Sprawa C-340/21

Streszczenie wniosku o wydanie orzeczenia w trybie prejudycjalnym złożonego zgodnie z art. 98 § 1 regulaminu postępowania przed Trybunałem

Data wpływu:

2 czerwca 2021 r.

Oznaczenie sądu odsyłającego:

Wyrchowen administratiwen syd (Bułgaria)

Data wydania postanowienia o wystąpieniu z wnioskiem o wydanie orzeczenia w trybie prejudycjalnym:

14 maja 2021 r.

Strona wnosząca skargę kasacyjną:

VB

Strona pozwana w postępowaniu kasacyjnym:

Nacionałna agencija za prichodite

Przedmiot postępowania głównego

Skarga na wyrok sądu, w którym oddalono jako bezzasadne powództwo o odszkodowanie za szkody niemajątkowe wyrządzone w następstwie niezgodnej z prawem bezczynności strony pozwanej działającej w charakterze administratora danych osobowych, polegającej na niewykonaniu w wystarczającym stopniu obowiązków określonych w Zakon za zasztita na licznite danni (ustawie o ochronie danych osobowych) i w rozporządzeniu 2016/679.

Przedmiot i podstawa prawna wniosku o wydanie orzeczenia w trybie prejudycjalnym

Odesłanie prejudycjalne, na podstawie art. 267 TFUE, dotyczące wykładni motywów 74, 85 i 146, art. 4 pkt 12, art. 5 ust. 2, art. 24, 32 i 82 rozporządzenia 2016/679.

Pytania prejudycjalne

1. Czy art. 24 i 32 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólnego rozporządzenia o ochronie danych) należy interpretować w ten sposób, że wystarczające jest zrealizowanie nieuprawnionego ujawnienia lub dostępu do danych osobowych w rozumieniu art. 4 pkt 12 rozporządzenia 2016/679 przez osoby, które nie są urzędnikami w administracji administratora danych osobowych i nie są pod jego kontrolą, aby przyjąć, że zastosowane środki techniczne i organizacyjne nie są odpowiednie?

2. Na wypadek udzielenia odpowiedzi przeczącej na pytanie pierwsze, jaki powinien być przedmiot i zakres sądowej kontroli zgodności z prawem przy weryfikacji, czy zastosowane przez administratora danych osobowych środki techniczne i organizacyjne, o których mowa w art. 32 rozporządzenia 2016/679, są odpowiednie?

3. Na wypadek udzielenia odpowiedzi przeczącej na pytanie pierwsze, czy zasadę rozliczalności określoną w art. 5 ust. 2 oraz art. 24 w związku z motywem 74 rozporządzenia 2016/679 należy interpretować w ten sposób, że w postępowaniu z powództwa określonego w art. 82 ust. 1 rozporządzenia 2016/679 na administratorze danych osobowych ciąży ciężar dowodu odnośnie do okoliczności, że zastosowane środki techniczne i organizacyjne, o których mowa w art. 32 rozporządzenia, są odpowiednie? Czy zarządzenie sporządzenia opinii przez biegłego sądowego można uznać za niezbędny i wystarczający środek dowodowy dla celów ustalenia, czy zastosowane przez administratora danych osobowych środki techniczne i organizacyjne są odpowiednie w sytuacji takiej jak rozpatrywana, w której nieuprawniony dostęp i ujawnianie danych osobowych jest rezultatem „ataku hakerskiego”?

4. Czy art. 82 ust. 3 rozporządzenia 2016/679 należy interpretować w ten sposób, że nieuprawnione ujawnienie lub dostęp do danych osobowych w rozumieniu art. 4 pkt 12 rozporządzenia 2016/679 – w niniejszym wypadku poprzez „atak hakerski” osób, które nie są urzędnikami w administracji administratora danych osobowych i nie są pod jego kontrolą – jest zdarzeniem, w odniesieniu do którego administrator danych osobowych w żaden sposób nie ponosi winy, i jest podstawą zwolnienia z odpowiedzialności?

5. Czy art. 82 ust. 1 i 2 w związku z motywami 85 i 146 preambuły rozporządzenia 2016/679 należy interpretować w ten sposób, że w sytuacji takiej jak rozpatrywana, w której naruszono bezpieczeństwo danych osobowych poprzez nieuprawniony dostęp i rozpowszechnianie danych osobowych zrealizowane w ramach „ataku hakerskiego”, same w sobie przeżyte przez podmiot danych osobowych obawy, zmartwienia i strach przed ewentualnym przyszłym nadużyciem danych osobowych – bez zaistnienia takiego nadużycia lub

wyrządzenia innej szkody podmiotowi danych – są objęte szerokim rozumieniem pojęcia szkód niematerialnych i stanowi [to] podstawę do zasądzenia odszkodowania?

Przepisy i orzecznictwo Unii Europejskiej

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (zwane dalej „rozporządzeniem") – motywy 1, 4, 6, 74, 75, 76, 77, 83, 85, 146, art. 4 pkt 2, 7 i 12, art. 5, 24, 32, 33, 79, 82.

Wyrok Trybunału Sprawiedliwości Unii Europejskiej z dnia 30 maja 2013 r., Worten, C- 342/12, EU:C:2013:355, pkt 24, 26.

Prawo krajowe

Administratiwnoprocesualen kodeks (kodeks postępowania administracyjnego) – art. 144 ust. 1, art. 203 i 208.

Grażdanski procesualen kodeks (kodeks postępowania cywilnego) – art. 154.

Zakon za otgowornostta na dyrżawata i obsztinite za wredi (ustawa o odpowiedzialności państwa i gmin za szkody) – art. 1.

Zakon za zasztita na licznite danni – art. 39 ust. 1 i 2, art. 59 ust. 1.

Zwięzłe przedstawienie okoliczności faktycznych i postępowania głównego

1 Nacionałna agencija za prichodite (narodowa agencja przychodów skarbowych i z tytułu składek zabezpieczenia społecznego, zwana dalej „NAP") jest administratorem danych osobowych w rozumieniu art. 4 ust. 7 rozporządzenia. Zgodnie z prawem krajowym jest ona wyspecjalizowanym organem państwowym przy ministyr na finansite (ministrze finansów) określającym, zabezpieczającym i egzekwującym wierzytelności publiczne oraz określone w prawie prywatne wierzytelności urzędowe. W wykonaniu zleconych jej funkcji publicznych przetwarza ona dane osobowe.

2 W dniu 15 lipca 2019 r. bułgarskie media opublikowały informacje, zgodnie z którymi miał miejsce nieuprawniony dostęp do systemu informacyjnego NAP, zaś w Internecie opublikowano informacje z bazy danych NAP obejmujące dane osobowe, podatkowe i ubezpieczeniowe. Dotkniętych tym naruszeniem jest 4 057 328 bułgarskich obywateli, a łącznie poszkodowanych jest 6 074 140 osób fizycznych – bułgarskich obywateli i cudzoziemców. Wśród osób poszkodowanych ujawnieniem wspomnianych danych jest VB.

3 Do chwili obecnej nie wydano orzeczenia w stosunku do osób odpowiedzialnych za niedozwolony dostęp – nazwany w środkach masowego przekazu „atakiem hakerskim”.

4 Po zaistnieniu niedozwolonego dostępu setki obywateli wniosły powództwa przeciwko NAP o zasądzenie odszkodowania za szkody niemajątkowe.

5 W dniu 16 września 2019 r. VB wniosła powództwo przeciwko NAP przed Administratiwen syd Sofija – grad (sąd administracyjny dla miasta Sofia) o zasądzenie odszkodowania w wysokości 1000 BGN (około 511 EUR) na podstawie art. 82 ust. 1 rozporządzenia, art. 1 ust. 1 Zakon za otgovornostta na dyrżawata i obsztinite za wredi oraz art. 39 ust. 1 Zakon za zasztita na licznite danni.

6 W pozwie złożonym w pierwszej instancji VB twierdzi, że NAP „nie wykonała w najlepszym stopniu” swojego obowiązku „zabezpieczenia swojego cyberbezpieczeństwa w bezusterkowy sposób” i „zapewnienia w najwyższym stopniu w skuteczny sposób bezpieczeństwa danych osobowych obywateli Republiki Bułgarii”. W związku z powyższym doszło do naruszenia bezpieczeństwa danych osobowych w rozumieniu art. 4 pkt 12 rozporządzenia i niezgodnego z prawem ujawnienia danych osobowych.

7 Według VB „brak dołożenia należytej staranności i zastosowania skutecznych środków ochrony bezpieczeństwa danych” stanowi bezczynność NAP w zakresie wykonywania jej obowiązków związanych z ochroną danych obywateli i skutkuje naruszeniem art. 24 i 32 rozporządzenia. Jako administrator danych osobowych NAP powinna była przetwarzać dane osobowe w sposób „zapewniający odpowiedni poziom bezpieczeństwa” – poprzez zastosowanie odpowiednich środków technicznych i organizacyjnych.

8 VB wskazuje, że w następstwie niewykonania obowiązków przez NAP poniosła szkody niemajątkowe, wyrażające się w zmartwieniach i obawach, że jej dane osobowe mogą być przedmiotem nadużycia w przyszłości, na przykład poprzez zabór jej majątku, nadużycia dotyczące jej rachunków bankowych, wyłudzenia kredytów na jej nazwisko, zmiany w zakresie jej stanu cywilnego lub kradzież jej tożsamości. Jest oburzona dokonanym „wielkim włamaniem do systemu informacyjnego NAP” i wydaje się jej, iż nie jest chroniona przez państwo. Obawia się szantażu, napadu lub porwania.

9 Według NAP powództwo jest bezzasadne. VB nie wniosła do NAP o udzielenie informacji o tym, do jakich konkretnie danych osobowych uzyskano dostęp.

10 Po zaistnieniu niedozwolonego dostępu NAP natychmiast podjęła środki w celu ochrony praw i interesów obywateli. Przeprowadzono spotkania z przedstawicielami i ekspertami służb bezpieczeństwa, izby notarialnej, rejestru działalności gospodarczej, stowarzyszenia banków komercyjnych i innych podmiotów, tak aby skoordynować działania mające na celu ograniczenie skutków

niedozwolonego dostępu. W witrynie internetowej NAP utworzono specjalne rubryki dotyczące cyberataku, w których publikuje się aktualne informacje.

11 Według NAP nie istnieje związek przyczynowy między podnoszonymi szkodami niemajątkowymi a niedozwolonym dostępem do danych osobowych. NAP została zaatakowana w złej wierze przez osoby trzecie, które nie są jej urzędnikami. Z tego względu nie powinna ponosić odpowiedzialności za spowodowane szkodliwe skutki.

12 NAP twierdzi, że przyjęła szereg środków, a mianowicie ustanowiła systemy zarządzania procesami i bezpieczeństwem informacji; zatwierdziła procedury, które są zgodne z międzynarodowymi standardami jakości ISO 9000 i ISO 9001; stosuje polityki, reguły, procedury, wskazówki i metodyki zarządzania bezpieczeństwem informacji.

13 NAP przedstawiła dowody, a mianowicie różne dokumenty wewnętrzne z okresu od stycznia 2013 r. do maja 2019 r. dotyczące: zawartości, trybu tworzenia, utrzymywania i dostępu do baz danych; wdrożenia systemów zarządzania bezpieczeństwem informacji; procedur prewencji; wewnętrznych reguł bezpieczeństwa sieci i informacji; wytycznych w zakresie pracy z informacjami; polityki ochrony danych osobowych; środków ochrony danych osobowych; metodologii i procedury oceny ryzyka.

14 W wyroku z dnia 27 listopada 2020 r. Administratiwen syd Sofija – grad oddalił skargę VB jako bezpodstawną.

15 Administratiwen syd Sofija – grad wskazuje, że nieuprawniony dostęp do bazy danych NAP miał miejsce w następstwie „ataku hakerskiego” osób, wobec których wszczęto postępowanie przygotowawcze, które jeszcze się nie zakończyło.

16 Niezgodny z prawem skutek nie umożliwia założenia, że administrator danych nie spełnił swoich obowiązków w zakresie stosowania odpowiednich środków technicznych i organizacyjnych w celu zapewnienia ochrony bazy danych – tak aby żadna osoba, w żaden sposób i za pomocą żadnych środków nie mogła uzyskać dostępu do tej bazy danych.

17 Administratiwen syd Sofija – grad jest zdania, że powódka powinna wskazać, jakie faktyczne (techniczne) czynności powinna zrealizować NAP, lecz ich nie wykonała lub wykonała je nieodpowiednio, tak że wywołała lub przyczyniła się do wywołania skutku wyrażającego się w nieuprawnionym dostępie i ujawnieniu danych osobowych.

18 Według Administratiwen syd Sofija – grad nie miała miejsca bezczynność administratora danych osobowych, biorąc pod uwagę przedstawione dowody. VB nie wyrządzono szkód niemajątkowych, za które należałoby się odszkodowanie. Przeżyty emocjonalny dyskomfort wywołany wiadomością o niedozwolonym dostępie do systemu informacyjnego NAP był zwykły, lecz nie stanowił

faktycznie zaistniałej szkody w rozumieniu ustawy. VB nie zainteresowała się tym, do których dokładnie z jej danych osobowych uzyskano dostęp, a takie zachowanie nie wykazuje istnienia silnego stresu emocjonalnego.

19 Administratiwen syd Sofija – grad przyjął, że publiczne ogłoszenie o niezgodnym z prawem dostępie do bazy danych NAP nie wywarło wpływu na życie VB, jeśli chodzi o jej samopoczucie, samoocenę, pracę, stosunki z bliskimi osobami i stan zdrowia. Nie istnieje związek przyczynowo–skutkowy z przeżytymi negatywnymi emocjami, ponieważ nie wynikały one z zachowania NAP.

20 VB zaskarżyła wyrok Administratiwen syd Sofija – grad przed sąd odsyłającym, Wyrchowen administratiwen syd (najwyższym sądem administracyjnym).

Zasadnicze argumenty stron w postępowaniu głównym

21 W skardze kasacyjnej VB twierdzi, że Administratiwen syd Sofija – grad nieprawidłowo rozłożył ciężar dowodu związany z wykazaniem negatywnej okoliczności, a mianowicie bezczynności administratora danych osobowych w zakresie stosowania odpowiednich środków technicznych i organizacyjnych.

22 Według VB stosowanie skutecznych środków jest objęte operacyjną samodzielnością NAP, w związku z czym niemożliwe jest opisanie, jakie dokładnie konkretne obowiązki powinni byli wykonywać urzędnicy NAP, lecz nie wykonali ich. Przedstawione przez NAP dowody nie wykazują, że zastosowane organizacyjne i techniczne środki są odpowiednie.

23 VB twierdzi, że zmartwienia związane z możliwymi w przyszłości nadużyciami danych osobowych nie są hipotetycznymi, lecz realnymi szkodami niemajątkowymi, które podlegają odszkodowaniu. Nie jest konieczne przedstawienie przez nią dowodów w celu wykazania zwykłych szkód niemajątkowych.

24 Według NAP Administratiwen syd Sofija – grad prawidłowo przyjął, że działając w charakterze administratora danych osobowych, NAP nie była bezczynna i przyjęła szereg środków technicznych i organizacyjnych w celu zapewnienia ochrony przy przetwarzaniu danych osobowych. Nie istnieją dowody faktycznego wyrządzenia szkód. Za zmartwienia i strach odnoszące się do przyszłych zdarzeń nie należy się odszkodowanie.

Zwięzłe przedstawienie uzasadnienia wniosku o wydanie orzeczenia w trybie prejudycjalnym

25 Podobne postępowania sądowe przeciwko NAP zakończyły się w pierwszej instancji wydaniem sprzecznych orzeczeń. Powództwa albo oddalano jako bezzasadne, albo uwzględniano w całości lub częściowo. Uregulowania

normatywne były interpretowane i stosowane w sprzeczny sposób w odniesieniu do wszystkich elementów odpowiedzialności administratora danych osobowych.

26 Według Wyrchowen administratiwen syd faktyczne znamiona odpowiedzialności określonej w art. 82 rozporządzenia obejmują: (i) naruszenie tego rozporządzenia przez administratora danych osobowych; (ii) wyrządzone podmiotowi danych osobowych szkody materialne lub niematerialne; (iii) związek przyczynowy między wyrządzoną szkodą a tym naruszeniem.

W przedmiocie pytania pierwszego

27 Zgodnie z art. 24 ust. 1 rozporządzenia administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z tym rozporządzeniem i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane.

28 W art. 32 rozporządzenia przewidziano obowiązki administratora dotyczące bezpieczeństwa przetwarzania, które są związane z jego odpowiedzialnością określoną w art. 24 i ją rozwijają, przy czym wskazano kryteria, zgodnie z którymi należy stosować odpowiednie środki techniczne i organizacyjne w celu zapewnienia poziomu bezpieczeństwa uwzględniającego ryzyko. Są to „stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze”.

29 W rozporządzeniu nie wskazano definicji pojęcia „odpowiednich środków technicznych i organizacyjnych”. W motywie 74 wskazano, że administrator powinien mieć obowiązek wdrożenia odpowiednich i skutecznych środków oraz powinien być w stanie wykazać, że czynności przetwarzania są zgodne z rozporządzeniem oraz że są skuteczne.

30 Powyższe prowadzi do wniosku, że administrator danych osobowych powinien dokonać oceny ryzyka według określonych w art. 32 rozporządzenia kryteriów, na podstawie których powinien zastosować środki techniczne i organizacyjne, które są odpowiednie przy uwzględnieniu wymaganego poziomu bezpieczeństwa danych osobowych według poziomu ryzyka. Poprzez ustanowienie odpowiednich środków technicznych i organizacyjnych administrator danych osobowych zapewnia przetwarzanie danych osobowych zgodnie z rozporządzeniem.

31 Ze wskazanych uregulowań prawnych wynika, że wybór odpowiednich środków technicznych i organizacyjnych jest związany z kwestią celowości. Ocena celowości przez administratora danych osobowych nie jest jednak przedmiotem kontroli sądowej, ponieważ sąd przeprowadza kontrolę zgodności z prawem. Równocześnie, przetwarzanie danych osobowych w warunkach samodzielności operacyjnej przy wyborze środków technicznych i organizacyjnych powinno mieć miejsce w ramach rozporządzenia i przy przestrzeganiu celu związanego z ochroną prawa podstawowego do ochrony danych osobowych osób fizycznych.

32 Mając na względzie powyższe, Wyrchowen administratiwen syd wnosi o wyjaśnienie, czy art. 24 i 32 rozporządzenia należy interpretować w ten sposób, że samo wystąpienie niezgodnego z prawem skutku w formie nieuprawnionego ujawnienia lub dostępu do danych osobowych w rozumieniu art. 4 pkt 12 rozporządzenia wykazuje, że zastosowane przez administratora danych osobowych środki techniczne i organizacyjne nie były odpowiednie.

Pytanie drugie (na wypadek udzielenia odpowiedzi przeczącej na pytanie pierwsze)

33 Ze względu na to, że wybór i stosowanie środków technicznych i organizacyjnych są objęte subiektywną oceną administratora danych osobowych i jego operacyjną samodzielnością, Wyrchowen administratiwen syd dąży do ustalenia, jaki powinien być przedmiot i zakres sądowej kontroli zgodności z prawem przy sprawdzeniu, czy zastosowane przez administratora danych osobowych środki techniczne i organizacyjne są odpowiednie i zgodne z art. 24 i 32 rozporządzenia.

34 Wyrchowen administratiwen syd powziął wątpliwości, czy wystarczające jest ustalenie przez sąd, w jaki sposób administrator danych osobowych wykonał wynikające z obydwu tych przepisów obowiązki, czy też sąd powinien zbadać co do istoty ustanowione i zastosowane środki techniczne i organizacyjne, które wskazano przecież wyłącznie przykładowo w rozporządzeniu, a ich ustanowienie jest dokonywane według ich celowości.

Pytanie trzecie (na wypadek udzielenia odpowiedzi przeczącej na pytanie pierwsze)

35 Zgodnie z art. 5 ust. 2 rozporządzenia administrator ponosi odpowiedzialność i powinien móc wykazać przestrzeganie określonych w art. 5 ust. 1 zasad dotyczących przetwarzania danych osobowych. W art. 24 ust. 1 rozporządzenia wskazano, że administrator danych osobowych „wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z […] rozporządzeniem i aby móc to wykazać”.

36 W art. 82 ust. 3 rozporządzenia umożliwiono administratorowi lub podmiotowi przetwarzającemu dane osobowe zwolnienie się z odpowiedzialności określonej w art. 82 ust. 2, „jeżeli udowodnią, że w żaden sposób nie ponoszą winy za zdarzenie, które doprowadziło do powstania szkody”. W tym ostatnim ustępie nałożono na administratora danych osobowych odpowiedzialność za szkody wynikające z przetwarzania dokonanego z naruszeniem przepisów rozporządzenia.

37 Zgodnie z prawem krajowym w postępowaniu wszczętym na podstawie powództwa każda ze stron powinna wykazać okoliczności faktyczne, na których opiera swoje żądania lub zarzuty. W analogicznych sprawach sądy pierwszej instancji rozkładały ciężar dowodu między powoda i pozwanego w różny sposób.

38 W niniejszym wypadku istotna jest kwestia, czy zasadę rozliczalności określoną w art. 5 ust. 2 w związku z motywem 74 i art. 24 ust. 1 rozporządzenia należy interpretować w ten sposób, że przepisy te rozkładają ciężar dowodu w ten sposób, że administrator danych osobowych, przeciwko któremu wniesiono powództwo dotyczące odpowiedzialności za szkody wyrządzone ze względu na naruszenie rozporządzenia, ma obowiązek, jako strona pozwana, wykazania, że zastosowane przez niego środki techniczne i organizacyjne są odpowiednie.

39 Poza kwestią związaną z przedmiotem i zakresem kontroli sądowej dotyczącej przestrzegania obowiązków określonych w rozporządzeniu istnieje kwestia, w jaki sposób i za pomocą jakich środków dowodowych należy przeprowadzić kontrolę ich przestrzegania, a w szczególności, czy zastosowano wszystkie odpowiednie środki techniczne i organizacyjne.

40 W sprawie NAP przedstawiła dowody zapewnienia ochrony sieci informacyjnych zgodnie ze wskazanymi w dokumentach standardami, lecz nie zarządzono sporządzenia opinii biegłego sądowego z zakresu techniki, w której ustalono by, czy środki techniczne i organizacyjne były odpowiednie w rozumieniu rozporządzenia. Wyrchowen administratiwen syd jest wiadome, że taki administrator danych osobowych, jakim jest NAP, ma obowiązek stosowania organizacyjnych, technologicznych i technicznych środków bezpieczeństwa sieciowego i informacyjnego, jakie są proporcjonalne w stosunku do zagrożeń wynikających z cyberprzestępczości, w celu zminimalizowania ryzyka ich realizacji. Jednakże dostęp biegłych sądowych do akt każdej sprawy na podstawie art. 82 rozporządzenia mógłby wywrzeć nowe, niekorzystne skutki względem ochrony danych osobowych.

41 Biorąc pod uwagę postęp techniczny, istniejące standardy ochrony informacyjnych systemów sieciowych i nieuprawniony dostęp w ramach „ataku hakerskiego” dokonanego przez osoby, które są podmiotami zewnętrznymi w stosunku do administracji administratora danych osobowych, Wyrchowen administratiwen syd dąży do ustalenia, czy zarządzenie sporządzenia opinii biegłego sądowego z zakresu techniki można uznać za niezbędny i wystarczający środek dowodowy, za pomocą którego można by ustalić, czy ustanowione i zastosowane środki techniczne i organizacyjne były odpowiednie, aby zapewnić ochronę danych osobowych.

W przedmiocie pytania czwartego

42 Działając w charakterze administratora uczestniczącego w przetwarzaniu danych osobowych, NAP ponosi odpowiedzialność, lecz może się z niej zwolnić na podstawie art. 82 ust. 3, jeżeli udowodni, że w żaden sposób nie ponosi winy za zdarzenie, które doprowadziło do powstania szkody.

43 W sprawie jest bezsporne, że dostęp do danych osobowych został uzyskany w następstwie „ataku hakerskiego” skierowanego przeciwko NAP, zaś nieuprawniony dostęp i ujawnienie danych osobowych nie miały miejsca przy

przetwarzaniu danych osobowych przez urzędników NAP ani ze względu na to przetwarzanie.

44 Wyrchowen administratiwen syd dąży do ustalenia, czy w niniejszym wypadku możliwe jest przyjęcie, że zaistniało zdarzenie, za które administrator danych osobowych w żaden sposób nie ponosi winy, i okoliczność ta, odpowiednio, zwalnia go z odpowiedzialności.

W przedmiocie pytania piątego

45 VB dochodzi odszkodowania za szkody niemajątkowe wyrażające się zmartwieniami, strachem, stresem, poczuciem braku bezpieczeństwa i obawami, że jej dane osobowe będą stanowiły w przyszłości przedmiot nadużyć na różne, opisane przez VB, sposoby. Nie istnieją informacje dotyczące popełnienia nadużyć z użyciem danych osobowych VB.

46 Jak wynika z motywów 75 i 85 rozporządzenia, przy wskazywaniu przykładów szkód materialnych lub niematerialnych uwzględnia się istotę danych osobowych i niekorzystne skutki dla podmiotów tych danych, a nie wyłącznie ich wewnętrzne przeżycia.

47 W motywie 146 rozporządzenia określono granicę odpowiedzialności i jest nią całość szkody, jaka mogła zostać wyrządzona danej osobie w wyniku przetwarzania danych naruszającego przepisy rozporządzenia.

48 Po jednokrotnym uzyskaniu dostępu do nich, dane osobowe podmiotu danych mogą być przedmiotem szeregu nadużyć o charakterze niemajątkowym i majątkowym, które mają znaczące skutki. W społeczeństwie znane są wypadki takich nadużyć, co może uzasadnić wyższy stopień niepokoju osób dotkniętych dokonanym „atakiem hakerskim”. W niniejszym wypadku, mając na względzie brak danych dotyczących już dokonanego nadużycia, przyszłe nadużycie jest tylko założeniem, hipotezą z prawdopodobnym, lecz niepewnym ryzykiem dla praw podmiotu danych osobowych.

49 Powyższe nasuwa pytanie, czy negatywne emocjonalne przeżycia podmiotu danych osobowych w takim kontekście – to jest sam fakt stworzenia niebezpieczeństwa wynikającego z ewentualnego niezgodnego z prawem użycia tych danych – są objęte szerokim rozumieniem pojęcia szkód niematerialnych i stanowi to podstawę do zasądzenia odszkodowania określonego w art. 82 ust. 1 w związku z motywem 146 rozporządzenia.

50 Możliwe jest jednak, iż art. 82 ust. 1 w związku z motywem 146 rozporządzenia nie można interpretować w ten sposób, że każde negatywne przeżycie, strach lub zmartwienie danej osoby uprawnia do odszkodowania za wyrządzoną szkodę niemajątkową – bez uprzedniego niezgodnego z prawem użycia danych osobowych, na przykład poprzez pozbawienie mienia, zaciągnięcie kredytów na nazwisko podmiotu danych osobowych lub kradzież tożsamości.