ANALELE ȘTIINȚIFICE ALE UNIVERSITAȚII „AL. I. CUZA" IAȘI
TOMUL LXIII, ȘTIINȚE JURIDICE, 2017, NR. II

INTERPRETAREA PRINCIPIILOR *PRIVACY BY DESIGN* ÎN ERA CLOUD COMPUTING

INTERPRETING THE *PRIVACY BY DESIGN* PRINCIPLES IN THE CLOUD COMPUTING ERA

LENUȚA ALBOAIE[1]

Rezumat: Odată cu existența unor tehnologii accesibile pe scară largă, numărul de utilizatori de servicii Internet a crescut și, ca efect, și cantitatea de date generată și stocată (inclusiv cele cu caracter personal) a crescut. În acest context, probleme ca securitatea și confidențialitatea datelor sunt de un real interes, iar soluțiile perfecte par un deziderat greu de atins. În lucrarea de față, în prima parte, creăm imaginea de ansamblu a evoluției tehnologice care a condus la tehnologii arondate Cloud Computing. În acest ecosistem, realizăm în partea a doua a lucrării o interpretare tehnică a principiilor *Privacy by Design* și deschidem o cale către o soluție software de respectare a acestora.
Cuvinte cheie: Cloud Computing, Privacy by Design, GDPR

Abstract: With the availability of widely available technologies, the number of Internet service users has increased and as a result the amount of data generated and stored (including personal data) has increased. In this context, issues such as data security and confidentiality are of real interest, and perfect solutions seem a difficult task to achieve. In the present paper, in the first part, we create the overall picture of the technological evolution that has led to Cloud Computing technologies. In this ecosystem, in the second part of the paper, we realize technical interpretation of the principles of *Privacy by Design* and open a path to a software solution to their compliance.
Keywords: Cloud Computing, Privacy by Design, GDPR

1. Cloud Computing

Cloud Computing este, conform Gardner, unul din principalele trend-uri în lumea IT alături de IoT (*Internet of Things*), *Business Analytics*,

[1] Conferențiar dr., Universitatea „Alexandru Ioan Cuza" din Iași, Facultatea de Informatică.

Inteligență Artificială sau *Machine Learning*. Secțiunea de față crează o imagine de ansamblu asupra pașilor care au fost necesari pentru atingerea nivelului tehnologic oferit de Cloud Computing în zilele noastre.

1.1 Pași înspre Cloud Computing

Cloud Computing reprezintă un conglomerat de tehnologii, iar forma actuală nu ar fi fost posibilă fără momente de referință din evoluția sistemelor distribuite[2].

Perioada anilor 1945 o putem considera esențială în evoluția calculatoarelor (cu transformări la nivelul memoriei, stocării, procesorului) și a rețelelor de calculatoare (apariția suitei de protocoale TCP/IP, a Internetului). Încă din această perioadă existau previziuni asupra modului cum va fi folosită puterea de calcul: *"(...) computing may someday be organised as a public utility just as the telephone system is a public utility..."*[3].

Realitatea de astăzi demonstrează că puterea de calcul a devenit cea de cincea utilitate, furnizata într-un mod similar utilităților tradiționale (gaz, electricitate, apă sau telefonie).

Din punct de vedere tehnologic, un moment important a fost reprezentat de apariția în anii '90 a conceptului de Grid Computing, denumit în acest fel prin analogie cu rețelele electrice (power grids)[4].

Studiile și experimentele din acea perioadă au observat că aproximativ 90% din puterea unui procesor nu era utilizată. Acest lucru se întâmpla în contextul în care numeroase probleme de calcul, de optimizare sau de simulare necesitau super-computere cu capabilități computaționale crescute.

Grid era o infrastructură de calcul distribuit destinată inițial proiectelor științifice și mai apoi și celor industriale. A permis executarea de task-uri pe mai multe mașini, privite ca un calculator unic. Grid Computing asigură de asemenea partajarea flexibilă, sigură și coordonată a resurselor

---

[2] L. Alboaie, *Cloud Computing – Nucleul Vieții Digitale a utilizatorilor*, în Revista Columna, Nr. 6/2017, Supliment cultural-științific al revistei STUDII ȘI COMUNICĂRI/DIS a Diviziei de Istoria Științei a CRIFST al Academiei Române, Comitetul Român de Istorie și Filosofia Științei și Tehnicii, Academia Română, ISSN: 1841-9852, 2017.

[3] S. Garfinkel, *The Cloud Imperative*, Business Report, 2011.

[4] C. Kesselman, I. Foster, S. Tuecke, *The Anatomy of the Grid: Enabling Scalable Virtual Organization*, în International Journal of High Performance Computing Applications, 2001, 15(3), pp. 200-222.

între colecții dinamice de indivizi, instituții și resurse. Dacă în faza inițială în Grid erau partajabile doar resursele hardware, integrarea cu tehnologiile arondate Web-ului au permis și partajarea aplicațiilor. Și astfel, din punct de vedere al specialiștilor, utilizarea aplicațiilor și serviciilor Grid a devenit o soluție completă[5].

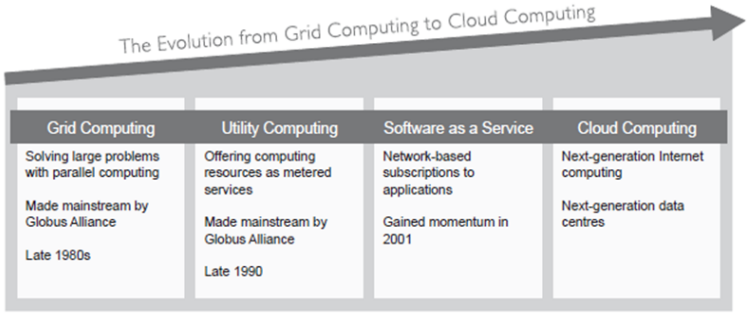
Din punctul de vedere al utilizatorilor finali, acest lucru nu a avut loc, motiv pentru care Grid Computing nu s-a bucurat de mediatizarea tehnologiilor asociate cu Cloud Computing.

În paralel cu dezvoltarea la nivel de Grid, prin furnizarea de putere computațională la cerere în stilul plătești ceea ce utilizezi (*pay-per-use*), a apărut paradigma SaaS (Software-as-a-Service).

SaaS desemnează software care este deținut, furnizat și gestionat de un furnizor. Comparând cu un sistem software tradițional, în acest caz utilizatorul plătește funcționalitatea pentru timpul de utilizare, dar utilizatorul nu deține softul și nu face investiții în infrastructura, în licențe etc[6].

Serviciile în acest caz sunt consumate pe principiul *pay-per-use* via unui Web browser sau API (*Application Programming Interface*). Ceea ce remarcam la acest nivel este faptul că orice utilizator este capabil să folosească servicii dacă folosește un simplu client browser.

Și am ajuns astfel, printr-o concurență a tehnologiei și a contextului mondial economic, la momentul în care Cloud Computing a prins formă[7].



The Evolution to Cloud Computing (adapted from IBM 2009)

Figura 1. Pași tehnologici spre Cloud Computing

[5] L. Alboaie, *op.cit.*
[6] *Ibidem.*
[7] M. Cafaro, G. Aloisio, *Grids, Clouds and Virtualization*, 2011.

Avem în figura 1 o perspectivă completa a pașilor care au condus la apariția Cloud Computing.

Apariția soluțiilor oferite de Cloud au fost salvatoare în special pentru companii mici și mijlocii, în contextul crizei economice din anii 2008. În acel moment, greu din punct de vedere economic, companiile mici/mijlocii au putut să se concentreze pe cheltuieli operaționale și mai puțin pe cele de capital, astfel s-a preferat achiziționarea de servicii/abonamente, decât plata unor sume mari într-o investiție[8].

1.2 Cloud Computing: servicii, avantaje și provocări

Denumirea de Cloud Computing a fost inspirată din diagramele care erau folosite pentru reprezentarea Internetului. Într-o definiție simplificată, putem vedea Cloud ca un sistem distribuit, care furnizează în Internet, într-un mod eficient, accesul la o mare varietate de servicii atât pentru specialiști, dar și pentru utilizatorii obișnuiți.

Acest lucru poate fi asigurat prin existenta mai multor categorii de servicii și amintim pe cele mai uzuale:

IaaS (Infrastructure as a Service)[9]

Aceste servicii permit închirierea de infrastructură (noduri de calcul, sisteme de stocare etc.) și construirea unui sistem IT. În acest caz, mediul poate fi controlat în totalitate de cel care l-a configurat/creat. Remarcăm însă faptul că sistemul este închiriat, deci resursele fizice efective sunt în grija (depozitare, răcire, securitate fizică) unui furnizor de servicii IaaS.

PaaS (Platform as a Service)[10]

Aceste servicii permit dezvoltarea unui sistem IT pe o platformă Cloud existentă, fără grija managementului resurselor la nivel scăzut. În acest caz, mediul nu mai poate fi controlat în totalitate, ci doar anumite aspecte pot fi personalizate.

SaaS (Software as a Service)

În acest caz se folosesc sisteme IT existente, oferite de un furnizor de servicii Cloud. Aceste servicii nu necesită cunoașterea de detalii tehnice.

---

[8] K. Stanoevska-Slabeva, T. Wozniak, S. Ristol, *Grid and Cloud Computing - A Business Perspective on Technology and Applications*, Editura Springer-Verlag Berlin Heidelberg, DOI 10.1007/978-3-642-05193-7, 2010.

[9] L. Alboaie, *op.cit.*

[10] L. Alboaie, *op.cit.*

Existența acestui nivel de servicii a asigurat de altfel o cunoaștere și utilizare a serviciilor Cloud până la nivelul utilizatorului obișnuit. Aceste servicii pot fi folosite în mod uniform (de pe orice platformă Windows, iOS, Android, Linux) și folosind dispozitive diverse.

Avem în figura 2 un top al celor mai buni furnizori de servicii Cloud în 2017[11]:

Figura 2. Top furnizori de servicii cloud în 2017

Dacă dorim să avem o imagine asupra numărului de utilizatori de servicii Cloud, putem în Internetlivestats[12] să vizualizăm în timp real statistici privind utilizarea diverselor sisteme și să avem în vedere că majoritatea aplicațiilor ca YouTube, Instagram, Facebook et.al. se bazează pe tehnologii arondate Cloud Computing.

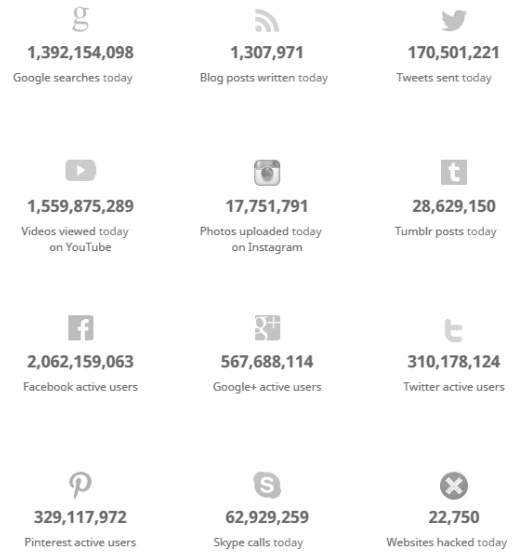


Figura 3. Utilizatori/clienți de servicii/aplicații Cloud

[11] Toptenreviews, [Online] la: www.toptenreviews.com/services/web-hosting/best-cloud-services/.

[12] Internetlivestats, 2017, [Online] la: http://www.internetlivestats.com/.

Dacă ne oprim asupra Facebook, mulți dintre utilizatori nu realizează că folosesc serviciile unor furnizori de Cloud și ignoră aspecte care țin de securitatea și confidențialitatea datelor lor. Trebuie să înțelegem că tehnologiile ne pot fi un bun aliat, dar și dușman dacă nu sunt folosite în mod corespunzător. Viața pe Internet, o concurează "cu succes" pe cea reală, și dacă în viata de zi cu zi ne pasă de siguranța noastră, acest lucru trebuie să se oglindească și în mediul online.

Într-adevăr, securitatea în Cloud ridică mari dificultăți, în contextul în care vorbim atât de asigurarea securității calculatoarelor, dar și a rețelelor de calculatoare. Este nevoie de un set larg de politici, tehnologii și controale care sa fie desfășurate pentru a proteja datele, aplicațiile și infrastructura din Cloud.

Un studiu realizat de CIGI (Centre for International Governance Innovation) asupra 24,225 utilizatori de Internet din 24 de tari, în perioada Decembrie 23, 2016 - Martie 21, 2017 în ţări ca Australia, Brazilia, Canada, China, Egipt, Franţa, Germania, Hong Kong (China), India, Indonesia, Italia, Japonia, Kenya, Mexic, Nigeria, Pakistan, Polonia, Republica Korea, Africa de Sud, Suedia, Tunisia, Turcia, Regatul Unit al Marii Britanii şi Irlandei de Nord şi Statele Unite ale Americii, arată că pas cu pas utilizatorii de servicii Cloud și servicii Internet în general, devin conștienți de problema securității[13]:

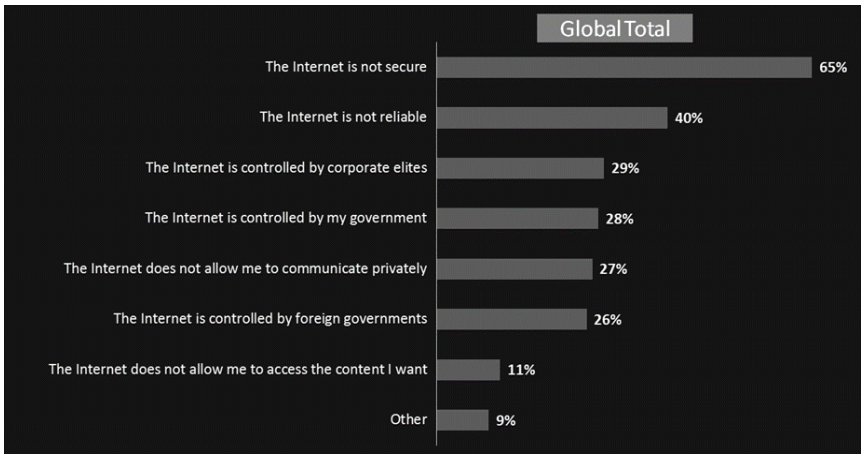


Figura 4. Temeri ale utilizatorilor legate de securitatea și confidențialitatea serviciilor

[13] CIGI – Centre for International Governance Innovation, https://www.cigionline.org/.

Înțelegând sau intuind aceste probleme existente, reacții diverse (utilizarea selectivă a unor aplicații, teama de a spune ce gândești, limitarea aplicațiilor utilizate, utilizarea Internetului mai puțin etc.) par a fi în opoziție cu scopul Internetului și Web-ului, cel de a avea un sistem deschis care să ofere un ecosistem în care cunoștințele și experiențele oamenilor să fie partajate, toate acestea contribuind la colaborarea care duce implicit la evoluția noastră globală.

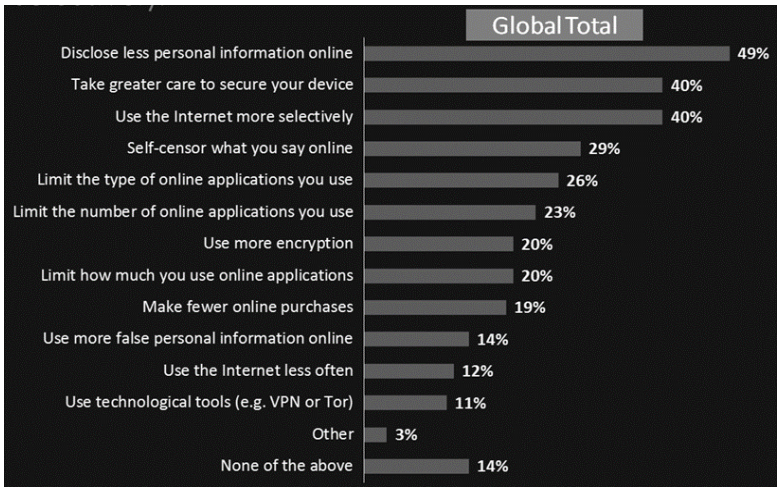


Figura 5. Potențiale reacții ale utilizatorilor la amenințările legate de securitate și confidențialitate

Evitarea apariției unui curent global, cu un comportament anti-Internet, ne conduce la încercarea de a găsi soluții pentru asigurarea securității și confidențialității datelor. Acest al doilea aspect este subiectul dezbătut în continuare în cadrul acestei lucrări.

2. Interpretarea principiilor Privacy by Design

Vom începe această secțiune prin a face distincția între conceptul de confidențialitate (eng. *privacy*) și securitate a unui sistem.

Privacy poate fi privit ca un nivel imediat peste nivelul de securitate. Într-un sistem putem avea securitate fără a avea *privacy*, dar nu putem avea *privacy* fără securitate. *Privacy* oferă o modalitate de acces granular la informație. Pentru clarificarea conceptului, să considerăm că o persoană fizică deține un cont bancar, accesibil din orice filială a băncii. Implicit, angajații băncii au acces la acest cont și se presupune că nimeni

altcineva. Până la acest nivel putem vorbi de asigurarea securității. Confidențialitatea intervine la nivelul în care accesul la datele asociate contului se face doar dacă există un *business case* sau o solicitare în acest sens și nu dacă un angajat al băncii "devine curios" în ceea ce privește informațiile particulare asociate contului.

Gândirea modernă asupra confidențialității gravitează în jurul principiilor *Privacy By Design* și a interpretării lor legale dată de GDPR (*EU General; Data Protection Regulation*).

Principiile *Privacy by Design* (PbD)[14] pot fi considerate ca stând la baza analizelor legate de probleme de confidenţialitate. Aceste principii sunt văzute ca fiind relativ vagi, fără a veni cu indicaţii concrete asupra modului lor de implementare, ceea ce conduce la multe interpretări, care fac aceste principii ca fiind greu de implementat din punct de vedere tehnic[15].

În această lucrare, ne vom referi prin termenul tehnic PbD ca să înțelegem o unificare a conceptelor consacrate de *Privacy by Design* şi *Privacy by Default*.

Privacy by Design (tradus uneori prin protecția datelor încă din faza de proiectare) presupune că anumite reguli trebuiesc încorporate în metodologiile de dezvoltare de software atunci când este vorba de prelucrarea datelor cu caracter personal. *Privacy by Default* (tradus uneori prin protecția datelor cu ajutorul setărilor implicite) înseamnă că, atunci când folosește un produs, consumatorul trebuie să îl găsească setat pe parametrii care oferă cea mai mare protecție.

În continuare vom realiza o interpretare a celor șapte principii PbD, așa cum se regăsesc ele în literatura științifică. Pentru o tratare mai elaborata, recomandăm *Privacy Policies Are Not Enough: We Need Software Transparency*[16], *Privacy Engineering: Proactively Embedding Privacy, by Design*[17], *Privacy by design: delivering the promises, Identity in the Information Society*[18].

---

[14] Privacy by Design, *The 7 Foundational Principles,* [Online] la: www.iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf , 2011.

[15] R. McKean, *EU Data Protection Reform – privacy-by-design,* [Online] la: http://www.olswang.com, 2014.

[16] A. Cavoukian, D. Jutla, *Privacy Policies Are Not Enough: We Need Software Transparency*, 2014.

[17] A. Cavoukian, S. Shapiro, R. J. Cronk, *Privacy Engineering: Proactively Embedding Privacy, by Design*, 2014.

[18] P. Hustinx, *Privacy by design: delivering the promises, Identity in the Information Society*, Volume 3, Issue 2, 2010, pp 253–255.

a) Proactive not reactive; Preventative not remedial

Primul principiu PbD stipulează faptul că protecția datelor private trebuie făcută în mod preventiv și nu reactiv. În mod evident, remedierea furtului datelor sau detecția faptului ca datele au fost copiate nu pot să mai împiedice răul care poate fi făcut prin folosirea ilegală a acestor date.

Acest principiu se refera atât la mijloace tehnice de prevenție, dar și la mijloace de natura organizațională (politici, standarde, cultura organizațională care să acorde importanţă problemelor de securitate și *privacy*).

b) Privacy as the default setting

Sistemele moderne tind să aibă un mare nivel de configurabilitate de către utilizatori și administratori. Principiul doi spune că toate configurațiile implicite pentru un utilizator nou ar trebui să activeze doar comportamentele sistemului care protejează datele personale și nu pe cele care permit scurgeri ale datelor personale. Să considerăm că avem o rețea socială şi setările asociate. Chiar dacă în sistem există o setare care face disponibil sau indisponibil către alții numărul de telefon sau email-ul, conform acestui principiu, setarea implicită ar trebui să fie cea în care datele private nu sunt disponibile. Din motive ce țin de exploatarea comercială, multe servicii internet actuale nu respectă acest principiu. O cauză a acestui comportament potențial dăunător social îl reprezintă beneficiile ce se pot obține din învățarea comportamentelor și colectarea datelor private de la utilizatori.

Acest principiu, aplicat în practică, se poate traduce prin implementarea unor mecanisme care asigură verificarea următoarelor aspecte: specificarea scopului de colectare a datelor, limitarea colectării de date doar la scopul specificat, minimizarea datelor (*Data Minimization*) colectate sau partajate, limitarea în timp a stocării datelor, limitarea folosirii datelor private doar pentru scopurile specificate.

c) Privacy embedded into design

Acest principiu PbD stipulează faptul că protecția datelor private trebuie să fie analizată și adăugata în design de la început, în mod preventiv și nu reactiv. În mod ideal, mecanisme ce asigură protecția datelor private ca și a mecanismelor de securitate ar trebui să fie verificabile formal încă din faza de proiectare a sistemelor. Totuși, din motive de complexitate și lipsa metodelor, această practică nu este larg întâlnită în acest moment. Efortul nostru de cercetare în domeniul coreografiilor verificabile este o contribuție

în acest sens[19,20,21].

d) Full functionality – positive-sum, not zero-sum

Acest principiu PbD își propune să nu prioritizeze interesele private în faţa intereselor de grup și sociale. Ca cetățeni ne dorim beneficiile comunicării între diferite organizații și actori sociali. Progresul și abundenţa materială se bazează pe exploatarea încrederii și a informațiilor cu caracter personal. Pentru a promova exploatarea comercială și pentru a facilita schimbul de bunuri și servicii în mod sănătos social, avem nevoie de sisteme robuste care să permită accesul la date conform legilor. Acest principiu este unul din cele mai puțin înțelese în comunitatea academică și uneori și în industrie datorită încercării de a rezolva probleme sociale cu mijloace tehnice. Acest principiu necesită o înțelegere mai amplă și o acceptare din arhitectura sistemelor a forțelor inevitabil contradictorii ce definesc conceptul de *privacy*. În esență, acest principiu respinge ideea ca protecția datelor reduce posibilitățile de exploatare comercială a datelor.

e) Visibility and transparency – keep it open

Ca urmare a principiului anterior, devine evident că nu se pot crea cutii magice care respectă la modul absolut drepturile și legile în vigoare. Datorită implicării umane, sistemele software vor fi mereu vulnerabile în faţa utilizatorilor lor. Totuși, existența unor mecanisme de audit sau logare detaliată a operațiilor și a accesului la datele sensibile pot diminua în mod semnificativ riscurile asociate. Acest principiu propune ca prin design să fie maximizată vizibilitatea și transparența asupra funcționarii și asupra modului cum este exploatat sistemul de către utilizatori. Orice implementare incorectă a acestui principiu poate transforma transparența într-o sursa de probleme legate de securitate și de protecție a datelor. Pe scurt, acest principiu se poate traduce prin verificarea următoarelor aspecte:

Atribuirea responsabilității - orice acces la date private ar trebui să fie logat și un audit ulterior ar trebui să poată verifica legalitatea accesului;

---

[19] L. Alboaie, S. Alboaie, A. Panu, *Swarm Communication – A Messaging Pattern Proposal for Dynamic Scalability in Cloud*, 15th IEEE International Conference on High Performance Computing and Communications (HPCC 2013), IEEE, pp. 1930-1937.

[20] S. Alboaie, L. Alboaie, A. Panu, *Levels of Privacy for e-Health systems in the cloud era*, 24th International Conference on Information Systems Development Harbin, China, August 25-27, 2015.

[21] S. Alboaie, L. Alboaie, M.-F. Vaida, *Web service transformations in a federated Enterprise Service Bus based on executable choreographies*, Proceedings of the Conference on Mathematical Foundations of Informatics MFOI 2016, Chișinău, Republic of Moldova, 2016.

Transparența - politicile și practicile legate de managementul datelor private trebuiesc făcute cunoscute celor cu un interes legitim în acest sens;

Conformitate - organizațiile care manipulează date private trebuie să respecte reguli, standarde și proceduri bine definite cu privire la modul în care folosesc aceste date.

f) End-to-end security – full lifecycle protection

Acest principiu scoate în mod explicit la lumina faptul că toate aspectele ce țin de exploatarea unui sistem pot contribui la respectarea sau încălcarea regulilor și politicilor referitoare la datele private. Protecția datelor trebuie să fie o preocupare continuă începând cu analiza, implementarea, mentenanța și modul cum sunt proiectate și respectate procedurile de exploatare a sistemelor software.

Acest principiu, intuitiv indică faptul că aspectele de securitate și modul de aplicare a standardelor și bunelor practici de securitate, constituie o necesitate în vederea obținerii unor sisteme ce respecta protecția datelor.

g) Respect for user privacy – keep it user-centric

În ciuda conflictului dintre interesele private și interesele de grup, acest principiu stipulează că atunci când exista dubiu ar trebui să fie prioritare interesele private ale utilizatorului. Acest principiu se poate traduce prin verificarea următoarelor aspecte:

Obținerea consimțământului: deținerea și folosirea datelor personale trebuie să se facă doar după obținerea acceptului;

Acuratețea: datele private trebuie sa fie corecte, complete, actualizate pentru a nu provoca daune persoanelor;

Accesul: persoanele trebuie sa aibă acces la propriile date și să poată să ceară ștergerea lor.

Dincolo de aspectele organizaționale adresate de PbD, o sumarizarea și operaționalizare a acestor principii ce s-ar adresa implementatorilor (arhitecți software și programatori) și nu specialiștilor în drept ar putea fi sumarizată prin următoarele puncte: *obținerea consimțământului, păstrarea calității datelor, obținerea doar a datelor de care este nevoie, dreptul de a fi uitat, transparență și acces, monitorizare, auditare și reacție imediate la breșe.*

Dat fiind caracterul interpretabil al acestor principii, dacă aspectele ce țin de *privacy* sunt lăsate doar în seama specialiștilor tehnici și a decidenților de business orientați spre eficiență și profit, interpretarea

principiilor poate fi mult mai relaxată decât ar fi optimul social.

În acest context, efortul echipei de cercetare din cadrul laboratorului ADS - Applied Distributed Systems (Facultatea de Informatica, Universitatea Alexandru Ioan Cuza din Iași), prin intermediul proiectului PrivateSKY[22] în domeniul coreografiilor verificabile este o contribuție în acest sens.

Fără a intra în detalii tehnice, menționăm că în cadrul *Towards a smart society through personal assistants employing executable choreographies*[23], pe baza cercetărilor efectuate[24,25,26] s-a prezentat o soluție prin care principiile PbD pot beneficia de suportul tehnic pentru implementarea de sisteme în acord cu cerințele legislației în vigoare.

3. Concluzii

Curentul actual este fără îndoială așa numitul *data-centric computing*, în care datele sunt nucleul societății informaționale[27] și ne referim aici la toate datele existente, atât cele cu caracter public, cât și cele cu caracter personal. Asa cum am văzut, tehnologiile Cloud sunt adânc încrustate în viața noastră și utilizatorii „plătesc" utilizarea Facebook, Google, ITunes, Instagram etc., deoarece toate acțiunile, legăturile și căutările lor sunt înregistrate și folosite în scopuri diverse. În acest context, este dificilă stabilirea unui echilibru între utilizarea acestor date care să ducă la un beneficiu global sau utilizarea acestora cu scopul de obținere a unor profituri punctuale. PbD si GDPR vin ca suport pentru crearea de sisteme informatice într-un viitor apropiat, capabile speram noi, să asigure un *safe data-centric computing*.

[22] PrivateSky, [Online] la https://profs.info.uaic.ro/~ads/PrivateSky.

[23] L. Alboaie, *Towards a smart society through personal assistants employing executable choreographies*, At 26th International Conference on Information Systems Development, Cyprus, 6-8 September 2017.

[24] L., Alboaie, S. Alboaie, A. Panu, *Swarm Communication (…).*

[25] S. Alboaie, L. Alboaie, A. Panu, *Levels of Privacy for e-Health systems (…).*

[26] S. Alboaie, L. Alboaie, M.-F. Vaida, *op.cit.*

[27] L. Alboaie, *Evoluția prelucrării și transmiterii datelor în societatea umană (in Romanian)*, în Revista Noema, Comitetul Român de Istorie și Filosofia Științei și Tehnicii, Volumul XI, Academia Română, ISSN: 1841-9852, 2012, pp.253-270.