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

0475/10/PL
WP 177

Opinia 6/2010 w sprawie stopnia ochrony danych osobowych we Wschodniej Republice Urugwaju

przyjęta dnia 12 października 2010 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, a w szczególności art. 29 i art. 30 ust. 1 lit. b) dyrektywy,

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

PRZYJMUJE NINIEJSZĄ OPINIĘ:

1. WPROWADZENIE

Dnia 20 października 2008 r. Misja Wschodniej Republiki Urugwaju (zwanej dalej „Urugwajem") przy Unii Europejskiej przesłała Komisji Europejskiej pismo z oficjalnym wnioskiem rządu urugwajskiego o wszczęcie postępowania w celu stwierdzenia, że Urugwaj zapewnia prawidłowy stopień ochrony w odniesieniu do przekazywania danych osobowych z UE/EWG, zgodnie z art. 25 ust. 6 dyrektywy 95/46/WE w sprawie ochrony danych („dyrektywy").

Aby przeprowadzić badanie, czy Urugwaj zapewnia prawidłowy poziom ochrony danych, Komisja zwróciła się do *Centre de Recherches Informatique et Droit* (zwanego dalej „CRID") z Uniwersytetu w Namur o sporządzenie sprawozdania. W tym obszernym sprawozdaniu przeanalizowano stopień, w jakim urugwajski system prawny spełnia wymogi w zakresie prawodawstwa w tej dziedzinie i mechanizmów stosowania przepisów służących ochronie danych osobowych, określonych w dokumencie roboczym „Przekazywanie danych osobowych do państw trzecich: stosowanie art. 25 i 26 unijnej dyrektywy o ochronie danych", zatwierdzonym przez grupę roboczą powołaną w związku z art. 29 dyrektywy dnia 24 lipca 1998 r. (dokument WP12). Władze urugwajskie, poprzez Biuro ds. Regulacji i Kontroli w zakresie Danych Osobowych (URCDP), przedstawiły uwagi w odpowiedzi na kwestie podniesione w tym sprawozdaniu, za zgodą rady wykonawczej URCDP z dnia 11 lutego 2010 r.

Wspomniane sprawozdanie oraz uwagi władz urugwajskich zostały ocenione przez podgrupę utworzoną specjalnie do tego celu w ramach grupy roboczej art. 29. Podgrupa przedłożyła grupie roboczej do rozważenia kwestię przesłania przez jej przewodniczącego pisma do władz urugwajskich, w którym po wydaniu pozytywnej oceny systemu ochrony danych w Urugwaju (ujętego przede wszystkim w ustawie nr 18,331, z dnia 11 sierpnia, w sprawie ochrony danych osobowych i czynności związanych z prawem „habeas data" [do dostępu do własnych danych osobowych] - LPDP <skrót od nazwy hiszpańskiej>, oraz dekrecie regulacyjnym z dnia 31 sierpnia 2009 r., w sprawie zmiany wspomnianej ustawy – DPDP) powiadamia się władze urugwajskie o kwestiach, które mogą wymagać dalszych objaśnień.

Władze urugwajskie, poprzez URCDP, przesłały grupie roboczej ds. ochrony danych powołanej na mocy art. 29 obszerne sprawozdanie, za zgodą rady wykonawczej URCDP z dnia 23 czerwca 2010 r., w którym zawarto odpowiedzi na pytania

postawione w piśmie. Władze urugwajskie przedstawiły również szereg dokumentów dotyczących sytuacji w zakresie ochrony danych w tym państwie, w tym roczne sprawozdanie URCDP za 2009 r. i jego sprawozdanie z działalności do 31 maja 2010 r., różne uchwały podjęte przez radę wykonawczą URCDP oraz stosowne przepisy prawne dotyczące kwestii ochrony danych osobowych.

We wrześniu 2010 r. niniejsze sprawozdanie zostało rozesłane członkom podgrupy, którzy je przeanalizowali, zwracając szczególną uwagę na kwestie podniesione w piśmie przesłanym władzom urugwajskim przez grupę roboczą. Po przeanalizowaniu wspomnianych informacji podgrupa uznaje, że można bez dalszej zwłoki przedłożyć niniejszy dokument grupie roboczej.

2. PRAWODAWSTWO W ZAKRESIE OCHRONY DANYCH W URUGWAJU

Konstytucja Wschodniej Republiki Urugwaju, uchwalona w 1967 r., nie przewiduje jednoznacznie prawa do prywatności i ochrony danych osobowych. Jednakże ustawa zasadnicza nie jest szczególnie dokładna w tym względzie, jeżeli uwzględnić fakt, że jej art. 72 stanowi, że „wykaz praw, obowiązków i gwarancji zawarty w konstytucji nie wyklucza innych praw, obowiązków i gwarancji, które są właściwe osobie ludzkiej lub które wywodzą się z republikańskiej formy rządów".

Ponadto w art. 332 konstytucji stwierdza się, że „stosowanie zapisów niniejszej Konstytucji, które uznają prawa osób fizycznych, oraz zapisów przyznających prawa i nakładających obowiązki na władze publiczne nie powinno być ograniczane brakiem stosownych przepisów, natomiast może być zastępowane poprzez odwoływanie się do fundamentów podobnych ustaw, zasad prawa i ogólnie przyjętych doktryn".

Grupa robocza potwierdza zatem, że powyższe dwa otwarte zdania uznają istnienie praw podstawowych osób fizycznych, które nie są jednoznacznie wyrażone w konstytucji Urugwaju. Wniosek ten znajduje potwierdzenie, jeżeli weźmie się pod uwagę fakt, że art. 1 ustawy 18,331, w sprawie ochrony danych osobowych i czynności związanych z prawem „habeas data" (LPDP) stwierdza z absolutną jednoznacznością, że „prawo do ochrony danych osobowych jest właściwe osobie ludzkiej, a więc jest ono ujęte w art. 72 konstytucji Republiki".

Wobec powyższego prawo podstawowe do ochrony danych osobowych, uznane jako takie w systemie prawnym Urugwaju, jest regulowane na mocy LPDP, którą proklamowano dnia 11 sierpnia 2008 r., a która zastępuje poprzednią ustawę w sprawie ochrony danych osobowych obowiązującą w odniesieniu do sprawozdań handlowych oraz czynności związanych z prawem „habeas data", wprowadzoną w 2004 r., i obecnie LPDP obejmuje w całości regulację tej kwestii we wszystkich obszarach działalności. Dlatego też art. 3 ustawy określa ogólną zasadę, że „przepisy niniejszej ustawy mają zastosowanie do danych osobowych zapisanych na dowolnym nośniku, na którym mogą być przetwarzane, oraz do dowolnego przyszłego wykorzystania tych danych przez podmioty publiczne lub prywatne".

Następnie, rozwijając przepisy wspomnianej LPDP, rząd Republiki, dnia 31 sierpnia 2009 r. wprowadził dekret regulacyjny rozwijający tę ustawę (DPDP). Preambuła tego aktu wskazuje, że „należy dostosować krajowy system prawny w tym względzie do

najbardziej akceptowanego porównywalnego systemu prawnego, zasadniczo do systemu ustanowionego przez państwa europejskie na mocy 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".

Dekret wprowadza pewne objaśnienia i zmiany regulacyjne w odniesieniu do szeregu przepisów przewidzianych w LPDP. W szczególności grupa robocza uważa, że trzeba wskazać tu przepisy dotyczące terytorialnego zakresu stosowania LPDP, bezpieczeństwa, wykonywania praw do dostępu, uaktualniania, wprowadzania i usuwania danych oraz szczegółowego uregulowania organizacji, uprawnień i funkcjonowania organu kontrolnego, zwanego Biurem ds. Regulacji i Kontroli w zakresie Danych Osobowych (URCDP).

Wreszcie grupa robocza podkreśla, że dokumentacja przesłana przez władze urugwajskie w odpowiedzi na przesłane przez nią pismo zawiera zgodę rady wykonawczej URCDP, w ramach której nakazuje ona „działanie w celu dopilnowania, aby Ministerstwo Spraw Zagranicznych wszczęło konieczne postępowanie z Radą Europy zmierzające do realizacji celów wskazanych w niniejszej uchwale, zgodnie z art. 23 konwencji 108 Rady Europy (konwencja strasburska) oraz jej dodatkowym protokołem z dnia 28 stycznia 1981 r. o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych".

3. OCENA, CZY PRAWODAWSTWO W ZAKRESIE OCHRONY DANYCH W URUGWAJU ZAPEWNIA PRAWIDŁOWY STOPIEŃ OCHRONY DANYCH OSOBOWYCH

Grupa robocza wskazuje, że jej ocena prawidłowości prawodawstwa obowiązującego w Urugwaju w zakresie ochrony danych osobowych odnosi się przede wszystkim do ustawy nr 18,331, z dnia 13 sierpnia, w sprawie ochrony danych osobowych i czynności związanych z prawem „habeas data" (LPDP) oraz dekretu regulacyjnego z dnia 31 sierpnia, przyjętego w odniesieniu do tej ustawy (DPDP).

Zapisy wspomnianej ustawy porównano z głównymi przepisami dyrektywy, przy uwzględnieniu sprawozdania grupy roboczej WP12. Sprawozdanie to określa szereg zasad, które stanowią „rdzeń" „istotnych" zasad dotyczących ochrony danych i wymogów związanych z procedurą/zastosowaniem, a zgodność z nimi można uznać za warunek minimalny, aby uznać ochronę danych za prawidłową.

3.1 Zakres zastosowania prawodawstwa

Jak już wskazano, z obiektywnego punktu widzenia art. 3 LPDP, odtworzony w art. 2 DPDP, określa zasadę, że przedmiotowy system regulacyjny „ma zastosowanie do danych osobowych zapisanych na dowolnym nośniku, na którym mogą być przetwarzane, oraz do dowolnego przyszłego wykorzystania tych danych przez podmioty publiczne lub prywatne". Jednocześnie, zgodnie z art. 2, przepisy dotyczące ochrony danych będą miały w odpowiednich przypadkach poprzez rozszerzenie, zastosowanie do osób prawnych.

Grupa robocza z zadowoleniem przyjmuje objaśnienia przedstawione przez władze urugwajskie w odpowiedzi na obawy wyrażone przez grupę roboczą w związku z tym, że ustawa nie ma zastosowania do „baz danych stworzonych i regulowanych na mocy specjalnych ustaw."

W odniesieniu do tej kwestii władze urugwajskie odpowiedziały, że przytoczone ustawy specjalne, których szereg przykładów przedstawiły, określają bardziej wymagający system ochrony danych osobowych niż system ujęty w ustawie ogólnej, którą zawsze stosuje się dodatkowo w odniesieniu do kwestii nieuregulowanych przepisami szczegółowymi, w ramach stosowania wyżej przywołanego art. 322 konstytucji Republiki.

Jeżeli chodzi o terytorialny zakres zastosowania ustawy, grupa robocza wyraziła zadowolenie, że DPDP w sposób jednoznaczny zawiera artykuł odnoszący się do tej kwestii, która jest w zasadzie rozwiązana identycznie, jak w systemie ustanowionym w art. 4 dyrektywy; gwarantuje to zatem zgodność z określonymi tam zasadami, a w szczególności z zasadą dotyczącą ograniczenia kolejnych transferów.

Dlatego też w wyżej wspomnianym art. 3 uznaje się, że przetwarzanie danych osobowych podlega LPDP, gdy:

- dane są przetwarzane przez administratorów baz danych lub osoby przetwarzające dane z siedzibą w Urugwaju, którzy prowadzą działalność w tym państwie, niezależnie od ich formy prawnej;

- administrator baz danych lub osoba przetwarzająca dane nie ma siedziby w Urugwaju, ale przetwarza dane za pomocą nośników zlokalizowanych w tym państwie.

Ponadto w artykule dodaje się, że wprowadza się wyjątek dotyczący drugiej reguły „w przypadkach, w których wyżej wspomniane nośniki są wykorzystywane wyłącznie do transferu danych, o ile administrator baz danych lub osoba przetwarzająca dane powoła, przed organem kontrolnym, przedstawiciela z siedzibą i stałym miejscem zamieszkania na terytorium kraju, który będzie spełniał obowiązki prawne objęte regulacją w ramach niniejszych przepisów".

Dlatego też w odniesieniu do wyżej wspomnianych objaśnień grupa robocza uważa, że zakres stosowania urugwajskiego prawodawstwa dotyczącego ochrony danych jest podobny do zakresu określonego w dyrektywie.

3.2. Zasady związane z treścią

a) Zasady podstawowe

1) Zasada ograniczenia celu: dane powinny być przetwarzane w konkretnym celu, a następnie wykorzystywane lub przekazywane dalej wyłącznie wtedy, gdy nie jest to niezgodne z celem ich przekazania. Jedyne wyjątki dotyczące tej zasady to te, które są konieczne w demokratycznym społeczeństwie z ważnych względów opisanych w art. 13 dyrektywy.

Grupa robocza z zadowoleniem stwierdza, że zasada ta jest wyraźnie ujęta w art. 5 lit. c) LPDP, który jednoznacznie określa, że działania administratorów baz danych, zarówno publicznych, jak i prywatnych, oraz ogólnie osób prowadzących czynności związane z danymi osobowymi osób trzecich powinny być zgodne z zasadą ograniczenia celu.

W art. 6 ustawy stwierdza się, że „żadnej bazy danych nie można wykorzystywać, aby naruszać prawa człowieka ani nie może to być w sprzeczności z ustawami i dobrymi obyczajami". Jednocześnie w art. 8 dodaje się, że „przetwarzane dane nie mogą być wykorzystywane do jakichkolwiek innych celów niż cele, do których zostały zebrane, ani nie mogą być sprzeczne z tymi celami".

Jedynym wyjątkiem od tego zapisu jest to, że „przepisy określają przypadki i procedury, gdy w drodze wyjątku i w odniesieniu do ich wartości historycznej, statystycznej lub naukowej oraz na podstawie szczegółowego prawodawstwa można przechowywać dane, nawet jeżeli nie istnieje ku temu bieżąca potrzeba ani zasadność". Artykuł 37 DPDP reguluje procedurę dotyczącą udzielania zezwoleń na przechowywanie danych do celów historycznych, statystycznych lub naukowych. Grupa robocza przyjmuje, że wyjątek ten jest podobny do wyjątku określonego w art. 6 ust. 1 lit. b) dyrektywy.

Podobnie art. 11 LPDP wskazuje, że „osoby fizyczne lub prawne, które zgodnie z prawem pozyskują informacje z bazy danych przetwarzającej dane, mają obowiązek wykorzystywania ich w taki sposób, aby zachować poufność oraz wyłącznie do zwykłych czynności związanych z prowadzoną działalnością gospodarczą lub zawodową, przy czym zabrania się rozpowszechniania wspomnianych informacji osobom trzecim".

Dlatego też grupa robocza uważa, że prawodawstwo urugwajskie jest zgodne z tą zasadą.

> **2) Zasada jakości danych i proporcjonalności:** dane powinny być dokładne i w razie konieczności uaktualniane. Dane powinny być prawidłowe, stosowne oraz nienadmierne ilościowo w stosunku do celów, do których są przekazywane lub dalej przetwarzane.

Zdaniem grupy roboczej zasada jest uregulowana w art. 7 LPDP poprzez tzw. „zasadę prawdziwości" wymienioną wśród głównych zasad przewodnich ustawy w art. 5 lit b).

Wyżej wspomniany art. 7 stanowi, że „dane osobowe zebrane do celów związanych z przetwarzaniem muszą być prawdziwe, prawidłowe, bezstronne i nienadmierne ilościowo w stosunku do celów, dla których zostały zgromadzone. Gromadzenie danych nie może być prowadzone w sposób nieuczciwy, oszukańczy, obraźliwy, poprzez wyłudzenie ani w żaden sposób sprzeczny z przepisami niniejszej ustawy".

Ponadto, LPDP wymaga, aby „dane były dokładne i, w razie konieczności, uaktualniane" i dodaje, że „w przypadku wykazania, że dane są niedokładne lub nieprawdziwe, administrator usuwa je, uzupełnia lub zastępuje je danymi dokładnymi, prawdziwymi i zaktualizowanymi, gdy tylko dowie się o zaistnieniu takiej sytuacji.

Ponadto wszelkie nieaktualne dane są usuwane zgodnie z przepisami niniejszej ustawy".

Wreszcie w art. 8 LPDP stwierdza się, że „dane są usuwane, gdy przestają być konieczne lub właściwe w odniesieniu do celów, do których zostały zebrane".

Grupa robocza bierze również pod uwagę wyjaśnienia władz urugwajskich dotyczące założenia legalności przetwarzania, o którym mowa w art. 9 lit. c) LPDP, który stanowi, że „uprzednia zgoda nie jest wymagana, gdy (…) są to wykazy z danymi osób fizycznych ograniczonymi do imion i nazwisk, numeru dokumentu tożsamości, narodowości, adresu i daty urodzenia. W przypadku osób prawnych analogiczne dane to nazwa przedsiębiorstwa, nazwa marki, pojedynczy numer podatnika, adres, numer telefonu i tożsamość osób odpowiedzialnych".

W tej kwestii władze urugwajskie wyjaśniły, że legitymizacja przewidziana w tym zapisie pod żadnym warunkiem nie może być rozumiana jako odmienna od zasad legitymizacji, proporcjonalności i ograniczenia celu. Dlatego też, nawet gdy nie jest konieczne uzyskanie zgody osoby zainteresowanej, administrator może przetwarzać dane opisywane w tym artykule jedynie w przypadku, gdy przetwarzanie takie mieści się w zakresie określonych, jednoznacznych i zgodnych z prawem celów, oraz o ile wspomniane dane są odpowiednie, stosowne i nienadmierne ilościowo w stosunku do wspomnianych celów i nie istnieje inna legitymizacja niż konieczna zgodność z obiema zasadami.

Mając na uwadze wszystkie powyższe ustalenia, grupa robocza uważa, że zasada proporcjonalności i jakości danych jest również ujęta w prawodawstwie urugwajskim.

> **3) Zasada przejrzystości:** osoby, których dane dotyczą, powinny być informowane o celu przetwarzania ich danych i o tożsamości osoby przetwarzającej dane w państwie trzecim oraz o wszelkich innych aspektach koniecznych do zapewnienia zgodności z zasadą sprawiedliwego traktowania. Jedyne dopuszczalne wyjątki muszą być ujęte w art. 11 ust. 23 oraz art. 13 dyrektywy.

Grupa robocza uważa, że obowiązek informowania osoby, której dane dotyczą, o przetwarzaniu jej danych, jest ujęty w art. 13 LPDP, zgodnie z którym, w przypadku gdy gromadzone są dane osobowe, osoby, których dane dotyczą, powinny być uprzednio wyraźnie, dokładnie i jednoznacznie poinformowane o następujących kwestiach:

- cele, do których dane będą przetwarzane, i możliwi odbiorcy lub rodzaj odbiorców;

- istnienie bazy danych, elektronicznej lub innego rodzaju, oraz tożsamość i adres administratora;

- obowiązkowy lub dobrowolny charakter odpowiedzi na przesłany kwestionariusz, w szczególności w odniesieniu do danych szczególnie chronionych;

- konsekwencje przekazania danych, niedostarczenia danych lub podania niedokładnych danych;

- możliwości osoby, której dane dotyczą, w zakresie wykonania swoich praw do dostępu, sprostowania lub usuwania danych;

Grupa robocza potwierdza również, że gdy podstawą przetwarzania jest zgoda osoby, której dane dotyczą, osoba ta będzie o tym informowana, zgodnie z wymogiem określonym w art. 9 LPDP i art. 5 DPDP, przy czym art. 5 DPDP określa, że „gdy do gromadzenia i przetwarzania danych wymagana jest zgoda osoby, której dane dotyczą, powinna ona zostać poinformowana w sposób jednoznacznie uświadamiający jej cel, w jakim dane będą wykorzystywane, i rodzaj działań podejmowanych przez administratora bazy danych lub osobę przetwarzającą dane. W przeciwnym razie zgoda zostanie uznana za nieważną".

Grupa robocza uwzględnia również objaśnienia przedstawione przez władze urugwajskie dotyczące obowiązku każdorazowego informowania osoby, której dane dotyczą. Dlatego też, pomimo że brzmienie art. 13 mogłoby sugerować, że obowiązek informowania osób, których dane dotyczą, odnosi się tylko do przypadków, w których osoba, której dane dotyczą, przekazuje dane dobrowolnie i za zgodą, władze urugwajskie twierdzą, że obowiązek ten jest bezwzględny, bezwarunkowy i nie zależy od powodów uzasadniających przetwarzanie danych. Obowiązek informowania osoby, której dane dotyczą, stosuje się we wszystkich przypadkach, niezależnie od tego, czy dane osobowe są wymagane od osoby, której dotyczą, czy od osoby trzeciej, oraz niezależnie od tego, czy przetwarzanie prowadzone jest za zgodą osoby, której dane dotyczą, czy z innego zgodnego z prawem względu.

Ponadto władze urugwajskie wyjaśniają, że w przypadku pozyskiwania danych poprzez osobę trzecią w wyniku transmisji danych, osoba lub podmiot przekazujący dane musi również uprzednio poinformować osobę, której dane dotyczą, o tym przekazaniu danych oraz o odbiorcach przekazanych danych, zgodnie z art. 13 LPDP.

> **4) Zasada bezpieczeństwa:** Administrator musi przyjąć odpowiednie środki techniczne i organizacyjne zapobiegające zagrożeniom związanym z przetwarzaniem danych. Osobom działającym z upoważnienia administratora, w tym osobie odpowiedzialnej za przetwarzanie danych, nie wolno przetwarzać danych inaczej niż na podstawie instrukcji administratora.

Grupa robocza podkreśla, że w ramach zasad wymienionych w art. 5 LPDP zasada bezpieczeństwa ujęta jest w lit. e).

Artykuł 10 ustawy rozwija tę zasadę poprzez stwierdzenie, że „administrator lub użytkownik bazy danych musi podejmować wszelkie konieczne środki zapewniające bezpieczeństwo i poufność danych osobowych. Środki te mają na celu zapobieganie zmianom danych, ich utracie, bezprawnemu przeglądaniu lub przetwarzaniu oraz wykrywanie przekazywania informacji, celowo lub nie, niezależnie od tego, czy ryzyko takie jest skutkiem działań człowieka czy wykorzystanych środków technicznych" i dodaje, że „zakazane jest zapisywanie danych osobowych w bazach danych, które nie spełniają technicznych wymogów bezpieczeństwa i integralności".

Ponadto w art. 7 DPDP dodaje się, że „zarówno administrator, jak i osoba odpowiedzialna za bazę danych lub przetwarzanie danych musi chronić przetwarzane dane osobowe poprzez użycie najbardziej odpowiednich środków technicznych i organizacyjnych zapewniających ich integralność, poufność i dostępność", przy czym charakterystyka osoby przetwarzającej dane jest taka sama, jak charakterystyka określona w dyrektywie.

Grupa robocza zauważa również, że art. 8 DPDP ustanawia obowiązek informowania zainteresowanych osób fizycznych o wszelkich ewentualnie zaistniałych naruszeniach bezpieczeństwa, stwierdzając, że „gdy administratorzy bazy danych lub osoby przetwarzające dane dowiadują się o naruszeniach bezpieczeństwa, które miały miejsce w dowolnym momencie prowadzonego przetwarzania danych i które mogą mieć znaczny wpływ na prawa danej osoby fizycznej, powinni poinformować ją o takim zdarzeniu".

Wreszcie w odniesieniu do regulacji w zakresie obowiązku poufności i zachowania tajemnicy ujętej w art. 11 LPDP, grupa robocza uważa, w oparciu o przekazane informacje, że prawodawstwo urugwajskie jest zgodne z zasadą bezpieczeństwa określoną w dokumencie WP12.

> **5) Prawo do dostępu, sprostowania i sprzeciwu:** osoba fizyczna musi mieć prawo do otrzymania kopii wszystkich danych, które jej dotyczą, oraz prawo do sprostowania wszelkich danych, które są nieprawidłowe. W niektórych sytuacjach osoba fizyczna musi mieć również możliwość wniesienia sprzeciwu wobec przetwarzania danych, które jej dotyczą. Jedyne wyjątki dotyczące tych praw powinny być zgodne z art. 13 dyrektywy.

W odniesieniu do prawa do dostępu art. 14 LPDP przewiduje, że „każda osoba fizyczna, której dane dotyczą, która uprzednio potwierdziła swoją tożsamość na podstawie dokumentu tożsamości lub odpowiedniego upoważnienia, ma prawo do otrzymania wszelkich informacji jej dotyczących przechowywanych w publicznej lub prywatnej bazie danych. To prawo do dostępu może być realizowane bezpłatnie jedynie raz na sześć miesięcy, chyba że będzie się wiązało z uzasadnionym interesem zgodnie z systemem prawnym".

Informacje takie „muszą zostać przekazane w ciągu pięciu dni roboczych od momentu złożenia odpowiedniego wniosku. Jeżeli w ciągu tego terminu nie zostanie udzielona odpowiedź na wniosek lub jeżeli spotka się on z odmową z powodów nie uzasadnionych na mocy niniejszej ustawy, zastosowanie mają przepisy 'habeas data'". Ponadto „informacje muszą być przekazane w sposób przejrzysty, bez kodowania, a w odpowiednich przypadkach muszą być uzupełnione wyjaśnieniem, w języku odpowiadającym przeciętnemu poziomowi wiedzy społeczeństwa, z wykorzystaniem powszechnie używanej terminologii".

W art. 14 stwierdza się również, że „informacje powinny być pełne i powinny obejmować cały zapis dotyczący danej osoby, nawet jeżeli wniosek dotyczy tylko jednego aspektu danych osobowych tej osoby. W żadnym razie sprawozdanie nie powinno ujawniać informacji dotyczących innych osób, nawet jeżeli są one powiązane z daną osobą" oraz „informacje mogą być przekazane pisemnie, drogą elektroniczną,

telefonicznie, obrazem lub innym odpowiednim sposobem, który ich posiadacz uzna za odpowiedni".

Grupa robocza uwzględnia objaśnienia przekazane przez władze urugwajskie, w których stwierdzają one, że bez względu na brzmienie art. 9 d) DPDP osoba fizyczna nie musi podawać żadnych powodów swojego wniosku, a potwierdzenie jej tożsamości jest do tego celu wystarczające. W szczególności grupa robocza bierze pod uwagę porozumienie URCDP z dnia 18 czerwca 2010 r., w której stwierdza się, że „aby wykonać prawo do dostępu określone w art. 14 ustawy nr 18.331 w sprawie ochrony danych osobowych i czynności związanych z prawem „habeas data", administrator bazy danych na uzasadnienie wniosku wymaga jedynie potwierdzenia tożsamości posiadacza danych".

W odniesieniu do innych praw osób fizycznych art. 15 LPDP stwierdza, że „każda osoba fizyczna lub prawna ma prawo do korygowania, uaktualniania, wprowadzania lub usuwania swoich danych osobowych, które są przechowywane w bazie danych po potwierdzeniu błędu, nieprawidłowego zapisu lub wyłączenia w informacjach jej dotyczących".

W ustawie dodaje się, że „administrator bazy danych lub osoba przetwarzająca musi sprostować, uaktualnić, wprowadzić lub usunąć takie informacje z zastosowaniem wszelkich koniecznych do tego celu czynności w terminie nieprzekraczającym pięciu dni roboczych od otrzymania wniosku osoby fizycznej lub, w odpowiednich przypadkach, musi poinformować o powodach uznania, że przepis ten nie ma zastosowania", oraz konkluduje się, że „niedopełnienie tego obowiązku przez administratora bazy danych lub osobę przetwarzającą lub niedotrzymanie terminu w tym względzie uprawnia osobę, której dane dotyczą, do odwołania się do prawa „habeas data" przewidzianego w niniejszej ustawie".
Grupa robocza odnotowuje objaśnienia zawarte w DPDP, skupiające się początkowo na definicjach określonych w art. 10-12.

Zgodnie z art. 10 prawo do korygowania danych zostało zdefiniowane w następujący sposób: „Prawo do korygowania danych jest prawem osoby, której dane dotyczą, do zmiany wszelkich danych, które są niedokładne lub niekompletne". Artykuł 11 definiuje prawo do uaktualniania w następujący sposób: „Prawo do uaktualniania danych jest prawem osoby, której dane dotyczą, do zmiany danych, które są niedokładne na dzień, w którym prawo to jest wykonywane"; a art. 12 definiuje prawo do wprowadzania danych w następujący sposób: „Prawo do wprowadzania danych jest prawem osoby, której dane dotyczą, do wprowadzania do bazy danych istotnych informacji jej dotyczących, gdy stwierdzono, że istnieje uzasadniony interes".

Ponadto art. 13 określa prawo do usuwania danych w następujący sposób: „Prawo do usuwania danych jest prawem osoby, której dane dotyczą, do usuwania danych, których wykorzystanie przez osoby trzecie jest bezprawne lub które okaże się nieodpowiednie lub nadmierne".

W odniesieniu do tej ustawy grupa robocza przyjmuje argumenty wskazane przez CRID w dwóch sprawozdaniach dotyczących prawidłowego poziomu ochrony danych w Urugwaju oraz w szczególności w uzupełnieniach dotyczących wdrażania DPDP,

uznając, że poprzez regulację dotyczącą prawa do usuwania danych prawo urugwajskie uznaje prawo do sprzeciwu określone w art. 14 dyrektywy.

W odniesieniu do wyjątków dotyczących wykonywania powyższych praw grupa robocza uważa, że zachowana jest zgodność z zasadami ochrony danych w przypadku tych wyjątków, które oparte są na potrzebie zachowania informacji do celów historycznych, statystycznych lub naukowych, zgodnie z obowiązującym prawem, lub w konsekwencji kontynuacji stosunków umownych między administratorem a osobą, której dane dotyczą, które uzasadniają przetwarzanie danych.

Ponadto grupa robocza uważa, że wyjątki określone w art. 26 LPDP, które uwzględniają „zagrożenia, które mogą powstać w związku z obronnością państwa lub bezpieczeństwem publicznym, ochroną praw i wolności osób trzecich lub potrzebami związanymi z prowadzonymi dochodzeniami" można uznać za podobne do wyjątków określonych w art. 13 dyrektywy. W szczególności grupa robocza bierze pod uwagę fakt, że sama ustawa przewiduje, w art. 26, że „każda osoba, której dane dotyczą, której odmówiono, całkowicie lub częściowo, wykonania praw wymienionych w poprzednich ustępach, może powiadomić o tym organ kontrolny, który rozstrzyga w kwestii zgodności lub niezgodności tej odmowy z prawem".

> **6) Ograniczenia w zakresie dalszego przekazywania danych do innych państw:** dalsze przekazywanie danych osobowych z państwa przeznaczenia będącego osobą trzecią do innego państwa może być dozwolone jedynie w przypadku, gdy to kolejne państwo również zapewnia prawidłowy stopień ochrony. Jedynymi dopuszczalnymi wyjątkami od tej zasady są wyjątki przewidziane w art. 26 ust. 1 dyrektywy

Grupa robocza zwraca uwagę, że prawo urugwajskie definiuje pojęcie międzynarodowego transferu danych podobnie do pojęcia określonego przez państwa członkowskie, zakładając, że obejmuje ono nie tylko transfery danych do administratorów danych z siedzibą w innym państwie, ale również przypadki, gdy dane są przekazywane podmiotowi przetwarzającemu.

Pojęcie to pochodzi z definicji eksportu i importu danych zawartych w art. 4 lit. e) i f) DPDP. Eksportera szczegółowo definiuje się jako „osobę fizyczną lub prawną, publiczną lub prywatną, z siedzibą na terytorium Urugwaju, która przekazuje dane osobowe do innego państwa, zgodnie z przepisami niniejszego dekretu", natomiast importerem jest „osoba fizyczna lub prawna, publiczna lub prywatna, która otrzymuje dane z innego państwa, w ramach międzynarodowego transferu, przy czym może to być administrator danych, podmiot przetwarzający dane lub osoba trzecia".

Artykuł 23 LPDP określa ogólną zasadę dotyczącą transferów, że „zabrania się przekazywania jakichkolwiek danych osobowych do państw lub organizacji międzynarodowych, które nie zapewniają prawidłowego stopnia ochrony zgodnie z normami prawa międzynarodowego i regionalnego". W ostatnich dwóch ustępach tego artykułu dodaje się, że „nie naruszając przepisów ustępu pierwszego niniejszego artykułu, Biuro ds. Regulacji i Kontroli w zakresie Danych Osobowych może zezwolić na transfer lub serię transferów danych osobowych do państwa trzeciego, które nie zapewnia prawidłowego stopnia ochrony, jeżeli administrator oferuje prawidłowe środki zabezpieczające w zakresie ochrony prywatności, praw i wolności osób

fizycznych oraz wykonywania ich odpowiednich praw. Takie środki zabezpieczające mogą wynikać z odpowiednich klauzul umownych".

Grupa robocza uznaje zatem, że zasady te stanowią system regulacyjny dla międzynarodowych transferów danych podobny do systemu określonego w art. 25 ust. 1 i 26 ust. 2 dyrektywy.

W art. 23 LPDP zamieszczone są również dwa wykazy wyjątków od takiego zezwolenia. Grupa robocza uważa, że drugi z tych wykazów jest taki sam, jak wyjątki określone w art. 26 ust. 2 dyrektywy, jako że wymienia się w nim następujące przypadki, które są wyłączone z obowiązku zezwolenia:

- w przypadku gdy osoba fizyczna udzieli jednoznacznej zgody na proponowany transfer;

- w przypadku gdy transfer jest konieczny do realizacji umowy między osobą fizyczną a administratorem lub do wdrożenia środków przedumownych podjętych na wniosek osoby fizycznej;

- w przypadku gdy transfer jest konieczny do zawarcia lub realizacji umowy lub gdy umowa ma być dopiero podpisana w interesie osoby fizycznej pomiędzy administratorem a osobą trzecią;

- w przypadku gdy transfer jest konieczny lub prawnie wymagany w celu zabezpieczenia ważnego interesu publicznego lub w celu uznania, wykonywania i ochrony prawa w postępowaniu sądowym;

- w przypadku gdy transfer jest konieczny do zabezpieczenia istotnych interesów osoby fizycznej;

- w przypadku gdy transfer jest realizowany z rejestru, który na mocy przepisów prawa ma udzielać informacji ogółowi społeczeństwa i jest ogólnodostępnym źródłem pozyskiwania informacji przez ogół społeczeństwa lub przez dowolną osobę, która może wykazać uzasadniony interes, pod warunkiem że w każdym przypadku spełnione są prawnie ustanowione wymogi dotyczące tych czynności.

Grupa robocza zauważa następnie, że pierwszy wykaz zawiera listę założeń, które jednak nie pokrywają się dosłownie z założeniami określonymi w art. 26 ust. 1 dyrektywy. W wykazie tym jako wyjątki od obowiązku zezwolenia pojawiają się następujące elementy:

a) międzynarodowa współpraca sądowa, na podstawie odpowiedniego instrumentu międzynarodowego, czy to traktatu czy konwencji, w zależności od okoliczności danej sprawy;

b) wymiana danych medycznych, gdy jest to wymagane do leczenia danej osoby ze względów zdrowia publicznego lub higieny;

c) transfery lub wymiany bankowe, w odniesieniu do odpowiednich transakcji i zgodnie z obowiązującym prawem;

d) umowy na podstawie traktatów międzynarodowych, których Wschodnia Republika Urugwaju jest stroną;

e) współpraca międzynarodowa między agencjami wywiadu służąca zwalczaniu przestępczości zorganizowanej, terroryzmu i handlu narkotykami.

Grupa robocza zwraca uwagę na swoje sprawozdanie 4/2002 w sprawie stopnia ochrony danych osobowych w Argentynie, podkreślając, że wyjątki wskazane w lit. b), c) i d) mogą sugerować, na pierwszy rzut oka, że istnieją dalsze wyjątki oprócz tych określonych w art. 26 ust. 1 dyrektywy, co miałoby wpływ na zastosowanie omawianej zasady.

Jednakże grupa robocza z zadowoleniem przyjmuje objaśnienia przedstawione przez władze urugwajskie, wyjaśniające, że nie można przyjmować, iż wyjątki te mają jakiekolwiek szersze zastosowanie niż to określone w art. 26 ust.1.

Zatem wyjątek przedstawiony w lit. c) odnosi się do istnienia stosunku umownego między osobą fizyczną a eksporterem, który koniecznie wymaga międzynarodowego transferu danych osobowych, aby umowa mogła być zrealizowana.

Wyjątki określone w lit. b) i d) zawsze należy interpretować w kontekście jednoczesnej analizy istnienia ważnego interesu publicznego, ratyfikacji umowy międzynarodowej wiążącej dla Urugwaju lub kwestii związanych ze zdrowiem publicznym w ramach ogólnego pojęcia „istotnego interesu publicznego."

Wobec powyższego, grupa robocza akceptuje te wyjaśnienia, ale zaleca przyjęcie środków służących zagwarantowaniu, że władze urugwajskie będą stosować taką interpretację analizowanych przepisów.

b) Zasady dodatkowe

Dokument WP12 odnosi się do niektórych zasad, które powinny być stosowane do konkretnych rodzajów przetwarzania, które obejmują w szczególności:

> **1) Dane szczególnie chronione –** w przypadku gdy w grę wchodzą kategorie danych „szczególnie chronionych" (wymienione w art. 8 dyrektywy), zastosować należy dodatkowe środki zabezpieczające, na przykład wymóg, aby osoby fizyczne wyraziły wyraźną zgodę na przetwarzanie danych.

Grupa robocza uważa, że zasada ta jest przestrzegana w urugwajskim prawodawstwie dotyczącym ochrony danych.

W art. 4 lit. e) LPDP dane szczególnie chronione definiuje się jako „dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub etyczne, przynależność do związków zawodowych lub informacje dotyczące zdrowia lub życia seksualnego". W szczególności, w odniesieniu do danych dotyczących zdrowia, sekcja 4 lit. d) DPDP precyzuje tę definicję w kategoriach podobnych do kategorii ustanowionych przez Trybunał Sprawiedliwości Unii Europejskiej, stwierdzając, że dane szczególnie chronione są to „informacje dotyczące

przeszłego, obecnego i przyszłego zdrowia fizycznego i psychicznego osoby," oraz dodając, że „obejmują one między innymi dane dotyczące zdrowia ludzi, na przykład stopień niepełnosprawności lub informacje genetyczne".

Artykuł 18 LPDP ustanawia ogólną zasadę, że „nikogo nie można zmuszać do przekazania danych szczególnie chronionych. Można je przetwarzać wyłącznie za wyraźną, pisemną zgodą osoby, której dane dotyczą," następnie stwierdza się, że „dane szczególnie chronione mogą być gromadzone i przetwarzane ze względu na interes ogólny dopuszczony na mocy prawa lub gdy organizacja wnioskująca ma do tego mandat prawny. Dane takie mogą być również przetwarzane do celów statystycznych lub naukowych, gdy nie ma to związku z osobą fizyczną, do której odnoszą się dane".

W art. 19, w odniesieniu do danych dotyczących zdrowia, stwierdza się, że „publiczne lub prywatne ośrodki zdrowia i specjaliści w zakresie nauk medycznych mogą gromadzić i przetwarzać dane osobowe dotyczące fizycznego lub psychicznego zdrowia pacjentów, którymi się zajmują lub których leczą lub leczyli, o ile przestrzegają zasad poufności, szczegółowych przepisów i zapisów niniejszej ustawy", a w art. 17, odnoszącym się do przekazywania danych dotyczących zdrowia, stwierdza się, że zgodę osób fizycznych można wyłączyć jedynie w przypadkach, które „dotyczą zdrowotnych danych osobowych i gdy jest to konieczne ze względów na zdrowie publiczne, higienę, sytuacje nadzwyczajne lub na potrzeby badań epidemiologicznych, przy jednoczesnej ochronie tożsamości osób, których dane dotyczą, poprzez odpowiednie mechanizmy rozdzielające".

Ponadto art. 19 zakazuje „tworzenia baz danych przechowujących informacje, które w sposób bezpośredni lub pośredni ujawniają dane szczególnie chronione. Wyjątki przewiduje się w odniesieniu do baz danych będących w posiadaniu partii politycznych, związków zawodowych, kościołów, związków wyznaniowych, stowarzyszeń, fundacji i innych podmiotów niekomercyjnych do celów politycznych, religijnych lub filozoficznych lub do baz danych związanych ze związkami zawodowymi lub odnoszącymi się do pochodzenia rasowego bądź etnicznego, zdrowia lub życia seksualnego, w odniesieniu do szczegółowych danych ich partnerów lub członków, przy czym ujawnianie takich danych zawsze wymaga uprzedniej zgody osoby, której dane dotyczą".

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

Grupa robocza uważa, że zasada ta jest ujęta w art. 21 LPD, który odnosi się do okoliczności „gromadzenia adresów domowych, dystrybucji dokumentów, reklamy, sprzedaży i innych podobnych czynności".

Dlatego też, po odnotowaniu, że „przetwarzane mogą być dane, które umożliwiają utworzenie pewnych profili do celów promocyjnych, komercyjnych lub reklamowych, lub dane, które umożliwiają określenie zwyczajów konsumentów, jeżeli dane te pojawiają się w dokumentach dostępnych dla ogółu społeczeństwa, zostały dostarczone przez same osoby fizyczne lub zostały pozyskane za ich zgodą", oraz uznając we wszystkich przypadkach możliwość swobodnego wykonywania prawa do dostępu, w

ostatnim ustępie artykułu stwierdza się wyraźnie, że „osoba, której dane dotyczą, może w dowolnym momencie zażądać usunięcia lub zablokowania swoich danych w bazach danych, do których zastosowanie ma niniejszy artykuł".

> **3) Zautomatyzowana decyzja indywidualna**: w przypadku gdy celem przekazania danych jest podjęcie zautomatyzowanej decyzji w rozumieniu art. 15 dyrektywy, zainteresowana strona musi mieć prawo do poznania uzasadnienia takiej decyzji i należy podjąć inne środki w celu ochrony uzasadnionych interesów tej osoby.

Grupa robocza potwierdza, że zasada ta jest wyraźnie ujęta w art. 16 DPL, który opiera się na ogólnej zasadzie, że „ludzie mają prawo, aby nie być przedmiotem decyzji o skutkach prawnych, która może mieć na nich znaczny wpływ, opartej na przetwarzaniu danych, zautomatyzowanej lub niezautomatyzowanej, której celem jest ocena konkretnych aspektów ich osobowości, takich jak między innymi wyniki w pracy, sytuacja kredytowa, wiarygodność lub zachowanie".

Ponadto ustęp trzeci tego artykułu określa zasadę podobną do zasady, którą określono w dokumencie WP12, jako że przewiduje on, że „dana osoba ma prawo do uzyskania od administratora informacji dotyczących zarówno kryteriów oceny jak i programu wykorzystanego do przetwarzania danych, które zastosowano przy sporządzaniu wydanej decyzji".

3.3. Procedura/mechanizmy wykonania

Wydana przez grupę roboczą opinia WP12 „Przekazywanie danych osobowych do państw trzecich: stosowanie art. 25 i 26 unijnej dyrektywy o ochronie danych" wskazuje, że aby ocenić, czy systemy prawne państw trzecich zapewniają prawidłowy stopień ochrony, konieczne jest zidentyfikowanie nadrzędnych celów systemu przepisów w zakresie ochrony danych, a na tej podstawie należy ocenić różne sądowe i pozasądowe mechanizmy proceduralne stosowane w państwach trzecich.

W tym względzie cele system ochrony danych ma w zasadzie trzy cele:

- zapewnienie prawidłowego poziomu zgodności z przepisami;
- zapewnienie wsparcia i pomocy osobom fizycznym, których dane dotyczą;
- zapewnienie odpowiednich środków odszkodowawczych dla osób poszkodowanych w przypadku nieprzestrzegania przepisów.

> **a) Zapewnienie prawidłowego poziomu zgodności z przepisami:** dobry system na ogół charakteryzuje się tym, że administratorzy doskonale rozumieją swoje obowiązki, a osoby fizyczne swoje prawa i sposoby wykonywania tych praw. Skuteczne sankcje i środki zniechęcające odgrywają ważną rolę w kontekście zagwarantowania przestrzegania przepisów, co oczywiście dotyczy również systemów bezpośredniej weryfikacji przez władze, audytorów lub niezależnych urzędników zajmujących się ochroną danych.

Grupa robocza uważa, że cel ten jest spełniony poprzez różne przepisy zawarte w prawodawstwie urugwajskim, w szczególności przez następujące elementy:

Biuro ds. Regulacji i Kontroli w zakresie Danych Osobowych (URCDP)

W art. 31 LPDP ustanowiono organ kontrolny w zakresie ochrony danych, o nazwie „Biuro ds. Regulacji i Kontroli w zakresie Danych Osobowych" (URCDP – skrót w języku hiszpańskim), który jest „autonomiczną jednostką Agencji ds. Rozwoju Administracji Elektronicznej i Społeczeństwa Informacyjnego (AGESIC – skrót w języku hiszpańskim). Ta niezależna jednostka ma niezwykle szeroką autonomię o charakterze technicznym".

AGESIC obejmuje autonomiczne jednostki, do których należą wyżej wspomniane URCDP oraz Biuro ds. Dostępu do Informacji Publicznych (UAIP – skrót w języku hiszpańskim).

Grupa robocza odnotowuje uwagi władz urugwajskich dotyczące istnienia „biur ds. regulacji", które są autonomicznymi organami w ramach struktury organizacyjnej państwa, z autonomią o charakterze technicznym, niepodlegającymi żadnemu rodzajowi mandatu ani instrukcjom w zakresie swoich uprawnień, który odpowiada ogólnie przyjętemu w prawie Urugwaju zakresowi uprawnień ogólnych i branżowych organów regulacyjnych. Organizacja URCDP jest podobna do organizacji jednostek utworzonych na potrzeby planowania w zakresie telekomunikacji, energetyki czy informacji publicznych.

Jeżeli chodzi o strukturę tej jednostki, art. 31 LPDP przewiduje, że URCDP „będzie zarządzany przez radę złożoną z trzech członków: dyrektora wykonawczego AGESIC i dwóch członków powołanych przez władzę wykonawczą na podstawie ich doświadczeń osobistych, doświadczenia zawodowego i wiedzy tym zakresie, gwarantujących ich niezależny osąd, efektywność, obiektywność i bezstronność w realizacji obowiązków". Grupa robocza zauważa, że przywołana „władza wykonawcza" odnosi się do urzędu Prezydenta Republiki oraz że procedura powoływania członków organu kontrolnego jest ustanowiona na mocy prawa urugwajskiego.

Radzie wykonawczej pomaga rada doradcza, złożona z pięciu członków:

- osoby znanej ze względu na swoje doświadczenia w promowaniu i ochronie praw człowieka, powołanej przez władzę ustawodawczą i która nie może być aktywnym członek parlamentu;

- przedstawiciela władzy sądowniczej;

- przedstawiciela ministerstwa publicznego;

- przedstawiciela środowiska akademickiego;

- przedstawiciela sektora prywatnego, który jest wybierany zgodnie z przepisami.

Jeżeli chodzi o niezależność wspomnianego organu, grupa robocza odnotowała wystarczające dowody w prawodawstwie urugwajskim, szczególnie od zatwierdzenia DPDP, aby stwierdzić, że ma ona zastosowanie w przypadku URCDP.

Po pierwsze, LPDP wyraźnie stwierdza, że członkowie rady wykonawczej „nie otrzymują nakazów ani instrukcji dotyczących kwestii technicznych"; a władze urugwajskie wyjaśniły, że wyrażenie to należy rozumieć w jak najszerszym sensie.

Ponadto w art. 29 DPDP stwierdza się, że „działania administracyjne URCDP są prowadzone zgodnie z zasadami bezstronności, sprawności, efektywności, prawdy merytorycznej, bezpośredniości, należytego postępowania, promowania zatrudnienia, dobrej wiary, uzasadnionych decyzji i prostoty, które stanowią interpretacyjne kryteria wszelkich rozstrzygania kwestii, które mogą powstać w trakcie przetwarzania dowolnej kwestii".

Jednocześnie w odniesieniu do mandatu członków rady wykonawczej, LPDP ustanawia tymczasową kadencję i w sposób wyraźny ogranicza możliwość zwolnienia, wskazując w art. 31, że „z wyjątkiem dyrektora wykonawczego AGESIC kadencja członków trwa cztery lata, a każdy z nich może zostać wybrany ponownie. Członkowie kończą swoją pracę jedynie w przypadku zakończenia kadencji i powołania następców lub gdy zostaną zwolnieni przez władzę wykonawczą, w przypadku braku kompetencji, zaniechania lub przestępstwa, z zachowaniem gwarancji należytego postępowania".

Grupa robocza z zadowoleniem odnotowuje, że przepisy ustanowione w DPDP wzmacniają rolę dwóch członków zasiadających w radzie wykonawczej oprócz dyrektora wykonawczego AGESIC, natomiast rola tego ostatniego została znacznie ograniczona, co gwarantuje większą niezależność organu kontrolnego.

W tym sensie art. 21 DPDP przewiduje, że „funkcję przewodniczącego URCDP przejmuje rotacyjnie i corocznie jeden z trzech członków rady wykonawczej, z wyjątkiem dyrektora wykonawczego Agencji ds. Rozwoju Administracji Elektronicznej i Społeczeństwa Informacyjnego (AGESIC). W czasie tymczasowej nieobecności przewodniczącego URCDP, funkcję przewodniczącego sprawuje tymczasowo członek powołany przez władzę wykonawczą", co tym samym eliminuje możliwość, aby funkcja przewodniczącego biura przypadła dyrektorowi wykonawczemu AGESIC.

Fakt ten ma szczególne znaczenie, jeżeli uwzględnić, iż w art. 24 lit. a) DPDP stwierdza się, że uchwały rady są podejmowane większością, i dodaje, że „w przypadku braku rozstrzygnięcia, dana kwestia jest omawiana w czasie kolejnego posiedzenia, a jeżeli nie nastąpi żadna zmiana, głos przewodniczącego liczy się podwójnie". Dzięki temu wyklucza się sytuację, w której pojedynczy sprzeciw dyrektora wykonawczego AGESIC, którego kadencja podlega innemu systemowi niż kadencje pozostałych członków rady wykonawczej, byłby podstawą jakiejkolwiek decyzji podejmowanej przez organ kontrolny.

Grupa robocza stwierdza również, że uprawnienia przewodniczącego URCDP obejmują obowiązek „przyjmowania w sytuacjach nadzwyczajnych wszelkich środków, jakie uzna za stosowne, i powiadamiania o nich w czasie najbliższego posiedzenia rady wykonawczej oraz przestrzegania wszelkich, nowych podjętych uchwał".

Wreszcie grupa robocza przyjmuje, że niezależność organu kontrolnego została wykazana w praktyce, jako że nie nastąpiła żadna zmiana w działalności tego organu w konsekwencji zmiany rządu, która miała miejsce w Urugwaju w 2009 r., co

przedstawiono w informacjach przekazanych grupie roboczej przez URCDP, dotyczących działalności biura w latach 2009 i 2010.

Jeżeli chodzi o uprawnienia tego organu, grupa robocza z zadowoleniem potwierdza, że są one takie same, jak uprawnienia ustanowione w art. 28 dyrektywy w odniesieniu do organów kontrolnych w zakresie ochrony danych. W art. 34 LPDP stwierdza się, że URCDP będzie pełnił następujące funkcje i miał następujące uprawnienia:

- udzielanie pomocy i porad osobom, które potrzebują pomocy i porady, aby zrozumieć zakres przedmiotowej ustawy i instrumentów prawnych dostępnych do ochrony praw zagwarantowanych przez tę ustawę;

- określanie zasad i przepisów mających zastosowanie w prowadzeniu działań, których ta ustawa dotyczy;

- sporządzanie spisu baz danych, których dotyczy ta ustawa, oraz prowadzenie stałego rejestru wspomnianych baz danych;

- monitorowanie stopnia, w jakim administratorzy baz danych przestrzegają przepisów regulujących integralność, prawdziwość i bezpieczeństwo danych, z możliwością przeprowadzania wszelkich kontroli koniecznych do tego celu;

- żądanie informacji od podmiotów publicznych i prywatnych, które muszą przekazać wszelkie informacje uzupełniające, dokumenty, programy i inne elementy wymagane w związku z przetwarzaniem danych osobowych. W takich przypadkach organ musi gwarantować bezpieczeństwo i poufność przekazanych informacji i elementów;

- wydawanie opinii na żądanie właściwych władz, w tym wniosków w sprawie kar administracyjnych z tytułu naruszeń ustawy lub jakichkolwiek przepisów lub decyzji regulujących przetwarzanie danych osobowych podlegających ustawie;

- w razie konieczności służenie władzy wykonawczej doradztwem w zakresie sporządzania projektów ustaw, które odnoszą się, w całości lub częściowo, do ochrony danych osobowych;

- bezpłatne informowanie wszystkich o istnieniu osobowych baz danych, ich celach i tożsamości administratorów baz danych.

Ponadto, jak przedstawiono poniżej, LPDP obejmuje szczegółowe przepisy odnoszące się do dochodzeń, kontroli i sankcji, a DPDP ustanawia szczegółowe przepisy dotyczące niektórych procedur, które zgłasza się do URCDP, w szczególności dotyczące rejestrowania, przetwarzania i autoryzowania międzynarodowych transferów danych.

Grupa robocza stwierdza, że URCDP przedstawiła dowody dotyczące wykonywania tych uprawnień w ramach różnych informacji przekazanych w czasie analizy prawidłowości ochrony danych opisanej w niniejszym dokumencie.

Z wszystkich powyższych względów, wniosek grupy roboczej dotyczący tego punktu jest taki, że w Urugwaju istnieje organ nadzorczy w zakresie ochrony danych, który ma konieczną niezależność i odpowiednie uprawnienia wykonawcze, podobne do uprawnień ustanowionych w art. 28 dyrektywy.

Środki egzekwowania i sankcje

W art. 12 LPDP stwierdza się, że „administrator ponosi odpowiedzialność za wszelkie naruszenia przepisów niniejszej ustawy".

Jednym z zadań przypisanych URCDP na mocy art. 34 lit. e) jest „żądanie informacji od podmiotów publicznych i prywatnych, które muszą przekazać wszelkie informacje uzupełniające, dokumenty, programy i inne elementy wymagane w odniesieniu do przetwarzania danych osobowych. W takich przypadkach organ musi gwarantować bezpieczeństwo i poufność przekazanych informacji i elementów.

Jednocześnie art. 35 LPDP ustanawia możliwość zastosowania środków przymusu w przypadku naruszenia przepisów ustawy. W artykule tym stwierdza się, że „organ kontrolny może nałożyć następujące sankcje na administratorów baz danych lub osoby przetwarzające dane w przypadku naruszenia przepisów ustawy:

a) ostrzeżenie;
b) grzywna w kwocie nie większej niż pięćset tysięcy jednostek indeksowych;
c) zawieszenie odpowiedniej bazy danych. W tym celu AGESIC jest uprawniony do zalecenia właściwym jednostkom sądowniczym, aby zawiesiły bazy danych, w przypadku których udowodniono naruszenie ustawy, na okres do sześciu dni roboczych.

Możliwości stosowania przez URCDP środków przymusu w odniesieniu do tej kwestii są również ujęte w art. 31 DPDP, zgodnie z którym organ kontrolny może:

- prowadzić kontrole, które rada wykonawcza uzna za stosowne, na podstawie uzasadnionej decyzji;

- składać wnioski do właściwego sądu o podjęcie odpowiednich środków, jeżeli pojawia się ryzyko utraty danych. Wniosek o podjęcie takich środków wymaga uzasadnionej decyzji rady wykonawczej;

- informować o wszystkich działaniach administratora bazy danych lub osobę przetwarzającą dane w celu potwierdzenia danych, dając im termin dziesięciu dni od dnia po powiadomieniu, w którym to terminie mają zająć się daną sprawą. Po upływie tego terminu, rozpatrywane działania zostają przekazane radzie wykonawczej, która ma 30 dni na wydanie decyzji. Przyjęta uchwała może być zaskarżona zgodnie z obowiązującymi przepisami.

Wobec powyższych ustaleń grupa robocza uważa, że prawodawstwo urugwajskie zapewnia środki dochodzeniowe i sankcje podobne do tych, które ustanowiono w art. 28 dyrektywy w odniesieniu do organów nadzorczych państw członkowskich.

b) Zapewnienie wsparcia i pomocy osobom fizycznym, których dane dotyczą. Osoba, której dane dotyczą, musi mieć możliwość szybkiego i skutecznego dochodzenia swoich praw, bez nadmiernych kosztów. W tym celu musi istnieć pewnego rodzaju mechanizm instytucjonalny, umożliwiający niezależne rozpatrywanie skarg.

Grupa robocza zauważa, że prawodawstwo Urugwaju wprowadziło różnorodne mechanizmy służące realizacji tego celu.

Po pierwsze w art. 34 lit. a) LPDP stwierdza się, że „organ kontrolny musi prowadzić wszelkie konieczne działania służące zapewnieniu zgodności z celami i innymi przepisami niniejszej ustawy". Jednym z jego zadań jest „udzielanie pomocy i porad osobom, które ich potrzebują, aby zrozumieć zakres niniejszej ustawy i instrumentów prawnych dostępnych do ochrony praw zagwarantowanych przez tę ustawę."

W wyniku takiego działania może zostać wszczęte postępowanie wyjaśniające, a w odpowiednich przypadkach, procedury karne, przy czym zgodnie z DPDP postępowanie może zostać wszczęte przez sam organ kontrolny lub na wniosek zainteresowanej strony.

Ponadto art. 34 lit. h) określa również, że zadaniem URCDP jest m.in. „bezpłatne informowanie wszystkich o istnieniu osobowych baz danych, ich celach i tożsamości administratorów baz danych", regulując procedury rejestracyjne i kwestie dotyczące rejestrów.

Oprócz powyższych obowiązków prawodawstwo urugwajskie przewiduje środki, które należy podejmować w celu zwiększania wiedzy o przepisach dotyczących ochrony danych zarówno wśród osób, których dane dotyczą, jak i wśród podmiotów, które są zobowiązane do przestrzegania tych przepisów.

Cel ten osiąga się m.in. przez zapewnianie przejrzystości w upowszechnianiu decyzji i opinii URCDP. W tym celu w ustępie pierwszym art. 25 DPDP stwierdza się, że „URCDP publikuje każdą podjętą decyzję na swojej stronie internetowej, po jej notyfikacji. Publikacji tej dokonuje się z zastosowaniem odpowiednich kryteriów gwarantujących wyłączenie danych osobowych".

Grupa robocza uważa, że drugim kanałem pomocy dla zainteresowanych stron zaniepokojonych w związku z ochroną swoich praw jest dochodzenie prawa „habeas data", przewidziane w rozdziale VII LPDP.

W art. 38 ustawy przewiduje się zatem, że osoba, której dane dotyczą, może wnieść skargę „habeas data" lub wystąpić pisemnie przeciwko wszystkim administratorom publicznych lub prywatnych baz danych, w następujących sytuacjach:

- gdy osoba, której dane dotyczą, chce zapoznać się z danymi osobowymi zarejestrowanymi w bazie danych lub podobnej bazie i jej wniosek spotyka się z odmową lub dane nie są przekazane przez administratora bazy danych w określonych prawem okolicznościach i ramach czasowych;

- gdy osoba, której dane dotyczą, zwraca się do administratora bazy danych lub osoby przetwarzającej bazę danych o sprostowanie, uaktualnienie, wyeliminowanie, wprowadzenie lub usunięcie danych, a administrator nie dostosowuje się do tego wniosku ani nie przedstawia dostatecznego uzasadnienia niedostosowania się do niego w terminie określonym prawem;

Jest to czynność prawna, która jest przeprowadzana szybko i która może zostać wszczęta przez osobę, której dane dotyczą, lub jej prawnych przedstawicieli, a w przypadku osób zmarłych, przez ich następców prawnych. Czynność tę regulują przepisy proceduralne, a ich elementy charakterystyczne są określone w LPDP.

Zgodnie z art. 43 LPDP „wyrok bazujący na nakazie „habeas data" powinien zawierać:

- wyraźne wskazanie organu lub osoby, przeciwko któremu/której wniesiono wniosek i przeciwko którego/której działaniu, czynowi lub zaniechaniu wydano decyzję dotyczącą „habeas data";

- precyzyjny nakaz określający, co powinno lub nie powinno zostać zrobione i, w odpowiednich przypadkach, okres obowiązywania przedmiotowej decyzji;

- termin wykonania decyzji, który jest ustalany przez sąd na podstawie okoliczności każdej sprawy, i nieprzekracza 15 kolejnych i nieprzerwanych dni kalendarzowych, licząc od daty powiadomienia.

Wobec powyższych informacji i jak już wskazano, grupa robocza uznaje, że prawodawstwo urugwajskie oferuje wystarczające mechanizmy zapewniające pomoc i wsparcie zainteresowanym stronom.

c) Zapewnienie odpowiednich środków odszkodowawczych dla osób poszkodowanych w przypadku nieprzestrzegania przepisów: jest to kluczowy element, który musi być uwzględniony w systemie umożliwiającym wydawanie decyzji sądowych i arbitrażowych, a w odpowiednich przypadkach udzielanie odszkodowań i nakładanie sankcji.

W art. 12 LPDP stwierdza się, że „administrator ponosi odpowiedzialność za wszelkie naruszenia przepisów niniejszej ustawy".

Grupa robocza zauważa, że na mocy przepisów tego artykułu i przepisów ogólnych urugwajskiego prawa cywilnego, a w szczególności kodeksu cywilnego, zainteresowana strona, która poniosła szkody w konsekwencji przetwarzania jej danych osobowych, może żądać odpowiednich środków odszkodowawczych. Takie środki odszkodowawcze mogą odnosić się zarówno do poniesionych szkód materialnych, jak i szkód moralnych.

Dlatego też grupa robocza uważa, że prawo urugwajskie przewiduje odpowiednią gwarancję w tym zakresie.

4. WYNIKI OCENY

W konkluzji, biorąc pod uwagę wszystkie powyższe czynniki, grupa robocza uważa, że **Wschodnia Republika Urugwaju zapewnia prawidłowy stopień ochrony** w rozumieniu 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 takich danych.

Grupa robocza podkreśla również fakt, że w ramach wszelkich decyzji podejmowanych przez Komisję, Komisja będzie ściśle obserwować zmiany w zakresie ochrony danych w Urugwaju i sposób stosowania przez organ ds. ochrony danych („URCDP") zasad ochrony danych, o których mowa w dokumencie WP12 i w niniejszym dokumencie.

Sporządzono w Brukseli, dnia 12 października 2010 r.

W imieniu grupy roboczej,
Przewodniczący
Jacob KOHNSTAMM