Polska delegacja do CCBE popiera rekomendacje przyjęte przez CCBE w przedmiocie implementacji dyrektywy w sprawie retencji danych, jak również stanowisko Rzecznika Generalnego Pedro Cruz Villalón z dnia 12 grudnia 2013 r. dotyczące niezgodności z prawem do prywatności i prawem do obrony norm zawartych w Dyrektywie 2006/24/WE Parlamentu Europejskiego i Rady z dnia 15 marca 2006 r. w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności.

Autonomia informacyjna jednostki jako część prawa do prywatności nabiera we współczesnym świecie coraz większego znaczenia, dlatego też potencjalna ingerencja państwa w to prawo wymaga spełnienia wymogów określonych w art. 8 ust. 2 Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności. Ochrona prawa do prywatności oraz danych osobowych przewidziana w art. 7 i 8 Karty Praw Podstawowych przypomina o konieczności przetwarzania danych rzetelnie w określonych celach i za zgodą osoby zainteresowanej lub na innej uzasadnionej podstawie przewidzianej ustawą, co powinno podlegać kontroli niezależnego organu.

Orzecznictwo Europejskiego Trybunału Praw Człowieka (m. in. sprawa S. i Marper przeciwko Wielkiej Brytanii) potwierdza, że już samo gromadzenie informacji o danej osobie ma bezpośredni wpływ na ochronę jej życia prywatnego, bez względu na to, czy dane te są następnie wykorzystywane. Również Europejski Trybunał Sprawiedliwości w orzeczeniu w połączonych sprawach C-92/09 i C-93/09, orzekł, że ograniczenia w zakresie ochrony danych osobowych są dopuszczalne jedynie pod warunkiem ich „ścisłej proporcjonalności", w stosunku do realizowanego celu.

Występująca w Europie debata o zgodności z prawami podstawowymi jednostek działaniami służb publicznych sięgających do danych, w szczególności billingów, czy danych indywidualizujących uczestników łączności elektronicznej, prowadzi do wniosku o niewystarczającym stopniu ochrony praw jednostki w obowiązującym prawie europejskim i ustawodawstwach krajowych. O tym, jak znaczne jest ryzyko nadużyć wobec jednostek na gruncie obecnej Dyrektywy i uchwalonego na jej podstawie prawa krajowego przekonać może najlepiej przykład polskiej implementacji, która od kilku lat jest przedmiotem ożywionej debaty publicznej, prowadzonej z udziałem polskiej Adwokatury.

Debata ta już zaowocowała zmianą części przepisów prawa telekomunikacyjnego, negatywnym raportem Najwyższej Izby Kontroli oraz skierowaniem do Trybunału Konstytucyjnego wniosku o stwierdzenie niezgodności z Konstytucją RP przepisów dotyczących dostępu do danych informatycznych przez szereg służb państwowych, w tym przez służby specjalne. W postępowaniu zainicjowanym przez połączone wnioski Rzecznika Praw Obywatelskich oraz Prokuratora Generalnego Trybunał zajmie się kwestią pominięcia w zakwestionowanych przepisach regulacji wyłączającej z kręgu podmiotów, które mogą być poddane kontroli operacyjnej, kategorii osób, od których pozyskanie informacji objętych tajemnicą m. in. adwokacką, dziennikarską, notarialną, radcy prawnego i lekarską, podlega zakazom dowodowym. Do udziału w rozprawie została zaproszona Naczelna Rada Adwokacka.

Działająca przy Naczelnej Radzie Adwokackiej Komisja Praw Człowieka, już w 2011 r. przygotowała raport dotyczący implementacji dyrektywy w prawie polskim, który stał się przyczynkiem do dyskusji o dostrzeżonych problemach w porządku prawnym. Państwo polskie, powołując się m. in. na konieczność zwalczania terroryzmu w wykonaniu dyrektywy przyjęło bowiem przepisy pozwalające na 24- miesięczny okres retencji danych, nie określiło także katalogu spraw, do których może być on stosowany, co umożliwiało występowanie o dane także w sprawach cywilnych, szczególnie rozwodowych. Co więcej, części służb specjalnych nie obejmuje żadna wewnętrzna, ani zewnętrzna kontrola, a dane są pozyskiwane od operatorów bez konieczności uprzedniej decyzji sądu. Również po zakończeniu gromadzenia danych nie jest ani nie było możliwe zbadanie zasadności ich pozyskania, np. w drodze sądowej kontroli następczej. O ile dane nie dały podstawy do dalszych czynności przeciwko inwigilowanej osobie, jednostka której dane gromadzono nie jest informowana o podjęciu wobec niej takich czynności. Potencjalnie więc możliwe jest badanie danych każdej jednostki, także tej, co do której nie istnieje żadne podejrzenie popełnienia jakiegokolwiek przestępstwa.

Regulacja taka jest niezgodna z Konstytucją RP oraz Europejską Konwencją o Ochronie Praw Człowieka i Podstawowych Wolności oraz Kartą Praw Podstawowych. Niewątpliwie istnieje konieczność ukształtowania prawa krajowego tak, aby stanowiło kompromis pomiędzy wymogami walki z przestępczością i zapewnienia bezpieczeństwa a respektowaniem praw jednostki. Jednak ani dotychczasowe ustawodawstwo, ani praktyka polskich władz publicznych nie chroniły w wystarczającym stopniu jednostek przed nadmierną lub

nieuzasadnioną inwigilacją. Przepisy nie zawierały także ograniczenia możliwości sięgania po dane lub wykorzystanie danych telekomunikacyjnych dotyczących dziennikarzy, lekarzy, adwokatów, radców prawnych czy notariuszy. Skutkowało to tym, iż w jednej z prowadzonych kontroli wobec dziennikarza, stwierdzono, iż jego informatorzy nie korzystają z ochrony tajemnicy dziennikarskiej, a zatem można badać i ustalać ich dane telekomunikacyjne, przez co niewątpliwie doszło do naruszenia, wbrew stanowisku władz, tajemnicy dziennikarskiej. Dane te są uzyskiwane przy okazji kontroli nie podlegającej ocenie sądu ani uprzedniej, ani następczej. Brak jest również konieczności uzyskania orzeczenia sądu na ewentualne odstępstwo od zachowania tajemnicy zawodowej, co pozostawia zbyt szeroki margines swobody służbom specjalnym.

Wskazane sytuacje jednoznacznie dowodzą, że aktualna ochrona praw jednostki w zakresie retencji danych w prawie europejskim nie jest wystarczająca, a pogarsza ją dodatkowo, niewłaściwa implementacja norm zawartych w dyrektywie, zmierzająca do nieproporcjonalnego ograniczenia wolności i swobód. Okoliczności te mają fundamentalne znacznie dla zapewnienia właściwego wykonywania prawa do obrony przez adwokatów, jak również prowadzenia korespondencji z klientami w sposób pozwalający zachować tajemnicę zawodową.

Mając na uwadze cele służące wprowadzeniu dyrektywy, koniecznym wydaje się jej zmiana poprzez skrócenie okresu retencji, a przede wszystkim doprowadzenie do zabezpieczania danych o połączeniach telekomunikacyjnych dopiero od momentu pojawienia się uzasadnionych podejrzeń o popełnienie przestępstwa przez daną osobę, nie zaś w odniesieniu do wszystkich osób. Celowym wydaje się także określenie katalogu przestępstw, który uzasadniałby gromadzenie danych, jak również doprecyzowanie kwestii kontroli zewnętrznej oraz powiadamiania jednostki o gromadzeniu jej danych. Niewątpliwie także konieczne jest zawarcie przepisów, pozwalających na pełną ochronę tajemnicy adwokackiej, umożliwiającej poszanowanie prawa do obrony oraz poszanowanie poufności, jaką powinny cechować się działania adwokata.