

Traducere din limba engleză

Logo

CCBE

Conseil des barreaux européens
Council of Bars and Law Societies of Europe
Association internationale sans but lucratif

Rue Joseph II, 40 / 8 - 1000 Bruxelles T. : +32 (0)2 234 65 10 - F. : +32 (0)2 234 65 11 Email : ccbe@ccbe.eu - www.ccbe.eu

CCBE privind supravegherea electronică în masă de către autoritățile guvernamentale (inclusiv datele avocaților europeni)

14/10/2013

Background

Consiliul Barourilor și Societăților de Drept din Europa (CCBE) este organizația reprezentativă a peste 1 milion de avocați europeni, prin intermediul barourilor și al societăților de avocatură din 32 de țări cu drepturi depline și 11 țări asociate și observatoare.

La data de 1 iulie 2013, CCBE a emis o declarație (a se vedea, de asemenea, atașată ca anexă la această declarație) privind practicile guvernamentale care implică exploatarea în masă a datelor în scopul supravegherii, în care CCBE și-a exprimat profunda îngrijorare cu privire la faptul că o valoare esențială a profesiei, secretul profesional, cunoscută în unele țări drept privilegiu profesional, este supusă unui risc grav, iar eroziunea acestui aspect al confidențialității va afecta încrederea în statul de drept.

Declarația CCBE s-a bazat pe rapoartele privind încălcarea în masă a drepturilor omului la viața privată și la datele cu caracter personal, realizate la scară sistematică de către agențiile guvernamentale ale principalelor puteri occidentale, inclusiv ale statelor membre ale Uniunii Europene. Astfel de reclamații indică încălcări clare ale Cartei Drepturilor Fundamentale a Uniunii Europene de către anumite organisme guvernamentale ale UE, în special, articolele 7¹ și 8² și, de

¹ **Articolul 7 - Respectarea vieții private și de familie**

Orice persoană are dreptul la respectarea vieții private și de familie, a domiciliului și a secretului comunicațiilor.

² **Articolul 8 - Protecția datelor cu caracter personal**

(1) Orice persoană are dreptul la protecția datelor cu caracter personal care o privesc.

(2) Asemenea date trebuie tratate în mod corect, în scopurile precizate și pe baza consimțământului persoanei interesate sau în temeiul unui alt motiv legitim prevăzut de lege. Orice persoană are dreptul de acces la datele colectate care o privesc, precum și dreptul de a obține rectificarea acestora.

(3) Respectarea acestor norme se supune controlului unei autorități independente.



asemenea, din cauza lipsei oricărui mecanism de revizuire judiciară adecvată, articolul 47³. În ceea ce privește pretinsul acces nediscriminatoriu și supravegherea pe scară largă a majorității comunicărilor dintre cetățenii din afara Statelor Unite, acesta se referea și la comunicările dintre avocați și clienții lor. Considerăm că acest tip de supraveghere în masă depășește expunerea la risc a unor drepturi specifice ale omului între persoane fizice și reprezintă o amenințare la adresa statului de drept recunoscut în democrațiile moderne.

Până la această dată, Uniunea Europeană sau statele membre ale acesteia nu au publicat rapoarte satisfăcătoare cu privire la reclamațiile mai sus-menționate. Fără o bază fermă de fapte referitoare la această chestiune, nu există nicio modalitate de a afla dacă a existat o încălcare a drepturilor fundamentale, cum ar fi articolul 8 alineatul (2) din Carta Drepturilor Fundamentale a Uniunii Europene sau articolul 12 din Directiva privind protecția datelor (95/46/CE), care face, de asemenea, imposibilă orice încercare de aplicare a acestor drepturi. Fiecare cetățean al UE are dreptul de a avea acces la datele care îl privesc, iar acest lucru include, de asemenea, în mod clar dreptul de a ști dacă a suferit o încălcare ilicită a confidențialității cibernetice de către un stat național. De asemenea, reprezintă o problemă faptul că negocierile bilaterale cu Statele Unite ale Americii pe această temă nu au fost deloc transparente până în prezent.

Pe baza rapoartelor din presă și a audierilor recente din cadrul Comisiei LIBE a Parlamentului European, CCBE reține că cele mai mari amenințări la adresa încrederii clienților în secretul profesional provin din două surse: a) lipsa încrederii în organele de stat cu puteri investigaționale secrete (există îngrijorări cu privire la faptul că vor folosi aceste puteri în afara limitelor mandatului lor democratic); și b) lipsa obiectivă a mijloacelor tehnice la dispoziția firmelor de avocatură pentru asigurarea secretului profesional în mod eficient.

În toate statele membre ale UE, secretul profesional al avocaților beneficiază de protecție ridicată, deși limitele și mijloacele de protecție juridică sunt diferite. Atât jurisprudența Curții Europene de Justiție, cât și Curtea Europeană a Drepturilor Omului recunosc acest drept. Cu toate acestea, pe baza unor informații recent dezvăluite cu privire la practica agențiilor de supraveghere din statele principale, a apărut îngrijorarea că protecția oferită de măsurile juridice ale statelor membre ale UE pentru secretul profesional ar putea să nu funcționeze în practică.

³ **Articolul 47 - Dreptul la o cale de atac eficientă și la un proces echitabil**

Orice persoană ale cărei drepturi și libertăți garantate de dreptul Uniunii sunt încălcate are dreptul la o cale de atac eficientă în fața unei instanțe judecătorești, în conformitate cu condițiile stabilite de prezentul articol.

Orice persoană are dreptul la un proces echitabil, public și într-un termen rezonabil, în fața unei instanțe judecătorești independente și imparțiale, constituită în prealabil prin lege. Orice persoană are posibilitatea de a fi consiliată, apărută și reprezentată.

Asistența juridică gratuită se acordă celor care nu dispun de resurse suficiente, în măsura în care aceasta este necesară pentru a-i asigura accesul efectiv la justiție.

Nu există încredere fără confidențialitate - repercusiuni asupra Agendei digitale pentru Europa

Rolul avocatului, indiferent dacă este privit din punctul de vedere al unei persoane fizice, al unei societăți sau statului, este acela de consilier și reprezentant de încredere al clientului, de profesionist respectat de terți și de participant indispensabil în administrarea corectă a justiției și a democrației. Partea esențială a profesiei de avocat este că aceștia i se vor comunica informații cu privire la chestiuni pe care clientul nu le-ar spune altor persoane – cele mai intime detalii ale vieții private sau cele mai valoroase secrete comerciale - și că avocatul este beneficiarul altor informații pe baza încrederii. Fără certitudinea confidențialității, nu poate exista încredere. Prin urmare, dacă cetățenilor și întreprinderilor din UE li se refuză dreptul la protecție împotriva divulgării comunicărilor cu avocații lor, acestora li se poate refuza accesul la consultanță juridică și la justiție.

Realizând un inventar al instrumentelor tehnice aflate la dispoziția firmelor de avocatură, inclusiv cele mai mari firme, CCBE reține că avocații folosesc în prezent sisteme de comunicații electronice și servicii cloud care nu sunt sigure, pentru că acum știm că au fost concepute cu tehnologii "backdoors" pe care agențiile guvernamentale le pot deschide. Cu toate acestea, după cum am aflat recent, chiar și cea mai mare dintre aceste agenții guvernamentale întâmpină uneori dificultăți privind controlul asupra informațiilor secrete la care acestea au acces. Este evident faptul că, cu cât există mai multe tehnologii "backdoors", cu atât infrastructura online va fi mai puțin sigură.

Dacă avocații folosesc astfel de comunicații electronice nesigure sau servicii de tip cloud, aceștia încalcă de facto obligațiile lor de controlori de date și regulile deontologice. Această problemă privind utilizarea unor comunicații nesigure nu este doar o problemă de formare sau de cultură, ci mai degrabă o problemă a tuturor întreprinderilor europene, cu excepția celor mai mari sau a celor din industria de apărare.

Ca o consecință a acestor circumstanțe, avocații se văd nevoiți să se confrunte cu o situație în care trebuie să aleagă între următoarele opțiuni:

- a) să continue să utilizeze comunicațiile electronice și serviciile cloud pe care le folosește publicul larg, știind că își încalcă obligația față de clienți de a păstra confidențialitatea informațiilor și, după ce atrag atenția asupra riscurilor, solicită pur și simplu, consimțământul informat al clienților pentru expunerea la astfel de riscuri; sau
- b) să utilizeze serviciile de comunicații electronice, disponibile datorită noilor investiții în construirea unui internet "exclusiv UE", complet separat, cu gateway-uri stricte care să pună în aplicare toate politicile stricte etc. și, astfel, să reconstruiască încrederea la nivelul UE – acceptând, în același timp, și ineficiența unor astfel de soluții, de exemplu costurile de reconstrucție; sau
- c) să nu utilizeze serviciile de e-mail, comunicații electronice sau cloud pentru comunicările cu clienții, să facă schimb de date doar prin intermediul unor suporturi de

date fizice, cum ar fi unitățile flash, sau utilizeze mașini de scris și servicii de expediere poștală și expresă.

Este evident că niciuna dintre alternativele de mai sus nu este realistă în practică și că această situație este complet inacceptabilă într-o societate democratică bazată pe statul de drept.

Acest lucru, la rândul său, va avea repercusiuni și asupra viitorului Agendei digitale pentru Europa, al cărei principal obiectiv este să ajute cetățenii și întreprinderile europene să valorifice la maxim tehnologiile digitale. Cu toate acestea, după cum se indică în Agenda digitală pentru Europa, "europenii nu vor adopta o tehnologie în care nu au încredere – epoca digitală nu este nici "Big Brother", nici "Vestul sălbatic cibernetic"⁴. Așa cum am arătat mai sus, acesta este un fapt semnificativ în cazul avocaților. Atâta timp cât secretul profesional dintre avocați și clienți nu poate fi garantat, furnizarea eficientă de servicii juridice va fi grav subminată. Având în vedere relația importantă dintre serviciile juridice și performanța economică - care rezultă din rolurile pe care serviciile juridice le joacă în facilitarea și susținerea piețelor - această situație va avea un impact negativ asupra economiei europene.⁵

Reconstruirea încrederii

Pe baza informațiilor recent dezvăluite privind practica unor agenții de supraveghere de stat, a devenit îngrijorător faptul că protecția oferită de măsurile legale ale statelor UE pentru păstrarea secretului profesional ar putea să nu fi funcționat în practică și ar fi putut exista cazuri în care statele membre ale UE au permis supravegherea electronică asupra propriilor resortisanți, încălcând propriile reguli naționale.

În plus, dacă într-un stat membru al UE se solicită prin lege un ordin judecătoresc pentru accesul la informații confidențiale deținute de avocați din altă țară, această condiție nu poate fi îndeplinită dacă instanța emitentă este stabilită prin definiție într-o țară străină, fără posibilitatea supravegherii de către un judecător din țara în care locuiește avocatul. În mod similar, motivele de securitate națională ale unui alt stat, fie că este vorba de UE sau nu, nu vor fi neapărat justificate ca motive de securitate națională în propriul stat membru și agențiile de securitate națională ale unui stat membru UE nu ar trebui să coopereze pentru o astfel de supraveghere fără respectarea normelor naționale privind secretul profesional.

⁴ Comunicarea Comisiei, o Agendă digitală pentru Europa, pagina 16, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CQM:2010:0245:FIN:EN:PDF>.

⁵ A se vedea Prof. George Yarrow și Dr. Christopher Decker, Institutul de Politici de Reglementare, Evaluarea semnificației economice a sectorului serviciilor juridice profesionale în Uniunea Europeană, august 2012. La pagina 3, se subliniază că "O relație deosebit de importantă între serviciile juridice și performanța economică provine din rolurile pe care serviciile juridice le joacă în facilitarea și susținerea piețelor. Activitatea principală a sectorului serviciilor juridice profesionale tinde să extindă activitatea pe piață în întreaga economie și, prin urmare, este strâns legată de performanța și de creșterea economică.



Recunoscând necesitatea ca organele guvernamentale în domeniul aplicării legii și securității naționale să efectueze supravegherea electronică a cetățenilor în anumite circumstanțe limitate, problema pierderii încrederii nu poate fi rezolvată decât prin mijloace politice: de exemplu, analizând cu atenție care sunt domeniile de supraveghere secretă care nu trebuie făcute publice și, corelativ, dacă participarea civică (inclusiv prin intermediul reprezentanților profesiei de avocat) ar putea fi utilă pentru redobândirea și menținerea încrederii publicului.

Recomandări

1. Referindu-se la poziția CCBE (adoptată la data de 7/9/2012) referitoare la pachetul de reforme propus privind protecția datelor, CCBE consideră că obligațiile autorităților de aplicare a legii privind protecția datelor cu caracter personal și a oricăror alte date care fac obiectul secretului profesional ar trebui să fie cel puțin la fel de extinse ca nivelul de protecție așteptată de la entitățile care controlează datele în sfera privată. Acest fapt consolidează necesitatea existenței unui regim unic și cuprinzător de protecție a datelor.
2. În plus, trebuie luate măsuri la nivelul UE pentru a stabili nivelul minim de protecție juridică acordată secretului profesional în cadrul supravegherii electronice guvernamentale, inclusiv utilizarea serviciilor de comunicații electronice sau a altui serviciu cloud pentru comunicările avocat-client. Utilizarea în relația avocat-client a acestor facilități ar trebui să fie protejată în același mod, indiferent dacă sunt stocate într-un centru de date sau într-un computer la cabinetul de avocatură sau personal. Conținutul care presupune un secret profesional și care este procesat de un serviciu de comunicații electronice sau de un furnizor de servicii cloud (inclusiv un furnizor de servicii de e-mail) nu trebuie să fie accesibil agențiilor guvernamentale. Furnizorii de servicii de comunicații electronice și de servicii de cloud ar trebui să fie obligați să ofere avocaților o opțiune de indicare a acestor informații - desigur, numai după o verificare atentă a faptului că utilizatorul respectiv este într-adevăr avocat, așa cum a pretins.
3. Trebuie stabilite standarde minime ale UE pentru supravegherea electronică, inclusiv necesitatea de a stabili limite rezonabile pentru invocarea securității naționale ca motiv pentru restrângerea dreptului la viață privată. Această activitate de reglementare trebuie să se bazeze pe rapoartele și sugestiile deja elaborate la nivel regional și internațional cu privire la acest subiect, de exemplu raportul lui Frank La Rue, raportor special al Consiliului pentru Drepturile Omului al Națiunilor Unite (a se vedea acest link) sau proiectul de raport al Comitetului Adunării Parlamentare a Consiliului Europei, "Compilație de bune practici privind cadrele juridice și instituționale și măsurile care

Traducere din limba engleză

asigură respectarea drepturilor omului de către agențiile de informații, în contextul combaterii terorismului, inclusiv supravegherea acestora" (a se vedea acest link).

4. UE trebuie să depună eforturi pentru consolidarea dreptului la confidențialitate la nivel internațional, de ex. pe baza protocoalelor opționale la articolul 17 din Pactul internațional privind drepturile civile și politice și prin consolidarea nivelului de protecție garantat în practică de principiile de confidențialitate "port sigur". În ceea ce privește țările europene din afara Spațiului Economic European, în cadrul procesului de modernizare în curs al convenției, UE trebuie să sprijine adoptarea unor excepții mai specifice și detaliate în temeiul articolului 9 din Convenția 108 pentru protecția persoanelor cu privire la prelucrarea automată a datelor cu caracter personal.
5. Dincolo de toate măsurile de protecție necesare care pot fi obținute prin mijloace politice și legislative, trebuie luate măsuri tehnice și pentru a reconstrui încrederea în serviciile de comunicații electronice și cloud. Măsurile tehnice care vizează îmbunătățirea siguranței internetului și a cloud computing-ului și accesul guvernamental supus mai mult controlului juridic trebuie, de asemenea, să țină seama de cerințele specifice care trebuie îndeplinite în ceea ce privește informațiile care fac obiectul obligațiilor privind secretul profesional și regulile privind privilegiul profesional juridic, în relația avocat-client. Cu alte cuvinte, infrastructurile de comunicații electronice și de servicii cloud trebuie să fie construite și în cazul în care funcționalitățile tehnice garantează că tehnologiile backdoors nu sunt folosite abuziv de guverne sau de terți.

Concluzie

Prin urmare, CCBE îndeamnă instituțiile UE să creeze cadrul juridic și tehnologic necesar pentru a remedia situația actuală în ceea ce privește supravegherea electronică în masă și pentru a proteja secretul profesional, care este un drept al tuturor cetățenilor UE și una dintre valorile fundamentale ale profesiei de avocat.

Traducere din limba engleză

ANEXĂ: Declarația CCBE privind practicile guvernamentale care implică exploatarea în masă a datelor în scopul supravegherii - 1 iulie 2013



Traducere din limba engleză

Logo

CCBE

Conseil des barreaux européens
Council of Bars and Law Societies of Europe
Association internationale sans but lucratif

Rue Joseph II, 40 / 8 - 1000 Bruxelles T. : +32 (0)2 234 65 10 - F. : +32 (0)2 234 65 11 Email : ccbe@ccbe.eu - www.ccbe.eu

Declarația CCBE privind practicile guvernamentale care implică exploatarea în masă a datelor în scopul supravegherii

01/07/2013

Consiliul Barourilor și Societăților de Drept din Europa (CCBE) reprezintă barourile și societățile de avocatură din 32 de țări membre și 11 țări asociate și observatoare, și prin intermediul acestora, peste 1 milion de avocați europeni.

CCBE a observat cu mare îngrijorare dezvăluirile recente ale practicilor guvernamentale care implică exploatarea în masă a datelor în scopul supravegherii.

CCBE a subliniat în repetate rânduri importanța secretului profesional (cunoscută în unele țări drept privilegiul profesional juridic) și ar dori să sublinieze că însăși Curtea Europeană de Justiție a declarat expres în decizia sa în cauza AM&S (cauza C-155/79) că: "confidențialitatea îndeplinește cerințele, a căror importanță este recunoscută în toate statele membre, ca orice persoană să aibă posibilitatea, fără constrângere, să consulte un avocat a cărui profesie implică acordarea de consultanță juridică independentă tuturor celor care au nevoie de ea" și a adăugat că "principiul protecției împotriva divulgării comunicărilor scrise între avocat și client se bazează, în principal, pe recunoașterea însăși a profesiei de avocat, în măsura în care contribuie la menținerea statului de drept și că dreptul la apărare trebuie respectat".

Acastă valoare de bază a profesiei de avocat este totuși atacată de organizații cu capacități tehnice extrem de sofisticate și mijloace financiare, inclusiv organisme de stat având puteri secrete de investigare.

Avocații nu au altă soluție decât să folosească tehnologia modernă atunci când comunică cu clienții, instanțele, colegii avocați și alte persoane. Totuși, acum se pare că o astfel de tehnologie nu poate fi utilizată în siguranță.

Eroziunea confidențialității comunicărilor dintre avocați și clienți afectează și încrederea cetățenilor în statul de drept.

Prin urmare, CCBE solicită instituțiilor UE să ia măsuri pentru protejarea și sporirea confidențialității comunicărilor avocat-client atunci când se utilizează tehnologii moderne. Astfel



Traducere din limba engleză

de măsuri ar putea include activități în domeniul standardizării tehnice (de exemplu, posibilitatea de a constitui un cont de avocat care să facă obiectul unei protecții mai mari împotriva exploatarei datelor) sau în domeniul instrumentelor de drept internațional.