

Smart (Re)Evolution: Dezvoltarea ecosistemelor de date și servicii din administrația publică

Costel CIUCHI

*Prof. Asoc., Facultatea de Electronică, Telecomunicații și Tehnologia Informației,
Universitatea Politehnica din București, România*

costel.ciuchi@gmail.com

Eduard MITITELU

*Masterand, Facultatea de Electronică, Telecomunicații și Tehnologia Informației,
Universitatea Politehnica din București, România*

eduard.mititelu@gmail.com

Bogdan ROȘAN

Masterand, Facultatea de Drept, Universitatea București, România

bogdan.rosan13@gmail.com

Sabina-Daniela AXINTE

*Doctorand, Facultatea de Electronică, Telecomunicații și Tehnologia Informației,
Universitatea Politehnica din București, România*

axinte_sabina@yahoo.com

Abstract

Adoptarea unor mecanisme bazate pe performanță și eficiență în domeniul digital necesită luarea în considerare a 3 provocări: actualizarea periodică a sistemelor informatice (hardware și software), monitorizarea deficitului de competențe profesionale în domeniu și asigurarea securității serviciilor/datelor prin modularizarea sistemelor și identificarea eventualelor blocaje (analize de risc - reziliență) pentru creșterea încrederii. Instituțiile guvernamentale utilizează modele rigide și fragmentate de proprietate

organizațională a datelor și se confruntă cu probleme curente cum ar fi: date offline, infrastructură IT închisă și lipsa abilităților analitice, toate acestea fiind un impediment în dezvoltarea capacităților de a crea servicii bazate pe date. Instituțiile publice utilizează prea puțin abilitățile practice și experiența celor cărora le oferă servicii. Modelele de succes și experiența din mediul privat privind capacitatea de adaptare și transformare utilizând noile tehnologii reprezintă obiective ce trebuie adoptate la nivelul statului la nivel central și local. Obiectivul articolului constă în posibilitatea dezvoltării unui model de guvernare inteligentă ca fundament al conceptului de smart-state, prin analiza a patru piloni de interacțiune privind provocările societății digitale: transparență, implicarea cetățenilor, schimb de informații (interoperabilitate instituțională) și securitate cibernetică (reziliență). Modelul dezvoltat prezintă un ansamblu de direcții necesare a fi implicate în dezvoltarea unui ecosistem colaborativ: resursele umane, cadrul legislativ național/instituțional și tehnologia. Evoluția structurală a instituțiilor publice nu trebuie să se concentreze doar pe evoluția tehnologică. Asigurarea unui cadru legislativ, managerial și operațional coerent reprezintă, cu precădere pentru factorii decizionali, elemente indispensabile în asigurarea unei bune guvernări. Diversitatea și particularitățile fluxurilor administrative complexe de la nivelul unei administrații guvernamentale necesită o abordare managerială integrată ce trebuie să cuprindă, pe lângă măsurile tehnice care trebuie adoptate în dezvoltarea serviciilor electronice, o serie de măsuri juridico-administrative care să asigure un cadru managerial și operațional coerent și practic.

Cuvinte cheie: *e-government, guvernare participativă, smart-administration, smart-state, fluxuri administrative.*

1. Introducere

În 2050, la nivel european, se preconizează că două treimi din populație va locui în orașe și va consuma 70% din energia disponibilă [1]. Astfel, pornind de la această predicție, se observă necesitatea de a dezvolta conceptul de Smart Cities nu numai din punct de vedere urbanistic, cât și digital. Printre prioritățile necesare a fi luate în considerare se regăsesc infrastructura digitală și mai ales necesitatea de a se asigura interoperabilitatea încă din faza de design a sistemelor dedicate Smart Cities. Abordarea „*interoperability by design*” este necesară deoarece acest concept necesită o colaborare optimă (bazată pe schimb de date și informații în timp real) între administrația publică, mediul economic local, organizațiile non-guvernamentale sau grupurile de inițiativă cetățenești non-formale la nivel local. De asemenea, conceptul de interoperabilitate este parte a unui eco-sistem național / internațional prin necesitatea interconectării structurilor administrației publice naționale europene, dar și a altor factori implicați în conceptul de Smart Cities. În ceea ce privește interconectarea sistemelor care deservește orașe inteligente, la nivel european s-a conturat inițiativa CoP-CITIES [2], care își propune un schimb de expertiză între diversele forme de abordare a conceptului Smart Cities, dar și dezvoltarea unor metode eficiente de interconectare digitală.

O digitalizare de succes a unei administrații publice presupune evoluția tuturor factorilor implicați la nivelul unei comunități: instituții publice locale, mediul privat local, dar și administrațiile centrale. În acest sens, evoluția accelerată a domeniului smart cities, susținut de o dezvoltare a componentei digitale este necesară adoptarea unui cadru legal articulat, dar și pregătirea unor resurse umane, tehnice și tehnologice pentru a parcurge cu succes toate etapele unui produs digital de tip Smart City.

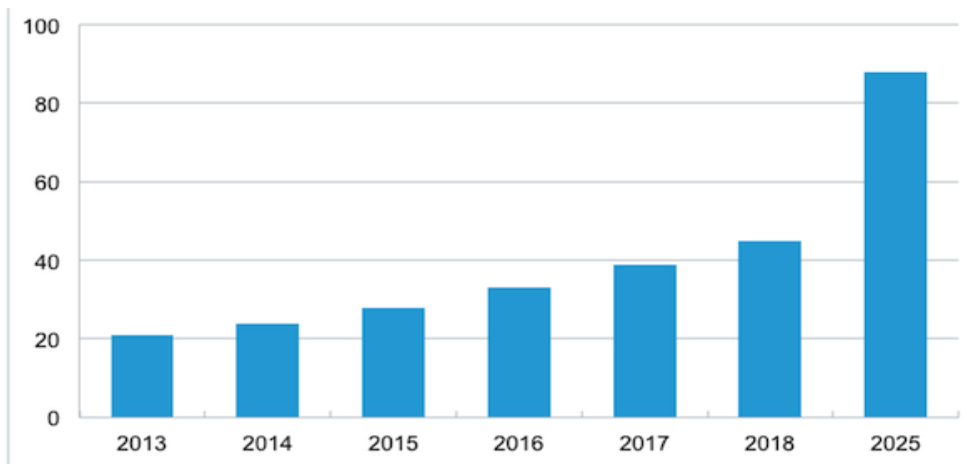


Figura 1. Evoluția numărului de Smart Cities la nivel internațional conform standardelor IHS Technology [3]

Deși conceptul de Smart Cities se concentrează în principal pe tehnologie și soluții tehnice, apare din ce în ce mai concretă ideea conform căreia implementarea unei agende a orașelor inteligente este mai probabil să aibă succes dacă este integrată într-o strategie mai largă de dezvoltare durabilă[4]. În acest context, analiza cadrului legislativ este imperioasă pentru a cunoaște care sunt, *de plano*, problemele pe care le ridică dezvoltarea de Smart Cities, în special în ceea ce privește mecanismele de colectare, utilizare și comunicare a datelor cu caracter personal și conformarea cu directivele europene privind e-privacy și securitatea cibernetică.

2. E-GOV - Analiza cadrului legislativ

Interoperabilitatea în cadrul unui Smart City trebuie să aibă ca punct de plecare un cadru legislativ coerent și flexibil, care să protejeze cetățenii de eventualele efecte negative prin atingeri aduse dreptului la viață privată, posibil a fi generate de potențiale dezvoltări eronate a interconectărilor și de publicarea accidentală a bazelor de date cu potențial vătămător.

În consecință, cadrul legislativ trebuie să fie conceput de asemenea natură încât să ofere mijloacele juridice necesare implementării unor mecanisme specifice de protecție a datelor cu caracter personal și, *in concreto*, să excludă posibilitatea

încălcării unor drepturi fundamentale. Este adevărat că infrastructura legislativă europeană permite asigurarea unei minime protecții a drepturilor și libertăților fundamentale, prin efectul infralegislativ al Regulamentelor și Directivelor, care au aplicabilitate directă în dreptul intern al statelor membre. Cu toate acestea, principiul *nemo censetur ignorare legem* (nimeni nu se poate prevala de necunoașterea legii) rămâne la nivel de deziderat, în contextul evoluției tehnologiilor și al accesibilității crescute a mediului Internet. Astfel, cel puțin în contextul în care se regăsește România, puterea legiuitoare ar trebui să manifeste mai mult interes în ceea ce privește transpunerea normelor europene în dreptul intern, pentru o mai bună adaptabilitate și personalizare a normelor proteguitoare la necesitățile concrete ale vieții sociale românești.

Începând cu data de 25 mai 2018 a intrat în vigoare Regulamentul (UE) 2016/679, cunoscut mai bine sub acronimul GDPR - General Data Protection Regulation, preluat și în legislația română prin Legea nr. 190/2018. Însă chiar din denumirea acestui Regulament se poate observa că reprezintă un set de reguli generale, instituind măsuri minime de ocrotire a datelor cu caracter personal. Regulamentul nu vizează doar actorii din domeniul privat care sunt operatori de date cu caracter personal, fiind aplicabil și domeniului public, autoritățile publice având la rândul lor obligații specifice GDPR, uneori chiar diferite de cele ale entităților private, în administrația publică responsabilitatea fiind mult mai accentuată.

Urmând principiile impuse de Regulamentul 2016/679, cadrul legislativ privind protecția datelor cu caracter personal trebuie să cunoască adaptări la specificul fiecărui domeniu de activitate, în speță în ceea ce privește modalitatea de interconectare a bazelor de date și fluxul de informații dintre operatorii privați și instituțiile publice, doar astfel putându-se ajunge la o veritabilă protecția a drepturilor fundamentale. Mai mult decât atât, este foarte important să reținem că aceste date esențiale pentru funcționarea unui oraș de tip Smart, date care pot fi cu caracter personal, nu sunt deținute doar de către autorități publice. Astfel, asemenea date se află în gestionarea unor operatori de furnizare a unor servicii publice locale, așa-numitele stabilimente de utilitate publică: furnizori de apă, gaz, curent, servicii de salubritate, transport public local sau chiar operatori *stricto sensu* privați - de exemplu, servicii de telecomunicații. În acest context a apărut noțiunea de „date de interes general” [5], reglementată deja în Franța în așa numita Lege a Republicii Digitale intrată în vigoare încă din data de 7 octombrie 2016, lege care în esență reglementează mecanisme de garantare a confidențialității și securității datelor pe care titularul trebuie să le pună la dispoziția autorităților ori la dispoziția operatorilor de servicii publice delegate.

Cu toate că problema datelor cu caracter personal este cea mai sensibilă, aceasta nu reprezintă singura problemă cu implicații legale în ceea ce privește modalitatea de reglementare a dezvoltării de Smart Cities. Având în vedere faptul că orașele de tip Smart se fundamentează pe o eficientă conlucrare a autorităților publice cu domeniul privat, se pot naște o serie de inconveniente în ceea ce privește relațiile contractuale, în legătură cu licitațiile publice, achizițiile directe, contracte de concesiune, contracte de parteneriat public-privat sau chiar contracte de drept

privat pur (unde și autoritățile publice acționează ca un operator privat). Problemele care pot apărea sunt derivate din natura interconectată a infrastructurii orașelor de tip Smart care, pentru a-și asigura o gestionare și o productivitate coerentă, va necesita o mai bună adaptare a relațiilor contractuale ce presupun implicare multipartită și o perioadă contractuală îndelungată.

De asemenea, o atenție deosebită va trebui acordată și modalității de planificare a orașelor de tip Smart, în special asupra regulilor de urbanism și a autorizațiilor de construire care vor trebui remodelate pentru a răspunde necesităților unui oraș de acest fel, care implică o multitudine de preocupări și de constrângeri ce necesită a fi antamate concomitent. În acest sens facem referire la necesitatea asigurării securității și confidențialității tehnologiilor în continuă schimbare, la tranziția energetică de la modalități tradiționale la cele inovative și performante, la supravegherea și îmbunătățirea traficului rutier prin gestionarea acestuia în vederea fluidizării zonelor urbane supraaglomerate.

În final, și legile de organizare și funcționare a administrațiilor publice locale trebuie adaptate pentru a găsi noi modalități de articulare a relației dintre instituțiile publice locale, cu resursele sale și cetățenii informați și conectați la viața de interes general, pe de o parte, și sectorul privat care va juca un rol primordial în construirea și dezvoltarea *de facto* a orașelor de tip Smart, pe de altă parte.

În acest sens, se observă că o colaborare dintre sectorul public și cel privat este absolut esențială pentru dezvoltarea armonioasă de Smart Cities, însă se impune a stabili dacă și în ce măsură se poate realiza o procesare în masă a unor date cu caracter personal și, mai mult, în ce măsură aceste date pot fi transferate pentru a deservi operațiunilor specifice ale Smart Cities. Astfel, din analiza reglementării europene în materie, dar și a legislației naționale, în principiu un asemenea transfer de date este permis, însă în anumite condiții [6].

Astfel, prelucrarea datelor cu caracter personal poate fi realizată, atât de către instituții publice, cât și de către operatori privați, însă, în primul rând, trebuie avut în vedere ce fel de date sunt exceptate de la prelucrare, spre exemplu cele care se referă la: origine rasială ori etnică, convingeri politice, orientare sexuală, apartenență sindicală ș.a. În al doilea rând, trebuie ca prelucrarea de date să aibă un scop bine determinat, serios și legitim, procedura de procesare a datelor trebuie să fie corectă și transparentă, iar procesarea trebuie să se limiteze doar la acele date care sunt indispensabile. În al treilea rând, trebuie respectate anumite proceduri și mecanisme de siguranță și trebuie oferite o serie de garanții care să protejeze integritatea și securitatea datelor cu caracter personal, astfel încât scopul operatorului de date cu caracter personal să fie atins, iar atingerea drepturilor persoanelor să fie minimă ori chiar inexistentă.

Nu în ultimul rând, trebuie respectate anumite condiții pentru prelucrarea datelor cu caracter personal, printre care se numără, într-adevăr necumulativ, interesul public, interesul legitim ori consimțământul persoanei. Din această perspectivă, este cert că la nivel legislativ pot fi implementate o serie de măsuri care să vizeze punerea în aplicare a unor servicii de tip Smart Cities pe considerentul acționării în interes public, ceea ce *de plano* presupune și un interes legitim. Astfel, prelucrarea de date cu caracter personal și transferarea ori comunicarea acestora

către alți operatori, pentru îndeplinirea unui scop comun și de interes general, este permisă în măsura în care se respectă cerințele legale și se oferă garanțiile necesare pentru protejarea acestor date.

3. Modelarea cadrului instituțional național

Cadrul instituțional pentru dezvoltarea Smart City trebuie să se bazeze pe 4 piloni principali: transparență, implicarea cetățenilor, schimb de informații (interoperabilitate instituțională) și securitate cibernetică (reziliență). Transparența presupune, într-un cadru general, cunoașterea de către societate a motivelor, faptelor, logicii și a bazei ce stau la baza deciziilor factorilor decidenți. Într-un Smart City, transparența trebuie să reprezinte o prioritate, atât pentru deciziile luate la nivelul comunității, cât și pentru modul de operare a datelor cetățenilor. Instrumentele ce oferă informațiile privind aspectele de transparență locală, națională și europeană trebuie să fie ușor accesibile cetățenilor.

Un oraș inteligent în primul rând este un oraș al cetățenilor, de aceea este necesară o implicare proactivă a acestora în viața comunității. Pentru a avea această implicare, în primul rând cetățenii au nevoie de instrumentele necesare pentru a fi parte activă în societate. Un astfel de instrument, ce îmbină implicarea cetățenilor cu transparența decizională, o reprezintă conceptul de bugetare participativă, ce se poate vedea implementat în Cluj-Napoca, Sibiu și Făgăraș, unde cetățenii pot propune și vota proiecte locale ce să fie bugetate și astfel realizate.

Schimbul de informații reprezintă o prioritate în primul rând pentru facilitarea unui acces ușor și rapid al cetățenilor la serviciile publice; acestea trebuie să aibă cursivitate și simplitate în utilizare astfel încât cetățenii să aibă cât mai puține fluxuri administrative de urmat pentru obținerea de documente sau informații din partea statului, dar și a mediului privat. Acest schimb de informații trebuie însă să respecte interesul cetățeanului privind stocarea și utilizarea datelor sale personale.

Securitatea cibernetică reprezintă un ansamblu complex de măsuri proactive și reactive care au drept scop asigurarea confidențialității, a integrității, autenticității, dar și evitarea răspândirii necontrolate a informațiilor în format electronic, care poate afecta în mod ireparabil resursele și serviciile publice ori private din spațiul cibernetic. Spațiul virtual a ajuns un element constant integrant al vieții personale. Noile tehnologii, infrastructurile cibernetice și conținuturile informaționale trebuie să beneficieze de un grad ridicat de protecție, deoarece acestea implică riscuri care pot afecta grav sau iremediabil fie la nivel de individ, fie întreaga entitatea ce gestionează aceste informații, în condițiile în care există numeroase acțiuni ostile desfășurate în spațiul cibernetic care vizează disponibilitatea, integritatea și funcționarea sistemelor informatice.

La nivelul legislației comunitare în materie de securitate cibernetică, în luna iulie 2016 a fost adoptată Directiva (UE) 1148/2016 [7] și care a fost transpusă și în legislația internă prin Legea nr. 362/2018. Acest cadru legislativ este deosebit de important deoarece aliniaza reglementarea internă la cadrul european comun de

răspuns la incidente de securitate cibernetică. Această nouă reglementare legislativă vizează asigurarea securității rețelelor și sistemelor informatice ce servesc unor activități esențiale pentru societatea și economia statului, vizând în special domenii de interes național precum: infrastructuri digitale, transporturi, sănătate sau energie. *In concreto*, această reglementare stabilește mecanisme de prevenție, detecție, dar și de reacție împotriva unor incidente ciberneticе astfel încât impactul acestora să fie minim pentru societate și economia națională.

4. Aplicații inteligente. Digitalizarea administrației publice

La nivel internațional se observă o perspectivă de încurajare a inițiativelor Smart City ce provin mediul privat, mediul academic, organizații non-guvernamentale sau din partea unor grupuri civice. Un exemplu de bună practică îl constituie colaborarea între autoritățile publice din Toronto și Sidewalk Labs (parte a Alphabet Inc., grup cunoscut mai ales pentru asocierea cu compania Google), ce își propune dezvoltarea inteligentă urbană a unui district din orașul Toronto. Această inițiativă poate fi considerată una de succes, pentru că presupune deschiderea unui mediu colaborativ pentru dezvoltarea conceptului de Smart City în acel district, prin organizarea de workshop-uri, spații de discuții online, aplicații tip open-source, cadre de dezbateră complexe, atât tehnice, juridice și economice a propunerilor de dezvoltare a conceptului. Această procedură de lucru evidențiază și pune în centrul conceptului de Smart City colaborarea între toți factorii implicați în viața unei urbe. Această inițiativă reiterează constant ideea în spațiul public că un Smart City nu presupune doar dezvoltarea de aplicații inteligente pentru un oraș, ci ansamblul de elemente componente (sistemizare urbanistică și a construcțiilor, îmbunătățirea sistemelor de transport, mecanismelor de întreținere și igienizare a unui oraș), prin intermediul unor modalități de optimizare și eficientizare cu ajutorul datelor și informațiilor care provin din utilizarea tehnologiilor din IT&C.

Una dintre cele mai interesante propuneri este un sistem de colectare eficientă a deșeurilor printr-un mecanism subteran de transport al acestora, ce presupune suport uman, dar mai ales utilizarea unor roboți. Această inițiativă va duce la o sistem de colectare mult mai bun, dar și la descongestionarea traficului, asigurând un trafic rutier fluid în cadrul districtului. Autorii acestui proiect și-au definit din start 5 piloni: diversitate, accesibilitate, servicii financiare ușor de accesat, echitate în oportunități și incluziune [8]. Previziunile economice așteptate pentru anul 2040 pe baza acestui proiect sunt: 44.000 locuri de muncă full-time (93.000 de locuri de muncă în total), un produs intern brut anual de 14,2 miliarde de dolari, taxe încasate de 4,3 miliarde de dolari, un hub global pentru inovație urbană.

Un alt aspect important în dezvoltarea unui Smart City este conceptul Small Data, care constituie posibilitatea de a reprezenta datele colectate și modelate pentru obiective specifice. Necesitatea principală în cadrul unui Smart City pe modelul de Small Data este reprezentat de optimizarea fluxurilor administrative pentru a exista un echilibru între, pe de o parte, creșterea securității și combaterea criminalității și a terorismului și, pe de altă parte, protecția vieții private și a datelor cu caracter personal. Small Data reprezintă unul dintre pilonii principali în

dezvoltarea comunităților Smart City, mai ales pentru rolul său în analiza vieții publice a comunității. Unul dintre pionierii analizei acestui aspect este Jan Gehl; prin studiile sale din Danemarca, acesta a dovedit că nivelul de accesibilitate a cetățenilor către serviciile publice este direct proporțional cu succesul unui oraș inteligent. De asemenea, în cadrul Institutului Gehl sunt dezvoltate constant instrumente pentru analiza vieții publice a comunității, cât și pentru analiza spațiilor publice. Astfel de instrumente reprezintă elemente ce necesită a fi utilizate constant de către comunitățile locale și trebuie să reprezinte o prioritate în procesul de digitalizare a unui Smart City.

Un alt factor ce va duce la evoluția orașelor tradiționale către Smart Cities este tehnologia 5G, ce presupune viteze mult mai ridicate decât tehnologia 4G și care va avea ca efect eliminarea rețelele clasice de cabluri pentru conectarea la Internet. Tehnologia 5G „poate include frecvențe mai mici, de la 600 MHz la 6 GHz. Cu toate acestea, vitezele în aceste frecvențe joase sunt cu mult mai mici decât sistemele noi 4G, estimate de la 15% până la 50% mai rapid” [9].

La nivel european, Comisia Europeană susține o inițiativă publică-privată [10] pentru infrastructura 5G, ce își propune:

- furnizarea unei capacități de acoperire a rețelelor wireless și a unor servicii publice variate de 1.000 ori mai bune decât cele din 2010;
- eficientizarea cu 90% a consumului de energie necesar furnizării de servicii, cu un focus principal pe rețelele de comunicațiile mobile unde consumul de energie dominant vine de la accesul la rețele radio;
- reducerea timpului mediu de creație a unui serviciu de la 90 de ore la 90 de minute;
- crearea unui mediu Internet sigur, de încredere, cu un downtime minim (aproape de zero) pentru furnizarea de servicii;
- facilitarea unei implementări foarte dense de legături de comunicații wireless ce să conecteze numeroase dispozitive wireless (de ordinul trilioanelor), utilizate de peste 7 miliarde de oameni;
- asigurarea unui panou mai larg de servicii și aplicații la costuri mai mici pentru toți cetățenii.

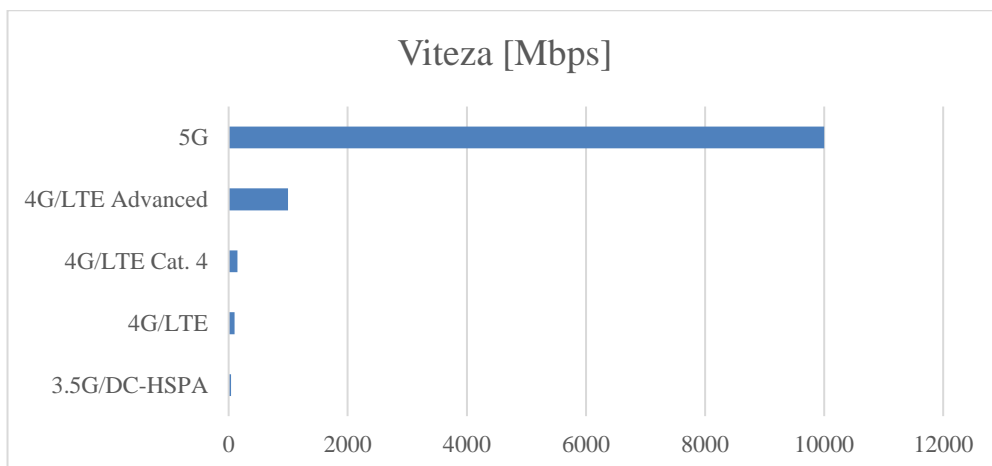


Figura 2. Evoluția vitezelor de operare în tehnologiile de telecomunicații

La nivel național, pornind de la datele deschise ale autorităților centrale, furnizate prin portalul data.gov.ro [11], au fost dezvoltate proiecte private și publice, ce reutilizează seturile de date ale instituțiilor publice. Printre acestea merită a fi amintite:

- meserii.ro - hartă interactivă a învățământului profesional și tehnic din România, care conectează meseriile pregătite în școală cu potențialul de cerere pe piața muncii și utilizează 6 seturi de date;
- termene.ro - vizualizări și selecții interactive ale contribuabililor cu datorii la cele 4 bugete, contracte, cumpărări directe SEAP etc.;
- VisitRo - oferă informații despre toate monumentele istorice din lista oficială publicată de Ministerul Culturii în 2015.

Una dintre problemele tehnice prezente în actualele sisteme informatice ale administrației publice locale și centrale este cea a interconectării bazelor de date. Această problemă provine de la faptul că sistemele informatice sunt construite pe diverse tipuri de baze de date, cât și cu tehnologii back-end diferite. Diversitatea tehnologiilor este o caracteristică necesară a fi eficient exploatată prin dezvoltarea de tehnologii tip magistrală de publicare a datelor (API-uri). Pentru a rezolva această problemă este necesară o soluție tehnică care să transpună datele din orice bază de date într-un format universal acceptat și care să le transmită într-un mod rapid și eficient. O soluție viabilă este STRAPI [12], proiect ce își propune transpunerea datelor în format JSON și livrarea acestora către orice aplicație prin API. Prin acest mecanism se pot interconecta noile aplicații ale mediului public sau privat la aplicații mai vechi, care funcționează în cadrul administrației publice.

Un aspect important al proiectelor actuale aflate în diverse stadii de implementare este reprezentat de aspecte care țin de securitate cibernetică. Manipularea datelor, intoxicarea factorilor decizionali și acțiunile de influențare a opiniei publice prin diverse metode persuasive reprezintă provocări care trebuie avute în vedere la dezvoltarea sistemelor complexe din cadrul Smart Cities. Particularitățile unei zone (unui oraș), obiceiurile specifice regiunii și

comportamentul locuitorilor sunt elemente necesar a fi luate în considerare în vederea asigurării unei abordări complexe și complete a fenomenului.

5. Testarea și validarea aplicațiilor software

Ultima decadă a reprezentat un salt uriaș atât în domeniul hardware, cât și software. Echipamentele coordonate de micro-controllere și microprocesoare sunt disponibile în orice industrie, fie că discutăm despre domeniul financiar-bancar, sănătate, transporturi, IT&C sau sisteme de mare răspundere funcțională. Funcționalitățile și managementul general al acestor echipamente sunt controlate prin software, local sau la distanță, iar operarea corectă a acestor echipamente, esențiale în cadrul conceptului Smart City, depinde în mare măsură de fiabilitatea sistemelor informaționale.

Calitatea a devenit unui din factorii determinanți în atingerea succesului în orice domeniu. Multe companii au recunoscut această dependență de produse software și depun eforturi pentru îmbunătățirea calității și a proceselor de dezvoltare a acestora. O modalitate de a realiza acest obiectiv este evaluarea sistematică și testarea software-ului. Testarea software reprezintă o investigație empirică realizată cu scopul de a oferi părților interesate informații referitoare la calitatea produsului sau serviciului supus testării, luând în considerare contextul operațional în care acesta din urmă va fi folosit. Testarea software mai poate fi definită ca un proces de validare și verificare a faptului că un program/aplicație/produs software corespunde cerințelor business-ului și cerințelor tehnice care au ghidat proiectarea și implementarea lui; rulează și se comportă corespunzător așteptărilor [13].

Funcțiile pe care trebuie să le îndeplinească un sistem, un subsistem sau o componentă pot fi descrise ca o specificație a cerințelor, cazuri de utilizare sau o specificație funcțională sau pot să fie nedocumentate. Testele funcționale se bazează pe funcții și caracteristici (descrise în documente sau înțelese de către testerii) și interoperabilitatea lor cu anumite sisteme și pot fi efectuate la toate nivelurile de testare (de exemplu, testele pentru componente pot fi bazate pe o specificație a componentelor). Un tip de testare funcțională, cum ar fi testarea securității, investighează funcțiile (de exemplu, un firewall) care au ca scop detectarea amenințărilor, cum ar fi aplicațiile malițioase. Un alt tip de testare funcțională, interoperabilitatea, evaluează capacitatea produsului software de a interacționa cu unul sau mai multe componente sau sisteme specificate.

Testarea non-funcțională include, dar nu se limitează la, testarea performanței, testarea sarcinii, testarea de stres, testarea utilizabilității, testarea mentenabilității, testarea fiabilității și testarea portabilității. Testarea non-funcțională poate fi efectuată la toate nivelurile de testare. Termenul de testare non-funcțională descrie testele necesare pentru măsurarea caracteristicilor sistemelor și a software-ului, care pot fi cuantificate pe o scară variabilă, cum ar fi timpii de răspuns pentru testarea performanțelor. Aceste teste pot fi raportate la un model de calitate, cum este cel definit în "Software Engineering - Product Quality" (ISO 9126) [14].

Principalul obiectiv al aplicațiilor dezvoltate pentru Smart Cities este de dezvolta produse și servicii inovatoare de înaltă calitate la un preț competitiv pentru clienții săi. Acest lucru necesită o viziune clară asupra domeniului de afaceri, a inovațiilor și a calității produselor. În aceste zile, clienții au așteptări foarte mari privind calitatea și fiabilitatea produselor software ceea ce dă o importanță deosebită etapei de testare. Testarea în conformitate cu standardele de calitate pot asigura dezvoltarea unor sisteme și aplicații informatice conforme cu necesitățile Smart Cities.

6. Concluzii

Pentru o bună dezvoltare a Smart Cities la nivel european este nevoie de o legislație piramidală care să aibă în vârf autoritățile locale și care să ofere un echilibru între privacy-ul cetățenilor și o interconectare eficientă pentru schimbul date între autorități și mediul privat care furnizează servicii digitale pentru cetățean. În România, dar și la nivel european, necesitatea operaționalizării mecanismelor de parteneriat public-privat la nivelul comunităților locale este prioritară deoarece cetățenii trebuie să beneficieze de servicii din ambele medii, iar acestea trebuie să ofere cel puțin aceleași standarde de calitate și eficiență.

Considerăm că o atitudine proactivă în vederea dezvoltării de Smart Cities se impune cu precădere, iar inițiativa va trebui preluată de la nivel central prin elaborarea de acte normative de tip descentralizat, care să conțină direcțiile și principiile normative în domeniu pentru a oferi și asigura o mai bună adaptare a fiecărei unități administrative în parte, astfel încât să răspundă exigențelor personalizate ale fiecăreia, iar în domeniile în care deja există o reglementare trebuie realizate amendamente care să fie în acord cu specificul orașelor de tip Smart. Un climat bazat pe încredere rămâne indispensabil pentru consolidarea rezilienței cibernetice generale, de aceea îmbunătățirea cooperării, a coordonării și a schimbului de informații între sectorul public și cel privat trebuie să fie scopul imediat al oricăror reglementări în materie de securitate cibernetică. Dezvoltarea competențelor și a gradului de conștientizare reprezintă elemente esențiale care trebuie să preocupe toate sectoarele societății, în condițiile în care, la nivel mondial există un deficit de competențe în acest domeniu [15]. Modelarea proceselor necesită luarea în considerare a elementelor sociale și juridice, nu numai componenta tehnologică. De altfel, abordarea trans-disciplinară a domeniului Smart Cities poate asigura o baza solidă pentru elaborarea și consolidarea unui concept integrat comun care să corespundă cu așteptările și condițiile unei comunități.

Bibliografie

- [1] European Commission, Smart Cities - Smart Living, <https://ec.europa.eu/digital-single-market/en/smart-cities>.
- [2] European Commission, CoP on CITIES, <https://ec.europa.eu/jrc/communities/en/community/2421/about>.

- [3] Smart Cities to Rise Fourfold in Number from 2013 to 2025, <https://technology.ihc.com/507030/smart-cities-to-rise-fourfold-in-number-from-2013-to-2025>
- [4] Strategia națională pentru dezvoltarea durabilă a României 2030, <http://dezvoltaredurabila.gov.ro/>.
- [5] Geffray, E., Auby, J.B., *The political and legal consequences of smart cities*, Field Actions Science Reports, Special Issue 16 | 2017, 11-15.
- [6] Europa ta - Uniunea Europeană, Protecția datelor în conformitate cu RGPD, https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_ro.htm.
- [7] Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune, <https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A32016L1148>.
- [8] Sidewalk Toronto, Planning for accessibility from the start, <https://medium.com/sidewalk-toronto/planning-for-accessibility-from-the-start-e7cea8552bc7>.
- [9] TELCOMA GLOBAL | 5G Technology Introduction. telcomaglobal.com.
- [10] European Commission, Towards 5G, <https://ec.europa.eu/digital-single-market/en/towards-5g>.
- [11] Seturi de date deschise, <https://data.gov.ro>.
- [12] Strapi - Open source, <https://strapi.io>.
- [13] Kaner, C., *Exploratory Testing*, Florida Institute of Technology, Quality Assurance Institute Worldwide Annual Software Testing Conference, Orlando, FL, November 2006.
- [14] Foundation Level Syllabus, International Software Testing Qualifications Board, <https://www.istqb.org/downloads/syllabi/foundation-level-syllabus.html>.
- [15] Curtea de Conturi Europeană, Provocări pentru o politică eficientă a UE în domeniul securității cibernetice, 2019, https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_RO.pdf.