

Patru piloni digitali pentru o Românie prosperă în deceniul 2020-2030

Recomandare tehnică de interes public pregătită de
Bogdan **BOCȘE**

Cuvânt înainte

Alegem să ne exprimăm patriotismul nu prin respectarea unui status quo defunct, nici prin scandări sau lozinci, ci prin a ne împărtăși viziunea noastră concretă, tehnică, pragmatică și incluzivă a unei Românie moderne, care își asumă cu responsabilitate punctele forte și slăbiciunile proprii și ne aduce pe toți împreună pentru a pune umărul la construirea țării pe care vrem să o avem în viitor. Ne dorim să aducem sub ochii tuturor șansa de a vedea un viitor în care tehnologia funcționează bine și în folosul cetățeanului, al societății.

Concret, în cele ce urmează vom defini cei patru piloni digitali ai dezvoltării României care, în ciuda apartenenței la ramuri sociale și instituționale diversificate, au o rădăcină comună: **competența informațională și digitală a românilor și României.**

În ciuda faptului că este prematur pentru a discuta despre planificare, este părerea noastră că, presupunând susținerea Legislativului și Executivului, următoarele inițiative sunt fezabil de inițiat în perioada 2020-2025, pentru a fi finalizate până în 2028-2030.

| | |
|---|-----------|
| I. Autonomie și siguranță | 3 |
| Încredere digitală cu rădăcini locale ("Trust Romania") | 3 |
| Context | 3 |
| Măsuri concrete | 3 |
| Cerințe tehnice | 4 |
| RoIntraNet: Autonomie și robustețe locale a infrastructurii Internet | 6 |
| Propuneri concrete | 6 |
| II. Educație pentru viitor | 8 |
| O țara de cetățeni digitali. Fără granițe. | 8 |
| Măsuri concrete | 8 |
| O țara de programatori. Fără discriminare. | 9 |
| Context | 9 |
| Măsuri concrete | 9 |
| III. Români conectați la pulsul economiei digitale | 10 |
| Creșterea acoperirii în populație și teritoriu a economiei digitale de producție (Digital Economy Coverage) | 10 |
| Libera circulație financiară-și-digitală între cetățeni Români | 11 |
| IV. Trasabilitate administrativă digitală | 12 |
| Arhitecturi de referință pentru toate proiectele de IT achiziționate sau comandate de către sectorul public | 12 |
| Măsuri concrete | 12 |
| Registru de evidență inter-instituțional, automat auditabil | 13 |
| Propuneri concrete | 13 |
| Sistem agreat de administrația centrală pentru preluarea din teritoriu, de la cetățeni a dovezilor video-fotografice pentru probleme raportate. | 14 |
| Propunere concretă | 14 |
| Digitalizarea serviciilor de protecție a consumatorului, printr-o aplicație de recunoașterea etichetelor folosind inteligență artificială, | 15 |
| Propunere concretă | 15 |

I. Autonomie și siguranță

Încredere digitală cu rădăcini locale ("Trust Romania")

Context

CertIFICATELE criptografice digitale sunt pânza din care e țesută încrederea în lumea digitală modernă. Beneficiem de aceste invizibile chei ale încrederii electronice de fiecare dată când ne verificăm mailul, de fiecare dată când facem o plată online. Dar nu realizăm că de multe ori acea încredere este mediată sau dependentă de instrumente invizibile pe care nu le controlăm.

Ca să dăm o dimensiune mai concretă poveștii, ne imaginăm toți oamenii cu meseria de lăcătuș, cei care fac și copiază lacăte și chei. Chiar dacă nu stăm prea mult să ne gândim la asta, vrem-nu vrem, un lăcătuș este investit cu încredere de către noi: ne bazăm pe treaba făcute de el ca să intrăm în casă, ne bazăm pe treaba lui ca să ne simțim în siguranță în casa noastră. Dacă un lăcătuș ți-ar cere buletinul și ar putea să îți vadă adresa, cu siguranță am fi cu toții mai precauți cu felul în care ne alegem lăcătușul.

CertIFICATELE digitale sunt echivalentul cheilor din lumea Internetului. La fel cum cheile și lacătele ne garantează siguranța noastră fizică, a celor dragi și a obiectelor fizice, certificatele digitale sunt o dovadă a încrederii pe care o putem avea în integritatea, secretitudinea și identitatea-originii datelor, când comunicăm cu ajutorul Internetului. În acest context, un mail, un mesaj, o plată sau înscrierea pe un site, toate aceste și multe altele sunt exemple de comunicație.

Din păcate, sistemul de IT din România se bazează în mod predominant pe astfel de certificate emise de autorități de certificare străine. Desigur, e un lucru bun să existe mai multe origini ale încrederii, atât în țară, cât și în străinătate. Însă a nu avea un echilibru între încrederea digitală de origine internă și cea de origine externă, ne limitează tuturor abilitatea de a dezvolta tehnologie de încredere, mai ales în sectorul public, și ne expune în mod inutil la riscuri personale, organizaționale și la nivel național.

Încrederea funcționează cel mai bine când este descentralizată și nu există câteva puncte centrale de care depinde funcționarea întregului sistem. În acest scop, companiile, instituțiile și cetățenii au nevoie de o metodă ieftină, facilă, accesibilă și popularizată de a cere, de a beneficia de și de a oferi încredere în piața digitală. Administrația centrală și cea locală trebuie să preia datoria întreținerii acestui nou fel de "ștampile" ale viitorului: mai ieftine, mai eficiente, mai sigure și aproape instantaneu de transportat.

Măsuri concrete

- **Legislativ:** revizuirea condițiilor de acceptabilitate în instanță a probelor, bazată pe tăria dovezilor criptografice aduse spre coroborarea lor, dar și de diversitatea autorităților care au stat martor la probarea respectivelor dovezi - aici este cheia și, deocamdată, și marele impediment.
- **Legislativ:** reglementarea modului de obținere a cărții de identitate digitale, de către cetățeni și companii, pe baza oferirii unei dovezi de absolvire a unui scurt curs de siguranță digitală. Eliberarea acestor dovezi de către structurile din subordinea Autorității pentru Digitalizarea României, cu

informarea Ministerului de Interne (Poliția Generală, Evidența Populației) și cu respectarea legislației europene despre eID.

- **Legislativ:** revizuirea legii pentru stabilirea condițiilor de echivalare între timbru sec, pe de o parte, și certificat digital și/sau semnătura digitală, a unui notar certificat. Integrarea competenței de a emite și semna certificate digitale în statutul notarilor publici -
 - Există deja legislație pentru acreditarea notarului public electronic.
 - Cum motivăm notarii să caute și să promoveze acreditarea notarului public electronic?
- **Legislativ:** obligativitatea, în 24-36 luni, a eliberării certificatelor și dovezilor solicitate de către persoane fizice și juridice, în format digital, citibil atât de om (format tipărit și afișabil) cât și de calculator (unul din formatele standard de reprezentare, împreună cu schema de corectitudine a acelei reprezentări), în conformitate cu litera GDPR și în continuitatea spiritului acestei reglementări europene.
- **Legislativ:** obligativitatea tuturor instituțiilor să garanteze prin statut că toate informațiile transmise prin Internet sau intranet-uri sunt securizate cu standardul TLS 1.2.
- **Legislativ:** reglementarea uniformă Registraturii Digitale, care să definească probele necesare dovedirii identității în cazul prezenței fizice (carte de identitate, prezență personală), în cazul prezenței digitale (certificat digital, semnătură biometrică, semnătură olografă) sau în cazul solicitărilor interinstituționale (semnate criptografic la ambele capete) -
 - Reglementarea [UE 910/2014 EIDAS](#) se referă la această problemă.
- **Legislativ:** reglementarea mijloacelor de probare criptografică a datelor certe, în coroborare cu identitatea și cu dovada momentului de timp (timestamp) din cel puțin o sursă de încredere.
- **Administrativ:** factorul public juridic: instituțiile de încredere emitente de certificate digitale - deocamdată sunt privații care operează în acest domeniu în regim de monopson (CERTSign, VeriSign etc) și unele autorități, dar cu utilizare restrânsă:
 - Stimularea concurenței în mediul privat în domeniul emiterii de certificate prin oferirea unor alternative de domeniu public, operate și oferite de instituții publice
 - De exemplu AADR emite certificate pentru utilizare doar în platforma pentru achiziții publice SEAP, SRI emite doar pentru uz intern etc).
- **Administrativ:** factorul privat juridic: certificate digitale semnate de notari

Cerințe tehnice

- **Echivalentul formularelor tip pentru epoca digitală:** Folosirea unui format standard și modern de reprezentarea a documentelor tip (**OpenAPI, GraphQL**), pentru creșterea previzibilității și eficienței circulației informației, încrederii și banilor între cetățeni și instituții sau între instituții. Standardizarea acestor frecvent-folosite documente reduce milioane de ore neproductive din economie, dedicate acum citirii și transcrierii din format fizic în format digital și vice-versa. Acest potențial de efort uman pentru oportunități productive sau de agrement.
- **Semnarea criptografică periodică** (orar, zilnic), automată a registrelor/jurnalelor de operațiuni pe fiecare mijloc de stocare activ sau pasiv (backup).

- **Auditarea periodică semi-automată a semnăturilor criptografice**, semi-supervizată de un operator uman desemnat, autentificat și identificat. Auditarea periodică semi-automată se manifestă printr-o convergență dintre principiul blockchain (immutability - nimic nu se șterge fără măcar să aflăm cu toții că s-a șters) și principiul reconcilierii contabile în dublu-registru (Double/Multiple-entry bookkeeping system; cotabilitate în partidă dublă sau multiplă)
 - Pentru clarificare, oferim un exemplu: Fie trei autorități emitente de certificate, CA1, CA2 și CA3. O relație de supra-încredere (audit) între CA1 și CA2 și CA3 este atunci când:
 - 1) CA1 pune la dispoziția lui CA2 și CA3 un rezumat* al certificatelor emise de CA1, în fiecare perioadă (eg. odată la două ore), și totodată
 - 2) CA2 pune la dispoziție la CA1 și CA3 un rezumat* al certificatelor emise de CA2, în fiecare perioadă (eg. odată la două ore)
 - 2) CA3 pune la dispoziție la CA1 și CA2 un rezumat* al certificatelor emise de CA3, în fiecare perioadă (eg. odată la două ore)
 - Rezumatul unei colecții de certificate conține cel puțin:
 - a) o numărare a certificatelor,
 - b) un hash cardinal (care nu ține cont de ordinea emiterii; se poate implementa folosind un filtru Bloom sau un hash criptografic aplicat pe o sortare lexicografică a identificatorilor)
 - c) un hash ordinal (care ține cont de ordinea emiterii)
 - d) un tabel Bloom care să ajute la descoperirea eventualelor discrepante
 - O lipsă de reconciliere automată a condițiilor (a-cantitate), (b,c-integritate) și (d-identitate) este motiv suficient pentru inspecție/verificare umană a motivului nereconcilierii.

RoIntraNet: Autonomie și robustețe locale a infrastructurii Internet

Pe măsură ce serviciile Internet au devenit parte a nucleului infrastructural, integritatea și securitatea națională depind de gradul de consolidare internă a rețelei publice de comunicații digitale a României. Dat fiind climatul geopolitic volatil, este valoroasă, pentru liniștea românilor, verificarea periodică a autonomiei interne chiar și în condiții de insularizare parțială sau totală față de Internet, cu cauze de origine internă, externă sau hibridă.

Propuneri concrete

- 1. Limitarea dependenței de actori externi pentru acces la servicii digitale uzuale**, pentru pregătire în situații de forță majoră sau urgență națională.
 - a. Auditarea mecanismelor de încredere la nivelul protocoalelor de rutare ale marilor furnizori de telefon
 - b. IP Routes - non-external IP route fallback
 - c. Replică DNS intra-național, cu latență de sincronizare garantată (funcțional în cazul pierderii conectivității cu exteriorul)
 - d. Firewall dinamic la nivel național, pe baza unei liste dinamice și scurte de agenți IP malițioși străini (de proveniență non-EU și non-NATO), capabil de filtrarea (shaping), redirecționarea (rerouting) sau, ca măsură de ultim resort, distrugerea (drop) traficului IP, identificat și confirmat ca fiind malițios, în baza unui mandat digital confirmat de instituții abilitate incluzând CERT-RO, pe o perioadă scurtă și bine-delimitată de timp.
Deprioritizarea automată a traficului video care nu e identificat ca fiind critic.
- 2. Infrastructură secundară de urgență** ("emergency shadow infrastructure") pentru comunicații critice, cu parametrul QoS (Quality of Service, parametru din stiva TCP/IP), strict ordonat după gradul de severitate, și insularizarea controlată a comunicațiilor în caz de urgență națională.
 - a. Măsurarea capacității infrastructurii de urgență de preluarea a cererii estimate sezonier, cu pas orar și ciclu anual, per fiecare palier de severitate-criticitate (QoS)
 - b. Estimări regionale ale impactului
 - c. Plan de insularizare parțială
- 3. Limitarea dependenței crescânde de servicii informatice externe** pentru a contracara o slăbiciune de ordin strategic a țării, care duce la imobilizare din punctul de vedere al accesului. Securizarea capacității de calcul pe teritoriul României în caz de izolare (insularizare) față de Internet parțială sau totală.
- 4. Reducerea dependenței de furnizori străini** prin acordarea de facilități bugetare instituțiilor care folosesc cel puțin 80% tehnologie open source. Condiționarea bonificărilor fiscale oferite companiilor de IT de utilizarea măsurabilă a contribuțiilor open source făcute de acestea, preferabil în jur de 10-20% din volumul codului scris.
- 5. Transparența codului** care procesează date personale prin înregistrarea lui la o autoritate neutră, a carei singură misiune este să publice codul peste o perioadă suficient de lungă, de ordinul 4-7 ani. Majoritatea codului fiind rescris sau înlocuit mai repede de atât în mod uzual,

impactul asupra competitivitatii pietei e redus. In acealasi timp, constinta faptului ca munca lor va fi vizibila si comparata cu a altora din aceeasi perioada reprezinta o **motivatie reputationala** de a nu cauta eficienta sau avantaje comerciale prin obscurizarea mijloacelor de operare sau de securizare. O alternativa superioara calitativ si tehnic, este recomandarea de auto-regulare, prin publicarea in avans a dovezilor criptografice ale scrierii codului, urmata de o publicare, la un interval de timp ales de furnizor (2 ani, 5 ani), a codului propriu-zis; nealterarea informatiilor publicate e garantata prin corespondenta criptografica cu dovezile publicate in prima instanta, in mod similar cu o parte din mecanismul blockchain ("Eventually open source code").

6. **Exerciții periodice scurte** (între 30 secunde-30minute) între operatorii telecom publici și privați, planificate în avans, publicate sau secrete, pentru pierderea selectiva a conectivității la nivel național sau regional (Connectivity drills).

II. Educație pentru viitor

O țara de cetățeni digitali. Fără granițe.

Competențele digitale sunt oportunitatea și obligația* tuturor cetățenilor, indiferent de vreun criteriu discriminatoriu conceput în prezent sau viitor.

***Dreptul rezultă ca abordarea unor oportunități în contextul unor obligații.**

Măsuri concrete

1. Interfețele digitale eficiente
 - a. Tastare corectă și rapidă pe tastaturi mecanice convenționale.
 - b. Patriotismul se manifestă digital inclusiv prin scrierea cu diacritice, atunci când folosim limba română.
 - c. Studiarea și comunicarea publică periodică de către operatorii de telefonie și de către Ministerul Educației a efectelor tastaturilor de tip touchscreen în dezvoltarea cognitivă a copiilor.
2. Interfețele digitale în serviciul public al echilibrării nevoilor și capabilităților umane
 - a. Studiarea și comunicarea publică periodică a timpilor maximi recomandați de folosire a ecranelor mici (mai puțin de 25cm diagonală, aproximativ 10 inch, exemplu: smart phone), a ecranelor medii (diagonala între 25-41 cm, exemplu: laptop, tablet), a ecranelor mari (diagonala mai mare de 41 cm, exemplu: televizor, ecran de lucru) și a ecranelor cvasi-oculare (care acoperă întreg spațiul vizual al omului, inclusiv realitate virtuală).
 - b. Studiu individual, bazat pe voluntari
 - c. Studiu partajat pe grupe de vârstă
 - d. Studiu cu proiecție pe efectul asupra abilităților (individual măsurate) cognitive, mnemonice, lingvistice, de imaginare, de analiză, de sinteză și planificare pe termen scurt (mai puțin de o zi), mediu (3-6 luni) sau lung (mai mult de un an).
 - e. Studiu efectelor autocorelativ proliferative sau excesive (care induc dependență)
 - f. Studiu efectelor asupra atenției.
3. Prevenție și responsabilizare: Siguranță de bază a interfețelor digitale
 - a. Definirea și promovarea conceptelor duale de **agent - avatar și identitate - imagine**.
 - b. Importanța securizării fizice și criptografice a datelor;
 - c. Importanța intimității fotografiilor, corelată potențialul de publicitate pe care îl are orice fotografie trimisă;
 - d. Campanie informare: Parole și siguranța cu doi factori
 - e. Campanie informare: Chei publice-private, Certificate
4. Oportunitatea și obligativitatea populației cu privire la informarea imparțială
 - a. Citirea și verificarea știrilor înainte popularizării sau distribuirii lor.

- b. Verificarea informațiilor și știrilor în trei surse de încredere, preferabil una din afara granițelor.

O țara de programatori. Fără discriminare.

Context

A învăța să programezi e cea mai scurtă cale sigură și universală afară din sărăcie. Toți copiii ar trebui să aibă șansa să-și dezvolte această claritate de exprimare și de gândire.

Compilerul nu te întreabă câți bani ai în cont. Compilerul nu te cheamă la meditații și nu îți cere șpagă ca să te treacă clasa. Compilerul nu te întreabă la ce dumnezeu te închini. Nu-l interesează nici ce culoare are pielea ta, nici dacă ești băiat sau fată. Pe compilerul îl interesează doar dacă, exprimi clar și corect ce ai scris în limbajul de programare. Atât.

Dreptul și oportunitatea de a învăța programare prin *_exercitiu practic și verificabil în automat_ pe platforme disponibile online*, compatibil cu device-uri mobile, fără discriminare, garantat pentru copiii Europei și pentru toți cetățenii Europei. Într-o lume a carei complexitate e creată de algoritmi, privirea populației de înțelegerea fundamentelor acestei tehnologii produce un clivaj adânc al inegalității de oportunitate în munca și în viață. Chiar dacă forma echivalente ale acestui drept există în diferite jurisdicții, acest drept este alienat de facto prin lipsa infrastructurii și prin lipsa personalului educat. Pentru a agrava situația, personalul didactic este marcat de un bagaj de cunoștințe cu un ciclu de reînnoire mult mai mic decât cel al industriei. ("Digital Technologies in Service of Education")

Măsuri concrete

- Platformă online, publică, open source cu provocări practice, rezolvabile de programare și digitalizare, corectate/validate automat.
- Utilizare autentificată sau anonimă (cu unele limitări).
- Trasarea valorilor comunității prin evidențierea contribuțiilor în propunerea de probleme sau materiale noi.
- Disponibilitate atât pe platforme laptop/desktop (Linux, Windows), dar și pe telefon (Progressive Web App/PWA).

Inițiative cetățenești care deservește această nevoie:

- [Emun.ro](#) - aplicație pentru vizualizarea grafică a secvențelor de cod și a componentelor lor
- [vCatalog](#) - aplicație pentru partajarea notelor între profesor, elev, părinte

III. Români conectați la pulsul economiei digitale

Creșterea acoperirii în populație și teritoriu a economiei digitale de producție (Digital Economy Coverage)

Promovarea și înlesnirea oportunităților de **educare profesională și financiară în mediul digital**, precum și oportunitățile de profesare într-o meserie digitală, inclusiv prin prestarea de muncă-la-distanță (remote work), pentru persoanele din zone defavorizate economic, prin intermediul instrumentelor informatice de instruire, examinare și lucru la distanță, cu validare în timp real sau cu mică întârziere (mai puțin de 10 minute) față de timpul real.

Măsuri concrete:

- Oportunități de educare profesională digitală pentru persoanele din zone defavorizate economic, prin instrumente de instruire și lucru la distanță, cu validare în timp real sau în timp scurt.
- Promovarea oportunităților de muncă-la-distanță, realizate prin instrumente digitale ieftine.
- Întreținerea unui registru digital public de furnizori agreați de muncă la distanță.
- Instruire care își asumă ca obiectiv obținerea unei productivități dovedibile și măsurabile prin aplicarea cunoștințelor digitale dobândite, pe parcursul programului și la finalul său.

Comentarii

De studiat în corelație cu programarea financiară multi-anuală 21-27, în acest sens. Neclar încă dacă vor fi doar pe POCU sau vor fi separat alocați și pe POCID. De urmărit, începând cu 2021, ghidurile de finanțare.

Libera circulație financiară-și-digitală între cetățeni Români

”Oricare doi **români**, aflați pe teritoriul **României**, știindu-și unul altuia cel puțin *numele complet, numărul de telefon și data nașterii*, își pot transmite până la 10.000 RON sau 2.500 EUR (în echivalent RON, la cursul afișat de BNR pentru acea zi) pe lună, la **comision zero**, folosind **mijloace digitale** sau **mergând** nu mai mult de **doi kilometri** de la locul de domiciliu, așteptând nu mai mult de **5 minute** pentru a primi un *bun-serviciu** și nu mai mult de **60 de secunde pentru a primi confirmarea**, identificabilă și la nevoie auditabilă, a *bunei-livrări** sau măcar a *bunului-incipit-de-livrare**.

Totodată, împreună cu transferul de bani, expeditorul poate atașa până la 1GB de informație, inclusiv video, audio sau text, care trebuie livrată destinatarului odată cu fondurile și care poate fi stocată până la 30 de zile, dar poate fi ștearsă și mai devreme, dacă expeditorul sau destinatarul decid ”

** Bunul-serviciu, buna-livrare și respectiv bunul-incipit-de-livrare sunt evaluate de către transmițătorul și receptorul fondurilor, la nu mai puțin de două zile și nu mai mult de 15 zile. Evaluarea se poate exprima proactiv, prin mijloace digitale, de către oricare dintre participanți. Reclamațiile se pot depune în formă digitală sau scrisă. Identificarea tranzacției se face pe baza unui identificator tipăribil (QR, barcode) care este primit pentru fiecare tranzacție.*

IV. Trasabilitate administrativă digitală

În atenția:

Agenției pentru Digitalizarea României

Ministerului Comunicațiilor și Societății Informaționale

Arhitecturi de referință pentru toate proiectele de IT achiziționate sau comandate de către sectorul public

Măsuri concrete

- Punerea la dispoziție a unui set minim de cerințe, specificații minimale și standarde minim-acceptabile din punct de vedere IT, cel puțin pentru următoarele aspect
 - Recomandare soluții standardizate
 - Arhitectura de securitate
 - Arhitectura de date
 - Arhitectura
- Realizarea a câte unui model funcțional pentru aplicații destinate unui scop, cu cod open source și folosind tehnologii open source.
- Publicarea și întreținerea unui plan multi-anual de implementări, împreună cu
- Publicarea unui catalog cu soluții comerciale și open source care sunt agreate și recomandate pentru anumite scopuri administrative comune:
 - ERP (Enterprise Resource Planning - Gestiunea Resurselor Organizaționale), incluzând contabilitate, stocuri, personal, registratură
 -
- Descrierea interfeței dorite a funcționalităților oricărei aplicații comandate într-un standard open source, cum ar fi OpenAPI sau GraphQL. Acest standard de specificare trebuie să asigure minim scrierea automată a codului de interfață în majoritatea limbajelor de programare de referință, pentru facilitarea transparenței între furnizori și pentru păstrarea coerența cerințelor între versiuni diferite sau implementări diferite ale aceluiași serviciu.
- Consolidarea unui registru public digital de specificații în format OpenAPI sau GraphQL, care să permită reutilizarea specificațiilor realizate în proiecte identice, similare sau înrudite.

Registru de evidență inter-instituțional, automat auditabil

Propuneri concrete

1. Blockchain inter-instituțional, dublu-criptat, eventual folosind tehnologie de tip Blockstack

2. Sistem de validare si micro-audit local, inter-institutional si/sau inter-regional in cadrul aceleiasi institutii, prin expunerea aceluiasi caz mai multor agenti (care au acelasi nivel de securitate)

4. Legislativ: reducerea folosirii canalelor nesecurizate, neauditabile sau pentru transmiterea informațiilor confidențiale, a datelor cu caracter personal ale cetățenilor (inclusiv date biometrice sau fotografii) sau a informațiilor cu caracter secret. Încurajarea folosirii mijloacelor securizate, autentificante și auditabile pentru comunicarea și confirmarea aprobărilor, deciziilor, constatărilor ordinelor de lucru (de serviciu) sau a altor bunuri informaționale relevante și în mod uzual necesare pentru îndeplinirea responsabilităților fiecărei funcții, la nivel intra-instituțional și inter-instituțional.

Sistem agreat de administrația centrală pentru preluarea din teritoriu, de la cetățeni a dovezilor video-fotografice pentru probleme raportate.

Eficientizarea comunicării între cetățean și autorități, locale sau centrale, este sub imperativul digitalizării, pentru asigurarea unui nivel de eficiență compatibil cu economia europeană și globală. Mai mult, este necesar ca în mod automat, fără a solicita intervenție umană, calitatea serviciilor prestate în teritoriu să fie vizibilă tuturor actorilor deopotrivă, atât la nivel central cât și local. În plus, implementarea unui ecosistem cu catalog comun de scheme de integrare (API-“Application Programming Interface”)

Garantarea integrității custodiale a dovezilor colectate prin mijloace criptografice de moderne.

Propunere concretă

- Aplicație compatibilă cu telefoane mobile Android și iOS, de tip progressive web app, prin intermediul căreia cetățenii pot raporta probleme locale sau regionale, încărcând media audio, video sau documente scanate.
- Starea statistică a cererilor se raportează public și periodic, pe circumscripții relevante, incluzând distribuția statistică a duratelor de rezolvare.
- Utilizatori au de ales între a se autentifica și a raporta anonim. Raportările anonime se tratează/analizează doar după ce sunt epuizate raportările autentificate.
- Abuzul reptat se penalizează
- Interoperabilitatea datelor la nivel județean și național prin standardizarea lor în format Open API sau GraphQL

Modele de referință:

<http://primariasector1.ro/sesizari-petitii-reclamatii.html>

Digitalizarea serviciilor de protecție a consumatorului, printr-o aplicație de recunoașterea etichetelor folosind inteligență artificială,

Propunere concretă

Ținerea unei evidențe rapide și corecte a tipurilor de alimente pe care le consumăm este un imperativ al unei diete sănătoase. Pentru a veni în întâmpinarea nevoilor consumatorilor într-o perioadă în care alegerile de consum devin tot mai dificile.

Note de final

Suntem un grup de profesioniști, cu experiență în mediul IT, atât din punct de vedere tehnic, comercial, economic, dar și juridic, care își folosesc cunoștințele și priceperea pentru a ajuta factorii legislativi și executivi, fără preferințe sau parti-pris-uri politice, să găsească noi formulări pentru provocările și soluțiile aduse de revoluția tehnologică a digitalizării, inteligenței artificiale și a sistemelor larg-distribuite.

Vă cerem ajutorul pentru a cârmui efortul și intențiile noastre de a consolida fundația României digitale a deceniului 2020-2030.



<https://deepviss.org>

Deep Vision