Universitatea „Babeș-Bolyai”

Facultatea de Drept

TEZĂ DE DOCTORAT

PREVENIREA ACCESULUI ILEGAL ÎN MEDIUL CLOUD COMPUTING

(cuprins și rezumat)

Conducător de doctorat:
Prof. univ. dr. Ioana VASIU

Student-doctorand:
Bogdan Alexandru URS

Cluj-Napoca

2022

CUPRINS

CUVINTE CHEIE

Mediul informatic; Cloud Computing; criminalitate informatică; acces ilegal; prevenirea accesului ilegal; Infrastructure as a Service; Platform as a Service; Software as a Service; Cloud public; Cloud privat; Cloud hibrid; Cloud de comunitate; obținerea de date informatice; încălcarea măsurilor de securitate; atacuri informatice; fraude informatice; mecanisme legale de prevenire; mecanisme tehnice de prevenire; mecanisme cu rol în managementul prevenirii; prevenirea în sectorul privat; prevenirea în sectorul public.

REZUMAT

Mediul Cloud Computing reprezintă unul dintre cele mai importante progrese tehnologice din ultimii ani, fiind un adevărat fenomen multifuncțional ce acoperă aproape toate aspectele revoluției digitale. Pornind de la procesarea, stocarea și analiza datelor, comunicații, rețele și infrastructuri, toate se regăsesc într-o formă sau alta în cadrul serviciilor Cloud Computing.

În ultimii ani, atacurile cibernetic au devenit din ce în ce mai periculoase și mai frecvente[1]. Complexitatea acestora reprezintă o amenințare gravă la adresa siguranței cetățenilor din întreaga lume. Infracționalitatea informatică reprezintă un domeniu de maximă importanță în materie penală. Sectorul este unul vast și extrem de complex din punct de vedere tehnic. În plus, acesta se află în permanentă schimbare și diversificare. Din punct de vedere legal, Cloud Computing-ul[2] este un mediu informatic propice activităților infracționale.

Cloud Computing-ul aduce o serie de noi posibilități pentru infracționalitatea informatică. Spre deosebire de etapele incipiente ale infracționalității cibernetice, în care accentul se punea pe diferite tipuri de contaminanți informatici, în perioada actuală, Cloud

[1] UNODC - Expert Group to Conduct a Comprehensive Study on Cybercrime 2021- *Compilation of all preliminary conclusions and recommendations suggested by Member States during the meetings of the Expert Group to Conduct a Comprehensive Study on Cybercrime held in 2018, 2019 and 2020*, p. 19-20, 21, 22. Sursa https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime-April-2021/CRP/V2101012.pdf

[2] Wall D. S., *Towards a Conceptualisation of Cloud (Cyber) Crime*, HAS 2017: Human Aspects of Information Security, Privacy and Trust, p. 529. Sursa https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3038866

Computing-ul creează posibilități noi de comitere a infracțiunilor informatice prin: puterea de calcul, infrastructura, mașinăriile virtuale, aplicațiile și platformele diverse[1] etc.

Accesul ilegal în mediul Cloud Computing reprezintă un element cheie pentru înțelegerea întregului fenomen infracțional, deoarece creează oportunități pentru realizarea altor infracțiuni informatice mult mai grave și mai periculoase. În esență, infracțiunea permite executarea unor atacuri informatice extrem de periculoase, care pot lua forma altor infracțiuni informatice, precum: fraude informatice, efectuarea de operațiuni financiare în mod fraudulos, interceptarea ilegală a unei transmisii de date informatice, alterarea integrității datelor informatice, perturbarea funcționării sistemelor informatice, transferul neautorizat de date informatice, fals informatic, șantaj, sabotaj informatic, infracțiuni referitoare la drepturile de autor, infracțiuni de terorism etc.

Accesul ilegal în mediul Cloud Computing și infracțiunile cibernetice asociate reprezintă un fenomen global și, prin urmare, este nevoie de un răspuns tot global, prin care să poată fi soluționat. Prevenirea accesului ilegal în mediul Cloud Computing reprezintă una dintre cele mai eficiente strategii de combatere a fenomenului, ce se propagă în același ritm cu dezvoltarea și răspândirea tehnologiei informațiilor și a comunicațiilor[2].

Primul titlu al tezei (Cloud Computing - mediul informatic) a fost structurat în două capitole. Primul capitol cuprinde aspecte preliminare, iar cel de-al doilea este dedicat mediului informatic și tehnologiei de tip Cloud Computing.

Am început **primul capitol** cu o serie de aspecte preliminare legate de obiectivele și metodologia cercetării. În continuare, am evidențiat pe scurt motivația alegerii temei și stadiul actual al cercetării.

Un prim obiectiv de cercetare a fost acela al studiului mediului Cloud Computing și al particularităților sale. Am definit mediul informatic și am explicat fiecare particularitate a tehnologiei Cloud Computing (servicii proprii la cerere, accesul la servicii prin intermediul unei rețele sau prin Internet, alocarea dinamică a resurselor, flexibilitatea serviciilor etc).

Cel de-al doilea obiectiv din cadrul prezentei lucrări îl constituie accesul în mediul Cloud Computing. Am ales să prezentăm la nivel conceptual, fără să intrăm excesiv în detalii

[1] Council of Europe - Cybercrime Convention Committee (T-CY), *Criminal justice access to data in the cloud: challenges*, Discussion paper prepared by the T-CY Cloud Evidence Group, T-CY (2015)10 Provisional, 26 May 2015 Strasbourg, France, p. 9-11. Sursa https://rm.coe.int/1680304b59

[2] Brewer R., Vel-Palumbo M., Hutchings A., Holt T., Goldsmith A., Maimon D., *Cybercrime Prevention Theory and Applications, Crime Prevention and Security Management*, ISBN 978-3-030-31068-4 ISBN 978-3-030-31069-1 (eBook), https://doi.org/10.1007/978-3-030-31069, p. 2, 3-5. Sursa https://link.springer.com/book/10.1007%2F978-3-030-31069-1

tehnice, mecanismele de control al accesului în mediul Cloud Computing. După cercetarea modului în care se face accesul legal în Cloud Computing, a fost necesar să studiem și modul în care se face accesul ilegal în mediul Cloud Computing.

Cel de-al treilea obiectiv al prezentei lucrări și cea mai importantă parte a cercetării noastre este prevenirea accesului ilegal în mediul Cloud Computing. Obiectivele de cercetare expuse anterior se concentrează pe acest ultim obiectiv extrem de important. Analiza problemelor actuale legate de prevenirea accesului ilegal țin de esența lucrării noastre. Prevenirea infracțiunii presupune găsirea celor mai eficiente soluții practice. Fie că este vorba despre metode de prevenire legale, tehnice sau manageriale, toate acestea sunt indispensabile pentru securitatea mediului Cloud Computing. Studiul respectivelor metode, precum și implementarea lor constituie un obiectiv de cercetare adecvat domeniului interdisciplinar pe care l-am ales. Având în vedere abordarea multidisciplinară a cercetării, pe parcursul lucrării am ales să consultăm literatura științifică de specialitate atât din domeniul dreptului, cât și pe cea din domeniul tehnologiei informației și a comunicațiilor.

Accesul ilegal în mediul Cloud Computing reprezintă o infracțiune complexă atât punct de vedere legal, cât și din punct de vedere tehnic. Prevenirea unei astfel de infracțiuni necesită o abordare nouă, în contextul în care accesul ilegal are un impact direct asupra altor infracțiuni cibernetice. Am ales această temă de cercetare chiar dacă studiul ei este destul de dificil având în vedere că, necesită atât cunoștințe din domeniul juridic, cât și cunoștințe practice avansate în domeniul tehnic al industriei informației și a comunicațiilor.

În capitolul doi ne-am propus să analizăm *in extenso* noțiunea de „mediu informatic" și tehnologia Cloud Computing. În esență, *„mediul informatic"* reprezintă un ansamblu de elemente hardware și software ce funcționează în mod unitar în cadrul sistemelor informatice și a rețelelor, ansamblu ce îndeplinește diferite funcții și interacțiuni (între sisteme informatice sau între oameni și sisteme informatice)[1]. *Cloud Computing-ul* este un model ce permite, prin intermediul unei rețele, accesul facil și omniprezent la un ansamblu de resurse de calcul configurabile (rețele, servere, mijloace de stocare, aplicații, servicii și altele), acces ce poate fi lansat și asigurat prin intermediul unor instrumente de management minime și cu o interacțiune redusă din partea furnizorului de servicii[2]. Tehnologia Cloud Computing prezintă următoarele caracteristici: alocarea dinamică a resurselor de calcul, accesul în Cloud este asigurat prin

[1] Această definiție a fost publicată de Urs B., *„Cloud Computing – mediul propice pentru criminalitatea informatică",* Revista „Dreptul " nr. 3/2018, , p. 142-143, ISSN 1018-0435, UJR București 2018.
[2] The National Institute of Standards and Technology (NIST), *The NIST Definition of Cloud Computing,*Recommendations of the National Institute of Standards and Technology. Sursa http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

intermediul unei rețele (Internet), furnizarea de servicii se face la cererea utilizatorilor, acestea fiind flexibile și existând posibilitatea de a fi cuantificate. Cele trei modele comune de *livrare* a serviciilor Cloud Computing sunt: „Infrastructure as a Service" (Iaas), „Platform as a Service" (PaaS) și „Software as a Service" (SaaS). Generic există patru modele de *implementare* a serviciilor Cloud Computing: Cloud-ul public, Cloud-ul privat, Cloud hibrid-ul și Cloud-ul comunitar.

Al doilea titlu al tezei (Accesul în mediul Cloud Computing și infracționalitatea informatică) reprezintă o analiză amplă a modului în care se face accesul legal în mediul Cloud Computing. Pornind de la aceasta, am trecut apoi la studiul infracțiunii prevăzute la art. 360 Cod pen., cu referire expresă la accesul ilegal în mediul Cloud Computing. În continuare, am explicat în detaliu implicațiile accesului ilegal asupra dinamicii fenomenului infracțional existent în mediul Cloud Computing.

Primul capitolul din acest titlu este dedicat accesului legal în mediul Cloud Computing. Acesta presupune respectarea unor etape și proceduri prestabilite. Dincolo de aspectele de natură tehnică, în esență este vorba despre acele mecanisme și modele cu rol în autentificarea și autorizarea utilizatorilor care accesează în mod legal serviciile Cloud Computing. Accesul utilizatorilor se face într-un mediu controlat, în care fiecare utilizator dispune de către diverse funcții și restricții, care sunt menite să mențină securitatea în Cloud Computing. În cadrul sistemelor de control, mecanismele de autentificare și cele de autorizare sunt configurate în mod automat, în funcție de cerințele furnizorilor de servicii.

În al doilea capitol am remarcat că deși există o serie de sisteme și mecanisme de control, accesul ilegal în mediul Cloud Computing reprezintă în continuare o problemă gravă la adresa securității mediului informatic. Infracțiunea de acces ilegal la un sistem informatic este reglementată în cuprinsul art. 360 din Codul penal român. În urma examinării legislației ce incriminează infracțiunea în Statele Unite ale Americii, Regatul Unit al Marii Britanii și al Irlandei de Nord, Australia, Germania și Franța am constatat faptul că nu există un consens în ceea ce privește conduita infracțională.

Infracțiunea de acces ilegal în mediul Cloud Computing este o infracțiune de pericol. Accesul ilegal la un sistem informatic reprezintă o infracțiune esențială, sau altfel spus o „platformă" ce face posibilă realizarea altor infracțiuni informatice[1]. În cele mai multe cazuri putem vorbi despre faptul că accesul ilegal este o infracțiune mijloc pentru comiterea infracțiunilor scop. Infracțiunea permite în principal realizarea unor atacuri informatice

[1] Vasiu I., Vasiu L., *Criminalitatea în cyberspațiu*, Editura Universul Juridic, București, 2011, p. 144

periculoase care pot lua forma altor infracțiuni informatice, precum: fraude informatice, efectuarea de operațiuni financiare în mod fraudulos, interceptarea ilegală a unei transmisii de date informatice, alterarea integrității datelor informatice, perturbarea funcționării sistemelor informatice, transferul neautorizat de date informatice, fals informatic, șantaj, sabotaj informatic, infracțiuni privind drepturile de autor, infracțiuni de terorism și altele.

În înțelesul dat de legiuitorul român, Cloud Computing-ul reprezintă un astfel de sistem informatic, prin prisma faptului că el conține atât componente *hardware,* cât și *software*, ce au ca funcție prelucrarea automată de date informatice prin intermediul unor programe informatice. Accesul ilegal în Cloud Computing presupune în esență pătrunderea (fie direct, fie la distanță) în componentele ce alcătuiesc mediul informatic. Prin *„acces"* se înțelege capacitatea de a interacționa logic integral sau cu o parte a sistemului informatic/mediului Cloud Computing, acțiune ce permite posibilitatea de a beneficia de resursele informatice, de a modifica funcțiile sistemului sau pentru a lansa diferite comenzi în sistem, fie la nivel local în mod direct, fie la distanță prin intermediul unei rețele informatice.

În opinia noastră, fie că este vorba despre o atitudine comisivă sau omisivă (menținerea accesului), pătrunderea în sistemul informatic constituie elementul esențial al infracțiunii. Legiuitorul penal a introdus o condiție esențială și anume aceea ca activitatea incriminată să se desfășoare „fără drept". În esență, lipsa autorizării reprezintă un element constitutiv al infracțiunii, deși în dreptul penal substanțial se face referire la accesul ilegal sau „fără drept". Practic, din perspectiva infracțiunii de acces ilegal la un sistem informatic, legiuitorul român a avut în vedere un spectru mai larg de opțiuni care includ atât noțiunea de „ilegal", cât și pe cea de „neautorizat" sau „fără drept", fiind vorba aici mai degrabă despre noțiuni interschimbabile[1].

Prima modalitate agravată a infracțiunii de acces ilegal în mediul Cloud Computing este prevăzută în art. 360 alin. (2) din Codul penal și vizează scopul obținerii de date informatice. După cum am explicat anterior, mediul Cloud Computing este constituit dintr-un ansamblu de elemente esențiale, datele informatice fiind unele dintre ele. Nu este necesar în acest caz ca scopul să se realizeze și să obțină datele informatice. Mai mult, dacă scopul special a existat anterior, iar accesul se realizează în forma de bază, este suficient pentru reținerea infracțiunii în forma agravată. Cea de-a doua modalitate agravată a infracțiunii de acces ilegal în mediul Cloud Computing este prevăzută în art. 360 alin. (3) din Codul penal și presupune încălcarea măsurilor de securitate.

[1] Zlati G., *Tratat de criminalitate informatică*, Vol. I, Editura Solomon, București, 2020, p. 216

Mediul, arhitectura și serviciile Cloud Computing sunt protejate prin intermediul unor proceduri, dispozitive și programe specializate, accesul fiind în general restricționat sau interzis pentru anumite categorii de utilizatori. Prin măsuri de securitate se înțeleg proceduri, dispozitive sau programe specializate, prin care accesul este restricționat sau interzis pentru anumite categorii de utilizatori. Chiar dacă în textul de lege sunt enumerate o serie de măsuri de securitate, pentru reținerea modalității agravate este suficient încălcarea unei singure măsuri. Nu este suficient ca măsurile de securitate să existe, ele trebuie să fie în funcțiune, iar pentru reținerea acestei modalități este necesară o eludare a funcționalității lor.

Caracteristicile mediului Cloud Computing au un impact direct asupra modalităților de comitere a infracțiunii de acces ilegal în mediul informatic. Cloud Computing-ul nu este un simplu sistem informatic. Astfel, o primă etapă și o particularitate de comitere a acestei infracțiuni o reprezintă stabilirea exactă a elementelor care urmează să fie accesate în mod ilegal. Ce-a dea doua particularitate sau etapă premergătoare accesului propriu-zis în mediul Cloud o reprezintă recunoașterea sau colectarea a cât mai multe informatice despre mediul sau serviciul ce urmează a fi accesat ilegal. Etapele necesare pentru stabilirea modului de acțiune și de recunoaștere constituie doar acte preparatorii pentru comiterea infracțiunii de acces ilegal în mediul Cloud. O altă particularitate ce ține de esența infracțiunii de acces ilegal în mediul Cloud Computing o constituie modul implicit de acțiune.

Accesul ilegal în mediul Cloud Computing se poate realiza fie la nivel de arhitectură și infrastructură (servere, echipamente de stocare și rețea, VM-uri etc.) fie la nivel de aplicații și servicii (instrumente pentru productivitate, comunicație „VoIP”, email, „backup” și altele). Strict din punct de vedere tehnic, accesul la nivel de infrastructură este mult mai dificil de realizat decât accesul la nivel de aplicație întrucât necesită cunoștințe avansate la nivel de vulnerabilități precum și metode complexe de exploatare a acestora. În cele din urmă, menținerea accesului și ascunderea urmelor infracțiunilor reprezintă operațiuni adiacente infracțiunii de acces ilegal în mediul Cloud Computing.

Accesul ilegal în mediul Cloud Computing rămâne în continuare problematic din punctul de vedere al aspectelor jurisdicționale. Aplicarea legii penale și procesul de înfăptuire al justiției sunt aspecte esențiale care țin de suveranitatea unui stat. Competența în materie penală este strâns legată de teritoriul geografic al acelui stat. În urma analizei și a studiului unor cazuri de infracțiuni informatice, am remarcat că accesul ilegal în mediul Cloud Computing a presupus acționarea de la distanță, uneori chiar din alte țări. Elementul internațional al accesului

ilegal în mediul Cloud și al altor infracțiuni informatice conexe este frecvent întâlnit în astfel de situații. Prin urmare, apar o serie de aspecte jurisdicționale, dar și unele conflicte de jurisdicție. Este foarte important să menționăm că, prin intermediul formelor de colaborare internațională, nu se aduce atingere suveranității statelor, respectiv a jurisdicției acestora ori a dreptului lor național.

Problemele legate de jurisdicție și aspectele de teritorialitate existente în mediul Cloud Computing derivă din componentele de extraneitate relevante în dinamica fenomenului infracțional. Funcționarea unui spectru variat de jurisdicții relevante în diferite țări poate conduce la situația în care mai multe țări susțin că ele au jurisdicție asupra unei infracțiuni informatice de acces ilegal. Conflictele sunt de cele mai multe ori de natură concurențială. Ele sunt cauzate de către diferite deficiențe care există la nivel de reglementări legislative. În general, în astfel de cazuri este necesar să existe la nivel de state o legislație specifică referitoare la soluționarea conflictelor de competență. De altfel, ar fi recomandat ca statele implicate să găsească soluții prin consultări și, de ce nu, chiar să colaboreze între ele pentru găsirea jurisdicției optime[1]. Suntem de părere că, în momentul în care a fost comisă o infracțiune cibernetică de acces ilegal în Cloud Computing sau o infracțiune cu implicații în Cloud, este posibil ca infracțiunea să se încadreze în jurisdicția mai multor state.

În cel de-al treilea capitol am studiat modul în care accesul ilegal afectează mediul Cloud Computing. Atacurile cibernetice au un rol crucial în săvârșirea infracțiunii de acces ilegal în mediul Cloud Computing. Studiul particularităților acestor atacuri informatice ne-a permis să identificăm acele mecanisme complexe ce generează accesul ilegal și fenomenul infracțional asociat acestuia. Este important de menționat că particularitățile atacurilor informatice urmăresc îndeaproape caracteristicile mediului Cloud Computing. Fiecare atac are o serie de caracteristici și particularități, care odată ce sunt materializate, dau naștere unor forme complexe de infracțiuni informatice. În cadrul cercetării noastre am analizat în detaliu atacurile de autentificare și de autorizare, atacurile de împachetare, atacul de tip „side channel", atacul de tip „Man in the Cloud", atacul de tip „Man in the Middle" și atacurile din „interior". Din punct de vedere legal, Cloud Computing-ul este un mediu informatic propice activităților infracționale.

[1] A se vedea Urs B., „*Investigațiile digitale în mediul Cloud Computing. Probleme și soluții*", Secțiune publicată în Revista „Dreptul " nr. 7/2019, p. 187-188, ISSN 1018-0435, UJR București 2019.

Din punctul nostru de vedere, marea problemă referitoare la acest mediu informatic complex o constituie migrația de la criminalitatea digitală clasică spre criminalitatea digitală complexă, ce este prezentă în Cloud Computing. Altfel spus, este vorba despre migrația de la o criminalitate informatică ce are la bază resurse computaționale oarecum limitate (de exemplu, un sistem informatic propriu) către o criminalitate digitală cu resurse practic nelimitate (prin infrastructură, platformă și aplicații). Migrația utilizatorilor spre Cloud Computing determină în mod automat și migrația criminalității informatice. În prezent există în Cloud Computing două mari categorii de infracțiuni: în prima categorie, *mediul informatic este ținta infracțiunii*, iar în cea de-a doua categorie, mediul Cloud este folosit ca *instrument de comitere a infracțiunilor*.

Titlul trei al tezei (Prevenirea accesului ilegal în mediul Cloud Computing) cuprinde o analiză riguroasă a modului în care sunt organizate și funcționează mecanismele de prevenire a infracționalității informatice. Cercetarea noastră se focalizează pe studiul mecanismelor legale, tehnice și manageriale de prevenire a infracționalității informatice. În ceea ce privește prevenirea accesului ilegal în mediul Cloud Computing am optat pentru o abordare diferențiată în funcție de rolul sectorului public și a celui privat. Studiul de cercetare efectuat asupra principalelor companii furnizoare de servicii Cloud Computing din țară și din străinătate ne-a fost de mare ajutor în acest demers științific.

Am început **primul capitol** din titlul al treilea cu organizarea metodologică a mecanismelor de prevenire a infracțiunilor informatice existente în mediul Cloud Computing. În esență acestea sunt implementate la nivel principial. Prevenirea infracțiunilor informatice reprezintă unul dintre cele mai eficiente mecanisme de combatere a fenomenului. Prevenția se concentrează pe reglementarea și pe atenuarea riscurilor, iar în contextul infracțiunilor informatice, mecanismul urmărește fie să prevină apariția și reapariția activității ilegale, fie cel puțin să atenueze daunele rezultate din comiterea ei. Prevenirea infracțiunilor informatice prezente în mediul Cloud Computing reprezintă un proces complex din punct de vedere legal, tehnic și managerial. Abordarea unui astfel de fenomen exclusiv din punct de vedere tehnic nu este suficient, chiar dacă la prima vedere, în ceea ce privește mediul și arhitectura infrastructurii Cloud Computing, partea tehnică are o importanță aparte. Fără elemente de ordin legal și managerial, metodele de prevenire tehnice își pierd eficiența. Aceasta constă în raportul de proporționalitate dintre numărul incidentelor sau al infracțiunilor informatice și numărul de incidente care au fost prevenite sau care nu și-au produs efectele.

Abordarea prevenirii din perspectiva utilizatorilor, a sectorului privat și celui de stat este de natură să cuprindă un spectru larg de mecanisme și măsuri, indiferent de părțile implicate. În urma cercetărilor efectuate am identificat faptul că modelul și gradul de utilizare al serviciilor Cloud Computing este corelat cu experiența utilizatorilor - concept ce derivă din interacțiunea dintre utilizatori și serviciile utilizate[1]. Experiența utilizatorilor se reflectă în mod direct asupra calității serviciilor Cloud Computing și implicit asupra dinamicii fenomenului infracțional ce are loc în mediul Cloud Computing. Eficiența formelor de prevenire a criminalității informatice variază mult în funcție de serviciile Cloud Computing ce sunt alese pe baza experienței de utilizare[2].

Capitolul doi se concentrează pe acele măsuri legale cu rol de prevenire. Sancțiunile de drept penal aplicabile constituie un mecanism extrem de eficient în prevenirea accesului ilegal și a altor infracțiuni informatice asociate. Pe parte de prevenire, funcția de intimidare a normei penale îl determină pe cel care intenționează să comită o infracțiune cibernetică să evalueze riscurile conduitei sale în raport cu sancțiunea incidentă[3]. În plus față de normele de drept penal există și alte acte normative cu implicații directe în prevenirea accesului ilegal în mediul Cloud Computing. Un astfel de act este Directiva UE 2016/1148 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice. Directiva face parte din strategia de securitate cibernetică a Comisiei Europene pentru Uniunea Europeană și a fost creată în scopul de a spori cooperarea dintre statele membre ale Uniunii Europene cu privire la aspectele de securitate cibernetică, prin impunerea unor norme minime de armonizare. Cloud Computing-ul reprezintă unul dintre factorii care au determinat reforma legislației pentru protecția datelor. Regulamentul (UE) 2016/679 privind protecția datelor este aplicabil în mod direct în toate statele membre ale Uniunii Europene și actualizează legislația privind protecția datelor astfel încât, pe de o parte, să fie protejate drepturile persoanelor fizice, iar, pe de altă parte, să le

[1] Urs B., Rusu C., Rusu V., Botella F., Quinones D., Urs I.,. Morales J., Cano S., Aciar S., Castro I. B., *"Forming Customer eXperience Professionals: A Comparative Study on Students' Perception"*, articol publicat în Human Systems Engineering and Design II, Proceedings of the 2nd International Conference on Human Systems Engineering and Design (IHSED2019): Future Trends and Applications, September 16-18, 2019, Universitat der Bundeswehr Munchen, Munich, Germany, Edited Springer Book (2nd ed. 2019, XXI, 1105 p., ISBN 978-3-030-27928-8, DOI 10.1007/978-3-030-27928-8, T. Ahram et al. (Eds.): IHSED 2019, AISC 1026, pp. 391–396, 2020, https://doi.org/10.1007/978-3-030-27928-8_60, p. 392. Sursa https://link.springer.com/chapter/10.1007%2F978-3-030-27928-8_60.

[2] Tabrizchi H., Rafsanjani M. K., *A survey on security challenges in cloud computing: issues, threats, and solutions*, The Journal of Supercomputing volume 76, pages 9493–9532 (2020), Springer, https://doi.org/10.1007/s11227-020-03213-1, p. 6, 15. Sursa https://ibook.pub/a-survey-on-security-challenges-in-cloud-computing-issues-threats-and-solutions.html

[3] Streteanu F., Nițu D., *Drept penal. Partea generală*, Vol. 2, Editura Universul Juridic, București, 2018, p. 278-279, 282.

permită companiilor să utilizeze datele cu caracter personal într-o manieră transparentă pe întreg teritoriul Uniunii Europene. Atacurile informatice a căror țintă este mediul Cloud Computing intră sub incidența Directivei 2013/40/UE, ce stabilește norme minime privind definirea infracțiunilor și a sancțiunilor. În plus, actul normativ îmbunătățește cooperarea dintre autorități, dar și dintre organismele specializate precum Eurojust, Europol, Centrul european de combatere a criminalității informatice și Agenția Uniunii Europene pentru Securitatea Rețelelor și a Informațiilor (ENISA).

Capitolul trei abordează mecanismele tehnice de securitate cu rol în prevenirea accesului ilegal. Securitatea tehnologiei reprezintă o componentă esențială în cadrul procesului de prevenire a accesului ilegal în mediul Cloud Computing. Măsurile de securitate cuprind o serie de standarde, prevederi legale, politici și proceduri de utilizare, principii de securitate dar și obligații contractuale ce acționează la nivel fizic, operațional, managerial și procedural. Implementarea acestora contribuie în mod activ la lupta împotriva infracționalității informatice și la diminuarea efectelor sale negative. Securitatea mediului Cloud Computing poate fi privită raportat la cele două părți implicate: utilizatorul și furnizorul de servicii. Responsabilitatea pentru securitatea mediului informatic este astfel divizată: furnizorul se ocupă de aspectele care țin de securitatea mediului și a infrastructurii, iar utilizatorul este responsabil pentru securitatea operării sistemului, a aplicațiilor și a datelor utilizate.

Din punct de vedere tehnic, prevenirea infracțiunii de acces ilegal și protecția datelor din Cloud Computing necesită utilizarea unor tehnologii diverse. Printre acestea se numără utilizarea unei conexiuni securizate (SSL/TLS), crearea unui Cloud Privat Virtual sau „Virtual Private Cloud” (VPC), accesul prin intermediul unei rețele virtuale private (VPN), criptarea datelor cu algoritmul AES („Advanced Encryption Standard”) etc. În prezent, una dintre cele mai eficiente metode de protecție împotriva accesului ilegal o constituie criptarea. Criptarea datelor contribuie atât la creșterea nivelului de securitate în mediul Cloud Computing, cât și la sporirea gradului de dificultate al unui eventual acces ilegal. Printre cele mai importante metode de criptare analizate se numără criptarea prin intermediul funcției „hash”, criptarea tradițională („simetrică”), criptarea cu două chei („asimetrică”) și criptarea homomorfică.

Capitolul patru se ocupă cu partea de management a mecanismelor de prevenire a acesului ilegal în Cloud Computing. Principiile de organizare a serviciilor Cloud Computing sunt elemente fundamentale ce țin de protecția datelor și a infrastructurii. Acestea oferă utilizatorilor și furnizorilor de servicii Cloud Computing un punct de pornire în evaluarea

mediului informatic și a securității sale. Organizarea unui cadru de securitate în mediul Cloud Computing se face de către furnizorul de servicii. Procedeul constă în implementarea controalelor de securitate și în recomandarea unor remedii la problemele de securitate din sistem (managementul configurărilor, analiza vulnerabilităților, monitorizarea preventivă și managementul incidentelor). Instrumentele de management și audit al securității serviciilor au un rol esențial în prevenirea accesului ilegal în mediul Cloud Computing. Managementul și auditul structurat sunt de natură să contribuie în mod direct la reducerea semnificativă a infracțiunilor de acces ilegal și chiar să descurajeze orice fel de tentativă în acest sens.

În prezent există o serie de organizații de specialitate precum „Cloud Security Alliance" (CSA), „International Organization for Standards" (ISO), „National Institute for Standards and Technology" (NIST), „The European Union Agency for Network and Information Security" (ENISA) și altele. Aceste organizații lucrează la implementarea standardelor de securitate în mediul Cloud Computing și la găsirea unor soluții referitoare la problemele de securitate ale utilizatorilor și ale furnizorilor de servicii. Printre aceste standarde putem enumera ISO/IEC 27017:2015, ISO/IEC 27018:2014, ISO/IEC 27036:2016, PCI-DSS, HIPAA/HITECH, FedRAMP, FIPS 140-2 etc.

Capitolul cinci tratează pe larg rolul sectorului public în prevenirea accesului ilegal în mediul Cloud Computing. Prevenirea infracțiunilor informatice prin tragerea la răspundere penală reprezintă o măsură cu un nivel ridicat de eficiență, în condițiile în care pedepsele au rolul de a-i descuraja pe cei ce le comit. Tragerea la răspundere penală și procesul de înfăptuire al justiției presupun dovedirea infracțiunilor informatice dincolo de orice dubiu, pentru aceasta fiind nevoie de dovezi în formă electronică. Politicile și strategiile naționale de prevenire a infracțiunilor informatice au un rol esențial în mediul Cloud Computing. În România există o politică generală guvernamentală privind protecția datelor personale. În plus, cooperarera internațională contribuie în mod semnificativ la prevenirea prin intermediul procedurilor de investigație în materie penală. De asemenea, subliniem importanța investigațiilor digitale în prevenirea și combaterea accesului ilegal în mediul Cloud Computing. Depistarea și tragerea la răspundere a persoanelor care săvârșesc infracțiuni informatice reprezintă o parte importantă a prevenirii.

Natura complexă a mediului Cloud Computing creează probleme în ceea ce privește investigarea infracțiunilor informatice. Diferențele de ordin legislativ, existente în multiple jurisdicții complică și mai mult aceste anchete penale. Investigarea infracțiunilor într-un mediu

informatic descentralizat necesită capacitatea de a colecta date informatice sub formă de dovezi digitale, ce se află dincolo de granițele naționale. Spre deosebire de metodele tradiționale de investigare a calculatoarelor și a diverselor dispozitive de tip singular (ce au o natură centralizată de funcționare a sistemului informatic), în cazul investigațiilor ce se efectuează în Cloud Computing nu există un control complet asupra artefactelor criminalistice (rute, jurnale de parcurs, elemente de stocare etc). Pentru orice investigație ce se efectuează în mediul Cloud Computing, sunt esențiale trei tipuri de date: informații referitoare la utilizatori, respectiv abonați, date privind traficul și conexiunea prin Internet sau printr-o altă rețea și date privind conținutul stocat în Cloud[1]. De obținerea acestor date depinde întreg parcursul unei anchete.

În capitolul șase a fost analizat rolul sectorului privat în prevenirea accesului ilegal în mediul Cloud Computing. Procedurile cu rol în securitatea și prevenirea accesului ilegal și a altor infracțiuni informatice din mediul Cloud Computing reprezintă reguli care trebuie respectate și implementate de către furnizorii de servicii și de către utilizatori. Acestea sunt menite să asigure securitatea mediului informatic, a sistemelor și a infrastructurii Cloud Computing la nivel fizic, operațional și procedural. În timp ce politicile de securitate se referă la prevenirea diferitelor incidente de securitate intenționate sau neintenționate, politicile de prevenire a infracțiunilor cibernetice se referă la acele incidente ce, în conformitate cu prevederile legale, sunt considerate a fi infracțiuni. Riscul reprezentat de accesul ilegal în mediul Cloud Computing și de celelalte infracțiunile informatice asociate acestuia, este estimat pe baza probabilității unui incident. În Cloud Computing, probabilitatea este asociată cu impactul negativ al incidentului asupra mediului informatic. Acțiunea directă a furnizorilor de servicii asupra mediului Cloud Computing se reflectă asupra măsurilor de detectare, prevenire și de atenuare pe care aceștia le implementează sau nu, tocmai pentru a reduce sau chiar pentru a înlătura riscul reprezentat de o anumită vulnerabilitate sau de o infracțiune informatică.

Furnizorii de servicii constituie principalul factor de impact raportat la securitatea mediului informatic, protecția datelor, evoluția factorilor ce determină fenomenul infracțional și rolul lor în prevenirea accesului ilegal în mediul Cloud Computing. Studiul principalilor furnizori de servicii Cloud din țară și din străinătate are rolul de a explica modalitatea în care aceștia implementează politicile de securitate și de prevenire a accesului ilegal și a altor

[1] Council of Europe - Cybercrime Convention Committee (T-CY) - *Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY Final report of the T-CY Cloud Evidence Group*, www.coe.int/cybercrime, 16 September 2016 Strasbourg, FranceT-CY (2016)5, p. 12. Sursa https://rm.coe.int/16806a495e

infracțiuni informatice prezente în mediul Cloud Computing. Cercetarea noastră s-a concentrat pe analiza tehnicilor de securitate existente la nivel de companii furnizoare de servicii Cloud Computing (Google Cloud Platform, Amazon Web Services, Microsoft Azure, IBM Cloud Computing și Sistec IT Solutions.) și pe evaluarea modului în care aceste companii acționează pentru protejarea datelor cu caracter personal.

În concluzie, considerăm că prevenirea accesului ilegal în mediul Cloud Computing reprezintă o problemă adecvată cercetării acestui domeniu interdisciplinar. În urma cercetării noastre am evidențiat că, prevenirea accesului ilegal reprezintă una dintre cele mai eficiente metode de combatere a fenomenului infracțional din mediul Cloud Computing. Am explicat faptul că, în esență, prevenirea reprezintă un fenomen nou și totodată complex din punct de vedere legal, tehnic și managerial. Pe parcursul cercetării noastre, am identificat o serie de instrumente și mecanisme care contribuie în mod direct la prevenirea accesului ilegal în mediul Cloud Computing. În primul rând, trebuie menționat faptul că prevenirea accesului ilegal în mediul Cloud Computing necesită schimbări în domeniul legislativ. Dintre aceste schimbări putem enumera impunerea unor măsuri pentru furnizorii de servicii Cloud Computing care au ca scop consolidarea cerințelor de securitate, simplificarea obligațiilor de raportare a incidentelor, introducerea unor măsuri de supraveghere mai eficiente și a unor cerințe de aplicare mult mai stricte, inclusiv regimuri noi de sancțiuni. În al doilea rând, este necesar să subliniem rolul furnizorului de servicii. Deși există diferențe în soluțiile tehnice de prevenire pe care aceste companii le implementează, suntem de părere că orice măsură contează, indiferent dacă este vorba despre sistemele de tip IDS și IDPS, Cloud-ul Privat Virtual, izolarea mașinăriilor virtuale și altele asemenea. În al treilea rând, avem convingerea că, pentru a preveni și combate fenomenul infracțional, care a luat în ultimii ani proporții globale, este necesară o bază de acțiune comună și, bineînțeles, investiții în cercetarea extensivă a acestuia, atât la nivel academic, cât și la nivelul factorilor decizionali. În final, nu putem spera decât că demersurile noastre de cercetare vor avea un impact direct asupra literaturii de specialitate din domeniul dreptului penal.