ASPECTE DE CONFIDENȚIALITATE LA PRELUCRAREA DATELOR DE LOCALIZARE

PRIVACY ASPECTS IN THE PROCESSING OF LOCATION DATA

Petru ISTRATI, ORCID: 0000-0001-6963-0930
Universitatea de Stat din Moldova

CZU: 342.721:343.522
e-mail: petruistrati@gmail.com

Evoluțiile tehnologice din ultimele decenii în domeniul obținerii datelor de localizare generează o mulțime de avantaje economice, științifice, sociale sau o utilizare specifică în domeniul militar.

Având în vedere că datele de geolocație pot avea precizie și acuratețe din ce în ce mai înaltă, se justifică ascendența îngrijorărilor cu privire la problemele de confidențialitate ce decurg din prelucrarea acestor date. În prezent, fiecare telefon mobil sau ceas „inteligent” este echipat cu o mulțime de diverși senzori (GPS-[Sistemul de Poziționare Globală]; senzor de proximitate; gyroscop; senzor de mișcare; microfon; pedometru; senzor de câmp magnetic; de temperatură; de umiditate etc.). Tehnologia care permite generarea datelor de localizare nu este utilizată în exclusivitate de dispozitivele de comunicare mobilă, dar și în trotinete și biciclete electrice sau autoturisme.

Datele de localizare sunt utilizate, în timp real, la scară largă în aplicațiile de prognoză meteo, hărți și navigație auto, închirieri autoturisme sau imobile, măsurări cadastrale, turism, sănătate și sport, în video registratoarele pentru traficul rutier, aplicații de matrimoniale, rețele de socializare ș.a.

Dezvăluirea cascadei de date ce sunt furnizate de aceste dispozitive și aplicații, în special cele cu privire la localizare, genereză riscuri majore pentru confidențialitate și chiar securitatea persoanei. Scopul prezentului rezumat este de a expune, fără caracter de exhaustivitate, doar câteva aspecte/teze referitor la probleme de confidențialitate la prelucrarea datelor de geolocație, soluțiile legislative existente, având ca obiectiv reliefarea tendințelor și a vectorilor de interpretare și aplicare a acestora.

Datele cu privire la geolocație pot reprezenta date cu caracter personal, noțiune definită la art. 2 al Convenției nr. 108/1981 („*date cu caracter personal” înseamnă orice informație referitoare la o persoană fizică, identificată sau identificabilă* [„*persoana respectivă*”]) [1, art. 2].

Nu de puține ori însă, din cauza sensibilității lor, datele cu privire la localizare pot constitui categorii speciale de date. Astfel, în mod individual sau combinate cu alte date, datele de localizare pot contribui la creionarea unui profil psihologic sau unui model de comportament al subiectului de date [a se vedea Hotărârea Curții de Justiție a Uniunii Europene în cauza (c-293/12) *Digital Rights Ireland Ltd v Minister for Communications,*

Marine and Natural Resources and Others and Kärntner Landesregierung and Others din 08.04.2014, pct. 26-28].

Un model de comportament poate include, de asemenea, categorii speciale de date, dacă, de exemplu, dezvăluie vizite la spitale și locuri religioase, prezența la demonstrații politice sau prezența în alte locații specifice care dezvăluie date despre, de exemplu, viața sexuală. Aceste profiluri pot fi folosite pentru a lua decizii care afectează în mod semnificativ subiectul datelor [2, p.7]. În cauza *Carpenter vs United States* (2018), Curtea Supremă a Statelor Unite a Americii a reiterat raționamentele expuse în cauzele *Katz* (1967) și *Jones* (2012) potrivit cărora indivizii, sub auspiciul celui de-al Patrulea amendament al Constituției, pot avea așteptări rezonabile privind intimitatea și confidențialitatea lor și atunci când se află în spații publice, iar referitor la identificarea prin date celulare, Curtea Supremă a reținut: *Un telefon mobil își urmărește cu fidelitate proprietarul dincolo de străzile publice și în reședințe private, cabinete medicale, sedii politice și alte locații potențial revelatoare. [...] În consecință, atunci când Guvernul urmărește locația unui telefon mobil, realizează o supraveghere aproape perfectă, ca și cum ar fi atașat un monitor de gleznă utilizatorului telefonului* [3, p.13].

Așadar, aproape fiecare posesor de telefon mobil, în mod voluntar, dar nu se știe cât de conștient, poartă cu sine un dispozitiv de supraveghere aproape perfect, care este unic identificabil prin codul IMEI (*International Mobile Equipment Identity*). În prezent, sistemul global de navigație prin satelit (GNSS), stațiile de bază ale Sistemului global pentru comunicații mobile (GSM) și Wi-Fi sunt cele trei tipuri principale de semnale radio utilizate pentru poziționarea în telefoane inteligente [4, p. 313].

Atunci când prelucrează datele cu caracter personal, furnizorii de informații geospațiale se califică fie ca „operatori de date", fie ca „persoane împuternicite de operator". Un operator de date determină scopurile și mijloacele pentru prelucrare, în timp ce o persoană împuternicită acționează la instrucțiunile operatorului de date. Operatorul de date este principalul destinatar normativ al legislației privind protecția datelor [5, p. 23].

În limitele prezentului rezumat ar fi dificil să expunem complet obligațiile operatorului care prelucrează date privind localizarea pentru a se conforma la legislația în vigoare (*preponderent cu referire la legislația Uniunii Europene*), însă pentru început acesta trebuie să fie sigur referitor la temeiul legal al prelucrării (ex.: consimțământul persoanei vizate, executarea unui contract, obligație legală etc.); să ia măsuri suficiente pentru a asigura confidențialitate și securitatea datelor prelucrate; să respecte drepturile subiecților de date etc.

În scopul prevenirii încălcării drepturilor subiecților și având în vedere că prelucrarea datelor cu privire la localizare implică de cele mai multe ori un volum mare de date, cu utilizarea noilor tehnologii, pentru evaluarea corectă a riscului este util și necesar ca operatorul să efectueze un studiu de evaluare a impactului asupra protecției datelor, așa cum este descris în Regulamentul General de Protecție a Datelor [6, considerent 90, 91 și art. 35]. De asemenea, în acord cu art. 25 al actului citat, operatorul prelucrării datelor

cu privire la geolocație, la proiectarea sistemelor de prelucrare a acestor date urmează să asigure protecția datelor începând cu momentul conceperii (*privacy by design*) și în mod implicit (*privacy by deafult*).

Aplicațiile ar trebui să utilizeze datele de localizare doar atunci când sunt active, să aibă facilități intuitive de deconectare a acestei opțiuni și să ofere cât mai multă transparență referitor la sistemul de prelucrare a acestor date. Spre exemplu, având în vedere practica de monitorizare a autoturismelor companiilor, angajații beneficiază de protecția vieții private și atunci când sunt la muncă (a se vedea cauza CtEDO*: Bărbulescu vs România*), persoanele să se poată aștepta la prelucrarea legală a datelor și atunci când sunt în locuri publice (a se vedea cauza CtEDO: *Uzun vs Germania*) și chiar și atunci când fac obiectul unei investigații de natură penală (a se vedea cauza CtEDO: *Ben Faiza vs Franța*).

În contextul economiei „Big Data”, în care capacitățile de prelucrare și stocare a informației cresc în progresie geometrică, datele cu privire la locație reprezintă o mică categorie de date, însă acompaniată cu altele poate provoca riscuri cu privire la securitate și confidențialitatea persoanei.

Localizarea geografică este o tehnologie minunată care stimulează inovația în multe domenii. Cu toate acestea, considerăm că există o nevoie clară de educație, precum și de cercetare privind proiectarea sistemelor care să țină seama de locație, oferind în același timp protecție maximă împotriva încălcării confidențialității [7, p. 6]. Nu este o exagerare să spunem că creșterea utilizării datelor bazate pe locație reprezintă una dintre cele mai mari provocări legate de confidențialitate confruntată vreodată [8, p. 8].

Referințe:

1. Convenția nr. 108 pentru protecția persoanelor referitor la prelucrarea automatizată a datelor cu caracter personal, încheiată la Strasbourg 28.01.1981.
2. „Article 29 Data Protection Working Party”, *Opinion 13/2011 on Geolocation services on smart mobile devices*; 881/11/EN WP 185, adopted on 16 May 2011.
3. *Carpenter vs. United States (2018)*, disponibilă la https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf (accesat la 29.08.2022).
4. BU-PASHA, Sh., ALÉN-SAVIKKO, A., MÄKINEN, J., GUINNESS, R., KORPISAARI, P. EU Law Perspectives on Location Data Privacy in Smartphones and Informed Consent for Transparency. In: *European Data Protection Law Review*, vol. 2 (2016), Issue 3.
5. World Geospatial Industry Council, ”*Geospatial Information and Privacy: Policy Perspectives and Imperatives for Geospatial Industry*”, 2020, disponibil: https://wgicouncil.org/wp-content/uploads/2020/03/Geospatial-Informaion-and-Privacy-report-Final.pdf (accesat la 30.08.2022).

6. Regulamentul UE 2016/679 al Parlamentului European și a Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46. In: *Jurnalul Oficial al Uniunii Europene*, L119/1 din 04.05.2016.
7. FRIEDLAND, G., SOMMER, R. *Cybercasing the Joint: On the Privacy Implications of Geo-Tagging*, în https://www1.icsi.berkeley.edu/pubs/networking/cybercasinghotsec10.pdf (accesat la 26.08.2022).
8. NOLAN, Ph., TABIN, I. *Geolocation services – where does the Article 29 Working Party stand?*. In: *Data Protection Ireland*, vol. 4, issue 4.