Zbiór Orzeczeń

WYROK TRYBUNAŁU (trzecia izba)

z dnia 14 grudnia 2023 r.*

Odesłanie prejudycjalne – Ochrona osób fizycznych w zakresie przetwarzania danych osobowych – Rozporządzenie (UE) 2016/679 – Artykuł 5 – Zasady dotyczące owego przetwarzania – Artykuł 24 – Obowiązki administratora – Artykuł 32 – Środki wdrożone w celu zapewnienia bezpieczeństwa przetwarzania – Ocena odpowiedniego charakteru takich środków – Granice kontroli sądowej – Przeprowadzanie dowodów – Artykuł 82 – Prawo do odszkodowania i odpowiedzialność – Ewentualne wyłączenie odpowiedzialności administratora w przypadku naruszenia popełnionego przez osoby trzecie – Żądanie zadośćuczynienia za szkodę niemajątkową wynikającą z obawy przed ewentualnym wykorzystaniem danych osobowych w sposób stanowiący nadużycie

W sprawie C-340/21

mającej za przedmiot wniosek o wydanie, na podstawie art. 267 TFUE, orzeczenia w trybie prejudycjalnym, złożony przez Varhoven administrativen sad (najwyższy sąd administracyjny, Bułgaria) postanowieniem z dnia 14 maja 2021 r., które wpłynęło do Trybunału w dniu 2 czerwca 2021 r., w postępowaniu:

VB

przeciwko

Natsionalna agentsia za prihodite,

TRYBUNAŁ (trzecia izba),

w składzie: K. Jürimäe, prezes izby, N. Piçarra, M. Safjan, N. Jääskinen (sprawozdawca) i M. Gavalec, sędziowie,

rzecznik generalny: G. Pitruzzella,

sekretarz: A. Calot Escobar,

uwzględniając pisemny etap postępowania,

rozważywszy uwagi, które przedstawili:

– w imieniu Natsionalna agentsia za prihodite – R. Spetsov,

* Język postępowania: bułgarski.

– w imieniu rządu bułgarskiego – M. Georgieva i L. Zaharieva, w charakterze pełnomocników,

– w imieniu rządu czeskiego – O. Serdula, M. Smolek i J. Vláčil, w charakterze pełnomocników,

– w imieniu Irlandii – M. Browne, Chief State Solicitor, A. Joyce, J. Quaney i M. Tierney, w charakterze pełnomocników, których wspierał D. Fennelly, BL,

– w imieniu rządu włoskiego – G. Palmieri, w charakterze pełnomocnika, którą wspierał E. De Bonis, avvocato dello Stato,

– w imieniu rządu portugalskiego – P. Barros da Costa, A. Pimenta, J. Ramos i C. Vieira Guerra, w charakterze pełnomocników,

– w imieniu Komisji Europejskiej – A. Bouchagiar, H. Kranenborg i N. Nikolova, w charakterze pełnomocników,

po zapoznaniu się z opinią rzecznika generalnego na posiedzeniu w dniu 27 kwietnia 2023 r.,

wydaje następujący

Wyrok

1 Wniosek o wydanie orzeczenia w trybie prejudycjalnym dotyczy wykładni art. 5 ust. 2, art. 24, 32 oraz art. 82 ust. 1–3 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) (Dz.U. 2016, L 119, s. 1, zwanego dalej „RODO”).

2 Wniosek ten został złożony w ramach sporu pomiędzy VB, będącą osobą fizyczną, a Natsionalna agentsia za prihodite (krajową agencją przychodów skarbowych, Bułgaria) (zwaną dalej „NAP”) w przedmiocie odszkodowania za szkodę niemajątkową, jaką wspomniana osoba miała ponieść z powodu zarzucanego uchybienia przez ten organ władzy publicznej obowiązkom prawnym ciążącym na nim jako na administratorze danych osobowych.

Ramy prawne

3 Motywy 4, 10, 11, 74, 76, 83, 85 i 146 RODO mają następujące brzmienie:

„(4) […] Niniejsze rozporządzenie nie narusza praw podstawowych, wolności i zasad uznanych w [Karcie praw podstawowych Unii Europejskiej] – zapisanych w Traktatach – w szczególności prawa do poszanowania życia prywatnego i rodzinnego, domu oraz komunikowania się, ochrony danych osobowych […], prawa do skutecznego środka prawnego i dostępu do bezstronnego sądu […].

[…]

(10) Aby zapewnić wysoki i spójny stopień ochrony osób fizycznych oraz usunąć przeszkody w przepływie danych osobowych w Unii [Europejskiej], należy zapewnić równorzędny we wszystkich państwach członkowskich stopień ochrony praw i wolności osób fizycznych w związku z przetwarzaniem takich danych. Należy zapewnić spójne i jednolite w całej Unii stosowanie przepisów o ochronie podstawowych praw i wolności osób fizycznych w związku z przetwarzaniem danych osobowych. […]

(11) Aby ochrona danych osobowych w Unii była skuteczna, należy wzmocnić i doprecyzować prawa osób, których dane dotyczą, oraz obowiązki podmiotów przetwarzających dane osobowe i decydujących o przetwarzaniu […].

[…]

(74) Należy nałożyć na administratora obowiązki i ustanowić odpowiedzialność prawną administratora za przetwarzanie danych osobowych przez niego samego lub w jego imieniu. W szczególności administrator powinien mieć obowiązek wdrożenia odpowiednich i skutecznych środków oraz powinien być w stanie wykazać, że czynności przetwarzania są zgodne z niniejszym rozporządzeniem oraz, że są skuteczne. Środki te powinny uwzględniać charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw i wolności osób fizycznych.

[…]

(76) Prawdopodobieństwo i powagę ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, należy określić poprzez odniesienie się do charakteru, zakresu, kontekstu i celów przetwarzania danych. Ryzyko należy oszacować na podstawie obiektywnej oceny, w ramach której stwierdza się, czy z operacjami przetwarzania danych wiąże się ryzyko lub wysokie ryzyko.

[…]

(83) W celu zachowania bezpieczeństwa i zapobiegania przetwarzaniu niezgodnemu z niniejszym rozporządzeniem administrator lub podmiot przetwarzający powinni oszacować ryzyko właściwe dla przetwarzania oraz wdrożyć środki – takie jak szyfrowanie – minimalizujące to ryzyko. Środki takie powinny zapewnić odpowiedni poziom bezpieczeństwa, w tym poufność, oraz uwzględniać stan wiedzy technicznej oraz koszty ich wdrożenia w stosunku do ryzyka i charakteru danych osobowych podlegających ochronie. Oceniając ryzyko w zakresie bezpieczeństwa danych, należy wziąć pod uwagę ryzyko związane z przetwarzaniem danych osobowych – takie jak przypadkowe lub niezgodne z prawem zniszczenie, utracenie, zmodyfikowanie, nieuprawnione ujawnienie lub nieuprawniony dostęp do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych – i mogące w szczególności prowadzić do uszczerbku fizycznego, szkód majątkowych lub niemajątkowych.

[…]

(85) Przy braku odpowiedniej i szybkiej reakcji naruszenie ochrony danych osobowych może skutkować powstaniem uszczerbku fizycznego, szkód majątkowych lub niemajątkowych u osób fizycznych, takich jak utrata kontroli nad własnymi danymi osobowymi lub ograniczenie praw, dyskryminacja, kradzież lub sfałszowanie tożsamości, strata finansowa,

nieuprawnione odwrócenie pseudonimizacji, naruszenie dobrego imienia, naruszenie poufności danych osobowych chronionych tajemnicą zawodową lub wszelkie inne znaczne szkody gospodarcze lub społeczne. Dlatego natychmiast po stwierdzeniu naruszenia ochrony danych osobowych administrator powinien zgłosić je organowi nadzorczemu bez zbędnej zwłoki […].

[…]

(146) Za szkodę, którą dana osoba poniosła wskutek przetwarzania w sposób naruszający niniejsze rozporządzenie, powinno przysługiwać odszkodowanie od administratora lub podmiotu przetwarzającego. Administrator lub podmiot przetwarzający powinni jednak zostać zwolnieni z odpowiedzialności prawnej, jeżeli udowodnią, że szkoda w żadnym razie nie powstała z ich winy. Pojęcie szkody należy interpretować szeroko, w świetle orzecznictwa Trybunału Sprawiedliwości, w sposób w pełni odzwierciedlający cele niniejszego rozporządzenia. Nie ma to wpływu na roszczenia z tytułu szkód wynikających z naruszenia innych przepisów prawa Unii lub prawa państwa członkowskiego. Przetwarzanie dokonywane w sposób naruszający niniejsze rozporządzenie obejmuje także przetwarzanie, które narusza akty delegowane i wykonawcze przyjęte na mocy niniejszego rozporządzenia oraz prawo państwa członkowskiego doprecyzowujące niniejsze rozporządzenie. Osoby, których dane dotyczą, powinny uzyskać pełne i skuteczne odszkodowanie za poniesione szkody. […]”.

4 Artykuł 4 tego rozporządzenia, zatytułowany „Definicje”, stanowi:

„Na użytek niniejszego rozporządzenia:

1) »dane osobowe« oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej (»osobie, której dane dotyczą«); […]

2) »przetwarzanie« oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany;

[…]

7) »administrator« oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; […]

[…]

10) »strona trzecia« oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które – z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe;

[…]

12) »naruszenie ochrony danych osobowych« oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;

[…]".

5 Artykuł 5 tego rozporządzenia, zatytułowany „Zasady dotyczące przetwarzania danych osobowych", przewiduje:

„1. Dane osobowe muszą być:

a) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą (»zgodność z prawem, rzetelność i przejrzystość«);

[…]

f) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych (»integralność i poufność«).

2. Administrator jest odpowiedzialny za przestrzeganie przepisów ust. 1 i musi być w stanie wykazać ich przestrzeganie (»rozliczalność«)".

6 Zgodnie z art. 24 RODO, zatytułowanym „Obowiązki administratora":

„1. Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane.

2. Jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki, o których mowa w ust. 1, obejmują wdrożenie przez administratora odpowiednich polityk ochrony danych.

3. Stosowanie zatwierdzonych kodeksów postępowania, o których mowa w art. 40, lub zatwierdzonego mechanizmu certyfikacji, o którym mowa w art. 42, może być wykorzystane jako element dla stwierdzenia przestrzegania przez administratora ciążących na nim obowiązków".

7 Artykuł 32 RODO, zatytułowany „Bezpieczeństwo przetwarzania", stanowi:

„1. Uwzględniając 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 zagrożenia, administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku, w tym między innymi w stosownym przypadku:

a) pseudonimizację i szyfrowanie danych osobowych;

b) zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;

c) zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;

d) regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

2. Oceniając, czy stopień bezpieczeństwa jest odpowiedni, uwzględnia się w szczególności ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

3. Wywiązywanie się z obowiązków, o których mowa w ust. 1 niniejszego artykułu, można wykazać między innymi poprzez stosowanie zatwierdzonego kodeksu postępowania, o którym mowa w art. 40 lub zatwierdzonego mechanizmu certyfikacji, o którym mowa w art. 42.

[…]".

8 Artykuł 79 owego rozporządzenia, zatytułowany „Prawo do skutecznego środka ochrony prawnej przed sądem przeciwko administratorowi lub podmiotowi przetwarzającemu", stanowi w ust. 1:

„Bez uszczerbku dla dostępnych administracyjnych lub pozasądowych środków ochrony prawnej, w tym prawa do wniesienia skargi do organu nadzorczego zgodnie z art. 77, każda osoba, której dane dotyczą, ma prawo do skutecznego środka ochrony prawnej przed sądem, jeżeli uzna ona, że prawa przysługujące jej na mocy niniejszego rozporządzenia zostały naruszone w wyniku przetwarzania jego danych osobowych z naruszeniem niniejszego rozporządzenia".

9 Artykuł 82 rzeczonego rozporządzenia, zatytułowany „Prawo do odszkodowania i odpowiedzialność", przewiduje w ust. 1–3:

„1. Każda osoba, która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia niniejszego rozporządzenia, ma prawo uzyskać od administratora lub podmiotu przetwarzającego odszkodowanie za poniesioną szkodę.

2. Każdy administrator uczestniczący w przetwarzaniu odpowiada za szkody spowodowane przetwarzaniem naruszającym niniejsze rozporządzenie. […]

3. Administrator lub podmiot przetwarzający zostają zwolnieni z odpowiedzialności wynikającej z ust. 2, jeżeli udowodnią, że w żaden sposób nie ponoszą winy za zdarzenie, które doprowadziło do powstania szkody".

Postępowanie główne i pytania prejudycjalne

10 NAP jest organem działającym przy bułgarskim ministrze finansów. W ramach swoich zadań, polegających między innymi na identyfikacji, zabezpieczaniu i odzyskiwaniu wierzytelności publicznoprawnych, jest on administratorem danych osobowych w rozumieniu art. 4 pkt 7 RODO.

11 W dniu 15 lipca 2019 r. media ujawniły, że miał miejsce nieuprawniony dostęp do systemu informatycznego NAP oraz że w następstwie tego cyberataku w Internecie opublikowano dane osobowe zawarte w tym systemie.

12 Zdarzenia te miały wpływ na ponad 6 mln osób fizycznych, będących obywatelami bułgarskimi lub zagranicznymi. Kilkaset z nich, w tym skarżąca w postępowaniu głównym, wytoczyło przeciwko NAP powództwa o odszkodowanie za szkodę niemajątkową wynikającą z ujawnienia ich danych osobowych.

13 W tym kontekście skarżąca w postępowaniu głównym wniosła do Administrativen sad Sofia-grad (sądu administracyjnego w Sofii, Bułgaria) powództwo o zasądzenie od NAP kwoty 1000 BGN (lewów (około 510 EUR) tytułem odszkodowania na podstawie art. 82 RODO i przepisów prawa bułgarskiego. Na poparcie tego żądania podniosła ona, że poniosła szkodę niemajątkową wynikającą z naruszenia danych osobowych w rozumieniu art. 4 pkt 12 RODO, a w szczególności z naruszenia bezpieczeństwa, które zostało spowodowane uchybieniem przez NAP obowiązkom ciążącym na nim w szczególności na mocy art. 5 ust. 1 lit. f) oraz art. 24 i 32 tego rozporządzenia. Poniesiona przez nią szkoda niemajątkowa polega jej zdaniem na obawie, iż jej dane osobowe, które zostały opublikowane bez jej zgody, mogłyby zostać w przyszłości wykorzystane w sposób stanowiący nadużycie lub że ona sama mogłaby zostać poddana szantażowi, agresji, a nawet zostać uprowadzona.

14 Na swoją obronę NAP podniósł przede wszystkim, że skarżąca w postępowaniu głównym nie zażądała od niego informacji o tym, jakie konkretnie dane zostały ujawnione. Następnie NAP przedstawił dokumenty mające na celu wykazanie, że przedsięwziął wszystkie niezbędne środki w celu zapobieżenia naruszeniu danych osobowych zawartych w jego systemie informatycznym, a także w celu ograniczenia skutków tego naruszenia i uspokojenia obywateli. Ponadto zdaniem NAP nie istniał związek przyczynowy między podnoszoną szkodą niemajątkową a wspomnianym naruszeniem. Wreszcie, podniósł on, że ze względu na to, iż sam był ofiarą nieprzychylnych działań ze strony osób, które nie były jego pracownikami, nie może on zostać pociągnięty do odpowiedzialności za szkodliwe skutki tych działań.

15 Orzeczeniem z dnia 27 listopada 2020 r. Administrativen sad Sofia-grad (sąd administracyjny w Sofii) oddalił powództwo skarżącej w postępowaniu głównym. Sąd ten uznał, po pierwsze, że nieuprawniony dostęp do bazy danych NAP wynikał z ataku hakerskiego ze strony osób trzecich, a po drugie, że skarżąca w postępowaniu głównym nie udowodniła bezczynności NAP w zakresie przyjęcia środków bezpieczeństwa. Ponadto uznał on, że skarżąca nie poniosła szkody niemajątkowej uprawniającej do odszkodowania.

16 Skarżąca w postępowaniu głównym wniosła skargę kasacyjną od tego orzeczenia do Varhoven administrativen sad (najwyższego sądu administracyjnego, Bułgaria), który jest sądem odsyłającym w niniejszej sprawie. Na poparcie swojej skargi kasacyjnej podnosi ona, że sąd pierwszej instancji naruszył prawo przy rozłożeniu ciężaru dowodu dotyczącego środków bezpieczeństwa podjętych przez NAP oraz że organ ten nie wykazał braku bezczynności w tym względzie. Ponadto skarżąca w postępowaniu głównym twierdzi, że obawa przed ewentualnym wykorzystaniem jej danych osobowych w przyszłości w sposób stanowiący nadużycie stanowi rzeczywistą, a nie hipotetyczną szkodę niemajątkową. W odpowiedzi NAP kwestionuje każdy z tych argumentów.

17 Sąd odsyłający rozważa przede wszystkim, czy samo stwierdzenie naruszenia ochrony danych osobowych pozwalałoby samo w sobie na wyciągnięcie wniosku, że środki wdrożone przez administratora tych danych nie były „odpowiednie” w rozumieniu art. 24 i 32 RODO.

18 Jednakże w przypadku gdyby stwierdzenie to było niewystarczające, aby dojść do takiego wniosku, sąd ten zastanawia się, po pierwsze, nad granicami kontroli, jaką powinny przeprowadzić sądy krajowe w celu dokonania oceny, czy rozpatrywane środki mają odpowiedni charakter, a po drugie, nad przepisami dotyczącymi przeprowadzania dowodów, które powinny mieć zastosowanie w tym kontekście, zarówno jeśli chodzi o ciężar dowodu, jak i środki dowodowe, w szczególności gdy do sądów tych wniesiono powództwo o odszkodowanie na podstawie art. 82 tego rozporządzenia.

19 Następnie sąd ten dąży do ustalenia, czy w świetle art. 82 ust. 3 wspomnianego rozporządzenia okoliczność, że naruszenie ochrony danych osobowych wynika z czynu popełnionego przez osoby trzecie, w niniejszym przypadku z cyberataku, stanowi czynnik zwalniający systematycznie administratora tych danych z odpowiedzialności za szkodę wyrządzoną osobie, której dane dotyczą.

20 Wreszcie, wspomniany sąd zastanawia się, czy obawa osoby, że jej dane osobowe mogłyby zostać w przyszłości wykorzystane w sposób stanowiący nadużycie, w niniejszym przypadku w następstwie nieuprawnionego dostępu do tych danych i ich ujawnienia przez cyberprzestępców, może sama w sobie stanowić „szkodę niemajątkową” w rozumieniu art. 82 ust. 1 RODO. W przypadku odpowiedzi twierdzącej osoba ta byłaby zwolniona z obowiązku wykazania, że osoby trzecie – przed jej wystąpieniem z żądaniem odszkodowania – w sposób niezgodny z prawem wykorzystały te dane, takie jak przywłaszczenie jej tożsamości.

21 W tych okolicznościach Varhoven administrativen sad (najwyższy sąd administracyjny) postanowił zawiesić postępowanie i zwrócić się do Trybunału z następującymi pytaniami prejudycjalnymi:

„1) Czy art. 24 i 32 rozporządzenia [RODO] należy interpretować w ten sposób, że wystarczające jest zrealizowanie nieuprawnionego ujawnienia lub dostępu do danych osobowych w rozumieniu art. 4 pkt 12 rozporządzenia [RODO] 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 [RODO], 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 [RODO] należy interpretować w ten sposób, że w postępowaniu z powództwa określonego w art. 82 ust. 1 [rzeczonego rozporządzenia] na administratorze danych osobowych ciąży ciężar dowodu odnośnie do okoliczności, że zastosowane środki techniczne i organizacyjne, o których mowa w art. 32 [tego] 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 [RODO] należy interpretować w ten sposób, że nieuprawnione ujawnienie lub dostęp do danych osobowych w rozumieniu art. 4 pkt 12 rozporządzenia [RODO] – 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 [tego rozporządzenia] 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 wykorzystaniem danych osobowych w sposób stanowiący nadużycie – bez zaistnienia takiego nadużycia lub wyrządzenia innej szkody podmiotowi danych – są objęte szerokim rozumieniem pojęcia szkód niematerialnych i stanowi [to] podstawę do zasądzenia odszkodowania?”.

W przedmiocie pytań prejudycjalnych

W przedmiocie pytania pierwszego

22 Poprzez pytanie pierwsze sąd odsyłający dąży w istocie do ustalenia, czy art. 24 i 32 RODO należy interpretować w ten sposób, że nieuprawnione ujawnienie danych osobowych lub nieuprawniony dostęp do takich danych przez „[osoby] trzecie” w rozumieniu art. 4 pkt 10 tego rozporządzenia wystarczają same w sobie do uznania, iż wdrożone przez danego administratora środki techniczne i organizacyjne nie były „odpowiednie” w rozumieniu tych art. 24 i 32.

23 Na wstępie należy przypomnieć, że zgodnie z utrwalonym orzecznictwem treści przepisu prawa Unii, który – tak jak art. 24 i 32 RODO – nie zawiera żadnego wyraźnego odesłania do prawa państw członkowskich w celu określenia jego znaczenia i zakresu, należy zazwyczaj nadawać w całej Unii autonomiczną i jednolitą wykładnię, której należy dokonywać z uwzględnieniem w szczególności treści tego przepisu, realizowanych przez niego celów oraz kontekstu, w jaki się on wpisuje [zob. podobnie wyroki: z dnia 18 stycznia 1984 r., Ekro, 327/82, EU:C:1984:11, pkt 11; z dnia 1 października 2019 r., Planet49, C-673/17, EU:C:2019:801, pkt 47, 48; a także z dnia 4 maja 2023 r., Österreichische Post (Szkoda niemajątkowa związana z przetwarzaniem danych osobowych), C-300/21, EU:C:2023:370, pkt 29].

24 W pierwszej kolejności, co się tyczy brzmienia stosownych przepisów, należy zauważyć, że art. 24 RODO przewiduje, że na administratorze danych osobowych ciąży ogólny obowiązek wdrożenia odpowiednich środków technicznych i organizacyjnych, aby zapewnić, by przetwarzanie to odbywało się zgodnie z tym rozporządzeniem, i być w stanie to wykazać.

25 W tym celu ów art. 24 wymienia w ust. 1 pewną liczbę kryteriów, które należy uwzględnić przy ocenie, czy takie środki mają odpowiedni charakter, a mianowicie charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i powadze zagrożenia. W przepisie tym uściślono, że środki te są w razie potrzeby poddawane przeglądom i uaktualniane.

26 W tym kontekście art. 32 RODO określa obowiązki administratora i ewentualnego podmiotu przetwarzającego w zakresie bezpieczeństwa tego przetwarzania. I tak ust. 1 tego artykułu stanowi, że powinni oni wdrożyć odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku, o którym mowa w poprzednim punkcie niniejszego wyroku, uwzględniając stan wiedzy technicznej, koszty wdrażania oraz charakter, zakres, kontekst i cele danego przetwarzania.

27 Podobnie ust. 2 tego artykułu stanowi, że oceniając, czy stopień bezpieczeństwa jest odpowiedni, uwzględnia się w szczególności ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.

28 Ponadto zarówno art. 24 ust. 3 tego rozporządzenia, jak i jego art. 32 ust. 3 wskazują, że administrator lub podmiot przetwarzający mogą wykazać, iż wywiązali się z obowiązków określonych odpowiednio w ust. 1 tych artykułów, opierając się na okoliczności, iż stosowali oni zatwierdzony kodeks postępowania lub zatwierdzony mechanizm certyfikacji, o których mowa w art. 40 i 42 wspomnianego rozporządzenia.

29 Zawarte w art. 32 ust. 1 i 2 RODO odniesienia do „stop[nia] bezpieczeństwa odpowiadając[ego] […] ryzyku” oraz „odpowiedni[ego]” „stop[nia] bezpieczeństwa” świadczą o tym, że rozporządzenie to ustanawia system zarządzania ryzykiem i w żaden sposób nie ma na celu wyeliminowania ryzyka naruszeń danych osobowych.

30 Z brzmienia art. 24 i 32 RODO wynika zatem, że przepisy te ograniczają się do nałożenia na administratora obowiązku przyjęcia środków technicznych i organizacyjnych mających na celu uniknięcie, na ile to możliwe, wszelkiego naruszenia ochrony danych osobowych. Okoliczność, czy takie środki mają odpowiedni charakter, należy oceniać w sposób konkretny, badając, czy środki te zostały wdrożone przez tego administratora z uwzględnieniem różnych kryteriów wskazanych w tych artykułach oraz potrzeb ochrony danych konkretnie związanych z danym przetwarzaniem, a także ryzyka wynikającego z tego przetwarzania.

31 W związku z tym art. 24 i 32 RODO nie można rozumieć w ten sposób, że nieuprawnione ujawnienie danych osobowych lub nieuprawniony dostęp do takich danych przez osobę trzecią wystarczają do stwierdzenia, że środki przyjęte przez danego administratora nie były odpowiednie w rozumieniu tych przepisów, nie umożliwiając nawet temu administratorowi przedstawienia dowodu przeciwnego.

32 Taka wykładnia nasuwa się tym bardziej, że art. 24 RODO wyraźnie przewiduje, iż administrator musi być w stanie wykazać zgodność wdrożonych przez niego środków z tym rozporządzeniem, której to możliwości zostałby pozbawiony w przypadku przyjęcia niewzruszalnego domniemania.

33 W drugiej kolejności argumenty wynikające z wykładni kontekstualnej i celowościowej potwierdzają taką interpretację art. 24 i 32 RODO.

34 Co się tyczy, po pierwsze, kontekstu, w jaki wpisują się te dwa artykuły, należy zauważyć, że z art. 5 ust. 2 RODO wynika, iż administrator musi być w stanie wykazać, że przestrzegał zasad dotyczących przetwarzania danych osobowych określonych w ust. 1 tego artykułu. Obowiązek ten został powtórzony i doprecyzowany w art. 24 ust. 1 i 3 oraz w art. 32 ust. 3 tego rozporządzenia w odniesieniu do obowiązku wdrożenia środków technicznych i organizacyjnych w celu ochrony takich danych przy przetwarzaniu przez tego administratora. Tymczasem taki obowiązek wykazania, że środki te mają odpowiedni charakter, byłby pozbawiony sensu, gdyby administrator był zobowiązany do zapobieżenia wszelkiego naruszenia ochrony tych danych.

35 Ponadto w motywie 74 RODO podkreślono, że ważne jest, aby administrator był zobowiązany do wdrożenia odpowiednich i skutecznych środków oraz był w stanie wykazać zgodność czynności przetwarzania z tym rozporządzeniem, w tym skuteczność środków, które powinny uwzględniać kryteria związane z cechami danego przetwarzania i wynikającym z niego ryzykiem, które są również określone w art. 24 i 32 tego rozporządzenia.

36 Podobnie zgodnie z motywem 76 tego rozporządzenia prawdopodobieństwo i powaga ryzyka zależą od specyfiki danego przetwarzania, a ryzyko to powinno podlegać obiektywnej ocenie.

37 Co więcej, z art. 82 ust. 2 i 3 RODO wynika, że o ile administrator jest odpowiedzialny za szkodę spowodowaną przetwarzaniem, które stanowi naruszenie tego rozporządzenia, o tyle jest on jednak zwolniony z odpowiedzialności, jeżeli udowodni, iż w żaden sposób nie ponosi winy za zdarzenie, które doprowadziło do powstania szkody.

38 Po drugie, wykładnię przedstawioną w pkt 31 niniejszego wyroku potwierdza również motyw 83 RODO, w którym wskazano w zdaniu pierwszym, że „[w] celu zachowania bezpieczeństwa i zapobiegania przetwarzaniu niezgodnemu z niniejszym rozporządzeniem administrator lub podmiot przetwarzający powinni oszacować ryzyko właściwe dla przetwarzania oraz wdrożyć środki […] minimalizujące to ryzyko”. Czyniąc to, prawodawca Unii wyraził swój zamiar „ograniczenia” ryzyka naruszenia ochrony danych osobowych, nie twierdząc, że można je wyeliminować.

39 W świetle powyższych rozważań na pytanie pierwsze należy odpowiedzieć, iż art. 24 i 32 RODO należy interpretować w ten sposób, że nieuprawnione ujawnienie danych osobowych lub nieuprawniony dostęp do takich danych przez „osoby trzecie” w rozumieniu art. 4 pkt 10 tego rozporządzenia nie wystarczają same w sobie do uznania, iż wdrożone przez danego administratora środki techniczne i organizacyjne nie były „odpowiednie” w rozumieniu tych art. 24 i 32.

W przedmiocie pytania drugiego

40 Poprzez pytanie drugie sąd odsyłający dąży w istocie do ustalenia, czy art. 32 RODO należy interpretować w ten sposób, że oceny, czy środki techniczne i organizacyjne wdrożone przez administratora na podstawie tego artykułu mają odpowiedni charakter, sądy krajowe powinny dokonywać w sposób konkretny, w szczególności uwzględniając ryzyko związane z danym przetwarzaniem.

41 W tym względzie należy przypomnieć, że – jak podkreślono w ramach odpowiedzi na pytanie pierwsze – art. 32 RODO wymaga, aby administrator i podmiot przetwarzający, w zależności od przypadku, wdrożyli odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku, z uwzględnieniem kryteriów oceny określonych

w ust. 1 tego artykułu. Ponadto w ust. 2 tego artykułu wymieniono w sposób niewyczerpujący szereg czynników, które są istotne dla oceny odpowiedniego stopnia bezpieczeństwa w świetle ryzyka wynikającego z danego przetwarzania.

42 Ze wspomnianego art. 32 ust. 1 i 2 wynika, że okoliczność, czy takie środki techniczne i organizacyjne mają odpowiedni charakter, należy oceniać w dwóch etapach. Po pierwsze, należy zidentyfikować ryzyko naruszenia ochrony danych osobowych wynikające z danego przetwarzania oraz jego ewentualne konsekwencje dla praw i wolności osób fizycznych. Oceny tej należy dokonywać w sposób konkretny, z uwzględnieniem prawdopodobieństwa zidentyfikowanego ryzyka i stopnia jego powagi. Po drugie, należy sprawdzić, czy środki wdrożone przez administratora odpowiadają temu ryzyku, biorąc pod uwagę stan wiedzy, koszty wdrożenia, a także charakter, zakres, kontekst i cele tego przetwarzania.

43 Prawdą jest, że administrator ma pewien zakres uznania przy określaniu odpowiednich środków technicznych i organizacyjnych, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku, jak wymaga tego art. 32 ust. 1 RODO. Niemniej jednak sąd krajowy powinien mieć możliwość skontrolowania złożonej oceny dokonanej przez administratora i w ten sposób upewnienia się, że przyjęte przez niego środki są w stanie zagwarantować taki stopień bezpieczeństwa.

44 Taka wykładnia może ponadto zapewnić, z jednej strony, skuteczność ochrony danych osobowych, na którą zwrócono uwagę w motywach 11 i 74 tego rozporządzenia, a z drugiej strony, prawo do skutecznego środka ochrony prawnej przed sądem względem administratora, chronione przez art. 79 ust. 1 wspomnianego rozporządzenia w związku z motywem 4 tego rozporządzenia.

45 W związku z tym, aby zweryfikować, czy środki techniczne i organizacyjne wdrożone na podstawie art. 32 RODO mają odpowiedni charakter, sąd krajowy nie powinien ograniczać się do ustalenia, w jaki sposób dany administrator danych zamierzał wypełnić obowiązki ciążące na nim na mocy tego artykułu, lecz powinien zbadać te środki co do istoty w świetle wszystkich kryteriów wymienionych w tym artykule, a także okoliczności danej sprawy i dowodów, którymi sąd ten dysponuje w tym względzie.

46 Takie badanie wymaga przeprowadzenia konkretnej analizy zarówno charakteru, jak i treści środków wdrożonych przez administratora, sposobu, w jaki środki te zostały zastosowane, oraz ich praktycznego wpływu na poziom bezpieczeństwa, jaki administrator ten był zobowiązany zapewnić, biorąc pod uwagę ryzyko związane z tym przetwarzaniem.

47 W konsekwencji na pytanie drugie trzeba odpowiedzieć, że art. 32 RODO należy interpretować w ten sposób, iż oceny, czy środki techniczne i organizacyjne wdrożone przez administratora na podstawie tego artykułu mają odpowiedni charakter, sądy krajowe powinny dokonywać w sposób konkretny, w szczególności uwzględniając ryzyko związane z danym przetwarzaniem oraz ustalając, czy charakter, istota i wdrożenie tych środków są dostosowane do tego ryzyka.

W przedmiocie pytania trzeciego

W przedmiocie części pierwszej pytania trzeciego

48 Poprzez część pierwszą pytania trzeciego sąd odsyłający dąży w istocie do ustalenia, czy zasadę rozliczalności administratora wyrażoną w art. 5 ust. 2 RODO i skonkretyzowaną w art. 24 tego rozporządzenia należy interpretować w ten sposób, że w ramach powództwa o odszkodowanie opartego na art. 82 tego rozporządzenia na danym administratorze spoczywa ciężar udowodnienia, że środki bezpieczeństwa, które wdrożył na podstawie art. 32 tego rozporządzenia, mają odpowiedni charakter.

49 W tym względzie należy w pierwszej kolejności przypomnieć, że art. 5 ust. 2 RODO ustanawia zasadę rozliczalności, zgodnie z którą administrator jest odpowiedzialny za przestrzeganie zasad dotyczących przetwarzania danych osobowych określonych w ust. 1 tego artykułu, oraz przewiduje, że wspomniany administrator musi być w stanie wykazać, że zasady te są przestrzegane.

50 W szczególności administrator powinien, zgodnie z zasadą integralności i poufności danych osobowych, o której mowa w art. 5 ust. 1 lit. f) tego rozporządzenia, zapewnić, aby takie dane były przetwarzane w sposób zapewniający ich odpowiednie bezpieczeństwo, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych, oraz musi być w stanie wykazać, że zasada ta jest przestrzegana.

51 Należy również zauważyć, że zarówno art. 24 ust. 1 RODO w świetle motywu 74 tego rozporządzenia, jak i art. 32 ust. 1 tego rozporządzenia nakładają na administratora, w odniesieniu do wszelkiego przetwarzania danych osobowych dokonywanego przez niego samego lub w jego imieniu, obowiązek wdrożenia odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie odbywało się w zgodzie z tym rozporządzeniem i aby móc to wykazać.

52 Z brzmienia art. 5 ust. 2, art. 24 ust. 1 i art. 32 ust. 1 RODO jednoznacznie wynika, że ciężar udowodnienia, iż dane osobowe są przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo tych danych w rozumieniu art. 5 ust. 1 lit. f) i art. 32 tego rozporządzenia, spoczywa na danym administratorze [zob. analogicznie wyroki: z dnia 4 maja 2023 r., Bundesrepublik Deutschland (Skrzynka doręczeń elektronicznych w sprawach sądowych), C-60/22, EU:C:2023:373, pkt 52, 53; a także z dnia 4 lipca 2023 r., Meta Platforms i in. (Ogólne warunki korzystania z sieci społecznościowej), C-252/21, EU:C:2023:537, pkt 95].

53 Te trzy artykuły ustanawiają zatem ogólną zasadę, którą w przypadku braku odmiennych wskazówek w RODO należy stosować również w ramach powództwa o odszkodowanie opartego na art. 82 tego rozporządzenia.

54 W drugiej kolejności należy stwierdzić, że powyższą wykładnię literalną potwierdza uwzględnienie celów realizowanych przez RODO.

55 Po pierwsze, ponieważ poziom ochrony, o którym mowa w RODO, jest zależny od środków bezpieczeństwa przyjętych przez administratorów danych osobowych, należy zachęcać ich do podjęcia wszelkich starań, aby zapobiec wystąpieniu operacji przetwarzania niezgodnych z tym rozporządzeniem, z uwagi na okoliczność, że ponoszą oni ciężar wykazania, iż środki te mają odpowiedni charakter.

56 Po drugie, gdyby należało uznać, że ciężar dowodu dotyczący odpowiedniego charakteru wspomnianych środków spoczywa na osobach, których dane dotyczą, zdefiniowanych w art. 4 pkt 1 RODO, wynikałoby z tego, że przewidziane w art. 82 ust. 1 RODO prawo do odszkodowania zostałoby w znacznym stopniu pozbawione skuteczności (effet utile), podczas gdy prawodawca Unii zamierzał wzmocnić zarówno prawa tych osób, jak i obowiązki administratorów w stosunku do przepisów poprzedzających to rozporządzenie, jak wskazuje motyw 11 tego rozporządzenia.

57 Na część pierwszą pytania trzeciego trzeba zatem odpowiedzieć, że zasadę rozliczalności administratora wyrażoną w art. 5 ust. 2 RODO i skonkretyzowaną w art. 24 tego rozporządzenia należy interpretować w ten sposób, iż w ramach powództwa o odszkodowanie opartego na art. 82 tego rozporządzenia na danym administratorze spoczywa ciężar udowodnienia, że środki bezpieczeństwa, które wdrożył na podstawie art. 32 tego rozporządzenia, mają odpowiedni charakter.

W przedmiocie części drugiej pytania trzeciego

58 Poprzez część drugą pytania trzeciego sąd odsyłający dąży w istocie do ustalenia, czy art. 32 RODO i zasadę skuteczności prawa Unii należy interpretować w ten sposób, że na potrzeby oceny, czy środki bezpieczeństwa wdrożone przez administratora na podstawie tego artykułu mają odpowiedni charakter, opinia biegłego sądowego stanowi niezbędny i wystarczający środek dowodowy.

59 W tym względzie należy przypomnieć, że zgodnie z utrwalonym orzecznictwem wobec braku norm Unii w danej dziedzinie do wewnętrznego porządku prawnego każdego państwa członkowskiego należy, na mocy zasady autonomii proceduralnej, uregulowanie szczegółowych aspektów proceduralnych dotyczących środków prawnych mających na celu ochronę uprawnień przysługujących podmiotom prawa, pod warunkiem jednak, że zasady te w sytuacjach objętych prawem Unii nie będą mniej korzystne niż te odnoszące się do podobnych sytuacji podlegających prawu krajowemu (zasada równoważności) oraz że w praktyce nie będą uniemożliwiały lub nie uczynią nadmiernie uciążliwym wykonywania uprawnień przyznanych w prawie Unii (zasada skuteczności) [wyrok z dnia 4 maja 2023 r., Österreichische Post (Szkoda niemajątkowa związana z przetwarzaniem danych osobowych), C-300/21, EU:C:2023:370, pkt 53 i przytoczone tam orzecznictwo].

60 W niniejszej sprawie należy zauważyć, że RODO nie zawiera przepisów dotyczących dopuszczania i mocy dowodowej środka dowodowego takiego jak opinia biegłego sądowego, które powinny być stosowane przez sądy krajowe rozpatrujące powództwo o odszkodowanie oparte na art. 82 tego rozporządzenia, mające za zadanie dokonanie oceny, w świetle art. 32 owego rozporządzenia, czy środki bezpieczeństwa wdrożone przez danego administratora mają odpowiedni charakter. W związku z tym zgodnie z tym, co zostało przypomniane w poprzednim punkcie niniejszego wyroku, i w braku norm prawa Unii w tej dziedzinie, do porządku prawnego każdego państwa członkowskiego należy określenie zasad dotyczących działań mających na celu zapewnienie podmiotom prawa ochrony uprawnień wynikających ze wspomnianego art. 82, a w szczególności

zasad dotyczących środków dowodowych umożliwiających ocenę, czy takie środki mają odpowiedni charakter w tym kontekście, z zastrzeżeniem poszanowania wspomnianych zasad równoważności i skuteczności [zob. analogicznie wyroki: z dnia 21 czerwca 2022 r., Ligue des droits humains, C-817/19, EU:C:2022:491, pkt 297; a także z dnia 4 maja 2023 r., Österreichische Post (Szkoda niemajątkowa związana z przetwarzaniem danych osobowych), C-300/21, EU:C:2023:370, pkt 54].

61 W niniejszym postępowaniu Trybunał nie dysponuje żadną informacją mogącą wzbudzać wątpliwości co do przestrzegania zasady równoważności. Inaczej jest w odniesieniu do zgodności z zasadą skuteczności, ponieważ samo brzmienie części drugiej pytania trzeciego wskazuje na skorzystanie z opinii biegłego sądowego jako „niezbędnego i wystarczającego środka dowodowego".

62 W szczególności krajowy przepis proceduralny, zgodnie z którym systematycznie „niezbędne" byłoby zlecanie przez sądy krajowe sporządzania opinii biegłego sądowego, mógłby naruszać zasadę skuteczności. Systematyczne korzystanie z takiej opinii mogłoby bowiem okazać się zbędne w świetle innych dowodów znajdujących się w posiadaniu sądu rozpoznającego sprawę, w szczególności, jak wskazał rząd bułgarski w uwagach na piśmie, w świetle wyników kontroli przestrzegania środków ochrony danych osobowych przeprowadzonej przez niezależny organ ustanowiony ustawą, pod warunkiem że kontrola ta została przeprowadzona w niedalekiej przeszłości, ponieważ zgodnie z art. 24 ust. 1 RODO wspomniane środki powinny być w razie potrzeby poddawane przeglądom i uaktualniane.

63 Ponadto, jak wskazała Komisja Europejska w uwagach na piśmie, zasada skuteczności mogłaby zostać naruszona, gdyby określenie „wystarczający" należało rozumieć jako oznaczające, że sąd krajowy powinien wywieść wyłącznie lub automatycznie ze sprawozdania z opinii biegłego sądowego, iż środki bezpieczeństwa wdrożone przez danego administratora są „odpowiednie" w rozumieniu art. 32 RODO. Otóż ochrona praw przyznanych przez to rozporządzenie, do której zmierza wspomniana zasada skuteczności, a w szczególności zagwarantowane w art. 79 ust. 1 tego rozporządzenia prawo do skutecznego środka ochrony prawnej przed sądem względem administratora, wymaga, by bezstronny sąd dokonał obiektywnej oceny, czy dane środki mają odpowiedni charakter, zamiast ograniczać się do takiego wnioskowania (zob. podobnie wyrok z dnia 12 stycznia 2023 r., Nemzeti Adatvédelmi és Információszabadság Hatóság, C-132/21, EU:C:2023:2, pkt 50).

64 W świetle powyższych rozważań na część drugą pytania trzeciego trzeba odpowiedzieć, że art. 32 RODO i zasadę skuteczności prawa Unii należy interpretować w ten sposób, iż na potrzeby oceny, czy środki bezpieczeństwa wdrożone przez administratora na podstawie tego artykułu mają odpowiedni charakter, opinia biegłego sądowego nie może systematycznie stanowić niezbędnego i wystarczającego środka dowodowego.

W przedmiocie pytania czwartego

65 Poprzez pytanie czwarte sąd odsyłający dąży w istocie do ustalenia, czy art. 82 ust. 3 RODO należy interpretować w ten sposób, że administrator jest na podstawie art. 82 ust. 1 i 2 tego rozporządzenia zwolniony z obowiązku naprawienia poniesionej przez daną osobę szkody z tego tylko powodu, iż szkoda ta wynika z nieuprawnionego ujawnienia danych osobowych lub nieuprawnionego dostępu do takich danych przez „osoby trzecie" w rozumieniu art. 4 pkt 10 tego rozporządzenia.

66 Na wstępie należy wyjaśnić, że z art. 4 pkt 10 RODO wynika, iż „osobami trzecimi" są w szczególności osoby inne niż te, które – z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe. Definicja ta obejmuje osoby, które nie są pracownikami administratora i nie przetwarzają danych pod jego kontrolą, takie jak te, o których mowa w pytaniu prejudycjalnym.

67 Następnie należy przypomnieć w pierwszej kolejności, że art. 82 ust. 2 RODO stanowi, iż „[k]ażdy administrator uczestniczący w przetwarzaniu odpowiada za szkody spowodowane przetwarzaniem naruszającym [to] rozporządzenie", a jego art. 82 ust. 3 przewiduje, iż administrator lub podmiot przetwarzający, stosownie do okoliczności, zostają zwolnieni z takiej odpowiedzialności, „jeżeli udowodnią, że w żaden sposób nie ponoszą winy za zdarzenie, które doprowadziło do powstania szkody".

68 Ponadto motyw 146 RODO, który odnosi się konkretnie do art. 82 tego rozporządzenia, wskazuje w zdaniach pierwszym i drugim, że „[z]a szkodę, którą dana osoba poniosła wskutek przetwarzania w sposób naruszający [to] rozporządzenie, powinno przysługiwać odszkodowanie od administratora lub podmiotu przetwarzającego" oraz że „powinni [oni] zostać zwolnieni z odpowiedzialności prawnej, jeżeli udowodnią, że szkoda w żadnym razie nie powstała z ich winy".

69 Z przepisów tych wynika, po pierwsze, że dany administrator powinien co do zasady naprawić szkodę spowodowaną naruszeniem tego rozporządzenia w związku z tym przetwarzaniem, a po drugie, iż może on zostać zwolniony z odpowiedzialności tylko wtedy, gdy udowodni, że w żaden sposób nie ponosi winy za zdarzenie, które doprowadziło do powstania szkody.

70 Tak więc, jak wynika z wyraźnego dodania określenia „w żadnym razie" w toku procedury ustawodawczej, okoliczności, w których administrator może ubiegać się o zwolnienie z odpowiedzialności cywilnej, jaką ponosi na podstawie art. 82 RODO, powinny być ściśle ograniczone do okoliczności, w których administrator ten jest w stanie wykazać, że nie ponosi winy za szkodę.

71 Jeżeli, tak jak w niniejszym przypadku, naruszenia ochrony danych osobowych w rozumieniu art. 4 pkt 12 RODO dopuścili się cyberprzestępcy, a zatem „osoby trzecie" w rozumieniu art. 4 pkt 10 tego rozporządzenia, za naruszenie to administrator nie ponosi winy, chyba że umożliwił on wspomniane naruszenie poprzez niedopełnienie obowiązku przewidzianego w RODO, a w szczególności obowiązku ochrony danych ciążącego na nim na mocy art. 5 ust. 1 lit. f) oraz art. 24 i 32 tego rozporządzenia.

72 I tak w przypadku naruszenia ochrony danych osobowych przez osobę trzecią administrator może zwolnić się z odpowiedzialności na podstawie art. 82 ust. 3 RODO poprzez udowodnienie, że nie istnieje żaden związek przyczynowy między ewentualnym naruszeniem przez niego obowiązku ochrony danych a szkodą poniesioną przez osobę fizyczną.

73 W drugiej kolejności powyższa wykładnia owego art. 82 ust. 3 jest również zgodna z określonym w motywach 10 i 11 RODO celem tego rozporządzenia polegającym na zapewnieniu wysokiego poziomu ochrony osób fizycznych w związku z przetwarzaniem ich danych osobowych.

74 W świetle całości powyższych rozważań na pytanie czwarte trzeba odpowiedzieć, że art. 82 ust. 3 RODO należy interpretować w ten sposób, iż administrator nie jest na podstawie art. 82 ust. 1 i 2 tego rozporządzenia zwolniony z obowiązku naprawienia poniesionej przez daną osobę szkody

z tego tylko powodu, iż szkoda ta wynika z nieuprawnionego ujawnienia danych osobowych lub nieuprawnionego dostępu do takich danych przez „osoby trzecie” w rozumieniu art. 4 pkt 10 tego rozporządzenia, gdyż ów administrator musi przy tym udowodnić, że w żaden sposób nie ponosi winy za zdarzenie, które doprowadziło do powstania szkody.

W przedmiocie pytania piątego

75 Poprzez pytanie piąte sąd odsyłający dąży w istocie do ustalenia, czy art. 82 ust. 1 RODO należy interpretować w ten sposób, że obawa przed ewentualnym wykorzystaniem przez osoby trzecie w sposób stanowiący nadużycie danych osobowych, jaką żywi osoba, której dane dotyczą, w następstwie naruszenia tego rozporządzenia może sama w sobie stanowić „szkodę niemajątkową” w rozumieniu tego przepisu.

76 W pierwszej kolejności, co się tyczy brzmienia art. 82 ust. 1 RODO, należy zauważyć, że stanowi on, iż „[k]ażda osoba, która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia niniejszego rozporządzenia, ma prawo uzyskać od administratora lub podmiotu przetwarzającego odszkodowanie za poniesioną szkodę”.

77 W tym względzie Trybunał zauważył, że z brzmienia art. 82 ust. 1 RODO jasno wynika, iż istnienie „szkody”, która została „poniesiona”, stanowi jedną z przesłanek przewidzianego w tym przepisie prawa do odszkodowania, podobnie jak istnienie naruszenia tego rozporządzenia i związku przyczynowego między tą szkodą a tym naruszeniem, przy czym te trzy przesłanki są kumulatywne [wyrok z dnia 4 maja 2023 r., Österreichische Post (Szkoda niemajątkowa związana z przetwarzaniem danych osobowych), C-300/21, EU:C:2023:370, pkt 32].

78 Ponadto, opierając się na względach związanych z wykładnią zarówno literalną, systemową, jak i celowościową, Trybunał zinterpretował art. 82 ust. 1 RODO w ten sposób, iż sprzeciwia się on przepisowi krajowemu lub praktyce krajowej, które uzależniają uzyskanie odszkodowania za „szkodę niemajątkową” w rozumieniu tego przepisu od warunku, by szkoda poniesiona przez osobę, której dane dotyczą, osiągnęła pewien stopień powagi [wyrok z dnia 4 maja 2023 r., Österreichische Post (Szkoda niemajątkowa związana z przetwarzaniem danych osobowych), C-300/21, EU:C:2023:370, pkt 51].

79 Przypomniawszy powyższe, należy podkreślić w niniejszym przypadku, że w art. 82 ust. 1 RODO nie dokonano rozróżnienia między sytuacjami, w których w następstwie potwierdzonego naruszenia przepisów tego rozporządzenia „szkoda niemajątkowa” podnoszona przez osobę, której dane dotyczą, z jednej strony jest związana z wykorzystaniem przez osoby trzecie jej danych osobowych w sposób stanowiący nadużycie, do którego doszło przed wystąpieniem przez nią z żądaniem odszkodowania, a z drugiej strony jest związana z obawą, jaką żywi ta osoba, że takie wykorzystanie mogłoby nastąpić w przyszłości.

80 W związku z tym brzmienie art. 82 ust. 1 RODO nie wyklucza, że pojęcie „szkody niemajątkowej” zawarte w tym przepisie obejmuje sytuację taką jak przedstawiona przez sąd odsyłający, w której osoba, której dane dotyczą, powołuje się, w celu uzyskania odszkodowania na podstawie tego przepisu, na swoją obawę, że jej dane osobowe mogłyby zostać w przyszłości wykorzystane przez osoby trzecie w sposób stanowiący nadużycie ze względu na naruszenie tego rozporządzenia, do którego doszło.

81 Ta literalna wykładnia znajduje potwierdzenie, w drugiej kolejności, w motywie 146 RODO, który dotyczy konkretnie prawa do odszkodowania przewidzianego w art. 82 ust. 1 tego rozporządzenia i który wskazuje w zdaniu trzecim, że „[p]ojęcie szkody należy interpretować szeroko, w świetle orzecznictwa Trybunału Sprawiedliwości, w sposób w pełni odzwierciedlający cele" tego rozporządzenia. Tymczasem wykładnia pojęcia „szkody niemajątkowej" w rozumieniu tego art. 82 ust. 1, która nie obejmowałaby sytuacji, w których osoba, której dotyczy naruszenie wspomnianego rozporządzenia, powołuje się na obawę, jaką żywi, że jej dane osobowe mogłyby zostać w przyszłości wykorzystane w sposób stanowiący nadużycie, nie odpowiadałaby szerokiej koncepcji tego pojęcia zamierzonej przez prawodawcę Unii [zob. analogicznie wyrok z dnia 4 maja 2023 r., Österreichische Post (Szkoda niemajątkowa związana z przetwarzaniem danych osobowych), C-300/21, EU:C:2023:370, pkt 37, 46].

82 Ponadto w motywie 85 zdanie pierwsze RODO wskazano, że „[p]rzy braku odpowiedniej i szybkiej reakcji naruszenie ochrony danych osobowych może skutkować powstaniem uszczerbku fizycznego, szkód majątkowych lub niemajątkowych u osób fizycznych, takich jak utrata kontroli nad własnymi danymi osobowymi lub ograniczenie praw, dyskryminacja, kradzież lub sfałszowanie tożsamości, strata finansowa, […] lub wszelkie inne znaczne szkody gospodarcze lub społeczne". Z tej przykładowej listy „szkód" lub „uszczerbków", jakie mogą ponieść osoby, których dane dotyczą, wynika, że prawodawca Unii zamierzał włączyć do tych pojęć w szczególności zwykłą „utratę kontroli" nad ich danymi w następstwie naruszenia tego rozporządzenia, nawet jeśli wykorzystanie rozpatrywanych danych w sposób stanowiący nadużycie nie nastąpiło konkretnie na niekorzyść tych osób.

83 W trzeciej i ostatniej kolejności wykładnia przedstawiona w pkt 80 niniejszego wyroku znajduje potwierdzenie w celach RODO, które należy w pełni uwzględnić przy definiowaniu pojęcia „szkody", jak wskazuje motyw 146 zdanie trzecie tego rozporządzenia. Tymczasem wykładnia art. 82 ust. 1 RODO, zgodnie z którą pojęcie „szkody niemajątkowej" w rozumieniu tego przepisu nie obejmuje sytuacji, w których osoba, której dane dotyczą, powołuje się wyłącznie na swoją obawę, że jej dane mogłyby zostać w przyszłości wykorzystane przez osoby trzecie w sposób stanowiący nadużycie, nie byłaby zgodna z przewidzianym w tym instrumencie zapewnieniem wysokiego poziomu ochrony osób fizycznych w zakresie przetwarzania danych osobowych w Unii.

84 Należy jednak podkreślić, że osoba, której dotyczy naruszenie RODO, które miało wobec niej negatywne konsekwencje, ma obowiązek wykazania, że konsekwencje te stanowią szkodę niemajątkową w rozumieniu art. 82 tego rozporządzenia [zob. podobnie wyrok z dnia 4 maja 2023 r., Österreichische Post (Szkoda niemajątkowa związana z przetwarzaniem danych osobowych), C-300/21, EU:C:2023:370, pkt 50].

85 W szczególności, jeżeli osoba domagająca się odszkodowania powołuje się na tej podstawie na obawę, że w przyszłości dojdzie do wykorzystania w sposób stanowiący nadużycie jej danych osobowych ze względu na istnienie takiego naruszenia, sąd krajowy rozpatrujący sprawę powinien zbadać, czy obawę tę należy uznać za uzasadnioną w rozpatrywanych szczególnych okolicznościach i w odniesieniu do osoby, której dane dotyczą.

86 W świetle powyższych rozważań na pytanie piąte trzeba odpowiedzieć, iż art. 82 ust. 1 RODO należy interpretować w ten sposób, że obawa przed ewentualnym wykorzystaniem przez osoby trzecie w sposób stanowiący nadużycie danych osobowych, jaką żywi osoba, której dane dotyczą, w następstwie naruszenia tego rozporządzenia może sama w sobie stanowić „szkodę niemajątkową" w rozumieniu tego przepisu.

W przedmiocie kosztów

87 Dla stron w postępowaniu głównym niniejsze postępowanie ma charakter incydentalny, dotyczy bowiem kwestii podniesionej przed sądem odsyłającym, do niego zatem należy rozstrzygnięcie o kosztach. Koszty poniesione w związku z przedstawieniem uwag Trybunałowi, inne niż koszty stron w postępowaniu głównym, nie podlegają zwrotowi.

Z powyższych względów Trybunał (trzecia izba) orzeka, co następuje:

1) **Artykuły 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:

   nieuprawnione ujawnienie danych osobowych lub nieuprawniony dostęp do takich danych przez „osoby trzecie” w rozumieniu art. 4 pkt 10 tego rozporządzenia nie wystarczają same w sobie do uznania, iż wdrożone przez danego administratora środki techniczne i organizacyjne nie były „odpowiednie” w rozumieniu tych art. 24 i 32.

2) **Artykuł 32 rozporządzenia 2016/679**

   należy interpretować w ten sposób, że:

   oceny, czy środki techniczne i organizacyjne wdrożone przez administratora na podstawie tego artykułu mają odpowiedni charakter, sądy krajowe powinny dokonywać w sposób konkretny, w szczególności uwzględniając ryzyko związane z danym przetwarzaniem oraz ustalając, czy charakter, istota i wdrożenie tych środków są dostosowane do tego ryzyka.

3) **Zasadę rozliczalności administratora wyrażoną w art. 5 ust. 2 rozporządzenia 2016/679 i skonkretyzowaną w jego art. 24**

   należy interpretować w ten sposób, że:

   w ramach powództwa o odszkodowanie opartego na art. 82 tego rozporządzenia na danym administratorze spoczywa ciężar udowodnienia, że środki bezpieczeństwa, które wdrożył na podstawie art. 32 tego rozporządzenia, mają odpowiedni charakter.

4) **Artykuł 32 rozporządzenia 2016/679 i zasadę skuteczności prawa Unii**

   należy interpretować w ten sposób, że:

   na potrzeby oceny, czy środki bezpieczeństwa wdrożone przez administratora na podstawie tego artykułu mają odpowiedni charakter, opinia biegłego sądowego nie może systematycznie stanowić niezbędnego i wystarczającego środka dowodowego.

5) **Artykuł 82 ust. 3 rozporządzenia 2016/679**

należy interpretować w ten sposób, że:

administrator nie jest na podstawie art. 82 ust. 1 i 2 tego rozporządzenia zwolniony z obowiązku naprawienia poniesionej przez daną osobę szkody z tego tylko powodu, iż szkoda ta wynika z nieuprawnionego ujawnienia danych osobowych lub nieuprawnionego dostępu do takich danych przez „osoby trzecie" w rozumieniu art. 4 pkt 10 tego rozporządzenia, gdyż ów administrator musi przy tym udowodnić, że w żaden sposób nie ponosi winy za zdarzenie, które doprowadziło do powstania szkody.

6) Artykuł 82 ust. 1 rozporządzenia 2016/679

należy interpretować w ten sposób, że:

obawa przed ewentualnym wykorzystaniem przez osoby trzecie w sposób stanowiący nadużycie danych osobowych, jaką żywi osoba, której dane dotyczą, w następstwie naruszenia tego rozporządzenia może sama w sobie stanowić „szkodę niemajątkową" w rozumieniu tego przepisu.

Podpisy