GRUPA ROBOCZA DS. OCHRONY DANYCH POWOŁANA NA MOCY ART. 29

02316-02/09/PL
WP 165

Opinia 6/2009 w sprawie stopnia ochrony danych osobowych w Izraelu

Przyjęta dnia 1 grudnia 2009 r.

Grupa robocza ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych

uwzględniając dyrektywę 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 (zwaną dalej „dyrektywą"), w szczególności jej art. 29 i art. 30 ust. 1 lit. b),

uwzględniając regulamin wewnętrzny grupy roboczej, w szczególności jego art. 12 i 14,

PRZYJMUJE NINIEJSZĄ OPINIĘ:

1. KONTEKST

Dnia 12 lipca 2007 r. Misja Izraela przy Unii Europejskiej złożyła wniosek do Komisji o wszczęcie procedury stwierdzenia, że Izrael zapewnia odpowiedni stopień ochrony w zakresie przewidzianym w art. 25 i art. 26 dyrektywy.

Aby zbadać, czy Izrael zapewnia odpowiedni stopień ochrony, Komisja zwróciła się do *Centre de Recherches Informatique et Droit* (zwanego dalej „CRID") z Uniwersytetu w Namur o przedstawienie obszernego sprawozdania analizującego, czy izraelski system prawny spełnia wymogi dotyczące stosowania przepisów o ochronie danych osobowych określonych w dokumencie roboczym „Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU data protection Directive", przyjętym przez grupę roboczą utworzoną na mocy art. 29 dyrektywy dnia 24 lipca 1998 r. (dokument WP12).

Wyżej wspomniane sprawozdanie oraz wstępna odpowiedź udzielona przez władze Izraela były przedmiotem dyskusji podgrupy ds. „bezpiecznej przystani" w czasie posiedzenia w dniu 18 marca 2009 r.

Na posiedzeniu podgrupa przedłożyła do zaopiniowania przez grupę roboczą wniosek przesłania przez przewodniczącego podgrupy pisma do władz izraelskich, które pozytywnie oceniając istniejący system ochrony danych w Izraelu, podkreśla kwestie wymagające dalszego wyjaśnienia.

Dnia 2 września 2009 r. władze izraelskie, poprzez Izraelski Urząd ds. Prawa, Informacji i Technologii (zwany dalej „ILITA"), przesłały grupie roboczej obszerne sprawozdanie, w którym udzieliły odpowiedzi na kwestie podniesione we wspomnianym piśmie.

Sprawozdanie to zostało przeanalizowane przez członków podgrupy i było przedmiotem posiedzenia w dniu 16 września 2009 r., na którym wysłuchano władze izraelskie. W czasie posiedzenia członkowie podgrupy poprosili władze izraelskie, reprezentowane przez Dyrektora ILITA oraz Dyrektora Departamentu Prawnego, o wyjaśnienie kwestii, które po wcześniejszym omówieniu sprawozdania przesłanego podgrupie wymagały jeszcze dalszych wyjaśnień.

Podgrupa poinformowała grupę roboczą, na posiedzeniu zorganizowanym w dniach 12-13 października 2009 r., o wnioskach ze spotkania w dniu 16 września oraz zaproponowała przyjęcie poniższej opinii, na zawartych w niej warunkach. Wniosek został przyjęty przez grupę roboczą na wspomnianym posiedzeniu.

2. PRAWO OCHRONY DANYCH W IZRAELU

Izraelski system prawny charakteryzuje się dwoma kluczowymi elementami, które odróżniają go od innych systemów prawnych oraz w szczególności od systemów prawnych państw członkowskich: po pierwsze Izrael nie posiada spisanej Konstytucji; po drugie, chociaż jego system można uznać za fundamentalnie związany z systemami prawnymi opartymi na zasadzie „common law", zawiera on pewne cechy wskazujące na wpływ prawa kontynentalnego.

Brak spisanej Konstytucji zastępuje istnienie tzw. „Praw podstawowych", którym Sąd Najwyższy Izraela nadał status konstytucyjny. Równocześnie status konstytucyjny mają również pewne podstawowe zasady i podstawowe prawa człowieka, takie jak równość, swoboda wypowiedzi czy wolność wyznania.

W tych ramach prawo do prywatności ujęto w sekcji 7 Praw podstawowych: Godność i wolność człowieka, które stanowi co następuje:

> *a) Wszyscy mają prawo do prywatności i intymności.*
> *b) Nie wolno wchodzić na teren prywatny osoby, która nie wyraziła na to zgody.*
> *c) Nie wolno prowadzić przeszukania na terenie prywatnym osoby ani rewizji osobistej czy też przeszukania rzeczy osobistych.*
> *d) Nie wolno naruszać poufności rozmowy czy też zapisków bądź dokumentów danej osoby.*

Równocześnie prawo do prywatności i ochrony danych osobowych reguluje Ustawa o ochronie prywatności (zwana dalej „UOP"), przyjęta w 1981 r. i poddana dziewięciu późniejszym zmianom. W 2007 r. przyjęto najistotniejszą zmianę, która ustanowiła nowe wymogi w zakresie przetwarzania danych osobowych oraz uregulowała organizację, uprawnienia i funkcje organu kontrolnego w zakresie ochrony danych osobowych bardziej szczegółowo i z większą precyzją niż czyniło to dotąd obowiązujące prawodawstwo, ustanawiając organ w ramach Ministerstwa Sprawiedliwości − Izraelski Urząd ds. Prawa, Informacji i Technologii (ILITA), który obejmuje wcześniejszego Rejestratora Baz Danych.

Ponadto zwrócono należytą uwagę na raport sporządzony w styczniu 2007 r. przez komitet ekspertów powołany przez Ministerstwo Sprawiedliwości, zwany „Raportem Schoffmana", w którym zawarto szereg zaleceń dotyczących zmiany prawodawstwa w zakresie ochrony danych. Są one obecnie rozpatrywane w celu przyjęcia nowych ram w zakresie ochrony danych.

Wreszcie prawodawstwo w zakresie ochrony danych, jeżeli chodzi o prawo pisane, dopełnia szereg decyzji przyjętych przez rząd izraelski, szczególnie w odniesieniu do wykonania UOP (na przykład w zakresie międzynarodowych transferów danych), jak również w odniesieniu do organizacji i funkcjonowania ILITA (na przykład w odniesieniu do czasu trwania i przyczyn ustania mandatu dyrektora ILITA).

Co więcej, jak wskazano powyżej, izraelski system prawny opiera się, w dużej mierze, na zasadach charakterystycznych dla systemów prawnych typu „common law". To dlatego spisane regulacje muszą w każdym wypadku być uzupełnione o wydane zgodnie z nimi wyroki, które mają wartość precedensową i stanowią bezpośrednio część źródeł prawa izraelskiego. W sprawozdaniu, o które wnioskował Komitet i które zostało sporządzone przez władze izraelskie, jak również w oświadczeniach wydanych przez te władze podczas spotkania wyjaśniającego przeprowadzonego przez podgrupę dnia 16 września 2009 r., grupie roboczej przedstawiono szereg postanowień sądowych, które muszą zostać uwzględnione przy ocenie, której ma dokonać grupa robocza.
Wreszcie, w niniejszej ocenie wstępnej należy zaznaczyć, że Izrael ratyfikował Międzynarodowy pakt praw obywatelskich i politycznych z 1966 r., chociaż w prawie izraelskim ratyfikacja umowy międzynarodowej nie oznacza bezpośredniego włączenia do prawa krajowego.

3. OCENA PRAWA OCHRONY DANYCH IZRAELA POD KĄTEM ODPOWIEDNIEGO STOPNIA OCHRONY DANYCH OSOBOWYCH

Grupa robocza podkreśla, że jej ocena odpowiedniego poziomu prawa ochrony danych w Izraelu skupia się na Ustawie o ochronie prywatności (UOP).

Przepisy ustawy, jak również orzecznictwo sądowe w zakresie ochrony danych osobowych, porównano z głównymi przepisami dyrektywy, uwzględniwszy opinię WP12 grupy roboczej. Opinia ta wyszczególnia szereg zasad, które stanowią „trzon" zasad materialnych w zakresie ochrony danych oraz wymogów „proceduralnych lub w zakresie egzekwowania prawa", zgodność z którymi można uznać za minimalny wymóg ochrony uznawany za odpowiedni".

3.1 Zakres przepisów regulujących ochronę danych w prawie izraelskim.

Podobnie jak w niektórych wcześniejszych przypadkach, grupa robocza uważa, że przed przystąpieniem do szczegółowej oceny spełnienia zasad zapisanych w dokumencie WP12 konieczne jest zbadanie zakresu zastosowania przepisów w zakresie ochrony danych w prawie izraelskim.

a) Pojęcie danych lub „informacji" osobowych.

W szczególności grupa robocza uważa za niezbędne uwzględnienie pojęcia „informacji osobowych", o którym mowa w UOP, oraz jego związku z pojęciem „danych osobowych" zapisanym w dyrektywie. Podobnie, konieczne będzie ustalenie, czy prawo izraelskie ustanawia odpowiednie środki ochrony danych w odniesieniu do ich przetwarzania lub czy wspomniane uregulowanie dotyczy jedynie całkowicie lub częściowo zautomatyzowanych systemów przetwarzania, uwzględniając ramy ochrony ustanowione na mocy dyrektywy.

W odniesieniu do pierwszej kwestii grupa robocza potwierdza, że definicja „informacji", o której mowa w sekcji 7 UOP, nie jest podobna do definicji zawartej w dyrektywie. Wspomniany powyżej przepis stwierdza zatem, że „informacje oznaczają dane na temat tożsamości, statusu osobowego, spraw intymnych, stanu zdrowia, sytuacji ekonomicznej, kwalifikacji zawodowych, opinii i przekonań danej osoby". Definicja ta odnosi się jedynie do niektórych kategorii danych i nie daje wiedzy, czy informacje dotyczące osoby niezidentyfikowanej ale możliwej do zidentyfikowania byłyby chronione na mocy UOP.

Jednakże grupa robocza uwzględnia wyjaśnienia złożone w tej kwestii przez władze izraelskie oraz, w szczególności, precedensy sądowe przedstawione przez nie, które oznaczają rozszerzenie prawnego pojęcia informacji, czyniąc je podobnym do pojęcia „danych o charakterze osobowym" przewidzianych w dyrektywie.

W szczególności wniosek taki nasuwa się wobec niektórych postanowień, jak to wydane przez Sąd Najwyższy Izraela w sprawie *Izrael przeciwko Bank Ha'Po'alim*, w którym stwierdzono, że „termin informacje (...) powinien obejmować dane, które można uzyskać z bazy danych, która nie jest indeksowana według poszczególnych nazwisk".

Grupa robocza, poza resztą dostarczonych postanowień, za szczególnie istotne uznaje orzecznictwo wynikające z postanowienia w sprawie *Rani Mor przeciwko Ynet* Sądu Okręgowego w Hajfie, odnoszącego się do adresu IP, gdzie wniosek z tego postanowienia można przyrównać do wniosku grupy roboczej, wskazując, że „identyfikowanie użytkownika on-line poprzez ujawnienie jego adresu IP bez jego zgody może stanowić naruszenie prywatności".

Stąd też w odniesieniu do pojęcia danych osobowych lub „informacji" na potrzeby zastosowania uregulowania dotyczącego ochrony danych, grupa robocza uważa, że orzecznictwo uzupełniło to, co ustanowiła UOP, umożliwiając z tej perspektywy uznanie środków ochronnych zapewnianych przez to prawo za ramy ochronne w odniesieniu do pojęcia danych osobowych, podobnego do pojęcia przewidzianego w dyrektywie.

b) Chronione systemy przetwarzania w prawie izraelskim.

Grupa robocza musi się odnieść w tym momencie do szczególnej struktury UOP, a w szczególności, do jej pierwszych dwóch rozdziałów: rozdział 1 odnosi się do naruszeń prywatności w ujęciu ogólnym, natomiast rozdział 2 reguluje ochronę prywatności w bazach danych.

Jeżeli chodzi o rozdział drugi, sekcja 7 UOP definiuje bazę danych jako „zbiór danych, przechowywany na nośniku magnetycznym lub optycznym i przeznaczony do przetwarzania komputerowego". W ten sposób system gwarancji ustanowiony w rozdziale 2 będzie miał zastosowanie wyłącznie do przypadków, w których ma miejsce zautomatyzowane przetwarzanie informacji, a nie do przypadków, w których zautomatyzowane przetwarzanie nie występuje.

Grupa robocza zwraca uwagę na wyjaśnienia złożone przez władze izraelskie, które stwierdziły, że obywatele są chronieni przed niezautomatyzowanym przetwarzaniem danych (lub przetwarzaniem ręcznym) przez środki ochronne ustanowione w rozdziale 1 UOP, w którym odzwierciedlono pewne zasady, takie jak ograniczenie celu, zachowanie tajemnicy i zgoda.

Niemniej jednak warto przypomnieć, że ochrona zapewniona przez dyrektywę tym rodzajom przetwarzania odnosi się nie tylko do wspomnianych zasad, ale do całokształtu systemu, a w szczególności do zasad zawartych w dokumencie WP12. Dlatego też, aby móc uznać stopień ochrony danych danego państwa w odniesieniu do niezautomatyzowanych systemów przetwarzania za odpowiedni, prawo krajowe danego państwa musiałoby respektować, przynajmniej w odniesieniu do tych systemów przetwarzania, wspomniane wyżej zasady.

Z tego powodu, ponieważ rozdział 1 nie uwzględnia wszystkich wspomnianych zasad, nie jest możliwe uznanie prawodawstwa izraelskiego za odpowiednie w odniesieniu do niezautomatyzowanych lub ręcznych systemów przetwarzania. W związku z tym grupa robocza chciałaby przypomnieć, że w „Raporcie Schoffmana" wysnuto ten sam wniosek, proponując reformę ram prawnych obowiązujących w Izraelu, polegającą na poszerzeniu wszystkich środków ochrony danych o ręczne systemy przetwarzania.

Dlatego też grupa robocza uważa, że analiza prawidłowości systemu ochrony danych w Izraelu nie może odnosić się do niezautomatyzowanego przetwarzania danych, gdyż wspomniane ramy nie ustanawiają środków ochrony przewidzianych w dokumencie WP12.

W tym względzie grupa robocza chce również wyjaśnić, że uważa, iż może kontynuować swoją analizę prawidłowości stopnia ochrony w odniesieniu do całkowicie lub częściowo zautomatyzowanych systemów przetwarzania. Dlatego też nie należy uznawać za wykluczone z analizy przeprowadzonej od tego momentu międzynarodowych transferów danych do Izraela, które są dokonywane środkami zautomatyzowanymi ani tych, które pomimo iż nie zostały dokonane wspomnianymi środkami, dotyczą danych, które później będą poddane zautomatyzowanemu przetwarzaniu w państwie Izrael.

Dlatego też z niniejszej oceny wyłączone będą jedynie te międzynarodowe transfery danych, w ramach których zarówno sam transfer, jak i późniejsze przetwarzanie danych, odbywa się wyłącznie w sposób niezautomatyzowany, gdyż jedynie w tych przypadkach przepisy rozdziału 1 UOP nie mają zastosowania.

Grupa robocza ma świadomość, że wielkość transferów wykluczonych z oceny odpowiedniego stopnia ochrony będzie szczątkowa i nie będzie miała znaczącego wpływu na stosowanie decyzji, która może zostać ostatecznie przyjęta; jednakże grupa robocza uważa, że istotną rzeczą jest dokonanie wspomnianego wyjątku w świetle przepisów dyrektywy. Jednocześnie grupa robocza zaleca przyjęcie przepisów przewidujących zastosowanie prawodawstwa izraelskiego do ręcznych baz danych, w ramach wprowadzanych w przyszłości zmian legislacyjnych, w szczególności tych związanych z wykonaniem zaleceń „Raportu Schoffmana"; umożliwi to rozszerzenie, w stosownych przypadkach, oceny na te systemy przetwarzania.

3.2. Zasady materialne

Uwzględniając powyższe spostrzeżenia, przejdziemy teraz do oceny stopnia ochrony danych w Izraelu w świetle zasad zawartych w dokumencie WP12, zaczynając od omówienia zawartych zasad, których powinno przestrzegać prawodawstwo państwa Izrael.

a) Zasady podstawowe

1) Zasada ograniczenia celu. Dane powinny być przetwarzane w konkretnym celu, a następnie wykorzystywane lub przekazywane dalej tylko pod warunkiem, że nie jest to niezgodne z celem ich przekazania. Jedynymi wyjątkami od tej zasady są wyłączenia konieczne w demokratycznym społeczeństwie z ważnych względów wymienionych w art. 13 dyrektywy.

Grupa robocza jest zdania, iż prawodawstwo izraelskie respektuje tę zasadę. Stąd ogólnie rzecz ujmując, art. 2 ust. 9 UOP stwierdza, iż „wykorzystywanie lub przekazywanie innej osobie informacji dotyczących spraw prywatnych danej osoby w celu innym niż ten, dla którego została ona udzielona" stanowi naruszenie prywatności.

Tę generalną zasadę potwierdza nawet art. 8 lit. b) ustawy, która przewiduje, że „danej osobie nie wolno wykorzystywać informacji zawartych w bazie danych, która wymaga rejestracji na mocy niniejszej sekcji, z wyjątkiem celu, dla którego ustanowiono daną bazę danych".

Ponadto w przypadkach, w których baza danych została zarejestrowana w organie kontrolnym, art. 9 lit. b pkt 2) UOP stwierdza, że wniosek musi wyszczególniać „cele, do których baza danych została ustanowiona oraz cele, do których informacja jest przeznaczona".

Grupa robocza potwierdza również, że sądy interpretują te przepisy podobnie, jak to przewiduje dyrektywa. W szczególności uwzględnia ona zakaz niezgodnego z przepisami wykorzystywania danych finansowych, do którego odniósł się Sąd Najwyższy Izraela w sprawie *Rejestrator Baz Danych przeciwko Ventura*.

> **2) Zasada jakości i proporcjonalności danych.** Dane powinny być dokładne i w stosownych przypadkach aktualizowane. Dane powinny być odpowiednie, rzeczowe oraz niewykraczające poza potrzeby wynikające z , dla których są one przekazywane lub dalej przetwarzane.

W odniesieniu do zasady jakości sensu stricte, grupa robocza uważa, że chociaż nie wymienia się jej jako niezależnej zasady, prawo izraelskie uznaje obowiązek przechowywania dokładnych danych oraz, w stosownych przypadkach, uaktualniania ich w ramach przepisu dotyczącego prawa do sprostowania, o którym mowa w sekcji 14 UOP.

W literze a) wspomnianej sekcji stwierdza się zatem, że „osoba, która dokonując wglądu do informacji na swój temat, stwierdzi, że nie są one poprawne, kompletne, jasne lub aktualne, może zwrócić się z wnioskiem do właściciela bazy danych lub, jeżeli właściciel nie jest rezydentem, do posiadacza takiej bazy danych o zmianę lub usunięcie informacji".

Litery b) i c) odnoszą się do decyzji właściciela bazy danych. Dlatego też „w przypadkach, w których właściciel bazy danych pozytywnie rozpatrzy wniosek na mocy litery a), dokonuje on niezbędnych zmian w informacjach i powiadamia o nich wszystkich, którzy otrzymali te informacje od niego w terminie przewidzianym przepisami".

W przypadku odmowy właściciel musi poinformować o tym osobę, której dotyczą dane, przytaczając sekcję 15, na mocy której „osoba zwracająca się z wnioskiem o udzielenie informacji może odwołać się od odmowy kontroli przez właściciela bazy danych na mocy sekcji 13 lub sekcji 13A oraz od zawiadomienia o decyzji odmownej na mocy sekcji 14 lit. c) do sądu pokoju w formie i w sposób przewidziany przepisami".

W odniesieniu do zasady proporcjonalności wynikającej z art. 6 ust. 1 lit. c) dyrektywy, grupa robocza potwierdza, że zasada ta nie jest wyraźnie uznawana w UOP. Jednakże grupa robocza z zadowoleniem przyjmuje wyjaśnienia i orzecznictwo przekazane przez władze izraelskie w związku z tą kwestią, które uzupełniają w znacznym stopniu wspomniane braki.

Grupa robocza uznaje zatem za satysfakcjonujące wyjaśnienia udzielone w odniesieniu do konstytucjonalnego zakresu zasady proporcjonalności, gdy przetwarzanie danych odbywa się w sektorze publicznym. W szczególności za wyjątkowo istotne uznaje prawo precedensowe wynikające z orzeczenia Sądu Najwyższego ogłoszonego w sprawie *Acri przeciwko Ministrowi Spraw Wewnętrznych,* przekazanego przez władze izraelskie, w którym znajduje się wyraźne odniesienie do uwzględnienia zasady proporcjonalności w rozumieniu dyrektywy.

Na tej samej zasadzie grupa robocza z zadowoleniem przyjmuje wyjaśnienia udzielone przez władze izraelskie w odniesieniu do prawnego wymogu proporcjonalności w przetwarzaniu, w oparciu o zasady zasadności środka i dobrej wiary. W tym sensie za szczególnie interesujący uznaje precedens ustanowiony w sprawie *Eisner przeciwko Richmond,* który ograniczył użycie kamer wideo w miejscu pracy oraz przez osoby trzecie na mocy wyroku Krajowego Sądu Pracy w Tel Awiwie. Grupa robocza również uznaje za istotne stosowanie zasady proporcjonalności w ramach ochrony konsumenta, jak również postanowienia sądowe, w których właściwe sądy oraz w szczególności Standardowy Sąd Kontraktowy w Jerozolimie unieważniły klauzule umożliwiające wymianę informacji w ramach grup biznesowych, jak w sprawie *Bank of Israel przeciwko First International Bank of Israel*.

W świetle powyższego orzecznictwa grupa robocza uważa, że zasada proporcjonalności została zagwarantowana w większości przypadków, w których możliwe byłoby zastosowanie nieproporcjonalnego przetwarzania danych osobowych oraz, w szczególności, że zasada proporcjonalności jest zasadą konstytucyjną, której należy przestrzegać podczas każdego przetwarzania danych w sektorze publicznym lub w sektorze prywatnym podczas wykonywania zadań publicznych.

Niemniej jednak grupa robocza uważa, że bardziej satysfakcjonującym rozwiązaniem byłoby, gdyby prawodawstwo izraelskie wyraźnie uwzględniło tę zasadę w celu zagwarantowania, aby działania wchodzące w zakres sektora prywatnego oraz różniące się od tych, co do których wydano już orzeczenia sądowe w oparciu o zasady zasadności i dobrej wiary, mogły w przyszłości sprostać problemom wykładni, które mogłyby utrudnić odpowiednią ochronę praw zainteresowanych osób fizycznych. W związku z tym grupa robocza przypomina, że uwzględnienie tej zasady w ramach UOP zostało zawarte we wnioskach „Raportu Schoffmana".

Tym samym, mimo że powyższy wniosek nie ma wpływu na ostateczną ocenę poziomu ochrony w państwie Izrael, grupa robocza uważa, że przyszłe zmiany legislacyjne, a w szczególności te związane z wykonaniem „Raportu Schoffmana", powinny uwzględniać przyjęcie przepisów przewidujących wyraźne zastosowanie zasady proporcjonalności w odniesieniu do ogółu przetwarzania danych osobowych w sektorach publicznym i prywatnym.

> **3) Zasada przejrzystości.** Osobom fizycznym należy zapewnić informacje na temat celu przetwarzania danych oraz tożsamości administratora danych w państwie trzecim, a także wszelkie inne informacje w zakresie niezbędnym do zapewnienia sprawiedliwego traktowania. Jedynymi dopuszczalnymi wyjątkami od tej zasady powinny być wyłączenia zgodne z art. 11 ust. 2 pkt 3 oraz art. 13 dyrektywy.

Grupa robocza uważa, że prawodawstwo państwa Izrael w wystarczający sposób wypełnia tę zasadzę.

Sekcja 11 UOP stanowi, że:

> „Do wniosku skierowanego do danej osoby o udzielenie informacji w celu ich przechowania i wykorzystywania w bazie danych należy dołączyć powiadomienie wskazujące
> (1) czy osoba ta ma prawny obowiązek udzielenia takich informacji lub czy ich udzielenie jest zależne od jej woli i zgody;
> (2) cel, w jakim składany jest wniosek o udzielenie tych informacji;
> *(3)* komu takie informacje mają być udzielone oraz cele udzielenia informacji."

Ponadto zgodnie z sekcją 13A ust. 1 UOP „właściciel bazy danych, który przechowuje ją w miejscu należącym do innej osoby (w niniejszej sekcji – posiadacza), odsyła osobę składającą wniosek do posiadacza, wraz z podaniem jego adresu, i pisemnie nakazuje posiadaczowi umożliwienie wglądu osobie składającej wniosek". Podobnie, zgodnie z ust. 2 „w przypadku gdy osoba składająca wniosek w pierwszej kolejności zwróci się do posiadacza, posiadacz informuje ją o tym, czy posiada dotyczące jej informacje, jak również podaje nazwisko i adres właściciela bazy danych".

> **4) Zasada bezpieczeństwa.** Administrator danych powinien podejmować techniczne i organizacyjne środki bezpieczeństwa, które są odpowiednio dostosowane do ryzyka związanego z przetwarzaniem. Żadnej osobie działającej z upoważnienia administratora danych, włącznie z osobą przetwarzającą dane, nie wolno przetwarzać ich bez instrukcji pochodzących od administratora danych.

Grupa robocza uważa, że państwo Izrael gwarantuje tę zasadę, uwzględniając w szczególności przepisy sekcji 16, 17, 17A i 17B UOP.

Sekcja 7 definiuje „bezpieczeństwo informacji" jako „ochronę integralności informacji lub ochronę przed ujawnieniem, wykorzystaniem lub kopiowaniem informacji bez prawnego zezwolenia", a sekcja 17 dodaje, że „właściciel bazy danych, posiadacz bazy danych i zarządzający ponoszą odpowiedzialność za bezpieczeństwo informacji w bazie danych".

Artykuł 17B w szczególności stanowi, że niektórzy właściciele bazy danych lub osoby ją przetwarzające muszą wyznaczyć odpowiednio wykwalifikowaną osobę nadzorującą bezpieczeństwo, która będzie odpowiedzialna za zadania związane z bezpieczeństwem.

Ponadto art. 16 uregulował obowiązek zachowania poufności w przetwarzaniu informacji, stanowiąc, że „zabronione jest ujawnianie jakichkolwiek informacji uzyskanych w związku z pełnieniem funkcji pracownika, administratora lub posiadacza bazy danych w celu innym niż wykonywanie obowiązków służbowych lub wdrażanie ustawy bądź na mocy nakazu sądu w związku z postępowaniem prawnym; w przypadku złożenia wniosku przed wszczęciem postępowania zostanie on rozpatrzony w sądzie pokoju". Niezastosowanie się do tego obowiązku podlega karze pozbawienia wolności do lat pięciu.

Wreszcie w art. 17A UOP jest mowa o posiadaczu; artykuł ten stanowi, co następuje:

> „a) Osoba, która posiada bazy danych różnych właścicieli zapewnia, aby dostęp do każdej bazy danych był udzielany jedynie osobom, które są do tego wyraźnie upoważnione na podstawie pisemnej umowy pomiędzy tą osobą a właścicielem konkretnej bazy danych.

b) Osoba, która posiada co najmniej pięć baz danych wymagających rejestracji zgodnie z sekcją 8 przekazuje corocznie Rejestratorowi listę baz danych znajdujących się w jej posiadaniu, ze wskazaniem nazwisk/nazw właścicieli tych baz danych, potwierdzonym pisemnym oświadczeniem, iż w odniesieniu do każdej z tych baz danych osoby uprawnione do dostępu do bazy danych zostały określone w drodze umowy pomiędzy tą osobą a właścicielem, oraz ze wskazaniem nazwiska osoby nadzorującej bezpieczeństwo, o której mowa w sekcji 17B."

5) **Prawo dostępu, sprostowania i sprzeciwu:** osoba, której dotyczą dane, powinna mieć prawo do otrzymania kopii wszystkich przetwarzanych danych, które jej dotyczą oraz prawo do sprostowania tych danych, gdy okażą się one nieprawidłowe. W niektórych sytuacjach wspomniana osoba powinna mieć również możliwość wniesienia sprzeciwu wobec przetwarzania danych, które jej dotyczą. Jedynymi wyjątkami od tych praw powinny być wyłączenia zgodne z art. 13 dyrektywy.

Sekcja 13 lit. a) UOP stanowi, że „każdy ma prawo wglądu, bądź to osobiście bądź też poprzez upoważnionego przez siebie na piśmie przedstawiciela lub swojego opiekuna, do wszelkich informacji na swój temat przechowywanych w bazie danych", z zastrzeżeniem sekcji 13 lit. b), która przewiduje, iż „właściciel bazy danych umożliwia, na wniosek osoby, o której mowa w lit. a) (zwanej dalej „osobą składającą wniosek"), wgląd do informacji w języku hebrajskim, arabskim lub angielskim".

W odniesieniu do prawa do sprostowania, sekcja 14 lit. a) UOP, poddana już analizie powyżej, stanowi, że „osoba, która dokonując wglądu do informacji na swój temat, stwierdzi, że nie są one poprawne, kompletne, jasne lub aktualne, może zwrócić się z wnioskiem do właściciela bazy danych lub, jeżeli właściciel nie jest rezydentem, do posiadacza bazy danych o zmianę lub usunięcie informacji".

Niespełnienie obowiązków nałożonych na administratorów na mocy powyższych sekcji stanowi przestępstwo zgodnie z art. 31 i może powodować odpowiedzialność cywilną wobec osoby, której dotyczą dane, zgodnie z sekcją 31B. Sekcje te zostaną omówione bardziej szczegółowo w dalszej części niniejszej opinii.

Jeżeli chodzi o prawo do sprzeciwu, sekcja 17F UOP wyraźnie ustanawia to prawo w odniesieniu do działań marketingu bezpośredniego, jak zostanie to przedstawione w dalszej części.

Wobec powyższego grupa robocza potwierdza, że prawodawstwo izraelskie nie ustanawia tego prawa w drodze ogólnej klauzuli. Przewiduje ono jednak, iż zgodnie z UOP dane mogą być gromadzone jedynie w ograniczonym celu (sekcja 8 lit. b), sekcja 2 ust. 9), o którym osoba, której dotyczą dane, została poinformowana (sekcja 11). Dlatego grupa robocza uważa, że osoba, której dotyczą dane, może sprzeciwić się przetwarzaniu danych argumentując, że przetwarzanie takie wykracza poza cel, do którego dane te były gromadzone lub że nie została ona o nim należycie poinformowana. W takim przypadku nadużycie w zakresie przetwarzania danych uznaje się za naruszenie prywatności na mocy sekcji 2 ust. 9 UOP, za przestępstwo na mocy sekcji 31A lit. a) pkt 1 oraz niedopełnienie wymogu informacyjnego, co stanowi przestępstwo na mocy sekcji 31A lit. a) pkt 3.

Sekcja 15 UOP stanowi ponadto, iż „do sądu pokoju w formie i w sposób przewidziany przepisami osoba zwracająca się z wnioskiem o udzielenie informacji może odwołać się od odmowy kontroli przez właściciela bazy danych na mocy sekcji 13 lub sekcji 13A oraz od zawiadomienia o decyzji odmownej na mocy sekcji 14 lit. c) do sądu pokoju w formie i w sposób przewidziany przepisami".

Wreszcie grupa robocza uważa, że wyłączenia dotyczące wykonywania prawa do dostępu, a tym samym do sprostowania, przewidziane w sekcji 13 lit. c) UOP, są zgodne z tymi zawartymi w art. 13 dyrektywy, które dotyczą państw członkowskich. W tym sensie grupa robocza pozytywnie ocenia orzecznictwo sądów w odniesieniu do wykonywania wspomnianych wyżej praw, a w szczególności orzeczenie wydane przez Sąd Najwyższy w sprawie *Fischler przeciwko Komendantowi Policji,* w którym osobie, której dotyczyły dane, przyznano prawo zapoznania się z informacjami na swój temat, zawartymi w aktach policyjnych.

Grupa robocza uważa zatem, że prawodawstwo państwa Izrael w wystarczającym stopniu gwarantuje prawa osób, których dotyczą dane, do dostępu do swoich danych, do wnioskowania o ich sprostowanie lub do sprzeciwu wobec ich przetwarzania, zgodnie z warunkami zawartymi w dokumencie WP12.

> **6) Ograniczenia w zakresie dalszego przekazywania danych:** dalsze przekazywanie danych osobowych przez odbiorcę pierwotnego przekazania danych powinno być dozwolone tylko w przypadku, gdy drugi odbiorca (tj. odbiorca kolejnego przekazania danych) również podlega przepisom gwarantującym prawidłowy stopień ochrony. Jedynymi dopuszczalnymi wyjątkami powinny być wyjątki zgodne z art. 26 ust. 1 dyrektywy (wyłączenia te zostały omówione w rozdziale piątym).

Oceniając zgodność z niniejszą zasadą, grupa robocza uwzględnia przepisy rozporządzeń dotyczących ochrony prywatności (przekazywanie baz danych za granicę) przyjęte przez rząd Izraela dnia 17 czerwca 2001 r.

Rozporządzenia te zakazują przekazywania danych do krajów trzecich, chyba że kraje te zapewniają stopień ochrony danych nie niższy niż stopień ustanowiony w prawie izraelskim, w szczególności w odniesieniu do kilku podstawowych zasad, takich jak zgodne z prawem gromadzenie i przetwarzanie danych, ograniczenie celu, jakość danych (dokładność i aktualność danych), poszanowanie prawa dostępu (a w konsekwencji, zgodnie z prawodawstwem izraelskim, prawa do sprostowania) oraz bezpieczeństwo danych.

Rozporządzenie 2 ust. 8 wyszczególnia kilka przypadków, które można uznać za domniemanie prawne odpowiedniego stopnia ochrony, obejmując państwa członkowskie, kraje będące stroną Konwencji 108 Rady Europy lub kraje, „w przypadku których Rejestrator Baz Danych ogłosił, że osiągnięto porozumienie z urzędem ds. ochrony prywatności państwa trzeciego".

Ustępy 1-7 rozporządzenia 2 przewidują szereg wyłączeń od tych ogólnych zasad:

- „jeżeli osoba, której dotyczą dane wyraziła zgodę.
- jeżeli nie można uzyskać zgody, a istotne jest przekazanie danych celem ochrony zdrowia danej osoby.

- jeżeli dane są przekazywane [zagranicznej] korporacji będącej własnością właściciela [miejscowej] bazy danych, a ten zagwarantował ochronę danych.
- jeżeli odbiorca danych zobowiązał się zapewnić ochronę danych, tak jak gdyby były one przechowywane w Izraelu.
- jeżeli dane są publicznie dostępne na mocy ustawowego upoważnienia.
- jeżeli przekazanie jest istotne z punktu widzenia ochrony porządku publicznego i bezpieczeństwa.
- jeżeli przekazanie jest wymagane na mocy prawa izraelskiego."

Rozporządzenie 3 zawiera zasadę odpowiedzialności, zgodnie z którą strona przekazująca powinna zadbać o otrzymanie od odbiorcy danych gwarancji, podjęto wystarczające środki celem zabezpieczenia danych oraz że dane nie będą przekazywane dalej.

Grupa robocza uważa również, że wymienione przepisy są zgodne z zasadą ograniczenia dalszego przekazywania danych oraz że gwarancje udzielone przez prawodawstwo izraelskie w tej kwestii umożliwiają zagwarantowanie odpowiedniego poszanowania praw obywateli Unii Europejskiej, których dane są przetwarzane w Izraelu.

Jednakże grupa robocza chciałaby przypomnieć kryteria interpretacyjne dotyczące wyłączeń ustanowionych w art. 26 ust. 1 dyrektywy i zawartych w dokumencie roboczym w sprawie wspólnej wykładni art. 26 ust. 1 dyrektywy 95/46/WE z dnia 24 października 1995 r. (dokument WP114) oraz zaleca władzom izraelskim dokonywanie wykładni wyłączeń zawartych we wspomnianej powyżej regule 2, zgodnie z kryteriami zawartymi we wspomnianym dokumencie i samej dyrektywie.

b) Zasady uzupełniające

Dokument WP12 odnosi się do pewnych zasad, które należy stosować w odniesieniu do określonych systemów przetwarzania, z naciskiem na:

> **1) Dane szczególnie chronione –** w przypadku kategorii danych „szczególnie chronionych" (wymienionych w art. 8 dyrektywy) należy zapewnić dodatkowe zabezpieczenia, takie jak wymóg udzielenia wyraźnej zgody na przetwarzanie danych, przez osobę, której dane dotyczą.

Sekcja 7 UOP zawiera pojęcie „danych szczególnie chronionych", które definiuje jako:

> „1. dane dotyczące tożsamości, spraw intymnych, stanu zdrowia, sytuacji ekonomicznej, opinii i przekonań osoby;
> 2. informacje, które zgodnie z nakazem Ministra Sprawiedliwości, za zgodą Komisji Knesetu ds. Konstytucji, Prawa i Sprawiedliwości, są informacjami szczególnie chronionymi.";

Grupa robocza uważa, że mimo iż powyższa lista nie pokrywa się w pełni z listą określoną w art. 8 dyrektywy, można ją uznać za podobną. W szczególności przyjmuje się, że informacje odnoszące się do opinii i przekonań obejmują znaczną część danych wymienionych we wspomnianym artykule. Ponadto grupa robocza wzywa władze izraelskie do uznania za informacje szczególnie chronione, nie tylko dlatego, że należą one do kategorii „spraw intymnych", te informacje, które odnoszą się do danych wymienionych w art. 8 dyrektywy, a

które nie mogą być uwzględnione w innych kategoriach przewidzianych przez UOP, a w szczególności danych dotyczących pochodzenia etnicznego lub preferencji seksualnych.

Grupa robocza potwierdza również, że zasadniczo dane można gromadzić jedynie za uprzednią zgodą osoby, której dane dotyczą, która to zgoda może być wyraźna lub dorozumiana, zgodnie z sekcją 3 UOP. Możliwość ta nie w pełni odpowiada wymogowi art. 8 dyrektywy, w którym stwierdza się, że zgoda musi być wyraźna.

Jednakże tę ewentualną lukę równoważy wspomniana sekcja 3, która wymaga, aby zgoda w każdym wypadku była świadoma. W ten sposób, zdaniem grupy roboczej, przetwarzanie danych może mieć miejsce jedynie w konsekwencji działania osoby, której dane dotyczą, a nie w wyniku bezpośredniego udzielenia zgody, jeżeli dana osoba została wyraźnie poinformowana o warunkach wyjaśnionych przy opisywaniu zasady przejrzystości.

Dlatego też, nawet jeżeli przetwarzanie danych może wynikać z dorozumianej zgody osoby, której dane dotyczą, grupa robocza uważa, że konieczne jest uprzednie działanie administratora danych, mające na celu poinformowanie osoby, której dane dotyczą, o wszystkich konsekwencjach działania związanego z udzielenie, zgody.

Dlatego też, nawet jeżeli nie istnieje reguła podobna do reguły przewidzianej w dyrektywie, grupa robocza uważa, że prawodawstwo Izraela należycie wypełnią tę zasadę.

> **2) Marketing bezpośredni –** w przypadku gdy dane są przekazywane na potrzeby marketingu bezpośredniego, osoba, której one dotyczą, powinna mieć możliwość wycofania zgody na wykorzystanie jej danych do takich celów w dowolnym momencie.

Grupa robocza z zadowoleniem potwierdza, że zasada ta jest wyraźnie uregulowana w prawodawstwie izraelskim, jako że w UOP, w rozdziale 2 znajduje się część w szczególności dotycząca „reklamy bezpośredniej", którą określa się jako „osobiste kontaktowanie się z osobą na podstawie jej przynależności do grupy ludności, która została wyznaczona na podstawie jednej cechy lub kilku cech osób uwzględnionych w bazie danych".

Prawodawstwo izraelskie zawiera szczegółowe zobowiązania w przypadku przetwarzania takich danych. W szczególności administratorzy danych zobowiązani są zgłosić dokumentację w organie kontrolnym oraz uaktualniać rejestr źródeł, z których pozyskano dane. Ponadto istnieją szczegółowe wymogi w zakresie informacji, które należy uwzględnić we wszystkich przesyłkach skierowanych do osób, których dotyczą dane.

Jeżeli chodzi o samą zasadę, grupa robocza uważa, że jest ona przestrzegana w ramach podsekcji b) i e) sekcji 17F UOP, które stanowią, że:

> „(b) Każdy ma prawo żądać na piśmie, od właściciela bazy danych wykorzystywanej do korespondencji reklamowej, usunięcia informacji dotyczących danej osoby z bazy danych.
> c) Każdy ma prawo żądać na piśmie, od właściciela bazy danych wykorzystywanej na potrzeby usług korespondencji reklamowej lub od właściciela bazy danych zawierającej informacje, na podstawie których nawiązano kontakt, aby informacje dotyczące tej osoby nie były dostarczane do osoby, kategorii osób lub konkretnych osób przez określony czas lub definitywnie.

d) W przypadku gdy osoba poinformowała właściciela bazy danych o swoim żądaniu zgodnie z literą b) lub c), właściciel bazy danych postępuje zgodnie z przekazanym żądaniem oraz powiadamia daną osobę na piśmie o podjęciu stosownych działań.
e) W przypadku gdy właściciel bazy danych nie przekazał powiadomienia określonego w literze d) w terminie 30 dni od dnia otrzymania żądania, osoba, której dotyczą informacje, może zwrócić się do sądu pokoju w sposób przewidziany przepisami o nakazanie właścicielowi bazy danych podjęcia określonych działań."

3) Zautomatyzowana decyzja indywidualna: w przypadku gdy celem przekazania danych jest podjęcie zautomatyzowanej decyzji indywidualnej w rozumieniu art. 15 dyrektywy, osoba fizyczna powinna mieć prawo poznać uzasadnienie takiej decyzji i należy podjąć inne środki w celu ochrony uzasadnionych interesów tej osoby fizycznej.

Grupa robocza potwierdza, że prawodawstwo izraelskie nie zawiera wyrażonego bezpośrednio przepisu dotyczącego tej zasady. Jednakże grupa robocza z zadowoleniem przyjmuje komentarze zawarte w sprawozdaniu sporządzonym przez CRID oraz wyjaśnienia przedstawione przez władze izraelskie wskazujące, że prawo izraelskie w każdym przypadku umożliwia osobie, której dane dotyczą, zgłoszenie sprzeciwu wobec podejmowania tego rodzaju decyzji.

W każdym wypadku, bez uszczerbku dla wniosku, że zasada ta jest na chwilę obecną spełniona, grupa robocza wzywa władze izraelskie do wyraźnego uwzględniania tej zasady w sposób podobny do podejścia określonego w art. 15 dyrektywy we wszystkich środkach regulacyjnych przyjmowanych w przyszłości w odniesieniu do tej kwestii.

3.3. Procedura/mechanizmy stosowania

Wydana przez grupę roboczą opinia WP12 zatytułowana „Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive" wskazuje, że aby zapewnić podstawę oceny odpowiedniego stopnia istniejącej ochrony danych, należy określić nadrzędne cele systemu procedur ochrony danych i na tej podstawie dokonać oceny różnych sądowych i pozasądowych mechanizmów proceduralnych stosowanych w państwach trzecich.

W tym względzie cele systemu ochrony danych są w zasadzie trojakie:

- zapewnienie właściwego poziomu zgodności z zasadami,
- zapewnienie wsparcia i pomocy osobom fizycznym, których dotyczą dane, w zakresie wykonywania ich praw,
- zapewnienie odpowiedniego zadośćuczynienia dla stronie poszkodowanej w przypadku nieprzestrzegania zasad.

a) Zapewnienie właściwego poziomu zgodności z zasadami: dobry system na ogół charakteryzuje się wysokim poziomem wiedzy wśród administratorów danych na temat ich obowiązków oraz wśród osób, których dane dotyczą, na temat przysługujących im praw i sposobów ich wykonywania. Istnienie skutecznych i odstraszających sankcji może odgrywać znaczącą rolę w zapewnieniu poszanowania zasad, podobnie jak istnienie systemów bezpośredniej weryfikacji dokonywanej przez władze, audytorów lub niezależnych urzędników ds. ochrony danych.

Izraelski Urząd ds. Prawa, Informacji i Technologii (ILITA).

Zgodnie z sekcją 7 UOP, stworzona zostaje funkcja Rejestratora Baz Danych, przy czym „Rejestrator oznacza osobę, która posiada kwalifikacje umożliwiające powołanie jej na sędziego sądu pokoju i która została powołana przez rząd, w drodze powiadomienia w Reshumot, do prowadzenia „Rejestru baz danych" (zwanego dalej „rejestrem") zgodnie z sekcją 12".

Funkcja rejestratora została obecnie , na mocy decyzji rządu Izraela z 2006 r., włączona do ILITA, stworzonego na mocy wyżej wspomnianej decyzji, a administrator Rejestru baz danych jest z kolei Dyrektorem ILITA. Ponadto do ILITA włączono również stanowiska Rejestratora Urzędów Certyfikacji oraz Rejestratora Usług w zakresie Danych Kredytowych.

Uprawnienia ILITA w zakresie egzekwowania prawa są uregulowane w sekcji 10 UOP. W tym względzie grupa robocza, zgodnie z powyższym wyjaśnieniem, uznaje, że uprawnienia te, przyznane na mocy prawa Rejestratorowi Baz Danych, odnoszą się do ILITA, do którego włączono funkcję rejestratora.

W szczególności UOP nadaje ILITA uprawnienia do rejestrowania i kontrolowania przetwarzania danych na warunkach wymienionych poniżej.

Grupa robocza odnotowuje ostatnie zmiany przyjęte przez rząd w zakresie powoływania i odwoływania Dyrektora ILITA, uznając, że zmiany nadają dyrektorowi, a zatem i samemu urzędowi, odpowiedni poziom niezależności pod kątem celów określonych dla organów kontrolnych podlegających przepisom dyrektywy. W szczególności uwzględnia się, że funkcje osób działających w ILITA oraz funkcja dyrektora tego urzędu mają charakter służby cywilnej, a nie podlegają jakiemukolwiek rodzajowi mandatu ani nie mają charakteru politycznego.

W tym względzie grupa robocza bierze pod uwagę fakt, że zgodnie z decyzją rządu 4660 (HC/195) z dnia 8 stycznia 2006 r. powołanie Dyrektora ILITA, jako urzędnika wysokiego szczebla, podlega wcześniejszej ocenie niezależnego komitetu, złożonego z pięciu członków, w skład którego wchodzą przedstawiciele organów publicznych, Akademii oraz nadzorowanych jednostek, którzy ustalają konieczne warunki, jakie musi spełniać kandydat, i proponują powołanie wybranej osoby.

Ponadto grupa robocza z zadowoleniem przyjmuje fakt, że zgodnie z decyzją rządu nr 4470 z dnia 8 lutego 2009 r. kadencję Dyrektora ILITA ustalono na sześć lat. Dyrektor ILITA może zostać zwolniony jedynie w szczególnych okolicznościach przez specjalną komisję służby cywilnej, której przewodzi były sędzia. Mechanizm ten jest podobny do mechanizmu stworzonego w Izraelu w odniesieniu między innymi do Komisarza ds. Przeciwdziałania Praktykom Monopolistycznym, Dyrektora Urzędu Regulacji Rynków Kapitałowych i Ubezpieczeń czy Naczelnego Księgowego w Ministerstwie Finansów. Ponadto decyzja o zwolnieniu Dyrektora ILITA podlega ocenie sądu, w ramach której należy przedstawić uzasadnienie. Wreszcie Dyrektora ILITA chroni izraelskie prawo pracy, w tym przepisy Prawa podstawowego: Swoboda zatrudnienia, reguły zasadności, proporcjonalności i sprawiedliwości proceduralnej.

Jeżeli chodzi o niezależność budżetową ILITA, grupa robocza uwzględnia wyjaśnienia udzielone przez władze izraelskie w odniesieniu do obowiązującego systemu budżetowego dotyczącego ogólnie organów kontrolnych w Izraelu, który jest podobny do systemu ILITA, i jednocześnie potwierdza, że środki przekazane w ciągu ostatnich kilku lat pozwalają uznać poziom niezależności urzędu za odpowiedni.

Ponadto grupa robocza bierze pod uwagę fakt, że zgodnie z sekcją 36S lit. b) UOP fundusze pochodzące z poboru opłat z tytułu rejestracji baz danych są przekazywane bezpośrednio do ILITA jako organu kontrolnego na prowadzenie działań powierzonych urzędowi na mocy prawa.

Grupa robocza bierze również pod uwagę oświadczenia złożone przez władze izraelskie, w których opisują one niezależność, z jaką wspomniane organy realizowały swoje obowiązki, w tym kontrole organów publicznych, takich jak Urząd Prokuratora Generalnego, Ministerstwo Spraw Wewnętrznych, Ministerstwo Transportu, Ministerstwo Obrony lub nawet Ministerstwo Sprawiedliwości, którego ILITA jest częścią.

Wreszcie grupa robocza uważa, że uprawnienia nadane ILITA, które obejmują nawet ściganie przestępstw przeciwko prywatności, oraz fakt, że ILITA powierzono organizację 32. międzynarodowej konferencji na temat ochrony prywatności i danych osobowych, która zgodnie z harmonogramem ma się odbyć w październiku 2010 r. w Jerozolimie, potwierdzają wysiłki czynione przez państwo Izrael w celu zagwarantowania istnienia organu ochrony danych osobowych oraz odpowiedniej ochrony tego prawa.

Wobec powyższego grupa robocza stwierdza, że na chwilę obecną państwo Izrael dysponuje organ kontrolny ds. ochrony danych, który posiada konieczną niezależność i odpowiednie uprawnienia w zakresie egzekwowania prawa, w zakresie podobnym do przewidzianego w art. 28 dyrektywy.

Środki egzekwowania prawa i sankcje

Po rozpatrzeniu skargi ILITA podejmuje decyzję, czy jest ona uzasadniona. Jeżeli tak, ILITA ma prawo wydać administratorowi bazy danych instrukcje dotyczące przestrzegania przepisów.

Sekcja 31A UOP zawiera listę przestępstw naruszenia przepisów. Należy zauważyć, że jak wspomniano powyżej, ILITA uzyskał uprawnienia do prowadzenia dochodzeń, zgodnie ze swoimi uprawnieniami w zakresie egzekwowania prawa, w sprawie takich przestępstw w ramach fazy poprzedzającej lub postępowania karnego prowadzonego przez sąd.

Ponadto ILITA jest uprawniony do nakładania grzywien administracyjnych z tytułu przestępstw wymienionych w sekcji 31A, zgodnie z załącznikiem *Regulations of Administrative Offenses (Administrative Fines – Privacy Protection), 2004 r.*, które wydał Minister Sprawiedliwości w ramach swoich uprawnień nadanych mu na mocy *Ustawy o wykroczeniach administracyjnych z 1985 r*. System grzywien administracyjnych umożliwia właściwemu decydentowi nałożenie grzywny, a pozwanemu umożliwia zapłacenie grzywny lub wniesienie o wszczęcie postępowania sądowego.

Równolegle z powyższymi sankcjami sekcja 10 lit. f) UOP przewiduje, że „w przypadku gdy posiadacz lub właściciel bazy danych naruszy jakikolwiek przepis tej ustawy lub rozporządzeń z niej wynikających lub nie wypełni wskazań przekazanych mu przez rejestratora, rejestrator może zawiesić rejestrację na ustalony przez siebie okres lub unieważnić rejestrację bazy danych w rejestrze, pod warunkiem że przed zawieszeniem lub unieważnieniem właściciel bazy danych uzyska możliwość zostania wysłuchanym".

Wobec powyższego grupa robocza uważa, że prawodawstwo izraelskie zawiera konieczne elementy gwarantujące odpowiedni poziomu zgodności z przepisami dotyczącymi ochrony danych.

> **b) Zapewnienie wsparcia i pomocy osobom fizycznym, których dotyczą dane,** w zakresie wykonywania ich praw. Osoby fizyczne muszą mieć możliwość egzekwowania swoich praw szybko i skutecznie oraz bez ponoszenia nadmiernych kosztów. W tym celu niezbędny jest pewnego rodzaju mechanizm instytucjonalny umożliwiający niezależne rozpatrywanie skarg.

Grupa robocza uważa, że prawodawstwo izraelskie w wystarczającym stopniu gwarantuje tę zasadę. W szczególności litery d) i e1) w sekcji 10 przewidują, co następuje:

> „(d) Minister Sprawiedliwości, za zgodą Komisji Knesetu ds. Konstytucji, Prawa i Sprawiedliwości ustanawia na mocy zarządzenia jednostkę nadzorczą, która sprawuje nadzór nad bazami danych, ich rejestracją oraz bezpieczeństwem danych w nich zawartych; wielkość jednostki jest uzależniona od potrzeb nadzorczych.
>
> e) Rejestrator stoi na czele jednostki nadzorczej i powołuje inspektorów do prowadzenia nadzoru zgodnie z ustawą; inspektorem nie może zostać osoba, która nie przejdzie odpowiedniego przeszkolenia zawodowego w dziedzinie komputeryzacji i bezpieczeństwa informacji oraz wykonywania praw wynikających z ustawy, a Policja Izraelska nie zgłosiła zastrzeżeń związanych z bezpieczeństwem publicznym względem powołania tej osoby .
>
> e1) W ramach wypełniania swoich obowiązków inspektor może –
>
> > 1) od każdej zaangażowanej osoby żądać dostarczenia informacji i dokumentów związanych z bazą danych;
> >
> > 2) wejść na teren, na którym zgodnie z jego uzasadnionym przekonaniem prowadzona jest baza danych, przeszukać to miejsce i zająć przedmioty, jeżeli jest przekonany, że jest to konieczne do zapewnienia egzekwowania ustawy i przeciwdziałania naruszaniu jej przepisów; w stosunku do przedmiotu zajętego na mocy niniejszej sekcji stosuje się przepisy rozporządzenia w sprawie postępowania karnego (areszt i przeszukanie) [nowa wersja], 5869 – 1969; w stosowych przypadkach, zasady dotyczące wejścia na teren obiektu wojskowego lub obiektu organu bezpieczeństwa w rozumieniu sekcji 19 lit. c) ustawy są ustalane przez Ministra Sprawiedliwości, po konsultacji z ministrem nadzorującym dany organ bezpieczeństwa; w niniejszym ustępie termin „przedmiot" obejmuje materiały i dane komputerowe określone w prawie komputerowym, 5765 – 1995;

3) niezależnie od przepisów określonych w ust. 2, inspektor nie może wejść na teren wykorzystywany jedynie jako miejsce zamieszkania w sposób inny niż na podstawie nakazu wydanego przez sędziego sądu pokoju."

c) Zapewnienie poszkodowanej stronie odpowiedniego zadośćuczynienia w przypadku nieprzestrzegania zasadami. Jest to kluczowy element, który musi obejmować system niezależnego orzecznictwa lub arbitrażu, umożliwiający w stosownych przypadkach wypłacanie odszkodowań oraz nakładanie sankcji.

Poza omówionymi powyżej sankcjami, zarówno na poziomie administracyjnym, jak i karnym, sekcja 31B UOP wskazuje, że „działanie lub zaniechanie naruszające przepisy rozdziału drugiego lub czwartego bądź naruszające przepisy wprowadzone na mocy niniejszej ustawy stanowią wykroczenie przewidziane w rozporządzeniu w sprawie wykroczeń o charakterze cywilnoprawnym".

Dlatego też grupa robocza uważa, że prawo Izraela w wystarczającym stopniu gwarantuje prawo osoby, której dane dotyczą, do odszkodowania za szkody wyrządzone względem jej praw lub majątku w konsekwencji niedozwolonego przetwarzania jej danych osobowych.

4. WYNIKI OCENY

Podsumowując, biorąc pod uwagę wszystkie powyższe czynniki, grupa robocza uważa, że **Izrael gwarantuje odpowiedni stopień ochrony** zgodnie z art. 25 ust. 6 dyrektywy 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 w odniesieniu do zautomatyzowanych międzynarodowych transferów danych lub w przypadku gdy nie są one zautomatyzowane w odniesieniu do danych podlegających dalszemu zautomatyzowanemu przetwarzaniu na terytorium Izraela.

Jednocześnie grupa robocza wzywa władze izraelskie, aby w zmianach legislacyjnych wprowadzanych w przyszłości, w szczególności tych dotyczących realizacji „Raportu Schoffmana", przyjęły przepisy przewidujące:

- Zastosowanie prawodawstwa izraelskiego do ręcznych baz danych w celu rozszerzenia oceny odpowiedniego stopnia ochrony na przypadki, które nie zostały uwzględnione we wnioskach zawartych w niniejszej opinii.

- Wyraźne zastosowanie zasady proporcjonalności w odniesieniu do ogółu przetwarzania danych osobowych w sektorze prywatnym.

- Dokonanie wykładni wyłączeń w zakresie międzynarodowych transferów danych on-line przewidzianych w art. 26 ust. 1 dyrektywy.

Grupa robocza stwierdza wreszcie, że w ramach, które zostaną ustanowione na mocy decyzji ostatecznie przyjętej przez Komisję, będzie ściśle przestrzegać środków przyjętych w zakresie kwestii omówionych powyżej.

Sporządzono w Brukseli, dnia 1 grudnia 2009 r.

W imieniu grupy roboczej
Przewodniczący
Alex TÜRK