 e-ISBN 978-9975-155-42-7; DOI 10.5281/zenodo.5669883

SECURITY OF PERSONAL DATA IN THE VIRTUAL ENVIRONMENT

SECURITATEA DATELOR CU CARACTER PERSONAL ÎN MEDIUL VIRTUAL

NEGOIȚA Ioan, student, specialitatea: FB
Academia de Studii Economice din Moldova
Republica Moldova, Chișinău, str. Bănulescu-Bodoni 61, www.ase.md
e-mail autor**:** negoita.ioan@ase.md

Abstract. *The research reflect the importance of personal data security of users of electronic platforms, because with the development of information technologies beneficial to the population have developed various methods of scams, cyber attacks, espionage and others that produce leaks of personal information, the elderly community being a more vulnerable component in this regard.*
Based on the analysis, it was found that there are currently an extremely large number of people who have been affected by hackers who seek to collect personal data and use them for financial gain.
The results obtained from this research will contribute to highlighting the problem of identity theft for illicit purposes in the online environment, globally, highlighting the causes of personal data leakage, exemplifying methods to prevent attacks by hackers and data protection for all categories of users of contemporary electronic platforms and services.
Key words: *Personal data, cyber security, electronic platforms.*

JEL CLASSIFICATION: L86, K24

INTRODUCERE. Evoluția pe scară largă a tehnologiilor informaționale și pătrunderea acestora practic în toate domeniile de activitate ale umanității a contribuit esențial la dezvoltarea societății globale, dar totodată acest sector rămâne vulnerabil față de riscurile existente și anume față de riscul furtului de date personale din sistemele informatice ale companiilor, dar și din bazele de date guvernamentale și personale ale utilizatorilor, ca rezultat al apariției unui număr are de metode escrocherii, atacuri cibernetice, spionaj electronic și alte tipuri de scurgeri de date.
Securitatea datelor cu caracter personal în mediul virtual devine prioritară în activitatea umană, care are ca scop prevenirea oricărui tip de atac cibernetic și menținerea stabilității în procesele utilizării informațiilor utilizatorilor.

CONȚINUTUL DE BAZĂ

Analiza surselor bibliografice. Cercetarea efectuată se bazează pe analiza literaturii de specialitate, diverse surse electronice, cât și regulamente interne de securitate cibernetică ale unor companii care utilizează în activitate date personale ale utilizatorilor.
Descrierea metodei de cercetare utilizată. Informația, reflectată în acest studiu, se bazează pe sursele de specialitate din domeniul tehnologiilor informaționale, care permit crearea unor viziuni clare despre noțiunea de securitate cibernetică, una dintre cele mai importante părți componente ale unei economii contemporane, care are ca scop protecția datelor confidențiale și creșterea vitezei de prelucrare a datelor și ca rezultat dezvoltarea economiei per ansamblu. La baza cercetării a stat metoda documentar-normativă, metoda comparației și metoda inducției.
Rezultatele obținute. Multitudinea de surse bibliografice definesc în același mod datele personale ale utilizatorilor sistemelor informatice. Conform informațiilor oferite de Centrul Național pentru Protecția Datelor cu Caracter Personal al Republicii Moldova, datele personale reprezintă: prenumele, numele, adresa, numărul de telefon, adresa electronică, datele de localizare, adresa IP, starea civilă, fotografia feței, obiceiurile și preferințele, identificatorii online și orice alte date ce țin de identitatea fizică, fiziologică, economică, culturală sau socială care pot fi utilizate pentru identificarea directă sau indirectă a unei persoane fizice [1].

Datele cu caracter personal, prelucrate de procesorii de date, sunt tratate în conformitate cu prevederile legislației în vigoare și normelor internaționale aplicabile, care reglementează protecția datelor cu caracter personal.

Unii dintre cei mai mari procesori de date personale atât ale clienților, cât și ale angajaților sunt băncile comerciale care se conduc după regulamentele interne stricte de prelucrare a acestora.

- Prelucrarea datelor cu caracter personal în cadrul băncii este bazată pe următoarele principii:
  legalitate, echitate și transparență – datele cu caracter personal sunt prelucrate cu bună-credinţă şi în conformitate cu dispoziţiile legale în vigoare, în mod echitabil și transparent față de persoana vizată;
- *limitarea scopului* – datele cu caracter personal sunt colectate în scopuri determinate, explicite și legitime și nu sunt prelucrate ulterior într-un mod incompatibil cu aceste scopuri;
- *minimizarea datelor* – datele cu caracter personal sunt adecvate, relevante și limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate;
- *exactitate* – datele cu caracter personal sunt exacte și, în cazul în care este necesar, să fie actualizate; se asigură că datele cu caracter personal care sunt inexacte, având în vedere scopurile pentru care sunt prelucrate, sunt șterse sau rectificate fără întârziere;
- *limitări legate de stocare* – datele cu caracter personal nu trebuie păstrate decât în măsura necesară scopurilor pentru care sunt prelucrate; datele pot fi stocate pe perioade mai lungi în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice, cu aplicarea măsurilor de ordin tehnic și organizatoric adecvate, în vederea garantării drepturilor și libertăților persoanei vizate;
- *integritate și confidențialitate* – se aplică măsuri tehnice sau organizatorice corespunzătoare, care asigură securitatea adecvată a datelor cu caracter personal, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, a distrugerii sau a deteriorării accidentale.

Banca prelucrează datele cu caracter personal având la bază următoarele temeiuri legale:

- obligația legală care îi revine Băncii conform legislației cu privire la activitatea băncilor;
- obligația de executare a prevederilor contractuale la care Banca este parte;
- interesul legitim al Băncii;
- consimțământul persoanei vizate (în cazurile prevăzute de lege).

Cu excepția cazurilor în care datele cu caracter personal sunt prelucrate în temeiul consimțământului persoanelor vizate, refuzul persoanelor de a fi prelucrate datele de către Bancă va face imposibilă prestarea serviciilor solicitate sau soluționarea cererilor acestora.

Banca prelucrează datele pe care le furnizează în mod direct subiecții datelor cu caracter personal, precum și datele care sunt generate ulterior, pe baza acestora, prin completarea cererilor şi formularelor, în dependenţă de serviciul solicitat. În vederea asigurării unor servicii financiar-bancare calitative și conformării la prevederile legale, în special din domeniul prevenirii spălării banilor şi finanţării terorismului, Banca poate să consulte baze de date publice/private și alte surse sigure și independente, în limitele legislației în vigoare. Datele cu caracter personal sunt prelucrate manual, automatizat sau mixt.

În dependență de scopul prelucrării datelor și/sau derularea relației contractuale cu Banca (angajat, client, partener), dar și având în vedere specificul activităților desfășurate de către Bancă, pot fi prelucrate următoarele categorii de date cu caracter personal:

- *date generale de identificare:* nume, prenume, patronimic și pseudonim (după caz), data şi locul naşterii, cetățenia;
- *date de contact:* domiciliul şi reşedinţa (dacă este cazul), numărul de telefon/fax, adresa de poştă electronică;
- *date atribuite de autorități publice:* codul numeric personal, seria şi numărul actului de identitate (după caz, copia actului de identitate);

- *date profesionale:* profesia, ocupaţia, numele angajatorului ori natura activităţii proprii, funcția publică deținută (dacă este cazul);
- *date privind situația familială:* stare civilă, număr copii, persoane aflate în întreținere;
- *date privind situația financiară:* venituri, tranzacții bancare și istoricul acestora, bunurile deţinute;
- *date bancare:* coduri de identificare, coduri IBAN atașate conturilor bancare, numerele cardurilor de plată, data expirării cardurilor;
- *semnătura electronică, semnătura olografă;*
- *imaginea:* foto (din actul de identitate furnizat) și video (înregistrată de camere de supraveghere video instalate în sediile Băncii);
- *vocea:* înregistrată în cadrul convorbirilor telefonice cu reprezentanții Băncii (de ex.: serviciile call center și suport carduri);
- *date necesare pentru evitarea fraudelor:* informații publice despre acuzații și condamnări legate de infracțiuni precum fraude, spălare de bani și finanțarea actelor de terorism;
- *date tehnice la utilizarea serviciilor prestate online sau la vizitarea site-ului Băncii:* parola de unică folosință (One Time Password); adresa IP (Internet Protocol), tipul și versiunea de browser, sistemul și platforma de operare, tipul dispozitivului și marca dispozitivului mobil și alte informații incluse în fișierele de tip cookie.

Banca evită să prelucreze date din categoria specială a datelor cu caracter personal (originea rasială sau etnică, convingerile politice, religioase, privind starea de sănătate sau viaţa intimă, precum şi cele privind condamnările penale) [2].

Chiar dacă în trecut securitatea cibernetică reprezenta o preocupare doar pentru departamentele de IT, în prezent, cu toții suntem vizați de aceste atacuri. Iată câteva exemple de atacuri cibernetice și cum le putem recunoaște:

- *Phishing-ul* - unul dintre cele mai întâlnite atacuri cibernetice. Scopul este colectarea de informații confidențiale, acum ar fi IDNP-ul, numere de card sau de cont, coduri PIN și folosirea acestora pentru a sustrage bani. Acest lucru se face prin trimiterea de mail-uri sau SMS-uri care par trimise din partea unei companii cunoscute. Infractorul poate ridica problema unor defecțiuni sau erori tehnice, care necesită reintroducerea datelor personale sau poate trimite mesaje care promit un premiu în schimbul datelor.
- *Scam-ul* - un exemplu de atac este frauda „Mesaj de la șef". Aceasta vizează angajații care sunt autorizați să efectueze plăți. Infractorul sună sau trimite un mail, spunând că este unul dintre managerii companiei. Acesta este bine informat cu privire la organizație și solicită efectuarea urgentă a unei plăți. De asemenea, folosește expresii precum „avem încredere în tine" și „rămâne între noi". În plus, angajatului i se cere să nu respecte procedura obișnuită de autorizare a plăților.
- *Spam-ul* reprezintă corespondența electronică pe care nu am "comandat-o". Acesta poate fi atât comercială, cât și necomercială sau poate fi spam de tip politic, de caritate, de promovare. În cazul în care primim un e-mail dintr-o sursă anonimă, cel mai sigur pas este să îl ștergem imediat. De multe ori, mesajele spam nu fac niciun rău, dar ideal ar fi ca acestea să nu fie citite, pentru a evita orice probleme.
- *Cryptojacking-ul* este periculos deoarece nu vedem că s-a instalat și nu suntem conștienți de prezența lui pe dispozitivul utilizat. Nu se întâmplă nimic și în continuare avem acces la datele noastre, iar hackerii nu extrag date personale, nu compromit fișiere, nu solicită recompense și nu blochează calculatoarele. Scopul cryptojacking-ului este de a folosi resursele calculatorului pentru a crea monede virtuale. Singurul lucru care poate ridica un semn de întrebare este consumul de energie mai ridicat al calculatorului [3].

Companiile care utilizează date personale permanent întreprind acțiuni de implementare și îmbunătățire a măsurilor de protecție a datelor cu caracter personal, prin:

- ajustarea controalelor de securitate în cadrul băncii la cerințele legislației în vigoare;

- menținerea și îmbunătățirea continuă a Sistemului de Management al Securității Informației (SMSI), implementat în bănci și conformarea cu cerințele standardului internațional ISO 27001;
- în cadrul băncilor sunt utilizate metode și tehnologii de securitate avansate, împreună cu politici stricte aplicate angajaților și procedurilor de lucru. Toate sistemele operaționale și de procesare a datelor rulează în medii securizate, astfel ca informația să fie protejată de acces neautorizat;
- angajații băncilor asigură confidenţialitatea şi securitatea prelucrării datelor cu caracter personal, respectarea şi executarea prevederilor actelor normative în domeniul prelucrării şi asigurării securităţii datelor cu caracter personal, inclusiv a procedurilor aprobate în ordinea stabilită în băncile comerciale.

CONCLUZII. Primul lucru pe care trebuie să îl avem în vedere când apare subiectul de protecție a datelor personale este găsirea unor soluții de securitate eficiente. De asemenea, în anumite condiții se impune o abordare specială a acestui aspect. În acest sens au fost create companii specializate în combaterea atacurilor cibernetice și a orice tip de escrocherii prin elaborarea programelor antivirus, aplicațiilor de securitate utilizate pe orice dispozitiv electronic, respectiv este necesar de a urma recomandările specialiștilor:

- menţinerea sistemul de operare actualizat la zi;
- folosirea unui program antivirus;
- folosirea unui *firewall* - sistem de securitate a rețelei care monitorizează și controlează traficul de rețea de intrare și de ieșire pe baza regulilor de securitate prestabilite;
- efectuarea copiilor de rezervă pentru fișierele importante;
- descărcarea aplicațiilor doar din sursele autorizate;
- folosirea parolelor de acces mai puternice;
- configurarea autentificării cu doi factori în conturile financiare și de e-mail;
- evitarea postării unor informaţii personale ca adresa şi numărul de telefon;
- evitarea folosirii unor parole care pot fi identificate uşor , chiar şi de cei apropiaţi;
- utilizarea unei adrese de email specială, diferită de cea strict personală sau profesională.

Respectarea recomandărilor menționate permite creșterea gradului de siguranță a datelor personale ale utilizatorilor în mediul virtual, precum și derularea proceselor care presupun folosirea datelor personale fără perturbări.

REFERINȚE BIBLIOGRAFICE:

1. *Protecția datelor pentru persoane fizice* [online]. [citat 28 martie 2021]. Disponibil: https://datepersonale.md/data-protection-for-individuals/
2. *Politica de securitate a datelor cu caracter personal în cadrul BC „MOLDOVA-AGROINDBANK" S.A."* [online]. [citat 28 martie 2021]. Disponibil: https://www.maib.md/files/2020/Info%20util/Extras_Politica_date_personale_MAIB_public.pdf.
3. *Cum recunoşti o tentativă de Phishing, Scam, Spam sau Cryptojacking?* [online]. [citat 28 martie 2021]. Disponibil: https://www.orange.ro/newsroom/stire/cum-recunosti-o-tentativa-de-phishing-scam-spam-sau-cryptojacking-1125.

Coordonator ştiinţific: CAPAȚINA Valentina, dr., conf. univ.
Academia de Studii Economice din Moldova
Republica Moldova, Chișinău, str. Bănulescu-Bodoni 61, www.ase.md
e-mail: valentina@ase.md