Data Privacy Alert

22 ianuarie 2016

În acest număr:

Schimbări în regimul de notificare al prelucrărilor de date cu caracter personal

Decizia Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal nr. 200/2015 din data de 28.12.2015 aduce o schimbare semnificativă în legătură cu obligația de a notifica autorității prelucrările de date cu caracter personal, în sensul că aceasta va deveni excepția în cazurile expres prevăzute de lege.

Este legitimă accesarea comunicărilor angajaților? Curtea Europeană spune „da, doar în cazuri excepționale”

În data de 12 ianuarie 2016, Curtea Europeană a Drepturilor Omului a pronunțat decizia sa în cazul Bărbulescu c. România și a stabilit că, deși viața privată trebuie respectată la locul de muncă, angajatorii pot fi îndreptățiți să monitorizeze corespondența privată a angajaților, dar doar în anumite circumstanțe specifice.

Schimbări în regimul de notificare al prelucrărilor de date cu caracter personal

În Monitorul Oficial nr. 969/28.12.2015 a fost publicată Decizia Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal (**"ANSPDCP"**) nr. 200/2015 (**"Decizia"**).

Schimbarea de regim juridic în ceea ce privește notificările la ANSPDCP

Principala modificare adusă prin Decizie legislației specifice în materia prelucrării datelor cu caracter personal este schimbarea regimului juridic de notificare a ANSPDCP.

Astfel, potrivit Deciziei, notificarea ANSPDCP cu privire la prelucrarea datelor cu caracter personal va deveni **excepția**, potrivit cazurilor prevăzute expres și menționate mai jos, **regula** fiind că prelucrarea datelor cu caracter personal este permisă fără realizarea unei notificări prealabile.

Acest nou regim juridic nu exonerează în niciun fel operatorul de celelalte obligații pe care acesta le are în baza Legii nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date, în special obligațiile privind asigurarea drepturilor persoanelor vizate, a confidențialității și a securității datelor.

Cazuri de notificare a prelucrărilor de date la ANSPDCP

Excepțiile menționate mai jos cu privire la care va fi necesară, în continuare, notificarea la ANSPDCP se justifică fie prin natura criteriilor pe care se bazează prelucrarea de date, fie având în vedere anumite calități ale persoanei ale căror date cu caracter personal se prelucrează sau având în vedere modalitatea prin care operează colectarea acestor date:

1. Prelucrarea datelor cu caracter personal legate de originea rasială sau etnică, de convingerile politice, religioase, filozofice ori de natură similară, de apartenența sindicală, precum și a datelor privind starea de sănătate și viața sexuală;
2. Prelucrarea datelor genetice și biometrice;
3. Prelucrarea datelor care permit, direct sau indirect, localizarea geografică a persoanelor fizice prin mijloace de comunicații electronice;
4. Prelucrarea datelor cu caracter personal ale minorilor, dacă această activitate a fost efectuată:
    - în cadrul activităților de marketing direct;
    - prin intermediul internetului sau al mesageriei electronice;
5. Prelucrarea datelor cu caracter personal referitoare la săvârșirea de infracțiuni de către persoana vizată ori la condamnări penale, măsuri de siguranță sau sancțiuni administrative ori contravenționale aplicate persoanei vizate, efectuată de către entități de drept privat;
6. Prelucrarea datelor cu caracter personal prin mijloace electronice, având ca scop monitorizarea și/sau evaluarea unor aspecte de personalitate, precum competența profesională, credibilitatea, comportamentul sau alte asemenea aspecte;
7. Prelucrarea datelor cu caracter personal prin mijloace electronice în cadrul unor sisteme de evidență având ca scop adoptarea unor decizii automate individuale în legătură cu analizarea solvabilității, a situației economico-financiare, a faptelor susceptibile de a atrage răspunderea disciplinară, contravențională sau penală a persoanelor fizice, de către entități de drept privat;
8. Prelucrarea datelor personale prin sisteme de supraveghere video, inclusiv transferul acestora într-un stat terț.

Prin excepție, nu va fi necesară notificarea la ANSPDCP în cazul în care prelucrarea este efectuată de către o persoană fizică, în interes personal, chiar dacă imaginile captate cuprind și cadre din spațiul public.

Totuși, **se va aplica regula generală**, în sensul că nu va fi necesară notificarea ANSPDCP chiar și cu privire **la cazurile prezentate mai sus** în măsura în care ne aflăm în una din următoarele situații:

1. Prelucrarea este prevăzută de lege (spre exemplu, instituțiile de credit);
2. Prelucrarea de date cu caracter personal se face în vederea transferului de date în străinătate în temeiul unei legi speciale sau a unui acord ratificat de România;
3. Prelucrarea datelor se face exclusiv în scopuri jurnalistice, literare sau artistice, dacă datele au fost făcute publice în mod manifest de către persoana vizată sau sunt strâns legate de calitatea de persoană publică a persoanei vizate ori de caracterul public al faptelor în care este implicată.

Data la care trebuie efectuată notificarea către ANSPDCP

Operatorul va trebui să notifice la ANSPDCP anterior prelucrării datelor cu caracter personal.

Totodată, în cazul în care prelucrarea se încadrează în una dintre situațiile prevăzute la pct. 1, 2, 5 de mai sus, ANSPDCP va dispune efectuarea unui **control prealabil**. În măsura în care ANSPDCP nu informează operatorul cu privire la efectuarea controlului în termen de cinci zile de la primirea notificării, operatorul va putea trece la prelucrarea datelor cu caracter personal.

Transferul datelor cu caracter personal în afara UE

Transferul datelor cu caracter personal către statele situate în afara Uniunii Europene, a Zonei Economice Europene, precum și către statele cărora Comisia Europeana nu le-a recunoscut, prin decizie, un nivel de protecție adecvat va face, în continuare, obiectul notificării ANSPDCP.

De asemenea, transferul datelor trebuie autorizat în prealabil de către ANSPDCP.

Este legitimă accesarea comunicărilor angajaților? Curtea Europeană spune „da, doar în cazuri excepționale”

În data de 12 ianuarie 2016, Curtea Europeană a Drepturilor Omului („Curtea”) a pronunțat decizia sa în cazul Bărbulescu c. România, ca urmare a cererii cu nr. 61496/08. În decizia sa, Curtea a stabilit că, deși există viață privată la locul de muncă, iar angajatorii nu au un drept prevăzut prin lege să monitorizeze comunicațiile angajaților, o asemenea ingerință este permisă în anumite condiții.

Circumstanțele relevante

Dl. Bărbulescu conducea activitatea de vânzări la o societate privată, în acest scop fiindu-i indicat de către angajator să creeze un cont de Yahoo Messenger. În ceea ce privește acest cont, menționăm că: (i) era un cont de Yahoo Messenger având ca scop comunicarea de tip „chat”, (ii) a fost creat de angajat la solicitarea angajatorului cu scopul de a răspunde la solicitările clienților și (iii) angajatul a declarat că a folosit contul exclusiv în scop profesional (atât prin regulamentul intern, precum și la solicitarea separată a angajatorului).

Pentru a verifica modul în care atribuțiile profesionale ale dlui Bărbulescu erau îndeplinite, angajatorul monitorizase contul de Yahoo Messenger al dlui Bărbulescu de la calculatorul societății. În plus, angajatorul susține că dl. Bărbulescu, folosind calculatorul societății și contul pe care i-a fost indicat să-l creeze în scop personal, acesta a încălcat prevederile exprese asumate prin regulamentul intern și, astfel, angajatorul a dispus concedierea dlui Bărbulescu.

Decizia de concediere a fost contestată de dl. Bărbulescu în fața instanțelor române competente, motivând că angajatorul încălcase dreptul reclamantului la viață privată și, mai precis, secretul corespondenței. Curtea de Apel București a stabilit definitiv că, din moment ce angajatul a susținut în cadrul procedurii disciplinare că nu folosise Yahoo Messenger în scop personal, angajatorul avea dreptul să verifice conținutul comunicărilor, întrucât acesta era singura metoda a angajatorului de a verifica această apărare.

Dl. Bărbulescu a susținut în fața Curții că decizia de concediere din partea angajatorului său s-a bazat pe o încălcare a dreptului său la respectarea vieții private și corespondenței, protejate prin articolul 8 din Convenția Europeană a Drepturilor Omului.

Analiza Curții

1. În acord cu jurisprudență sa constantă, Curtea a considerat că mesajele transmise prin contul de Yahoo Messenger ar trebui incluse în noțiunea de „viață privată” și „corespondență”, prevăzute de articolul 8 din Convenția Europeană a Drepturilor Omului;

2. În absența unui avertisment din partea angajatorului că asemenea comunicări ar putea fi monitorizate, un angajat ar avea o așteptare rezonabilă de intimitate când comunică printr-un mijloc pus la dispoziție de angajator. De asemenea, în situația particulară a dlui Bărbulescu, Curtea a examinat dacă reclamantul avea o așteptare rezonabilă de intimitate când comunica printr-un cont de Yahoo Messenger pe care îl înregistrase la instrucțiunile angajatorului, chiar dacă regulamentul intern al angajatorului interzicea utilizarea bunurilor societății în scop personal;

3. **Curtea a analizat dacă dreptul la respectarea vieții private și corespondenței este proporțional cu interesul angajatorului și a stabilit că angajatorul avea un interes legitim întrucât următoarele condiții sunt întrunite cumulativ:**

    - comunicările reclamantului au fost accesate doar în cadrul procedurii disciplinare, ca rezultat al propriilor susțineri că nu a fost folosit contul de Yahoo Messenger în scop personal;

- monitorizarea însăși a fost limitată la contul de Yahoo Messenger, nefiind extinsă la alte comunicări de la acel cont sau la alte înregistrări de la acel calculator;
- instanțele naționale nu au acordat relevanță deosebită conținutului precis al comunicărilor reclamantului, bazându-se pe transcrierile acestora numai în măsura în care dovedeau abaterea disciplinară a reclamantului, respectiv că acesta folosise calculatorul societății în scop personal în timpul programului de lucru. Nu existau mențiuni în hotărârile acestora referitoare la circumstanțele specifice pe care reclamantul le-a comunicat; de asemenea, identitatea părților cu care a comunicat nu este publicată;
- reclamantul nu a explicat convingător de ce folosise contul de Yahoo Messenger în scop personal.

Concluzie

Curtea a concluzionat că, deși există viață privată la locul de muncă și angajatorii nu au dreptul de a urmări comunicările angajaților, o asemenea ingerință ar putea fi acceptabilă dacă dreptul la respectarea vieții private și corespondenței este proporțional cu interesul angajatorului. În cazul dlui Bărbulescu, comunicările reclamantului au fost accesate pentru a verifica modul în care erau îndeplinite sarcinile sale profesionale, în cadrul procedurii disciplinare, ca urmare a propriilor susțineri în sensul că nu fusese folosit contul de Yahoo Messenger în scop personal.

Vă rugăm să aveți în vedere că decizia Curții privește o situație particulară, iar concluziile Curții ar trebui interpretate în lumina tuturor particularităților speței. Vă rugăm să rețineți că monitorizarea comunicărilor angajaților de către angajator nu a fost impusă angajaților ca o măsură preventivă sau continuă. Astfel, această decizie nu poate fi invocată ca atare în situații similare, iar o evaluarea completă a situației concrete trebuie efectuată de la caz la caz.

Consecințe și următorii pași

Având în vedere circumstanțele speței, în măsura în care la nivelul societății dumneavoastră are loc o monitorizare a activității angajaților, trebuie avute în vedere, printre altele, următoarele aspecte:

- Politica sau regulamentul intern să includă detalii legate de monitorizare (motive, circumstanțe etc.);
- Să fie stabilite reguli clare privind modalitatea de monitorizare și numărul de persoane care pot verifica și controla activitatea angajaților să fie limitat;
- Să fie verificate condițiile privind necesitatea și proporționalitatea măsurii, prin raportare la cazul concret.

Dacă aveți întrebări cu privire la aspectele menționate în acest buletin informativ, vă rugăm să ne contactați.

Andrei Burz-Pinzaru
Partener Reff & Asociații
Avocat
+40 21 207 52 05

Andrei Ionescu
Partener, Deloitte Risk Advisory
+40 21 207 54 85

Florentina Munteanu
Partener Asociat Reff & Asociații
Avocat
+40 21 207 52 75

Cătălina-Teodora Stroe
Manager, Deloitte Risk Advisory
+40 21 222 16 61

Maria-Silvia Axinescu
Avocat senior coordonator Reff & Asociații
+40 (21) 207 54 28