REZUMAT

În ultima perioadă, transformarea digitală și securitatea cibernetică au devenit doi piloni fundamentali pentru succesul organizațiilor. Pe fondul unei creșteri constante a incidentelor de securitate cibernetică și al presiunii tot mai mari asupra companiilor de a adopta tehnologii digitale, organizațiile simt o nevoie tot mai acută de a explora în profunzime modul în care aceste două componente interacționează și influențează, în mod specific, rezultatele organizaționale. Deși literatura de specialitate existentă oferă perspective variate asupra conceptelor de securitate cibernetică și transformare digitală, impactul direct al acestor factori asupra performanței companiilor rămâne încă insuficient cercetat la nivel organizațional.

Prezenta teză de doctorat investighează relațiile complexe dintre transformarea digitală, securitatea cibernetică și performanța organizațională în cadrul companiilor private care își desfășoară activitatea în România, plasând analiza în contextul mai larg al cadrelor de reglementare europene și al relevanței emergente a analizei volumelor mari de date (Big Data analytics). Importanța acestei teme rezidă tocmai în abordarea unei lacune evidente din literatura de specialitate, oferind o analiză integrată a unor domenii tratate până acum preponderent în mod izolat. Pe măsură ce digitalizarea pătrunde tot mai mult în procesele, strategiile și modelele de afaceri ale organizațiilor, înțelegerea legăturii și a echilibrului dintre inovația tehnologică, securitatea informațiilor și conformitatea cu reglementările legale a devenit critică atât pentru mediul academic, cât și pentru cel profesional. Cercetarea este concepută pentru a oferi o perspectivă cuprinzătoare și interdisciplinară asupra modului în care inițiativele tehnologice și cele legate de securitate, atunci când sunt gestionate eficient și aliniate la cerințele de reglementare ale UE, pot spori reziliența organizațională, eficiența operațională și performanța strategică a companiilor.

Acest demers de cercetare doctorală este motivat de necesitatea de a dobândi o înțelegere mai profundă a impactului pe termen lung pe care deciziile tehnologice și cele legate de securitate îl au asupra performanței organizaționale. Transformarea digitală a devenit un motor al competitivității și sustenabilității organizaționale, incluzând adesea adoptarea unor tehnologii avansate, reproiectarea sau recalibrarea proceselor în interiorul afacerii și cultivarea unei culturi organizaționale orientate spre digitalizare și automatizări. Organizațiile care nu reușesc să integreze capabilitățile digitale riscă să devină irelevante pe piețele deja aflate într-o evoluție rapidă. Cu toate acestea, deși digitalizarea oferă oportunități nenumărate pentru o mai bună eficiență, un grad de inovare mai mare și o extindere mai amplă pe piață, aceasta crește în același timp un grad de risc, prin expunerea la amenințări cibernetice,

breșe de securitate a datelor sau chiar a unor perturbări operaționale. În acest context, securitatea cibernetică nu mai este o preocupare pur tehnică sau defensive, ci a devenit un facilitator strategic care protejează activele organizaționale, cultivă încrederea părților interesate și asigură continuitatea activității.

Mai mult, Uniunea Europeană, prin inițiative precum GDPR, NIS2 și DORA, a stabilit un mediu de reglementare complex la care organizațiile trebuie să se adapteze în timpul transformării digitale. Conformitatea cu aceste cadre nu implică doar obligații legale, ci modelează și procesul de luare a deciziilor strategice, guvernanța datelor și integrarea tehnologiilor emergente, cum ar fi cazul analizei volumelor mari de date (Big Data analytics). Prin urmare, această cercetare investighează modul în care transformarea digitală, practicile de securitate cibernetică, capabilitățile Big Data și conformitatea cu reglementările UE interacționează pentru a influența performanța organizațională, incluzând atât rezultate tangibile, cum ar fi performanțele financiare și operaționale, cât și rezultate intangibile, precum reputația, încrederea și capacitatea de inovare.

Arhitectura acestei cercetări este ghidată de cinci obiective fundamentale, interconectate structural, menite să ofere o perspectivă de ansamblu asupra fenomenelor studiate. Primul obiectiv vizează evaluarea riguroasă a impactului pe care inițiativele de transformare digitală îl exercită asupra performanței organizaționale globale. Cel de-al doilea urmărește determinarea influenței capabilităților de securitate cibernetică asupra rezilienței corporative și a rezultatelor operaționale. Ulterior, demersul se concentrează pe analizarea contribuției analizei Big Data în fundamentarea procesului decizional și în obținerea unui avantaj competitiv sustenabil. În cele din urmă, cercetarea examinează implicațiile strategice ale cadrelor de reglementare ale Uniunii Europene asupra politicilor digitale și de securitate, culminând cu dezvoltarea și validarea unui model integrat, capabil să explice mecanismele cauzale prin care acești factori interacționează în configurarea succesului în afaceri. Pentru a asigura rigoarea metodologică, aceste obiective generale sunt operaționalizate prin intermediul a trei întrebări centrale de cercetare, articulate în jurul unor nuclee tematice distincte. Prima întrebare explorează în ce măsură procesul de transformare digitală reconfigurează și solicită sistemele de apărare cibernetică ale organizațiilor. Cea de-a doua direcție de investigație evaluează impactul direct al investițiilor în securitatea informațională asupra indicatorilor de performanță organizațională. În fine, a treia întrebare vizează identificarea și ierarhizarea elementelor structurale esențiale pentru proiectarea unui cadru de securitate cibernetică rezilient și eficient, adaptat nevoilor specifice ale entităților aflate în plină tranziție tehnologică.

Fundamentul teoretic al acestei cercetări extrage perspective din mai multe arii ale literaturii de specialitate. Transformarea digitală este conceptualizată ca un proces socio-tehnic care integrează adoptarea tehnologiei cu strategia organizațională, optimizarea proceselor și schimbarea culturală. Perspectivele din faza calitativă au dezvăluit că, deși tehnologiile avansate, cum ar fi AI, IoT și analiza datelor, sunt centrale pentru eforturile de transformare, factorii umani, organizaționali și de reglementare sunt la fel de critici, confirmând că transformarea digitală este un fenomen strategic multidimensional. Securitatea cibernetică este poziționată atât ca un imperativ strategic, cât și operațional, care permite organizațiilor să gestioneze riscurile, să protejeze proprietatea intelectuală, să mențină reziliența operațională și să păstreze încrederea părților interesate. Securitatea cibernetică eficientă necesită măsuri de protecție tehnică, politici formale, mecanisme de răspuns la incidente și programe de conștientizare a angajaților. În contextul IMM-urilor, luarea deciziilor manageriale este influențată de constrângerile de resurse, de evoluția amenințărilor și de presiunile de reglementare. Analiza Big Data este încadrată ca un facilitator atât al transformării digitale, cât și al securității cibernetice, sprijinind luarea deciziilor în cunoștință de cauză, perspectivele predictive și gestionarea proactivă a riscurilor. Conformitatea cu reglementările, în special în contextul european, este tratată atât ca o constrângere, cât și ca o oportunitate, modelând comportamentul organizațional, managementul riscului și implementarea strategică a inițiativelor digitale. Modelul conceptual integrează aceste constructe, ipotetizând relații directe, indirecte și de mediere între transformarea digitală, securitatea cibernetică, Big Data, conformitatea UE și performanța organizațională.

Metodologic, studiul adoptă un design de cercetare de tip metode mixte (mixed-methods), care integrează tehnici de analiză calitativă și cantitativă pentru a oferi o înțelegere cuprinzătoare a fenomenelor investigate. Cercetarea începe cu o revizuire sistematică a literaturii academice, menită să clarifice fundamentele conceptuale ale transformării digitale, securității cibernetice și performanței organizaționale, precum și să identifice inconsistențele teoretice și relațiile insuficient explorate între aceste constructe. Această etapă este completată de o analiză bibliometrică realizată cu ajutorul VOSviewer, care mapează structura intelectuală a domeniilor de cercetare relevante. Rezultatele bibliometrice identifică temele de cercetare dominante, publicațiile influente și autorii de frunte, dezvăluind totodată evoluția interesului de cercetare și gradul de convergență în timp între studiile privind transformarea digitală și cele privind securitatea cibernetică. Cu toate acestea, ca o limitare inerentă, analiza bibliometrică s-a bazat în principal pe publicații indexate în Scopus, putând exclude contribuții relevante din surse non-engleze sau rapoarte industriale (white papers).

Etapa calitativă a studiului a implicat nouă interviuri semi-structurate aprofundate cu manageri și reprezentanți ai IMM-urilor din diferite sectoare economice. Participanții au fost selectați intenționat pe baza experienței lor profesionale, a expertizei în transformare digitală sau securitate cibernetică și a contextului organizațional, asigurând perspective diverse și o acoperire cuprinzătoare. Interviurile au fost realizate prin întâlniri față în față, conversații telefonice și corespondență prin e-mail (fapt ce constituie o limitare metodologică prin variația formatului de colectare), iar datele rezultate au fost analizate cu ajutorul ATLAS.ti pentru a identifica modele recurente, teme emergente și interrelații. Constatările calitative au indicat că transformarea digitală este recunoscută ca un fenomen multidimensional care implică adoptarea tehnologiei, optimizarea proceselor, leadership-ul strategic și adaptarea culturală. Managerii au subliniat rolul critic al măsurilor de securitate cibernetică și al conformității cu reglementările în implementarea cu succes a inițiativelor digitale, confirmând că transformarea digitală este un proces socio-tehnic și integrat strategic. Perspectivele derivate din această fază au fundamentat dezvoltarea instrumentului de sondaj cantitativ, operaționalizarea constructelor cheie și rafinarea modelului conceptual.

Etapa cantitativă a utilizat un chestionar structurat distribuit unui eșantion de 125 de companii private din România. Sondajul a surprins atât datele demografice ale respondenților și caracteristicile organizaționale, cât și măsuri privind transformarea digitală, practicile de securitate cibernetică, analiza Big Data, conformitatea cu reglementările UE și performanța organizațională. Constructele au fost operaționalizate folosind itemi reflectivi dezvoltați pe baza literaturii de specialitate și a perspectivelor calitative, asigurând validitatea de conținut și relevanța contextuală. Datele au fost analizate utilizând Modelarea prin Ecuații Structurale bazată pe cele mai Mici Pătrate Parțiale (PLS-SEM) în SmartPLS 4.0. Modelul de măsurare a fost evaluat riguros pentru fiabilitate și validitate utilizând indicatorul Alfa al lui Cronbach, Fiabilitatea Compozită (Composite Reliability), Varianța Medie Extrasă (AVE), criteriul Fornell-Larcker și raportul Heterotrait-Monotrait (HTMT). Toate constructele au demonstrat o consistență internă puternică, validitate convergentă și validitate discriminantă, susținând robustețea analizelor structurale ulterioare.

Pornind de la perspectivele oferite de analiza literaturii și cea bibliometrică, componenta empirică a cercetării examinează datele colectate de la un eșantion reprezentativ de companii dintr-o varietate de industrii, iar tehnici de analiză statistică sunt aplicate pentru a investiga relațiile dintre inițiativele de transformare digitală, practicile de securitate cibernetică și indicatorii de performanță organizațională. Rezultatele empirice demonstrează că transformarea digitală exercită o influență pozitivă semnificativă asupra performanței organizaționale atunci când este susținută de capabilități

adecvate de securitate cibernetică. Dimpotrivă, o maturitate insuficientă a securității cibernetice amplifică consecințele negative ale digitalizării, expunând organizațiile la perturbări operaționale, pierderi financiare și riscuri reputaționale. În același timp, constatările permit identificarea atât a beneficiilor, cât și a limitărilor transformării digitale în contextul cerințelor de securitate cibernetică și contribuie la validarea modelului propus. Rezultatele indică, de asemenea, că securitatea cibernetică joacă un rol de mediere și de moderare în relația dintre transformarea digitală și performanța organizațională. Organizațiile care integrează considerentele de securitate cibernetică în strategiile lor de transformare digitală obțin rezultate superioare de performanță și demonstrează o reziliență mai mare în fața amenințărilor cibernetice. Aceste constatări subliniază importanța alinierii inovației tehnologice cu cadre solide de guvernanță a securității.

Rezultatele calitative au indicat că transformarea digitală este recunoscută ca un fenomen multidimensional ce implică adoptarea tehnologiei, optimizarea proceselor, leadership-ul strategic și adaptarea culturală. Managerii au subliniat rolul critic al măsurilor de securitate cibernetică și al conformității cu reglementările în implementarea cu succes a inițiativelor digitale, confirmând că transformarea digitală este un proces socio-tehnic și încorporat strategic. Informațiile obținute în această etapă au fundamentat dezvoltarea instrumentului de sondaj cantitativ, operaționalizarea constructelor cheie și rafinarea modelului conceptual.

Rezultatele calitative consolidează aceste concluzii, arătând că organizațiile se confruntă cu diverse provocări și oportunități în implementarea inițiativelor de transformare digitală și securitate cibernetică. Factorii umani, organizaționali și de reglementare au fost subliniați în mod constant ca fiind esențiali pentru succes, tehnologia servind ca un facilitator și nu ca un motor izolat. Modelele observate în cadrul interviurilor au evidențiat atât convergență, cât și diversitate în perspectivele manageriale, reflectând diferențe de industrie, disponibilitate a resurselor și maturitate organizațională. Alături de dovezile cantitative, aceste rezultate oferă o înțelegere holistică a modului în care dimensiunile tehnologice, organizaționale și de reglementare interacționează pentru a modela rezultatele performanței în IMM-uri.

Rezultatele empirice demonstrează că inițiativele de transformare digitală generează un impact pozitiv semnificativ asupra performanței organizaționale, în timp ce practicile de securitate cibernetică îmbunătățesc în mod direct rezultatele performanței. S-a constatat că abilitățile Big Data consolidează atât eficiența transformării digitale, cât și pe cea a securității cibernetice. Conformitatea cu reglementările UE a influențat pozitiv atât transformarea digitală, cât și practicile de securitate cibernetică. Ipoteza de mediere, conform căreia Big Data și conformitatea UE sporesc efectul

transformării digitale și al securității cibernetice asupra performanței organizaționale, a fost parțial susținută. Efectele indirecte relevă faptul că organizațiile care valorifică perspectivele oferite de date și care respectă standardele UE înregistrează rezultate operaționale și strategice superioare, evidențiind importanța alinierii la reglementări atât ca o constrângere, cât și ca un factor facilitator pentru succesul afacerii. Aceste constatări sunt deosebit de relevante în lumina dezbaterilor actuale privind presiunile exercitate de companiile tehnologice globale pentru a dereglementa cadrele europene, sugerând că conformitatea poate conferi avantaje strategice atunci când este integrată eficient în practica organizațională. Toate constructele au demonstrat o consistență internă puternică, validitate convergentă și validitate discriminantă, susținând robustețea analizelor structurale ulterioare. Modelul s-a dovedit statistic robust, înregistrând indicatori de ajustare optimi. Rezultatele empirice colectate demonstrează că modelul conceptual propus are o putere explicativă moderată spre puternică, explicând 24,4% din varianța Transformării Digitale, 27,9% din cea a Securității Cibernetice și 43,6% din varianța Performanței Companiei.

O concluzie centrală a studiului este că Transformarea Digitală acționează ca un motor cheie al Performanței Companiei (confirmând ipoteza H1). Digitalizarea proceselor, combinată cu integrarea deciziilor bazate pe date și automatizarea, conduce la o eficiență operațională superioară și o reactivitate crescută pe piață. De asemenea, a fost confirmată ipoteza H2, dezvăluind că o securitate cibernetică matură nu reprezintă doar o barieră defensivă sau un cost, ci un facilitator strategic direct al performanței și al încrederii partenerilor de afaceri.În ceea ce privește capabilitățile Big Data, rezultatele au validat ipoteza H3 și parțial H4, confirmând că aceste competențe de analiză sunt esențiale pentru succesul Transformării Digitale și contribuie semnificativ la eficiența Securității Cibernetice, oferind suport pentru managementul proactiv al riscurilor. Influența conformității cu reglementările UE (H5) a fost validată ca un determinant structural major. Alinierea la reglementări exercită o influență pozitivă și înalt semnificativă atât asupra Transformării Digitale, cât și asupra Securității Cibernetice. Această constatare oferă o contra-narrativă importantă la criticile aduse de marile companii tehnologice (Big Tech), demonstrând că reglementările europene (GDPR, NIS2, DORA, DSA) nu blochează inovarea, ci mai degrabă instituționalizează bunele practici și creează un avantaj competitiv echitabil pentru actorii mai mici, cum sunt IMM-urile. Ipoteza de mediere H6, care propunea că Big Data și reglementările UE mediază relația dintre Transformarea Digitală, Securitatea Cibernetică și Performanța Companiei a fost parțial susținută. Efectele indirecte indică faptul că ambele constructe au roluri de mediere semnificative, intensificând căile prin care tehnologia se traduce în rezultate măsurabile; în mod specific, relațiile indirecte și arată că organizațiile care extrag valoare din

date și respectă standardele UE obțin rezultate financiare și operaționale superioare.Pe de altă parte, insuficiența maturității în securitatea cibernetică amplifică consecințele negative ale digitalizării, expunând organizațiile la perturbări operaționale, pierderi financiare și riscuri reputaționale. În același timp, constatările permit identificarea atât a beneficiilor, cât și a limitărilor transformării digitale în contextul cerințelor de securitate cibernetică și contribuie la validarea modelului propus. Organizațiile care integrează considerentele de securitate cibernetică în strategiile lor de transformare digitală obțin rezultate de performanță superioare și manifestă o reziliență mai mare în fața amenințărilor cibernetice.

Pe baza rezultatelor combinate ale analizelor bibliometrice și empirice, teza dezvoltă și validează empiric un model structural și conceptual care explică modul în care transformarea digitală și securitatea cibernetică interacționează pentru a influența performanța organizațională, extinzând astfel cadrele teoretice existente în domeniile sistemelor informaționale și ale studiilor organizaționale.

Studiul recunoaște și o serie de limitări metodologice importante. Din punct de vedere temporal, faza calitativă a fost realizată între august și octombrie 2024, în timp ce faza cantitativă a avut loc în iulie 2025, ceea ce ar fi putut omite schimbări intermediare de dinamică. De asemenea, utilizarea datelor de tip transversal (cross-sectional) limitează capacitatea de a induce relații stricte de cauzalitate pe termen lung, fiind recomandate pe viitor designuri longitudinale. Utilizarea datelor auto-raportate (self-reported data) poate introduce un bias de dezirabilitate socială sau de percepție, element ce ar putea fi corectat în studii viitoare prin integrarea unor indicatori financiari obiectivi sau audituri externe. Totodată, specificitatea geografică (focalizarea pe companii din România/UE) limitează transferabilitatea directă a rezultatelor în regiuni cu alte niveluri de maturitate instituțională (cum ar fi America de Nord sau Asia-Pacific). Din punct de vedere conceptual, modelul s-a limitat la 5 constructe mari, lăsând loc pentru cercetări viitoare care să includă variabile precum cultura organizațională sau stilul de leadership.

Studiul aduce contribuții atât teoretice, cât și practice. Extinde înțelegerea transformării digitale prin integrarea securității cibernetice, a analizei Big Data și a conformității cu reglementările UE într-un cadru conceptual coerent, validat empiric în contextul românesc prin prisma teoriei resurselor (RBV), a capabilităților dinamice și a teoriei instituționale. Din perspectivă managerială, constatările sugerează că organizațiile ar trebui să adopte o abordare integrată, care combină adoptarea tehnologiei, măsurile de securitate, analiza datelor și conștientizarea reglementărilor pentru a maximiza performanța organizațională. În plus, cultivarea unei culturi de conștientizare a securității cibernetice și oferirea de instruire continuă sunt esențiale, în special pentru IMM-urile cu resurse limitate.

Originalitatea acestei cercetări doctorale constă în abordarea sa interdisciplinară și în dezvoltarea unui model fundamentat empiric, care integrează transformarea digitală și securitatea cibernetică într-un cadru analitic orientat spre performanță. Prin corelarea perspectivelor teoretice cu dovezile empirice, teza contribuie la avansarea cunoștințelor în domeniile strategiei digitale și managementului securității cibernetice.

Din perspectivă practică, rezultatele oferă perspective concrete și aplicabile pentru manageri și factorii de decizie politică, sprijinind un proces decizional bazat pe dovezi în ceea ce privește investițiile digitale și guvernanța securității cibernetice. Modelul propus servește ca un instrument strategic pentru organizațiile care urmăresc să își optimizeze performanța, atenuând în același timp riscurile cibernetice într-un mediu digital din ce în ce mai complex.

În concluzie, această cercetare doctorală arată faptul că transformarea digitală și securitatea cibernetică sunt capabilități strategice care se consolidează reciproc, iar eficiența lor este potențată de practicile analizei Big Data și de conformitatea cu reglementările UE. Studiul confirmă că tehnologia singură nu este suficientă pentru a asigura succesul organizațional, iar dimensiunile umane, organizaționale și de reglementare joacă un rol decisiv. Prin utilizarea unui design bazat pe metode mixte, cercetarea îmbină profunzimea contextuală cu rigoarea empirică, oferind un cadru cuprinzător pentru înțelegerea modului în care digitalizarea, securitatea cibernetică, datele și reglementările modelează împreună rezultatele organizaționale. Rezultatele obținute pot fi utilizate în practică de către manageri, pot de asemenea dezvolta și îmbogăți partea de cercetare academică privind transformarea socio-tehnică și impactul reglementărilor și, totodată, pun bazele unor studii viitoare care să examineze comparații între țări, dinamici specifice diferitelor sectoare și evoluția cadrelor legislative.