Agnieszka Grzelak,
dr nauk prawnych, adiunkt w Katedrze Prawa Europejskiego Szkoły Głównej Handlowej

Tezy wystąpienia
„Projekt dyrektywy a dotychczasowe regulacje w zakresie ochrony danych osobowych w obszarze współpracy policyjnej i sądowej w sprawach karnych”

Zastrzeżenie: niniejsze tezy mają charakter wyłącznie roboczy i odzwierciedlają osobiste poglądy autorki. Pełna wersja wystąpienia zostanie opublikowana w formie artykułu w jednym z czołowych czasopism prawniczych poświęconych prawu UE.

1. Wprowadzenie

W ramach wprowadzenia:
- Współpraca policyjna i sądowa w sprawach karnych – jak powszechnie wiadomo – rozwija się dynamicznie - dość wspomnieć o ogromnym rozroście prawodawstwa w ostatnich latach i reformach przewidzianych przez Traktat z Lizbony (praktycznie uwspólnotawiających ten obszar).
- Podejmowane są działania zmierzające do usprawnienia transgranicznej wymiany informacji istotnych dla ochrony porządku publicznego. Wprowadzenie zasady dostępności odzwierciedla bardziej ogólną tendencję do ułatwiania wymiany informacji istotnych dla ochrony porządku publicznego Zmiany te wymagają przyjęcia instrumentu prawnego, który zagwarantuje skuteczną ochronę danych osobowych we wszystkich państwach członkowskich Unii Europejskiej w oparciu o wspólne normy (minimalne?).
- Należy pamiętać, że przetwarzanie danych w ramach współpracy policyjnej i sądowej w sprawach karnych z samej swojej natury tworzy ryzyko dla jednostki i wymaga bardzo wysokiego poziomu ochrony. Każde odstępstwo od ogólnych zasad ochrony powinno być zatem szczegółowo uzasadnione, a miedzy interesem ochrony porządku publicznego a interesem ochrony praw jednostki powinien zostać zachowany równomierny – chociaż trudny do wyważenia – balans.

Na wstępie należy podkreślić trzy sprawy:

1) Po pierwsze, obecne ogólne ramy prawne w zakresie ochrony danych w tej dziedzinie są niewystarczające z przyczyn, o których powiem w dalszej części wystąpienia. W tym miejscu zaznaczę, że przede wszystkim obowiązująca nadal dyrektywa 95/46/WE[i] nie ma zastosowania do przetwarzania danych osobowych w przypadku tych rodzajów działalności, które nie były objęte zakresem ówczesnego prawa wspólnotowego, takich jak współpraca w sprawach karnych (art. 3 ust. 2 dyrektywy).

2) Po drugie, pomimo, że w większości państw członkowskich zakres przepisów wdrażających ww. dyrektywę czy też ogólnie dotyczących ochrony danych jest szerszy niż wymaga tego sama dyrektywa i nie wyłącza przetwarzania danych do celów ochrony porządku publicznego, przepisy krajowe w tym zakresie znacznie różnią się od siebie. Poziom ochrony praw jednostki w odniesieniu do przetwarzania danych przez właściwe organy we wszystkich państwach członkowskich powinien być jednakowy.

3) Po trzecie, standard minimum dotyczący ochrony danych w zakresie współpracy policyjnej i sądowej w sprawach karnych w Europie wyznacza obecnie konwencja nr 108 Rady Europy[ii]. która wiąże wszystkie państwa członkowskie, ale nie zapewnia wystarczająco szczegółowej ochrony (ma zbyt ogólny charakter, jest już nieco „przestarzała” w treści), a zalecenie Komitetu Ministrów Rady Europy R(87)15[iii] nie ma mocy wiążącej. Ponadto, Konwencja nie uwzględnia szczególnego charakteru wymiany danych przez organy policyjne i sądowe.

4) Po czwarte, należy podkreślić, że dane osobowe przetwarzane przez organy ścigania czy wymiaru sprawiedliwości są często danymi wrażliwymi i zostają one uzyskane przez organy policyjne i sądowe w wyniku postępowania prowadzonego w danej sprawie. Organy policyjne/ sądowe będą bardziej skłonne do wymiany tego rodzaju danych z organami innych państw członkowskich, gdy będą miały pewność, że poziom ochrony w innym państwie członkowskim jest wystarczający. Konieczne jest zatem zagwarantowanie poufności i bezpieczeństwa danych**,** a także ograniczenie dostępu do danych i ich dalszego wykorzystywania. Harmonizacja krajowych zasad w zakresie danych osobowych w dziedzinie policji i wymiaru sprawiedliwości, w tym odpowiednie zabezpieczenia dotyczące ochrony tych danych, mogą zatem zwiększać wzajemne zaufanie oraz skuteczność samej wymiany, a także gwarantować wysoki poziom ochrony jednostki.

2. Obecne ramy prawne – ochrona danych w odniesieniu do współpracy policyjnej i sądowej w sprawach karnych w prawie UE

Obowiązujący stan prawny jest skomplikowany i po części jest to rezultat systemu prawnego Unii Europejskiej przed Traktatem z Lizbony. W efekcie istnienia struktury filarowej UE, przetwarzanie danych osobowych w I filarze (w zakresie objętym dyrektywą 95/46/WE) zasadniczo objęło przetwarzanie „komercyjne”, czyli przetwarzanie danych dokonywane przez jednostki prywatne w ramach prowadzonej przez nie działalności. Przetwarzanie danych w ramach d. III filaru UE odnosi się natomiast do przetwarzania danych przez organy wymiaru sprawiedliwości i organy ścigania (policję, organy celne, sądy), wykonujące swoje obowiązki związane z zagwarantowaniem porządku i bezpieczeństwa publicznego.

W efekcie rozbicia, rozwój prawodawstwa w zakresie ochrony danych był nierównomierny**,** jeśli chodzi o dawny I i III filar UE. Przetwarzanie danych w I filarze zostało objęte spójnymi regulacjami, wynikającymi z ww. dyrektywy 95/46/WE. Od momentu jej przyjęcia dyrektywy, w ramach I filaru UE ukształtowało się całe *acquis*: prawodawstwo, instytucje (grupa art. 29, EIOD) czy też orzecznictwo ETS.

W przypadku d. III filaru UE rozwój prawodawstwa następował w odwrotnej kolejności z uwzględnieniem wskazanego wyżej standardu minimum. W ramach prawa UE rozwijały się zatem regulacje szczegółowe, dotyczące ochrony danych w szczególnych ramach prawnych – wymieniam te najistotniejsze:

- w ramach Systemu Informacyjnego Schengen – Konwencja wykonawcza do Układu z Schengen oraz obecnie akty prawne dotyczące SIS II, w szczególności decyzja 2007/533/WSiSW[iv];
- w ramach Europolu – decyzja 2009/371/WSiSW[v] (dawniej Konwencja o Europolu), ale także umowy zawierane przez Europol z p. III
- w ramach Eurojustu – decyzja 2002/187/WSiSW[vi], zmieniona w 2009 r.
- decyzja włączająca do prawa UE Konwencję z Prüm – 2008/615/WSiSW i 2008/616/WSiSW[vii],
- inne, również zawierające przepisy odnoszące się do ochrony danych:

- Konwencja o pomocy wzajemnej w sprawach karnych z 2000 r.
- decyzja ramowa 2006/960/WSiSW[viii] dotycząca wymiany danych wywiadowczych
- decyzje ramowe dotyczące ENA[ix], czy późniejsze – np. ECRIS[x] (wymiana informacji z rejestrów karnych)
- umowy międzynarodowe dotyczące przekazywania danych PNR[xi] i in.

Generalnie zatem nastąpiło odwrócenie kierunku rozwoju – prawodawstwo dotyczące ochrony danych w ramach d. III filaru UE rozwijało się *ad hoc:* zamiast przyjąć ogólny tekst prawny określający standard, a następnie później rozwiązania szczegółowe, potrzebne dla szczególnych instytucji, tu prawo rozwinęło się w odwrotnej kolejności. Dopiero w 2008 r. przyjęto **decyzję ramową 2008/977/WSiSW w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych**[xii], bardziej ogólną w tym sensie, że dotyczyła różnych aspektów współpracy policyjnej, ale nie ustanawiającą standardu postępowania ze względu na ograniczony zakres przedmiotowy jej zastosowania, o czym będzie mowa dalej.

Prace nad decyzją ramową w sprawie ochrony danych były żmudne, trudne i nieefektywne. Ogólne przyczyny ich podjęcia, ujmując w skrócie, były następujące:

- konwencja Rady Europy nr 108 z 1981 r. nie uwzględniała szczególnych potrzeb (współczesnych) dla wymiany danych między organami ścigania;
- pojawiały się nowe metody zbierania i przetwarzania danych – np. w ramach dyrektywy o retencji danych[xiii] i konieczne stało się dostosowanie przepisów do obowiązujących rozwiązań;
- regulacje sektorowe, szczególne, osiągnęły swój „pułap” – pojawiła się potrzeba zintegrowania całości rozproszonych rozwiązań.

Projektów decyzji ramowej było bardzo dużo – należy rozważyć, że pierwsze przewidywały bardzo szeroki zakres ochrony, oparty o postanowienia dyrektywy z 1995 r., gwarantujący podobne prawa i ochronę instytucjonalną (grupa robocza, krajowe organy nadzorcze). Problemem stała się jednak podstawa prawna – nie wszystkie państwa członkowskie zgodziły się, że podstawy traktatowe d. III filaru UE są wystarczające by przyjąć akt prawny, regulujący całościowo ochronę danych w tym obszarze. Ostatecznie uchwalony akt prawny nie przypominał już zupełnie pierwotnego projektu – został ograniczony przedmiotowo, a każda z zasad została otoczona wyjątkami, które powodowały w zasadzie brak kontroli nad jej stosowaniem. Dużo zastrzeżeń w trakcie prac legislacyjnych zgłaszał Europejski Inspektor Ochrony Danych, który cały czas postulował szeroki zakres regulacji i objęcie nim zarówno aspektu transgranicznego (przekazywania danych między państwami, co w efekcie nastąpiło), jak i krajowego (do czego nie doszło).

3. Problemy wynikające z decyzji ramowej 2008/977/WSiSW

Należy postawić pytanie: jakie problemy stwarza obowiązujący stan prawny (przepisy decyzji ramowej w sprawie ochrony danych czy obowiązujące szczególne regulacje) i następnie zastanowić się, czy przedstawiony w styczniu 2012 r. projekt dyrektywy odpowiada na te wyzwania - innymi słowy czy będzie miał swoją wartość dodaną w stosunku do obowiązującego stanu prawnego.

Podstawowe problemy:

1) decyzja ramowa ogranicza swój zakres przedmiotowy wyłącznie do transgranicznej wymiany danych

Jest to ograniczenie o charakterze podstawowym, pozostawiające poza zakresem regulacji przetwarzanie danych wewnątrz państw członkowskich – państwa mogą zatem regulować te kwestie w sposób dowolny (zgodny ze wskazanym w punkcie 1 minimum regulacji, wynikającym z Konwencji nr 108). Tego typu ograniczenie w praktyce jest trudne do przeprowadzenia, zwłaszcza że sprawy prowadzone są często w oparciu o dane pochodzące z różnych źródeł. Rodzi to również problemy z wdrażaniem tych postanowień[xiv] i jak się okazuje, w praktyce:

- niektóre państwa członkowskie w kwestii ochrony danych przetwarzanych w ramach współpracy policyjnej ogólnie odsyłają do ustawodawstwa dotyczącego ochrony danych (wykraczają poza to, co jest nakazane decyzją ramową),
- niektóre państwa uzupełniają ustawodawstwo o regulacje dotyczące policji czy wymiaru sprawiedliwości (w sposób niekoniecznie zgodny z ogólnymi standardami),
- w niektórych państwach te kwestie w ogóle nie są regulowane (czyli wdrożona jest jedynie decyzja ramowa w zakresie minimum).

2) W obowiązującej nadal decyzji ramowej w sprawie ochrony danych podstawowe zasady ochrony danych, ustanowione w Konwencji nr 108, są zachowane, jednak otoczone są szeregiem wyjątków. Dochodzi też do odejścia od treści zalecenia 87(15).
Przykładowo należy wskazać na:

- brak przepisu nakazującego usunięcie danych w przypadku dalszego ich przetwarzania;
- zbyt szerokie wyłączenia od zasady celowości;
- brak przepisów nakazujących wyróżnienie różnych kategorii danych, odpowiednio do stopnia ich poprawności i wiarygodności;
- brak przepisów nakazujących wyróżnienie danych opartych na faktach/opiniach/ocenach;
- brak przepisów wprowadzających rozróżnienie między różnymi kategoriami osób, których dane dotyczą (podejrzany, świadek, ofiara) - potrzebne z jednej strony dla ochrony tych osób, ale z drugiej – dla pełnego wykorzystania tych danych;
- brak przepisów określających specjalne gwarancje dotyczące danych odnoszących się do osób spoza kręgu osób podejrzanych;
- brak przepisów dotyczących przetwarzania danych genetycznych na potrzeby postępowania karnego czy procedury sądowej[xv].

3) Decyzja ramowa nie zastępuje różnych – wskazanych w punkcie 2 niniejszego referatu - **sektorowych aktów** zawierających albo rozwiązania szczegółowe (odmienne od przewidzianych w decyzji ramowej) albo odsyłające do Konwencji 108 i zalecenia 87 (15).

Decyzja ramowa pozostawia obowiązujące wszystkie wcześniej przyjęte akty prawne. Rodzi to szereg niejasności, pozostawia też wiele pola do interpretacji. Powoduje brak pewności prawnej i niejasność co do konsekwencji prawnych. W art. 29 decyzja ramowa stanowi o pierwszeństwie w przypadku aktów przyjętych przed jej wejściem w życie, tymczasem szereg aktów jednak przyjęty został już po wejściu w życie decyzji ramowej, np. decyzja ramowa 2009/314/WSiSW (która w ogóle nie odnosi się do decyzji ramowej w sprawie ochrony danych), decyzja 2009/316/WSiSW (w przypadku której decyzja ramowa w sprawie ochrony danych ma zastosowanie do komputerowej wymiany danych między państwami członkowskim), decyzja 2009/371/WSiSW (określająca szczególne zasady przetwarzania danych, uwzględniające specyfikę tej instytucji) czy też decyzja ramowa 2009/948/WSiSW (odwołująca się do decyzji ramowej w sprawie ochrony danych w przypadku wymiany danych). W efekcie, pomiędzy regulacjami pojawiają się rozbieżności, utrudniające ich stosowanie. Jedynie przykładowo można wskazać na różnice:

a) w zakresie pojęcia „dane osobowe”

Definicja danych osobowych zawarta w art. 2a decyzji ramowej 2008/977/WSiSW jest zbieżna z definicją zawartą w dyrektywie 95/46/WE, ale już np. definicja zawarta w decyzji dotyczącej SIS II (art. 3d) jest taka sama jedynie w części ogólnej, natomiast nie precyzuje, co oznacza pojęcie „możliwej do zidentyfikowania osoby”.

b) ograniczenia w zasadzie celowości

Dyrektywa 95/46/WE określa, że dane mogą być zbierane tylko do określonych, jednoznacznych i legalnych celów i zakazuje przetwarzania w sposób niezgodny z tymi celami. Z kolei decyzja ramowa w sprawie ochrony danych reguluje tę kwestię podobnie (art. 3), ale jednak pozostawia państwom członkowskim prawo do bardziej szczegółowego określenia, jakie jeszcze cele należy uznać za niezgodne z celem, do którego dane będą pierwotnie gromadzone. Decyzja 2008/615/WSiSW stanowi zaś, że chociaż przetwarzanie danych jest dozwolone wyłącznie dla celów, dla których dane zostały pierwotnie przekazane, to jednak przetwarzanie w innych celach jest również dopuszczalne. Takie sformułowania oznaczają, że w praktyce dane osobowe, przetwarzane przez właściwe organy policyjne w jednym państwie i przekazywane do innego państwa mogą być przetwarzane dla celów innych niż te, dla których pierwotnie zostały zgromadzone.

c) prawo dostępu do danych

Zgodnie z art. 17 decyzji ramowej 2008/977/WSiSW, każda osoba, której dane dotyczą ma prawo otrzymać przynajmniej potwierdzenie, że dane zostały przekazane lub udostępnione oraz informacje o odbiorcy lub przynajmniej potwierdzenie ze strony krajowego organu nadzoru, że dokonano wszystkich koniecznych weryfikacji. Z kolei zarówno decyzja dotycząca Eurojustu, jak i decyzja o Europolu zawierają przepisy określające prawo dostępu do danych. W przypadku pozostałych aktów prawnych, jedynie decyzja dotycząca SIS II i decyzja 2008/615/WSiSW zawierają ogólne, odsyłające do prawa krajowego, przepisy dotyczące dostępu do danych.

Te różnice można mnożyć – czy to w odniesieniu do zakresu przekazywanych informacji czy też podstawy prawnej do przetwarzania i in.

4) W zakresie procedury przekazywania danych do państw trzecich, uregulowanej w art. 13 decyzji ramowej – podstawowy podnoszony zarzut dotyczy pozostawienia oceny adekwatności systemu państwa trzeciego samym państwom członkowskim. Decyzja ramowa nie określa żadnych precyzyjnych przesłanek pozwalających jednoznacznie ustalić kryteria dokonywania takiej oceny i w efekcie praktyka państw członkowskich w tym zakresie jest rozbieżna.

5) Kolejny problem - decyzja ramowa w sprawie ochrony danych nie dotyczy przetwarzania danych przez podmioty, które nie są organem policyjnym lub sądowym, a które przetwarzają dane w związku z porządkiem publicznym (jak np. przewoźnicy lotniczy, przetwarzający dane PNR na potrzeby walki z terroryzmem).

6) Brak kompetencji Komisji w sytuacji, w której decyzja ramowa nie jest wdrożona prawidłowo lub w ogóle przez państwa członkowskie, tymczasem poziom wdrożenia nawet tego minimum, jak wynika ze sprawozdania KOM(2012) 12 wersja ostateczna, nie jest zadowalający.

7) W odniesieniu do ochrony danych w d. III filarze, na poziomie UE nie działa żaden organ na wzór np. Grupy roboczej art. 29.

Komisja Europejska dostrzegła problemy wynikające z decyzji ramowej, już bowiem w komunikacie z 2010 r.[xvi] podkreśla się brak regulacji dla omawianego obszaru, szeroki zakres wyjątków w zakresie podstawowych standardów ochrony, a także brak precyzyjnego określenia relacji miedzy istniejącymi instrumentami prawnymi.

4. Założenia reformy – kwestie ogólne

W dniu 25 stycznia 2012 r. Komisja przedstawiła dwa projekty: rozporządzenia ogólnego[xvii] i – będącej przedmiotem referatu - dyrektywy Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych przez właściwe organy do celów zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich i ścigania albo wykonywania kar kryminalnych oraz swobodnego przepływu tych danych[xviii].

Stało się to możliwe, ponieważ pojawiły się nowe ramy traktatowe (art. 16 TFUE), stwarzając podstawę prawną dla przyjmowania norm dotyczących ochrony danych również w obszarze współpracy policyjnej i sądowej w sprawach karnych[xix]. Komisja przygotowując projekt dyrektywy miała do wyboru realistycznie dwie opcje:

1) przedstawić jeden, spójny, ustanawiający standardy tekst, który będzie określał zasady ogólne przetwarzania danych w UE,
2) kontynuować rozróżnienie między podejściem ogólnym, a podejściem szczególnym dla spraw związanych z bezpieczeństwem.

Komisja zdecydowała się na wybór opcji nr 2. Stworzenie całościowego systemu ochrony danych nie wyklucza szczególnych przepisów w sektorze policyjnym/sądowym. Zgodzić należy się zatem i ocenić pozytywnie to, że przyjęta będzie osobna regulacja – akt ten dotyczy bowiem dziedziny, w której ochrona danych musi niewątpliwie być uregulowana w sposób szczególny, chociażby ze względu na konieczność przechowywania danych w długim okresie, konieczność ciągłego porównywania danych z napływającymi informacjami, brak dostępu podejrzanych do danych na swój temat, problem profilowania itp. Te szczególne cechy skutkują koniecznością przyjęcia szczególnych uregulowań. W relacji do systemu ogólnego, określonego w projekcie rozporządzenia, projekt dyrektywy przyjmuje – jak się wydaje - podejście wyważone: z jednej strony bowiem określa szczególne warunki przetwarzania danych w tym obszarze (art. 5 czy art. 6), ale również zastosowanie znajdą ogólne zasady (a nie wyjątki od nich).

Dużym znakiem zapytania pozostaje wybór instrumentu prawnego: **dlaczego w przypadku systemu ogólnego będziemy mieć do czynienia z rozporządzeniem, a więc aktem obowiązującym bezpośrednio, tu zaś z dyrektywą**, która będzie musiała być wdrożona do porządku krajowego państw. W takiej sytuacji na pewno nie będzie mowy o jednolitych ramach prawnych dla całego systemu ochrony danych osobowych w UE. Należy wskazać, że może to spowodować nierówności w systemie ochrony danych między państwami (które znów w różny sposób wdrożą poszczególne, niejasne – o czym dalej – przepisy), ale i tak jest bardzo pozytywnym krokiem naprzód w stosunku do obowiązującej decyzji ramowej. Na dodatek rodzi to pewne trudności praktyczne: art. 49 projektu dyrektywy określa zadania Europejskiej Rady Ochrony Danych, czyli organu, którego zadania nie powinny wynikać z aktu, który dopiero musi zostać wdrożony do prawa krajowego, lecz z aktu obowiązującego bezpośrednio (rozporządzenia lub może decyzji).

5. Wstępna ocena przedstawionych przepisów/ założeń projektu dyrektywy

Większość ogólnych – systemowych - problemów wskazanych w odniesieniu do decyzji ramowej zostanie uregulowana. Z uzasadnienia wynika, że tam, gdzie to możliwe dyrektywa powtarza postanowienia projektu rozporządzenia oraz dyrektywy z 1995 r., także wprowadza inne propozycje Komisji, które nie były wcześniej uwzględnione na etapie prac nad projektem decyzji ramowej z 2008 r. Nie wszystkie propozycje jednak budzą optymizm.

Przykłady rozwiązań problematycznych:

5.1. W art. 2 ust. 3 projektu dyrektywy przewidziano ograniczenia jej zakresu przedmiotowego - nie znajdzie ona zastosowania w ramach działalności wykraczającej poza zakres prawa Unii, w szczególności dotyczącej bezpieczeństwa narodowego. Jest to niewątpliwie pokłosie art. 72 i 73 TFUE, pozostawiającego pewne kwestie z zakresu bezpieczeństwa wewnętrznego i narodowego kompetencjom państw członkowskich. Problemem może być tutaj samo zdefiniowanie pojęcia „bezpieczeństwo narodowe” – każde z państw może postrzegać ten termin odmiennie, o czym pisałam w komentarzu do TFUE.

Jest to jednak bardzo poważny sygnał wskazujący na niepełność regulacji i możliwość wprowadzenia pewnych wyłomów w jednolitym systemie współpracy. Wymaga to dalszej analizy, ale może to świadczyć o tym, że projekt nie reguluje w pełni krajowego przetwarzania danych. Postęp zatem jest o tyle, że projekt dyrektywy nie ogranicza się wyłącznie do transgranicznego przekazywania danych. O jednolitości systemu w całej UE raczej jednak mowy nie będzie.

5.2. Dyrektywa ani nie uchyli (czego właściwie nie spodziewałam się), **ale nawet nie ustanowi hierarchii** między obowiązującymi aktami prawnymi. Wręcz przeciwnie - pozostawia bez uszczerbku wcześniej przyjęte akty prawne w tym zakresie (art. 59 projektu), a zatem zamiast ujednolicać system – będziemy mieć nadal mnogość aktów prawnych regulujących współpracę w sprawach karnych. **To zdecydowanie stoi w sprzeczności z postulatem stworzenia jednolitych ram prawnych.** Co prawda, projekt przewiduje konieczność dokonania przeglądu aktów, ale dopiero 3 lata po wejściu w życie dyrektywy (art. 61 ust. 2) – jest to zdecydowanie za długi okres, zwłaszcza że obowiązujące przepisy pozostają w sprzeczności.

5.3. Problem rozdziału przetwarzania danych na potrzeby komercyjne od przetwarzania danych na potrzeby bezpieczeństwa nie jest zasadniczo rozwiązany zwłaszcza, że dane przechowywane w systemach komercyjnych mogą być wykorzystywane dla potrzeb organów ścigania (przykład: retencja danych telekomunikacyjnych), ale może być też odwrotnie – gdy policja będzie udostępniała dane na inne cele niż zwalczanie przestępczości. Orzecznictwo ETS tu nie pomaga, bo – przykładowo - chociaż przekazywanie danych pasażerów (PNR) jest uznawane za powiązane z bezpieczeństwem, to jednak *de facto* stanowi przetwarzanie komercyjne (zwłaszcza dokonywane przez linie lotnicze).

W efekcie – należałoby odwrócić logikę - kryterium regulacji (przetwarzania) powinny stanowić dane, a nie organ przetwarzający. **Dyrektywa tego problemu nie podnosi.**

Dyrektywa praktycznie w ogóle nie reguluje kwestii dostępu policji do danych w sektorze prywatnym. To poważny brak, na który zresztą zwrócił już uwagę EIOD w swoim pierwszym prasowym oświadczeniu z 25 stycznia 2012 r. na temat tego projektu.

5.4. Pozytywnie należy ocenić kwestie instytucjonalne, w szczególności powołanie Europejskiej Rady Ochrony Danych, której przyznane zostaną kompetencje w zakresie ochrony danych w omawianym obszarze. To było od dawna postulowane.

Ponadto, Komisja proponuje poddanie przetwarzania danych kontroli krajowego organu nadzorczego. Wprowadzenie nadzoru krajowego organu ochrony danych jest bardzo ważne, przy zastrzeżeniu, że będzie miał mandat do efektywnej kontroli. Tu można mieć pewne wątpliwości, chociażby z tego powodu, że w art. 44 projektu spod kontroli wyłącza się sądy, które – przy całej specyfice niezawisłości – nie są zwolnione z ochrony danych.

Inne problemy:

- nie wiadomo, dlaczego w projekcie dyrektywy nie wprowadzono *data protection impast assessment*, zwłaszcza że takie ustalenia podjęła Rada na posiedzeniu 24 lutego 2011 r.
- w art. 23 ust. 2 projektu inaczej niż w art. 28 ust. 2 projektu rozporządzenia reguluje się zobowiązania nałożone na administratora i podmioty przetwarzające - czy na pewno jest uzasadnienie dla zróżnicowania?
- znaczące różnice w uprawnieniach organów nadzorczych między art. 53 projektu rozporządzenia a art. 46 projektu dyrektywy – również bez uzasadnienia;
- różnice między art. 47 projektu dyrektywy a art. 54 projektu rozporządzenia – dlaczego sprawozdania nie mają być udostępniane parlamentom narodowym, zwłaszcza, że obowiązek taki potwierdzony jest orzecznictwem ETS (sprawa C-518/07 Komisja p. Niemcy)

5.5. W odniesieniu do konkretnych propozycji szczegółowych należy zauważyć, że:

Projekt dyrektywy podzielony jest na 11 rozdziałów, każdy regulujący szczególny aspekt ochrony danych.

Rozdział I – określa przepisy ogólne, w tym zakres przedmiotowy dyrektywy, rozszerzając ją na krajowe przetwarzanie danych (art. 2 ust. 1). W rozdziale tym zawarte są również definicje, w tym zupełnie nowe, takie jak naruszenie danych osobowych, dane genetyczne (ważne – uwzględnienie orzecznictwa ETPCz) czy dane biometryczne.

Projekt dyrektywy definiuje również **pojęcie „właściwego organu”** – bardzo szeroko, jako każdy organ publiczny właściwy do celów zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich lub ścigania oraz wykonywania kar. Na marginesie, przypuszczam, że organy, które w Polsce do tej pory nie podlegały kontroli GIODO będą protestowały przeciwko takiemu ujęciu. Należy jednak zwrócić uwagę, że w obu przedstawionych projektach termin ten powinien być stosowany jednakowo, a tymczasem w projekcie dyrektywy znajduje się wskazanie, że chodzi o organ „publiczny” (tego nie ma w projekcie rozporządzenia – art. 2 ust. 2 lit. e projektu rozporządzenia).

Rozdział II – określa zasady dotyczące przetwarzania danych osobowych, w większości przypadków powtarzając zasady wynikające z dyrektywy z 1995 r. i z projektu rozporządzenia. Z kwestii szczególnych wskazać należy przepis określający rozróżnianie kategorii osób, których dane dotyczą (świadkowie, skazani, ofiary itp.) – jest to wystąpienie naprzeciw postulatom wyżej – art. 5 projektu, chociaż **nie ma żadnych wskazówek, w jaki sposób to rozróżnienie powinno być potraktowane, tzn. co dalej z tego wynika i jakie są konsekwencje.** Brakuje chyba również ogólnej kategorii osób „niepodejrzanych”. Nie jestem również pewna, czy konieczne jest sformułowanie „w możliwym zakresie” – co to może bowiem oznaczać?

W projekcie podkreśla się znaczenie zasady minimalizmu, ogólny zakaz dotyczący przetwarzania szczególnych danych osobowych (w art. 8 – chociaż tu również brakuje wskazówek co do konsekwencji poza ogólnym sformułowaniem w punkcie 26 preambuły), czy też środki oparte na profilowaniu (art. 9 – o tym dalej). **Generalnie zatem większość wątpliwości, które pojawiały się w odniesieniu do decyzji ramowej zostają w projekcie dyrektywy usunięte, tyle tylko że gwarantowany projektem dyrektywy poziom ochrony nie jest nadal satysfakcjonujący, chociażby dlatego, że szereg przepisów budzi**

wątpliwości w zakresie spójności z projektem rozporządzenia. Ogólnie zatem jest niewątpliwie postęp wobec obowiązujących regulacji, ale czy nie ma zbyt dużych rozbieżności w relacji do projektu rozporządzenia?

Przykłady:

- w art. 4 projektu dyrektywy, stanowiącym odpowiednik art. 5 projektu rozprządzenia, różnice dotyczą zasady celowości. W szczególności, nie ma wyjaśnienia, co może oznaczać „przetwarzanie niezgodne z celami”. W preambule do projektu rozporządzenia jest próba wyjaśnienia, ale w projekcie dyrektywy nie ma odpowiedniego sformułowania w preambule. Pojawia się zatem pytanie, czy dalsze przetwarzanie danych w celu zwalczania przestępczości (ale innym niż cel pierwotny) będzie dopuszczalne? Nie powinno.
- niejasna jest również relacja między art. 4b a art. 7 projektu dyrektywy, w szczególności b, c i d. Może trzeba jednak te przepisy na nowo doprecyzować? Na przykład stworzyć przepisy dotyczące legalnego przetwarzania danych, w celach określonych, dozwolonych, początkowych – a dopiero później przepisy dotyczące możliwości przetwarzania danych na cele które są niezgodne z celem pierwotnym? Postulować należy zatem zastąpienie art. 7 pkt b-d jednym jasnym przepisem, wskazującym ogólne przesłanki zezwalające na odstąpienie od zasady ogólnej. Ponadto, co prawda w art. 7 lit. b projektu przewidziano, że państwa członkowskie będą gwarantować przetwarzanie danych wyłącznie w sytuacji, gdy jest to niezbędne do wypełnienia obowiązku ciążącego na administratorze, to jednak nie ma tutaj określonych żadnych szczególnych gwarancji. Trzeba wskazać, że w tym zakresie zasada 5 Zalecenia 87(15) jest o wiele dalej idąca – czyżby zatem regres również wobec istniejących (chociaż nie wiążących) standardów minimalnych?
- W projekcie dyrektywy nie ma przepisu o legalności przetwarzania danych dla celów naukowych czy historycznych (jest w rozporządzeniu).
- Nie ma przepisu dotyczącego okresu przechowywania danych – por. zasada 7 zalecenia 87(15).
- Nie ma przepisu na wzór art. 5f projektu rozporządzenia, dotyczącego konieczności udowodnienia dla każdej operacji – jej zgodności z przepisami dyrektywy. W projekcie dyrektywy mowa jest wyłącznie o zapewnieniu zgodności (art. 4f), a nie o udowodnieniu zgodności.
- Art. 6 projektu dyrektywy, dotyczący różnego poziomu dokładności i wiarygodności danych to ważny przepis, bo w przypadku przetwarzania danych przez odpowiednie służby, często dochodzi do oparcia wniosków o przypuszczenia, a nie o fakty. Jednak użycie sformułowania „na ile to możliwe” zdecydowanie osłabia skuteczność tego przepisu.

Prawa podmiotu danych określa **rozdział III projektu dyrektywy**, w tym prawo do informacji, dostęp do danych czy możliwość sprzeciwu wobec przetwarzania danych. Generalnie propozycje należy ocenić pozytywnie, zwłaszcza w kontekście obowiązującej decyzji ramowej. Nie sposób jednak nie wskazać dalszych wątpliwości, np.:

- W przeciwieństwie do projektu rozporządzenia (art. 12 ust. 2) – w art. 10 ust. 4 projektu dyrektywy nie określa się limitu czasowego dla administratora do poinformowania osoby o sposobie reakcji na wniosek – mowa jest o „niezwłoczności”, podczas gdy rozporządzenie określa jeden miesiąc. Oznacza to praktycznie osłabienie praw jednostki. Ponadto, w art. 10 ust. 5 projektu używa się pojęcia „wnioski dokuczliwe” – co to znaczy? Dlaczego nie użyto pojęcia z projektu rozporządzenia? I jeszcze – zasada 5 rekomendacji 87(15) szerzej określa obowiązki administratora (tu brak).
- Ograniczenie praw jednostki – oczywiście z racji tematyki ograniczenia muszą iść dalej niż w systemie ogólnym, tyle że ograniczenia powinny być niezbędne i proporcjonalne.

Pozytywnie zatem należy ocenić art. 11 ust. 4 i art. 13 projektu dyrektywy. Pewne wątpliwości można wyrazić co do braku w art. 15 i 16 przyczyn ograniczających wskazane tam prawa.

– W art. 16 projektu dyrektywy - różnica w stosunku do projektu rozporządzenia art. 17 ust. 4 i ust. 5 – administrator zamiast usunąć dane oznacza je, podczas gdy w rozporządzeniu mowa jest o ograniczeniu przetwarzania – tu chyba konieczne jest dostosowanie.

Rozdziały **IV, VI i VII** to przepisy wykonawcze, związane z administratorem i podmiotem przetwarzającym, niezależnymi organami nadzorczymi czy też przepisy dotyczące współpracy państw. Uzupełniają je przepisy rozdziału **VIII** (środki ochrony prawne, odpowiedzialność, sankcje) oraz przepisy dotyczące międzynarodowego transferu danych (rozdział **V** – tu też można podnieść szereg dalszych wątpliwości, chociaż pozytywnie należy ocenić to, że to Komisja oceniać ma adekwatność poziomu ochrony, a nie państwa członkowskie).

5.6. *Last, but not least* – profilowanie

Nie odnosząc się do rozróżnienia w terminologii, profilowanie można odnaleźć w kilku aktach (projektach aktów) UE (np. w projekcie dyrektywy w sprawie europejskiego systemu PNR[xx]), co ma związek z podejmowaniem działań zapobiegających aktom kryminalnym i atakom terrorystycznym, jeszcze zanim będą miały miejsce. W tych przypadkach nie ma jednak mowy o ochronie danych jednostek. Wspomniany projekt dyrektywy dotyczący EU-PNR w art. 11 nie stanowi nic o warunkach przetwarzania danych. Również ani decyzja ramowa w sprawie ochrony danych ani dyrektywa 95/46/WE nie odnosiły się do tego tematu w sposób szczególny, ale raczej jednostkowo (w art. 7 i odpowiednio w art. 15) – mówiąc o automatycznych decyzjach w sprawie jednostki. Ogólnie zatem należy stwierdzić, że profilowanie nabiera praktycznego znaczenia, jest coraz częściej wykorzystywane, jednak nie rozwijało się do tej pory prawodawstwo zapewniające adekwatny poziom ochrony danych.

Projekt dyrektywy odnosi się do kwestii profilowania bezpośrednio w art. 9, próbując w szczególności sformułować definicję profilowania: środki oparte wyłącznie na automatycznym przetwarzaniu danych mającym służyć ocenie niektórych aspektów o charakterze osobistym podmiotu danych. Projekt wydaje się zatem ograniczać profilowanie wyłącznie do operacji *ad hoc* – wyklucza chyba również np. profilowanie nie oceniające, lecz po prostu identyfikujące dane. Pewną wątpliwość budzi sama definicja profilowania i ograniczenie w niej niekorzystnych skutków dla podmiotu danych wyłącznie do skutków prawnych, a przecież niekorzystne skutki mają najczęściej skutek faktyczny.

Wydaje się, że zastosowane podejście ma charakter realistyczny – jest to niewątpliwie postęp w stosunku do aktualnego stanu rzeczy. Uwzględnia, że istnieje konieczność profilowania, ale jednocześnie poddaje je pewnym warunkom. Wydaje się, że najważniejszym jest to, że nie może opierać się na danych sensytywnych. Wymaga również od państw członkowskich przyjęcia określonych przepisów – ocenie będzie podlegać zgodność takich przepisów z postanowieniami dyrektywy.

6. Wnioski

1. Temat ochrony danych w ramach współpracy w sprawach karnych dyskutowany już od kilku lat. Wzrostowi regulacji z zakresu bezpieczeństwa nie towarzyszyły przepisy dotyczące efektywnej ochrony danych. Dopiero w 2008 r. pojawiła się decyzja

ramowa w sprawie ochrony danych. W tym kontekście projekt dyrektywy należy ocenić pozytywnie (z pewnymi wątpliwościami wskazanymi wyżej), bowiem ma ona objąć zarówno aspekt krajowy, jak i transgraniczny – czyli ustanowić standard minimum przetwarzania danych.

2. Ochrona danych w ramach współpracy policyjnej i sądowej w sprawach karnych cechuje się pewnymi odmiennościami, które uzasadniają odróżnienie zasad od innych domen. W projekcie dyrektywy Komisja odnotowuje te różnice, ale jednocześnie próbuje zrównać poziom ochrony z systemem ogólnym, chociaż – nie wydaje się – by wystarczająco skutecznie. Problemy zasadnicze: dlaczego zaproponowano dyrektywę? Dlaczego pojawiają się różnice w standardzie ochrony między rozporządzeniem a dyrektywą (które nie mają wyraźnego uzasadnienia)? I wreszcie – dlaczego pewne prawa jednostek są osłabione w projekcie dyrektywy w porównaniu do rozporządzenia?

3. Na tym etapie można stwierdzić, że projekt – jeśli stanie się obowiązującym prawem - przyczyni się do poprawy praw jednostki w zakresie ochrony danych przynajmniej w tych państwach, które do tej pory stosownych regulacji nie posiadały. Wyposaża podmioty w środki które umożliwią im efektywną ochronę danych. Jest to szczególnie istotne w kontekście nowych wyzwań, prowadzących do profilowania i rozmaitych sieci danych. Docenić zatem należy objęcie projektem procedur krajowych, ale będzie to mieć znaczenie o tyle, o ile faktycznie – co nie jest pewne - wzrośnie poziom ochrony. Wydaje się zatem, że projekt jest krokiem naprzód, ale w niektórych momentach – zwłaszcza, gdy następuje odejście od zalecenia Komitetu Ministrów Rady Europy 87(15) – również krokiem w tył.

4. Zasadniczo projekt dyrektywy ma odpowiedzieć na wskazane wyżej problemy, której pojawiają się w odniesieniu do projektu decyzji ramowej. Pozytywnie należy ocenić przejęcie podstawowych zasad z dyrektywy 95/46/WE. Niektórych kwestii jednak w ogóle nie uregulowano - postulować można chociażby odwrócenie ciężaru dowodu na korzyść jednostki albo prawo do bycia poinformowanym o zakończeniu przetwarzania danych w sytuacji, w której nie ma już potrzeby prowadzenia dalszego postępowania. Z kwestii ogólniejszych pojawia się pytanie dotyczące braku *Impact assesment.*

5. Pewien niepokój budzi przekazanie kompetencji Komisji do wydawania aktów delegowanych, chociaż w projekcie dyrektywy tylko w jednym miejscu - w odniesieniu do doprecyzowania kryteriów i wymogów dotyczących stwierdzenia naruszenia danych osobowych – art. 28. To jest bardzo ważne zagadnienie i brak konkretnych przepisów lub chociażby założeń takiego aktu zdecydowanie utrudnia całościową ocenę rozwiązania.

6. Proces legislacyjny w sytuacji istnienia wielu wątpliwości i przełomowego charakteru projektu, będzie bardzo trudny zarówno na poziomie UE, jak i na poziomie krajowym, bowiem zmiany mają charakter dość głęboki.

[i] Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, Dz. Urz. UE L 281, 23.11.1995, s. 31

[ii] Konwencja nr 108 Rady Europy sporządzona w Strasburgu dnia 28 stycznia 1981 r. o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych (Dz.U. z 2003 r. Nr 3, poz. 25), uzupełniona Protokołem dodatkowym (Dz. U. z 2005 r. Nr 11, poz. 1).

[iii] Rekomendacja R(87) 15 z dnia 17 września 1987 r. dotycząca ochrony danych osobowych wykorzystywanych w sektorze policji.

[iv] Decyzja Rady 2007/533/WSiSW z dnia 12 czerwca 2007 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji (SIS II), Dz. Urz. L 205 z 7.8.2007, s. 63-84

[v] Decyzja Rady z dnia 6 kwietnia 2009 r. ustanawiająca Europejski Urząd Policji (Europol), Dz. Urz. UE L 121, 15.5.2009, s. 37 – 46.

[vi] Decyzja Rady z dnia 28 lutego 2002 r. ustanawiająca Eurojust w celu zintensyfikowania walki z poważną przestępczością, Dz. Urz. 63, 6.3.2002, s. 1-13 oraz późniejsze zmiany

[vii] Decyzja Rady 2008/615/WSiSW z dnia 23 czerwca 2008 r. w sprawie intensyfikacji współpracy transgranicznej, szczególnie w zwalczaniu terroryzmu i przestępczości transgranicznej, Dz. Urz. L 219 z 6.8.2008, str. 1—11 oraz Decyzja Rady 2008/616/WSiSW z dnia 23 czerwca 2008 r. w sprawie wdrożenia decyzji 2008/615/WSiSW w sprawie intensyfikacji współpracy transgranicznej, szczególnie w zwalczaniu terroryzmu i przestępczości transgranicznej, Dz. Urz. L 210 z 6.8.2008, str. 12—72

[viii] Decyzja ramowa Rady 2006/960/WSiSW z dnia 18 grudnia 2006 r. w sprawie uproszczenia wymiany informacji i danych wywiadowczych między organami ścigania państw członkowskich Unii Europejskiej, Dz. Urz. UE L 386, 29.12.2006, s. 89-100

[ix] Decyzja ramowa Rady z dnia 13 czerwca 2002 r. w sprawie europejskiego nakazu aresztowania i procedury wydawania osób między Państwami Członkowskimi, Dz. Urz. L 190 z 18.7.2002, s. 1—20

[x] Decyzja ramowa Rady 2009/315/WSiSW z dnia 26 lutego 2009 r. w sprawie organizacji wymiany informacji pochodzących z rejestru karnego pomiędzy państwami członkowskimi oraz treści tych informacji, Dz. Urz. L 93 z 7.4.2009, s. 23—32.

[xi] Por. Komunikat Komisji w sprawie globalnego podejścia do przekazywania danych dotyczących przelotu pasażera (PNR) państwom trzecim, KOM(2010) 492 wersja ostateczna.

[xii] Decyzja ramowa Rady 2008/977/WSiSW z dnia 27 listopada 2008 r. w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych, Dz. Urz. L 350 z 30.12.2008, s. 60; dalej jako: decyzja ramowa w sprawie ochrony danych

[xiii] Tu trzeba dodać, że Rada obiecała Parlamentowi Europejskiemu podczas prac nad tą dyrektywą przyjęcie decyzji ramowej regulującej ochronę danych – dyrektywa nakłada obowiązki na podmioty prywatne związane z przechowywaniem danych na cele – ogólnie – szeroko postępowania karnego, bez zapewnienia minimum harmonizacji w zakresie ochrony danych.

[xiv] Por. sprawozdanie z wdrożenia decyzji ramowej przedstawione przez Komisję również w dniu 25 stycznia 2012 r. (KOM(2012) 12 wersja ostateczna).

[xv] Konieczność ochrony danych wynika z orzecznictwa ETPCz, m.in. w sprawie *Marper*.

[xvi] KOM(2010) 609 wersja ostateczna.

[xvii] KOM(2010) 9 wersja ostateczna.

[xviii] KOM(2012) 10 wersja ostateczna.

[xix] Warto zauważyć, że w deklaracji nr 21 dołączonej do Aktu końcowego konferencji międzyrządowej 2007, państwa członkowskie zgodziły się, że w zakresie współpracy policyjnej i sądowej w sprawach karnych dla ochrony danych może być potrzebna szczególna regulacja prawna.

[xx] KOM(2011) 32 wersja ostateczna.