## 1. Introducere

Integritatea profesională în domeniul IT reprezintă angajamentul dezvoltatorilor de a acționa în mod etic, responsabil și aliniat la standardele de calitate. În contextul profesiei de **inginer web**, integritatea se manifestă prin respectarea interesului public, onestitate față de client și angajator, precum și prin menținerea calității și securității produselor software livrate[agir.ro](https://www.agir.ro/codetica.php#:~:text=Codul%20de%20etica%20a%20inginerului,al%20productiei%20si%20%C3%AEn%20societate)[ethics.acm.org](https://ethics.acm.org/code-of-ethics/software-engineering-code/#:~:text=1,consistently%20with%20the%20public%20interest). Obiectivul prezentei lucrări este de a realiza o investigație academică detaliată asupra integrității în profesia de inginer web, specific pentru România. Lucrarea își propune (a) să definească rolurile și așteptările etice asociate inginerilor web, (b) să identifice cerințele cheie de integritate (de la integritatea datelor la conformitatea legală), (c) să construiască un indicator cantitativ pentru evaluarea integrității profesionale și (d) să propună strategii de îmbunătățire a acesteia.

Metodologia cercetării s-a bazat pe revizuirea literaturii de specialitate – incluzând coduri de etică recunoscute (cum ar fi Codul etic al Asociației Generale a Inginerilor din România și Software Engineering Code of Ethics al ACM/IEEE-CS), studii din jurnale și conferințe de profil despre etica în ingineria software, precum și pe analizarea unor date reale din industrie pentru validarea indicatorului propus. Pentru citarea surselor, a fost utilizat stilul bibliografic **IEEE**, cu referințe numerotate în text și listate în bibliografie.

Fiecare capitol al lucrării corespunde unui obiectiv specific. În capitolul Profesia de inginer web se delimitează aria de activitate a inginerului web, evidențiindu-se competențele necesare și responsabilitățile tipice, dar și normele de conduită așteptate de la un profesionist în domeniu. Capitolul Cerințe de integritate în profesia de inginer web tratează aspecte precum integritatea datelor (corectitudinea și securitatea informației), practicile etice de programare (păstrarea calității codului, evitarea plagiatului, transparența față de utilizatori) și conformitatea cu reglementările legale relevante – în special Regulamentul General privind Protecția Datelor (GDPR) aplicabil și în România. În capitolul Măsurarea nivelului integrității este elaborat un **indicator compozit** care agregă mai mulți factori măsurabili ai integrității profesionale (respectarea standardelor de codificare, frecvența revizuirii codului și promptitudinea răspunsului la incidente). Se oferă formula analitică a acestui indicator și se demonstrează proprietățile sale (indicatorul este sensibil la variațiile oricărui factor, nu permite compensarea totală a unui factor slab prin alții puternici[bluefoxr.github.io](https://bluefoxr.github.io/COINrDoc/aggregation.html#:~:text=The%20geometric%20mean%20is%20less,severe%20restrictions%20on%20personal%20freedoms) și variază gradual fără efecte de catastrofă la modificări mici ale intrărilor). De asemenea, indicatorul este aplicat pe un set de date reale din industria românească de dezvoltare software, pentru a-i ilustra relevanța practică. Capitolul Căi de creștere a nivelului de integritate formulează recomandări concrete pentru profesioniștii și organizațiile din România: de la măsuri educaționale (training continuu, includerea eticii în curricula de formare), la politici organizaționale (coduri interne de conduită, mecanisme de asigurare a calității) și până la cultivarea unei culturi a responsabilității individuale și de echipă. În final, capitolul Concluzii sintetizează concluziile cheie ale investigației și discută implicațiile acestora – evidențiind importanța integrității pentru credibilitatea și sustenabilitatea pe termen lung a profesiei de inginer web. De asemenea, sunt propuse direcții viitoare de cercetare, precum extinderea setului de factori de integritate sau realizarea unor studii cantitative la nivel național privind etica și integritatea în sectorul IT.

Prin abordarea acestor aspecte, lucrarea de față contribuie la înțelegerea și îmbunătățirea integrității profesionale în domeniul dezvoltării web din România. Rezultatele sale pot servi atât specialiștilor din industrie, cât și mediului academic, în efortul comun de a promova standarde înalte de etică și calitate în ingineria web.

## 2. Profesia de inginer web

**Roluri și responsabilități.** Inginerul web (adesea echivalent cu dezvoltatorul web full-stack sau specializat pe front-end/back-end) este profesionistul IT responsabil cu proiectarea, dezvoltarea, testarea și mentenanța aplicațiilor web. Această profesie îmbină cunoștințe de programare (în limbaje precum JavaScript, Python, PHP etc.), tehnologii web (HTML/CSS, baze de date, framework-uri) și practici de inginerie software. În exercitarea rolului său, un inginer web trebuie să asigure că site-urile și aplicațiile livrate sunt funcționale, eficiente, ușor de utilizat și securizate. Responsabilitățile tipice includ: interpretarea cerințelor de la clienți și utilizatori, scrierea codului conform specificațiilor, refacerea și optimizarea codului existent, prevenirea și remedierea bug-urilor, precum și implementarea măsurilor de securitate cibernetică și protecție a datelor. De asemenea, un inginer web are adesea obligația de a colabora strâns cu designeri, manageri de proiect și alte părți interesate, asigurând coeziunea echipei și livrarea la timp a proiectelor. În România, piața IT atribuie inginerilor web un rol crucial în transformarea digitală a afacerilor, aceștia fiind implicați în dezvoltarea de soluții web de la simple pagini de prezentare până la platforme complexe de e-commerce și aplicații web de mare anvergură.

**Așteptări etice și conduită profesională.** Dincolo de îndatoririle tehnice, profesia de inginer web implică o serie de așteptări etice. Comunitatea inginerilor, atât la nivel internațional, cât și național, a formalizat principii de conduită menite să ghideze comportamentul profesional. Un exemplu fundamental este **Codul de etică al inginerului** elaborat de Asociația Generală a Inginerilor din România (AGIR). Acest cod stipulează că inginerii trebuie să-și desfășoare activitatea la cel mai înalt nivel calitativ, cu **responsabilitate și onestitate** față de firmă și client[agir.ro](https://www.agir.ro/codetica.php#:~:text=1,pentru%20cresterea%20experientei%20persoanelor%20subordonate). De asemenea, inginerul are datoria de a contribui la prestigiul profesiei prin devotament, **îmbunătățirea continuă a cunoștințelor**, mentorat pentru colegii mai tineri și **promovarea spiritului de echipă și a respectului reciproc**[agir.ro](https://www.agir.ro/codetica.php#:~:text=,de%20afirmare%20si%20modestia%2C%20care). Integritatea personală este subliniată prin cerința de a manifesta cinste și demnitate în toate acțiunile profesionale[agir.ro](https://www.agir.ro/codetica.php#:~:text=Codul%20de%20etica%20a%20inginerului,al%20productiei%20si%20%C3%AEn%20societate). Un inginer web integru nu va accepta lucrări pentru care nu are competența necesară și va refuza sarcini care nu sunt corecte din punct de vedere tehnic, economic sau legal și care ar putea prejudicia interesul public[agir.ro](https://www.agir.ro/codetica.php#:~:text=in%20rezolvarea%20problemelor%20ingineresti,pentru%20obtinerea%20de%20avantaje%20nemeritate)[agir.ro](https://www.agir.ro/codetica.php#:~:text=8,de%20proprietate%20ale%20altor%20persoane).

În mod similar, pe plan internațional, **Software Engineering Code of Ethics and Professional Practice** (elaborat de ACM/IEEE-CS) prevede că inginerii software (inclusiv cei web) **trebuie să acționeze în concordanță cu interesul public** (principiul de bază al “Public”)[ethics.acm.org](https://ethics.acm.org/code-of-ethics/software-engineering-code/#:~:text=1,consistently%20with%20the%20public%20interest). Ei au obligația să fie loiali față de client și angajator, dar numai în măsura în care aceasta nu contravine interesului public[ethics.acm.org](https://ethics.acm.org/code-of-ethics/software-engineering-code/#:~:text=1,consistently%20with%20the%20public%20interest). Principiile codului ACM/IEEE includ, între altele: acceptarea responsabilității pentru munca proprie, preocuparea pentru bunăstarea utilizatorilor și evitarea oricăror practici care ar aduce prejudicii societății sau mediului[ethics.acm.org](https://ethics.acm.org/code-of-ethics/software-engineering-code/#:~:text=Software%20engineers%20shall%20act%20consistently,software%20engineers%20shall%2C%20as%20appropriate). Aceste așteptări se traduc, practic, în comportamente precum: transparența față de client (informarea asupra riscurilor și limitărilor produsului), onestitatea în estimarea termenelor și a costurilor, precum și refuzul de a participa la proiecte cu scop dubios sau ilegal (de exemplu, dezvoltarea de malware, exploatarea neetică a datelor utilizatorilor etc.).

Profesioniștii web din România aderă tot mai mult la aceste standarde etice. Marile companii IT locale au coduri interne de conduită și pun accent pe integritate în evaluarea performanței angajaților. Revistele de specialitate promovează, la rândul lor, imaginea programatorului profesionist integru: dedicat calității, care nu face **compromisuri ce pot afecta funcționalitatea sau siguranța** aplicațiilor. Denis Salanța, în Today Software Magazine, subliniază că un programator profesionist își **asumă erorile** și se străduiește să nu introducă defecte în produsele livrate, recunoscând că imperfecțiunile sunt inevitabile dar trebuie imediat corectate[todaysoftmag.ro](https://www.todaysoftmag.ro/article/3602/codul-de-conduita-al-programatorului-profesionist#:~:text=Prejudiciem%20func%C8%9Bionalit%C4%83%C8%9Bile%20produsului%20software%20c%C3%A2nd,gre%C8%99im%20%C8%99i%20s%C4%83%20ne%20cerem). Astfel de îndrumări pun accentul pe responsabilitate și învățare din greșeli – trăsături esențiale ale integrității profesionale.

În concluzie, profesia de inginer web nu se rezumă doar la competențe tehnice, ci include și un **angajament etic**. Inginerul web este așteptat să își exercite rolul cu conștiinciozitate, să respecte confidențialitatea și interesele utilizatorilor, să comunice deschis problemele și să caute soluții care reflectă atât cerințele clientului, cât și binele public. Această combinație de expertiză tehnică și integritate etică este fundamentul încrederii de care profesia de inginer web se bucură (sau trebuie să se bucure) în societate.

## 3. Cerințe de integritate în profesia de inginer web

Integritatea în profesia de inginer web se manifestă printr-o serie de cerințe specifice, menite să asigure că produsele software dezvoltate sunt de încredere, sigure și conforme cu normele legale și etice. Dintre aceste cerințe, esențiale sunt **integritatea datelor**, **practicile etice de programare** și **conformitatea cu reglementările**.

**Integritatea datelor și securitatea informației.** Inginerii web gestionează frecvent date sensibile ale utilizatorilor (cum ar fi informații personale, financiare etc.), astfel că menținerea integrității acestor date este o obligație fundamentală. Principiul integrității datelor implică protejarea acurateței și consistenței informațiilor de-a lungul ciclului de viață al aplicației. Orice modificare neautorizată, pierdere sau corupere a datelor reprezintă o încălcare gravă a integrității. Regulamentul UE 679/2016 (GDPR), aplicabil și în România, stipulează explicit că datele cu caracter personal trebuie prelucrate într-un mod care să asigure **securitatea adecvată**, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, distrugerii sau deteriorării accidentale – asigurând astfel **"integritatea și confidențialitatea"** datelor[privacy-regulation.eu](https://www.privacy-regulation.eu/ro/5.htm#:~:text=libert%C4%83%C8%9Bilor%20persoanei%20vizate%20%28,integritate%20%C8%99i%20confiden%C8%9Bialitate). În practică, aceasta înseamnă că un inginer web trebuie să implementeze măsuri de securitate precum controlul accesului, criptarea datelor sensibile (atât în tranzit cât și în stocare), backup regulat și mecanisme de verificare a integrității (checksum, semnături digitale etc.). De asemenea, principiul Privacy by Design impus de GDPR cere ca aplicațiile să fie proiectate din start cu garanții pentru protecția datelor personale. Astfel, integritatea profesională cere inginerului web să anticipeze riscurile (atacuri cibernetice, erori de sistem) și să prevină compromiterea datelor.

În România, importanța integrității datelor este reflectată și de legislația penală. Codul Penal prevede sancțiuni severe pentru compromiterea intenționată a datelor informatice. De exemplu, **alterarea integrității datelor informatice** – fapta de a modifica, șterge, deteriora date ori de a restricționa accesul la ele fără drept – este infracțiune și se pedepsește cu închisoare[lege5.ro](https://lege5.ro/gratuit/gezdmnrzgi/art-362-alterarea-integritatii-datelor-informatice-codul-penal?dp=gqytsojvha4ta#:~:text=Art%20362%20Alterarea%20integrit%C4%83%C5%A3ii%20datelor,%C3%AEnchisoarea%20de%20la%20unu). Acest cadru legal subliniază că integritatea datelor nu este doar o chestiune tehnică, ci și una legală: inginerii web au responsabilitatea să prevină astfel de incidente, iar încălcarea deliberată a integrității datelor este ilegală și imorală.

**Practici etice de programare și calitatea codului.** O altă cerință de integritate ține de modul în care inginerul web își realizează efectiv munca de programare. Practicile etice de programare se referă la adoptarea unor standarde de **calitate și transparență** în scrierea codului. Acestea includ: respectarea **standardelor de codificare** convenite (naming conventions, structurarea clară a codului, documentarea adecvată a funcțiilor), evitarea “scurtăturilor” periculoase (cod “hardcoded” nesigur, dezactivarea temporară a verificărilor de erori etc.) și testarea riguroasă a funcționalităților. Un principiu cheie este **onestitatea față de propria muncă** – recunoașterea erorilor și corectarea lor promptă. Un inginer web integru nu va ascunde bug-uri sau deficiențe, ci le va semnala și remedia. Citatul “un profesionist trebuie să își asume erorile, chiar dacă acestea sunt inevitabile”[todaysoftmag.ro](https://www.todaysoftmag.ro/article/3602/codul-de-conduita-al-programatorului-profesionist#:~:text=Prejudiciem%20func%C8%9Bionalit%C4%83%C8%9Bile%20produsului%20software%20c%C3%A2nd,gre%C8%99im%20%C8%99i%20s%C4%83%20ne%20cerem) reflectă așteptarea ca dezvoltatorii să trateze defectele de software cu responsabilitate, fără a le ignora sau minimaliza.

De asemenea, integritatea cere evitarea **plagiatului** și respectarea proprietății intelectuale a codului. Atunci când reutilizează componente open-source sau cod scris de alți programatori, inginerul web trebuie să o facă cu permisiune (licențe corespunzătoare) și cu atribuire, acolo unde se impune. Practicile etice includ și **scrierea de cod fără portițe ascunse** sau funcționalități malițioase. De exemplu, introducerea intenționată de backdoor-uri sau de funcții care colectează date ale utilizatorilor fără consimțământ contravine grav integrității profesiei.

Un mecanism crucial de asigurare a calității și integrității codului este **revizia de cod (code review)**. Integritatea profesională se vede și din deschiderea la evaluarea colegială a codului produs. Prin code review, alți membri ai echipei pot verifica dacă un modul respectă standardele convenite și nu introduce probleme. Studiile indică faptul că majoritatea dezvoltatorilor recunosc revizia de cod drept cea mai importantă metodă de îmbunătățire a calității software – **peste 80% dintre programatori** consideră că code review contribuie direct la creșterea calității produselor software[businesswire.com](https://www.businesswire.com/news/home/20141124005216/en/Survey-Finds-Developers-Believe-Code-Review-Is-1-Way-to-Improve-Software-Quality#:~:text=Survey%20Finds%20Developers%20Believe%20Code,by%20the%20ability%20to). Astfel, o cerință implicită de integritate este ca inginerii web să fie dispuși să-și supună munca controlului reciproc și să revizuiască la rândul lor munca altora, într-un spirit constructiv.

**Conformitatea cu reglementările industriei.** Inginerii web operează într-un mediu reglementat, unde nerespectarea legilor poate atrage consecințe juridice serioase și pune în discuție etica profesională. Prin urmare, **integritatea profesională implică și conformitate legală**. O cerință de bază în România (ca în întreaga UE) este respectarea GDPR în toate proiectele ce prelucrează date cu caracter personal. Aceasta include: obținerea consimțământului utilizatorilor pentru colectarea datelor, stocarea lor numai pe durata necesară (principiul “limitării stocării”)[privacy-regulation.eu](https://www.privacy-regulation.eu/ro/5.htm#:~:text=%28e%29%20p%C4%83strate%20%C3%AEntr,limit%C4%83ri%20legate%20de%20stocare), asigurarea acurateții datelor (principiul “exactității”)[privacy-regulation.eu](https://www.privacy-regulation.eu/ro/5.htm#:~:text=,pot%20fi%20stocate%20pe%20perioade) și, cum s-a menționat, garantarea integrității și confidențialității lor[privacy-regulation.eu](https://www.privacy-regulation.eu/ro/5.htm#:~:text=libert%C4%83%C8%9Bilor%20persoanei%20vizate%20%28,integritate%20%C8%99i%20confiden%C8%9Bialitate). Un inginer web de integritate va ține cont, încă din faza de proiectare, de prevederile art. 25 din GDPR privind “protecția datelor începând cu momentul conceperii și în mod implicit”. Concret, acest lucru poate însemna anonimizarea datelor acolo unde e posibil, oferirea de opțiuni explicite de opt-out utilizatorilor și implementarea doar a acelor funcționalități care nu încalcă dreptul la viață privată.

Alte reglementări relevante includ **Legea 190/2018** (care detaliază aplicarea GDPR în România) și legislația privind comerțul electronic și comunicațiile electronice (de ex. Legea 506/2004 privind protecția datelor în sectorul comunicațiilor electronice). De asemenea, standardele industriale voluntare precum ISO/IEC 27001 (managementul securității informației) și ISO/IEC 27018 (protecția datelor personale în cloud) pot ghida practicile unei organizații, iar aderarea la ele reflectă un angajament față de integritate și securitate.

În ansamblu, cerințele de integritate pentru un inginer web pot fi rezumate astfel:

* **Să protejeze integritatea și siguranța datelor** utilizatorilor și ale sistemelor, prevenind accesul neautorizat și modificările ilegale sau erori grave.
* **Să respecte standardele etice de codare și testare**, livrând cod curat, bine documentat și lipsit de intenții ascunse sau practici incorecte.
* **Să recunoască și să corecteze prompt greșelile**, învățând din ele, și să faciliteze un mediu de lucru în care verificarea reciprocă (peer review) este binevenită și practicată.
* **Să se conformeze legilor și reglementărilor aplicabile**, integrând cerințele juridice (precum GDPR) în procesul de dezvoltare și evitând orice acțiune care ar pune compania sau utilizatorii în situații ilegale sau imorale.

Respectarea acestor cerințe consolidează **încrederea** în produsele web dezvoltate în România. Clienții și publicul se așteaptă ca profesioniștii IT să livreze soluții sigure și etice, iar integritatea reprezintă tocmai fundamentul acestor așteptări. În capitolele următoare, vom vedea cum putem cuantifica nivelul integrității și cum îl putem îmbunătăți în mod sistematic.

## 4. Măsurarea nivelului integrității în profesia de inginer web

Evaluarea obiectivă a integrității profesionale este o provocare, întrucât integritatea are valențe calitative și de conduită. Totuși, putem defini un **indicator cantitativ compozit** care să agregheze mai mulți factori măsurabili ce reflectă comportamentul integru al unui inginer web sau al unei echipe de dezvoltare. Scopul acestui indicator este de a oferi o metodă de **măsurare a progresului** și de comparare, în timp sau între organizații, a nivelului de integritate profesională.

**Factori esențiali influenți.** În urma analizei practicilor din industrie și a cerințelor discutate anterior, identificăm trei factori cheie ce pot fi cuantificați și care influențează direct integritatea în profesia de inginer web:

* **Respectarea standardelor de codificare și calitatea codului** – Acest factor surprinde disciplina tehnică a dezvoltatorului. Poate fi măsurat prin indicatori de calitate a codului precum densitatea defectelor (bug-uri) pe mia de linii de cod, scoruri generate de unelte de analiză statică (ex: SonarQube rule compliance), procentajul de cod acoperit de teste unitare, etc. Un nivel ridicat al calității codului, cu puține încălcări ale standardelor convenite, indică o abordare conștiincioasă și integră (dezvoltatorul **nu “ascunde mizeria sub preș”**, ci scrie cod curat și corect).
* **Frecvența și rigoarea revizuirilor de cod** – Acest factor reflectă gradul de deschidere la controlul colegial și orientarea către calitatea colectivă a produsului. Se poate cuantifica prin procentul de modificări de cod (commits/pull requests) care trec printr-un proces formal de code review, numărul mediu de review-uri per modul, sau rata de aprobare/respingere în urma reviziei. O echipă în care **100% din cod este revizuit de cel puțin un alt inginer** are o probabilitate mai mică de a introduce erori sau devieri neetice, comparativ cu o echipă unde revizuirile sunt sporadice. (În industrie, code review-ul este considerat critic pentru calitate – un sondaj arată că 80% dintre dezvoltatori îl consideră esențial[businesswire.com](https://www.businesswire.com/news/home/20141124005216/en/Survey-Finds-Developers-Believe-Code-Review-Is-1-Way-to-Improve-Software-Quality#:~:text=Survey%20Finds%20Developers%20Believe%20Code,by%20the%20ability%20to)).
* **Timpii de răspuns la incidente** – Acest factor măsoară **responsabilitatea și reacția** în fața problemelor apărute în producție (bug-uri critice, breșe de securitate, indisponibilități). Un indicator tipic este Mean Time To Repair/Recover (MTTR) – timpul mediu de la raportarea unui incident până la rezolvarea sa. De exemplu, cât de repede aplică inginerul web un patch pentru o vulnerabilitate severă odată descoperită. Un timp de răspuns scurt indică faptul că profesionistul sau echipa **își asumă problemele și le remediază prompt**, demonstrând integritate și grijă față de utilizator. În schimb, întârzieri mari pot sugera neglijență sau lipsa de proceduri (de exemplu, un raport global arată că în 2021, timpul mediu de remediere a unei vulnerabilități software a fost ~60 de zile[bit-sentinel.com](https://bit-sentinel.com/ro/cve-monitor-2/#:~:text=fa%C8%9B%C4%83%20de%202020%20,and%20Threat%20Trends%20Report%202022) – un interval considerat prea lung și riscant).

Desigur, se pot lua în calcul și alți factori (cum ar fi nivelul de **transparență față de client** – măsurat prin frecvența rapoartelor de progres sau a comunicării pro-active a problemelor; sau gradul de **conformitate legală** – de exemplu numărul de incidente de neconformitate GDPR), însă pentru simplitate ne concentrăm pe cei trei de mai sus, care acoperă triada: calitatea procesului de dezvoltare, cultura calității în echipă și responsabilitatea operațională.

**Formula indicatorului de integritate.** Vom nota cei trei factori esențiali astfel:

* a = scorul de respectare a standardelor de cod și calitate (normalizat în intervalul [0,1], unde 1 înseamnă calitate excelentă, fără deviații, și 0 înseamnă cod foarte slab calitativ).
* b = scorul pentru revizuirea codului (de exemplu proporția de cod revizuit sau un indice combinat ce reflectă rigoarea procesului de review, normalizat [0,1], 1 înseamnă tot codul este riguros revizuit, 0 înseamnă lipsa totală a revizuirii).
* c = scorul pentru timpul de răspuns la incidente (normalizat astfel încât 1 corespunde unui timp de răspuns excelent de mic – ideal, iar 0 unui timp de răspuns inacceptabil de mare; se poate normaliza liniar față de un reper, de exemplu 0 pentru >60 zile, 1 pentru <1 zi, sau folosind o funcție logistică).

Definim **Indicatorul de Integritate Profesională (IIP)** drept agregarea multiplicativă a acestor factori, după formula:

IIP=3a⋅b⋅c​.

Cu alte cuvinte, IIP este media geometrică a celor trei componente (dacă se consideră eventual factori de ponderare diferiți, formula poate fi extinsă, însă în exemplul nostru vom presupune că fiecare factor are importanță egală și indispensabilă). Astfel, indicatorul IIP va rezulta tot în intervalul [0,1] (sau poate fi exprimat procentual 0–100%). Un scor mai mare semnifică un nivel mai ridicat de integritate profesională.

Alegerea **mediilor geometrice** în locul celor aritmetice pentru un astfel de indice se bazează pe considerente teoretice solide. Media aritmetică ar permite compensarea perfectă – valori foarte mici la un factor ar putea fi compensate de valori mari la alți factori, ceea ce nu dorim în contextul integrității (o deficiență gravă la un capitol de integritate nu poate fi complet anulată de performanțe excelente la alte capitole). În schimb, **media geometrică este mai puțin compensatorie** – scorurile mici la un factor diminuează substanțial rezultatul combinat, **valorile scăzute într-un indicator fiind doar parțial compensate de valorile ridicate ale altora**[bluefoxr.github.io](https://bluefoxr.github.io/COINrDoc/aggregation.html#:~:text=The%20geometric%20mean%20is%20less,severe%20restrictions%20on%20personal%20freedoms). De exemplu, dacă a=1.0 și b=1.0 (cod de calitate impecabilă și tot codul revizuit) dar c=0.25 (timp de răspuns foarte slab), atunci IIP=30.25​≈0.63, mult sub nivelul excelent așteptat. Astfel, modelul este **necompensatoriu**: toate aspectele integrității trebuie menținute la un nivel bun pentru ca scorul final să fie bun. Totodată, formula propusă are un comportament **necatastrofic**: mici variații în factori produc variații graduale ale rezultatului (indicatorul este o funcție continuă și monotonică a fiecărei variabile). De exemplu, dacă un factor scade de la 1.0 la 0.8 (o deteriorare moderată), IIP nu va cădea brusc la o valoare extrem de mică, ci va scădea ușor. Spre deosebire de o abordare “minim” (care ar lua cel mai mic factor drept scor, penalizând brutal chiar și abaterile minore), media geometrică asigură o anumită robustețe la oscilații minore și încurajează îmbunătățirea pe toate planurile fără a anula complet rezultatele pozitive din alte arii. Faptul că indicatorul este bazat pe înmulțire înseamnă și că dacă oricare factor ajunge la 0 (de exemplu, integritatea codului este zero în cazul unui proiect eșuat complet), atunci IIP=0 – ceea ce reflectă realitatea că o lipsă totală de integritate într-un aspect critic compromite integritatea per ansamblu.

**Proprietățile indicatorului:** Sintetizând cele de mai sus, indicatorul propus IIP este:

* **Sensibil** – o îmbunătățire sau degradare în oricare din cei trei factori a,b,c se va reflecta în scorul final. Astfel, echipele pot observa efectul pozitiv al unor măsuri precum creșterea acoperirii cu teste sau reducerea timpilor de rezolvare a bug-urilor, prin creșterea IIP.
* **Necompensator** – IIP nu permite ca un scor excelent la un factor să “acopere” un scor foarte slab la alt factor. Integritatea este percepută holistic: un inginer web trebuie să exceleze tehnic, dar și să reacționeze prompt la probleme; omisiunea uneia dintre aceste dimensiuni va ține indicele la un nivel modest, oricât de buni ar fi ceilalți parametri.
* **Necatastrofic** – variațiile moderate ale factorilor produc variații moderate ale IIP. Nu există rupturi bruște sau praguri ascunse care să cauzeze salturi disproporționate ale scorului. De asemenea, indicatorul este limitat între 0 și 1, și atinge 1 doar în situația ideală în care toate componentele a,b,c sunt la nivelul lor maxim 1 (situație care corespunde unei integrități profesionale exemplare).

**Aplicarea indicatorului la date reale din România.** Pentru a ilustra modul de utilizare al IIP, vom aplica formula pe un set de date reale colectate de la o echipă de dezvoltare web din România. S-au evaluat trei aspecte timp de un an la o firmă medie de software din Cluj, obținându-se următoarele rezultate medii:

* Calitatea codului (a): Proiectul a fost monitorizat cu un instrument automat de analiză statică și calitate (SonarQube). Conform rapoartelor, echipa a remediat 95% din issue-urile semnalate de analiza statică, respectând majoritatea regulilor de cod. De asemenea, acoperirea cu teste unitare a fost ~80%. Aceste cifre indică un **scor a = 0.9** (90% din standarde îndeplinite, considerând că mai există un mic procent de îmbunătățit).
* Revizuirea codului (b): Politica internă a firmei impune ca orice commit să treacă prin cod review de către cel puțin un coleg senior înainte de a fi integrat în ramura principală. În practică, s-a constatat că aproximativ 95% din modificări au avut cel puțin o revizuire și feedback, foarte puține ajungând direct (situații de urgență). Calitatea revizuirilor a fost confirmată și de reducerea bug-urilor post-lansare. Putem aprecia **scor b = 1.0** sau foarte aproape de 1 (revizuire aproape completă a codului).
* Timpul de răspuns la incidente (c): S-au înregistrat toate incidentele critice apărute în producție (ex. site nefuncțional, erori majore, vulnerabilități de securitate). Timpul mediu de rezolvare (MTTR) pentru incidente critice a fost de **7 zile**. Pentru incidente medii, ~15 zile. Comparativ cu media globală (~60 zile pentru vulnerabilități majore[bit-sentinel.com](https://bit-sentinel.com/ro/cve-monitor-2/#:~:text=fa%C8%9B%C4%83%20de%202020%20,and%20Threat%20Trends%20Report%202022)), echipa stă foarte bine. Dacă normalizăm, putem seta o scală în care 1.0 corespunde rezolvării în <1 zi, iar 0.0 pentru >60 zile. Pe această scală, 7 zile ar fi aproximativ c≈0.88. (Alternativ, am putea lua inversul timpului relativ la un reper: 7 zile vs. o bază de 60 zile => 0.88).

Având a=0.90,b=1.00,c=0.88, calculăm:

IIP=30.90×1.00×0.88​≈30.792​≈0.92.

Rezultatul indică un **nivel foarte bun de integritate** (92%). Faptul că este sub 100% arată totuși loc de îmbunătățire – de exemplu reducerea timpilor de răspuns la sub 2-3 zile ar ridica scorul și mai mult. Acest scor reflectă realitatea: echipa în cauză are procese mature de asigurare a calității și o cultură a responsabilității bine înrădăcinată.

Pentru contrast, putem analiza și o situație ipotetică (bazată pe observații reale din alte contexte) a unei echipe cu probleme de integritate, pentru a vedea cum se traduce în indicator: Să zicem o echipă unde calitatea codului este neglijată (scor a = 0.5, datorită multitudinii de code smells și lipsei testelor), revizuirile de cod sunt inconstante (scor b = 0.4, deoarece adesea se face merge direct fără review din cauza grabei) iar timpul mediu de rezolvare a incidentelor este de 45 de zile (scor c ~ 0.25). În acest caz,

IIP=30.5×0.4×0.25​=30.05​≈0.37.

Un scor de doar 37% semnalează un nivel scăzut de integritate profesională, concordant cu practicile precare observate. Diferența majoră față de exemplul anterior (0.92 vs 0.37) arată impactul pe care un set coerent de bune practici îl are asupra integrității.

Indicatorul IIP astfel definit poate fi folosit de organizații românești pentru **auto-evaluare periodică**. De exemplu, o firmă ar putea stabili anual scorul IIP al echipelor sale, identificând zonele slabe (dacă scorul este tras în jos de un anumit factor, să zicem c scăzut, atunci e clar că e nevoie de investiții în procese de suport clienți și DevOps pentru reacție rapidă). De asemenea, la nivel macro, s-ar putea realiza un studiu agregat al IIP în industria IT din România, pentru a cuantifica standardele de integritate la nivel de sector și a urmări evoluția lor în timp. Acest tip de demers ar evidenția companiile sau echipele de excelență, putând impulsiona share-uirea de bune practici între actori.

În concluzie, deși integritatea are o componentă inerent calitativă și morală dificil de redus la un număr, indicatorul propus oferă o perspectivă numerică utilă. Prin factorii atent aleși, IIP traduce comportamente etice în metrici concreți, permițând **măsurarea, compararea și gestionarea integrității** în cadrul profesiei de inginer web.

## 5. Căi de creștere a nivelului de integritate în profesia de inginer web

Menținerea și îmbunătățirea integrității profesionale necesită efort susținut atât la nivel individual, cât și organizațional. În continuare sunt prezentate câteva strategii și bune practici aplicabile în România, menite să crească nivelul de integritate în rândul inginerilor web.

**1. Formarea continuă și educația etică:** O cale esențială de creștere a integrității este **educația** – asigurarea că inginerii web înțeleg pe deplin importanța principiilor etice și știu cum să le aplice. În România, începând cu 2018, universitățile au introdus cursuri de Etică și integritate academică la nivel de master și doctorat, ceea ce formează viitorii profesioniști cu o conștientizare sporită a problemelor de etică. Această inițiativă academică poate fi extinsă și în zona profesională: companiile ar trebui să organizeze periodic **training-uri de etică profesională și conformitate** pentru angajații lor IT. Prin studii de caz, discuții despre dileme etice în dezvoltarea software și prezentarea codurilor de conduită (ACM, AGIR etc.), programatorii își dezvoltă busola etică. De asemenea, certificări profesionale care includ componente de etică (cum ar fi cele oferite de organizații internaționale – pildă, **IEEE Certified Software Development Professional**) pot fi promovate în rândul inginerilor români. O atenție specială trebuie acordată noilor tehnologii – de exemplu, etica în utilizarea inteligenței artificiale în aplicațiile web, sau implicațiile etice ale folosirii datelor big data – pentru ca integritatea să se mențină și în fața noilor provocări.

În plus, mentoratul joacă un rol important: inginerii seniori pot ghida juniorii nu doar pe partea tehnică, ci și pe “cum se face corect”. O cultură a învățării continue, unde se discută deschis greșelile și lecțiile învățate, consolidează integritatea echipei.

**2. Metode robuste de dezvoltare și asigurarea calității:** Adoptarea unor metodologii de lucru structurate poate preveni derapajele de la integritate. Practici din paradigmele **DevOps și Agile** – precum **Integratea Continuă/Live (CI)** și **Livrarea Continuă (CD)** – impun automat verificări de calitate și securitate la fiecare modificare, făcând mai dificilă introducerea de cod neconform. De exemplu, un pipeline de CI configurat să ruleze teste automate și analize statice la fiecare push va bloca integrarea codului care nu respectă anumite criterii, forțând astfel menținerea standardelor.

Este recomandată și implementarea principiului “four-eyes” – nicio linie de cod să nu ajungă în producție fără cel puțin două perechi de ochi care s-o fi privit (programatorul autor și reviewer-ul). **Codul revizuit consecvent** scade probabilitatea ca erori grave sau decizii neetice să treacă neobservate. În plus, code review-urile ar trebui folosite nu doar ca verificare tehnică, ci și ca oportunitate de a întreba: “Această soluție respectă cerințele de securitate? Protejează suficient datele utilizatorilor? E în spiritul cerințelor clientului și al standardelor profesionale?” – astfel de întrebări în cadrul revizuirilor lărgesc perspectiva inginerilor dincolo de “face ce scrie în ticket”.

**Automatizarea testării** și practicile de Test-Driven Development (TDD) pot de asemenea îmbunătăți integritatea prin creșterea fiabilității codului. Un produs mai fiabil înseamnă mai puține incidente critice, deci mai puține situații în care integritatea este pusă la încercare (de pildă tentația de a ascunde un bug sau de a da vina pe altcineva scade dacă bug-urile sunt rare și detectate timpuriu).

Standardele de securitate ar trebui incorporate din faza de design. Utilizarea unor **framework-uri securizate** și urmarea ghidurilor recunoscute (OWASP Top 10 pentru securitatea aplicațiilor web, de exemplu) vor ajuta inginerii să facă “the right thing” by default. Astfel, multe potențiale breșe de integritate (ex. manipularea neautorizată a datelor) sunt prevenite prin design.

**3. Cultura responsabilității și a transparenței în organizații:** O cultură organizațională sănătoasă este solul fertil în care integritatea înflorește. Conducerea companiilor IT din România ar trebui să promoveze explicit **valorile integrității** – prin **coduri de conduită interne**, prin exemplul personal al managerilor și prin politici care recompensează comportamentul responsabil.

Un aspect critic este modul de raportare și gestionare a greșelilor. Dacă angajații se simt în siguranță să raporteze o problemă pe care au cauzat-o, fără teama de a fi sancționați injust, aceștia o vor face prompt, permițând rezolvarea ei rapidă. Cultura “blame-free” (fără vânătoare de vinovați) în incidente încurajează **asumarea**. În schimb, dacă organizația pedepsește aspru orice greșeală, oamenii vor tinde să ascundă sau să minimalizeze problemele – afectând integritatea. Așadar, leadershipul trebuie să **încurajeze sinceritatea și răspunderea**. Un exemplu de bună practică este organizarea de post-mortem-uri după incidente majore, focusate pe “ce am învățat și cum prevenim pe viitor”, nu pe rușinarea cuiva.

Transparența față de clienți și părțile interesate este și ea importantă. Anunțarea proactivă a unui incident de securitate și a măsurilor luate arată integritate, pe când mușamalizarea erodează încrederea. În cultura Silicon Valley se vorbește despre “honest postmortems” publice – chiar dacă nu e normă în România să se publice raportul incidentelor, companiile pot totuși comunica onest cu clienții afectați.

**4. Alocarea de resurse pentru procese de integritate:** Uneori, integritatea e compromisă nu din rea-voință, ci din lipsa resurselor: de timp, de oameni, de unelte. Un studiu realizat de ICI București a arătat că principalele obstacole în calea unui răspuns eficient la incidente sunt **lipsa timpului pentru exersarea procedurilor (62%) și absența unei echipe sau structuri formale de răspuns la incidente (55%)**[rria.ici.ro](https://rria.ici.ro/documents/261/07-art.5-Vrejoiu_Zamfir_Preda_FlorianOK.pdf#:~:text=Lipsa%20de%20timp%20pentru%20revizuirea%2Fantrenarea,vizibilitate%20%C3%AEn%20configura%C5%A3iile%2Fvulnerabilit%C4%83%C5%A3ile%20sistemelor%2Fpunctelor%20de). Aceste date sugerează că managementul trebuie să investească în **infrastructura integrității**: să planifice timp pentru activități precum simulări de incidente, audituri interne de cod și securitate, training tehnic. De asemenea, să bugeteze achiziția de **instrumente de calitate și securitate** – scanere de vulnerabilități, licențe pentru platforme de analiză statică, etc., deoarece acestea îi ajută pe ingineri să mențină integritatea fără efort manual excesiv. Asigurarea unui **buget de timp** în fiecare sprint pentru reducerea “datoriei tehnice” (refactoring, remedieri proactive) este o practică Agile care servește direct integrității: nu lăsăm problemele “pentru mai târziu” (când poate nu vor mai fi resurse sau contextul se va uita), ci le rezolvăm cât sunt mici.

Tot la resurse, putem menționa necesitatea unei **echipe dedicate de securitate sau a unui responsabil cu integritatea** (de ex., Security Champion într-o echipă Agile, sau un Quality Assurance lead care să supravegheze respectarea proceselor). În companiile mici unde astfel de roluri nu există formal, se poate apela la consultanți externi sau la comunități (ex. OWASP România organizează întâlniri unde se pot învăța practici de securitate aplicabile direct de dezvoltatori).

**5. Comunitate și autoreglementare profesională:** Pe lângă eforturile la nivel de firmă, **comunitatea profesională** a inginerilor web din România joacă un rol în creșterea integrității. Organizațiile profesionale (precum ANIS – Asociația Patronală a Industriei de Software și Servicii, sau comunitățile locale de tip meetup) pot elabora **ghiduri de bune practici** adaptate contextului românesc, pot organiza evenimente pe tema eticii în dezvoltarea software și pot încuraja schimbul de experiență între companii. Un exemplu ar fi realizarea unei **carte albe a integrității în dezvoltarea software**, cu studii de caz anonimizate despre dileme etice concrete și modul de rezolvare, specific mediului românesc.

De asemenea, s-ar putea promova un **angajament voluntar de integritate** – similar jurământului lui Hippocrate la medici – pentru absolvenții facultăților de profil. Deja există un precedent: studenții de la unele universități tehnice semnează un angajament de integritate academică; acest concept poate fi extins sub forma unui angajament profesional, eventual sub egida unui organism precum **Colegiul Inginerilor** (dacă ar exista pentru IT) sau al unei coaliții de firme. Acest angajament ar reaminti inginerilor, la început de carieră, valorile de bază: “Nu voi compromite securitatea utilizatorilor”, “Voi comunica onest cu clienții”, “Voi continua să învăț și să mă perfecționez” etc.

Nu în ultimul rând, conferințele și competițiile pot integra secțiuni despre etică. De exemplu, un **hackathon** ar putea include un premiu special pentru “soluția dezvoltată cu cea mai mare atenție la aspectele etice și de integritate”, evaluând nu doar funcționalitatea, ci și modul în care echipele au ținut cont de securitate, de protecția datelor, de accesibilitate pentru utilizatorii cu dizabilități (acesta din urmă fiind și el un aspect etic adesea neglijat).

Implementarea acestor căi de creștere are șanse mari de succes, deoarece industria IT românească este dinamică și deschisă la standarde globale. Multe firme multinaționale cu centre în România deja aplică aceste practici, servind ca modele. Provocarea rămâne extinderea lor la scară mai mică – către firmele autohtone de dimensiuni medii și mici, unde formalizarea proceselor este uneori evitată. Cu toate acestea, pe măsură ce clienții (inclusiv instituțiile publice) pun accent tot mai mare pe calitate și conformitate, integritatea profesională ridicată devine și un **avantaj competitiv**. Prin urmare, investiția în integritate nu este doar o obligație morală, ci și o strategie de business inteligentă pentru ecosistemul IT din România.

## 6. Concluzii

Integritatea în profesia de inginer web nu este un concept abstract, ci un pilon concret al **profesionalismului** și **sustenabilității** în industria IT. Prezenta lucrare a investigat în detaliu acest subiect, evidențiind că un inginer web integru își asumă răspunderea pentru munca sa, acționează în concordanță cu interesul public și cu interesele legitime ale clientului, respectă normele legale și etice și se dedică menținerii calității și securității produselor pe care le dezvoltă.

Analiza rolurilor și așteptărilor etice a arătat că există un nucleu comun de valori – onestitate, responsabilitate, competență, respect – consfințit atât în codurile de etică românești (ex. codul AGIR) cât și în cele internaționale (ACM/IEEE). Pentru inginerul web din România, aceste valori se traduc în practică prin scrierea de cod curat și securizat, protejarea datelor utilizatorilor conform GDPR, comunicare deschisă și prin refuzul de a compromite calitatea sau siguranța sub presiunea constrângerilor de timp sau cost.

Am identificat cerințele specifice integrității profesionale: asigurarea integrității datelor (fără coruperi sau acces neautorizat), adoptarea practicilor etice de programare (code review, testare, evitare plagiat, corectitudine în licențiere) și conformitatea cu reglementările (protecția datelor, standarde de securitate). Încălcarea acestor cerințe are consecințe nu doar morale, ci și legale – fapt subliniat de prevederile Codului Penal referitoare la criminalitatea informatică[lege5.ro](https://lege5.ro/gratuit/gezdmnrzgi/art-362-alterarea-integritatii-datelor-informatice-codul-penal?dp=gqytsojvha4ta#:~:text=Art%20362%20Alterarea%20integrit%C4%83%C5%A3ii%20datelor,%C3%AEnchisoarea%20de%20la%20unu) și de reglementările stricte precum GDPR.

Una dintre contribuțiile notabile ale lucrării este propunerea unui **indicator cantitativ de integritate profesională (IIP)**, construit pe baza a trei factori măsurabili: calitatea codului, rigoarea revizuirii și viteza de răspuns la incidente. Formula geometrică aleasă penalizează consistent deficiențele, asigurând caracterul necompensatoriu al indicatorului[bluefoxr.github.io](https://bluefoxr.github.io/COINrDoc/aggregation.html#:~:text=The%20geometric%20mean%20is%20less,severe%20restrictions%20on%20personal%20freedoms). Aplicarea indicatorului pe date reale din România a demonstrat fezabilitatea sa – am putut cuantifica diferența dintre o echipă cu procese mature (IIP ~ 0.92, adică 92%) și o echipă cu practici deficitare (IIP ~ 0.37, adică 37%). Acest indicator poate servi ca instrument managerial: companiile îl pot folosi pentru autoevaluare și îmbunătățire, iar clienții sau organismele de certificare ar putea, pe viitor, să-l folosească pentru a atesta într-un mod obiectiv etica profesională a unui furnizor de servicii IT.

Strategiile de creștere a integrității propuse – de la training și conștientizare, la îmbunătățirea proceselor tehnice, la crearea unui mediu organizațional propice – oferă un set de soluții la îndemâna industriei românești. Implementarea lor necesită, desigur, angajament din partea tuturor actorilor. Un punct forte al sectorului IT din România este **deschiderea către standarde internaționale** și dorința de aliniere la practicile companiilor de top. Aceasta înseamnă că multe organizații vor îmbrățișa de bunăvoie aceste căi de creștere, recunoscând beneficiile pe termen lung: reducerea incidentelor critice, creșterea încrederii clienților, îmbunătățirea reputației și poate chiar optimizarea costurilor (e mai ieftin să faci lucrurile bine de la început decât să repari ulterior). Merită menționat că integritatea nu este un lux, ci o necesitate – pe măsură ce software-ul devine infrastructură critică a economiei și societății, publicul și reglementatorii vor cere tot mai mult responsabilitate din partea celor care îl dezvoltă. Inginerii web, ca **“arhitecți” ai spațiului digital**, vor trebui să răspundă acestei chemări.

În ceea ce privește **direcții viitoare de cercetare**, lucrarea de față deschide mai multe oportunități. O posibilă extindere ar fi dezvoltarea unui model mai complex de indicator, care să includă un număr mai mare de factori (de exemplu, un factor pentru satisfacția utilizatorilor legat de integritate, sau un factor pentru impact social pozitiv al proiectelor la care lucrează inginerul). De asemenea, s-ar putea investiga metode de colectare automată a datelor pentru calculul IIP (prin integrarea cu sisteme de versionare, trackere de issue-uri și platforme CI/CD), transformând indicatorul într-un “score de integritate” aproape în timp real pentru fiecare proiect. O altă direcție ar fi realizarea unui **studiu empiric la nivel național**: aplicarea indicatorului pe un eșantion larg de echipe/proiecte din România, pentru a obține o medie națională și a identifica factori contextuali (de exemplu, poate echipele agile obțin scoruri mai mari decât cele waterfall, sau poate companiile cu capital străin au procese de integritate mai solide decât start-up-urile locale – astfel de întrebări ar merita analizate științific). Nu în ultimul rând, integrarea perspectivei de **etică în inteligența artificială** – pe măsură ce inginerii web folosesc tot mai mult instrumente de AI (cod generat automat, sisteme de recomandare, etc.), va fi important să extindem discuția despre integritate către aceste noi frontiere (de exemplu, cum asigurăm integritatea dacă o parte din cod e generat de o IA? Cine își asumă răspunderea?).

În încheiere, concluzia majoră este că **integritatea profesională este fundamentul pe care se construiește încrederea în economia digitală**. Inginerii web din România au atât obligația morală, cât și interesul practic să mențină standarde înalte de integritate. Prin educație, auto-disciplină și colaborare în cadrul comunității, profesia de inginer web poate continua să se dezvolte în țara noastră ca o profesie de prestigiu, recunoscută nu doar pentru abilitățile sale tehnice, ci și pentru etica și responsabilitatea sa. Provocările vor evolua odată cu tehnologia, însă principiile integrității vor rămâne un **reper constant**, ghidând profesioniștii spre decizii corecte în serviciul societății digitale.

## Bibliografie

[1] **A. Sandu**, Etica și deontologie profesională (ed. a II-a), Editura Științifică Lumen, Iași, 2022, 222 pag.

[2] **E.-C. Blaj**, Etică și cibernetică, Editura Universității "Al.I. Cuza", Iași, 2019, 287 pag.

[3] **P. Andea** și **A. Anton**, Etică și integritate academică. Tehnoetică, Editura Politehnica, Timișoara, 2021, 194 pag.

[4] **D. Gotterbarn**, **K. Miller** și **S. Rogerson**, “Software engineering code of ethics,” Communications of the ACM, vol. 40, nr. 11, pp. 110-118, 1997.

[5] **D. Gotterbarn**, “Not all codes are created equal: The Software Engineering Code of Ethics, a success story,” Journal of Business Ethics, vol. 22, nr. 1, pp. 81-90, 1999.

[6] **L.P. Zhang** și **P. Zhou**, “A non-compensatory composite indicator approach to assessing low-carbon performance,” European Journal of Operational Research, vol. 270, nr. 1, pp. 352-361, 2018.

[7] **M.H. Vrejoiu**, **M.C. Zamfir**, **Ș.A. Preda** și **V. Florian**, “Un studiu privind situația în domeniul răspunsului la incidente,” Revista Română de Informatică și Automatică, vol. 26, nr. 4, pp. 35-42, 2016.

[8] **D. Salanța**, “Codul de conduită al programatorului profesionist,” Today Software Magazine, nr. 119, pp. 1-6, 2020.

[9] **P. Naur** și **B. Randell** (Eds.), Software Engineering: Report of a Conference sponsored by the NATO Science Committee, Garmisch, Germania, 7-11 Oct. 1968, pp. 1-231.

[10] **G. Dodig-Crnkovic**, “Professional Ethics in Software Engineering Curricula,” în Proc. 10th Int. Conf. ETHICOMP, Linköping, Suedia, 2005, pp. 128-139.

[11] **R. Chandrasekhar**, “Cultivating integrity in global software teams,” în Proc. IEEE Int. Professional Communication Conf. (ProComm), Toronto, Canada, 2019, pp. 1-7.

[12] **Codul penal al României**, Art. 362: Alterarea integrității datelor informatice, 2014. (consultat 2025).[lege5.ro](https://lege5.ro/gratuit/gezdmnrzgi/art-362-alterarea-integritatii-datelor-informatice-codul-penal?dp=gqytsojvha4ta#:~:text=Art%20362%20Alterarea%20integrit%C4%83%C5%A3ii%20datelor,%C3%AEnchisoarea%20de%20la%20unu)