

Aplicațiile de urmarire (contact tracing apps) în contextul COVID-19: o perspectiva asupra protecției datelor cu caracter personal



Dupa aproape doua luni de izolare, tot mai multe state din Uniunea Europeana încep sa relaxeze treptat masurile restrictive luate în contextul pandemiei COVID-19. În acest context, preocuparea autoritaților din diverse țari europene se îndreapta din ce în ce mai mult spre utilizarea noilor tehnologii, pentru a sprijini masurile adoptate în cadrul planurilor de relaxare și pentru a preveni reapariția unui nou val de îmbolnaviri în etapa ieșirii din izolare. În mod specific, avem în vedere dezvoltarea unor aplicații, cunoscute generic drept „contact tracing apps”, care pot fi instalate pe telefoanele mobile și care ar avea drept scop, în principal, informarea utilizatorilor asupra masurilor luate de autorități, uneori în combinație cu un chestionar de autodiagnosticare și implementare a unor funcționalități de alerta ca utilizatorul s-a aflat recent în proximitatea unei persoane diagnosticate pozitiv cu COVID-19, care utilizeaza la rândul ei aceeași aplicație.

Prin urmare, este vorba despre aplicații de stabilire a proximitații dintre persoane, bazate pe utilizarea tehnologiei Bluetooth pentru a determina apropierea dintre device-urile mobile care au instalata aplicația, fara a utiliza tehnologii de geolocalizare a persoanelor. Un alt aspect important subliniat de autoritațile care au exprimat recent opinii pe acest subiect este ca instalarea și utilizarea aplicațiilor de catre utilizatori trebuie sa se faca exclusiv în mod voluntar din partea acestora (de exemplu, autoritațile de protecție a datelor din Marea Britanie – 17 aprilie 2020; Franta – 24 aprilie 2020, Belgia – 30 aprilie 2020, Italia – 29 aprilie 2020).

În același timp, utilizarea noilor tehnologii și a modalitaților inovatoare de prelucrare a datelor trebuie sa respecte întotdeauna drepturile și libertațile fundamentale, în special drepturile la viața privata și la protecția datelor cu caracter personal.

Pentru a adresa aceste aspecte, în continuarea Recomandarii (UE) 2020/518 (link) emise de Comisia Europeana pe 8 aprilie 2020, care a evidențiat necesitatea elaborarii unei abordari comune în utilizarea tehnologiei în lupta împotriva coronavirusului la nivelul UE, la data de 15 aprilie 2020, Comisia (prin eHealth Network) a publicat un set de masuri (Toolbox) aplicabile la nivelul statelor member UE privind utilizarea aplicatiilor mobile pentru a sprijini urmarirea contactelor în contextul crizei COVID-19, însoțite la data de 17 aprilie 2020 de o comunicare privind Orientarile în domeniul protecției datelor privind aplicațiile care sprijina combaterea pandemiei de COVID-19. Totodata, în susținerea adoptarii unor abordari comune în dezvoltarea acestor aplicații, la 21 aprilie 2020, Comitetul European pentru Protecția Datelor a emis Ghidul nr. 4/2020 privind utilizarea instrumentelor de urmarire a datelor de localizare și de contact în contextul izbucnirii COVID-19, subliniind principiile care trebuie avute în vedere în dezvoltarea acestor aplicații, astfel încât drepturile persoanelor vizate sa fie respectate, iar prelucrarea sa fie adecvata, necesara și proporționala.

Principalele cerințe care trebuie respectate în dezvoltarea aplicațiilor de urmarire

1. *Utilizarea voluntara:* Setul de instrumente și orientari elaborate la nivel european se refera exclusiv la aplicațiile de urmarire care vor fi utilizate în mod voluntar în lupta împotriva coronavirusului, descarcarea, instalarea și utilizarea acestora fiind facute în mod voluntar de catre cetățeni.
2. *Implicarea autoritatilor naționale de sanatate publica, care sa aiba și responsabilitățile în calitate de operatori de date:* O alta cerința esențiala cuprinsa în recomandarile la nivel european este ca aplicațiile sa fie dezvoltate cu aprobarea autoritaților naționale de sanatate publica. Totodata, recomandarile stabilesc mai multe funcții și cerințe pe care aplicațiile trebuie sa le îndeplineasca, în special pentru a asigura respectarea Regulamentului general privind protecția datelor (EU) 2016/679 (GDPR) și a Directivei privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice (în România, transpusa prin Legea nr. 506/2004). Printre altele, aplicațiile ar trebui proiectate astfel încât autoritațile naționale de sanatate (sau entitățile care îndeplinesc sarcini în interesul public în domeniul sanatații) sa fie operatorii de date, cu toate responsabilitățile care decurg din aceasta calitate.
3. *Importanța implicării și consultării autoritaților de protecție a datelor:* Un alt element cheie este implicarea și consultarea autoritaților de protecție a datelor, în timp ce Comisia atrage atenția și asupra prevederilor GDPR privind evaluarea impactului asupra protecției datelor, care ar trebui efectuata înainte de implementare, având în vedere ca prelucrarea datelor prin intermediul aplicației este susceptibila sa genereze un risc ridicat pentru drepturile și libertățile persoanelor. Aceeași recomandare este reiterata și de alte autorități în domeniul protecției datelor, în opiniile mai sus menționate.
4. *Aplicarea unor masuri de securitate adecvate și eficiente:* Una dintre prioritățile dezvoltatorilor de aplicații trebuie sa fie reprezentata de aplicarea unor masuri și mecanisme de securitate adecvate, într-o maniera care sa asigure toate garanțiile necesare respectării drepturilor si libertăților fundamentale. În acest sens, pentru a limita intruziunea funcționalităților aplicației și pentru a crea cadrul pentru o utilizare de încredere și responsabila, aplicațiile ar trebui sa asigure securitatea datelor prin utilizarea tehnicilor criptografice de ultima generație, sa limiteze dezvaluirea / accesul la date, sa asigure exactitatea datelor pentru a minimiza riscul de a identifica în mod eronat contactele cu o persoana infectata (cu alte cuvinte, pentru a minimiza riscul rezultatelor fals pozitive) și sa permita auditarea arhitecturii aplicației de catre experți tehnici independenți.
5. *Din perspectiva utilizatorilor:* Recomandarile elaborate la nivel european conțin și o serie de masuri pentru a asigura respectarea drepturilor și libertăților fundamentale și cerința ca aplicatiile sa fie folosite doar pentru scopurile specific definite și în limitele stabilite de aceste recomandari, nefiind folosite în scopuri intruzive, precum supravegherea în masa. Acestea includ masuri precum:
 - 5.1. *Lipsa unor consecințe negative* - Întrucât instalarea aplicației este voluntara, nu ar trebui sa existe consecințe negative pentru persoana care decide sa nu descarce sau sa nu utilizeze aplicația.
 - 5.2. *Consimțământ specific* – Conform recomandarilor Comisiei, consimțământul ar trebui sa fie acordat de utilizator în mod specific pentru fiecare funcționalitate diferita a aplicației, nu pentru toate „la pachet” (de exemplu, separat pentru primirea informarilor de la autorități, fața de activarea funcționalităților privind avertizarile de proximitate).
 - 5.3. *Asigurarea efectiva a exercitarii drepturilor persoanelor vizate* reprezinta o alta masura esențiala (în

special cu privire la dreptul de acces, rectificare, ștergere, prevazute de GDPR).

6. *Informarea în mod corespunzător a utilizatorilor cu privire la prelucrarea datelor*, având drept scop asigurarea conformității cu prevederile GDPR. Recomandarile la nivel european ofera, de asemenea, mai multe principii pentru strategiile de comunicare, menționând inclusiv posibilitatea statelor membre de a stabili un singur punct de comunicare la nivel național (cum ar fi autoritățile din domeniul sănătății) și de a prezenta informațiile cheie pentru public cu privire la dezvoltarea și funcționalitățile aplicațiilor, scopurile, mecanismele de control și garanții de securitate în vigoare, dar și avertismente cu privire la utilizarea unor aplicații mobile neautorizate. O astfel de comunicare ar trebui făcută regulat, din timp și cu o frecvență larg cunoscută publicului.

7. *Minimizarea datelor prelucrate și neutilizarea datelor de localizare*: Scopul funcționalității aplicațiilor de urmarire a contactelor este de a notifica cât mai rapid persoanele care s-au aflat în imediata apropiere a unei persoane infectate, ca factor esențial pentru a întrerupe răspândirea COVID-19 și, de asemenea, pentru a preveni reapariția acestuia în faza de ieșire din criza. Pentru a obține acest lucru, Comisia observa ca *datele de proximitate* ar putea fi necesare, considerând, de asemenea, comunicațiile Bluetooth Low Energy între dispozitive ca fiind mai precise pentru identificarea contactelor de proximitate și, prin urmare, mai adecvate decât utilizarea datelor de geolocalizare, care pot fi considerate prea intruzive în viața privată a utilizatorilor. Având în vedere ca scopul aplicațiilor de urmarire nu este de a monitoriza mișcarea persoanelor ori de a monitoriza punerea în aplicare a măsurilor impuse de autorități, ci de a determina proximitatea cu persoanele infectate și de a îndruma persoanele să adopte o anumită conduită (spre exemplu autoizolarea), datele de localizare nu apar ca fiind necesare pentru scopul funcționalității acestor aplicații.

8. *Utilizarea doar pentru durata strict necesară*: Aceste aplicații trebuie să fie utilizate numai pentru durata de timp necesară pentru a asigura prevenirea, combaterea și stoparea răspândirii coronavirusului, fiind dezinstalate și demontate de către dezvoltatorul aplicației imediat ce nu mai sunt necesare, iar datele cu caracter personal șterse în mod ireversibil.

Exista în continuare o serie de aspecte privite cu rezerva sau care sunt subiect de dezbateri, în legătura cu implementarea acestor aplicații, legate în special de tehnologia folosită, modalitatea de stocare a datelor (descentralizat, pe dispozitivele individuale sau centralizat, pe un server administrat de autoritățile naționale de sănătate), utilizarea de date agregate și anonimizate versus complexitatea tehnicilor de anonimizare pentru ca acestea să fie eficiente, sau temeiul legal adecvat pentru prelucrarea datelor, în special dacă este vorba de date privind sănătatea. Prin urmare, acesta rămâne un subiect de abordat cu atenție și responsabilitate, pentru a atinge un echilibru real între beneficiile pe care le poate presupune utilizarea noilor tehnologii și protecția drepturilor și libertăților fundamentale ale persoanelor.