

Bogdan Alexandru Urs

**Accesul ilegal
în mediul Cloud Computing**

Editura
Hamangiu
2023

CUPRINS

INTRODUCERE	1
TITLUL I. ACCESUL ÎN MEDIUL CLOUD COMPUTING ȘI INFRAȚIONALITATEA INFORMATICĂ	9
CAPITOLUL I. MEDIUL ȘI TEHNOLOGIA CLOUD COMPUTING	9
<i>Secțiunea 1. Definiția mediului informatic și a tehnologiei Cloud Computing</i>	9
<i>Secțiunea a 2-a. Caracteristicile tehnologiei Cloud Computing</i>	11
§1. Servicii proprii la cerere	12
§2. Acces extins la servicii prin rețea	13
§3. Alocarea dinamică a resurselor	14
§4. Servicii flexibile	15
§5. Servicii măsurabile	15
<i>Secțiunea a 3-a. Modele de livrare a serviciilor Cloud Computing</i>	16
§1. „Infrastructure as a Service”	17
§2. „Platform as a Service”	19
§3. „Software as a Service”	21
<i>Secțiunea a 4-a. Modele de implementare a serviciilor Cloud Computing</i>	22
§1. Cloud-ul public	24
§2. Cloud-ul privat	28
§3. Cloud-ul hibrid	32
§4. Cloud-ul de comunitate	37
CAPITOLUL AL II-LEA. ACCESUL LEGAL ÎN MEDIUL CLOUD COMPUTING	42
<i>Secțiunea 1. Controlul accesului în Cloud Computing</i>	42
<i>Secțiunea a 2-a. Mecanisme de autentificare</i>	44
§1. Mecanismele fizice de securitate	45
§2. Mecanismele digitale de securitate	45
<i>Secțiunea a 3-a. Mecanisme de autorizare</i>	46
§1. Mecanismul de control obligatoriu al accesului	47
§2. Mecanismul de control discreționar al accesului	47
§3. Mecanismul de control al accesului bazat pe roluri	48
§4. Mecanismul de control al accesului bazat pe atribute	49
§5. Mecanismul de control hibrid al accesului de tip „fine-grained”	49
<i>Secțiunea a 4-a. Sisteme de control al accesului în Cloud Computing</i>	50

CAPITOLUL AL III-LEA. ACCESUL ILEGAL ÎN MEDIUL CLOUD COMPUTING	54
<i>Secțiunea 1. Aspecte generale. Reglementare</i>	54
<i>Secțiunea a 2-a. Elemente de drept comparat</i>	55
§1. Statele Unite ale Americii	56
§2. Regatul Unit al Marii Britanii și al Irlandei de Nord	59
§3. Australia	61
§4. Germania	63
§5. Franța	64
§6. Tipologia accesului ilegal în dreptul comparat	65
<i>Secțiunea a 3-a. Obiectul infracțiunii</i>	66
<i>Secțiunea a 4-a. Subiecții infracțiunii</i>	68
<i>Secțiunea a 5-a. Latura obiectivă</i>	69
§1. Mediul Cloud Computing – „sistem informatic”	70
§2. Noțiunea de „acces” la un sistem informatic	72
§3. Accesul „fără drept” sau ilegal	74
§4. Particularitățile accesului ilegal în mediul Cloud Computing	77
§5. Tipologia atacurilor informatice prin care se materializează accesul ilegal	80
5.1. Atacurile de autentificare și cele de autorizare	82
5.2. Atacurile de împachetare	85
5.3. Atacul de tip „side channel”	87
5.4. Atacul de tip „Man in the Cloud”	91
5.5. Atacul de tip „Man in the Middle”	94
5.6. Atacurile din „interior”	96
§6. Aspecte practice	99
6.1. Accesul ilegal în mediul Cloud Computing	99
6.2. Accesul ilegal în diferite servicii bazate pe tehnologia Cloud	101
6.3. Accesul ilegal în servicii Cloud Computing de tip e-mail	103
6.4. Accesul ilegal în Cloud realizat de angajați sau foști angajați	105
6.5. Accesul ilegal în mediul Cloud Computing și diverse fraude informatice conexe	107
6.6. Accesul ilegal în Cloud asociat cu alte infracțiuni informatice	109
6.7. Accesul în diferite medii Cloud Computing cu implicații în pornografia infantilă	111
<i>Secțiunea a 6-a. Latura subiectivă</i>	112
<i>Secțiunea a 7-a. Formele infracțiunii</i>	113
<i>Secțiunea a 8-a. Modalități normative agravate</i>	115
§1. Prima modalitate agravată (obținerea de date informatice)	115

§2. A doua modalitate agravată (încălcarea măsurilor de securitate)	117
<i>Secțiunea a 9-a. Aspecte jurisdicționale</i>	119
<i>Secțiunea a 10-a. Relația dintre accesul ilegal și alte infracțiuni informatice</i>	131
§1. Relația cu fraudă informatică (art. 249 C. pen.)	132
§2. Relația cu falsul informatic (art. 325 C. pen.)	133
§3. Relația cu alterarea integrității datelor informatice (art. 362 C. pen.)	134
§4. Relația cu perturbarea funcționării sistemelor informatice (art. 363 C. pen.)	135
§5. Relația cu operațiuni ilegale cu dispozitive sau programe informatice (art. 365 C. pen.)	135

CAPITOLUL AL IV-LEA. ACCESUL ILEGAL ȘI FENOMENUL INFRAȚIONAL DIN MEDIUL CLOUD COMPUTING	137
<i>Secțiunea 1. Mediul Cloud Computing în paradigma infraționalității informatice</i>	137
<i>Secțiunea a 2-a. Migrația infraționalității informatice spre mediul Cloud Computing</i>	144
<i>Secțiunea a 3-a. Factorii ce influențează fenomenul migrației infraționalității informatice</i>	155
§1. Cantitatea vastă de date procesate și stocate în Cloud Computing	156
§2. Puterea de procesare a informației și infrastructura dinamică a mediului	158
§3. Disponibilitatea extinsă a serviciilor și a tehnologiei Cloud Computing	159
§4. Posibilitatea de a șterge rapid eventualele dovezi ale activității infraționale	160
§5. Facilitatea de a lansa rapid atacuri informatice la scară largă	162
§6. Existența unor instrumente propice săvârșirii de infracțiuni informatice	163
§7. Diversitatea infracțiunilor informatice comise în mediul Cloud Computing	165
<i>Secțiunea a 4-a. Formele criminalității informatice din mediul Cloud Computing</i>	167
§1. Cloud Computing-ul în calitate de țintă a infracțiunilor informatice	170
§2. Cloud Computing – un instrument pentru săvârșirea de infracțiuni informatice	173

<i>Secțiunea a 5-a. Implicațiile fenomenului infracțional din mediul Cloud Computing</i>	176
§1. Fraude informatice complexe	177
§2. Fraude informatice clasice	180
§3. Accesul ilegal și perturbarea funcționării sistemelor Cloud Computing	182
§4. Pornografia infantilă prin intermediul sistemelor Cloud Computing	184
§5. Cloud Computing-ul și pornografia infantilă în România	186
TITLUL AL II-LEA. PREVENIREA ACCESULUI ILEGAL ÎN MEDIUL CLOUD COMPUTING	189
CAPITOLUL I. ORGANIZAREA ȘI FUNCȚIILE MECANISMELOR DE PREVENIRE	189
<i>Secțiunea 1. Cadrul general de prevenire a infracționalității informatice</i>	189
<i>Secțiunea a 2-a. Principiile și formele de organizare a mecanismelor de prevenire</i>	193
<i>Secțiunea a 3-a. Mecanisme legale, tehnice și manageriale de prevenire a infracționalității informatice</i>	197
<i>Secțiunea a 4-a. Prevenirea prin prisma utilizatorilor, a sectorului privat și a celui de stat</i>	201
<i>Secțiunea a 5-a. Implementarea strategiilor de prevenire a infracționalității cibernetice</i>	205
CAPITOLUL AL II-LEA. MECANISME LEGALE DE PREVENIRE A ACCESULUI ILEGAL ÎN MEDIUL CLOUD COMPUTING	209
<i>Secțiunea 1. Politici privind utilizarea legală și responsabilă a serviciilor Cloud Computing</i>	209
<i>Secțiunea a 2-a. Implicațiile măsurilor legale în securitatea mediului Cloud Computing</i>	215
<i>Secțiunea a 3-a. Directiva (UE) 2016/1148</i>	216
<i>Secțiunea a 4-a. Regulamentul (UE) 2016/679</i>	222
<i>Secțiunea a 5-a. Directiva (UE) 2016/680</i>	229
<i>Secțiunea a 6-a. Directiva 2013/40/UE</i>	232
<i>Secțiunea a 7-a. Directiva 2002/58/CE</i>	237
<i>Secțiunea a 8-a. Comunicarea (2019) 250</i>	244
<i>Secțiunea a 9-a. Regulamentul (UE) nr. 910/2014</i>	252

CAPITOLUL AL III-LEA. MECANISME TEHNICE DE SECURITATE CU ROL ÎN PREVENIREA ACCESULUI ILEGAL ÎN MEDIUL CLOUD COMPUTING	265
<i>Secțiunea 1. Securitatea ca metodă de prevenire a accesului ilegal</i>	265
<i>Secțiunea a 2-a. Importanța implementării tehnicilor de securitate cibernetică</i>	270
<i>Secțiunea a 3-a. Mijloace și proceduri tehnice de protecție a datelor</i>	272
<i>Secțiunea a 4-a. Criptarea ca mijloc tehnic de securitate și prevenire a accesului ilegal în mediul Cloud Computing</i>	278
§1. Criptarea prin intermediul funcției „hash”	283
§2. Criptarea tradițională (criptarea „simetrică”)	284
§3. Criptarea cu două chei (criptarea „asimetrică”)	286
§4. Criptarea homomorfică („homomorphic encryption”)	289
CAPITOLUL AL IV-LEA. ASPECTE PRIVIND MANAGEMENTUL PREVENIRII ACCESULUI ILEGAL ÎN MEDIUL CLOUD COMPUTING	291
<i>Secțiunea 1. Principiile de organizare a serviciilor Cloud Computing</i>	291
<i>Secțiunea a 2-a. Managementul securității serviciilor și procedurile de organizare a acestora</i>	296
<i>Secțiunea a 3-a. Instrumente de management și audit al securității serviciilor</i>	303
<i>Secțiunea a 4-a. Organizații internaționale cu rol în managementul securității mediului Cloud Computing</i>	309
§1. Cloud Security Alliance (CSA)	310
§2. Institutul Național de Standarde și Tehnologie din Statele Unite ale Americii (NIST)	311
§3. Agenția Uniunii Europene pentru Securitatea Rețelelor și a Informațiilor (ENISA)	312
§4. Centrul de Cercetare în Cloud Computing al companiei Microsoft (MCCRC)	314
<i>Secțiunea a 5-a. Standarde internaționale care asigură un management al securității în mediul Cloud Computing</i>	315
CAPITOLUL AL V-LEA. PREVENIREA ACCESULUI ILEGAL ÎN MEDIUL CLOUD COMPUTING ȘI ROLUL SECTORULUI PUBLIC	322
<i>Secțiunea 1. Strategii naționale de prevenire a infracțiunilor informatică</i>	322
<i>Secțiunea a 2-a. Prevenirea accesului ilegal și protecția datelor în România</i>	323

<i>Secțiunea a 3-a. Cooperarea internațională și lupta împotriva infracționalității informatice</i>	327
<i>Secțiunea a 4-a. Importanța investigațiilor digitale în prevenirea și combaterea accesului ilegal în mediul Cloud Computing</i>	330
<i>Secțiunea a 5-a. Descentralizarea datelor și problema accesului ilegal în Cloud Computing</i>	336
<i>Secțiunea a 6-a. Investigatorii și accesul acestora la datele stocate în Cloud</i>	344
<i>Secțiunea a 7-a. Obținerea datelor referitoare la utilizatori</i>	345
<i>Secțiunea a 8-a. Analiza traficului de date din Cloud Computing</i>	349
<i>Secțiunea a 9-a. Probleme referitoare la datele de conținut și stocarea acestora</i>	351

CAPITOLUL AL VI-LEA. PREVENIREA ACCESULUI ILEGAL ÎN MEDIUL CLOUD COMPUTING ȘI ROLUL SECTORULUI PRIVAT

PRIVAT	355
<i>Secțiunea 1. Prevenirea accesului ilegal prin procedurile de securitate</i>	355
<i>Secțiunea a 2-a. Riscul și prevenirea accesului ilegal în sectorul privat</i>	359
<i>Secțiunea a 3-a. Rolul și funcțiile furnizorilor de servicii în prevenirea accesului ilegal în mediul Cloud Computing</i>	363
<i>Secțiunea a 4-a. Studii de caz privind implementarea mecanismelor de prevenire a accesului ilegal în sectorul privat</i>	368
§1. Google Cloud Platform	369
1.1. Implementarea de către Google Cloud a mecanismelor de prevenire	370
1.2. Securitatea și protecția datelor în Google Cloud	374
§2. Amazon Web Services	377
2.1. Mecanismele de prevenire și securitate ale Amazon Web Services	378
2.2. Protecția și securitatea datelor în Amazon Web Services	381
§3. Microsoft Azure	384
3.1. Prevenirea accesului ilegal în Microsoft Azure	384
3.2. Protecția datelor în Microsoft Cloud Azure	387
§4. IBM Cloud Computing	389
4.1. Securitatea serviciilor IBM Cloud	390
4.2. Protecția datelor cu caracter personal în IBM Cloud	392
§5. Sistec IT Solutions	393
<i>Secțiunea a 5-a. Analiza principalelor mecanisme de prevenire din sectorul privat</i>	395

<i>Secțiunea a 6-a. Implementarea de către furnizorii de servicii a noilor tehnologii de prevenire a accesului ilegal</i>	397
§1. Sistemele de detectare a intruziunilor de tip IDS	397
1.1. Sistemele de detectare a intruziunilor bazate pe gazdă	399
1.2. Sistemele de detectare a intruziunilor bazate pe rețea	401
1.3. Sistemele de detectare a intruziunilor bazate pe „hypervisor”	401
1.4. Sistemele distribuite de detectare a intruziunilor	402
§2. Sistemele de detectare și prevenire a intruziunilor de tip IDPS	403
§3. Utilizarea unui Cloud Privat Virtual	405
§4. Virtualizarea și izolarea mașinărilor virtuale	406
CONCLUZII	409
BIBLIOGRAFIE SELECTIVĂ	423