MINUNATA LUME DIGITALĂ – ÎNTRE GDPR ȘI ANARHIA DATELOR

Autor: Iulian-Alfred Husac | 11 octombrie 2022

Lumea digitală este o lume a contrastelor. Până nu demult nereglementată[1], în această lume anarhică întâlneai o moștenire legislativă învechită (Directiva cu privire la protecția datelor, 1995), nesocotită de lăcomia marilor platforme digitale care, conștientizând valoarea noii resurse, stocau și foloseau datele personale ale utilizatorilor fără vreo constrângere reală… o lume în care nu se întâmplau foarte multe, în afară de câteva *scandaluri* (sic!) de tipul *Cambridge Analytica*, *TalkTalk*, ș.a., în care informațiile personale a câtorva milioane de utilizatori au fost sustrase și instrumentate după bunul plac al noilor dobânditori.

Apoi a fost adoptat Regulamentul General al Uniunii Europene privind protecția datelor (încetățenit ca GDPR) care, cu toată neliniștea publică creată în jurul său, a marcat totuși un pas înainte față de protecția de care dispuneau în trecut subiecții de drept privat. Astfel, ceea ce îmi propun să susțin în acest articol este că, în ciuda protecției conferite de GDPR, datele personale ale indivizilor sunt în continuare la dispoziția solicitatorilor și, în consecință, pot fi instrumentate cu ușurință de actorii lumii digitale. Această situație este nedreaptă din două motive: *problema consimțământului* și *inevitabilitatea oferirii de date cu caracter personal*.

Mai întâi, pentru a înțelege mai bine de ce datele personale contează și care este miza în ceea ce le privește (altfel zis, *la raison d'être* al GDPR), voi descrie modelul de *business* din spatele marilor platforme online. În literatura de specialitate se face distincție între rețelele sociale și cele de *sharing*[2] (*Social Networks and Sharing Networks*). În categoria rețelelor sociale se încadrează platforme ca Twitter, Facebook, LinkedIn, iar în categoria celor de *sharing* YouTube, Snapchat sau Instagram. Analiza mea se va axa cu precădere pe rețelele de socializare.

Modelul de *business* din spatele Social Media

Revenind la modelul de *business*, acesta se bazează în mare parte pe modul de folosire

de către utilizator a rețelelor sociale. Mai exact, platformele de Social Media permit crearea de conturi de utilizator, în baza cărora persoane fizice și juridice interacționează prin mijloacele tehnice de comunicare puse la dispoziția lor: postări, anunțuri, comentarii, like-uri, distribuiri. Tot ce trebuie să facă utilizatorul este să-și insereze datele personale, astfel încât să-și contureze *identitatea virtuală*. Cum marile rețele sociale își oferă serviciile în mod gratuit, sursa de venit o constituie pentru ele spațiul oferit publicității. Modelul de *business* este exact acesta: companiile care doresc să-și facă publicitate sau să promoveze un anumit tip de conținut plătesc rețelele sociale pentru ca acesta să fie vizionat de anumiți utilizatori. Mai mult, și utilizatorii pot fi selectați în funcție de cerințele plătitorului (care pot varia de la foarte generale, precum țara de unde se conectează, la foarte exacte, precum o anumită pagină pe care utilizatorul a apreciat-o).

De ce datele personale contează în modelul de *business* al rețelelor sociale? Pentru că algoritmul rețelelor de socializare permite confirmarea identității celui care a vizionat postarea sau reclama. Astfel, conținutul vizionat de utilizator este rezultatul sortării efectuate de algoritmi, care încearcă să direcționeze un conținut cât mai particularizat. Motivul pentru care companiile își fac publicitate pe rețelele sociale este că pot obține foarte ușor date care să releve dacă campania lor a ajuns la publicul țintă sau nu. Desigur, introducerea altor variabile în această ecuație ne ilustrează și potențialele riscuri și importanța pe care o au datele cu caracter personal. De exemplu, un conținut cu un caracter extrem de convingător poate fi direcționat unui anumit sector sau grup de utilizatori vulnerabili, care să fie influențat într-un anume fel sau făcut să acționeze în cauză. Exemplele sunt nelimitate, la fel ca pericolele care rezidă în spatele acestui mecanism.

GDPR – definiții și întrebări

GDPR a definit datele cu caracter personal ca fiind „orice informații privind o persoană fizică identificată sau identificabilă („persoana vizată”); o persoană fizică identificabilă este o persoană care poate fi identificată, direct sau indirect, în special prin referire la un element de identificare, cum ar fi un nume, un număr de identificare, date de localizare, un identificator online, sau la unul sau mai multe elemente specifice, proprii identității sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale”[3]. Prima parte a enumerării (nume, număr de identificare etc.) o constituie datele personale propriu-zise, iar a doua parte, privitoare la elementele specifice identității fizice, fiziologice, genetice, psihice etc., sunt așa-numitele date personale sensibile.

În modelul de *business* ilustrat mai sus, datele de identificare ale persoanei joacă rolul cel mai important. Și totuși, de ce GDPR nu este suficient? De ce modelul de *business* continuă să funcționeze într-o lume a anarhiei datelor cu caracter personal, când se consfințesc drepturi ale utilizatorilor și se impun obligații în special sectorului privat?

Problema consimțământului

O încercare de răspuns pleacă de la problema consimțământului în mediul digital. Acesta este definit în GDPR în următorii termeni: „orice manifestare de voință liberă, specifică, informată și lipsită de ambiguitate a persoanei vizate prin care aceasta acceptă, printr-o declarație sau printr-o acțiune fără echivoc, ca datele cu caracter personal care o privesc să fie prelucrate”[4].

În plan digital, problema consimțământului pornește chiar de la definiția acestuia, mai exact de la una din condițiile sale intrinseci, aceea de a fi *informat*. A fi informat înseamnă, în termeni colocviali, a avea cunoștință despre ceva, a avea informații (aproximativ) exacte despre o situație. Ori, această condiție a consimțământului, pentru care există și o obligație (de a informa) a platformelor sociale este satisfăcută doar în litera ei, nu și în spirit, prin aceea că însești utilizarea platformei implică o formă subînțeleasă și continuă de consimțământ. În afară de momentul creării unui cont, rețelele sociale evită să informeze utilizatorii, iar utilizatorii trec cu vederea faptul că nu sunt pe deplin și constant informați. Într-un astfel de scenariu este dificil de imaginat că utilizatorul de rând poate să aibă o imagine *informată*, deci să aibă cunoștințe asupra modului și scopului precis în care algoritmul din spatele rețelelor de socializare adună informații și urmărește activitatea pe alte site-uri, prelucrând toate aceste date pentru a-i oferi un *conținut personalizat* (altă sintagmă extrem de vagă și interpretabilă).

Un alt aspect cel puțin problematic și care, prin complexitatea sa, poate face obiectul unei analize de sine stătătoare, este că, deși consimțim să ne împărtășim datele personale, niciodată nu reușim să negociem cu site-uri sau rețele de socializare de pe o poziție de egalitate cu privire la ce informații dorim să oferim mai exact. Puterea de negociere a utilizatorului este limitată, iar accesul său pe o rețea socială depinde adesea de cât de multe informații personale inserează în formularele de creare a contului de utilizator.

La fel, după intrarea în vigoare a GDPR, opțiunile care ți se prezintă la accesarea unui site oarecare ca utilizator european sunt următoarele: „Accept toate”, „Vreau să modific setările individual”, sau „Resping toate”. În acest context, termenul *toate* se referă la instrumentele (*cookies*) de identificare a utilizatorului de internet în mediul online. Bifând oricare dintre cele trei opțiuni, datele cu caracter personal vor fi în continuare prelucrate, dar cu o capacitate diferită de a genera *conținut personalizat*. Cu alte cuvinte, fiecare dintre cele trei opțiuni presupune consimțământul utilizatorului (prin *click*) și au același efect (colectează date de identificare), doar precizia afișării în viitor de reclame sau alt conținut fiind influențată.

Inevitabilitatea oferirii de date

În ciuda definiției pe care GDPR o dă datelor cu caracter personal, există un set de date

care îi scapă: datele comportamentale (*behavioral data*). Ele reprezintă un set de informații care descriu comportamentul unui utilizator de internet pe un site, fiind alcătuite din *click*-uri, taste apăsate, timp petrecut pe o pagină și orice altă activitate care presupune o acțiune din partea acestuia. Mai mult decât a înțelege „ce" și „cum" dorește un utilizator de la un site, datele comportamentale pot spune „de ce" utilizatorul acționează într-un fel.

Platformele digitale au înțeles potențialul economic al acestui tip de date și le comercializează liber, alături de alte tipuri de date mai bine protejate (circumscrise noțiunii de date cu caracter personal). Problema cu colectarea datelor comportamentale este că profită de un aspect pur psihologic: neatenția umană. Fiind bombardați de o sumedenie de informații sub formă de text, imagine sau video, scăpăm din vedere faptul că până și comportamentul nostru în mediul digital este *înregistrat*. De aici și până la asumarea faptului că este inevitabil ca în interacțiunea noastră cu lumea digitală să oferim fără să vrem date rămâne loc doar de o simplă constatare.

În *Recital 39 on GDPR – Principles of Data Processing*, pe lângă enumerarea principiilor procesării de date (principiul legalității, transparenței etc.), se statuează că „Persoanele reale ar trebui informate despre riscurile, regulile, mijloacele de protecție și drepturile cu privire la procesare (de date cu caracter personal n.n.)"[5]. Asta nu înseamnă că persoanele în cauză ar trebui atenționate, având în minte exemplul datelor comportamentale, despre orice mecanism informatic care colectează date personale într-un mod mai puțin evident, dar care fac posibilă stabilirea unei identități? Altfel spus, ar putea fi invocat articolul 13 din Regulament, care pune bazele notificării pe care orice operator trebuie să o furnizeze persoanei căruia i se colectează date personale (sau care pot duce la identificarea sa): de la identitatea operatorului și datele sale de contact, până la durata stocării datelor și chiar posibilitatea ca, la cerere, acestea să fie șterse. Într-o asemenea cheie de interpretare (largă), datele comportamentale ar putea intra sub incidența GDPR.

Așadar, pericolul pe care îl constituie specularea, pe de o parte, a consimțământului parțial invalid date fiind rațiunile de mai sus și, pe de altă parte, a datelor cu caracter comportamental, este cât se poate de real. Ne confruntăm cu o lume digitală a contrastelor care, pe cât este de reglementată, pe atât este de orientată să eludeze orice fel de constrângere legală în mersul ei. Ne rămâne posibilitatea de a rămâne pasivi în fața acestui colos digital sau de a fi proactivi în a ne proteja pe noi și datele noastre personale. Dacă decidem să fim proactivi, GDPR nu trebuie să fie decât începutul.

NOTE

1. Mai exact 25.05.2018 – momentul intrării în vigoare a Regulamentului (UE)

679/2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date. Disponibil la adresa: https://legislatie.just.ro/Public/DetaliiDocumentAfis/201834. ↑

2. O. Burns, *Social Media and Data Privacy*, în „The GDPR challenge. Privacy, Technology, and Compliance in an Age of Accelerating Change" (ed. A. Taal), CRC Press, Boca Raton, 2022, p. 68. ↑

3. Articolul 4, pct. 1 din Regulamentul (UE) 679/2016. ↑

4. Articolul 4, pct. 11 din Regulamentul (UE) 679/2016. ↑

5. Pentru întreaga anexă, a se accesa adresa: https://gdpr-info.eu/recitals/no-39/. ↑

Imagine: rawpixel