

Analiză — Legea codului sursă deschis

Analiză — Legea privind codul sursă deschis și reutilizarea în sectorul public

Comentarii în limbaj clar. Referințe verificate.

1. Pe scurt: ce face legea și ce impresie lasă

Propunerea este bună ca intenție și bine structurată. Ideea de bază, „bani publici, cod public” (*public money, public code*), este corectă și modernă. Legea impune trei lucruri esențiale:

1. **Publicarea codului sursă** plătit din bani publici, într-un depozit național (DNCP).
2. **Reutilizarea cu prioritate** a soluțiilor existente, printr-un catalog național.
3. **Prevenirea captivității față de furnizori** (vendor lock-in), prin clauze contractuale obligatorii de predare a codului, documentației și a artefactelor de build.

Structura pe capitole este logică și acoperă lanțul complet: definiții, guvernanta, publicare, reutilizare, contribuții externe, monitorizare, sancțiuni. Este comparabilă ca ambiție cu legile din Italia și Bulgaria.

Problema principală **nu** este viziunea, ci **executabilitatea**. Prea multe elemente critice sunt împinse către „normele metodologice”, iar câteva mecanisme cheie (termene, verificarea reală a codului, sancționarea persoanelor, nu doar a instituțiilor) sunt slabe sau lipsesc. Așa cum e scrisă acum, legea riscă să producă „conformare pe hârtie”: cod aruncat într-un depozit, nefuncțional și neîntreținut.

2. Puncte tari

- **Principiul publicării ca regulă** (art. 3 lit. a), cu excepții limitate și revizuite anual (art. 14). Este abordarea corectă.
 - **Reutilizarea obligatorie cu verificare prealabilă** înainte de achiziție (art. 16) și sancțiune pentru nerespectare (art. 27). Puține legi merg atât de departe.
 - **Predarea completă** (art. 19): nu doar codul, ci și instrucțiunile de build, artefactele, documentația, testele. Aceasta este diferența dintre un cod folosibil și unul mort.
 - **Clauzele contractuale abuzive considerate nescrise** (art. 17 alin. 3). Foarte puternic juridic: neutralizează încercările furnizorilor de a bloca drepturile statului.
 - **Recepția condiționată** de predare (art. 19 alin. 2). Leagă banii de conformare, singurul lucru care contează cu adevărat pentru furnizori.
 - **Lista componentelor software (SBOM)** și evidența licențelor (art. 2 lit. g, art. 19 lit. f, art. 25). Aliniat cu bunele practici de securitate din UE.
 - **Excluderea explicită a secretelor** din publicare (art. 11 alin. 4): parole, chei, certificate, date personale. Corect și necesar.
-

3. Probleme identificate

3.1. Probleme de fond (structurale)

P1. Totul depinde de normele metodologice. Expresia „potrivit normelor metodologice” apare de zeci de ori. Elemente esențiale rămân nedefinite în lege: lista licențelor acceptate, ce înseamnă „soluție reutilizabilă adecvată”, ce este un „sistem digital critic”, cum se face verificarea tehnică a codului predat. Riscul: dacă normele întârzie sau sunt slabe, legea devine literă moartă. Termenul de 90 de zile (art. 28) este nerealist pentru volumul de detaliu necesar.

P2. Se sancționează instituția, nu persoana. Toate amenzile din art. 27 lovesc „entitatea publică”. În practică asta înseamnă că banii se mută dintr-un buzunar public în altul, iar funcționarul responsabil nu simte nimic. Nu există răspundere personală clară pentru responsabilul desemnat la art. 10. Comparativ, mecanismele care funcționează leagă răspunderea de persoana decidentă.

P3. „Publicat” nu înseamnă „funcțional”. Legea cere publicarea codului, dar nu impune ca el să fie compilabil/rulabil de un terț. Un furnizor poate publica un cod incomplet, fără istoric real, obfuscat sau fără dependențe, și să bifeze formal obligația. Art. 19 cere artefactele de build, dar nu există o probă de reproductibilitate („build-ul se reface din sursa publicată”).

P4. Momentul publicării este prea târziu și necontrolat pe parcurs. Publicarea „cel târziu la data recepției finale” (art. 11 alin. 3) înseamnă că, pe toată durata dezvoltării (adesea ani), codul rămâne închis. Bulgaria a ales dezvoltarea *în public de la început*, într-un depozit public. Publicarea la final permite predarea unui „bloc” unic, greu de auditat și de reutilizat.

P5. Fără buget și fără resurse umane dedicate. Oficiul se înființează „în limita numărului maxim de posturi aprobat” pentru ADR (art. 4 alin. 1), adică fără posturi noi. A administra un depozit național de cod, un catalog, verificări de securitate, revizuirii anuale de excepții și un raport anual, fără oameni și fără buget dedicat, este nerealist. Este cel mai frecvent mod în care astfel de legi eșuează în România.

P6. Excepțiile pot deveni regula. Art. 14 permite excepții prelungibile anual „pentru cel mult 12 luni” de fiecare dată, dar fără o limită totală a numărului de prelungiri. O excepție se poate reînnoi la nesfârșit. Nu există prag/plafon după care exceptarea nu mai poate fi prelungită și nici obligația de a publica un plan de remediere.

P7. Aplicare doar pentru proiecte noi. Art. 29 aplică obligațiile doar procedurilor și proiectelor *inițiate după* intrarea în vigoare. Tot stocul existent de software public (adesea cel mai captiv față de furnizori) rămâne complet în afara legii. Nu există nicio obligație, nici măcar graduală, pentru sistemele în derulare la reînnoirea sau modificarea contractelor.

P14. Verificare concentrată la ADR, fără control extern. ADR operează DNCP, aprobă excepțiile, monitorizează, constată și sancționează, și dezvoltă la rândul ei software. Ajunge să își verifice propria conformare (cauză proprie), fără control extern independent și fără rol pentru Curtea de Conturi. A fost adăugat art. 26¹: control al Curții de Conturi plus structură independentă pentru soluțiile ADR.

P15. Lipsa unui mecanism de semnalare. Legea nu prevede cum poate cineva sesiza o încălcare (cod nepublicat, secrete scurse, excepție falsă) și nici un canal de raportare a vulnerabilităților de securitate în codul public. Fără sesizare, protecția avertizorilor și divulgare coordonată a

vulnerabilităților, verificarea depinde exclusiv de resursele ADR. A fost adăugat art. 26² (sesizări, Legea nr. 361/2022) și art. 25 alin. (3)-(4) (CVD cu DNSC).

P16. Automatizare neexploatăată. Legea e construită din elemente verificabile automat (DNCP, SBOM standard, catalog, listă de licențe), dar nu prevede controale automate. Verificarea manuală nu scadează la mii de proiecte. A fost adăugat art. 5 alin. (7)-(8) (porți automate la publicare) și art. 16 alin. (3) (verificarea reutilizării prin integrare cu SEAP).

3.2. Probleme juridice și de tehnică legislativă

P8. Domeniu de aplicare incomplet la art. 1 vs. art. 2. Art. 1 alin. (2) definește entitățile prin „furnizarea unui serviciu public digital”. Multe soluții publice (ex. sisteme interne de management, unelte de analiză, software administrativ) nu furnizează direct un „serviciu public digital” către cetățean, dar sunt plătite din bani publici. Riscă să scape.

P9. Numerotare greșită a capitolelor. Există două capitole „VII” (Contravenții și Dispoziții finale). Dispozițiile finale ar trebui să fie Capitolul VIII. Eroare de redactare, dar trebuie corectată înainte de adoptare.

P10. Relația cu legislația privind proprietatea intelectuală și achizițiile nu este pe deplin articulată. Legea invocă OUG 41/2016 (achiziții), dar nu clarifică raportul cu Legea nr. 8/1996 privind dreptul de autor (cine deține codul dezvoltat de angajați vs. contractori), nici cu Legea nr. 98/2016 privind achizițiile publice. Cine deține drepturile patrimoniale de autor asupra codului dezvoltat intern nu este stabilit explicit.

P11. „Considerate nescrise” (art. 17 alin. 3) poate intra în tensiune cu contracte deja semnate. Formularea e bună pentru contracte viitoare, dar aplicarea la contracte în derulare ar ridica probleme de neretroactivitate (art. 15 din Constituție). Art. 29 pare să rezolve prin limitare la proiecte noi, dar relația nu e explicită.

P12. GDPR și open data — trimiteri insuficiente. Se menționează protecția datelor ca principiu, dar nu există trimitere la Regulamentul (UE) 2016/679 (GDPR) și nici la Directiva (UE) 2019/1024 privind datele deschise. Dicționarul de date (art. 22) și publicarea ar trebui ancorate explicit în aceste cadre.

P13. Alinierea la Interoperable Europe Act lipsește ca referință directă. Art. 4 lit. g și art. 5 alin. 2 vorbesc de cooperare și platforme europene, dar nu citează Regulamentul (UE) 2024/903 (Interoperable Europe Act), care este direct aplicabil și impune deja partajarea soluțiilor de interoperabilitate, inclusiv cod sursă. Legea română ar trebui să se conecteze explicit la acest cadru și la Portalul Interoperable Europe.

3.3. Probleme tehnice (din perspectivă software/SaaS)

T1. Lipsa reproductibilității build-ului. Vezi P3. Fără o cerință de „build reproductibil” și de verificare automată, predarea codului nu garantează că poți reconstrui aplicația.

T2. Nu se tratează dependențele SaaS și serviciile cloud gestionate. Multe soluții moderne nu sunt „cod” livrat, ci servicii SaaS. Legea vizează codul la comandă, dar nu clarifică ce se întâmplă când statul cumpără un abonament SaaS cu configurări la comandă. Portabilitatea datelor (art. 18) atinge subiectul, dar insuficient.

T3. Mentenanța codului publicat nu are model de finanțare. Codul publicat trebuie întreținut (vulnerabilități, actualizări). Art. 9 cere „plan minimal de mentenanță”, dar nu spune cine plătește și din ce buget. Cod publicat și neîntreținut devine un risc de securitate, nu un beneficiu.

T4. Securitatea prin obscuritate nu e interzisă explicit ca justificare. Art. 14 lit. b (expunerea de „elemente operaționale critice de securitate”) poate fi folosit abuziv ca „nu publicăm pentru că e nesigur să arătăm codul”. Principiul corect este invers (Kerckhoffs): securitatea nu trebuie să depindă de secretul codului, ci al cheilor. Ar trebui spus explicit.

T5. Contribuțiile externe fără CLA/DCO clar. Art. 23-24 pomenesc „clarificarea drepturilor asupra contribuțiilor”, dar lasă totul în norme. Fără un mecanism clar (Contributor License Agreement sau Developer Certificate of Origin), integrarea contribuțiilor externe creează risc juridic asupra proprietății codului.

T6. Doar codul și operarea, nu și cunoașterea de dezvoltare. Legea acoperă codul, documentația operațională, artefactele de build, testele, interfețele și dicționarul de date, dar nu cere predarea și publicarea artefactelor din amonte: analiza de cerințe, specificațiile funcționale și tehnice, arhitectura, deciziile de proiectare, regulile de business și logica decizională. Codul spune *ce face*, nu *de ce*; fără aceste artefacte, reutilizarea (art. 15-16) rămâne teoretică, iar auditul de conformitate este dificil. În plus, pentru soluțiile care iau ori susțin decizii despre cetățeni, lipsa o obligație de transparență a logicii decizionale, aliniată cu abordarea franceză (Legea nr. 2016-1321), cu art. 22 GDPR și cu Regulamentul (UE) 2024/1689 (AI Act). A fost adăugat art. 21¹ și extinse art. 2, 11, 19.

T7. Inteligența artificială tratată ca simplu „cod”. Cea mai mare zonă oarbă. Legea presupune implicit că soluția = cod sursă. La sistemele AI, codul este partea mică; comportamentul e dat de modelul antrenat (greutăți), datele de antrenare, pipeline-ul și hiperparametrii. Publicarea „codului” unui sistem AI produce transparență falsă. În plus: (a) reproductibilitatea de la art. 11¹ este imposibilă fără greutate plus date plus configurație; (b) dependența de modele de bază externe (LLM-uri prin API) este o formă acută de captivitate și un risc de suveranitate, cu model drift care schimbă deciziile fără schimbare de cod; (c) „logica decizională” a unui model e o cutie neagră, deci transparența cere fișe de model, nu publicarea regulilor; (d) datele de antrenare ridică probleme de GDPR și de proprietate intelectuală. A fost adăugat Capitolul V¹ (art. 25¹ - 25⁵), corelat cu Regulamentul (UE) 2024/1689 (AI Act), fără a-l dubla.

4. Comparație cu legi și cadre similare

Toate referințele de mai jos au fost verificate.

4.1. Bulgaria — Legea guvernării electronice (amendamente 2016)

Bulgaria a modificat *Electronic Governance Act* în 2016 (în vigoare din 1 iulie 2016): tot software-ul nou scris **pentru** guvern trebuie să fie open source și **dezvoltat într-un depozit public de la început**, administrat de agenția de e-guvernare. Agențiile de securitate și informații sunt exceptate.

- **Ce face mai bine ca propunerea RO:** dezvoltarea în public de la început (nu doar la recepția finală). Vezi P4.
- **Similar:** depozit național, excepții pentru securitate națională.

- Surse: [TechCrunch](#), [Global Government Forum](#).

4.2. Italia — Codice dell'Amministrazione Digitale (CAD), art. 68-69

Când o administrație publică italiană dezvoltă sau comandă software, are obligația (art. 69 CAD) să îl publice într-un depozit public sub licență deschisă, pentru reutilizare de către alte administrații. Titularul drepturilor pe codul sursă trebuie să fie administrația (art. 69 alin. 2). Platforma este *Developers Italia*, iar linii directoare detaliate impun standarde de lizibilitate, documentare și înregistrare.

- **Ce face mai bine ca propunerea RO:** modelul „reuse-first” este operaționalizat printr-un catalog și ghiduri tehnice mature; obligația de titularitate a drepturilor e explicit în lege (rezolvă P10).
- **Similar:** catalog de reutilizare, licențe deschise, depozit național.
- Surse: [Developers Italia — publication](#), [Linii directoare achiziție și reutilizare](#).

4.3. Franța — Loi pour une République numérique (Legea nr. 2016-1321)

Codul sursă produs de administrații este un **document administrativ comunicabil** (deci accesibil publicului la cerere și reutilizabil), codificând jurisprudența CADA. Un decret stabilește lista licențelor deschise aplicabile. Refuzul e posibil dacă publicarea riscă securitatea sistemelor informatice.

- **Ce e diferit:** modelul francez este „acces la cerere + open source implicit”, nu neapărat publicare proactivă totală. Propunerea RO merge mai departe (publicare ca regulă).
- **De împrumutat:** lista licențelor stabilită prin act normativ clar; abordarea „code.gouv.fr”.
- Surse: [Légifrance — LOI n° 2016-1321](#), [Wikipedia — Loi pour une République numérique](#).

4.4. UE — Interoperable Europe Act, Regulamentul (UE) 2024/903

În vigoare din 11 aprilie 2024. Impune un nivel ridicat de interoperabilitate a sectorului public, partajarea soluțiilor de interoperabilitate (inclusiv **cod sursă și documentație**) între entități publice, cu prioritate pentru soluții fără licențe restrictive, și un Portal Interoperable Europe. Nu obligă la renunțarea la drepturile de proprietate intelectuală.

- **Relevanță directă:** este drept UE aplicabil României. Propunerea RO ar trebui să se ancoreze explicit în el (vezi P13) și să conecteze DNCP la Portalul european.
- Surse: [Regulamentul \(UE\) 2024/903 — EUR-Lex](#), [Interoperable Europe Portal](#).

4.5. UE — Directiva (UE) 2019/1024 privind datele deschise

Cadrul pentru reutilizarea informațiilor din sectorul public. Relevantă pentru dicționarul de date (art. 22) și pentru principiul reutilizării. Ar trebui citată.

4.6. Germania — Public Money Public Code / OpenCoDE / ZenDiS

Germania nu are (încă) o lege federală unică echivalentă, dar a construit **infrastructura**: platforma [OpenCoDE](#) și Centrul pentru Suveranitate Digitală ([ZenDiS](#)). Lecția: **infrastructura și guvernanta finanțată contează mai mult decât textul legii**. Întărește P5.

4.7. SUA – Federal Source Code Policy (M-16-21) și code.gov

Politică federală din 2016: cod personalizat reutilizabil între agenții, cu un pilot de minim 20% cod publicat open source, prin portalul code.gov. Model de indicatori și țintă cantitativă. Propunerea RO are indicatori (art. 26) dar **nu are ținte** cantitative.

4.8. Campania FSFE „Public Money, Public Code”

Cadrul conceptual pe care se sprijină întreaga propunere. Util de citat în expunerea de motive.

5. Analiza loopholes (portite de evitare)

Modul în care o entitate sau un furnizor de rea-credință ar putea eluda legea, așa cum e scrisă acum:

L1. „Serviciu public digital” ca filtru de scăpare. (art. 1 alin. 2) O instituție poate susține că un sistem intern „nu furnizează un serviciu public digital” și deci iese din domeniul legii. → *Închide P8.*

L2. Fragmentarea achizițiilor sub praguri. Împărțind un proiect mare în multe contracte mici de „mentenanță” sau „servicii”, o instituție poate evita clasificarea ca „dezvoltare software la comandă” și obligațiile art. 17-19.

L3. Abuzul de excepții reînnoibile. (art. 14 alin. 2) Excepția „de cel mult 12 luni” se poate reînnoi indefinit. Fără plafon total, o instituție poate ține codul închis permanent, an de an. → *Necesită limită dură.*

L4. Publicare formală, dar inutilizabilă. (art. 11) Se publică un cod incomplet, fără istoric real (un singur commit), fără dependențe sau fără instrucțiuni de build funcționale. Formal „publicat”, practic mort. Sancțiunea de la art. 27 lit. d vizează „nepublicarea”, nu „publicarea de mântuială”. → *Necesită criteriile de completitudine și verificare.*

L5. „Standard comercial” deghizat. (art. 1 alin. 3) Un furnizor structurează o dezvoltare la comandă ca „licențiere de produs standard cu configurare”, pentru a beneficia de excepția pentru software comercial standard. Granița dintre „configurare” și „dezvoltare la comandă” nu e definită.

L6. Predare parțială acceptată la recepție. (art. 13) „Publicarea integrală nu este posibilă” este o formulare vagă care poate fi invocată de rutină pentru a publica doar interfețe și metadata, nu codul real.

L7. Amendă mai mică decât costul conformării. Amenzile (5.000-100.000 lei) sunt mici față de valoarea unui contract IT public (adesea milioane de lei) și, oricum, se plătesc din bani publici (P2). Pentru un furnizor, poate fi mai ieftin să nu se conformeze. → *Sancțiunea reală trebuie legată de contract (ex. blocarea plății, rezilierea, penalități contractuale), nu doar contravenție.*

L8. Neutilizarea „justificată motivat”. (art. 16 alin. 2) Obligația de reutilizare are portita „justificată motivat neutilizarea”. Fără criterii stricte și fără validare independentă, orice instituție poate scrie o justificare formală ca să dezvolte de la zero cu furnizorul preferat.

L9. Contribuții externe ca vector de captură. (art. 23-24) Fără CLA/DCO și fără reguli anti-conflict de interese ferme, un furnizor își poate „dona” componente proprietare parțiale în codul public pentru a-și consolida poziția și a crea dependență.

L10. „Inițiate după intrarea în vigoare”. (art. 29) Proiectele mari se pot „iniția” formal cu o zi înainte de intrarea în vigoare pentru a scăpa de obligații pe toată durata lor (adesea 4-7 ani).

L11. Fără termen pentru publicarea excepțiilor. Nu există obligația ca lista excepțiilor active și motivarea lor să fie publică în timp real; apare doar agregat în raportul anual (art. 26 lit. b). O excepție poate trece neobservată un an întreg.

L12. Nucleu proprietar cu module „open” de suprafață. (art. 1 alin. 3, art. 12 alin. 3, art. 14 lit. c) Furnizorul dezvoltă la comandă doar module ori extensii care se conectează la un „core” proprietar al său. Modulele se publică formal, dar nucleul rămâne închis (exceptat ca drept al terților). Fără o obligație de menținere a compatibilității interfeței pe o durată determinată, furnizorul poate schimba oricând API-ul nucleului, făcând modulele publicate inutilizabile. Rezultatul: obligația de publicare e bifată, dar captivitatea față de furnizor rămâne intactă. Este o variantă mai subtilă a L4. Nici textul inițial, nici cel consolidat inițial nu impuneau menținerea compatibilității; a fost adăugat art. 20² pentru a închide porțița. Legat de aceasta: lipsa și o „durată anticipată de viață” a soluției, care să ancoreze în timp obligațiile de mentenanță și compatibilitate (adăugat art. 20¹).

6. Concluzie

Propunerea este una dintre cele mai bine gândite inițiative de digitalizare din ultimii ani și merită susținută. Dar, în forma actuală, are trei vulnerabilități care îi pot anula efectul:

1. **Delegare excesivă către norme** — legea trebuie să fixeze ea însăși elementele critice (licențe, praguri, definiții).
2. **Sanțiuni și răspundere slabe** — fără răspundere personală și fără consecințe contractuale reale, conformarea rămâne formală.
3. **Fără resurse și fără infrastructură finanțată** — un Oficiu fără posturi și fără buget nu poate opera un depozit național.

Soluțiile concrete sunt prezentate în documentul de îmbunătățiri.