**Bogdan Alexandru Urs**

# Accesul ilegal în mediul Cloud Computing

Editura Hamangiu
2023

# CUPRINS

# CAPITOLUL AL IV-LEA.
# ACCESUL ILEGAL ŞI FENOMENUL INFRACŢIONAL DIN MEDIUL CLOUD COMPUTING

## *Secţiunea 1. Mediul Cloud Computing în paradigma infracţionalităţii informatice*

Încă din cele mai vechi timpuri, cooperarea şi schimbul de informații au stat la baza progresului omenirii. Apariția societății informaționale şi a cyber-spațiului, domeniul mondial ce permite schimbul de informații şi creează interacțiuni între oameni, servicii şi dispozitive electronice, contribuie în mod direct la acest progres. I. Vasiu şi L. Vasiu preiau definiția NIST[1] şi explică *cyberspațiul* ca fiind domeniul global în mediul informațional, constând dintr-o serie de rețele, echipamente şi infrastructuri informatice care sunt menite să mențină distribuția informațiilor şi a comunicațiilor la nivel mondial prin intermediul Internetului[2]. Datorită beneficiilor aduse de evoluția tehnologiei, spațiul cibernetic[3] a devenit astăzi un ansamblu de resurse folosite în comun de către cetățeni, întreprinderi, infrastructuri de informații şi guverne, fără a fi stabilit un mod clar de delimitare între toate aceste grupuri diferite[4]. În următorii ani se estimează că spațiul cibernetic[5] va deveni din ce în ce mai complex, odată cu creşterea numărului de rețele, infrastructuri şi dispozitive care sunt conectate la Internet[6].

---

[1] NIST, *Managing Information Security Risk: Organization, Mission, and Information System View*, 2011, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf.

[2] I. VASIU, L. VASIU, *Dreptul tehnologiei informațiilor şi comunicațiilor*, *op. cit.*, p. 6. Concept definit de către NIST, *Managing Information Security Risk: Organization, Mission, and Information System View,* 2011.

[3] Tutorialspoint, *Information Security & Cyber Law, Cyber Law & IT Act Overview*, https://www.tutorialspoint.com/information_security_cyber_law/introduction.htm, accesat la data de 2 februarie 2020.

[4] Johnson D. R., Post D. G., *Law and Borders – The Rise of Law in Cyberspace*, în Stanford Law Review, vol. 48, p. 1367, https://ssrn.com/abstract=535 or http://dx.doi.org/10.2139/ssrn.535, accesat la data de 2 februarie 2020.

[5] D. BURT, A. KLEINER, J.P. NICHOLAS, K. SULLIVAN, *Cyber space 2025. Today's Decisions. Tomorrow's Terrain, Navigating the Future of Cybersecurity Policy*, June 2014, p. 1, 2, 4-9, http://download.microsoft.com/download/c/7/7/c7775937-748e-4e95-85fb-24581f16b588/cyberspace%202025%20today's%20decisions,%20tomorrow's%20terrain.pdf, accesat la data de 2 februarie 2020.

[6] Această secțiune a fost publicată de B. URS, *Cloud Computing – mediul propice...*, *op. cit.*, p. 145.

Creşterea accentuată a tehnologiei digitale a avut un impact semnificativ asupra societății moderne, a modului de funcționare a economiei, politicii şi culturii, dar şi asupra vieții de zi cu zi a fiecărui individ[1]. Astăzi, accesul uşor la tehnologia digitală constituie una dintre necesitățile bunului mers al societății noastre moderne[2]. Dacă ne referim strict la spațiul cibernetic, ce este caracterizat prin lipsa frontierelor, dinamism şi anonimat, remarcăm că el creează o serie de oportunități pentru dezvoltarea societății informaționale, însă, din păcate, aduce şi o serie de riscuri cu privire la modul în care societatea noastră informațională funcționează[3]. Odată cu dezvoltarea spațiului cibernetic şi a societății informaționale a apărut şi conceptul de criminalitate informatică. În ultimii ani, atacurile cibernetice au devenit din ce în ce mai periculoase şi mai des întâlnite. Complexitatea şi frecvența acestora reprezintă o amenințare gravă la adresa siguranței cetățenilor din întreaga lume[4]. Pagubele create de astfel de atacuri sunt semnificative. Dacă avem în vedere atacurile informatice complexe[5], capabile să închidă centrifuga unei centrale nucleare sau să modifice parametrii de funcționare ai sistemelor de apărare aeriană cu rachetă ori să oprească alimentarea cu energie electrică şi cu apă potabilă, înțelegem cu adevărat amploarea fenomenului infracțional din mediul digital[6].

Răspândirea unei învățături de securitate cibernetică[7] printre utilizatorii sistemelor informatice şi de comunicații constituie o prioritate într-o societate informațională. Frecvent utilizatorii sunt informați puțin în legătură cu

---

[1] F. ZHAO, *E-government development and the digital economy: a reciprocal relationship*, în Internet Research, vol. 25, nr. 5/2014, DOI: 10.1108/IntR-02-2014-0055, p. 734-766, https://www.emeraldinsight.com/doi/full/10.1108/IntR-02-2014-0055., accesat la data de 3 martie 020.

[2] Media Development Investment Fund, *Media development's role in social, economic, and political progress*, MDIF New York White Paper, p. 2-5, https://www.mdif.org/wp-content/uploads/2014/08/Media-Developments-Role-in-Social-Economic-and-Political-Progress-Literature-Review.pdf, accesat la data de 3 martie 2020.

[3] B. HUGHES, D. BOHL, M. IRFAN, E. MARGOLESE-MALIN, J. SOLÓRZANO, *Cyber Benefits and Risks: Quantitatively Understanding and Forecasting the Balance*, Extended Project Report from the Frederick S. Pardee Center for International Futures, Josef Korbel School of International Studies, University of Denver, September 2015, p. 13-14, 26, 49-52, https://pardee.du.edu/sites/default/files/Cyber%20Risk%20Pardee%20Extended%20Report.pdf, accesat la data de 3 martie 2020.

[4] D.S. WALL, *The Internet as a Conduit for Criminal Activity*, *op. cit.*, p. 1-3.

[5] Wurldtech, *The impact of cyber attacks on critical infrastructure*, https://www.ge.com/digital/sites/default/files/Wurldtech-Impact-of-Cyber-Attacks-on-Critical-Infrastructure-infographic.pdf, accesat la data de 2 februarie 2020.

[6] O.A. HATHAWAY, R. CROOTOF, P. LEVITZ, H. PROCTOR, A.E. NOWLAN, W. PERDUE, J. SPIEGEL, *The Law of Cyber-Attack*, în California Law Review, vol. 100, nr. 4/2012, Yale Law & Economics Research Paper No. 453, Yale Law School, Public Law Working Paper No. 258, p. 819-823, https://ssrn.com/abstract=2134932, accesat la data de 2 februarie 2020.

[7] S.J. ROSS, *Creating a Culture of Security, Creating a Culture of Security*, Risk Masters International LLC Presentation, p. 2-4, http://www.pminj.org/16-mtg/files/03njmtg.pdf, accesat la data de 3 martie 2020.

eventualele riscuri, dar şi cu soluțiile de combatere a lor[1]. Aici trebuie să intervină statul prin organismele sale competente. El trebuie să dispună de mijloacele necesare pentru a înfăptui justiția în domeniul cibernetic[2]. Cunoaşterea în profunzime a riscurilor şi a amenințărilor derivate din activitățile desfăşurate în spațiul cibernetic[3], precum şi a modului de prevenire sau de combatere a acestora necesită o strategie eficientă, bazată pe o bună cooperare la nivel internațional între factorii de impact din acest domeniu[4]. Problematica criminalității şi a securității cibernetice[5] a devenit prioritară pentru o serie de state din Uniunea Europeană şi nu numai[6]. Incidentele de securitate cibernetică şi atacurile cibernetice majore cu care s-au confruntat în ultimii ani statele şi organizațiile internaționale au determinat conştientizarea, la nivel global, a necesității adoptării unor strategii şi politici în domeniul securității cibernetice[7].

Pentru a înțelege mai bine implicațiile accesului ilegal în mediul Cloud Computing, pe parcursul întregii lucrări explicăm concepte şi standarde consacrate la nivel internațional de către diferite organisme de specialitate (NIST, CERT, ENISA, ISO, CSA etc.). Studiul accesului ilegal şi al infracționalității informatice din Cloud Computing implică înțelegerea unor noțiuni precum: „mediu informatic", „sistem informatic", „Cloud Computing", „virtualizare", „atac cibernetic", „amenințare", „vulnerabilitate", „securitate", „date informatice" şi altele. Dat fiind specificul temei de cercetare, am definit încă de la începutul lucrării conceptul de mediu informatic şi tehnologia Cloud Computing, aşa cum acestea au fost explicate de către experții din domeniu, precum şi alte concepte relevante referitoare la infracționalitatea informatică. Cercetarea accesului ilegal în mediul Cloud Computing şi a criminalității informatice specifice acestui mediu cibernetic presupune o analiză amplă a dinamicii societății informaționale şi a atacurilor ce au loc asupra

[1] ENISA, *Cyber Security Culture in Organisations*, November 2017, p. 7-9, https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations/at_download/fullReport, accesat la data de 3 martie 2020.

[2] A se vedea B. Urs, *Investigațiile digitale în mediul Cloud Computing...*, *op. cit.*, p. 176.

[3] Deloitte, *Responding to cyber threats in the new reality. A shift in paradigm is vital*, Deloitte & Touche Enterprise Risk Services Pte Ltd White Paper, p. 4-6, https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sea-risk-cyber-thought-leadership-noexp.pdf, accesat la data de 3 martie 2020.

[4] CERT.RO, *Cyber security strategy of Romania*, Document NCSS-RO, p. 6-7, https://cert.ro/vezi/document/NCSS-Ro, accesat la data de 3 martie 2020.

[5] European Commission, *Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions „Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace"*, *op. cit.*, p. 2-5.

[6] European Parliament, *Cybersecurity in the EU Common Security and Defence Policy (CSDP). Challenges and risks for the EU*, *op. cit.*, p. 7-9, 10, 27, 36-37.

[7] H.G. nr. 271/2013 pentru aprobarea Strategiei de securitate cibernetică a României şi a Planului de acțiune la nivel național privind implementarea Sistemului național de securitate cibernetică, p. 4-5.

mediului Cloud sau a atacurilor ce sunt realizate cu ajutorul serviciilor şi a resurselor de tip Cloud Computing.

Conform unui studiu realizat de United Nations Office on Drugs and Crime (UNODC)[1], criminalitatea informatică a luat o amploare semnificativă din cauza conectivității globale. Cele două rapoarte efectuate de Symantec în anul 2016[2], respectiv 2017[3] confirmă acest aspect. Spre deosebire de formele clasice sau tradiționale (fizice) de comitere a infracțiunilor, criminalitatea informatică este mult mai greu de detectat, mai ales dacă este vorba despre o persoană care „şterge" urmele activității sale infracționale[4]. Mai mult, fenomenul infracțional informatic este adesea dificil de localizat în termeni jurisdicționali, având în vedere caracterul transfrontalier al rețelelor informatice[5]. Adesea, infractorii cibernetici utilizează metode noi sau le adaptează şi le transformă pe cele de care dispun prin intermediul diferitelor echipamente, programe şi viruşi informatici, toate în scopul de a-şi desfăşura activitatea ilicită. De multe ori, aceştia încearcă să creeze dificultăți pentru organele cu rol în aplicarea legii penale, prin exploatarea lacunelor din legislația națională sau a lacunelor existente în legislația altor state[6]. Dacă ne raportăm la consecințe, activitatea infracțională exercitată în spațiul cibernetic poate lua diferite forme severe, în funcție de impactul negativ asupra victimelor[7]. În ceea ce ne priveşte, dorim ca prin intermediul cercetării noastre să găsim soluții la problema accesului ilegal şi a criminalității informatice din mediul Cloud Computing. Considerăm că cercetarea din acest domeniu interdisciplinar necesită o abordare specializată pe diferite

[1] UNODC, *Comprehensive Study on Cybercrime. Draft – February 2013*, *op. cit.*, p. 4, 6, 7.

[2] Symantec, *Internet Security Threat Report (ISTR)*, vol. 21, April 2016, p. 8, https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf, accesat la data de 7 noiembrie 2017.

[3] Symantec, *Internet Security Threat Report (ISTR)*, vol. 22, April 2017, p. 10-12, https://digitalhubshare.symantec.com/content/dam/Atlantis/campaigns-and-launches/FY17/Threat%20Protection/ISTR22_Main-FINAL-JUN8.pdf, accesat la data de 7 noiembrie 2017.

[4] S.W. Brenner, *Cybercrime Investigation and Prosecution: The Role of Penal and Procedural Law*, 2001, p. 14-17, https://pdfs.semanticscholar.org/b034/fbe9599d105e54be889cccae9552da203cab.pdf, accesat la data de 7 noiembrie 2017.

[5] I. Vasiu, L. Vasiu, *Malicious Cyber Activity Distribution, Attribution, and Retribution*, în Advanced Cyberlaw and Electronic Security, Accent Publishing, 2017, p. 9-19, https://ssrn.com/abstract=2966010, accesat la data de 7 noiembrie 2017.

[6] V.S. Chowbe, *The Concept of Cyber-Crime: Nature & Scope*, 2011, https://ssrn.com/abstract=1766238, http://dx.doi.org/10.2139/ssrn.1766238, accesat la data de 7 noiembrie 2017.

[7] Norton, *Cybercrime Report: The Human Impact*, 2010, p. 5, 9, 14-15, https://www.symantec.com/content/en/us/home_homeoffice/media/pdf/cybercrime_report/Norton_USA-Human%20Impact-A4_Aug4-2.pdf, accesat la data de 7 noiembrie 2017.

ramuri ale criminalității informatice, respectiv pe analiza şi studiul mediilor informatice complexe, şi nu doar o abordare generală[1].

Studiul realizat de către compania Symantec[2] relevă faptul că exploatarea rețelelor informatice, furtul de identitate, spionajul cibernetic, propagarea de malware, crearea de botnet-uri şi altele asemenea sunt incidente care s-au extins în ultimii ani într-un fenomen major global ce afectează industria, apărarea, aplicarea legii, mediul academic şi sectorul privat. Pericolul reprezentat de fenomenul infracțional este cât se poate de real[3]. Fie că este vorba despre utilizatori legitimi sau despre infractori cibernetici, pentru toți Cloud Computing-ul a devenit extrem de folositor[4]. Ne referim aici la infractori cibernetici specializați, care cu ajutorul resurselor oferite de tehnologia Cloud Computing îşi extind rapid activitățile ilegale pentru a comite în spațiul cibernetic infracțiuni din ce în ce mai diverse şi mai greu de depistat (fraude informatice, spionaj industrial, terorism cibernetic, pornografie infantilă etc.)[5].

Din perspectiva noastră, contextul în care ne aflăm este unul propice studiului acestui mediu informatic dinamic. Agenția Uniunii Europene pentru Securitatea Rețelelor şi a Informațiilor (ENISA) arată într-un ghid[6] faptul că nimeni nu garantează că furnizorii de servicii de tip Cloud nu permit accesul la informațiile stocate în Cloud unor terțe părți, fie că este vorba despre organizații private sau guvernamentale. Mai mult, în cazul unor atacuri informatice direcționate cu un scop precis, anumite informații sensibile localizate în Cloud ar putea ajunge în mâinile atacatorilor. Cantitatea vastă de date ce este transferată în cadrul rețelelor şi infrastructurii de tip Cloud Computing devine o țintă atractivă şi astfel securitatea mediului informatic devine indispensabilă[7]. Conform T-CY Cloud Evidence Group, Cloud Computing-ul creează o serie de provocări legate de mijloacele de combatere a atacurilor,

---

[1] Această secțiune a fost publicată de B. URS, *Cloud Computing – mediul propice...*, *op. cit.*, p. 145-146.

[2] Symantec, *Internet Security Threat Report (ISTR)*, 2017, p. 16-21, https://resource.elq.symantec.com/e/f2., accesat la data de 7 noiembrie 2017.

[3] Information Warfare Monitor, Shadowserver Foundation, *Shadows in the Cloud: Investigating Cyber Espionage 2.0*, Joint Report, R03-2010 Web Version, p. 2, http://www.nartv.org/mirror/shadows-in-the-cloud.pdf, accesat la data de 7 noiembrie 2017.

[4] U. GASSER, *Cloud Innovation and the Law: Issues, Approaches, and Interplay*, The Berkman Center for Internet & Society Research, 2410271 Research Publication No. 2014-7, March 17, 2014, p. 2-5, http://ssrn.com/abstract=2410271, accesat la data de 7 noiembrie 2017.

[5] E. MILLS, *Cybercrime moves to the cloud*, https://www.cnet.com/news/cyber crime-moves-to-the-cloud/, accesat la data de 7 noiembrie 2017.

[6] ENISA, *Cloud Security Guide for SMEs*, April 2015, p. 4, https://www.enisa.europa.eu/publications/cloud-security-guide-for-smes/at_download/fullReport, accesat la data de 7 noiembrie 2017.

[7] L. TAWALBEH, G. SALDAMLI, *Reconsidering big data security and privacy in cloud and mobile cloud systems*, în Journal of King Saud University – Computer and Information Sciences, 2019, p. 4, 5, 7, https://www.sciencedirect.com/science/article/pii/S1319157819303337?via%3Dihub, accesat la data de 2 noiembrie 2020.

dar şi provocări referitoare la impedimentele cu care se confruntă organele cu rol în aplicarea legii, cum ar fi imposibilitatea de a localiza eficient datele stocate şi procesate în mediul informatic[1].

Cloud Computing-ul reprezintă una dintre cele mai importante evoluții tehnologice apărute în ultimii ani. Avantajele utilizării în mod curent a mediului şi a tehnologiei de tip Cloud au dus la adoptarea la scară largă a acestor servicii şi rețele informatice. Tehnologia şi serviciile de tip Cloud Computing constau în utilizarea rețelelor informatice, în special a Internetului, pentru a permite utilizatorilor accesul rapid la aplicații şi platforme digitale[2]. Capacitatea de prelucrare şi stocare a datelor informatice, dar şi spațiul extensiv pentru memorie sunt elemente care determină alegerea unor astfel de servicii digitale[3]. În general, utilizatorii recurg la folosirea resurselor informatice de tip Cloud Computing datorită costurilor reduse. Întrucât resursele sunt accesibile la cerere, ele pot fi configurate după nevoile utilizatorilor[4]. Altfel spus, expansiunea acestor noi tipuri de tehnologii poate fi explicată, pe de o parte, de eficacitatea costurilor pe care o implică utilizarea lor la scară largă (în comparație cu tehnologii similare), iar, pe de altă parte, poate fi explicată şi de caracterul dinamic al infrastructurii şi serviciilor de tip Cloud Computing[5].

Mediul informatic, respectiv arhitectura şi sistemele care stau la baza tehnologiei Cloud Computing, prezintă complexitate atât din punct de vedere tehnic, cât şi legal. Din punct de vedere tehnic, Cloud Computing-ul acoperă aproape toate aspectele ce privesc tehnologia informației şi a

---

[1] T-CY Cloud Evidence Gro, Cybercrime Convention Committee (T-CY), *Criminal justice access to data in the cloud: Cooperation with „foreign" service providers*, Background paper prepared by the T-CY Cloud Evidence Group, T-CY (2016)2, p. 5-7, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168064b77d, accesat la data de 7 noiembrie 2017.

[2] S.K. CHOUDHARY, R.S. JADOUN, H.L. MANDORIYA, A. KUMAR, *Latest development of cloud computing technology, characteristics, challenge, services & applications*, în OSR Journal of Computer Engineering, vol. 16, nr. 6/2014, p. 57-58, 60-61, https://www.researchgate.net/publication/284455605_Latest_development_of_cloud_computing_technology_characteristics_challenge_services_applications, accesat la data de 2 noiembrie 2020.

[3] Grupul de lucru pentru protecția datelor instituit în temeiul Articolului 29 – 01037/12/RO WG196, *Avizul nr. 05/2012 privind „cloud computing", adoptat la 1 iulie 2012*, p. 5, http://ec.europa.eu/justice/data-protection/index_ro.htm, accesat la data de 9 noiembrie 2017.

[4] A. SHAWIS, M. SALAMA, *Cloud Computing: Paradigms and Technologies*, p. 43, http://www.springer.com/cda/content/document/cda_downloaddocument/9783642350153-c2.pdf?SGWID=0-0-45-1429336-p175276227, accesat la data de 9 noiembrie 2017.

[5] L. ALBOAIE, *Cloud Computing – Properties and characteristics*, Concurrent and Distributed Programming, Master Course 2017, „Alexandru Ioan Cuza" University of Iasi, Faculty of Computer Science, p. 10, https://profs.info.uaic.ro/~adria/teach/courses/pcd/resources/C3_CloudComputing_en.pdf, accesat la data de 9 noiembrie 2017.

comunicațiilor[1]. Calculatoarele, mijloacele de stocare, echipamentele de rețea, Internetul, echipamentele pentru crearea, procesarea, stocarea, securitatea şi fluxul datelor în formă electronică, toate se regăsesc într-o formă sau alta în această tehnologie digitală. Cloud-ul nu este doar un server, ci mai degrabă o platformă ce îmbină o serie de echipamente fizice (hardware) cu virtualizarea, instrumentele automate, sistemele de operare, dar şi o serie de aplicații (software) care sunt utilizate pentru a îndeplini funcții-cheie în cadrul rețelei şi al infrastructurii[2]. Pe plan mondial, există o varietate largă de servicii de tip Cloud Computing care sunt oferite de către diverşi furnizori din industria tehnologiei informației[3]. Printre acestea putem enumera: aplicații de tip software, sisteme de prelucrare a datelor, servicii de comunicații, servicii de asistență pentru dezvoltarea de aplicații şi găzduirea web avansată, maşinării virtuale, spațiu de stocare şi altele[4].

Din punct de vedere legal, Cloud Computing-ul este un mediu informatic propice activităților infracționale. La fel ca în cazul altor componente ale spațiului cibernetic, de exemplu, rețelele de socializare (apariția şi dezvoltarea rețelelor de socializare contribuie în mod direct la infracționalitatea tradițională şi la cea informatică[5]), odată cu creşterea numărului de utilizatori ai tehnologiei Cloud Computing, criminalitatea cibernetică specifică acestui mediu informatic a luat amploare[6]. În ultimii ani, o parte semnificativă a criminalității informatice a început să se deplaseze spre zona de Cloud Computing[7]. O posibilă explicație a acestui fenomen ar fi aceea că sunt utilizate resursele informatice externe din Cloud pentru a lansa şi executa diferite activități infracționale de la distanță şi din orice locație (adesea, cei ce săvârşesc infracțiuni informatice cu ajutorul sistemelor şi serviciilor Cloud Computing se află în state diferite)[8]. Din punctul nostru de vedere, marea

[1] Q. Zhang, L. Cheng, R. Boutaba, *Cloud computing: state-of-the-art and research challenges*, în Journal of Internet Services and Applications, vol. 1, 2010, DOI 10.1007/s13174-010-0007-6, p. 9-12, http://ai2-s2-pdfs.s3.amazonaws.com/6109/3ca3afcc72f04bebbbad7b9fd98d09438122.pdf, accesat la data de 9 noiembrie 2017.

[2] D. Quintero, R. Ceron, R. Garcia da Silva, A. Ghosal, V. Hu, H.C. Li, K. Marthi, S.F. Shi, S. Velica, *Technical Computing Clouds*, IBM RedBook, October 2013, p. 5, 8-11, http://www.redbooks.ibm.com/redbooks/pdfs/sg248144.pdf, accesat la data de 9 noiembrie 2017.

[3] KPMG, *Journey to the Cloud*, p. 3-5, 6, 8, https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2017/02/the-creative-cios-agenda-journey-to-cloud.Pdf, accesat la data de 9 noiembrie 2017.

[4] Această secțiune a fost publicată de B. Urs, *Cloud Computing – mediul propice...*, *op. cit.*, p. 143.

[5] S. Ackerman, K. Schutte, *Social Media as a Vector for Cyber Crime*, April 7, 2015, p. 2, 8, 11, 12, 39-41, https://www.isaca.org/chapters5/Cincinnati/Events/Documents/Past%20Presentations/2015/Social%20Media%20as%20Vector%20for%20Cyber%20Crime.pdf, accesat la data de 9 noiembrie 2017.

[6] J. Plunkett, N. Le-Khac, M. Kechadi, *op. cit.*, p. 3-5.

[7] E. Mills, *op. cit.*

[8] G. Meyer, A. Stander, *Cloud Computing: The Digital Forensics Challenge*, Proceedings of Informing Science & IT Education Conference (InSITE), 2015, p. 286, 291,

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 şi aplicații). Sub aspect legal, ne interesează în mod direct factorii care facilitează acest proces de migrație, întrucât este vorba despre studiul fenomenului infracțional (aplicarea legii penale, jurisdicția[1], investigarea infracțiunilor[2] şi tragerea la răspundere a celor ce săvârşesc infracțiuni în mediul informatic). În prezent, evoluția sistemelor de calcul se află în strânsă legătură cu evoluția criminalității informatice. Din păcate, mijloacele de săvârşire a infracțiunilor informatice au devenit din ce în ce mai complexe, însă aceasta este doar o parte a problemei. Cealaltă parte a problemei constă în faptul că aceste mijloace au devenit uşor de utilizat[3].

## *Secţiunea a 2-a. Migraţia infracţionalităţii informatice spre mediul Cloud Computing*

Cloud-ul a devenit tehnologia principală de stocare şi procesare a datelor. Fie că vorbim despre companii, organizații guvernamentale sau utilizatori privați[4], într-o formă sau alta toți folosesc mediul şi tehnologia Cloud Computing[5]. Mulți utilizatori au început să migreze către zona de Cloud Computing, iar în prezent majoritatea companiilor îşi mută aplicațiile şi îşi stochează datele în Cloud[6]. De asemenea, există şi companii care folosesc doar anumite servicii de tip Cloud, însă multe dintre acestea intenționează în curând să migreze în Cloud. Motivele ce determină această tranziție sunt

---

http://proceedings.informingscience.org/InSITE2015/InSITE15p285-299Meyer1562.pdf, accesat la data de 9 noiembrie 2017.

[1] H. ENNAJAH, E. CHOW, *op. cit.*, p. 47, 50, 52-53.

[2] X. FU, Z. LING, W. YU, J. LUO, *Cyber Crime Scene Investigations (C2SI) through Cloud Computing*, IEEE 30th International Conference on Distributed Computing Systems Workshops, p. 1-3, http://www.cs.uml.edu/~xinwenfu/paper/SPCC10_Fu.pdf, accesat la data de 9 noiembrie 2017.

[3] Această secțiune a fost publicată de B. URS, *Cloud Computing – mediul propice...*, *op. cit.*, p. 144.

[4] Government Business, *Cloud migration: The key considerations for the public sector*, https://governmentbusiness.co.uk/features/cloud-migration-key-considerations-public-sector, accesat la data de 5 mai 2020.

[5] Wired, *The Government's Mass Migration to the Cloud*, https://www.wired.com/insights/2012/07/government-cloud-migration/, accesat la data de 5 mai 2020.

[6] M. MOHAMED, A. ABDEL-MAWGOUD, E. AL-KADY, M. BESHAY, *Cloud Migration Strategy for Legacy Systems using AWS Platform*, Cairo Technical Report 2019, p. 7-8, https://www.researchgate.net/publication/335390319_Cloud_Migration_Strategy_for_Legacy_Systems_using_AWS_Platform, accesat la data de 5 mai 2020.

diverse şi multiple. Unele companii îşi modernizează platformele de date pentru a beneficia de noi aplicații şi servicii avansate. Alți utilizatori aleg Cloud-ul din motive de securitate sau pentru costurile şi performanța ridicată oferite de mediul informatic[1]. Dar, concret, ce presupune acest proces şi cum se realizează? În linii mari, migrația în Cloud sau către mediul Cloud reprezintă un proces de mutare a operațiunilor digitale către zona de Cloud Computing. În esență, tot acest proces este similar cu mutarea fizică, cu excepția faptului că implică transferul datelor, al aplicațiilor şi proceselor digitale către un centru de date ce aparține furnizorilor de servicii Cloud Computing[2].

La fel ca în cazul oricărui proces de tranziție, migrația către Cloud necesită o informare corespunzătoare cu privire la date, aplicații şi servicii, precum şi o pregătire temeinică înainte de începerea procesului[3]. Nu este vorba despre un proces dificil de realizat, din contră, este un proces facil ce va aduce beneficii utilizatorilor. Fie că sunt atraşi de costuri reduse sau din alte motive, este cert că utilizatorii se vor bucura de o mai bună flexibilitate în ceea ce priveşte resursele şi serviciile, fiindcă toate aceste beneficii vin în sprijinul companiilor şi al utilizatorilor[4]. Pe scurt, migrația în Cloud presupune trecerea de la infrastructura proprie sau locală către o infrastructură de tip Cloud. Migrația poate implica unul[5] sau mai multe modele şi tipuri de Cloud[6]. Unele dintre acestea pot să fie publice, caz în care serviciile sunt livrate prin Internet, iar altele pot să fie private, constând într-o infrastructură Cloud securizată, ce este disponibilă doar pentru o anumită organizație[7]. De asemenea, pot să fie utilizate în acest proces în mod obişnuit mai multe

---

[1] Deloitte, *Why organizations are moving to the cloud*, https://www2.deloitte.com/us/en/insights/industry/technology/why-organizations-are-moving-to-the-cloud.html, accesat la data de 5 mai 2020.

[2] M. BHOPALE, *Cloud Migration Benefits and Its Challenges Issue*, în OSR Journal of Computer Engineering, p. 41, 42, 44, http://www.iosrjournals.org/iosr-jce/papers/sicete-volume1/8.pdf, accesat la data de 5 mai 2020.

[3] AppDynamics, *What is Cloud Migration?*, https://www.appdynamics.com/solutions/cloud/cloud-migration/what-is-cloud-migration, accesat la data de 5 mai 2020.

[4] A. KHAJEH-HOSSEINI, D. GRENWOOD, I. SOMMERVILLE, *Cloud Migration: A Case Study of Migrating an Enterprise IT System to IaaS*, IEEE 3rd International Conference on Cloud Computing, 2010, p. 3-5, 7, 8, https://arxiv.org/ftp/arxiv/papers/1002/1002.3492.pdf, accesat la data de 5 mai 2020.

[5] C. PAHL, H. XIONG, *Migration to PaaS Clouds – Migration Process and Architectural Concerns*, IEEE 7th International Symposium on the Maintenance and Evolution of Service-Oriented and Cloud-Based Systems, 2013, p. 4, 5, http://doras.dcu.ie/19227/1/MESOCA13.pdf, accesat la data de 5 mai 2020.

[6] C. PAHL, H. XIONG, R. WALSHE, *A Comparison of On-premise to Cloud Migration Approaches*, European Conference on Service-Oriented and Cloud Computing (ESOCC 2013), p. 3, 5, 6, 8, 11, 13, https://doras.dcu.ie/18475/1/migration.pdf, accesat la data de 5 mai 2020.

[7] AWS, *Migrating your Existing Applications to the AWS Cloud*, p. 4, 5, 8-9, 10, 12, https://d0.awsstatic.com/whitepapers/cloud-migration-main.pdf, accesat la data de 5 mai 2020.

tipuri de Cloud, atât publice, cât şi private sau într-un mediu Cloud hibrid ori poate fi ales un mediu Cloud de tip comunitar[1]. Practic, fiecare utilizator poate migra către un tip sau un model anume de Cloud în funcție de propriile necesități[2].

În ceea ce priveşte soluțiile şi tehnologiile de calcul, fie că ne referim la cele de tip hardware sau software, acestea ajung să se învechească şi să fie ineficiente în scurt timp[3]. Prin urmare, deşi la un moment dat aceste soluții sunt funcționale şi dau randament, după trecerea timpului ele îşi pierde din eficiență. Ritmul alert de dezvoltare a tehnologiilor digitale este de natură să cauzeze rapid un proces de înlocuire a echipamentelor de calcul[4]. Utilizatorii ce rulează aplicații şi sisteme mai vechi sunt nevoiți să le schimbe[5] pentru a nu rămâne în urma concurenței lor şi pentru a nu risca pierderea sau procesarea ineficientă a datelor lor informatice. În plus, elementele hardware şi software vechi pot să fie nesigure sau pot rula extrem de lent, fapt ce îngreunează mult procesul tehnologic şi munca utilizatorilor. Infrastructura de serviciu utilizată de companii include servere, echipamente de rețea, aplicații, baze de date şi orice alt software sau hardware necesar pentru desfăşurarea activității[6]. Fie că ne referim la o companie, o instituție sau un utilizator privat, regulile tehnologiei se aplică în mod universal, iar trecerea timpului este aplicabilă şi dispozitivelor electronice. Infrastructura veche, cum ar fi sistemele învechite sau dispozitive firewall fizice neactualizate, pot încetini procesele acestor entități[7]. De asemenea, dacă la toate acestea adăugăm riscurile de securitate, este lesne de înțeles de ce tehnologia trebuie reînnoită în mod constant[8]. În general, infrastructura veche

---

[1] Denizon, *Hybrid Cloud Migration*, https://www.denizon.com/hybrid-cloud-migration/, accesat la data de 5 mai 2020.

[2] IBM, *What is cloud migration?*, https://www.ibm.com/cloud/learn/cloud-migration, accesat la data de 5 mai 2020.

[3] Science ABC, *Why Do Computers Slow Down Over Time?*, https://www.scienceabc.com/eyeopeners/why-do-computers-slow-down-with-time.html, accesat la data de 5 mai 2020.

[4] UNPAN, *Rapid Development of Information Technology in the 20th Century*, p. 2, 5, 9, https://publicadministration.un.org/published/courses/1343/Course2451/v2010_11_2_16_5_13/media/content/Part1_68335.pdf, accesat la data de 5 mai 2020.

[5] O. Asaolu, *On the Emergence of New Computer Technologies*, în Educational Technology & Society, vol. 9, nr. 1/2006, p. 336, 337, https://www.researchgate.net/publication/220374546_On_the_Emergence_of_New_Computer_Technologies, accesat la data de 5 mai 2020.

[6] Cloudflare, *What Is Cloud Migration? Cloud Migration Strategy*, https://www.cloudflare.com/learning/cloud/what-is-cloud-migration/#:~:text=Cloud%20migration%20is%20the%20process%20of%20moving%20digital%20business%20operations,up%20and%20moving%20physical%20goods., accesat la data de 5 mai 2020.

[7] Cisco, *Why Aging Infrastructure Is a Growing Problem*, https://blogs.cisco.com/security/why-aging-infrastructure-is-a-growing-problem, accesat la data de 5 mai 2020.

[8] TrendMicro, *Breaking down old and new threats to critical infrastructure*, https://blog.trendmicro.com/breaking-down-old-and-new-threats-to-critical-infrastructure/, accesat la data de 5 mai 2020.

este găzduită de obicei la fața locului, ceea ce înseamnă că este amplasată fizic în clădiri sau pe proprietăți în care îşi desfăşoară activitatea cei ce o dețin. Costurile de adaptare, îmbunătățire şi înlocuire a unor astfel de echipamente ajung să fie foarte mari în timp[1]. Tocmai de aceea multe dintre aceste companii, instituții şi utilizatori preferă să închirieze servicii de tip Cloud Computing în loc să cumpere echipamente noi şi licențe pentru aplicații[2].

Având în vedere faptul că migrația către mediul Cloud Computing vine la pachet cu o serie de beneficii pentru cei ce aleg să facă acest pas, există mai multe feluri sau tipuri de realizare a procesului de migrație[3]. În general, fie că este vorba despre migrația datelor, a aplicațiilor sau a resurselor, pentru marea majoritate a utilizatorilor, acest proces reprezintă o evoluție naturală. Scopul urmărit de către utilizatorii ce urmează acest proces este unul determinat de necesitățile proprii[4]. Reducerea costurilor, infrastructura îmbunătățită, capacitatea de procesare şi calcul, toți aceşti factori vor determina tipul de migrație ales[5]. Primul tip de migrație este cel al migrației datelor sau, altfel spus, migrația stocării acestora. Procesul presupune mutarea datelor dintr-un spațiu de stocare local către un mediu de stocare în Cloud, mult mai modern şi care oferă capacități de stocare extinsă[6]. Performanța semnificativ mai rapidă şi faptul că datele pot fi replicate şi recuperate instant reprezintă beneficii pentru orice utilizator. Eficiența din punct de vedere al costurilor este şi ea de menționat. De altfel, un spațiu de stocare la nivel local care să fie rapid şi cu o capacitate mare este mult mai dificil de achiziționat din punct de vedere al costurilor decât spațiul de stocare în Cloud[7]. Un al doilea tip de migrație este cel al resurselor de procesare. Procesul de mutare a resurselor presupune trecerea lor către o infrastructură Cloud pentru tot ce ține de procesarea ce se făcea anterior la

[1] Juriba, *The Hidden Costs of Your Aging IT Infrastructure*, https://blog.juriba.com/the-hidden-costs-of-an-aging-it-infrastructure, accesat la data de 5 mai 2020.

[2] Xperience, *Cloud vs On Premise Software: Which is Best for Your Business?*, https://www.xperience-group.com/cloud-vs-on-premise-software/, accesat la data de 5 mai 2020.

[3] Cuelogic, *What are the benefits of cloud migration? Reasons you should migrate*, https://www.cuelogic.com/blog/benefits-of-cloud-migration, accesat la data de 5 mai 2020.

[4] BluePi, *7 Advantages of Cloud Migration*, https://www.bluepiit.com/blog/7-advantages-cloud-migration/, accesat la data de 5 mai 2020.

[5] Morpheus Data, *10 Advantages of Cloud Migration*, https://morpheusdata.com/cloud-blog/10-advantages-of-cloud-migration/, accesat la data de 5 mai 2020.

[6] V. KUSHWAH, A. SAXENA, *A Security Approach for Data Migration in Cloud Computing*, în International Journal of Scientific and Research Publications, vol. 3, nr. 5/2013, p. 3-5, https://www.researchgate.net/publication/236658752_A_Security_approach_for_Data_Migration_in_Cloud_Computing, accesat la data de 5 mai 2020.

[7] M. ANSAR, M. ASHRAF, M. FATIMA, *Data Migration in Cloud: A Systematic Review*, în American Scientific Research Journal for Engineering, Technology, and Sciences, vol. 48, nr. 1/2018, p. 75, 77, 83, 86, https://asrjetsjournal.org/index.php/American_Scientific_Journal/article/download/4450/1573/, accesat la data de 5 mai 2020.

nivel local[1]. Puterea mare de procesare a serviciilor Cloud implică în unele cazuri şi un proces de mutare a datelor, a aplicațiilor sau a altor elemente. În cele mai multe cazuri, implică şi o migrare a stocării datelor[2]. Cel de-al treilea tip de migrație este cel al migrației aplicațiilor. Procesul de mutare a aplicațiilor se face de la nivel local, de pe un dispozitiv personal către aplicații ce rulează în Cloud[3]. Înlocuirea şi înnoirea licențelor pentru aplicații aduc costuri ridicate pentru companii şi utilizatori. Prin închirierea de aplicații la nivel de Cloud, aceste costuri sunt semnificativ reduse[4]. De altfel, mutarea întregii aplicații către un model Cloud presupune transferul de date între şi către infrastructuri Cloud şi, de asemenea, poate implica mutarea datelor informatice[5].

Efectuarea cu succes a migrației[6] către mediul Cloud Computing necesită planificarea şi executarea unei strategii cuprinzătoare, ce stabileşte printre altele obiectivele migrației, creează un calendar, anticipează provocările şi defineşte succesul proiectului[7]. Strategiile de migrație iau în considerare ce sarcini de lucru trebuie mutate în Cloud, precum şi ce sarcini rămân la nivel local. În principiu, strategia de migrare ar trebui să acopere cazurile de utilizare specifice pentru fiecare sarcină de lucru[8]. Aceasta poa-

---

[1] H. GOUDARZI, M. GHASEMAZAR, M. PEDRAM, *SLA-based Optimization of Power and Migration Cost in Cloud Computing*, 12th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID 2012), p. 1-3, http://sportlab.usc.edu/~hadi/index_files/SLA-based%20Optimization%20of%20Power%20and%20Migration%20Cost%20in%20Cloud%20Computing.pdf, accesat la data de 5 mai 2020.

[2] Nimbo, *Data Center Migration to the Cloud*, March 2015, p. 4, 5, 7, https://d0.awsstatic.com/whitepapers/datacenter-migration-to-the-cloud-Nimbo.pdf, accesat la data de 5 mai 2020.

[3] V. TRAN, J. KEUNG, A. LIU, A. FEKETE, *Application Migration to Cloud: A Taxonomy of Critical Factors*, SECLOUD '11: Proceedings of the 2nd International Workshop on Software Engineering for Cloud Computing, May 2011, DOI: 10.1145/1985500.1985505, p. 3-5, http://echronos.org/publications/nicta_full_text/4977.pdf, accesat la data de 5 mai 2020.

[4] NetApp Blog, *A Guide to Migrating Applications to the Cloud*, 2018, https://blog.netapp.com/a-guide-to-migrating-application-to-the-cloud/, accesat la data de 5 mai 2020.

[5] NetApp, *What Is Data Migration?*, https://www.netapp.com/us/info/what-is-data-migration.aspx, accesat la data de 5 mai 2020.

[6] N. KHAN, A. AL-YASIRI, *Framework for Cloud Computing Adoption: A Road Map for SMEs to Cloud Migration,* în International Journal on Cloud Computing: Services and Architecture, vol. 5, nr. 5-6/2015, p. 5-6, 7, 8, 10, https://arxiv.org/ftp/arxiv/papers/1601/1601.01608.pdf, accesat la data de 5 mai 2020.

[7] New Relic, *Preparing to Adopt the Cloud: A 10-Step Cloud Migration Checklist*, https://blog.newrelic.com/engineering/cloud-migration-checklist/, accesat la data de 5 mai 2020.

[8] J. OPARA-MARTINS, R. SAHANDI, F. TIAN, *Critical analysis of vendor lock-in and its impact on cloud computing migration: a business perspective*, în Journal of Cloud Computing: Advances, Systems and Applications, 2016, DOI: 10.1186/s13677-016-0054-z, p. 5-7, 9, 11, 12, 15, https://link.springer.com/content/pdf/10.1186/s13677-016-0054-z.pdf, accesat la data de 5 mai 2020.

te include aplicații, date, cerințe, necesități şi alte elemente ce sunt necesare strategiei în discuție. Definirea cazurilor de utilizare trebuie să se realizeze în avans pentru a permite astfel crearea unei strategii durabile ce permite executarea cu succes a întregului proces de migrație[1]. De asemenea, strategia de migrație trebuie să acopere în mod obişnuit evaluările riscurilor, bugetul disponibil, elementele de securitate, precum şi tipul sau modelele de Cloud alese, care vor găzdui astfel fiecare dintre sarcinile de lucru ce vor fi relocate. Mai mult, strategiile de migrație ar trebui să abordeze gestionarea mediului informatic într-un mod consecvent şi simplificat[2]. Elementele planului de securitate ar trebui să includă, printre altele, dacă se criptează toate sau anumite tipuri de date, respectarea reglementărilor referitoare la datele în mişcare şi în repaus şi cerințele de replicare. După ce strategia a fost realizată, este necesar să se facă implementarea ei şi apoi să se treacă la etapele de migrație[3]. O abordare pas cu pas poate ajuta la succesul migrației, deoarece aceasta permite efectuarea de ajustări dacă se consideră necesar[4]. În cele mai multe cazuri, paşii sau procesele pe care un utilizator le urmează în timpul procesului de migrație în Cloud variază în funcție de diverşi factori şi de resursele ce se doresc a fi mutate. Pe lângă aceşti factori, putem enumera: cerințele de performanță şi securitate, selectarea unui furnizor de servicii, calculul costurilor, portabilitatea datelor şi a aplicațiilor, integritatea şi securitatea datelor etc.[5]

În prezent, utilizatorii cheltuiesc sume mari de bani dezvoltând şi instalând echipamente şi aplicații de tip hardware şi software necesare pentru a-şi desfăşura activitatea. În esență, conceptul de Cloud Computing presupune închirierea şi mutarea sistemelor şi a resurselor esențiale pentru utilizatorii săi[6]. Cloud Computing-ul vine în sprijinul acestora cu o serie de

---

[1] Flatworld Solutions, *Migrating Data to Cloud – Limitations and Opportunities*, https://www.flatworldsolutions.com/data-management/articles/pros-cons-cloud-data-migration.php, accesat la data de 5 mai 2020.

[2] R. Rai, G. Sahoo, S. Mehfuz, *Exploring the factors influencing the cloud computing adoption: a systematic study on cloud migration*, în SpringerPlus Open Journal, 2015, DOI: 10.1186/s40064-015-0962-2, p. 3, 5, 6, 7-8, https://link.springer.com/content/pdf/10.1186/s40064-015-0962-2.pdf, accesat la data de 5 mai 2020.

[3] Cloud Management Insider, *Cloud Migration Strategy: A Methodology for Cloud Adoption*, https://www.cloudmanagementinsider.com/cloud-migration-transition-from-on-premise-to-cloud/, accesat la data de 5 mai 2020.

[4] IBM, *Strategies, plans, and checklists. Cloud migration strategy*, https://www.ibm.com/cloud/learn/cloud-migration, accesat la data de 5 mai 2020.

[5] TechTarget, *What is cloud migration? An introduction to moving to the cloud*, https://searchcloudcomputing.techtarget.com/definition/cloud-migration, accesat la data de 5 mai 2020.

[6] A. Iqbal, R. Colomo-Palacios, *Key Opportunities and Challenges of Data Migration in Cloud: Results from a Multivocal Literature Review*, în Procedia Computer Science, Special Issue: International Conference on ENTERprise Information Systems (CENTERIS), International Conference on Project MANagement (ProjMAN), International Conference on Health and Social Care Information Systems and Technologies (HCist), vol. 164, 2019, p. 48-55, p. 51-53, https://pdf.sciencedirectassets.com/280203/1-

beneficii, care fac extrem de facilă migrația sau tranziția către acest mediu informatic. Principalul beneficiu al acestor servicii, dacă putem spune aşa, îl reprezintă costurile reduse. Trecerea la Cloud Computing îi scuteşte pe utilizatori de achiziționarea unor echipamente scumpe, aceştia fiind nevoiți să plătească numai pentru serviciile alese. Cloud Computing-ul promite o putere de calcul sporită, minimizând în acelaşi timp cerințele operaționale. De altfel, tehnologia presupune şi reducerea costurilor cu energia electrică[1]. Un alt beneficiu oferit de Cloud Computing, ce stă la baza migrației către acest mediu informatic, îl reprezintă securitatea. Furnizorii de servicii oferă soluții digitale sigure. Aceştia fac investiții masive în resurse şi tehnologie tocmai pentru a oferi un nivel ridicat de securitate şi integritate a datelor informatice. În cele mai multe cazuri, stocarea datelor în Cloud Computing este mai sigură decât stocarea pe servere fizice sau în locații proprii[2]. Mai mult, cei ce dețin date în Cloud le pot şterge de la distanță sau le pot muta rapid în altă locație Cloud[3]. Flexibilitatea reprezintă un alt beneficiu adus de către tehnologia Cloud Computing. Cu un spațiu de stocare flexibil şi cu resurse configurabile, Cloud-ul devine extrem de atractiv pentru utilizatori[4]. Practic, utilizatorii beneficiază de performanțe ridicate, iar în cazul în care cerințele lor cresc sau scad, aceştia pot face rapid ajustările necesare. Tot ce trebuie să facă este să acceseze datele sau resursele din Cloud şi să le configureze în funcție de noile necesități. Un alt beneficiu sau motiv pentru care utilizatorii migrează către mediul Cloud este spectrul larg de opțiuni disponibile. Gama largă de modele şi opțiuni aduce caracteristici şi tarife diverse pentru fiecare serviciu de care utilizatorul are nevoie[5].

Conectivitatea şi accesibilitatea stau la baza migrației către acest mediu informatic extrem de dinamic. Cloud-ul menține utilizatorii conectați indiferent unde lucrează, oricând şi oriunde. Utilizatorii pot accesa fişiere oricând,

---

s2.0-S1877050920X00020/1-s2.0-S1877050919321921/main.pdf, accesat la data de 5 mai 2020.

[1] Webroot, *5 Financial Benefits of Moving to the Cloud. How SMBs and small/home office users can save money with cloud computing*, https://www.webroot.com/ie/en/resources/tips-articles/five-financial-benefits-of-moving-to-the-cloud, accesat la data de 5 mai 2020.

[2] GrowthBusiness, *7 reasons why your business needs to move to the cloud*, https://www.growthbusiness.co.uk/7-reasons-business-needs-move-cloud-2552054/, accesat la data de 5 mai 2020.

[3] IBIS Technology, *7 Reasons Why You Should Move from On-Premise to Cloud Computing*,
https://ibistechnology.com/why-you-should-move-from-on-premise-to-cloud-computing/, accesat la data de 5 mai 2020.

[4] Software Advisory Service, *12 Benefits of Moving to the Cloud in 2019*, https://www.softwareadvisoryservice.com/en/blog/why-move-to-the-cloud-12-benefits-of-cloud-computing-in-2019/#:~:text=Moving%20to%20the%20cloud%20means,protect%20and%20recover%20your%20data., accesat la data de 5 mai 2020.

[5] Xpedition, *8 advantages of moving to the cloud*, https://www.xpedition.co.uk/article/should-i-move-to-the-cloud-8-reasons-why-you-need-to/, accesat la data de 5 mai 2020.

oriunde, folosind orice dispozitiv. Aceasta înseamnă că nu mai există riscul ca fişierele să fie stocate într-un calculator izolat. Mai mult, serviciile Cloud beneficiază de o implementare rapidă[1], practic acestea pot fi implementate în câteva ore sau zile, ceea ce este mult mai rapid decât săptămânile, lunile sau anii necesari pentru planificarea strategică, cumpărarea, construirea şi implementarea unei infrastructuri personale.

În cele din urmă, este important să menționăm că în calea migrației către mediul Cloud Computing pot exista şi anumite inconveniente, riscuri[2] sau chiar dezavantaje[3]. Printre acestea[4] se numără dependența de platformă şi de furnizorul de servicii, latența[5] şi timpul în care serviciile nu funcționează[6], complexitatea arhitecturii Cloud[7], precum şi anumite aplicații ce nu sunt implementate în mod corespunzător[8]. Din punctul nostru de vedere, toate beneficiile aduse de către migrația în Cloud Computing înlătură în mare parte aproape orice inconvenient legat de acest proces de tranziție, cu excepția, bineînțeles, a fenomenului infracțional.

Criminalitatea informatică reprezintă un fenomen actual ce se desfăşoară la nivel global. Amploarea fenomenului infracțional din diferite medii şi tehnologii digitale este generată, pe de o parte, de atacurile informatice din ce în ce mai complexe şi mai frecvente, iar, pe de altă parte, ea se datorează noilor tehnologii ce facilitează acest fenomen. Cloud Computing-ul[9], rețelele de socializare[10], monedele virtuale de

[1] Salesforce Blog, *Why Move to the Cloud? 10 Benefits of Cloud Computing*, https://www.salesforce.com/uk/blog/2015/11/why-move-to-the-cloud-10-benefits-of-cloud-computing.html, accesat la data de 5 mai 2020.

[2] InformationWeek, *Cloud Migration: 12 Risks and How to Avoid Them*, https://www.informationweek.com/cloud/cloud-migration-12-risks-and-how-to-avoid-them/a/d-id/1336756, accesat la data de 5 mai 2020.

[3] CPO Magazine, *Lift and Shift Cloud Migration: Benefits, Disadvantages and Use Cases*, 2019, https://www.cpomagazine.com/cyber-security/lift-and-shift-cloud-migration-benefits-disadvantages-and-use-cases/, accesat la data de 5 mai 2020.

[4] T. Morrow, *12 Risks, Threats, & Vulnerabilities in Moving to the Cloud*, Carnegie Mellon University Software Engineering Institute, 2018, https://insights.sei.cmu.edu/sei_blog/2018/03/12-risks-threats-vulnerabilities-in-moving-to-the-cloud.html, accesat la data de 5 mai 2020.

[5] TechTarget, *What are some cloud migration challenges or limitations?*, https://searchstorage.techtarget.com/answer/What-are-some-cloud-migration-challenges-or-limitations, accesat la data de 5 mai 2020.

[6] Dinarys, *9 Cloud Migration Risks to Consider*, https://dinarys.com/blog/9-cloud-migration-risks-to-consider, accesat la data de 5 mai 2020.

[7] N-IX, *7 risks in cloud migration and how to avoid them*, https://www.n-ix.com/risks-cloud-migration-how-avoid/, accesat la data de 5 mai 2020.

[8] IBM, *Cloud migration risks*, https://www.ibm.com/cloud/learn/cloud-migration, accesat la data de 5 mai 2020.

[9] ITU, *Understanding cybercrime: Phenomena, challenges and legal response*, *op. cit.*, 2012, p. 84.

[10] ITU, *Social media companies contribute to cybercrime*, în The Insider, vol. 14, 2012, p. 2-3, http://www.impact-alliance.org/download/pdf/resource-centre/newsletter/IMPACT-insider-vol14.pdf, accesat la data de 11 noiembrie 2017.

tipul Bitcoins[1] sau volumele mari de date (Big Data)[2] sunt doar câteva exemple de tendințe şi tehnologii moderne care facilitează criminalitatea informatică existentă în prezent[3]. Spre deosebire de formele tradiționale sau clasice ale criminalității din societate, infracționalitatea informatică presupune utilizarea unor dispozitive electronice, în special a sistemelor informatice şi a altor dispozitive digitale. Dacă în cazul infracționalității tradiționale interacțiunile sunt preponderent fizice (de exemplu, furtul unui obiect), în cazul infracționalității informatice evenimentele se desfăşoară în general fără să fie necesară o interacțiune de ordin fizic (de exemplu, alterarea unor date informatice)[4].

Criminalitatea informatică poate fi explicată şi prin prisma disponibilității mijloacelor şi a dispozitivelor electronice cu care sunt săvârşite astfel de infracțiuni[5]. Acest aspect constituie unul dintre motivele ce au determinat o schimbare a raportului dintre cele două forme ale criminalității din societatea noastră[6], respectiv au determinat în ultimii ani creşterea infracționalității informatice în raport cu infracționalitatea clasică[7]. Pericolul reprezentat de infracționalitatea informatică este unul serios şi derivă dintr-o serie de consecințe grave pe care infracțiunile şi atacurile informatice le pot avea asupra siguranței cetățenilor, a statelor sau chiar la nivel internațional[8]. Frecvent ținte ale unor atacuri cibernetice periculoase sunt chiar persoane, companii, infrastructuri naționale şi guverne. Criptarea şi anonimizarea constituie o mare problemă în încercarea de a opri fenomenul ce se desfăşoară la nivel global[9]. Utilizarea unor programe şi dispozitive de tip malware poate fi uşor ascunsă[10]. Tocmai de aceea este dificil să se

---

[1] ITU, *Understanding cybercrime: Phenomena, challenges and legal response*, *op. cit.*, 2012, p. 39.

[2] A.M. ALMADAHKAH, *Big Data in Computer Cyber Security Systems*, în International Journal of Computer Science and Network Security, vol. 16, nr. 4/2016, p. 56-57, 61-63, http://paper.ijcsns.org/07_book/201604/20160409.pdf, accesat la data de 11 noiembrie 2017.

[3] A.D. SOFAER, S.E. GOODMAN, *op. cit.*, p. 1-3, 6, 7.

[4] Tutorialspoint, *Cyber Law Objectives – Emerging Trends of Cyber Law*, https://www.tutorialspoint.com/information_security_cyber_law/cyber_law_objectives.htm.

[5] Security Alliance, *The Convergence of Cybercrime and Traditional Crime*, https://www.secalliance.com/blog/convergence-cybercrime-traditional-crime/.

[6] K. MITNICK, *Cyber Crime and Traditional Crime – Are They Connected? Turn the Alarm Back on Improving Good Governance with E-Policy Management*, în e-Security, CyberSecurity Malaysia, vol. 26, nr. 1/2011, p. 3, 5, 8-9, http://www.cybersecurity.my/data/content_files/12/852.pdf, accesat la data de 11 noiembrie 2017.

[7] KrebsOnSecurity, *Cybercrime Overtakes Traditional Crime in UK*, https://krebsonsecurity.com/2016/07/cybercrime-overtakes-traditional-crime-in-uk/.

[8] Tutorialspoint, *Cyber Crime – Nature of Threat*, https://www.tutorialspoint.com/information_security_cyber_law/introduction.htm, accesat la data de 11 noiembrie 2017.

[9] Această secțiune a fost publicată de B. URS, *Migrația criminalității informatice în mediul Cloud Computing*, în Dreptul nr. 6/2018, p. 148.

[10] A. SEGER, *Cybercrime: threats and challenges*, Workshop on cybercrime legislation and training of judges, p. 2, 3, 6, http://www.coe.int/t/dg1/legalcooperation/economic

determine exact identitatea sau originea atacatorului. În multe cazuri, motivația acestuia poate reprezenta o enigmă. De altfel, elemente precum ținta, efectele şi circumstanțele în care s-au desfăşurat evenimentele pot furniza unele indicii cu privire la atacator[1]. Libertatea de a acționa într-un spațiu fără frontiere este nelimitată. De multe ori, criminali cibernetici, terorişti sau chiar state reprezintă sursa acestor atacuri informatice. Posibilitățile de comitere a unor astfel de atacuri sunt nelimitate[2], iar în fiecare zi apar noi forme şi metode de propagare a acțiunilor dăunătoare[3].

Analiza unui mediu informatic complex cum este şi Cloud Computing-ul presupune culegerea anumitor date statistice[4] publicate de către organisme de specialitate[5]. Conform unui studiu realizat de Centrul European de Criminalitate Informatică al Europol[6], mai mult de 30% dintre țările europene au în desfăşurare investigații digitale privind activități de criminalitate informatică în Cloud Computing, ceea ce însemnă că deja a început fenomenul migrației criminalității informatice spre zona de Cloud Computing. Majoritatea țărilor care au furnizat informații pentru întocmirea acestui raport apreciază că amenințările ce vizează mediul Cloud sunt cotate între medii sau mari ca gravitate, fiind, totodată, în creştere. Aproape 50% dintre autoritățile care au rol în investigarea infracțiunilor de criminalitate informatică au raportat necesitatea de a colecta dovezi în mediul Cloud Computing. Datele furnizate de acest raport ne confirmă faptul că există incidente şi infracțiuni informatice în mediul Cloud Computing. Raportul menționează şi unele atacuri (de exemplu, de tipul „ransomware" sau de răscumpărare a datelor) care au existat împotriva furnizorilor de servicii Cloud. În ceea ce priveşte aplicarea legii penale de către organele statului, problema devine din ce în ce mai serioasă, mai ales că aduce provocări de ordin juridic, tehnic şi

---

crime/cybercrime/cy%20activity%20bul/cy%20activity%20bul%20AS%20threat_en.pdf, accesat la data de 11 noiembrie 2017.

[1] University of Washington Computer Science & Engineering, *Cyber-Criminal Activity and Analysis*, White Paper Fall 2005, p. 4-6, 20-22, https://courses.cs.washington.edu/courses/csep590/05au/whitepaper_turnin/team2-whitepaper.pdf, accesat la data de 11 noiembrie 2017.

[2] RSA, *2016: Current State of Cybercrime*, RSA Whitepaper, p. 2-4, https://www.rsa.com/content/dam/rsa/PDF/2016/05/2016-current-state-of-cybercrime.pdf, accesat la data de 11 noiembrie 2017.

[3] J. ACHKOSKI, M. DOJCHINOVSKI, *Cyber terrorism and cyber crime: Threats for cyber security*, Proceedings of First Annual International Scientific Conference, Makedonski Brod, Macedonia, 9 June 2012, p. 2-6, http://eprints.ugd.edu.mk/6502/2/__ugd.edu.mk_private_UserFiles_biljana.kosturanova_Desktop_Trudovi_Jugoslav%20Achkoski_Scientific%20Papers_elektronska%20verzija_Cyber%20Terrorism%20and%20Cyber%20Crime%20–%20Threats%20for%20Cyber%20Security_rev_JA.pdf, accesat la data de 11 noiembrie 2017.

[4] Varonis, *134 Cybersecurity Statistics and Trends for 2021*, https://www.varonis.com/blog/cybersecurity-statistics/.

[5] Interpol, *ASEAN Cyberthreat Assessment 2021*, *op. cit.*, p. 11, 16, 21.

[6] Europol, *Internet Organised Crime Threat Assessment (IOCTA) 2016*, *op. cit.*, p. 52-53.

operațional. Deşi în prezent aproximativ 50% dintre autoritățile care aplică legea cooperează pentru soluționarea problemei cu sectorul academic şi cel industrial, doar 41% dintre acestea au efectuat stagii de pregătire profesională specializată[1]. Unul dintre obiectivele importante pe care îl vom aborda în cadrul cercetării noastre este legat de prevenirea fenomenului infracțional în sectorul public prin investigarea şi tragerea la răspundere a celor ce săvârşesc infracțiuni în Cloud Computing sau infracțiuni ce au legătură cu mediul informatic. Suntem de părere că, datorită complexității mediului informatic, cei care investighează infracțiunile informatice cu implicații în Cloud Computing nu vor reuşi să facă mari progrese fără o pregătire profesională adecvată.

Migrația utilizatorilor determină în mod automat şi migrația criminalității informatice. Pe măsură ce marile companii şi organizații îşi mută datele în Cloud, aceste date devin ținte din ce în ce mai atractive pentru infractorii cibernetici[2]. În ultimii ani, cantitatea de date informatice stocate în mediul Cloud Computing a crescut în mod constant[3]. În prezent, majoritatea datelor se află oarecum în „posesia" unor companii care furnizează servicii Cloud precum Google Cloud Platform, Amazon Web Services, Microsoft Azure şi IBM[4]. Fiecare client poate reprezenta o verigă slabă pentru securitatea unui furnizor de servicii Cloud Computing. Prin intermediul unor astfel de slăbiciuni, un atacator ar putea să „se infiltreze" în sistem şi astfel ar reuşi să sustragă sau să compromită datele informatice a milioane de utilizatori. Mai mult, odată ce a fost obținut accesul într-un astfel de sistem, breşa de securitate creată poate constitui o sursă pentru viitoare atacuri cibernetice coordonate către alte sisteme şi rețele[5]. Adesea atacurile cibernetice efectuate asupra furnizorilor de servicii Cloud Computing se materializează prin accesul ilegal la date şi servicii, fraude informatice, alterarea integrității datelor informatice (în special a datelor referitoare la informații financiare personale, informații privind sănătatea, secrete comerciale şi alte date cu caracter confidențial), perturbarea funcționării serviciilor etc.[6] Pe cât sunt de variate aceste categorii de atacuri, pe atât sunt de periculoase.

---

[1] Această secțiune a fost publicată de B. URS, *Migrația criminalității informatice...*, *op. cit.*, p. 149-150.

[2] A. APPAZOV, *op. cit.*, p. 26.

[3] CNBC Tech, *Microsoft's cloud business is growing almost twice as fast as Amazon's, with Google far behind*, https://www.cnbc.com/2017/04/27/microsoft-azure-growing-faster-than-aws-google-cloud-behind.html, accesat la data de 11 noiembrie 2017.

[4] ChannelE2E, *Cloud Market share 2017*, *op. cit.*

[5] W. JANSEN, T. GRANCE, *Guidelines on Security and Privacy in Public Cloud Computing*, NIST Special Publication 800-144, December 2011, p. 9, 12-13, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf, accesat la data de 11 noiembrie 2017.

[6] E. SCHULWOLF, *Cybersecurity 2017 – The Year in Preview: Emerging Security Threats*, November 30, 2016, https://casetext.com/posts/cybersecurity-2017-the-year-in-preview-emerging-security-threats, accesat la data de 11 noiembrie 2017.