

# Apărarea avocaturii la frontiera digitală

## Deschidere:

Traian Briciu, *Președintele UNBR*  
Daniel Fenechiu, *Vicepreședinte UNBR*

## Panel 1:

Mijloace de combatere a  
avocaturii ilegale în mediul online  
Moderator: Liviu Mihai, *Vicepreședinte UNBR*

## Panel 2:

Peisajul actual al amenințărilor cibernetice  
pentru avocați  
Moderator: Cătălin Filișan, *Membru al Comisiei  
Permanente a UNBR*

## Panel 3:

Soluții IT și tehnologii pentru protejarea  
activităților avocatului  
Moderator: Sergiu Capisizu, *Consilier UNBR*



## CONCLUZIILE CONFERINȚEI APĂRAREA AVOCATURII LA FRONTIERA DIGITALĂ

**Avocat Traian Briciu, președintele UNBR:**  
***Apărarea avocaturii la frontiera digitală. Trei direcții strategice***

### **EXTRAS VIDEO AICI**

În cadrul conferinței organizate Uniunea Națională a Barourilor din România, președintele UNBR, Traian Briciu, a deschis dezbaterile invocând trei teme fundamentale care vizează evoluția profesiei de avocat într-un peisaj juridic tot mai digitalizat și globalizat. Principalele idei ce au stat la baza acestei conferințe vor continua să fie dezbătute în seria de conferințe ce vor urma.

### ***Provocările noii avocaturii ilegale***

Prima problemă adusă în atenție de președintele UNBR a fost schimbarea provocărilor legate de exercitarea ilegală a profesiei. Dacă în anii 2000, principalul obstacol era reprezentat de identificarea celor care pretindeau a fi avocați fără a fi calificați, lucrurile s-au schimbat în prezent. Astăzi, principalul pericol provine din zona online, unde site-urile care pretind a oferi consultanță juridică pot fi operate de persoane necalificate, uneori chiar de entități necunoscute sau inexistente. Conform președintelui UNBR, identificarea acestor entități ilegale este mult mai dificilă decât în trecut, iar mecanismele clasice de reglementare, precum plângerile legale, nu mai sunt eficiente. De aceea, este necesar să se adopte o abordare inovativă, în care profesia de avocat să devină activă în protejarea sa.



### ***Protecția informațiilor în era digitală***

Al doilea punct abordat a fost vulnerabilitatea profesiei de avocat în fața atacurilor cibernetice și a riscurilor legate de protecția informațiilor confidențiale. Profesia de avocat este una în care secretul profesional și confidențialitatea informațiilor sunt esențiale. În fața riscurilor tot mai mari, protejarea datelor sensibile ale clienților devine o prioritate majoră. Președintele UNBR, Traian Briciu a subliniat importanța unui sistem robust de securitate cibernetică, mai ales în domenii de activitate extrem de sensibile, cum ar fi achizițiile publice sau concurența neloială, unde orice breșă de securitate poate afecta grav reputația unui cabinet sau a unei firme de avocatură.

### ***Digitalizarea sistemului judiciar și accesul avocaților la informațiile din dosare***

De-a lungul anilor, avocații au cerut un acces privilegiat la documentele și informațiile relevante pentru apărarea clienților lor, iar implementarea sistemului ECRIS 5 ar putea răspunde la această necesitate. În plus, pentru a putea beneficia de această tehnologie, profesia de avocat trebuie să se adapteze rapid la noile cerințe tehnice, lucru care presupune o investiție continuă în formarea profesională și tehnologică a avocaților.

### ***Transformarea digitală a avocaturii este inevitabilă***

Traian Briciu a subliniat că profesia de avocat nu mai poate supraviețui în fața noilor provocări fără a evolua tehnologic. Schimbările propuse vor fi discutate în continuare în cadrul unor conferințe și dezbateri, având ca scop integrarea unor soluții inovatoare care să răspundă noilor provocări și să sprijine avocații în protejarea drepturilor și intereselor clienților lor într-un peisaj tot mai digitalizat.

În încheiere, președintele UNBR a mulțumit pentru sprijinul acordat de către vicepreședintele Fenechiu, evidențiind că propunerile privind digitalizarea serviciilor avocațiale trebuie să devină o prioritate pentru profesia juridică. Chiar dacă au existat obstacole și decizii controversate în trecut, direcția este clară: avocatura trebuie să se adapteze rapid, iar acest lucru poate fi realizat doar printr-o abordare tehnologică și inovativă.



**Avocat Daniel Fenechiu, Vicepreședinte UNBR:**

***Digitalizarea avocaturii este inevitabilă - confidențialitatea a fost și va rămâne un principiu esențial al profesiei de avocat***

**EXTRAS VIDEO AICI**

Într-un discurs amplu, Vicepreședintele UNBR, Daniel Fenechiu a abordat teme esențiale despre digitalizarea avocaturii și provocările pe care profesia le întâmpină în contextul tehnologic actual. Mesaje cheie s-au concentrat pe necesitatea adaptării la progresul tehnologic, depășirea obstacolelor din trecut și identificarea soluțiilor pentru viitor.

Le mulțumesc lui Traian Briciu și lui Liviu Mihai, pentru că acum am ajuns să discutăm deschis despre provocările profesiei de avocat, în contextul digitalizării. În trecut, am avut momente în care nu înțelegeam pe deplin ce se întâmplă, dar acum, cred că e clar pentru toți că digitalizarea este o necesitate absolută, iar profesia trebuie să se adapteze la acest nou context.

Am avut mai multe întâlniri, am discutat despre inteligența artificială, despre cum va evolua avocatura în acest context. La început, ne întrebam ce se va întâmpla cu avocații când inteligența artificială va pătrunde în domeniul nostru. După patru ani, constatăm că multe dintre uneltele digitale, inclusiv ChatGPT, sunt deja un ajutor important pentru avocați. Sunt state care, însă, interzic utilizarea unor astfel de tehnologii din teama că ar putea fi manipulate, însă există și o cerință crescută de a digitaliza procesele judiciare.

Este esențial ca profesia noastră să țină pasul cu progresele tehnologice, altfel riscă să fie depășită de alte profesii. Multe dintre proiectele de digitalizare sunt foarte bine gândite pentru a ajuta profesia, însă rezistența la schimbare este mare. Acum trebuie să ținem cont de faptul că nu doar avocații trebuie să își asume schimbările, dar și instituțiile trebuie să se alinieze.

În ceea ce privește protecția datelor, aceasta trebuie să fie o prioritate. Confidențialitatea a fost și va rămâne un principiu esențial al profesiei de avocat, dar trebuie să recunoaștem că, odată cu avansul tehnologic, acest secret profesional a suferit unele limitări naturale. În orice caz, trebuie să găsim un echilibru între utilizarea tehnologiei și păstrarea protecției datelor.

Digitalizarea avocaturii, protecția datelor și combaterea avocaturii ilegale sunt provocările pe care trebuie să le abordăm cu seriozitate. UNBR trebuie să continue să dezvolte soluții pentru a sprijini profesia și a o adapta la noile realități. Conferințele viitoare, ca cea din 10 aprilie, sunt esențiale pentru a dezbate aceste teme și a adresa propunerile legislative care vor sprijini digitalizarea avocaturii.

***Digitalizarea este o necesitate, nu o alegere***

Daniel Fenechiu a subliniat că "epoca digitală a venit peste noi și depinde doar de noi cum o întâmpinăm". A atras atenția asupra importanței conectării avocaților la platforme digitale integrate, care să le ofere acces la baze de date esențiale și să faciliteze colaborarea cu instituțiile publice, menționând platforma UNBR ca exemplu de inițiativă ce ar fi putut revoluționa accesul tinerilor avocați la tehnologie.

***Lecțiile învățate și Viitorul Digital***

Amintind dezbaterile din timpul pandemiei despre inteligența artificială și instrumentele tehnologice, Daniel Fenechiu a punctat faptul că ceea ce părea futurist acum câțiva ani a devenit astăzi indispensabil: „ChatGPT-ul este prietenul multor avocați.” Totodată, a evidențiat diferențele dintre deschiderea avocaților față de digitalizare și temerile privind confidențialitatea și riscurile cibernetice.

***Apel la participare și la unitate***

Daniel Fenechiu a încurajat avocații să participe activ la dezbaterile viitoare, inclusiv la conferința programată pe 10 aprilie, dedicată perspectivelor legislative și digitale. „Poate reușim să venim cu un proiect care, chiar dacă nu va fi perfect, poate fi perfecționat pe parcursul legislativ”, a afirmat acesta. Vicepreședintele UNBR a încheiat cu un apel la unitate și la o viziune comună pentru viitorul profesiei: „Hai să ne concentrăm pe viitor. Ce-a fost, a fost. Fiecare are greșelile lui. Important este să progresăm împreună.”

Rămâne de văzut cum avocații vor valorifica oportunitățile pe care le oferă digitalizarea și cum se vor poziționa față de noile provocări legislative și tehnologice.



## PANEL 1:

### *Mijloace de combatere a avocaturii ilegale în mediul online*

#### EXTRAS VIDEO AICI

**Moderator:** Avocat Liviu Mihai, Vicepreședinte UNBR

**Participanți la dezbateri:** judecător Roxana Chiuriu, Directorul Direcției Afaceri Europene, Relații Internaționale și Programe din cadrul CSM; Călin Cozan, Reprezentant ANCOM; Adrian-Victor Vevera, Directorul General al Institutului de Cercetare-Dezvoltare în Informatică, ICI București; Cătălin Marius Joița, Decanul Baroului Brașov, Gabriel Nicolae, Decanul Baroului Vrancea, Laurian Ostafciuc, Consilier UNBR; Danny Bârdan, Consilier UNBR.

Dacă avocatura ilegală „tradițională” a fost în mare parte eliminată prin măsuri legislative, practicile neautorizate din mediul digital necesită strategii pluridisciplinare. Combaterea avocaturii ilegale din online necesită măsuri strategice, cum ar fi validarea digitală a avocaților și crearea de instrumente care să blocheze rapid site-urile ilegale.

Aceste provocări au fost discutate în cadrul primului panel al conferinței „Apărarea avocaturii la frontiera digitală”, care a reunit experți din domeniul juridic și tehnologic. Din dezbateri au rezultat mai multe idei care, abordate într-o viziune integratoare, ar putea contribui la combaterea fenomenului avocaturii ilegale și afirmarea și diferențierea avocaților autorizați în mediul online.

**În principal, s-au conturat următoarele posibilități de combatere a avocaturii ilegale din mediul online:**

- **Crearea unor mecanisme de validare rapidă a site-urilor și platformelor care oferă servicii juridice, astfel încât doar cele autorizate să poată funcționa.**

S-a subliniat necesitatea validării digitale a avocaților în scopul creării unei identități profesionale clare, în mediul online. Avocații ar trebui să aibă o identitate digitală verificabilă (cum ar fi certificatul electronic calificat sau un sigiliu digital UNBR), care să ateste autenticitatea lor în mediul online.

Site-urile oficiale ale avocaților ar trebui să includă marcaje de autenticitate și linkuri către o bază de date oficială.

S-a conturat propunerea de a colabora cu platformele mari online (Google, Facebook) pentru a afișa avocații autorizați în rezultate de căutare verificate.



Roxana CHIUARIU, Directorul Direcției Afaceri Europene, Relații Internaționale și Programe din cadrul CSM

Conferința „Apărarea avocaturii la frontiera digitală”, Uniunea Națională a Barourilor din România



- **Blocarea rapidă a site-urilor ilegale**

S-a propus dezvoltarea unor mecanisme eficiente pentru identificarea și închiderea site-urilor care oferă servicii juridice neautorizate.

- **Implementarea noului sistem ECRIS V, care oferă posibilitatea interconectării cu platformele UNBR și ale barourilor**

Digitalizarea sistemului judiciar și integrarea acestuia cu platformele UNBR și ale barourilor reprezintă o prioritate pentru eficiență și accesibilitate. Noul sistem ECRIS V, care este în prezent în faza finală de dezvoltare și implementare, va oferi instrumente foarte utile în combaterea fenomenului avocaturii ilegale, ca urmare a interconectării cu sistemele informatice ale Uniunii Naționale a Barourilor din România. Integrarea ECRIS 5 cu sistemele barourilor va reduce birocrăția și va permite accesul rapid la dosare. Avocații vor avea acces privilegiat la informații judiciare, facilitând relația profesională cu instanțele și reducând timpul pierdut în gestionarea dosarelor. Crearea unor politici eficiente care să protejeze avocații autorizați și să limiteze avocatura ilegală.

- **Protecția confidențialității datelor și educația continuă în domeniul tehnologic sunt fundamentale pentru consolidarea profesiei în era digitală**

Orice breșă de securitate poate afecta încrederea și credibilitatea profesiei, iar „ilegalii” vor profita pentru a-și face loc. S-a subliniat utilitatea implementării unor soluții de securitate avansate, precum criptarea informațiilor și autentificarea cu doi factori (2FA)

Organizarea de programe de formare continuă pentru avocați în domeniul securității cibernetice, pentru a preveni vulnerabilitățile la atacuri informatice.

- **Colaborarea interinstituțională**

Consolidarea cooperării dintre UNBR, instanțele de judecată și alte autorități, precum DNSC și ANCOM, pentru dezvoltarea unor soluții integrate.

**Concluzie:**

Combaterea avocaturii ilegale în era digitală necesită o abordare complexă, bazată pe inovație tehnologică, colaborare interinstituțională și educație continuă. Prin măsuri integrate și strategii proactive, avocații autorizați pot reafirma profesionalismul și credibilitatea în mediul online.



## PANEL 2:

### *Peisajul actual al amenințărilor cibernetice și protecția avocaților în mediul digital*

#### EXTRAS VIDEO AICI

**Moderator:** Cătălin Filișan, Membru al Comisiei Permanente a UNBR

Participanți la dezbatere: Dan Cîmpean, Director General DNSC, Găgiu Petre Adrian, Reprezentant ANCOM, Deniss Bogdan Onofrei Riza, Șef al Laboratorului Forensic al ICI București; Bogdan Grosu, Consilier UNBR

În cadrul conferinței, au fost subliniate mai multe avertismente legate de faptul că avocații sunt din ce în ce mai vizați de atacuri informatice, din cauza naturii sensibile a informațiilor financiare, comerciale sau juridice pe care le gestionează. Aceste informații pot fi extrem de valoroase pentru atacatori și pot fi vândute, utilizate în scopuri de șantaj sau exploatare pentru a obține avantaje în conflicte juridice sau comerciale.

Firmele mai mici și avocații independenți sunt considerați ținte mai ușoare, deoarece de obicei nu investesc în securitate cibernetică avansată. Majoritatea avocaților nu sunt suficient de pregătiți în ceea ce privește riscurile cibernetice, ceea ce îi face mai vulnerabili la atacuri. Orice atac asupra confidențialității datelor afectează direct reputația avocatului și încrederea clienților.

**Experții participanți la conferință au avertizat asupra tipurilor de atacuri informatice care pot viza avocații, au explicat „simptomele” acestor atacuri, pentru a le putea recunoaște:**

- **Ransomware**

Este cel mai frecvent și periculos tip de atac. Atacatorii criptează fișierele și solicită o răscumpărare (de obicei în criptomonede) pentru a debloca datele. Acest tip de atac paralizează activitatea profesională și poate duce la pierderi semnificative de date și bani;

- **Phishing**

Emailuri frauduloase care pretind că sunt de la clienți, colegi sau instituții oficiale. Prin acestea, atacatorii încearcă să obțină date de autentificare sau informații sensibile. Acest tip de atac se bazează pe manipulare psihologică (social engineering) pentru a convinge avocatul să divulge informații sau să acceseze linkuri malițioase;



- **Atacuri asupra infrastructurii IT**

Exploatarea vulnerabilităților din software-urile utilizate de avocați (ex. sisteme de gestiune a dosarelor, emailuri sau platforme de colaborare online). Atacurile pot include instalarea de malware pentru spionarea activităților sau extragerea datelor;

- **Atacuri asupra rețelelor Wi-Fi nesigure**

Avocații care folosesc rețele Wi-Fi publice fără protecție adecvată pot fi ținte ușoare pentru interceptarea comunicațiilor.

***Recomandări discutate în conferință pentru a combate aceste atacuri:***

- **Creșterea nivelului de conștientizare și educație digitală**

Participarea la programe de formare și workshop-uri organizate de instituții specializate, cum ar fi Directoratul Național de Securitate Cibernetică (DNSC).

Crearea unor ghiduri de bune practici în securitatea cibernetică, adaptate specific profesiei de avocat.

- **Investiții în soluții de securitate cibernetică**

Implementarea soluțiilor de securitate, cum ar fi antivirusuri avansate, firewall-uri și sisteme de detectare a intruziunilor (IDS).

Utilizarea criptării pentru protecția documentelor și a corespondenței sensibile.

Implementarea autentificării cu doi factori (2FA) pentru toate conturile profesionale.

- **Protecția datelor și backup regulat**

Crearea de copii de siguranță (backup) periodice ale datelor, stocate în medii securizate.

Adoptarea unor politici stricte de confidențialitate pentru gestionarea datelor clienților.

- **Colaborarea cu instituțiile statului**

Colaborarea cu DNSC și alte autorități relevante pentru a raporta și investiga incidentele ciberneticе.

Încheierea de parteneriate cu instituții care oferă sprijin în securitate cibernetică.

- **Adoptarea unor proceduri interne stricte**

Introducerea unor politici clare de acces la date și resurse IT, limitând accesul doar la personal autorizat.

Organizarea unor audituri periodice de securitate pentru a identifica și remedia vulnerabilitățile.

- **Utilizarea platformelor sigure pentru comunicare**

Evitarea utilizării rețelelor publice de Wi-Fi fără protecție adecvată.

Folosirea unor platforme sigure pentru comunicarea cu clienții, cum ar fi cele care asigură criptarea end-to-end.

- **Pregătirea pentru situații de criză**

Crearea unui plan de răspuns la incidente (Incident Response Plan) pentru a gestiona rapid și eficient atacurile ciberneticе.

Organizarea de simulări pentru pregătirea personalului în cazul unui atac.

- **Validarea și monitorizarea aplicațiilor și site-urilor utilizate**

◇ Folosirea doar a aplicațiilor și software-urilor verificate pentru gestionarea dosarelor și comunicare.

◇ Monitorizarea constantă a activităților online pentru a detecta comportamente suspecte.

**Concluzie:**

Avocații sunt vizați de atacuri ciberneticе din cauza valorii informațiilor pe care le dețin, iar prevenirea acestor atacuri necesită atât măsuri tehnice, cât și o schimbare de mentalitate. Protecția datelor și securitatea digitală trebuie să devină priorități pentru profesia de avocat. Creșterea nivelului de educație în securitatea cibernetică este vitală pentru a preveni pierderile de date și atacurile asupra profesiei.

## PANEL 3:

### *Soluții IT și tehnologii pentru protejarea activităților avocatului*

#### EXTRAS VIDEO AICI

**Moderator:** Sergiu Capisizu, Consilier UNBR

Participanți la dezbatere: Dna Camelia Ivan, Expert în Digitalizare și Cybersecurity; Camelia Săvoiu, Reprezentant al Fondul Roman de Contragarantare; Jud. Claudiu Dragusin, Membru CSM; judecător Cosmin Sterea Grossu, Șef al Serviciului Informatică și Statistică Judiciară CSM; Tudor Colțan, avocat Baroul București

Principalele aspecte abordate în cadrul dezbaterilor se referă la necesitatea securizării infrastructurii IT a unui cabinet de avocatură (soluții de protecție, criptare, backup-uri) precum și implementarea soluțiilor de securitate pentru gestionarea corespondenței electronice și documentelor sensibile.

Educația digitală a avocaților este esențială în zilele noastre pentru a face față provocărilor din mediul online. Altfel, avocații pot fi expuși unor riscuri reputaționale (cauzate de incidente cibernetice, a furtului de identitate și utilizarea frauduloasă a identității avocatului de către alte persoane sau pur și simplu din cauza amprente digitale pe care o lasă în mediul online). De asemenea, utilizarea eronată a AI în avocatură poate compromite profesionalismul și integritatea deciziilor.

**În cadrul dezbaterilor au rezultat mai multe propuneri de soluții pentru protejarea activității avocatului:**

- **Crearea unei „liste de încredere” pentru avocați, similară cu cea pentru furnizorii de servicii de încredere (trust services)**
  - ◊ Această listă ar putea avea un dublu rol: pe de o parte, protejează publicul împotriva avocaturii ilegale, iar pe de altă parte, oferă avocaților autorizați un instrument pentru a-și consolida prezența și credibilitatea în mediul online.
  - ◊ Avocații din această listă ar putea beneficia de un statut special în ecosistemele digitale, precum motoarele de căutare (Google, Facebook) sau platformele judiciare, pentru a fi afișați prioritar ca profesioniști autorizați.





- **Digitalizare și automatizare:**

- ◊ Implementarea unui sistem ECRIS V cu identificare unică a avocaților și integrarea semnăturilor electronice calificate.
- ◊ Dezvoltarea unui dosar electronic național compatibil cu cerințele legislative actuale.

- **Educație și formare continuă:**

- ◊ Integrarea unor module obligatorii despre digitalizare și securitate cibernetică în formarea avocaților stagiați
- ◊ Organizarea de conferințe și sesiuni de instruire pentru formarea continuă a avocaților
- ◊ Crearea unui chatbot pentru informații juridice de bază, conectat la aplicația „CautAvocat”.

- **Gestionarea reputației:**

- ◊ Promovarea unui comportament online etic și profesional
- ◊ Crearea de strategii pentru monitorizarea și recuperarea reputației după incidente online.

- **Adaptare la evoluția AI:**

- ◊ Adoptarea AI în avocatură pentru eficiență, dar cu utilizare controlată și verificată.
- ◊ Dezvoltarea unor standarde și reglementări clare privind utilizarea AI în domeniul juridic.

### **Concluzii:**

Digitalizarea avocaturii este inevitabilă și necesară pentru a răspunde cerințelor actuale ale justiției și ale clienților. Este esențială colaborarea dintre instituțiile juridice, barouri și experți pentru a implementa soluții tehnologice sigure și eficiente.

Protecția datelor și reputației este crucială, iar avocații trebuie să își asume un rol activ în adoptarea de măsuri preventive și corective. Soluțiile tehnologice trebuie integrate în mod eficient pentru a sprijini

