Recomandări privind publicarea datelor cu caracter pesonal

pe rețelele de socializare

Reieșind din creșterea semnificativă a numărului de rețele de socializare din ultimul deceniu, precum și din necesitatea stringentă de a proteja confidențialitatea datelor cu caracter personal ale persoanelor fizice, Centrul Național pentru Protecția Datelor cu Caracter Personal (CNPDCP) vine cu următoarele recomandări:

Odată cu apariția rețelelor de socializare, precum Twitter, Tumblr, Facebook, Telegram, Instagram, Linked In, Tik Tok, Snapchat etc., viața socială s-a schimbat radical, acestea devenind un instrument puternic pentru a socializa, a face noi prieteni și cunoștințe, a distribui imagini foto, video sau pentru a promova o informație. Persoanele împărtășesc cu ușurință știri, imagini, opinii personale și aproape orice se întâmplă în viața lor. Divulgarea datelor cu caracter personal creează un mediu favorabil pentru companiile de publicitate, persoanele care lansează apeluri caritabile (strângeri false de fonduri în scop umanitar), persoanele ce intenționează să se răzbune, infractorii cibernetici, iar acest lucru ar putea presupune colectarea datelor sensibile despre activitățile, interesele, caracteristicile personale, opiniile politice, obiceiurile și comportamentele online ale persoanelor.

Informațiile cu caracter personal pe care o persoană le publică online, alături de datele care descriu acțiunile sale și interacțiunile cu alte persoane, pot crea un profil cuprinzător, care ar putea să conțină activitățile și pasiunile persoanei respective.

În linii mari, **serviciile de socializare în rețea (SSR)** pot fi definite ca platforme de comunicare online care oferă persoanelor posibilitatea de a se alătura unei rețele sau de a crea comunități/grupuri de utilizatori care împărtășesc aceleași opinii și prezintă anumite caracteristici comune:

- utilizatorii sunt invitați să furnizeze date cu caracter personal cu scopul de a crea așa numite „conturi/profile”, ce conțin o descriere personală;

- SSR oferă, de asemenea, instrumente ce permit utilizatorilor să publice propriile materiale (conținut generat de utilizator, cum ar fi o fotografie, muzică, videoclipuri sau link-uri către alte site-uri);

- „socializarea în rețea” este facilitată de utilizarea unor instrumente care oferă pentru fiecare utilizator o listă de contacte prin intermediul căreia utilizatorii pot interacționa între ei.

Prin prisma cadrului legislativ național ce reglementează domeniul protecției datelor cu caracter personal, **furnizorii SSR sunt operatori de date**. Aceștia pun la dispoziție metodele de prelucrare a datelor utilizatorilor și furnizează toate mijloacele/serviciile „de bază” ce țin de gestionarea utilizatorilor (de exemplu înregistrarea și ștergerea conturilor de utilizator). De asemenea, **furnizorii de aplicații pot fi operatori de date**, în situația în

care creează aplicații care funcționează/rulează alături de SSR și dacă utilizatorii decid să utilizeze o astfel de aplicație.

În majoritatea cazurilor, utilizatorii sunt considerați a fi subiecții datelor. Legislația în domeniul protecției datelor **nu impune obligațiile care revin unui operator de date unei persoane fizice - utilizator care prelucrează datele cu caracter personal „în cursul unei activități exclusiv personale sau domestice" – așa-numita „excepție a activităților domestice”**.

Totuși, în anumite situații, există posibilitatea ca activitățile unui utilizator SSR să nu fie acoperite de excepția activităților domestice și să se considere că utilizatorul a preluat unele dintre obligațiile unui operator de date, în aceste cazuri, fiind necesară respectarea prevederilor legislației în domeniul protecției datelor cu caracter personal.

Astfel, utilizatorul SSR va fi considerat operator și **excepția activităților domestice nu se va aplica** în următoarele situații:

- *Utilizatorul acționează în numele unei societăți sau asociații, fie oricare altă entitate; sau dacă utilizează SSR în special ca o platformă de promovare a obiectivelor comerciale, politice sau caritabile.* În acest caz, acestuia îi revine calitatea și, respectiv, responsabilitatea unui operator de date care divulgă date cu caracter personal unui alt operator de date (SSR) și părților terțe (alți utilizatori SSR sau alți eventuali operatori de date care au acces la aceste date). **În aceste situații, utilizatorul trebuie să aibă consimțământul persoanelor vizate sau să invoce un alt temei legitim prevăzut de Legea nr. 133/2011 privind protecția datelor cu caracter personal**.

- În general, accesul la datele (date de profil, publicări, relatări…) cu care operează/acționează un utilizator este limitat la contactele selectate de acesta. *În anumite situații, însă, lista de contacte terțe ale utilizatorilor se poate extinde, fără ca utilizatorul în cauză să cunoască unele contacte care au acces la contul său.* **Un număr ridicat de contacte poate fi un indiciu că excepția activităților domestice nu se aplică și că utilizatorul poate fi considerat operator de date**. Astfel, **dacă accesul la informațiile din profil se extinde dincolo de contactele selectate de utilizator**, ca în cazul conferirii dreptului de acces la un profil tuturor membrilor SSR sau **când datele sunt indexabile de motoarele de căutare**, **accesul nu se limitează la domeniul personal sau domestic.** În mod similar, dacă un utilizator ia o decizie informată de a extinde accesul la profilul său prin acceptarea mai multor persoane în afara „prietenilor” selectați, **acesta va trebui să își asume responsabilitățile unui operator de date.**

- Totodată, trebuie să se rețină că și *în cazul în care nu se aplică excepția activităților domestice, utilizatorul SSR poate beneficia de alte excepții, precum excepția pentru scopuri jurnalistice, artistice sau literare*. În aceste cazuri, trebuie să se obțină un echilibru între libertatea de expresie și dreptul la viață privată.

Nu în ultimul rând se va preciza că **și în cazul în care se aplică excepția activităților domestice, un utilizator poate fi considerat răspunzător conform dispozițiilor generale ale legislației naționale civile sau penale în cauză** (de exemplu, calomniere, răspundere delictuală pentru încălcarea dreptului la personalitate, răspundere penală).

Respectiv, **utilizatorii SSR trebuie să demonstreze precauție maximă ce date cu caracter personal publică, ce scriu în public, ce fotografii/înregistrări video sau audio plasează sau cui acordă încredere pe o rețea de socializare**.

Totodată, CNPDCP atenționează că, colectarea şi prelucrarea de date cu caracter personal pe rețelele de socializare, ca și orice prelucrare de date, trebuie să fie efectuată în strictă conformitate cu prevederile Legii privind protecția datelor cu caracter personal, iar datele cu caracter personal care fac obiectul prelucrării trebuie să fie: prelucrate în mod corect şi conform prevederilor legii; colectate în scopuri determinate, explicite şi legitime, iar ulterior să nu fie prelucrate într-un mod incompatibil cu aceste scopuri; adecvate, pertinente şi neexcesive în ceea ce priveşte scopul pentru care sînt colectate şi/sau prelucrate ulterior.

Astfel, CNPDCP îndeamnă subiecții de date să-și protejeze confidențialitatea vieții private înainte de a publica sau a distribui anumite informații pe rețelele de socializare sau pe orice altă platformă online.

Este foarte important ca utilizatorii rețelelor de socializare să citească cu atenție și să înțeleagă:

- ***Termenii de confidențialitate*** (de exemplu, conținutul care poate fi partajat cu o terță parte, posibilitatea de a șterge conținutul de pe site etc.);
- ***Caracteristicile site-ului*** (de exemplu, cine vă poate vedea mesajele, dacă vor fi doar destinatari specificați sau toți utilizatorii de pe platformă etc.);
- ***Ce informații biografice ar trebui furnizate*** (de exemplu, datele biografice, cum ar fi: numele complet, anul nașterii, vârsta sau adresa, ar trebui să fie utilizate doar la înregistrarea contului și nicidecum oferite altor utilizatori de pe rețelele de socializare),
- ***Informații despre cont*** (de exemplu, informațiile sensibile, cum ar fi: școala frecventată, afilierea politică, informații despre contul bancar, locul de trai/domiciliul etc., nu ar trebui furnizate niciodată);
- ***Cine sunt potențialii „Prieteni”*** (de exemplu, prin analiza profilului persoanelor respective, pentru a înțelege cine sunt, ce fac și ce fel de conținut distribuie);
- ***Necesitatea de a dezactiva funcțiile de partajare a locației gadgetului utilizat***;
- ***Atenție maximă la postarea online a fotografiilor/înregistrărilor video sau audio*** (ar putea fi foarte dificil să fie șterse, cum ar fi în cazul metadatelor sau dacă cineva le-a copiat, le-a partajat sau le-a distribuit pe alte site-uri sau rețele de socializare) etc.

Chiar dacă, este destul de greu de a controla confidențialitatea vieții private în rețelele de socializare, acest lucru nu este imposibil. CNPDCP accentuează asupra responsabilității fiecărui cetățean în vederea asigurării protecției datelor cu caracter personal, or, securitatea și confidențialitatea acestor date trebuie să constituie o prioritate.