Perspectivele evoluţiei legislative la nivelul Uniunii Europene şi în plan naţional în ceea ce priveşte secretul profesional şi confidenţialitatea comunicărilor dintre avocat şi client. Preocupări actuale privind secretul profesional în cadrul profesiei de avocat în România.

Av. dr. Florea Gheorghe

Dispoziţiile legii 82/2012 privind reţinerea datelor generate sau prelucrate de furnizorii de reţele publice de comunicaţii electronice şi de furnizorii de servicii de comunicaţii electronice destinate publicului, precum şi pentru modificarea şi completarea legii 506/2004 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul comunicaţiilor electronice au fost declarate neconstituţionale.

Legea, cunoscută în spaţiul public sub denumirea *Legea „Big Brother*" se referă la obligaţia operatorilor/furnizorilor din reţelele publice/ sfera serviciilor de comunicaţii electronice de a reţine timp de 6 luni date despre comunicaţiile telefonice sau electronice ale abonaţilor. Aceste date nu privesc conţinutul comunicaţiilor, ci sunt doar date tehnice care stabilesc identităţile celor care comunică, timpii în care are loc comunicaţia, locaţia, etc.. Datele reţinute sunt puse la dispoziţia organelor de cercetare penală, cu încuviinţarea unui judecător.

Decizia Curţii Constituţionale a avut în vedere că în aprilie 2014 Curtea Europeană de Justiţie a decis că Directiva 24/2006 privind reţinerea datelor din comunicaţiile electronice (*efectuate prin telefon sau prin internet*) nu respectă legislaţia europeană.

Principala concluzie a Curţii de Justiţie a Uniunii Europene (răspunzând unor sesizări făcute de Austria şi Irlanda) a fost că Directiva privind Reţinerea Datelor presupune o imixtiune „*amplă şi deosebit de îngrijorătoare*" în drepturile fundamentale la protejarea vieţii private şi la confidenţialitatea datelor cu caracter personal, *„fără ca această imixtiune să se limiteze la ceea ce este strict necesar".*

Curtea de Justiţie a concluzionat că, impunând stocarea datelor din telecom şi permiţând statelor membre să acceseze aceste date, Directiva încalcă mai multe drepturi fundamentale ale omului.

Problema esenţială în conflictul dintre interesul general şi interesul personal în conflictul identificat de Curte este *„proporţionalitatea (între scop şi mijlloace)",* care se referă la raportul dintre nevoia de a putea folosi date de identificare din telecom pentru anchete penale, pe de-o parte, şi felul în care sunt stocate şi folosite aceste date, pe de altă parte, astfel încât să respecte şi drepturile abonaţilor.

Curtea a recunoscut principiul stocării datelor şi legitimitatea lui pentru asigurarea securităţii cetăţenilor europeni, dar a decis că mijloacele prin care ea a fost implementată sunt abuzive şi ilegale şi că e nevoie de măsuri concrete pentru a o rescrie astfel încât să fie eliminate problemele

Unul dintre motivele pentru care legea a fost declarată neconstituţională este că nu a respectat articolele 7 şi 8 din Carta Drepturilor Fundamentale a Uniunii Europene.

Articolul 7 se referă la „respectarea vieţii private şi de familie" şi statuează că **„***orice persoană are dreptul la respectarea vieţii private şi de familie, a domiciliului şi a secretului comunicaţiilor*". Articolul 8 se referă la „protecţia datelor cu caracter personal" şi stabileşte că *„orice persoană are dreptul la protecţia datelor cu caracter personal care o privesc*".

S-a stabilit că *„asemenea date trebuie tratate în mod corect, în scopurile precizate şi pe baza consimţământului 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 şi dreptul de a obţine rectificarea acestora*" şi că *„respectarea acestor norme se supune controlului unei autorităţi independente".*

Printre problemele identificate de Curte sunt enumerate: posibilitatea stabilirii identităţii unei persoane cu care abonatul sau utilizatorul comunică şi mijloacele de comunicare; identificarea momentului şi locului comunicării, precum şi a frecvenţei ei între un utilizator sau abonat şi o altă persoană. *„Luate împreună, aceste date pot oferi informaţii foarte exacte despre viaţa personală a persoanelor ale căror date sunt stocate, cum ar fi obiceiurile de zi cu zi, locurile permanente sau temporare de rezidenţă (...), activităţile desfăşurate, interacţiunile sociale şi mediile frecventate*".

Interese generale impun intervenţia legiuitorului român pentru a se realiza obiectivele vizate de politica europeană în domeniu, ceea ce impune obligaţia de a veghea la realizarea unei legislaţii sănătoase, care să ofere garanţii şi mijloace de apărare a drepturilor şi intereselor în conflict.

Cunoaşterea reglementărilor şi proiectelor europene, evaluarea contextului actual şi a perspectivelor evoluţiei legislative în plan naţional, evocarea recomandărilor Consiliului Barourilor si a Societăţilor de Drept din Europa (în continuare CCBE) sunt imperios necesare în condiţiile în care dispoziţiile art. 11, art. 35 şi art. 36 din Legea nr. 51/1995 pentru organizarea şi exercitarea profesiei de avocat (în continuare *Legea*), prevederile art. 8 şi 9 din Statutul profesiei de avocat se impun a fi raportate la prevederile noului Cod de procedura penală, la prevederile legale privind secretul fiscal şi la cele privind secretul bancar. Legea nr. 656 din 7 decembrie 2002 pentru prevenirea şi sancţionarea spălării banilor, precum şi pentru instituirea unor măsuri de prevenire şi combatere a finanţării terorismului se aplică în România, în ceea ce priveşte avocaţii, în condiţiile Protocolului nr. 8136 / 07.11.2005 – 637/05.11.2005 încheiat între Oficiul Naţional de Prevenire şi Combatere a Spălării Banilor şi Uniunea Naţională a Barourilor din România, în care datele şi informaţiile furnizate sunt confidenţiale şi păstrează categoria de clasificare atribuită conform Legii nr. 182 / 2002 privind protecţia informaţiilor clasificate.

Sunt luate măsuri privind protecţia secretului profesional. Perspectiva obligă comunitatea profesională a avocaţilor să vegheze ca astfel de măsuri să fie consecvente şi aplicate cu rigoare.

I. Reglementările şi proiectele europene care vor avea impact în legislaţia naţională în ceea ce priveşte protecţia vieţii private împotriva supravegherii electronice în masă

Adâncirea frământărilor privind securitatea europeană în paralel cu dezvăluirile lui Edward Snowden cu privire la amploarea acţiunilor de supraveghere în masă asupra cetăţenilor au readus în prim plan problemele legate de dezechilibrul produs între reglementările privind protecţia vieţii private şi cele privind combaterea terorismului şi a criminalităţii. Acestea din urmă sunt priorităţi absolute pentru majoritatea guvernelor. Garanţiile respectării unor drepturi fundamentale, în special ale dreptului la viaţă privată, s-au atenuat în faţa avalanşei de reglementări care permit accesul serviciilor de informaţii la date personale, chiar fără o autorizare prealabilă din partea unei instanţe, ajungându-se ca fiecare cetăţean să poată fi tratat ca suspect şi să fie supravegheat.

Aceste aspecte i-au obligat pe liderii politici să abordeze provocările legate de supravegherea şi controlul serviciilor de informaţii şi să evalueze impactului acestor activităţi asupra drepturilor fundamentale şi asupra statului de drept. De aceea, la nivelul Uniunii Europene, se petrec reforme profunde în contextul reglementărilor privind protecţia datelor şi a vieţii private în paralel cu cea privind retenţia datelor şi accesul la acestea. Deşi modificarea acestor reglementări constituie priorităţi ale Comisiei Europene şi ale Parlamentului European, procesul legislativ înaintează dificil dată fiind complexitatea problematicii amplificate continuu de noi evenimente şi noi provocări legate de tehnologie, care generează necesitatea unor soluţii noi.

Pentru a înţelege ce se întâmplă în plan european şi în plan naţional sub aspectul reglementărilor privind protecţia datelor personale privitor la stocarea şi accesul la date trebuie să ne raportăm la contextul european şi cel global întrucât suntem din ce în ce mai interconectaţi nu numai ca stat membru UE dar şi la nivelul comunicaţiilor electronice. Orice eveniment major petrecut în lume are reverberaţii legislative în România. Nu mai putem vorbi de context legislativ naţional rupt de cel European şi global, deoarece transmiterea informaţiilor în mediul virtual creează ambiguităţi fără precedent în legătură cu principiul teritorialităţii aplicării legii. În ultima vreme sunt din ce în ce mai multe iniţiative de armonizare a legislaţiei europene la nivel transatlantic şi toate procedurile legislative europene legate de reglementările în domeniul datelor au implicat şi implică negocieri şi acorduri cu Statele Unite ale Americii.

Conform Rezoluţiei Parlamentului European din 12 martie 2014 referitoare la programul de supraveghere al Agenţiei Naţionale de Securitate (NSA) a Statele Unite ale Americii, la organismele de supraveghere din diferite state membre şi la impactul acestora asupra drepturilor fundamentale ale cetăţenilor UE şi asupra cooperării transatlantice în materie de justiţie şi de afaceri interne dezvăluirile făcute începând din iunie 2013 au cauzat numeroase îngrijorări la nivelul UE în legătură cu:

– amploarea sistemelor de supraveghere făcute cunoscute atât în SUA, cât şi în statele membre ale UE;

– încălcarea standardelor juridice, a drepturilor fundamentale şi a standardelor în materie de protecţie a datelor din UE;

– nivelul de încredere dintre UE şi SUA în calitate de parteneri transatlantici;

– gradul de cooperare şi de implicare al unor state membre ale UE în programele de supraveghere ale SUA sau în programe echivalente de la nivel naţional conform dezvăluirilor din mass-media;

– lipsa controlului şi a supravegherii efective exercitate de autorităţile politice americane şi de unele state membre ale UE asupra serviciilor lor de informaţii;

– posibilitatea ca aceste acţiuni de supraveghere în masă să fie utilizate pentru alte motive decât securitatea naţională şi lupta împotriva terorismului în sensul strict al cuvântului, ca de exemplu pentru spionaj economic şi industrial sau pentru stabilirea de profiluri pe motive politice;

– subminarea libertăţii presei şi a comunicaţiilor dintre membrii anumitor profesii care se bucură de privilegiul confidenţialităţii, cum sunt, printre alţii, avocaţii şi medicii;

– rolurile serviciilor de informaţii şi ale companiilor private din domeniul IT şi al comunicaţiilor, precum şi gradul de implicare al acestora;

– liniile de demarcare din ce în ce mai neclare dintre aplicarea legii şi activităţile de spionaj, care fac ca fiecare cetăţean să fie tratat ca suspect şi să fie supravegheat;

– ameninţările la adresa vieţii private în era digitală şi impactul supravegherii de masă asupra cetăţenilor şi a societăţii;

Avem convingerea că pe măsură ce avansează tehnologia, acestea se vor extinde la nivel mondial întrucât odată cu avansarea societăţii digitale, s-a dovedit de nenumărate ori că orice eveniment petrecut în orice colţ al lumii produce turbulenţe în sistemul legislative european, bineînţeles cu reverberaţii şi în România.

În acest context este necesară cunoaşterea de către autorităţile publice şi de avocaţi a principalelor reglementări şi proceduri legislative europene aflate în derulare în domeniul datelor şi incidenţa acestora asupra legislaţiei naţionale, cu evidenţierea poziţiilor legislative şi a prevederi speciale la nivel UE în ceea ce priveşte secretul profesional şi confidenţialitatea comunicărilor avocat client. Noi, avocaţii, avem datoria să clarificăm şi să impunem cu mai multă forţă principiul confidenţialităţii comunicărilor între avocat şi client în viitoarele reglementări, ca o condiţie esenţială a înfăptuirii justiţiei într-un stat de drept.

*

La 12 martie 2014 Parlamentul European a adoptat Rezoluţia referitoare la programul de supraveghere al Agenţiei Naţionale de Securitate (NSA) a SUA, la organismele de supraveghere din diferite state membre şi la impactul acestora asupra drepturilor fundamentale ale cetăţenilor UE şi asupra cooperării transatlantice în materie de justiţie şi de afaceri interne (2013/2188(INI))

Rezoluţia oferă o perspectivă clară în ceea ce priveşte viitoarele reglementări menite să asigure protecţia vieţii private împotriva supravegherii în masă, dar mai ales dă indicaţii exprese privind abordarea principiului confidenţialităţii comunicărilor dintre avocat şi client în cadrul acestora. Rezoluţia dă detalii asupra planului de acţiune la nivel European în privinţa reformelor legislative în domeniul datelor.

Se subliniază expres, de mai multe ori, necesitatea protecţiei confidenţialităţii comunicărilor avocat client. Capitolul I al Rezoluţiei, denumit „*Impactul supravegherii în masă*" (litera G, alin. 7) reţine că una dintre principalele îngrijorări la nivel UE în urma dezvăluirilor făcute de Snowden începând din iunie 2013 este „**subminarea libertăţii presei** şi a **comunicaţiilor dintre membrii anumitor profesii care se bucură de privilegiul confidenţialităţii, cum sunt, printre alţii, avocaţii** şi medicii"

În capitolul „Constatări principale" (punctul 11) se prevede expres că Parlamentul European „**consideră esenţială protejarea privilegiului secretului profesional al avocaţilor**, jurnaliştilor, medicilor şi al altor persoane care exercită profesii reglementate de activităţile de supraveghere în masă; **subliniază în special că orice incertitudini legate de confidenţialitatea informaţiilor comunicate în cadrul relaţiei dintre avocat şi client ar putea avea un impact negativ asupra dreptului cetăţenilor la consiliere juridică, asupra accesului la justiţie şi asupra dreptului la un proces echitabil"**

Planul de priorităţi al Parlamentului European este calificat în Rezoluţie drept „Un **habeas corpus digital european** - **protejarea drepturilor fundamentale în era digitală**". Este vitală **necesitatea protecţiei dreptului publicului de a primi informaţii imparţiale şi respectarea confidenţialităţii profesionale, inclusiv în relaţia avocat-client** (punctul 132, Acţiunea 6 din Rezoluţie).

Rezoluţia prevede că acest „habeas corpus digital european” include opt acţiuni, iar prin punerea în aplicare a actului ce le va sintetiza se va asigura:

– Acţiunea 1: adoptarea pachetului de măsuri privind protecţia datelor în 2014;

– Acţiunea 2: încheierea acordului-cadru între UE şi SUA care să garanteze dreptul fundamental al cetăţenilor la viaţă privată şi la protecţia datelor şi să asigure căi de atac adecvate pentru cetăţenii UE, inclusiv în cazuri de transfer de date din UE în SUA în scopuri de aplicare a legii;

– Acţiunea 3: suspendarea „sferei de siguranţă” până la finalizarea unei analize complete şi remedierea actualelor lacune, asigurându-se că transferurile de date cu caracter personal în scopuri comerciale din Uniune în SUA pot fi efectuate doar în conformitate cu cele mai ridicate standarde ale UE;

– Acţiunea 4: suspendarea acordului TFTP (Programul de urmărire a finanţărilor în scopuri teroriste) până la (i) finalizarea negocierilor privind acordul-cadru; (ii) finalizarea unei investigaţii detaliate bazate pe o analiză a UE şi abordarea adecvată a tuturor preocupărilor menţionate de Parlament în Rezoluţia sa din 23 octombrie 2013;

– Acţiunea 5: evaluarea oricărui acord, mecanism sau schimb cu ţări terţe care implică date cu caracter personal, cu scopul de a se asigura că dreptul la viaţă privată şi la protecţia datelor cu caracter personal nu este încălcat ca urmare a activităţilor de supraveghere, precum şi luarea măsurilor de monitorizare necesare;

– Acţiunea 6: protejarea statului de drept şi a drepturilor fundamentale ale cetăţenilor UE (inclusiv împotriva ameninţărilor la adresa libertăţii presei), **a dreptului publicului de a primi informaţii imparţiale şi a confidenţialităţii profesionale (inclusiv în relaţia avocat-client),** precum şi asigurarea unei protecţii sporite a denunţătorilor;

– Acţiunea 7: elaborarea unei strategii europene privind independenţa informatică sporită (un „Nou acord digital – New Deal”, inclusiv alocarea resurselor adecvate la nivel naţional şi la nivelul UE) pentru dezvoltarea industriei informatice şi pentru a permite întreprinderilor europene să exploateze avantajul concurenţial al vieţii private;

– Acţiunea 8: evoluţia UE ca jucător de referinţă cu privire la guvernanţa democratică şi neutră a internetului;

La finalul Rezoluţiei (punctul 133) Parlamentul European invită instituţiile UE şi statele membre să promoveze habeas corpusul digital european care protejează drepturile fundamentale în era digitală; îşi ia angajamentul de a acţiona ca susţinător al drepturilor cetăţenilor UE, conform următorului **calendar de monitorizare a punerii în aplicare:**

– un grup de monitorizare bazat pe o echipă de anchetă a Comisiei pentru libertăţi civile, justiţie şi afaceri interne a Parlamentului European, responsabil de monitorizarea oricăror noi dezvăluiri referitoare la mandatul anchetei şi controlul punerii în aplicare a acestei rezoluţii urma să îşi desfăşoare activitatea în perioada aprilie 2013 - martie 2015;

– începând din iulie 2014 s-a aplicat un mecanism de supraveghere durabil pentru transferurile de date şi căile de atac din cadrul comisiei competente;

– în primăvara anului 2014 s-a înregistrat o solicitare formală adresată Consiliului European de a include „Habeas corpusul digital european - protejarea drepturilor fundamentale în era digitală”

în orientările care urmează să fie adoptate în temeiul articolului 68 din Tratatul pentru Funcţionarea Uniunii Europene;

– în toamna anului 2014 s-a dat publicităţii un angajament potrivit căruia „Habeas corpusul digital european - protejarea drepturilor fundamentale în era digitală" alături de recomandările aferente vor servi ca un criteriu-cheie pentru aprobarea lucrărilor finale ale următoarei Comisii Europene;

– în 2014 s-a preconizat o conferinţă care să reunească experţi europeni de nivel înalt în diferite domenii care concură la securitatea informatică (inclusiv matematică, criptografie şi tehnologiile de consolidare a confidenţialităţii) pentru a ajuta la stimularea unei strategii informatice a UE pentru următoarea legislatură;

– în 2014-2015 a fost planificată o reunire regulată unui grup pe tema încredere/date/drepturile cetăţenilor între Parlamentul European şi Congresul SUA, precum şi cu alte parlamente implicate ale ţărilor terţe, inclusiv Brazilia;

– pentru 2014-2015 este preconizată o conferinţă cu organismele de supraveghere a serviciilor de informaţii ale parlamentelor naţionale europene;

Potrivit punctului 131 din Rezoluţie, Parlamentul European hotărăşte să prezinte cetăţenilor şi instituţiilor UE, precum şi statelor membre, recomandările enumerate sub forma unui Plan de priorităţi pentru viitoarea legislatură; invită Comisia şi celelalte instituţii, organisme, oficii şi agenţii ale UE menţionate în prezenta rezoluţie, în conformitate cu articolul 265 din TFUE, să dea curs recomandărilor şi solicitărilor din această rezoluţie;

A intervenit Decizia Curţii de Justiţie a Uniunii Europene din 8 aprilie 2014 prin care se anulează Directiva 2006/24/EC privind reţinerea datelor - HOTĂRÂREA CJUE (Marea Cameră) din 8 aprilie 2014 în cauzele conexate C‑293/12 şi C‑594/12

Directiva a fost declarată nevalidă deoarece nu respectă principiul proporţionalităţii (ca principiu general de drept european) deoarece ar fi trebuit să prevadă mai multe garanţii pentru a proteja drepturile fundamentale la respectarea vieţii private şi la protecţia datelor cu caracter personal. Pe de altă parte, Curtea a considerat că păstrarea datelor serveşte, în condiţii clare şi precise, un interes legitim şi general, şi anume lupta împotriva formelor grave de criminalitate şi de protecţie a siguranţei publice.

În condiţiile în care Curtea declară că retenţia datelor corespunde unui scop legitim, ne putem aştepta curând la o nouă propunere de directivă privind reţinerea şi stocarea datelor. Criticile la adresa Directivei 2006/24/EC sunt reflectate în cuprinsul Deciziei CJUE. Principalele aspecte de neconformare a Directivei cu principiile fundamentale ale dreptului european, ca răspuns la aceste critici, ne pun în temă cu dispoziţiile pe care ar trebui să le conţină noua reglementare.

Criticile sunt în principal următoarele:

- În Directivă se făcea doar o trimitere generală la infracţiunile grave fără să prevadă un criteriu obiectiv care să permită delimitarea accesului autorităţilor naţionale competente la date şi utilizarea lor ulterioară în scopul prevenirii, detectării sau urmăririi penale în legătură cu infracţiuni care, având în vedere amploarea şi gravitatea ingerinţei în drepturile fundamentale consacrate la articolele 7 şi 8 din Carta Europeană a Drepturilor Omului, pot fi considerate ca fiind suficient de grave pentru a justifica o astfel de ingerinţă;

- Directiva 2006/24 nu prevede în mod expres că accesul la datele reţinute şi utilizarea ulterioară a datelor în cauză trebuie să fie restricţionate în mod strict la scopul prevenirii şi al detectării infracţiunilor delimitate precis sau al desfăşurării urmăririi penale aferente acestora, ci se limitează să prevadă că fiecare stat membru defineşte procedurile care trebuie să fie urmate şi condiţiile care trebuie să fie îndeplinite pentru a obţine acces la datele păstrate în conformitate cu cerinţele de necesitate şi proporţionalitate;
- Directiva 2006/24 nu prevede niciun criteriu obiectiv care să permită limitarea numărului de persoane ce dispun de autorizaţia de acces şi de utilizare ulterioară a datelor păstrate la strictul necesar în lumina obiectivului urmărit. Mai ales, **accesul la datele păstrate de autorităţile naţionale competente nu este condiţionat de un control prealabil efectuat fie de o instanţă, fie de o entitate administrativă independentă prin a căror decizie se urmăreşte limitarea accesului la date şi a utilizării lor la ceea ce este strict necesar în vederea atingerii obiectivului urmărit şi care este adoptată în urma unei cereri motivate a acestor autorităţi formulate în cadrul procedurilor de prevenire, de detectare sau de urmărire penală. În directivă nu s-a prevăzut nici o obligaţie precisă a statelor membre privind stabilirea unor astfel de limitări.**

Trebuie să ne aşteptăm ca în anul următor să fie supus consultării publice un nou proiect de directivă privind reţinerea şi stocarea datelor, care va avea în centrul dezbaterilor următoarele aspecte:

- configurarea unui criteriu obiectiv care să permită delimitarea accesului autorităţilor naţionale competente la date şi utilizarea lor ulterioară;
- găsirea unor soluţii legale pentru restricţionarea în mod strict a accesului la date la scopul prevenirii şi al detectării infracţiunilor delimitate precis;
- condiţionarea accesului la datele păstrate de autorităţile naţionale competente de un control prealabil efectuat fie de o instanţă, fie de o entitate administrativă independentă.

Având în vedere rolul avocatului în apărarea drepturilor şi a libertăţilor fundamentale şi în înfăptuirea statului de drept, avocaţii europeni, inclusiv cei din România sunt datori să-şi aducă aportul în timpul consultărilor publice care vor urma, astfel încât să fie identificate noi garanţii ale respectării drepturilor fundamentale şi să fie găsit echilibrul între dispoziţiile care apără dreptul la siguranţă al cetăţenilor europeni şi dreptul lor la viaţă private. Este o misiune extreme de dificilă, însă face parte din îndatoririle noastre ca avocaţi şi respectarea jurământului pe care l-am depus la intrarea în profesie, să apărăm statul de drept şi drepturile şi libertăţile fundamentale ale cetăţenilor.

În 2012, Comisia Europeană a propus o reformă majoră a legislaţiei protecţiei datelor, publicând Propunerea de Directivă a Parlamentului European şi a Consiliului privind protecţia persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autorităţile competente în scopul prevenirii, identificării, investigării sau urmăririi penale a infracţiunilor sau al executării pedepselor şi la libera circulaţie a acestor date

Iniţial pachetul de reformă a legislaţiei privind protecţia datelor avea termen de finalizare în 2014. Termenul s-a prelungit pentru 2015 din cauza noilor probleme care s-au ivit pe parcurs, generate de dezvăluirile legate de supravegherea în masă şi de evoluţia accelerată a tehnologiilor care devansează continuu procesul legislativ.
Evoluţia proiectului de Directivă este sinuoasă.

La 25 ianuarie 2012, Comisia a adoptat un pachet de reformă a normelor UE privind protecţia datelor, inclusiv o propunere de regulament conţinând normele generale privind protecţia datelor şi o propunere de directivă privind protecţia datelor în domeniul aplicării legii.
La 7 martie 2012, Autoritatea Europeană pentru Protecţia Datelor (AEPD) a adoptat un aviz care conţine observaţii detaliate pe marginea ambelor propuneri legislative. Deşi AEPD salută propunerea de regulament, deoarece aceasta constituie un uriaş pas înainte pentru protecţia datelor în Europa, pe de altă parte, îşi exprimă profunda dezamăgire în legătură cu propunerea de directivă privind protecţia datelor în domeniul aplicării legii. AEPD regretă alegerea Comisiei de a reglementa acest aspect prin intermediul unui instrument legislativ autonom care prevede un nivel inadecvat de protecţie şi care este mult inferior faţă de propunerea de regulament.
Dată fiind complexitatea problemelor, reglementările în acest domeniu avansează greu, iar pe parcursul procedurilor legislative apar mereu alte probleme.
Referitor la propunerea de Directivă pe 12 martie 2014 aceasta a primit avizul Parlamentului European în primă lectură şi de atunci nu a mai avansat în proceduri.
A fost adoptată Rezoluţia legislativă a Parlamentului European din 12 martie 2014 referitoare la propunerea de Regulament al Parlamentului European şi al Consiliului privind protecţia persoanelor fizice referitor la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date (denumit *Regulament general privind protecţia datelor*), la care s-au făcut deja o serie de amendamente.

Mai sunt mulţi paşi de făcut până când propunerea va deveni Directivă, aceasta fiind deocamdată blocată în controverse. Pe parcurs vor fi invocate cu necesitate şi se va impune susţinerea si examinarea unor amendamente. De exemplu, „***reglementarea dreptului de a fi uitat***", ca urmare a Deciziei Curţii de Justiţie a Uniunii Europene în cauza Gonzales vs Google din 13 mai 2014, potrivit căreia operatorul unui motor de căutare pe internet răspunde pentru prelucrarea pe care o efectuează în ceea ce priveşte datele cu caracter personal care apar pe pagini web publicate de terţi. Astfel, în cazul în care, ca urmare a unei căutări efectuate plecând de la numele unei persoane, lista de rezultate afişează un link către o pagină web care conţine informaţii referitoare la această persoană, persoana vizată se poate adresa direct operatorului sau, dacă acesta nu dă curs cererii sale, poate sesiza autorităţile competente pentru a obţine, în anumite condiţii, eliminarea acestui link de pe lista de rezultate.
Le 10.10.2014 au avut loc dezbateri în Consiliu cu privire la propunerea de Directivă, ajungându-se la concluzia că ar fi necesară o nouă analiză de impact asupra protecţiei datelor pentru a evalua, în special, originea, natura, caracterul distinctiv şi gravitatea riscului.

*

Evoluţia accelerată a tehnologiei aduce continuu noi probleme în demersurile legislative, care datorită procedurilor pe care trebuie să le urmeze nu pot ţine pasul cu inventivitatea informatică.

Apar probleme şi pentru că prin apariţia sistemelor de cloud computing, operatorii de date personale nu mai sunt stabiliţi în Uniunea Europeană, iar reglementările nu le sunt opozabile.

Propunerea de Regulament privind protecţia datelor în UE conţine, de asemenea, diferite obligaţii impuse companiilor, care vor fi relevante pentru furnizorii de cloud, inclusiv numirea de responsabili cu protecţia datelor, care trebuie să păstreze o evidenţă detaliată a datelor cu caracter personal care sunt colectate şi trebuie realizate evaluări de impact de confidenţialitate.

Există, de asemenea, obligaţia de a pune în aplicare măsuri de securitate tehnice şi organizatorice adecvate şi o cerinţă de a raporta încălcări ale securităţii „fără întârzieri nejustificate". Este ştiut

faptul că avocaţii folosesc din ce în ce mai mult sistemele de cloud computing pentru a partaja informaţii şi documente cu clienţii lor, astfel încât şi din acest punct de vedere intrarea în vigoare a noilor reglementări în domeniul protecţiei datelor vor avea incidenţă direct asupra activităţii lor.

În ceea ce priveşte agenda digitală a Comisiei Europene, în septembrie 2012, Comisia Europeană a adoptat o strategie pentru "Realizarea potenţialului de Cloud Computing din Europa". Conform comunicării Comisiei Europene cu privire la acest demers, strategia anunţată este urmarea propunerii de actualizare a normelor privind protecţia datelor, prezentată de Comisie în 2012, şi precede Strategia europeană pentru securitatea informatică.
În aceeaşi comunicare, se mai arată că "elaborarea acestor norme europene privind cloud computingul constituie o condiţie prealabilă pentru crearea spaţiului digital omogen ce va permite realizarea unei adevărate pieţe unice digitale" şi că "în prezent, din cauza lipsei unor standarde comune şi a unor contracte clare, numeroşi utilizatori potenţiali nu pot adopta soluţii de tip cloud computing deoarece nu sunt siguri ce standarde şi certificate le sunt necesare pentru a răspunde exigenţelor acestora şi pentru a respecta obligaţiile juridice care decurg din aplicarea lor, de exemplu pentru a garanta că propriile date sau cele ale clienţilor lor sunt în siguranţă sau că aplicaţiile sunt interoperabile. De asemenea, furnizorii de servicii de cloud computing şi utilizatorii acestora au nevoie de norme mai clare cu privire la furnizarea acestor servicii; de exemplu, ei trebuie să ştie unde se vor soluţiona litigiile sau în ce mod să se asigure că transferul date şi software de la un furnizor de servicii de cloud computing la altul va fi uşor de realizat".

La 7 februarie 2013, Comisia Europeană a **anunţat Planul UE în domeniul securităţii cibernetice pentru protejarea internetului deschis, a libertăţii online şi a oportunităţilor generate de internet.** Comisia Europeană a publicat, împreună cu Înaltul Reprezentant al Uniunii pentru afaceri externe şi politica de securitate, o strategie în domeniul securităţii cibernetice, precum şi o propunere de directivă a Comisiei privind securitatea reţelelor şi a informaţiei (NIS)., al cărei text a fost adoptat în primă lectură, cu amendamente, de Parlamentul European prin Rezoluţia legislativă a Parlamentului European din 13 martie 2014 referitoare la propunerea de directivă a Parlamentului European şi a Consiliului privind măsuri de asigurare a unui nivel comun ridicat de securitate a reţelelor şi a informaţiei în Uniune
Scopul Directivei este de "a asigura un nivel comun ridicat de securitate a reţelelor şi a informaţiei" şi obligă o serie de companii cheie ale economiei, inclusiv cloud providerii, să-şi securizeze sistemele şi să raporteze cyber incidentele.

S-a adoptat şi Directiva 2013/48/UE a Parlamentului European şi a Consiliului din 22 octombrie 2013 privind dreptul de a avea acces la un avocat în cadrul procedurilor penale şi al procedurilor privind mandatul european de arestare, precum şi dreptul ca o persoană terţă să fie informată în urma privării de libertate şi dreptul de a comunica cu persoane terţe şi cu autorităţi consulare în timpul privării de libertate

Monitorizarea transpunerii în dreptul intern a acestei directive (termen limită de transpunere 27 noiembrie 2016) este extrem de importantă întrucât impune cu forţă respectarea confidenţialităţii avocat client şi detaliază modul în care se poate realiza.
Conform art. 4, intitulat „Confidenţialitate", „Statele membre respectă confidenţialitatea comunicării dintre persoanele suspectate sau acuzate şi avocatul lor în exercitarea dreptului de a avea acces la un avocat prevăzut în prezenta directivă. O astfel de comunicare include întrevederi, corespondenţă, conversaţii telefonice şi alte forme de comunicare permise în temeiul dreptului intern"

Punctul 33 din Preambulul Directivei prevede: „Confidenţialitatea comunicării dintre persoane suspectate sau acuzate şi avocatul lor este esenţială pentru asigurarea exercitării efective a dreptului la apărare şi este o parte esenţială a dreptului la un proces echitabil. Prin urmare, statele membre ar trebui să respecte confidenţialitatea întrevederilor şi a altor forme de comunicare dintre avocat şi persoana suspectată sau acuzată în exercitarea dreptului de a avea acces la un avocat prevăzut în prezenta directivă, fără derogare. Prezenta directivă nu aduce atingere procedurilor care abordează situaţia în care există circumstanţe de fapt şi obiective care determină bănuiala că avocatul este implicat într-o infracţiune alături de persoana suspectată sau acuzată. Orice activitate infracţională a unui avocat ar trebui să nu fie considerată asistenţă legitimă acordată persoanelor suspectate sau acuzate în cadrul prezentei directive. Obligaţia de a respecta confidenţialitatea implică nu numai faptul că statele membre ar trebui să se abţină de la amestecul în această comunicare sau în avea acces la această comunicare, dar şi faptul că, atunci când persoanele suspectate sau acuzate sunt lipsite de libertate sau se găsesc într-un loc aflat sub controlul statului, statele membre ar trebui să garanteze faptul că modalităţile de comunicare susţin şi protejează confidenţialitatea. Aceasta nu aduce atingere mecanismelor existente în centrele de detenţie, menite să împiedice trimiterea de colete ilicite către deţinuţi, cum ar fi verificarea corespondenţei, cu condiţia ca astfel de mecanisme să nu permită autorităţilor competente să citească corespondenţa dintre persoanele suspectate sau acuzate şi avocatul lor. Prezenta directivă nu aduce atingere nici procedurilor din dreptul intern conform cărora transmiterea corespondenţei poate fi respinsă dacă expeditorul nu este de acord ca corespondenţa să fie în primul rând trimisă unei instanţe competente”.

II. Contextul şi perspectivele evoluţiei legislative în plan naţional

În domeniul reglementărilor privind reţinerea datelor, este evident că proiectele legislative UE şi jurisprudenţa CJUE, expuse în secţiunea precedent, vor avea un puternic impact la nivel naţional întrucât vor trebui transpuse. În privinţa unora, impactul s-a produs deja şi mă refer în principal la abrogarea Directivei privind protecţia datelor care a avut ca efect constatarea neconstituţionalităţii Legii nr. 82/2012 privind reţinerea datelor generate sau prelucrate de furnizorii de reţele publice de comunicaţii electronice şi de furnizorii de servicii de comunicaţii electronice destinate publicului (Legea Big Brother) precum şi a Legii pentru modificarea şi completarea Ordonanţei de urgenţă a Guvernului nr.111/2011 privind comunicaţiile electronice (Legea cartelelor prepay).

La 8 iulie 2014 Legea „Big Brother” este declarată neconstituţională în integralitatea ei prin Decizia Curţii Constituţionale nr.440 /2014 referitoare la excepţia de neconstituţionalitate a dispoziţiilor Legii nr.82/2012 privind reţinerea datelor generate sau prelucrate de furnizorii de reţele publice de comunicaţii electronice şi de furnizorii de servicii de comunicaţii electronice destinate publicului, precum şi pentru modificarea şi completarea Legii nr. 506/2004 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul comunicaţiilor electronice şi ale art.152 din Codul de procedură penală Pe 16 septembrie 2014 Curtea constată neconstituţionalitatea Legii “cartelelor pre pay” în integralitatea ei prin DECIZIA CCR Nr.461/2014 prin care admite obiecţia de neconstituţionalitate a dispoziţiilor Legii pentru modificarea şi completarea Ordonanţei de urgenţă a Guvernului nr.111/2011 privind comunicaţiile electronice

Curtea a precizat în motivarea deciziei că operaţiunea de reţinere şi stocare a datelor nu contravine prin ea însăşi dreptului la viaţă intima, familială şi private ori secretului corespondenţei. Însă accesul la aceste date şi utilizarea lor nu sunt însoţite de garanţiile necesare care să asigure ocrotirea drepturilor fundamentale menţionate, **în special faptul că organele cu atribuţii în domeniul securităţii naţionale au acces la aceste date fără autorizarea judecătorului**. Curtea a apreciat că

doar în cazul accesului şi a utilizării acestor date, se ridică problema conformităţii reglementărilor legale cu dispoziţiile constituţionale deoarece, spre deosebire de organele de urmărire penală, organele de stat cu atribuţii în domeniul securităţii naţionale pot accesa şi folosi datele stocate fără a fi nevoie de autorizarea instanţei de judecată. Acestea sunt Serviciul Român de Informaţii, Serviciul de Informaţii Externe şi Serviciul de Protecţie şi Pază, dar şi Ministerul Apărării Naţionale, Ministerul Afacerilor Interne şi Ministerul Justiţiei prin structurile de informaţii cu atribuţii specifice domeniilor lor de activitate.

În premieră, în motivarea deciziei Curtea face consideraţii cu privire la efectele deciziei sale, „până la adoptarea de către Parlament a unei noi legi privind reţinerea datelor, care să respecte prevederile şi exigenţele constituţionale":

„ (…) organele judiciare şi organele de stat cu atribuţii în domeniul siguranţei naţionale nu mai au acces la datele care au fost reţinute şi stocate deja în baza Directivei 2006/24/CE şi a Legii nr.82/2012 în vederea utilizării lor în cadrul activităţilor definite de art.1 alin.(1) din Legea nr.82/2012. De asemenea, organele judiciare şi cele cu atribuţii în domeniul siguranţei naţionale nu au temei legal şi constituţional nici pentru accesarea şi utilizarea datelor reţinute de către furnizori pentru facturare, plăţi pentru interconectare ori în alte scopuri comerciale, pe care să le folosească în cadrul activităţilor de prevenire, de cercetare, de descoperire şi de urmărire penală a infracţiunilor grave sau pentru rezolvarea cauzelor cu personae dispărute ori pentru punerea în executare a unui mandat de arestare sau de executare a pedepsei, tocmai datorită caracterului, naturii şi scopului diferit al acestora, aşa cum este prevăzut de Directiva 2002/58/CE." (punctul 79 din Decizia Curţii Constituţionale nr. 440 din 8 iulie 2014).

Aşadar, suntem în situaţia unui vid legislative în ceea ce priveşte reţinerea şi stocarea datelor, atât la nivel intern, cât şi la nivel european, ceea ce înseamnă că trebuie să ne aşteptam la un nou proiect de lege privind reţinerea datelor. Încă nu ştim dacă autorităţile vor aştepta o nouă directivă UE pentru a propune o nouă lege. Este mai probabil să pornească o iniţiativă proprie în acest sens. Alegerile din noiembrie au suspendat discuţiile cu privire la această problemă însă e foarte posibil ca acestea să reapară curând în prim plan, având în vedere îngrijorările legate de conflictul din Ucraina şi faptul că statul roman se află în plină campanie împotriva corupţiei iar DNA şi alte autorităţi în domeniul siguranţei statului au revendicat urgenţa unui nou proiect de lege privind reţinerea şi stocarea datelor.

În domeniul protecţiei datelor vor urma schimbări de anvergură după adoptarea la nivel European şi intrarea în vigoare a Proiectului de Regulament al Parlamentului European şi al Consiliului privind protecţia persoanelor fizice faţă de prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date (de aplicabilitate directă după adoptare) precum şi a Proiectului de Directivă a Parlamentului European şi a Consiliului privind protecţia persoanelor fizice faţă de prelucrările efectuate de către autorităţile competente în scopul prevenirii, cercetării, constatării sau urmăririi penale a infracţiunilor ori executării pedepselor penale şi libera circulaţie a acestor date.
Deocamdată este în vigoare Lege nr. 677 din 21 noiembrie 2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date, care la fel ca şi Directiva pe care o transpune (Directiva 95/46/EC privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date) este depăşită în multe privinţe, din cauza globalizării şi evoluţiei fără precedent a tehnologiei. În propunerea de directivă apar reglementări noi cu privire la „dreptul de a fi uitat" sau „dreptul la portabilitatea datelor" care permite persoanei în cauză să transfere datele personale între furnizorii de servicii .

Operatorii de date personale cum ar fi furnizorii de internet sau motoarele de căutare vor fi obligaţi să comunice cine culege datele şi în ce scop. În general, accesul la propriile date este facilitat.

Pe 16 septembrie 2014 Camera Deputaţilor a adoptat **tacit Legea securităţii cibernetice a României,** care acum se află în proceduri legislative la Senat, în aşteptarea avizelor şi a rapoartelor pentru a fi pusă în dezbatere.
Acest proiect, este „inspirat" din Directiva NIS (Network & Information Security) care nu este în vigoare şi se află încă în fază de proiect în procedura legislativă a dreptului Uniunii Europene. Conform expunerii de motive, scopul Directivei este acela de „a asigura un nivel comun ridicat de securitate a reţelelor şi a informaţiei", ceea ce înseamnă „îmbunătăţirea securităţii internetului şi a reţelelor private, precum şi a sistemelor informatice pe care se bazează funcţionarea societăţii şi a economiei". Scopul acestei Directive, care presupune implicit şi protecţia datelor a fost însă deturnat în proiectul de lege aflat acum în procedură parlamentară. Proiectul de lege prevede noi ingerinţe în viaţa privată şi o nouă cale de acces la date personale, întrucât, potrivit proiectului de lege autorităţile faţă de care există obligaţia informării şi dreptul de acces la date sunt SRI, MApN, MAI, SIE, Oficiului Registrului Naţional al Informaţiilor Secrete de Stat, Serviciului de Telecomunicaţii Speciale, Serviciului de Protecţie şi Pază, Centrul Naţional de Răspuns la Incidente de Securitate Cibernetică (CERT-RO) şi Autoritatea Naţională pentru Administrare şi Reglementare în Comunicaţii (ANCOM). Dispoziţiile care prevăd accesul la date a acestor instituţii sunt chiar contrare Directivei NIS, conform textului adoptat de Parlamentul European prin Rezoluţia legislativă a Parlamentului European din 13 martie 2014 referitoare la propunerea de directivă a Parlamentului European şi a Consiliului privind măsuri de asigurare a unui nivel comun ridicat de securitate a reţelelor şi a informaţiei în Uniune.
Conform amendamentului 11 din rezoluţia citată, „Autorităţile competente şi punctele unice de contact ar trebui să fie organisme civile, care să funcţioneze integral pe baza controlului democratic, **şi nu ar trebui să desfăşoare activităţi în domeniul informaţiilor, al aplicării legii sau al apărării** şi nici să fie legate organizaţional în vreun fel de organismele active în aceste domenii".
Contrar acestor prevederi ale Rezoluţiei, proiectul privind legea securităţii cibernetice a României permite accesul la date a tuturor acestor autorităţi! Mai mult, conform art. 10 alin. 1 din proiect, Serviciul Român de informaţii este desemnat ca autoritate naţională în domeniul securităţii cibernetice, calitate în care asigură coordonarea tehnică a Consiliului Operativ de Securitate Cibernetică (COSC) precum şi organizarea şi executarea activităţilor care privesc securitatea cibernetică a României.
O altă îngrijorare în legătură cu proiectul în discuţie este sfera de aplicabilitate care este practic nelimitată în privinţa persoanelor vizate. Conform art. 2 din proiect, legea se va aplica tuturor persoanelor juridice de drept public sau privat, care au calitatea de proprietari, administratori, operatori sau utilizatori de infrastructuri cibernetice, denumiţi deţinători de infrastructuri cibernetice.
Consiliul Legislativ a dat aviz favorabil acestui proiect, cu amendamente ce ţin mai mult de normele de tehnică legislative. Trebuie precizat că şi la Cameră toate avizele de la comisii au fost favorabile. În prezent se mai aşteaptă raportul Comisiei pentru apărare, ordine publică şi siguranţă naţională a Senatului pentru ca proiectul să intre în dezbatere în camera decizională.

*

În acest context, în care aşteptăm sau asistăm deja la derularea unor proiecte de lege privind accesul la date, trebuie iniţiate demersuri pentru a grăbi transpunerea **Directiva 2013/48/UE a Parlamentului European şi a Consiliului din 22 octombrie 2013 privind dreptul de a avea acces la un**

avocat în cadrul procedurilor penale şi al procedurilor privind mandatul european de arestare, precum şi dreptul ca o persoană terţă să fie informată în urma privării de libertate şi dreptul de a comunica cu persoane terţe şi cu autorităţi consulare în timpul privării de libertate

Având în vedere că alte proiecte de acte normative care implică ingerinţe în viaţa privată sunt „pe rolul" autorităţilor, transpunerea acestei Directive este esenţială deoarece prin prevederile pe care le conţine, întăreşte garanţiile privind apărarea secretului profesional şi a confidenţialităţii comunicărilor dintre avocat şi client, măcar în domeniul penal. Conform Articolului 4, „Statele membre respectă confidenţialitatea comunicării dintre persoanele suspectate sau acuzate şi avocatul lor în exercitarea dreptului de a avea acces la un avocat prevăzut în prezenta directivă. O astfel de comunicare include întrevederi, corespondenţă, conversaţii telefonice şi alte forme de comunicare permise în temeiul dreptului intern".

În privinţa sistemelor **de cloud** folosite de avocaţi avem deocamdată un vid legislativ.
De aceea este necesară mare atenţie în folosirea acestui sistem de stocare a datelor deoarece avocaţii au obligaţia legală de a păstra secretul profesional şi implicit de a se asigura în privinţa aceasta.
Folosirea cloud-ului implică un risc în lipsa garanţiilor legale privind protecţia datelor.

III. Recomandările CCBE în contextual reformelor legislative în domeniul datelor

În ultima perioadă, Consiliului Barourilor Europene şi-a exprimat poziţia în mod repetat faţă de evenimentele legislative şi judiciare petrecute în plan European, făcând recomandări atât forurilor legislative cât şi barourilor şi uniunilor profesionale membre. Abordarea CCBE porneşte de la viziunea, general acceptată, că pentru ca statul de drept să funcţioneze corespunzător, o condiţie esenţială este ca profesiile juridice să fie puternice şi independente. Iar pentru ca avocaţii să fie eficienţi în apărarea drepturilor clienţilor lor, trebuie să existe încredere în privinţa confidenţialităţii comunicărilor dintre avocaţi şi clienţii. Fără o astfel de protecţie, chiar funcţionarea statului de drept este subminată.

Problema s-a acutizat şi a escaladat în complexitate odată cu utilizarea în măsură tot mai mare a mijloacelor electronice de comunicare, şi, mai recent, a cloud-ului, aspecte care au început să pună această piatră de temelie sub presiune. Informaţiile secrete sau privilegiate deţinute de către avocaţi şi clienţii lor sunt în permanent sub ameninţarea supravegherii de către guverne, în contextual luptei împotriva terorismului şi a corupţiei. Informaţii care odată erau depozitate la biroul avocatului, literalmente sub cheie, sunt transmise între avocat şi client de mijloace electronice, pe Internet, şi, din ce în ce mult sunt stocate în cloud, fiind puse astfel în într-un spaţiu care se află mai mult sub o protecţie tehnică (criptarea) decât juridică. Documente confidenţiale sunt transmise prin e-mail sau stocate în cloud pe servere aflate pe alte continente şi vulnerabile de a fi interceptate şi citite nu doar agenţiile de securitate ale statului de origine, dar şi de puterilor străine, care cu ştim cât sunt de prietenoase. Astfel, datele sunt mai expuse decât a fost vreodată.

În acest context, CCBE şi-a îndreptat atenţia asupra acestor aspecte legate de noile ameninţări la adresa secretului profesional şi a confidenţialităţii comunicărilor între avocat şi client, a luat poziţie în faţa forurilor legislative europene şi a făcut nenumărate apeluri către avocaţii din barourile şi uniunile profesionale membre pentru a identifica noile garanţii ale respectării acestor drepturi.

În **Recomandările Consiliului Barourilor Europene (CCBE) ca urmare a anulării Directivei privind retenţia** datelor din 12.09.2014, în cazul în care legislaţia naţională nu este în conformitate cu preocuparea proporţionalităţii ridicată de CJUE, precum şi cu preocupările CCBE privind apărarea secretului profesional şi a comunicărilor confidenţiale între avocat şi client, cu necesitatea unei autorizaţii judiciare prealabile pentru accesarea datelor, durata şi scopul păstrării datelor, se propune ca membrii CCBE ar trebui să ia următoarele măsuri:

a) Identificarea de strategii pentru a iniţia o schimbare în legislaţia naţională în cazul în care este necesar (de exemplu, lobby parlamentar, lansarea unei campanii de conştientizare publică, etc.).

b) Mediatizarea tuturor cazurilor individuale în care clienţii / avocaţii sunt afectaţi negativ de nerespectarea confidenţialităţii şi să caute consultanţă juridică cu privire la posibilele soluţii, cu referire la hotărârea CJUE

c) Să aducă astfel de încălcări în atenţia autorităţilor responsabile cu protecţia datelor (de exemplu, Autorităţile pentru protecţia datelor, ministere, departamente specializate etc.). Mai mult decât atât, ori de câte ori este cazul, membrii CCBE ar trebui să încerce să iniţieze acţiuni în justiţie împotriva oricărei reglementări naţionale, în privinţa căreia se poate argumenta că este contrară hotărârii CJUE, inclusiv prin sprijinirea acestor acţiuni de către avocaţi individuale sau firme de avocatura (de exemplu, prin *amicus curiae brief*, dacă este cazul).

d) Să facă referire specifică la hotărârea CJUE în orice document, declaraţie publică şi scrisoare adresată oficialilor guvernamentali sau aleşi cu privire la protecţia datelor în contextul stocării şi reţinerii datelor.

e) Să aducă orice problemă ce ţine de aceste aspecte în atenţia Comisiei Europene

f) Să informeze CCBE cu privire la stadiul punerii în aplicare a Directivei privind retenţia datelor în statul respectiv şi să înştiinţeze CCBE în legătură cu modul în care poate sprijini membrul CCBE în acţiunile ce au drept scop schimbarea legislaţiei naţionale, acolo unde este necesar.

g) Să ia în considerare posibilităţile de a contesta legea de punere în aplicare a directivei privind retenţia datelor înaintea organismului constituţional relevant (de exemplu, Curtea Constituţională sau instanţele de drept comun, etc. aşa cum prevede legislaţia naţională).

Sub toate aceste aspecte, trebuie să avem în vedere că şi în condiţiile în care, în România, Legea nr. 82/2012 privind reţinerea datelor a fost declarată neconstituţională, există o legislaţie secundară care trebuie analizată şi atacată în instanţele de contencios ori de câte ori ne confruntăm cu reglementări în contradicţie cu Decizia CJUE.

Pe baza concluziilor din **Studiul comparativ privind supravegherea guvernamentală a datelor avocaţilor în Cloud** din 4.04.2014, CCBE invită Comisia Europeană să se asigure că orice regim de reglementare a interceptării comunicaţiilor este în vigoare într-un stat membru, acesta ar trebui să garanteze inviolabilitatea datelor şi a altor elemente de probă care intră sub incidenţa principiului secretului profesional.

Din acest motiv:

a) Ar trebui să existe o armonizare a unui nivel minim de protecţie a secretului profesional, indiferent că sunt date de trafic, metadate sau de conţinut şi indiferent de modul în care organismele

guvernamentale necesită acces la date şi dacă scopul reglementării este securitatea naţională sau lupta pentru prevenirea criminalităţii.

b) Nivelul minim al protecţiei comunicaţiilor care conţin secretul profesional ar trebui să fie şi în lumea electronică la fel cum este în cea a documentelor pe hârtie.

Nu în ultimul rând, având în vedere Rezoluţia referitoare la programul de supraveghere al Agenţiei Naţionale de Securitate (NSA) a SUA, la organismele de supraveghere din diferite state membre şi la impactul acestora asupra drepturilor fundamentale ale cetăţenilor UE şi asupra cooperării transatlantice în materie de justiţie şi de afaceri interne (2013/2188(INI)), CCBE invită Parlamentului European să ia măsuri urgente pentru a stabili "Habeas corpusul digital european - protejarea drepturilor fundamentale într-o epocă digitală" inclusiv protecţia confidenţialităţii relaţiei avocat-client, astfel cum este prevăzut în Acţiunea 6 din Rezoluţie.

În Răspunsul la consultările Comisiei Europene privind Raportul Trusted Cloud Europe, din 28.05.2014, CCBE are observaţii de ordin general în privinţa raportului final al consiliului de conducere al Parteneriatului European pentru Servicii Cloud, **raport denumit Înfiinţarea Serviciilor Cloud Europene de Încredere, (în continuare Raport).** Fie că vor sau nu, avocaţii nu pot ignora tendinţa spre utilizarea serviciilor de cloud computing. CCBE ia în considerare faptul că avocaţii, precum şi alţi profesionişti, ar dori utilizeze serviciile de cloud pentru a avea acces la costuri eficiente şi pentru a tine pasul cu cele mai recente tendinţele tehnologice. Nu este doar o chestiune de a economisi costurile de tehnologie şi îmbunătăţirea eficienţei de afaceri, dar, de asemenea, o chestiune de a oferi clienţilor servicii de cea mai buna calitate. Clienţii se bazează din ce în ce mai mult pe utilizarea serviciilor de cloud. CCBE înţelege avantajele oferite de cloud computing pentru furnizarea de soluţii rapide, economice, fiabile şi flexibile precum şi faptul că avocaţii sunt dornici să utilizeze cloud, la fel ca şi alţi profesionişti, însă atrage atenţia că mediul de reglementare actual, în care operează avocaţii, tinde să împiedice capacitatea lor de a utilizează cloud-ul pe deplin în scopuri profesionale.

În primul rând, trebuie să aibă în vedere cerinţele Directivei privind protecţia datelor, în special în privinţa dificultăţilor generate de transmiterea datelor în afara Spaţiului Economic European (SEE), având în vedere standardele inferioare de protecţie a datelor care se aplică în multe jurisdicţii din afara SEE. O preocupare deosebită este în legătură cu practica furnizorilor serviciilor de cloud de a-şi rezerva dreptul de a stoca date oriunde în lume, în colaborare marii furnizori de servicii cloud care pot fi supuse reglementărilor “de mână lungă” ale SUA sau ale altor jurisdicţii străine, din afara SEE. În al doilea rând, există norme profesionale şi deontologice incidente avocaţilor care pre prevăd ca obligaţie majoră apărarea secretului profesional şi a relaţiei de confidenţialitate cu clientul.

De aceea, de câţiva ani, cloud computing a fost în topul ordinii de zi a CCBE, atât din cauza multiplelor sale avantaje potenţiale semnificative, dar şi pentru că, aşa cum s-a menţionat anterior, avocaţii trebuie să fie conştienţi de riscuri să respecte secretul profesional şi obligaţia de confidenţialitate. În acest scop, CCBE a adoptat în 2012, un set de orientări pentru a face avocaţii mai conştienţi de diversele riscuri asociate cu cloud computing-ul şi pentru a-i ajuta în luarea deciziilor tehnologice cunoştinţă de cauză.

În privinţa observaţiilor făcute de CCBE cu privire la Raportul privind Înfiinţarea Serviciilor Cloud Europene de Încredere, CCBE învederează că sunt anumite probleme care nu sunt abordate în mod adecvat în Raport. Acestea sunt următoarele:

1) Cadrul de reglementare în care operează profesiile legale poate inhiba abordarea serviciilor de cloud computing de către avocaţi.
Cu toate acestea, avocaţilor sau uniunilor profesionale le este greu, pe cont propriu, să se impună semnificativ în faţa tendinţei generale în cloud computing. Cu foarte puţine excepţii, avocaţii nu au puterea să negocieze condiţiile standard impuse de cei mai mulţi furnizori de cloud. Iar în cazul în care aceşti termeni includ dreptul de a stoca date în afara SEE, acest lucru poate împiedica utilizarea unui astfel de serviciu de cloud de către avocaţi. Nu este posibil pentru toate societăţile de avocatură, dar cele mai mari pot avea propriul cloud privat. Însă este puţin probabil ca avocaţii individuali şi firmele de avocatură să aibă suficientă putere de cumpărare, chiar şi prin achiziţii centralizate, pentru a susţine o categorie aparte de cloud pentru servicii avocaţiale.

2) În plus, având în vedere că avocaţii au obligaţii foarte stricte în privinţa păstrării confidenţialităţii comunicărilor cu clientul şi chiar dacă de exemplu furnizorii de servicii de cloud îşi restrâng răspunderea în cazul încălcării confidenţialităţii, majoritatea avocaţilor nu sunt în măsură să facă acelaşi lucru faţă de clienţii lor.

3) Ceea ce a reieşit clar din Studiul CCBE privind Supravegherea guvernamentală a datelor avocaţilor în Cloud a fost că protecţia legală a comunicărilor avocat-client împotriva accesului guvernamental nu este la fel de puternică în mediul cloud ca şi în incinta fizică a avocatului. În consecinţă, avocatul îşi serveşte mai bine clienţii atunci când nu le expune datele la riscul unor astfel de practici. Această diferenţă considerabilă în ceea ce priveşte protecţia comunicările avocat-client nu va fi modificată în mod corect prin adoptarea propunerii de regulament privind protecţia datelor.

4) În cazul în care un avocat doreşte să folosească orice serviciu de cloud, trebuie să ceară acordul prealabil al clientului şi să aibă aprobarea expresă a acestuia de a permite utilizarea cloud-ului. Se ajunge până acolo încât clientul este în măsură să dea o astfel de aprobare pentru toate comunicările avocatului. Acest lucru nu este de dorit nici din perspectiva de a vinde servicii juridice, şi nici, mult mai important, din perspectiva de a respecta în mod corespunzător interesele legitime ale clienţilor.

5) De asemenea, Organismele profesionale nu sunt în măsură să acorde o derogare pentru avocaţi (chiar presupunând că astfel de ar putea fi posibil), deoarece nu este numai o chestiune tehnică de amplasare a datelor, dar este, de asemenea, o chestiune legală de jurisdicţie. În cazul în care furnizorul de servicii cloud relevante a fost mandatat de legea jurisdicţiei incidente acestuia pentru a permite accesul la date sau informaţii confidenţiale, avocatul devine expus fără prevederi contractuale care ar putea fi invocate împotriva furnizorului de servicii, chiar dacă acordarea unui astfel de acces este în contradicţie cu obligaţiile avocatului faţă de clientul său. Este evident că organismele cu drept de reglementare nu vor fi în măsură să armonizeze fragmentat legile naţionale cu practicile (în special din statele extra-SEE), care creează o astfel de anomalie.

6) Pe scurt, nu este realist să ne aşteptăm de la organizaţii profesionale, cum ar fi CCBE, să fie în măsură să „se asigure că orientările şi politicile lor sunt cel puţin cloud neutre (de exemplu, permite servicii de cloud.) "(pagina 17 din Raport). Avocaţii sunt supuşi legii statului lor şi obligaţiilor impuse de corpul lor profesional (care, la rândul său, funcţionează sub rezerva legilor naţionale) şi atâta timp cât legislaţia naţională nu este neutră cloud, nu exista aproape nimic de făcut în această privinţă de către organizaţiile/corpurile profesionale.

7) De asemenea, este important de subliniat că acţiunile din Raport (paginile 23-24) nu în măsură să spargă un cerc vicios al diferitelor autorităţi de reglementare, care aşteaptă unele după altele. Secţiunea din Raport privind acţiunile care trebuie întreprinse de către statele membre este prea blând formulată uşor pentru a fi eficace: „alinierea, reforma şi armonizarea cadrului legal şi a

politicilor pot fi adecvate în anumite cazuri" (pagina 18). Este nevoie să se sublinieze faptul că acest lucru nu este suficient: piedicile în calea adoptării serviciilor cloud sunt derivate în mod substanţial din dreptul european şi legile statelor membre. Nu este într-adevăr nici un punct de referinţă pentru „colectarea celor mai bune practici" şi elaborarea unui „cadru flexibil comun" sau pentru încercarea de a construi un „consens sistematic" prin consultări (pagina 14) în sectoarele în care serviciile de cloud computing sunt inhibate de lege.

8) CCBE recomandă iniţierea unor acţiuni pentru ajungerea la un consens care vizează statele membre, organismele profesionale şi utilizatorii cloud, care să înceapă imediat şi nu de la începutul anului 2015, pentru a asigura beneficii optime (de exemplu clauzele contractuale cloud sigure şi corecte) sau consultaţii pentru a asigura acceptarea acestora mai târziu.

*

În concluzie, în acest context, profesia de avocat se află sub o ameninţare fără precedent întrucât un pilon fundamental al existenţei acesteia, confidenţialitatea comunicărilor avocat client, este sub semnul îndoielilor. Pe de altă parte, avocaţii se află într-un moment crucial al reformelor legislative la care trebuie să pună umărul pentru găsirea soluţiilor de echilibrare a legislaţiei privind protecţia vieţii private faţă de reglementările absolut necesare pentru siguranţa cetăţenilor, pentru identificarea de noi garanţii ale protecţiei drepturilor fundamentale ale cetăţenilor, a confidenţialităţii comunicărilor avocat client, ca o condiţie esenţială a înfăptuirii justiţiei şi a statului de drept.

Prin urmare, avocaţii sunt datori să monitorizeze evoluţia legislativă în domeniul datelor şi să intervină cu opinii atunci când vor avea loc consultările publice la nivel naţional, astfel încât orice atingeri aduse secretului profesional şi confidenţialităţii comunicărilor dintre avocat şi client să fie devoalate din start pentru că acestea au un impact negativ asupra dreptului cetăţenilor la consiliere juridică, asupra accesului la justiţie şi asupra dreptului la un proces echitabil, cu un efect dezastruos asupra profesiei şi activităţii avocaţiale.

*

IV. Compatibilitatea activităţii de colectare a datelor generate sau prelucrate în legătură cu furnizarea serviciilor de comunicaţii electronice accesibile publicului sau de reţele de comunicaţii publice cu legislaţia privind profesia de avocat relativă la secretul profesional al avocatului

Secretul profesional reprezintă unul dintre cele mai elementele indispensabile exercitării adecvate a profesiei de avocat. Acesta este motivul pentru care, art. 11 din Legea nr. 51/1995 stabileşte că avocatul este dator să păstreze secretul profesional privitor la orice aspect al cauzei care i-a fost încredinţată.

Pentru a garanta respectarea secretului profesional, art. 35 din aceeaşi Lege prevede:

„(1) Pentru asigurarea secretului profesional, actele şi lucrările cu caracter profesional aflate asupra avocatului sau în cabinetul său sunt inviolabile. Percheziţionarea avocatului, a domiciliului ori a cabinetului său sau ridicarea de înscrisuri şi bunuri nu poate fi făcută decât de procuror, în baza unui mandat emis în condiţiile legii.
(2) Nu vor putea fi ascultate şi înregistrate, cu niciun fel de mijloace tehnice, convorbirile telefonice ale avocatului şi nici nu va putea fi interceptată şi înregistrată corespondenţa sa cu caracter profesional, decât în condiţiile şi cu procedura prevăzute de lege."

Art. 36 din Lege de avocat stipulează:

„(1) Contactul dintre avocat şi clientul său nu poate fi stânjenit sau controlat, direct sau indirect, de niciun organ al statului.
(2) În cazul în care clientul se află în stare de arest sau detenţie, administraţia locului de arest ori detenţie are obligaţia de a lua măsurile necesare pentru respectarea drepturilor prevăzute la alin. (1)."
Statutul profesiei de avocat este mult mai precis. Potrivit art. 1 alin. 2 lit. e) din Statutul profesiei de avocat unul dintre principiile fundamentale ale exercitării acestei profesii este păstrarea secretului profesional. Principiul este detaliat de mai multe prevederi ale Statutului care fac referire la informațiile și înscrisurile care cad sub incidența secretului profesional, acestea fiind în principiu legate de aspectele cauzei care a fost încredințată de client avocatului.

Potrivit art. 8 din Statului profesiei de avocat,

„(1) Secretul profesional este de ordine publică.

(2) Avocatul este dator să păstreze secretul profesional privitor la orice aspect al cauzei care i-a fost încredințată.

(3) Avocatul nu poate fi obligat în nicio circumstanță și de către nicio persoană să divulge secretul profesional. Avocatul nu poate fi dezlegat de secretul profesional nici de către clientul său și nici de către o altă autoritate sau persoană. Se exceptează însă cazurile în care avocatul este urmărit penal, disciplinar sau atunci când există o contestație în privința onorariilor convenite, exclusiv pentru necesități stricte pentru apărarea sa.

(4) Obligația de a păstra secretul profesional nu împiedică avocatul să folosească informațiile cu privire la un fost client, dacă acestea au devenit publice."

Potrivit art. 9 din Statutul profesiei de avocat,

„(1) Obligația de a păstra secretul profesional este absolută și nelimitată în timp. Obligația se întinde asupra tuturor activităților avocatului, ale asociaților săi, ale avocaților colaboratori, ale avocaților salarizați din cadrul formei de exercitare a profesiei, inclusiv asupra raporturilor cu alți avocați.

(2) Obligația de a păstra secretul profesional revine și persoanelor cu care avocatul conlucrează în exercitarea profesiei, precum și salariaților săi. Avocatul este dator să le aducă la cunoștință această obligație.

(3) Obligația de a păstra secretul profesional revine tuturor organelor profesiei de avocat și salariaților acestora cu privire la informațiile cunoscute în exercitarea funcțiilor și atribuțiilor ce le revin."

Potrivit art. 10 din Statutul profesiei de avocat,

„(1) Orice comunicare sau corespondență profesională între avocați, între avocat și client, între avocat și organele profesiei, indiferent de forma în care a fost făcută, este confidențială.

(2) În relațiile cu avocații înscriși într-un barou dintr-un stat membru al Uniunii Europene, avocatul este obligat să respecte dispozițiile speciale prevăzute de Codul deontologic al avocaților din Uniunea Europeană.

(3) În relațiile cu un avocat înscris într-un barou din afara Uniunii Europene, avocatul trebuie să se asigure, înainte de a schimba informații confidențiale, că în țara în care își exercită profesia confratele străin există norme ce permit asigurarea confidențialității corespondenței și, în caz contrar, să încheie un acord de confidențialitate sau să îl întrebe pe clientul său dacă acceptă, în scris, riscul unui schimb de informații neconfidențiale.

(4) Corespondența și informațiile transmise între avocați sau între avocat și client, indiferent de tipul de suport, nu pot fi în niciun caz aduse ca probe în justiție și nici nu pot fi lipsite de caracterul confidențial."

Potrivit art. 113 din Statutul profesiei de avocat,

„Avocatul este confidentul clientului în legătură cu cazul încredințat. Confidențialitatea și secretul profesional garantează încrederea în avocat și constituie obligații fundamentale ale avocatului."

Potrivit art. 228 alin. 2 din Statutul profesiei de avocat

„(2) Secretul profesional vizează toate informațiile și datele de orice tip, în orice formă și pe orice suport, furnizate avocatului de către client în scopul acordării asistenței juridice și în legătură cu care clientul a solicitat păstrarea confidențialității, precum și orice documente redactate de avocat care conțin sau se fundamentează pe informațiile ori datele furnizate de client în scopul acordării asistenței juridice și a căror confidențialitate a fost solicitată de client."

În corelare cu aceste reguli, art. 306 alin. (6) din Codul de procedură penală stabileşte că:
„*Secretul bancar şi cel profesional, cu excepţia secretului profesional al avocatului, nu sunt opozabile procurorului, după începerea urmăririi penale.*"

Toate aceste prevederi legale permit concluzia că secretul profesional al avocatului reprezintă un concept larg, care include, pe lângă dreptul şi obligaţia avocatului de a nu dezvălui nimănui informaţiile comunicate de către client, şi dreptul la protecţia lucrărilor cu caracter profesional şi chiar şi protecţia contactului dintre avocat şi clientul său care nu poate fi stânjenit şi înregistrat ambiental, interceptat, etc.
În prezent comunicările dintre avocat şi client, dintre avocaţi, indiferent de natura acestora, se realizează într-o proporţie covârşitoare cu ajutorul tehnologiilor electronice tot mai inovative. Nivelul protecţiei secretului profesional în cadrul contactului şi comunicărilor dintre avocat şi clientul său, dintre avocaţi, dintre avocaţi şi instanţe, poate fi analizat prin abordarea problematicii din cel puţin două perspective:

- care este măsura în care principiile dreptului european permit ingerinţa în sfera contactului dintre avocat şi client;
- care este maniera în care Codul de procedură penală permite supravegherea tehnică a contactului dintre avocat şi client prin interceptarea comunicaţiilor sau a oricărui tip de comunicare la distanţă.

Hotărârea Curţii de Justiţiei a Uniunii Europene din 8 aprilie 2014 – evocată mai sus – permite identificarea sensului limitelor dreptului la confidenţialitate şi restrângerea justificată legal a acestuia.

Hotărârea a explicat că, pentru combaterea eficace a criminalităţii grave, în special a criminalităţii organizate şi a terorismului, care prezintă o importanţă primordială pentru garantarea siguranţei publice în spaţiul european, este necesară utilizarea tehnicilor moderne de anchetă.

Sunt necesare însă prevede norme clare şi precise care să reglementeze conţinutul şi aplicarea măsurilor în discuţie şi să impună cerinţe minime, astfel încât persoanele ale căror date au fost păstrate să dispună de garanţii suficiente care să permită protejarea în mod eficient a datelor lor cu caracter personal împotriva riscurilor de abuz, precum şi împotriva oricărui acces şi a oricărei utilizări ilicite a acestor date.

Sunt semnificative următoarele dezlegări date de hotărâre:

„58. Astfel, pe de o parte, Directiva 2006/24 priveşte în mod global ansamblul persoanelor care utilizează servicii de comunicaţii electronice, fără însă ca persoanele ale căror date sunt păstrate să se regăsească, fie şi în mod indirect, într-o situaţie susceptibilă să declanşeze începerea urmăririi penale. Directiva se aplică, aşadar, chiar şi acelor persoane în privinţa cărora nu există niciun indiciu de natură să sugereze că comportamentul lor poate avea o legătură, chiar indirectă sau îndepărtată, cu infracţiuni grave. În plus, directiva menţionată nu prevede nicio excepţie, astfel încât ea se aplică chiar şi acelor persoane ale căror comunicaţii sunt supuse, potrivit normelor dreptului naţional, ***secretului profesional****.*

59. Pe de altă parte, deşi urmăreşte să contribuie la combaterea criminalităţii grave, directiva menţionată nu impune existenţa unei relaţii între datele a căror păstrare este prevăzută şi o ameninţare pentru siguranţa publică şi în special aceasta nu se limitează la păstrarea fie a unor date aferente unei perioade temporale şi/sau unei zone geografice determinate şi/sau unui cerc de persoane determinate care ar putea fi implicate, într-un mod sau altul, în săvârşirea unei infracţiuni grave, fie a unor date referitoare la persoane care ar putea contribui, pentru alte motive, prin păstrarea datelor lor, la prevenirea, la detectarea sau la urmărirea penală a infracţiunilor grave.

60. În al doilea rând, la această lipsă generală de limite se adaugă faptul că Directiva 2006/24 nu prevede niciun criteriu obiectiv care să permită delimitarea accesului autorităţilor naţionale competente la date şi utilizarea lor ulterioară în scopul prevenirii, detectării sau urmăririi penale în legătură cu infracţiuni care, având în vedere amploarea şi gravitatea ingerinţei în drepturile fundamentale consacrate la articolele 7 şi 8 din cartă, pot fi considerate ca fiind suficient de grave pentru a justifica o astfel de ingerinţă. Dimpotrivă, Directiva 2006/24 se limitează la a face trimitere în general, la articolul 1 alineatul (1), la infracţiunile grave, astfel cum sunt definite de fiecare stat membru în dreptul său intern.

61. În plus, în ceea ce priveşte accesul autorităţilor naţionale competente la date şi utilizarea lor ulterioară, Directiva 2006/24 nu conţine condiţiile materiale şi procedurale aferente. Articolul 4 din această directivă, care reglementează accesul acestor autorităţi la datele păstrate, nu prevede în mod expres că accesul respectiv şi utilizarea ulterioară a datelor în cauză trebuie să fie restricţionate în mod strict la scopul prevenirii şi al detectării infracţiunilor delimitate precis sau al desfăşurării urmăririi penale aferente acestora, ci se limitează să prevadă că fiecare stat membru defineşte

procedurile care trebuie să fie urmate şi condiţiile care trebuie să fie îndeplinite pentru a obţine acces la datele păstrate în conformitate cu cerinţele de necesitate şi proporţionalitate.
62. În special, Directiva 2006/24 nu prevede niciun criteriu obiectiv care să permită limitarea numărului de persoane ce dispun de autorizaţia de acces şi de utilizare ulterioară a datelor păstrate la strictul necesar în lumina obiectivului urmărit. Mai ales, accesul la datele păstrate de autorităţile naţionale competente nu este condiţionat de un control prealabil efectuat fie de o instanţă, fie de o entitate administrativă independentă prin a căror decizie se urmăreşte limitarea accesului la date şi a utilizării lor la ceea ce este strict necesar în vederea atingerii obiectivului urmărit şi care este adoptată în urma unei cereri motivate a acestor autorităţi formulate în cadrul procedurilor de prevenire, de detectare sau de urmărire penală. În directivă nu s-a prevăzut nici o obligaţie precisă a statelor membre privind stabilirea unor astfel de limitări.
63. În al treilea rând, în ceea ce priveşte durata de păstrare a datelor, Directiva 2006/24 impune, la articolul 6, păstrarea acestora pentru o perioadă de cel puţin şase luni, fără a se face vreo distincţie între categoriile de date prevăzute la articolul 5 din această directivă în funcţie de utilitatea lor eventuală în scopul realizării obiectivului urmărit sau în funcţie de persoanele vizate.
64. În plus, durata respectivă este de minimum şase luni şi maximum 24 de luni, fără a se preciza că stabilirea duratei de păstrare trebuie să fie întemeiată pe criterii obiective pentru a garanta limitarea acesteia la strictul necesar."

Decizia nr. 440 din 8 iulie 2014 a Curţii Constituţionale a preluat argumentele Hotărârii Curţii de Justiţie a Uniunii Europene şi a reţinut că lipsa unei dispoziţii legale care să condiţioneze transmiterea datelor reţinute de către furnizorii de reţele publice de comunicaţii electronice şi furnizorii de servicii de comunicaţii electronice destinate publicului de necesitatea unei autorizări prealabile emise de un organ de jurisdicţie echivalează cu insuficienţa garanţiilor necesare ocrotirii eficiente a drepturilor. În acest sens, Curtea Constituţională a statuat:

„62. Astfel, aşa cum a fost arătat anterior, potrivit dispoziţiilor art. 1 din Legea nr. 82/2012, au acces la datele reţinute conform prevederilor acestei legi, organele de urmărire penală, instanţele de judecată şi organele de stat cu atribuţii în domeniul siguranţei naţionale. Însă, potrivit dispoziţiilor art. 18 din Legea nr. 82/2012, doar organele de urmărire penală sunt obligate să respecte dispoziţiile art. 152 din Codul de procedură penală, această obligaţie nefiind prevăzută şi pentru organele de stat cu atribuţii în domeniul securităţii naţionale, care pot accesa aceste date în conformitate cu „legile speciale în materie", aşa cum prevede art. 16 alin.(1) din Legea nr. 82/2012. Prin urmare, doar solicitarea adresată de organele de urmărire penală furnizorilor de reţele publice de comunicaţii electronice şi furnizorilor de servicii de comunicaţii electronice destinate publicului de transmitere a datelor reţinute este supusă autorizării prealabile a judecătorului de drepturi şi libertăţi.
63. Solicitările de acces la datele reţinute în vederea utilizării lor în scopul prevăzut de lege, formulate de către organele de stat cu atribuţii în domeniul securităţii naţionale, nu sunt supuse autorizării sau aprobării instanţei judecătoreşti, lipsind astfel garanţia unei protecţii eficiente a datelor păstrate împotriva riscurilor de abuz precum şi împotriva oricărui acces şi a oricărei utilizări ilicite a acestor date. Această împrejurare este de natură a constitui o ingerinţă în drepturile fundamentale la viaţă

intimă, familială şi privată şi a secretului corespondenţei şi, prin urmare, contravine dispoziţiilor constituţionale care consacră şi protejează aceste drepturi."

De la publicarea Deciziei Curţii Constituţionale în Monitorul Oficial, furnizorii de reţele publice de comunicaţii electronice şi furnizorii de servicii de comunicaţii electronice destinate publicului nu mai au posibilitatea legală de a reţine anumite date generate sau prelucrate în cadrul activităţii lor şi de a le pune la dispoziţia organelor judiciare şi ale celor cu atribuţii în domeniul siguranţei naţionale. Prin excepţie şi exclusiv în baza consimţământului prealabil al persoanei ale cărei date sunt prelucrate, pot fi reţinute de către aceşti furnizori doar datele necesare pentru facturare sau plăţi pentru interconectare ori alte date prelucrate în scopuri de comercializare, aşa cum prevede Directiva 2002/58/CE a Parlamentului European şi a Consiliului din 12 iulie 2002 privind prelucrarea datelor personale şi protejarea confidenţialităţii în sectorul comunicaţiilor publice. Organele judiciare penale şi organele de stat cu atribuţii în domeniul siguranţei naţionale nu mai au acces la datele care au fost reţinute şi stocate deja în baza Legii nr. 82/2012. În plus, organele judiciare şi cele cu atribuţii în domeniul siguranţei naţionale nu mai au niciun temei legal pentru accesarea şi utilizarea datelor reţinute de către furnizori pentru facturare, plăţi pentru interconectare ori în alte scopuri comerciale, pe care să le folosească în cadrul activităţilor de prevenire, de cercetare, de descoperire şi de urmărire penală a infracţiunilor grave sau pentru rezolvarea cauzelor cu persoane dispărute ori pentru punerea în executare a unui mandat de arestare sau de executare a pedepsei, datorită caracterului, naturii şi scopului diferit al acestora, aşa cum este prevăzut de Directiva 2002/58/CE.

Se impune să constatăm că, în pofida neajunsurilor identificare în reglementarea Directivei 2006/24, legislaţia internă nu permite stocarea conţinutului comunicaţiilor electronice, motiv pentru care s-ar realiza doar indirect stânjenirea ori controlul contactului dintre avocat şi client.

Potrivit Codului de procedură penală, conţinutul tuturor comunicaţiilor şi a oricărui tip de comunicare la distanţă poate fi interceptat şi, implicit, cunoscut de către organele judiciare penale cu autorizarea judecătorului de drepturi şi libertăţi (art. 140) ori, în caz de urgenţă, cu autorizarea procurorului (art. 141).

Din această perspectivă, se pune problema de a stabili în ce măsură supravegherea tehnică a contactului dintre avocat şi client este compatibilă cu însăşi existenţa secretului profesional. De vreme ce informaţiile acoperite de secretul profesional devin cunoscute organelor judiciare penale cu ocazia interceptării contactului dintre avocat şi client, apare în mod firesc întrebarea: mai există un secret profesional în privinţa acestora?

Răspunsul la această întrebare se regăseşte la art. 139 alin. (4) din Codul de procedură penală, potrivit căruia:

„*Raportul dintre avocat şi persoana pe care o asistă sau o reprezintă nu poate forma obiectul supravegherii tehnice decât dacă există date că avocatul săvârşeşte ori pregăteşte săvârşirea unei infracţiuni dintre cele prevăzute la alin. (2). Dacă pe parcursul sau după executarea măsurii rezultă că activităţile de supraveghere tehnică au vizat şi raporturile dintre avocat şi suspectul ori inculpatul pe care acesta îl apără, probele obţinute nu pot fi folosite în cadrul niciunui proces penal, urmând a fi*

distruse, de îndată, de către procuror. Judecătorul care a dispus măsura este informat, de îndată, de către procuror. Atunci când apreciază necesar, judecătorul dispune informarea avocatului."

Se poate observa că raportul dintre avocat şi clientul său, indiferent de natura civilă sau penală a cauzei în care a intervenit raportul profesional, poate face obiectul supravegherii tehnice numai în cazul în care există date că avocatul săvârşeşte ori pregăteşte săvârşirea uneia dintre infracţiunile limitativ de art. 139 alin. 2 din Codul de procedură penală: *infracţiuni contra securităţii naţionale prevăzute de Codul penal şi de legi speciale, precum şi în cazul infracţiunilor de trafic de droguri, de trafic de arme, de trafic de persoane, acte de terorism, de spălare a banilor, de falsificare de monede ori alte valori, de falsificare de instrumente de plată electronică, contra patrimoniului, de şantaj, de viol, de lipsire de libertate, de evaziune fiscală, în cazul infracţiunilor de corupţie şi al infracţiunilor asimilate infracţiunilor de corupţie, infracţiunilor împotriva intereselor financiare ale Uniunii Europene, al infracţiunilor care se săvârşesc prin sisteme informatice sau mijloace de comunicaţii electronice ori în cazul altor infracţiuni pentru care legea prevede pedeapsa închisorii de 5 ani sau mai mare*.

În cazul în care persoana supravegheată nu este avocatul, ci clientul acestuia, de vreme ce persoanele care realizează în mod efectiv supravegherea tehnică au obligaţia de a păstra confidenţialitatea informaţiilor la care au acces, iar probele obţinute prin supravegherea tehnică a raporturilor dintre avocat şi clientul pe care îl apără nu pot fi folosite în cadrul niciunui proces penal, deşi sunt supuse unor ingerinţe din partea autorităţilor statului, informaţiile comunicate între avocat şi suspectul sau inculpatul pe care îl apără rămân în sfera secretului profesional şi sunt protejate de privilegiul avocat – client.

Cu toate acestea, este în afara oricărei discuţii că principiul egalităţii de arme dintre acuzare şi apărare este profund lezat, întrucât acuzarea va cunoaşte în mod negreşit care este strategia apărării.

Trebuie să remarcăm că, deşi procurorul este obligat să informeze, în cel mai scurt timp, judecătorul de drepturi şi libertăţi care a dispus măsura despre interceptarea contactului dintre avocat şi suspectul sau inculpatul pe care acesta îl apără, judecătorul are doar facultatea de a aduce acest fapt la cunoştinţa avocatului, ceea ce, din nou, ridică probleme serioase prin prisma egalităţii de arme.

Fără a avea pretenţii de exhaustivitate, iată, deci, câteva dintre problemele pe care le ridică normele din domeniul dreptului penal, menite să contribuie la asigurarea confidenţialităţii contactului dintre avocat şi clientul său.

*

Sunt probleme şi cu privire la procedura de exercitare a dreptului organelor fiscale de a determina situaţia fiscală a contribuabilului, potrivit art. 7 alin. (2) – (4) din O.G. nr. 92/2003 privind Codul de procedura fiscală.

Art. 59 din Codul de procedură fiscală prevede:

„(1) Pot refuza să furnizeze informații cu privire la datele de care au luat cunoștință în exercitarea activității lor preoții, avocații, notarii publici, consultanții fiscali, executorii judecătorești, auditorii, experții contabili, medicii și psihoterapeuții, cu excepția informațiilor cu privire la îndeplinirea obligațiilor fiscale stabilite de lege în sarcina lor.

(2) Sunt asimilate persoanelor prevăzute la alin. (1) asistenții, precum și persoanele care participă la activitatea profesională a acestora.

(3) Persoanele prevăzute la alin. (1), cu excepția preoților, pot furniza informații, cu acordul persoanei despre care au fost solicitate informațiile.

(4) În regim derogatoriu de la prevederile alin. (1)-(3), în vederea clarificării și stabilirii reale a situației fiscale a contribuabililor, organele fiscale au competența de a solicita informații și documente cu relevanță fiscală ori pentru identificarea contribuabililor sau a materiei impozabile ori taxabile, după caz, iar notarii publici, avocații, executorii judecătorești, organele de poliție, organele vamale, serviciile publice comunitare regim permise de conducere și înmatriculare a vehiculelor, serviciile publice comunitare pentru eliberarea pașapoartelor simple, serviciile publice comunitare de evidență a persoanelor, precum și orice altă entitate care deține informații ori documente cu privire la bunuri impozabile sau taxabile, după caz, ori la persoane care au calitatea de contribuabil au obligația furnizării acestora fără plată."

Avocatul are dreptul de a nu divulga organelor fiscale informaţii supuse secretului profesional, cu excepţia acordului expres al persoanei despre care au fost solicitate informaţiile (art. 59 alin. 3 din Codul de procedură fiscală). De la acest principiu sunt exceptate informaţiile legate de îndeplinirea de către avocat a obligaţiilor fiscale care îi revin şi informaţiile, documentele care au relevanţă fiscală sau servesc identificării contribuabililor sau a materiei impozabile sau taxabile, respectiv cele din contractul de asistenţă juridică.

Acestea din urmă trebuie să fie identificate ca atare de către organul fiscal în cererea de informaţii adresată avocatului, pentru că regimul derogatoriu de la aplicarea secretului profesional al avocatului prevăzut de art. 59 alin. (4) din Codul de procedură fiscală, cu caracter de informaţii publice, nu pot fi comunicate în forma prevăzută în contractul de asistenţă juridică care este obiect al obligaţiei protejării secretului profesional cu privire la date ce vizează cauza încredinţată de client sau obiectul activităţii avocatului.

Preeminenţa secretului profesional în acest caz obligă organul fiscal să demonstreze condiţia legală sub care sunt solicitate informaţii de acest gen, deoarece stocarea şi folosirea lor de către organul fiscal, obiect al confidenţialităţii controlului fiscal – este exclusă. De aceea organele fiscale nu pot solicita contractul de asistenţă juridică în integralitatea sa ci doar tipurile de informaţii identificate ca relevante fiscal din perspectiva şi condiţiile de mai sus.

Nu constituie obiect al preocupărilor prezentei comunicări raportul dintre secretul profesional al avocatului şi secretul bancar, corelaţie care impune concluzii particulare, inclusiv din perspectiva eventualelor baze de date ce pot fi realizate pe baza unor informaţii de domeniu.

Av. dr. Florea Gheorghe