CONFIDENȚIALITATE ȘI SECURITATE ÎN ERA DIGITALĂ: PROVOCĂRI CONTEMPORANE ȘI DIRECȚII VIITOARE

PRIVACY AND SECURITY IN THE DIGITAL AGE: CONTEMPORARY CHALLENGES AND FUTURE DIRECTIONS

CZU: 342.738:004.056.5 **https://doi.org/10.5281/zenodo.7889212**

Daniela GÎNCO-FODOR[1]

ABSTRACT. *The topicality of the researched theme resides in the idea of presenting the contemporary problems encountered in the process of protecting personal data in the digital age. Privacy and security are at the heart of civil rights from which all other human rights and freedoms derive, and the digital age is in full swing, so the challenges and future directions for the development of this subject need to be addressed.*

Keywords: *privacy, security, digital age.*

Introducere

În goana spre a ne depăși propria ființă, uităm că astfel, pierdem tot … securitate, confidențialitate, identitate, personalitate.

Astăzi, este practic imposibil să ne imaginăm viața în absența interacțiunii cu computerul. Fiecare domeniu uman de activitate necesită recurgerea la rețele informatice și de comunicare racordate global. Conexiunile de acest gen asigură un suport esențial în toate domeniile de activitate: social, economic, financiar, politic și, nu în ultimul rând, cel de securitate. Dar în tot acest amalgam de informații, există riscul de a deveni victima atacurilor cibernetice, atât pe rețelele sociale, cât și prin intermediul „capcanei pentru click-uri". Toate acestea creează un habitat optim pentru a rămâne expuși amenințărilor și furtului de informații personale. Însă, pentru a ne securiza datele și a rămâne imuni, trebuie să respectăm anumite reguli vitale, care sunt necesare în mediul informațional.

Confidențialitatea este un drept fundamental al omului, cu semnificație internațională și este recunoscută în diferite documente internaționale și regionale [1]. Confidențialitatea este capacitatea unui individ sau a unui grup de persoane de a proteja viața privată și mediul privat, inclusiv informațiile despre ei înșiși. S-ar putea pune mai multe întrebări, de exemplu: „Ce este viața privată? Care sunt granițele acestui domeniu?". Răspunsurile concrete la aceste întrebări ar putea fi formulate pe baza culturii naționale și a caracteristicilor specifice ale individului, dar există teme comune, care ar putea fi discutate pentru determina-

[1] Daniela GÎNCO-FODOR, Studentă, Facultatea de drept, Universitatea de Stat din Moldova, https://orcid.org/0000-0001-8362-908X , gfdannelly@mail.ru

rea hotarelor generale ale domeniului de „viețuire privată”. În general, domeniul confidențialității se suprapune parțial cu confidențialitatea informațiilor personale și protecția acestora (acces, utilizare, diseminare, transfer etc.). Din acest motiv, fiecare persoană are dreptul la protecția datelor sale personale [3, p.7].

Dreptul la intimitate formează fundamentul comun al libertății de conștiință, dreptul de a fi în siguranță, dreptul de a refuza auto incriminarea. Era digitală actuală extinde definiția confidențialității ca *intimitate în mediul digital (e-privacy*) [2, p.97] și sugerează că dreptul la confidențialitate ar trebui văzut ca un drept independent care merită în sine protecție legală [2, p.100]. În acest sens, se poate propune următoarea definiție de lucru pentru dreptul la viață privată: Dreptul la viață privată este dreptul nostru de a păstra un domeniu în jurul nostru, care include toate acele lucruri care fac parte din noi, cum ar fi corpul nostru, casa, proprietate, gânduri, sentimente, secrete și identitate. Dreptul la confidențialitate ne oferă posibilitatea de a alege ce părți din acest domeniu pot fi accesate de alții și de a controla măsura, modul și momentul utilizării acelor părți pe care alegem să le dezvăluim.

Importanța păstrării confidențialității și securității în era digitală

Creșterea rolului Tehnologiilor Informaționale (IT) în societate, utilizarea pe scară largă a computerelor și procesarea informațiilor în sfera publică în ultimele 3 decenii, impun dezvoltarea unei politici puternice pentru protecția datelor cu caracter personal, începând cu primele legi în diferite țări în cursul anilor 1970 (Țara Hesse în Germania, Suedia, SUA, Germania, Franța etc.). Următoarea etapă a fost adoptarea documentelor care formează cadrul legal european de bază. Acest proces a condus la adoptarea Regulamentului general privind protecția datelor (GDPR) în 2016, care a intrat în vigoare la 28 mai 2018.

Securitatea informației poate fi definită pe scurt ca starea de protecție a resurselor informaționale cu diferite tipuri de date care sunt stocate, procesate sau transmise prin utilizarea sistemelor și rețelelor informatice. Trebuie să protejeze datele de diferite acțiuni interne și/sau externe care ar putea cauza perturbări ale funcțiilor sistemului, inclusiv accesul neautentificat și neautorizat. Această protecție trebuie realizată prin utilizarea unor mijloace și instrumente speciale (software și hardware) pe baza unei politici de securitate puternice. Securitatea informațiilor este o parte importantă a securității în general, care este determinată ca totul despre protejarea activelor critice și valoroase, iar articolul marchează diferite părți, dar fără a se limita la securitatea computerelor, securitatea internetului, securitatea comunicațiilor, securitatea rețelei, securitatea cererilor, securitatea datelor și securitatea informațiilor [4, p.12].

O problemă pentru securitatea informațiilor este discutată în contextul utilizării inteligenței artificiale și, în special, al învățării profunde în viziunea computerizată. Articolul confirmă popularitatea rețelelor sociale online (OSN) pen-

tru partajarea diferitor tipuri de informații, dar observă că atacatorul exploatează conturi false pentru a distribui informații înșelătoare, cum ar fi malware, viruși sau URL-uri rău intenționate [5].

Confidențialitatea, ca drept fundamental al omului, este asociată cu necesitatea și obligația de a păstra secretă viața privată a persoanelor. Confidențialitatea informațiilor personale presupune protejarea datelor în timpul accesului, utilizării, difuzării și transferului din interior și din exterior. Aceste cerințe definesc două drepturi importante – dreptul la confidențialitate și dreptul la protecția datelor. Era digitală actuală extinde definiția confidențialității prin „confidențialitate în mediul digital" sau „e-privacy", care este prevăzută în Regulamentul general privind protecția datelor – GDPR [6].

Motivele apariției provocărilor contemporane în asigurarea confidențialității și securității datelor personale în era digitală

Există termeni specifici în domeniul securității resurselor informaționale:

- Securitatea informațiilor este protecția informațiilor sub toate formele posibile (electronic, tipărit sau de altă natură);
- Securitatea computerelor acoperă funcționarea sistemelor și rețelelor informatice și a informațiilor prelucrate de acestea;
- Protecția informațiilor include practici de management al riscurilor legate de utilizarea, prelucrarea, stocarea și transmiterea informațiilor, inclusiv a sistemelor și proceselor în acest scop, cu scopul principal de a preveni pierderea datelor în situații critice.

Câteva motive ale potențialelor amenințări sunt:

- creșterea puternică a volumului de informații procesate și stocate;
- utilizarea masivă a rețelelor de calculatoare și integrarea acestora;
- extinderea numărului de utilizatori care au acces la sistem și resursele informaționale;
- unirea diferitelor fonduri de informații într-o bază de date comună și permiterea accesului multiplu la aceasta;
- îndepărtarea semnificativă a infractorului de obiectul atacului;
- atacul poate viza atât un anumit computer, cât și o conexiune de rețea;
- capacitatea de a ataca infrastructura și protocoalele de rețea;
- atacuri la serviciile de telecomunicații.

Provocările erei digitale pentru confidențialitate și protecția datelor

Securitatea informațiilor și protecția datelor sunt domenii dinamice, care sunt în mod constant influențate de progresele tehnologiilor din era digitală și de inovația în practicile de afaceri.

Dezvoltarea TIC reflectă regulile de organizare a protecției datelor și schimbă înțelegerea pentru definirea datelor cu caracter personal, gestionarea transfe-

rului transfrontalier de date, confidențialitatea utilizatorilor în era digitală, drepturile utilizatorilor și obligațiile operatorilor de date.

Un sondaj în rândul utilizatorilor de internet arată că 74% dintre cetățenii UE cred că descoperirea datelor cu caracter personal este o parte din ce în ce mai integrantă a lumii digitale. Pe de altă parte, doar 26% dintre utilizatorii de computere sociale și 18% dintre cumpărătorii online cred că au acces deplin la datele lor personale.

Se pot pune multe întrebări despre cum și unde sunt stocate datele noastre personale, cine le poate evalua, cine este responsabil pentru protecția datelor, ce politică se aplică pentru stocarea datelor cu caracter personal și pentru păstrarea confidențialității acestora, care este garanția transferului corect al datelor între diferite noduri prin intermediul rețelei globale.

Pot fi date diverse exemple pe internet. Unul pertinent ar fi din „Opțiunile de confidențialitate" publicate pe un site, unde sunt indicate categoriile de date cu caracter personal colectate, cum ar fi „numele, sexul, ziua de naștere sau vârsta, pagina de pornire, fotografia de profil, fusul orar, adresa de e-mail, țara, interesele și comentariile și conținutul pe care l-ați postat/partajat" [7]. Multe dintre aceste categorii nu au legătură cu domeniul specific al site-ului. Aceste provocări necesită a fi discutate detaliat.

Provocări de calcul social (SoC)

În multe cazuri, site-urile web joacă rolul unei *uși deschise* – în timpul înregistrării preliminare sau la prima vizită cu doar un click utilizatorii pot accepta *Politica de confidențialitate,* fără a citi textul. Rezultatul este acceptarea deplină a tuturor condițiilor, fără ca utilizatorul să le cunoască cu adevărat. În acest caz, el nu știe exact ce se va întâmpla cu datele sale personale din profilul utilizatorului creat.

În alte cazuri, datele personale ale utilizatorului sunt stocate numai după o singură vizită și transferate automat în centru, fără știrea și acordul proprietarului.

În unele cazuri, este posibil ca un media să nu furnizeze informații despre *Politica de confidențialitate* sau să solicite prea multe informații personale atunci când utilizatorul se înregistrează, ceea ce depășește scopul definit al mass-media.

O altă problemă este locația datelor personale stocate undeva în rețeaua globală.

Problema de mai sus determină un alt aspect negativ la îndeplinirea *dreptului de a fi uitat/șters* în cazul refuzului utilizării ulterioare.

Cerințe pentru limitarea impactului negativ

Era digitală oferă diverse posibilități tehnologice de rezolvare a problemelor din viața de zi cu zi a oamenilor, dar, așa cum sa prezentat în secțiunea anterioară,

creează și dezavantaje și consecințe negative pentru persoanele care sunt utilizatori de servicii electronice. Anumite cerințe și oportunități pot fi propuse pentru limitarea impactului negativ al tehnologiilor digitale în condițiile confidențialității și protecției datelor utilizatorilor:

- Cerința de a da consimțământul explicit și deplin pentru colectarea și utilizarea datelor cu caracter personal;
- Accesul ușor al utilizatorilor la propriile date personale și controlul asupra acestora;
- Obligarea furnizorilor de servicii de rețea să informeze consumatorii în mod clar și transparent cum vor fi utilizate datele furnizate;
- Asigurarea drepturilor de portabilitate pentru datele personale (transfer mai ușor de la un furnizor la altul).

Pentru a îndeplini aceste sarcini, sistemul trebuie organizat ca un set de componente care suportă următoarele funcții și cerințe: cerințe pentru managementul general al securității; protecția perimetrului; securitatea mediului; cerințe de protecție serioasă a rețelei; securitatea sistemului, cerințe pentru securitatea infrastructurii IT și protecția mediului virtualizat.

Metode de protecție a datelor cu caracter personal (PDP)

Protecția datelor cu caracter personal (PDP) se ocupă de relațiile dintre persoane și societate, prezentate de diferite subiecte și autorități precum guvern, stat, instituții, organizații publice și private, companii etc. Prelucrarea datelor cu caracter personal trebuie să se bazeze pe reguli solide pentru protecția datelor, păstrarea confidențialității persoanei vizate. Din acest motiv, toate instituțiile care prelucrează date cu caracter personal (personal, operator de date) trebuie să elaboreze și să aplice o politică clară și promptă de protecție a datelor ca parte a politicii de securitate a informațiilor și a politicii de securitate în general.

Metodele prezentate de protecția datelor sunt:

- *Blocare* – împiedică accesul utilizatorului neautorizat în încăperile în care sunt stocate datele;
- *Managementul Accesului* – asigură utilizarea în siguranță a tuturor resurselor de informații și utilizarea tuturor resurselor sistemului prin verificarea drepturilor de acces, definite preliminar pentru fiecare utilizator;
- *Criptare* – oferă utilizarea algoritmilor criptografici pentru a cripta datele făcându-le de neînțeles pentru un utilizator nelegitim;
- *Identificare* – identificarea personalului și a componentelor individuale ale sistemului care sunt înregistrate ca utilizatori legitimi și pentru care au fost definite drepturi de acces;
- *Control* – metode, care protejează datele de activitățile neautorizate ale utilizatorilor legitimi;

- *Sancțiuni* – programul de protecție descrie regulile interne de prelucrare și utilizare a informațiilor, precum și responsabilitatea consumatorilor conform normelor legale și legilor

Concluzie

Confidențialitatea și securitatea în era digitală sunt probleme actuale ce vizează fiecare membru al societății. Din aceste considerente, informarea în masă cu privire la riscurile absenței unor garanții suficiente pentru protecția datelor cu caracter personal și cu privire la măsurile de precauție în domeniu este indispensabilă.***Un om informat este un om protejat!***

Referințe bibliografie:

1. Bloustein E.J., Pallone N.J. *Individual and Group Privacy*, New York: Routledge, 2017.
2. Romansky R. A survey of digital world opportunities and challenges for user's privacy. In: *International Journal of Information Technology and Security*, 2017, no.4, vol.9, pp. 97-112. [citat la 06.12.2022]. Disponibil: https://www.researchgate.net/profile/Radi-Romansky/publication/321475317_A_SURVEY_ON_DIGITAL_WORLD_OPPORTUNITIES_AND_CHALLENGES_FOR_USER'S_PRIVACY/links/5a22d18e4585155dd41c8e99/A-SURVEY-ON-DIGITAL-WORLD-OPPORTUNITIES-AND-CHALLENGES-FOR-USERS-PRIVACY.pdf
3. Alsmadi I., Burdwell R., Aleroud A., Wahbeh A., Al-Qudahn M, Al-Omari A. Introduction to information security. In: *Practical Information Security*, Springer: 2018, pp.1-16. [citat la 06.12.2022]. Disponibil: https://www.springer.com/gp/book/9783319721187.
4. Oostveen M., Irion U., The golden age of personal data: How to regulate an enabling fundamental right? In: *Personal Data in Competition, Consumer Protection and Intellectual Property Law"* (eds. M. Bakhoum, B. Conde Gallego, MO Mackenrodt, G. Surblytė-Namavičienė), Springer: 2018, pp.7-26. [citat la 06.12.2022]. Disponibil: https://link.springer.com/chapter/10.1007/978-3-662-57646-5_2
5. Wandra P, Jie H., DeepProfile: Finding fake profile in online social network using dynamic CNN. In: *Journal of Information Security and Applications*, 2020, vol. 52, 102465. https://doi.org/10.1016/j.jisa.2020.102465 [citat la 06.12.2022]. Disponibil: https://www.sciencedirect.com/science/article/abs/pii/S2214212619303801
6. Regulamentul (UE) 2916/679 al Parlamentului European și al Consiliu-

lui din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date și de abrogare a Directivei 95/46/CE (General Data Protect Regulation). In: Jurnalul Oficial al Uniunii Europene, 4.5.2016, L 119/1. [citat la 06.12.2022]. Disponibil: https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32016R0679&from=EL

7. Facebook. *Opţiunile de confidenţialitate.*

Coordonat:
Natalia CRECIUN, dr. în drept, lector univ., USM