afla CNP-ul doar printr-un simplu bruteforce, cu 999 incercari, ulterior validand CNP-ul prin autentificarea reusita.
- **Potential risc de furt conturi (Risc Mediu):** In contextul in care un numar de telefon (neasociat contului) si CNP-ul profesionistilor sunt unicele date necesare pentru resetarea parolei, un atacator care cunoaste CNP-ul victimei ar putea sa se utilizeze de acesta, si un numar virtual, pentru a obtine acces in contul victimei.
- **Potential risc de deanonimizare a voturilor prin platforma (Risc Redus):** In contextul problemelor sus mentionate, un atacator care dispune de CNP-ul persoanei (de pe care se poate obtine, in mod direct, codul CCBE), ar putea da bruteforce pe hash pentru a afla variabilele necunoscute (**CodSecuritate, Pozitii Votate**). In lipsa unui seed unic, atacul devine, de asemenea, exponential mai usor.

Recomandari de natura tehnica:

- Abordarea unei scheme de incredere "Zero Trust". Furnizarea minimului necesar de incredere utilizatorilor, pana la demonstrarea autorizatiei de accesare a datelor (spre exemplu, prin autentificarea intr-un cont cu privilegii).
- Modificarea schemei de autentificare cat aceasta sa includa informatii care nu pot fi deduse in baza informatiilor publice (Spre exemplu, prin utilizarea unui email si cod utilizator, si validarea manuala a cererilor de schimbare a parolei in baza unui document semnat cu semnatura electronica calificata).
- Restrictionarea accesului la API-uri interne, in contextul in care accesul nu este necesar pentru functionarea platformei.

Pentru orice detaliu de natura tehnica, sau orice alta intrebare, va stau la dispozitie pe email, sau telefonic.

Multumesc Mult,
Deleanu Stefan-Lucian

Stefan-Lucian Deleanu
Director / ENTRYRISE S.R.L

Articolul face referire la url : InternalWebServices Web Service (ifep.ro) care ar fi fost anterior acelei date și susceptibil de a furniza date cu carcater personal din tabloul avocatilor din Romania, prin introducerea unor criterii simple de cautare. https://www.ifep.ro/Ws/InternalWebServices.asmx?op=GetPersonal

URL ul furnizeaza o optiune de a trimite o cerere SOAP către un server web prin intermediul metodei POST.

URL- ul exista si in prezent dar completarea de criterii nu mai returneaza nici un rezultat.

In acest sens, se concluzioneaza, ca daca pana la acea data a existat respectiva posibilitate, care de altfel nu poate fi exclusa prin datele ce se detin la dosar, in prezent nu mai există aceasta posibilitate.

Documentatia si datele furnizate de catre U.N.B.R.:

1.

17042024_Raport_Evaluare_Raspuns_Incident_Analiza_Digital_Forensics_IFEP_v1.0.pdf, cuprinde analiza detaliată a logurilor sistemului pentru IFEP și din care se desprind concluziile investigației efectuate în cauză, astfel cum sunt redate în cele ce urmează:

" Trasee de Audit: În cadrul investigației de digital forensics realizate pentru Uniunea Națională a Barourilor din România (UNBR), s-au identificat câteva limitări semnificative în ceea ce privește configurarea și gestionarea logurilor sistemului IT. Aceste deficiențe au avut un impact direct asupra capacității noastre de a reconstitui evenimentele și de a evalua amploarea unui posibil incident de securitate." Din cauza configurațiilor inadecvate ale logurilor și a schimbării versiunii platformei între momentul presupusei breșe și timpul investigației, este dificil de determinat cu precizie dacă un acces neautorizat a avut loc. În plus, nu a fost păstrată o imagine a platformei de la momentul incidentului, ceea ce îngreunează reconstituirea exactă a stării de securitate. Cu toate acestea, analiza actuală nu a identificat dovezi directe ale unei breșe.

Acest raport prezintă rezultatele analizei detaliate a logurilor sistemului pentru IFEP (fisiere de jurnalizare – 11584 fisiere au fost analizate), cu accent pe identificarea oricăror scurgeri de date potențiale din portalul UNBR. Pe baza analizei amănunțite a logurilor disponibile la momentul evaluării și a configurației sistemului de logare existent, raportul constată că nu există dovezi digitale care să indice scurgeri de date din portal.

Analiza a relevat că sistemul de logare a fost configurat să înregistreze doar activități din IP-uri interne (din rețeaua 192.168.1.0/24) și de pe endpoint-uri de test specifice (railways.tests.ifep.ro). Această configurație limitează semnificativ capacitatea de a obține o perspectivă completă asupra tuturor solicitărilor și interacțiunilor cu portalul, excluzând în mod efectiv orice acces extern direct din analiză.

Logurile furnizate, care acoperă perioada presupusului incident, nu oferă informații suficiente despre evenimentele de autentificare sau modificările de configurare ale sistemului. Această lipsă de detalii ne împiedică să urmărim eficient cine s-a conectat la sistem, când exact s-au realizat aceste conexiuni și dacă au existat încercări nereușite de autentificare - un posibil indicator al unor tentative de acces neautorizat.
În plus, absența informațiilor specific legate de modificările de configurare obstrucționează capacitatea noastră de a identifica și evalua acțiunile interne ce ar putea influența negativ integritatea și securitatea sistemului.
Analiza a relevat că, deși a administratorul platformei, Intra Connect SRL, a reacționat la notificarea incidentului, lipsa unui protocol standardizat de răspuns la incidente a limitat capacitatea de a gestiona eficient situația. Administratorul a efectuat revizuiri ale configurațiilor de securitate și a verificat jurnalele disponibile, însă aceste acțiuni au fost constrânse de lipsa solutiilor specifice de monitorizare pentru intruziuni si setările inițiale de baza ale sistemului de logare.

Concluzii Raportul rezulta simi p

Concluzii

Raportul concluzionează că, în prezent, platforma este securizată conform rezultatelor recente ale testelor de penetrare, care indică faptul că o breșă similară cu cea presupusă nu ar putea avea loc în configurația actuală a platformei. Aceasta nu exclude posibilitatea unui incident anterior, ci subliniază limitările tehnice ale echipamentelor și procedurilor de logare folosite în momentul presupusului incident. "

Așadar, astfel cum a rezultat din acest audit de securitate, pe baza datelor și informațiilor deținute și în condițiile în care vesiunea platformei s-a schimat între timp, nu s-a putut stabili în mod retroactiv, existența vreunei breșe de Securitate, dar nici nu s-a înlăturat posibilitatea existenței unei asemenea presupuse breșe, incident notificat în cauză de către numitul **DELEANU ȘTEFAN LUCIAN**, încă din luna februarie 2023 către **IFEP**.

Totodată, nu s-au putut stabili indicii privind existența vreunei interogări/autentificări externe în mod neautorizat.

2. 17042024_Raport_Teste_de_Penetrare_pentru_Platforma_IFEP_v1.0-1.pdf

*" În cadrul testelor de penetrare efectuate recent pe platforma IFEP, a fost identificată o singură vulnerabilitate de **nivel scăzut**: detaliile excesive în mesajele de eroare. Este important de înțeles că, în funcționarea oricărei aplicații digitale, întâlnim momente neprevăzute care pot genera erori. Răspunsurile sistemului la aceste situații pot varia de la simpla notificare a utilizatorului că a survenit o eroare, până la furnizarea unor informații suplimentare despre natura problemei.*
Cu toate că scopul acestor mesaje este de a ajuta în identificarea și rezolvarea erorilor, unele dintre ele pot oferi detalii neintenționate despre structura internă a sistemului (de exemplu, versiunea serverului sau detalii tehnice). Această practică poate oferi un avantaj neașteptat persoanelor rău-intenționate, permițându-le să găsească puncte slabe specifice pe care să le exploateze în atacuri mai sofisticate.
Astfel de mesaje "verbale" pot dezvălui informații despre componentele software folosite, ceea ce ar putea indica metode de atac prin Injecție SQL (SQLi) sau Cross-Site Scripting (XSS), sau chiar pot facilita identificarea numelor de utilizator prin enumerare.

Rezultate Teste de Penetrare:

- *Vulnerabilități de Nivel Scăzut: Prezența unor vulnerabilități minore, cum ar fi informațiile excesive în mesajele de eroare, care ar putea fi exploatate de atacatori pentru a obține detalii despre infrastructura tehnică.*
- *Recomandarea de revizuire a politicilor de gestionare a erorilor pentru a minimiza riscurile.*
- *Stabilitatea Sistemului: În general, platforma a arătat o stabilitate impresionantă, neexpunând vulnerabilități critice sau semnificative în timpul testelor de penetrare.*

Concluzii: *Evaluarea a evidențiat că, deși platforma IFEP este bine protejată și robustă în fața amenințărilor cibernetice, există nevoia de îmbunătățire continuă a gestionării erorilor pentru a crește securitatea. Este esențială implementarea unor măsuri suplimentare de*

securitate pentru a contracara posibilele breşe care pot fi exploatate prin vulnerabilităţile minore identificate."

Răspunsul şi testul efectuat, mai sus amintit, a privit de fapt versiunea platformei de la momentul investigaţiei.

3 Raspuns ***INTRA CONNECT SRL*** *(administratorul platformei)- solicitare DIICOT.docx*

-

- *Metode de extragere a datelor: datele sunt extrase prin următoarele metode:*
  - *interogări directe ale bazei de date cu rezultat afişat în formularele web;*
  - *interogări web service interne prin afişare rezultat în diverse obiecte existente în aplicaţii (gen obiecte de tip select);*
  - *execute metode de export date în excel, prin intermediul unor evenimente integrate în aplicaţie;*
  - *interogări API externe pe bază de API Key şi furnizare date în format JSON.*
- *Interfeţe publice de acces:*
  - *https://www.ifep.ro/Justice/Lawyers/LawyersPanel.aspx - interogare directă a bazei de date;*
  - *https://cautavocat.ro/ - extragere periodică a datelor prin API, populare bază de date aferentă website-ului şi afişare informaţii în paginile web;*
  - *Aplicaţia de mobil a UNBR – interogare API pentru validarea calităţii de avocat a utilizatorului.*
- *Securitate şi acces:*
  - *accesul la API se realizează pe bază de API key, fiind implementate şi mecanisme de filtrare la nivel de IP*
  - *accesul la metodele existente în web service-ul intern sunt securizate prin API Key, filtrare la nivel de IP şi autentificare (pot fi consumate doar de utilizatorii autentificaţi).*
- *Interfeţe de test şi mentenanţă: testarea aplicaţiei se realizează prin publicarea unei versiuni beta pe serverul de producţie, la adresa https://www-staging.ifep.ro„*

Aşadar, din analiza conţinutului acestor date si documente, a rezultat că, în urma auditului local de Securitate, nu s-a putut stabili cu certitudine dacă anterior datei de **05.01.2024** a existat o bresa de securitate care sa vulnerabilizeze datele cu caracter personal existente pe platforma **IFEP**.

Totusi acest lucru este în contradictoriu cu cele menţionate de catre **UNBR** prin reprezentanti in sesizarile catre DIICOT si ANSPDCP. De asemenea acest fapt este in contradictoriu şi cu elementele tehnice prezentate în datele publicate despre bresa de securitate şi in avertizările transmise de numitul **STEFAN DELEANU**.

Imposibilitatea auditului local de securitate, de stabilire retroactivă a existenței sau nu a respectivei breșe de securitate sesizată și notificată în cauză, s-a datorat (astfel cum de altfel se și menționează în raportul mai sus amintit), faptului că, inadecvata configurație ale logurilor și a schimbării versiunii platformei între momentul presupusei breșe și momentu linvestigației a făcut dificilă determinarea cu precizie dacă un acces neautorizat a avut loc. În plus, nu a fost păstrată o imagine a platformei de la momentul incidentului, ceea ce a îngreunat reconstituirea exactă a stării de securitate.

De asemenea, a rezultat că logurile furnizate, care acoperă perioada presupusului incident, nu au oferit informații suficiente despre evenimentele de autentificare sau modificările de configurare ale sistemului. Această lipsă de detalii a împiedicat să se urmărească în mod eficient cine s-a conectat la sistem, când exact s-au realizat aceste conexiuni și dacă au existat încercări nereușite de autentificare - un posibil indicator al unor tentative de acces neautorizat.

In acest sens, se concluzionează că, dacă la momentul sesizarii bresei ar fi putut exista posibilitatea afisarii in modul de dezvoltator a unor date suplimentare, date transmise de catre API, la pachet cu datele afisate, la momentul actual infrastructura nu mai furnizează astfel de date.

În fapt, **STEFAN DELEANU** indica faptul ca breșa de securitate a existat în site-ul **UNBR** incepand cu aprilie 2021 si a durat pana la mijlocul anului 2023.

Rezultatele analizei facute de catre acesta:
Risk assessment and CVSS details - 5.5/10
The vulnerability was assessed based on criticality, impact, and exploitability using the CVSS scoring metric, with an estimated CVSS Score of:

- CVSS Base Score: 7.5/10
- Impact Subscore: 3.6/1o
- Exploitability Subscore: 3.9/10
- CVSS Temporal Score: 7.2/10
- CVSS Environmental Score: 5.5/10
- Modified Impact Subscore: 1.8/10
- Overall CVSS Score: 5.5/10

În prezent, aceste date nu mai pot fi verificate faptic pe site-ul **UNBR** si pe infrastructura respectiva deoarece API-ul si site-ul au fost modificate de catre proprietar.

Au rezultat astfel date și indicii temeinice, că date suplimentare, nenecesare (exp. CNP), au fost expuse de sistem, public, către internet, datorită configurării defectuoase a API, indicii ce susțin de altfel varianta prezentată de către **DELEANU STEFAN**.

Din analiza răspunsului Autoritatății Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal (A.N.S.P.D.C.P.), au rezultat urmatoarele:

- sesizările formulate de Uniunea Națională a Barourilor din România (UNBR) înregistrate a ANSPDCP sub nr. 422/10.01.2024, 448/10.01.2024 și 694/15.01.2024;

sesizarea formulată de Corpul Experţilor Contabili şi Contabililor Autorizaţi din România (CECCAR) înregistrată la ANSPDCP sub nr. 1402/25.01.2024.

Cu privire la această situaţie, **ANSPDCP** a demarat investigaţii la operatorii **UNBR** (pe data de 11.01.2024) şi **CECCAR** (pe data de 10.01.2024), ca urmare a sesizărilor formulate anterior de numitul **DELEANU ŞTEFAN-LUCIAN** (în data de 07.09.2023, 03.01.2024, respectiv 08.01.2024) şi a formularului de notificare a încălcării securităţii datelor cu caracter personal transmis de **CECCAR** în data de 08.01.2024. Din analiza tuturor răspunsurilor și datelor comunicate în prezenta cauză, s-a considerat faptul că nu au rezultat date concrete de natură să contureze în mod legitim faptul că, la baza incidentelor de securitate soldate cu expunerea publică a datelor cu caracter persoanal, a stat o acțiune intruzivă, ilicită, efectuată fără drept asupra bazelor de date, acțiune care să aibe ca scop obținerea de date confidențiale aparținând celor două corpuri profesionale.

A rezultat faptul că numitul **DELEANU ŞTEFAN-LUCIAN** a avertizat asupra breșelor de securitate în data de **07.09.2023**, **CECCAR** și respectiv în data de **28.02.2023**, **UNBR**. Cu toate acestea, se constată că a existat un spatiu mare de timp între semnalarea problemelor tehnice și raportările facute de **CECCAR**, respectiv **UNBR** la **ANSPDCP**, neexistând un raționament sau motiv logic sau legal pentru aceast ecart.

În consecință, pe baza datelor existente si obtinute, a analizelor efectuate, se poate concluziona faptul ca au existat probleme certe în construcția , managerierea si programarea infrastructurii celor 2 site-uri (CECCAR si UNRR), situație care a condus la posibilitatea obiectiva de accesare publică a unor date personale de către utilizatori legitimi ai spațiului de internet. Printre acești utilizatori a figurat si numitul **DELEANU ŞTEFAN-LUCIAN**, care în fapt a și sesizat breșele de securitate la instituțiile reclamante, demers finalizat cu formularea unor plângeri penale împotriva acestuia.

Fiind audiat în cauză, numitul **DELEANU ŞTEFAN-LUCIAN** a confirmat încă o dată aspectele de fapt care au stat la baza constatării și notificării celor două breșe și incidente de securitate care au putut conduce la posibilitatea accesării publice în rețeaua de internet și luării la cunoștință într-un mod neîngrădit a datelor cu caracter personal.

În esență, a acesta a declarat că firma sa, **ENTRYRISE S.R.L.** are o componenta care furnizeaza sabloane pentru infiintarea si desfasurarea activitatii de societati comerciale, sens în care, cauta permanet colaboratori pe acest segment. In continuare, a procedat la crearea unui proces automat (program informatic) de obtinere a datelor publice de pe site-ul **CECCAR** referitoare la contabili afisati, pentru a i se crea o lista de potentiali colaboratori pe care urma sa ii contacteze. Programul informatic creat este legitim si a fost creat de el, avand o arhitectura simpla care descarca si salva informatiile afisate pe site-ul **CECCAR** la acea data, urmand ca ulterior sa

le organizeze in alt format. Acest tip de program este folosit in mod curent pe Internetul public pentru diverse activitati de acumulare si structurare de date inclusiv pentru marketing sau crearea de arhive, inclusiv de catre Google. Dupa ce a rulat programul, datele publice au fost descarcate peste noapte, a doua zi s-a uitat pe ele si a remarcat faptul ca exista o discrepanta evidenta intre ce se afisa in fereastra de browser si datele furnizate efectiv catre browser (prin API) de catre serverele **CECCAR**. In fapt , datele furnizate catre browser de catre serverele **CECCAR** contineau pe langa cele afisate si date care nu ar fi trebuit sa fie transmise de catre server, respectiv CNP, domiciliu, seria si numarul cartii de identitate. Văzand acest lucru si avand expertiza in domeniu, a concluzionat rapid ca exista o problema de securitate cu site-ul si serverul respectiv, deoarece aceste date nu ar fi trebuit sa fie transmise de catre server .

De asemenea a mentionat faptul ca datele transmise de server in format extins care contineau si date cu caracter personal erau transmise automat catre orice sistem informatic (utilizator al site-ului) care efectua o cautare simpla vizuala pe site, cu particularitatea ca datele personale extinse erau transmise de catre server catre browserul utilizatorului (oricare ar fi el), dar nu erau afisate pe ecran, ele fiind primite de browserul utilizatorului si salvate in fisierele temporare ale browserului respectiv si prezente in memoria RAM.

Acest aspect este prevalent in toate comunicatiile dintre un browser si un server web, in sensul ca de cele mai multe ori serverul web trimite mult mai multe date si informatii decat percepe un utilizator pe ecran. Particularitatea aici este ca in mod concret serverul web **CECCAR** ar fi trebuit sa fie setat sa nu trimita datele cu caracter personal extins pe care **CECCAR** le detinea pe arhitectura sa, pentru ca in caz contrar oricine le putea descarca involuntar prin simpla accesare a site-ului si vizualizare a unui contabil sau a unei liste de contabili. Nu își mai aduce acum aminte exact data, dar la scurt timp dupa ce a sesizat problema, a notificat **CECCAR**, prin email si concomitent in aceeasi comunicare a sesizat problema la **ANSPDCP** (in BCC – BCC insemana ca mesajul email a fost transmis in acelasi timp la CECCAR si la ANSPDCP, dar CECCAR nu putea sa vada ca ANSPDCP a primit acelasi email de notificare).

CECCAR i-a raspuns pe email, dar nu își mai aduc amintește ce i-au scris, insa acel mesaj este pus pe site-ul unde a notificat public existenta incidentului. **ANSPDCP** i-a raspuns la mesajul email si i-a spus ca initial nu poate confirma existenta vulnerabilitatii. A presupus astfel ca ei au cerut date de la **CECCAR** si acestia din urma au infirmat existenta unei astfel de vulnerabilitati. Ulterior a transmis catre **ANSPDCP** copia datelor publice pe care le-a descarcat spunandu-le ca **CECCAR** a indus in eroare **ANSPDCP** cu privire la existenta acelei vulnerabilitati si brese. **ANSPDCP** i-a confirmat ca a primit datele si i-a solicitat sa trimită orice alta informatie despre situatia descrisa. Le-a trimis in plus corespondenta cu DPO-ul **CECCAR** (DPO - persoana responsabila cu protectia datelor cu caracter personal). Ulterior nu își mai amintește daca

ANSPDCP a mai facut comunicari directe catre el pe aceasta problema, avand multe mesaje pe diverse probleme cu acestia. La scurt timp a sesizat ca CECCAR a remediat vulnerabilitatea, dar nu a informat contabilii, asa cum prevede legea. Discutand cu prieteni contabili pe Messenger, acestia i-au comunicat ca nu au fost informatii despre existenta bresei. Astfel, a decis sa transmită mesaje de avertizare către contabili afișați pe site, prin email. Mesajul continea date despre cand a fost gasita vulnerabilitatea, tipul de datele personale expuse (nu datele propriu zise), informatii cu privire la riscurile la care au fost expusi si datele de contact ANSPDCP.

Dupa ceva timp a vazut pe grupurile de Facebook ale contabililor o serie de postari ale acestora in care spuneau ca au primit mesaje si email-uri de la CECCAR in care se mentiona ca nu a existat nici o vulnerabilitate si că îl vor face plângere pentru furt de date. A mentionat faptul ca plangerea penala facuta de CECCAR s-a formulat doar dupa ce el a informat contabilii despre vulnerabilitate. Personal consideră astfel că plangerea penala a fost facuta ca o masura punitiva si de răzbunare impotriva sa, pe motiv ca a facut publica existenta vulnerabilitatii si a informat ANSPDCP si toti contabili despre asta.

Fata de cele mentionate mai sus a precizat ca nu a desfasurat nici o activitate infractionala de tip hacking, datele pe care le-a obtinut fiind accesibile in mod public si nerestrictionat, putând fi accesate si descărcate automat de orice utilizator al site-ului CECCAR, el fiind doar cel care a remarcat vulnerabilitatea si a facut notificare despre ea. De altfel, a sters aceste date descărcate imediat dupa ce a notificat ANSPDCP. Referitor la situația si vulnerabilitatea descoperită pe site-ul UNBR, a mentionat ca atunci cand se căutau pe Google toate paginile web de pe site-ul www.IFEP.ro, exista o pagina web publica care descria modul in care se pot accesa mai multe API-uri publice (API ul este o interfața de programare automata specifica serverelor web care, printre alte functii, in cazul de fata, permite vizualizarea tuturor avocatilor, baroul de provenienta si adresa email). Primul API permitea accesarea numelui, baroului și adresei de email, iar al doilea API public permitea accesarea numelui, CNP-ului si a identificatorului unic din sistem din baza de date (un număr crescător atribuit de sistem pentru fiecare dintre avocati). A intrat din browser pe ele, apasand click pe butonul „get lawyers", a introdus caracterul „spatiu" si intr-o căsuța de filtrare a scris sa imi afiseze „100000" si a apasat butonul „cautare". In acel moment, site-ul i-a transmis urmatoarele date aferente avocatilor: identificatorului unic din sistem din baza de date, adresa de email , nume/prenume, baroul de provenienta. Tot din browser a dat click pe butonul „get full lawyers", a urmat aceleasi etape si i-a afisat pe ecran: nume/prenume, identificatorului unic din sistem din baza de date, baroul de provenienta si CNP-ul. In urmatoarea zi, a notificat administratorul platformei IFEP.ro, respectiv firma INTRACONECT (despre care a aflat ulterior, deoarece in prima instanta a initiat contactul prin helpdesk@ifep.ro) si le-a spus ca

API-urile publice par a transmite date care nu ar fi trebuit transmise (ex. CNP) . A asteptat un raspuns, dar nu l-a mai primit.

Ulterior a transmis avocatilor prin e-mail un mesaj in care le descria problema pe care o descoperise, riscurile asociate si sa il contacteze pentru mai multe detalii. Unii dintre ei l-au contactat solicitandu-i informatii suplimentare despre bresa de securitate, el comunicându-le aceste informatii. Le-a spus ca problema a fost remediată intre timp, dar ca o perioada de timp aceste tipuri de date au fost expuse public. Vulnerabilitatea si descrierea situației a fost trimisa de catre el si catre ANSPDCP in fereastra de timp dintre momentul remedierii vulnerabilității si informarea pe care a trimis-o eu catre avocati. Plangerea facuta de catre UNBR a venit dupa ce a informat avocatii, la aproximativ o luna de zile dupa informarea avocatilor, nu își mai aduce aminte exact și la un an distanta de momentul în care el a sesizat vulnerabilitatea la helpdesk@ifep.ro. Nu a stiut mult timp despre faptul ca **UNBR** a facut plangere penala impotriva sa, afland cu ocazia acestei audieri. Consideră ca aceasta plangere penala are de asemenea un caracter de represalii impotriva sa, fiind facută târziu si fiind nefondata. La un moment dat pe Facebook, a fost contactat de catre o persoana care s-a prezentat ca fiind in conducerea UNBR si care l-a intrebat daca situatia descrisa este adevarată , iar el a confirmat.

A mai mentionat faptul ca pe site-ul pe care erau furnizate functiile API se facea mentiunea expresa despre cum se pot accesa acestea, descrierea serviciului, modul de accesare a acestuia si ghidul de accesare a datelor.

Având în vedere toate aspectele de fapt rezultate din probele administrate în cauză, procurorul de caz a apreciat că nu poate fi angajată răspunderea penală a numitului **DELEANU ŞTEFAN-LUCIAN**, totodată și în calitate de reprezentant al societății **ENTRYRISE S.R.L.**, sub aspectul săvârșirii celor două infracțiuni reclamate în cauză de către reprezentanții **UNBR** și **CECAR**, respectiv infracțiunile de **acces ilegal la un sistem informatic și transfer neautorizat de date informatice,** fapte de natură informatică și îndreptate împotriva siguranței și integrității sistemelor și datelor informatice, faptele nefiind prevăzute de legea penală, atât sub aspectul tipicității obiective legat de faptul că acțiunile pretins ilicite s-ar fi făcut în mod nelegal/neautorizat cât și sub aspectul laturii subiective, lipsind însăși intenția făptuitorului de a accesa părți nepublice ale site-ului și de a transfera în mod fraudulos date confidențiale și private.

***

Împotriva soluţiei de clasare dispusă prin ordonanţa mai sus menţionată, la data de **02.11.2025,** în termen legal, a formulat plângere petenta **U.N.B.R.,** prin Cabinet de Avocat - Av. Dragu Marius, care a solicitat desfiinţarea soluţiei de clasare, ca fiind nelegală și netemeinică și completarea urmăririi penale pentru a pune în mișcare acțiunea penală împotriva persoanei fizice și a persoanei juridice **ENTRYRISE S.R.L.**

Totodată, în completarea urmăririi penale, s-au solicitat: audierea persoanei vătămate **U.N.B.R.** și a reprezentanților firmei IT administratoare ale platformei informatice; efectuarea de percheziții informatice; ridicarea echipamentelor și suporturilor de stocare; efectuarea unei expertize tehnice; reaudierea persoanei fizice după expertiză; asigurarea accesului efectiv la dosar și analizarea confiscării speciale, precum și administrarea tuturor probelor necesare pentru lămurirea completă a cauzei.

În motivarea plângerii, s-au arătat și solicitat în esență următoarele:

<u>Aspecte de nelegalitate:</u>

- procurorul a pronunțat o soluție prematură, cu încălcarea obligației legale de a administra toate probele esențiale, soluția întemeindu-se aproape exclusiv pe declarația numitului **DELEANU ȘTEFAN- LUCIAN**, fără a se efectua și administra alte probe apreciate ca necesare și mai sus amintite.
- omisiunea de a soluționa distinct răspunderea penală a persoanei juridice **ENTRYRISE S.R.L.**
- refuzul parchetului de a permite accesul la dosar și de a recunoaște apărătorul ales

<u>Aspecte de netemeinicie:</u>

- Parchetul a transmis solicitări către firmele care asigurau mentenanța și hosting-ul platformelor informatice ale **UNBR** și **CECCAR**. pentru a obține informații privind eventuale accesări neautorizate, iar aceste firme ar fi confirmat existența unor accesări externe ale serverelor **UNBR** și **CECCAR**.
- Interpretarea subiectivă a declarației de martor a numitului **DELEANU ȘTEFAN-LUCIAN**
- În mod contradictoriu cu cele declarate de martorul **DELEANU ȘTEFAN-LUCIAN**, procurorul a reținut în ordonanța de clasare următoarele paragrafe: "*Din declarațiile persoanei audiate nu rezulta intenția de a prejudicia instituțiile vătămate, ci intenția de a semnala deficiențele de securitate... Nu există elemente care să ateste intenția infracțională, fapta nefiind săvârșită cu scopul de a obține un avantaj necuvenit.* " Ulterior, concluzia devine decisivă pentru soluția de clasare: "*Accesul nu poate fi calificat ea fiind fără drept, in condițiile în care persoana audiată a acționat din convingerea că realizează o activitate utilă public.* " Această concluzie este contradictorie și nelegală.
- Nu poate fi acceptată ideea că autorul faptelor sesizate a descărcat mai multe informații din sistemele informatice și pe care le a stocat fie pe cloud, fie pe dispozitivele personale și acesta să nu fie tras la răspundere și nici o măsură să nu fie luată de parchet.

- Cercetarea persoanei juridice **ENTRYRISE S.R.L.** - lipsa cercetării și a analizei persoanei jurdice care este cerută prin plângerea penală depusă de către **U.N.B.R.**
- parchetul nu a dispus ridicarea dispozitivelor folosite (calculatoare, servere, conturi cloud etc.)
- Soluția a fost întemeiată aproape exclusiv pe declarația numitului **DELEANU ŞTEFAN-LUCIAN**, și pe câteva adrese sumare ale instituțiilor **UNBR** și **CECCAR**. fără o verificare reală a situației de fapt și fără administrarea probatoriului necesar.
- Din analiza înscrisurilor anexate (Anexa - postările publice realizate în august 2025), rezultă că numitul **DELEANU ŞTEFAN-LUCIAN** continuă și în prezent activitățile care au constituit obiectul dosarului penal anterior, respectiv accesarea și prelucrarea neautorizată a datelor informatice aparținând unor instituții ale statului.

..Dl. Deleanu continuă în prezent cu aceeași activitate pe site-urile Portal.Just și a CSM procedând întocmai ca și cum este de bună credință, verificând in continuare breșe de securitate și la alte instituții publice și colectând date din sistemul de justiție.

***

Examinând criticile invocate și întregul conținut al plângerii formulate în cauză, raportat la actele dosarului şi ordonanţa de clasare emisă în cauză, atât sub aspectul motivelor de fapt cât şi al temeiului legal care au stat la baza soluției, reținem următoarele:

Apreciem că procurorul de caz a emis soluția de clasare pe baza și în urma administrării acelor probe considerate ca fiind utile și concludente raportat la susținerile persoanei vătămate și apărările persoanei reclamate. Nu a fost avută în vedere în mod exclusiv declarația de martor a făptuitorului **DELEANU ŞTEFAN-LUCIAN**. Neadministrarea altor probe, printre care și a mijloacelor de probă indicate de către petentă în conținutul prezentei plângeri (audiere reprezentant petentă/firmă IT; expertiza informatică, perchezitie informatică;) a avut la bază aceleași criterii ce țin de utilitate și oportunitate, în condițiile în care aspectele și circumstanțele faptice referitoare la incidentul și evenimentele petrecute încă de la începutul anului 2023 la nivelul platformei **IFEP**, au putut fi stabilite de o manieră rezonabilă și legitimă atât prin activitățile și verificările efectuate, a datelor și informațiilor comunicate de altfel de către petenta **UNBR**, firmelor care s-au ocupat atât cu administrarea platformei/efectuarea auditului de securitate, cât și prin declarația persoanei reclamate, aceasta din urmă reiterând și în scris aspectele pe care le-a expus anterior și public, însoțite cu date tehnice și care au privit contextul în care acesta a ajuns să sesizeze și să notifice **UNBR** cu privire la cele constatate.

În plus, unele dintre probele solicitate, nu numai că nu au apărut utile pe parcursul urmăririi penale, ci au fost și sunt în continuare și imposibil de efectuat (cazul expertizei, în condițiile în care, astfel cum s-a reținut din chiar datele comunicate în cauză, inclusiv raportul de audit local și

comunicat, a constatat dificultăți în analiza efectuată, între timp, de la data presupusei breșe și data investigației, platforma informatică suferind modificări).

Nu a existat astfel niciun dublu în ceea ce privește accesul martorului la respectivul Api/endpoint public care (fără a se stabili dacă a avut la bază o acțiune intenționată, sau o eroare tehnică) i-a transmis pe lângă date generale și date cu caracter personal (precum CNP) aferente avocaților. De altfel, tocmai faptul că acesta a intrat într-un mod nerestricționat în posesia respectivelor date confidențiale suplimentare, l-a făcut să constate că este vorba despre o problemă de securitate și a procedat la sesizarea și notificarea acesteia către adiministratorul platformei și ulterior a notificat o parte dintre titulari și a făcut public respectivul incident. Or, ridicarea de la martor a eventualului dispozitiv informatic care să dovedească odată în plus dacă acesta a intrat sau nu în posesia respectivelor date nu a fost necesară, mai ales în condițiile în care, raportat la soluția pronunțată, dispozitivul nu este supus vreunei măsuri de siguranță, respectiv confiscare specială.

Toate probele și activitățile de urmărire penală au fost efectuate prin raportare la faptele sesizate, fapte ce au privit pe făptuitor, atât ca persoană fizică cât și ca reprezentant legal al societății reclamate, neputându-se considera o abordare diferită de soluționare a cauzei și de tratare a răspunderii penale.

Nu poate fi primită nici susținerea cu privire la existența unui refuz din partea parchetului de a recunoaște apărătorul petentei și dreptul acestuia de a studia dosarul, în cauză, nefiind identificată nici o astfel de cerere formulată și adusă la cunoștința organului de urmărire penală, pe parcursul urmăririi penale. Singura cerere se plasează la un moment ulterior soluționării cauzei.

Cu privire la pretinsele aspecte legate de netemeincia solutiei de clasare, respectiv faptul că firma care asigura mentenanța și hosting-ul platformei informatice a **UNBR** ar fi confirmat existența unor accesări externe neautorizate, considerăm că un astfel de răspuns nu a fost identificat în cauză. Dimpotrivă, astfel cum s-a reținut și în cuprinsul motivării soluției de clasare, din răspunsurile comunicate, a rezultat faptul că, în cadrul investigației de digital forensics realizate pentru Uniunea Națională a Barourilor din România (UNBR), s-au identificat câteva limitări semnificative în ceea ce privește configurarea și gestionarea logurilor sistemului IT. Aceste deficiențe au avut un impact direct asupra capacității de a reconstitui evenimentele și de a evalua amploarea unui posibil incident de securitate. Din cauza configurațiilor inadecvate ale logurilor și a schimbării versiunii platformei între momentul presupusei breșe și timpul investigației, a fost dificil de determinat cu precizie dacă un acces neautorizat a avut loc. Totodată, logurile furnizate, care acoperă perioada presupusului incident, nu au oferit informații suficiente despre evenimentele de autentificare sau modificările de configurare ale sistemului. Această lipsă de detalii a împiedicat să se poată stabili în mod eficient, cine s-a conectat la sistem, când exact s-au realizat respectivele

conexiuni și dacă au existat sau nu încercări nereușite de autentificare - un posibil indicator al unor tentative de acces neautorizat.

Chiar și în aceste condiții, al analizei și comunicării propriilor investigații și date deținute, petenta invocă cu prilejul prezentei plângeri faptul că parchetul s-a limitat la a prelua în mod formal aceste informații fără verificări tehnice suplimentare, fără a fi indicate în opinia petentei, care ar fi fost în mod concret acele date tehnice disponibile și concludente care să facă obiectul respectivelor verificări tehnice.

Se vorbește de o interpretare subiectivă a declarației martorului **DELEANU ŞTEFAN-LUCIAN**, de către organul de urmărire penală, afirmație contrazisă însă de modul în care organul de urmărire penală a procedat la stabilirea situației de fapt, coroborând toate datele și informațiile furnizate de părți, raportat inclusiv la aspectele declarate în calitatate de martor de persoana reclamată, aspecte și date tehnice (legate de respectivul API/Endpoint-uri publice, breșă constatată și notificată administratorului platformei ifep încă din februarie 2023, aspecte expuse și ulterior, public), care de altfel nu au fost combătute în niciun fel de către petentă.

Așadar, **UNBR** nu a recunoscut existența sau posibilitatea existenței unui astfel de incident/breșe de securitate, dar nici nu a combătut de o manieră rezonabilă notificările și aspectele ce le-au fost semnalate de îndată de către martor, în scopul remedierii incidentului de securitate. Totodată, nu s-a indicat și nici nu au rezultat din datele și informațiile comunicate, vreo altă modalitate faptică concretă, cu caracter intruziv, o anumită acțiune ilicită prin care să se fi procedat la o accesare frauduloasă a sistemelor informatice, acțiune ce putea astfel fi considerată ca fiind în mod evident îndreptată împotriva siguranței și integrității respectivului sistem informatic și a anumitor date considerate private și neexpuse în niciun moment în mod public.

Deși situația este asemănătoare, dar nu identică, totuși CECAR (astfel cum rezultă din analiza raspunsurilor comunicate de aceasta) a recunoscut aspectele constatate și și transmise de către același martor **DELEANU ŞTEFAN-LUCIAN**, cu privire la faptul că sistemul informatic a avut o perioada în care a transmis prin API către browserele utilizatorilor mai multe date decat sunt transmise in prezent in baza unui Search Query (interogare), existand posibilitatea reala ca un utilizator legitim sa poata obtine mai multe date despre persoane decat numele, prenumele, numarul de telefon si orasul.

In concret o persoana sau un program automat (program la care face referire de altfel și martorul audiat), putea obtine in mod public si neîmpiedicat de masuri de securitate date persoanale suplimentare despre persoanele afisate pe site-ul CECCAR (inclusiv date privind CNP-ul).

Se vorbește în conținutul plângerii, inclusiv la faptul că procurorul ar fi reținut aspecte de fapt ce ar contraveni celor declarate de martor, în sensul că martorul ar fi recunoscut că a săvârșit

infracțiunile de acces ilegal la un sistem informatic și de transfer neautorizat de date informatice, însă procurorul reține aspecte de natură să-l exonereze de răspundere penală.

Nu putem fi de acord nici cu această remarcă, în condițiile în care, nu numai că paragrafele la care se face referire și care ar fi fost menționate de către procuror nu se regăsesc de a asemenea manieră în motivarea ordonanței de clasare, dar nici martorul audiat nu a recunoscut în vreun moment că ar acționat cu intenția de a accesa și a trasfera date confidențiale din sisteme protejate și nepublice, acțiuni care să fie efectuate în mod implicit fără drept, ci dimpotrivă, a constatat că accesul la anumite date date personale (care erau furnizate printr-un API public, alături de alte date generale), nu era la acel moment protejat și îngrădit.

Totodată, din studierea întregului conținut al plângerii formulate, se constată că aspectele și nemulțumirile invederate au privit în majoritatea lor, atât petenta **UNBR** cât și **CECAR**, deși cu privire la aceasta din urmă, nu există reprezentativitate și nici nu a fost formulată o plângere distictă de către această persoană vătămată.

Nu în ultimul rând, se solicită o infirmare a soluției și o reluare a urmăririi penale, pentru anumite motive extrinseci obiectului sesizării și urmăririi penale efectuate în cauză, respectiv pentru faptul că, în urma unor verificări din surse publice, a rezultat că aceeași persoană ar dovedi aceeași perseverență infracțională cu privire la accesarea și transferarea neatorizată de date din sistemele informatice aparținând altor instituții publice, în cauză, Ministerul Justiției și Consiliul Superior al Magistraturii.

În urma studierii anexelor depuse și totodată printr-o simplă accesare a postărilor în spațiul public, se poate observa motivul și împrejurările care au stat la baza constatării și notificării similare a respectivelor breșe de securitate, nefiind de altfel formulate plângeri penale de către titularii legitimi, pentru săvârșirea vreunei fapte îndreptate împotriva sistemelor sau datelor informatice și nerezultând date concrete pe parcursul urmăririi penale care să fundamenteze o eventuală sesizare din oficiu sau, după caz, o extindere a urmăririi penale.

Raportat la toate aceste aspecte, apreciem că faptele sesizate nu se pot imputa persoanelor reclamate, nici din punct de vedere obiectiv și nici subiectiv.

Nu se poate astfel considera că în cauză, acesta a acționat în forma de vinovăție prevăzută de lege, respectiv cu intenția calificată de a obține, fără drept, date confidențiale cu caracter personal (exp. CNP, adrese de mail) aparținând avocaților/contabililor, prin operațiuni intruzive și neautorizate și care să fi avut drept țintă sistemele informatice care stocau astfel de date private și neexpuse în mod public, orice dubiu care poartă asupra acestor din urmă aspecte, profitând întodeauna persoanei cercetate, potrivit principiului "in dubio pro reo".

În cauză, nu sunt îndeplinite și întrunite cerințele pentru existența elementului material constitutiv sub aspectul tipicității obiective ale unor asemenea fapte penale și deopotrivă, nu se

poate considera că acțiunile, întreprinse în cauză de numitul **DELEANU STEFAN – LUCIAN** (pe neglijență/neatenție la o expunere către public a unor date cu caracter personal), de accesare, interogare, căutare și descărcare de date din sistemele informatice accesibile publicului, au fost îndeplinite fără drept.

Pentru aceste motive și în urma analizei tuturor criticilor din plângerea formulată raportat la actele dosarului şi ordonanţa de clasare emisă în cauză, apreciem că soluţia emisă în cauză este legală şi temeinică, atât sub aspectul motivelor de fapt cât şi al temeiului legal care au stat la baza acesteia.

Prin urmare, se va respinge ca nefondată plângerea formulată în cauză, nefiind identificate motive care să atragă o infirmare parţială a ordonanţei de clasare în ceea ce privește faptele sesizate de către petenta **U.N.B.R.**, fapte similare cu cele sesizate în aceeași cauză de către **C.E.C.A.R.**

Faţă de aceste considerente, în temeiul dispozițiilor art. 339 Cod procedură penală,

DISPUN:

1. **Respingerea** ca nefondată a plângerii formulate de către petenta **UNIUNEA NAȚIONALĂ A BAROURILOR DIN ROMÂNIA,** prin reprezentantul convenţional, avocat Dragu Marius, împotriva ordonanței nr. **364/19/P/2024** din data de **02.10.2025**, prin care s-a dispus clasarea cauzei.

2. Ordonanta se comunică petentei **UNIUNEA NAȚIONALĂ A BAROURILOR DIN ROMÂNIA,** sediul reprezentantului convenţional.

3. În conformitate cu prevederile art. 340 din Codul de procedură penală, petenta are posibilitatea de a face plângere, în termen de 20 de zile de la comunicare, la judecătorul de cameră preliminară din cadrul Tribunalului Bucureşti, instanţă competentă să judece cauza în primă instanţă.

MINISTERUL PUBLIC - ROMÂNIA - Direcția de Investigare a Infracțiunilor de Criminalitate Organizată și Terorism - PARCHETUL DE PE LÂNGĂ I.C.C.J.

PROCUROR ȘEF SECȚIE [redacted]

****
*** Rezultate transmitere ***
****

Transmiterea s-a incheiat.

Nr. lucrare	0674
Adresa	00213193858
Numele	
Oră inceput	22/12 08:43
Durată apel	00'22
Pagini	1
Rezultat	OK

147

TRIBUNALUL BUCUREȘTI
SECȚIA I PENALĂ
Operator de date cu caracter personal 2891/4460
Dosar nr. 46976/3/2025
Termen la data de 30.01.2026, CSC8, ora 09.00, sala 239
Emisă la data 22.12.2025
FAX 021 408 37 73

CĂTRE
PARCHETUL DE PE LÂNGĂ ÎNALTA CURTE DE CASAȚIE ȘI JUSTIȚIE

DIRECȚIA DE INVESTIGARE A INFRACȚIUNILOR DE CRIMINALITATE ORGANIZATĂ ȘI TERORISM

Dosar nr. 364/19/P/2024

În baza dispozițiilor date de instanța de judecată, în cauza cu numărul de mai sus având ca obiect plângerea formulată în baza disp. art. 340 C.p.p. de către petenta Uniunea Națională a Barourilor din România vă adresăm solicitarea ca anterior termenului de judecată din data de 30.01.2026, CSC8, ora 09.00, sala 239 să ne înaintați:

- dosarul de urmărire penală nr. 364/19/P/2024 (în format letric sau electronic),
- ordonanța procurorului șef de secție,
- dovada de comunicare a ordonanței procurorului șef de secție către petentă.

Facem mențiunea că dosarul de urmărire penală vă va fi restituit imediat ce nu ne va mai fi necesar.

De asemenea, vă adresăm solicitarea de a ne comunica ordonanța de clasare în format electronic - word (adresa de mail rotaru.amelia@just.ro).

Vă mulțumim pentru colaborare.

JUDECĂTOR DE CAMERĂ PRELIMINARĂ **GREFIER**

[redacted] [redacted]

ROMÂNIA

TRIBUNALUL BUCUREŞTI

Bucureşti, B-dul Unirii nr. 37, sector 3

REGISTRATURA SECŢIEI I PENALĂ

PROCES VERBAL,

Încheiat astăzi, 16.12.2025

Primind plângerea formulată de petenta **Uniunea Națională a Barourilor din România**, împotriva ordonanței de clasare din data de 02.10.2025, emisă în dosarul de urmărire penală nr. 364/19/P/2024 al Parchetul de pe lângă Înalta Curte de Casație și Justiție – Direcția de Investigare a Infracțiunilor de Criminalitate Organizată și Terorism, şi având în vedere dispoziţiile art. 102 alin. (2) din Regulamentul de Ordine Interioară a Instanţelor Judecătoreşti, am procedat la efectuarea verificărilor privind dosarele în care s-au îndeplinit acte sau măsuri procesuale de către judecătorul de drepturi şi libertăţi, în cauza penală ce face obiectul dosarului de urmărire penală mai sus menţionat.

În urma verificărilor efectuate a rezultat faptul că nu au fost soluţionate astfel de cereri.

Grefier,

[redacted]

TRIBUNALUL BUCUREȘTI
DOSAR NR. _____/_____/2025

Primit, astăzi 16.12 **.....2025**

S-a repartizat aleatoriu completului..... C1C8 .....

cu termen la ..... 2001 .....**2025**

Semnătură persoană desemnată
cu repartizarea aleatorie
.....

R E Z O L U Ț I E

din data de_____

Deleanu Ștefan-Lucian

(+) intimatii < ENTRY RISE SRL

☒ se citează petentul/contestatorul/părţile/persoana vătămată/inculpatul

□ se emite adresă către Baroul București pentru a se desemna un avocat din oficiu pentru petent/ contestator;

□ se încunoştinţează avocatul ales;

□ se vor efectua verificări în baza de date: □ ROCRIS (cazier judiciar)
□ PATRIMVEN
□ ONRC
□ DEPABD
□ ANP
□ SIMDPPL (centre de reţinere şi arest)

□ pune în vedere revizuentului să completeze cererea până la primul termen de judecată, sub sancţiunea inadmisibilităţii, cu precizarea în scris a motivelor avute în vedere, cu arătarea cazului de revizuire pe care se întemeiază şi a mijloacelor de probă în dovedirea acestuia; la cerere se vor alătura copii de pe înscrisurile de care înţelege a se folosi în proces, certificate pentru conformitate cu originalul, iar când înscrisurile sunt redactate într-o limbă străină, ele se vor alătura în traducere efectuată de un traducător autorizat;

□ pune în vedere contestatorului să precizeze până la primul termen de judecată cazurile de contestaţie pe care le invocă, precum şi motivele aduse în sprijinul acestora;

□ se emite adresă către Judecătoria/Tribunalul/Curtea de Apel _____ pentru a se depune s.p._____/_____, cu referat privind data si modalitatea rămânerii definitive;

□

Alte măsuri: adr dup + ord. proc sf + dovada com. ordonantei proc sf catre petenta

CABINET DE AVOCAT "DRAGU MARIUS"

ADRESA: B-dul Unirii Nr.20, Bl.5c, Sc.A, Ap.3, Sector 4, București
TEL.0735844899, email-mariusdragu@yahoo.com, FAX 031.434.0792

101

Către:
DIICOT- STRUCTURA CENTRALĂ
DOSAR NR. 364/19/P/2024

DOMNULE PROCUROR-ȘEF,

Subscrisa **UNIUNEA NAȚIONALĂ A BAROURILOR DIN ROMÂNIA**, cu sediul în București, Sector 5, Splaiul Independenței nr. 5, Palatul de Justiție, identificată prin C.I.F. RO 4315974, reprezentată legal prin Președinte Av. dr. Traian - Cornel BRICIU, reprezentantă convențional prin *avocat Dragu Marius*, e-mail: unbr@unbr.ro, în calitate de parte vătămată, în temeiul art. 81 alin. (1) lit. c) și e) și art. 94 alin. (1) și (2), formulăm:

CERERE DE CONSULTARE ȘI FOTOCOPIERE

Prin prezenta vă aducem la cunoștință faptul că, la data de **13.10.2025**, mi-a fost comunicată **Ordonanța de clasare nr. 364/19/P/2024**, împotriva căreia legea recunoaște dreptul subscrisei de a formula plângere în termen de **20 de zile** de la comunicare, conform dispozițiilor art. 339–341 Cod procedură penală.
Având în vedere necesitatea pregătirii apărărilor și a unei plângeri motivate, **solicit, în temeiul art. 94 alin. (1) și (2) CPP**, următoarele:

1. **Studierea dosarului penal nr. 364/19/P/2024**;
2. **Eliberarea de fotocopii**, pe cheltuiala subscrisei, după actele și probele administrate în cauză, care au stat la baza soluției de clasare.

Accesul la dosar este indispensabil pentru exercitarea dreptului la apărare și pentru depunerea în termen legal a plângerii împotriva soluției dispuse.

Anexă:

- copie ordonanță de clasare;
- copie împuternicire avocațială.
- copie legitimație.

Pentru programare avem rugămintea ca dl. avocat Marius Dragu să fie contactat la telefon 0735.844.899 sau pe e-mail mariusdragu@yahoo.com

UNIUNEA NAȚIONALĂ A BAROURILOR DIN ROMÂNIA
prin avocat Dragu Marius

DATA
13.10.2025