Zbiór Orzeczeń

OPINIA RZECZNIKA GENERALNEGO
GIOVANNIEGO PITRUZZELLI
przedstawiona w dniu 27 kwietnia 2023 r. [1]

Sprawa C-340/21

VB
przeciwko
Natsionalna agentsia za prihodite

[wniosek o wydanie orzeczenia w trybie prejudycjalnym złożony przez Varhoven administrativen sad (najwyższy sąd administracyjny, Bułgaria)]

Odesłanie prejudycjalne – Ochrona danych osobowych – Rozporządzenie (UE) 2016/679 – Odpowiedzialność administratora – Bezpieczeństwo przetwarzania – Naruszenie bezpieczeństwa przetwarzania danych osobowych – Szkoda niemajątkowa spowodowana bezczynnością administratora – Powództwo o odszkodowanie

Czy niezgodne z prawem ujawnienie danych osobowych będących w posiadaniu agencji publicznej, które zostało spowodowane atakiem hakerskim, może stanowić podstawę odszkodowania za szkodę niemajątkową na rzecz osoby, której dane dotyczą, tylko z tego powodu, że obawia się ona ewentualnego nieuczciwego wykorzystania jej danych w przyszłości? Jakie są kryteria przypisania odpowiedzialności administratorowi? W jaki sposób rozkłada się ciężar dowodu w postępowaniu? Jaki jest zakres kontroli sądu?

I. Ramy prawne

1. Artykuł 4 rozporządzenia 2016/679 [2] (zwanego dalej „rozporządzeniem”), zatytułowany „Definicje”, stanowi:

„Na użytek niniejszego rozporządzenia:

[…]

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

[1] Język oryginału: włoski.

[2] 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).

[…]”.

2. Artykuł 5, zatytułowany „Zasady dotyczące przetwarzania danych osobowych”, stanowi:

„1. Dane osobowe muszą być:

[…]

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«)”.

3. Artykuł 24 rozporządzenia, zatytułowany „Obowiązki administratora”, stanowi:

„1. Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze, 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”.

4. Artykuł 32, 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, administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku, w tym między innymi w stosownym przypadku:

[…]

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.

[…]”.

5. Artykuł 82 tego rozporządzenia, zatytułowany „Prawo do odszkodowania i odpowiedzialność”, stanowi:

„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”.

II. Okoliczności faktyczne, postępowanie główne i pytania prejudycjalne

6. W dniu 15 lipca 2019 r. bułgarskie media rozpowszechniły informację, zgodnie z którą miał miejsce nieuprawniony dostęp do systemu informatycznego Natsionalna agentsia za prihodite (narodowej agencji przychodów skarbowych i z tytułu składek zabezpieczenia społecznego, Bułgaria, zwanej dalej „NAP” [3]), a także, że w Internecie opublikowano różne informacje podatkowe i ubezpieczeniowe dotyczące milionów osób, zarówno obywateli bułgarskich, jak i cudzoziemców.

7. Szereg osób, w tym V.B., skarżąca w postępowaniu głównym, wniosło powództwa przeciwko NAP o zasądzenie odszkodowania za szkody niemajątkowe.

8. W niniejszej sprawie skarżąca w postępowaniu głównym wniosła powództwo do Administrativen sad Sofia-grad (sądu administracyjnego dla miasta Sofia, Bułgaria; zwanego dalej „ASSG”), utrzymując, że NAP naruszyła przepisy krajowe, a także obowiązek przetwarzania danych osobowych jako administrator w sposób „zapewniający odpowiednie standardy bezpieczeństwa” – poprzez zastosowanie odpowiednich środków technicznych i organizacyjnych zgodnie z art. 24 i 32 rozporządzenia nr 2016/679. Skarżąca wskazała ponadto, że poniosła szkody niemajątkowe wyrażające się w niepokoju i obawach, że jej dane osobowe mogą zostać wykorzystane w sposób nieuczciwy w przyszłości.

9. Druga strona postępowania podkreśliła natomiast, że nie otrzymała od skarżącej w postępowaniu głównym żadnego wniosku o udzielenie informacji o tym, do jakich konkretnie danych osobowych uzyskano dostęp. Ponadto, w następstwie informacji o włamaniu do systemu przeprowadziła ona spotkania z ekspertami w celu ochrony praw i interesów obywateli. Zdaniem NAP nie istniał również związek przyczynowy między atakiem komputerowym a podnoszoną szkodą, ponieważ agencja wdrożyła wszystkie systemy zarządzania procesami i bezpieczeństwa informacji zgodnie z obowiązującymi w tej dziedzinie normami międzynarodowymi.

[3] NAP jest administratorem w rozumieniu art. 4 pkt 7 rozporządzenia. Zgodnie z prawem krajowym jest ona organem administracji posiadającym szczególne kompetencje, podlegającym ministrowi finansów oraz odpowiedzialnym za ustalenie, zabezpieczenie i egzekwowanie finansów, a także ustalenie, zabezpieczenie i egzekwowanie wierzytelności państwa, wierzytelności publicznych i określonych na mocy ustawy wierzytelności prywatnych. W wykonaniu powierzonych jej uprawnień publicznych przetwarza ona dane osobowe.

10. Sąd pierwszej instancji, ASSG, oddalił powództwo, uznając, że NAP nie ponosi winy za ujawnienie danych, że ciężar dowodu co do odpowiedniego charakteru przyjętych środków spoczywa na skarżącej i wreszcie, że żadna szkoda niemajątkowa nie podlega naprawieniu.

11. Wyrok wydany w pierwszej instancji został następnie środek zaskarżony do Varhoven administrativen sad (najwyższego sądu administracyjnego, Bułgaria). Wśród podniesionych zarzutów skarżąca w postępowaniu głównym podkreśliła, że sąd pierwszej instancji błędnie rozłożył ciężar dowodu w odniesieniu do braku przyjęcia środków bezpieczeństwa. Szkoda niemajątkowa również nie powinna być objęta ciężarem dowodu, ponieważ nie chodzi o jedynie potencjalną, lecz rzeczywistą szkodę niemajątkową.

12. NAP ze swej strony powtórzyła, że przyjęła niezbędne środki techniczne i organizacyjne jako administrator oraz zakwestionowała istnienie dowodu rzeczywistej szkody niemajątkowej. Niepokój i obawy są bowiem stanami emocjonalnymi, które nie podlegają odszkodowaniu.

13. Sąd odsyłający zwrócił uwagę na odmienne rozstrzygnięcia w odniesieniu do poszczególnych postępowań, które poszkodowani wszczęli oddzielnie przeciwko NAP w celu uzyskania odszkodowania za szkody niemajątkowe.

14. W tym kontekście sąd odsyłający zawiesił postępowanie i zwrócił się do Trybunału z następującymi pytaniami prejudycjalnymi:

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?”.

III. Analiza prawna

A. Uwagi wstępne

15. Przedmiotem niniejszej sprawy są interesujące, a częściowo nowe kwestie dotyczące wykładni różnych przepisów rozporządzenia [4].

16. Pięć pytań prejudycjalnych dotyczy tej samej kwestii: warunków przyznania odszkodowania za szkodę niemajątkową osobie, której dane osobowe, będące w posiadaniu agencji publicznej, zostały opublikowane w Internecie w wyniku ataku hakerskiego.

17. Dla ułatwienia zaproponuję odrębne zwięzłe odpowiedzi na wszystkie pytania prejudycjalne zawarte w postanowieniu odsyłającym, choć zdaję sobie sprawę, że na płaszczyźnie konceptualnej pytania te pokrywają się w pewnym stopniu, ponieważ cztery pierwsze pytania mają na celu określenie przesłanek możliwości przypisania administratorowi [5] naruszenia przepisów rozporządzenia, a piąte pytanie odnosi się konkretnie do pojęcia szkody niemajątkowej dla celów zasądzenia odszkodowania [6].

[4] Artykułu 5 ust. 2 (dotyczącego zasady odpowiedzialności każdego administratora danych osobowych), art. 24 (dotyczącego środków, które powinien wdrożyć ten administrator, aby przetwarzanie odbywało się zgodnie z tym rozporządzeniem), art. 32 (dotyczącego tego obowiązku w szczególności w odniesieniu do bezpieczeństwa przetwarzania) oraz art. 82 ust. 1–3 (dotyczącego odszkodowania za szkody wynikające z naruszenia tego rozporządzenia oraz możliwości przyjęcia przez administratora środków w celu zapewnienia zgodności z owym rozporządzeniem), a także motywów 74, 85 i 146, które są powiązane z wymienionymi artykułami.

[5] a) pierwsze pytanie ma na celu wyjaśnienie kwestii, czy z samego naruszenia systemów można wywnioskować, że wprowadzone środki są nieodpowiednie; b) drugie pytanie odnosi się do zakresu kontroli sądowej dotyczącej tego, czy wspomniane środki są odpowiednie; c) trzecie pytanie odnosi się do ciężaru dowodu dotyczącego samego faktu, czy owe środki są odpowiednie, oraz niektórych technicznych zasad przeprowadzania dowodu; d) czwarte pytanie dotyczy tego, czy okoliczność, że atak na system nastąpił z zewnątrz, ma znaczenie dla celów zwolnienia z odpowiedzialności.

[6] Jeśli chodzi o przywołane przepisy rozporządzenia, to pierwsze trzy pytania dotyczą aspektów odpowiedzialności administratora w odniesieniu do odpowiedniego charakteru środków, jakie należy przyjąć (art. 5, 24 i 32), a pytania czwarte i piąte dotyczą przesłanek zwolnienia z odpowiedzialności i pojęcia szkody niemajątkowej podlegającej naprawieniu (art. 82).

18. Pragnę zauważyć, że obecnie przed Trybunałem toczy się kilka spraw dotyczących art. 82 rozporządzenia, a w jednej z nich przedstawiono już opinię rzecznika generalnego, którą uwzględnię w niniejszej analizie [7].

19. Uważam, że przed rozpoczęciem analizy przedstawionych pytań należy poczynić kilka uwag wstępnych dotyczących zasad i celów rozporządzenia, które będą przydatne w celu udzielenia odpowiedzi na każde z pytań prejudycjalnych.

20. Artykuł 24 rozporządzenia ustanawia w sposób ogólny obowiązek wdrożenia przez administratora odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie odbywało się zgodnie z samym rozporządzeniem i aby móc to wykazać, natomiast art. 32 ustanawia bardziej szczegółowo ten sam obowiązek w odniesieniu do bezpieczeństwa przetwarzania. Artykuły 24 i 32 precyzują to, co jest już przewidziane w art. 5 ust. 2, który wprowadza „zasadę rozliczalności" właśnie wśród „zasad mających zastosowanie do przetwarzania danych osobowych". Zasada ta wynika logicznie z „zasady integralności i poufności" przewidzianej w art. 5 ust. 1 lit. f) i stanowi jej uzupełnienie, a obie zasady należy interpretować w świetle podejścia opartego na ryzyku, na którym opiera się rozporządzenie.

21. Zasada rozliczalności jest jednym z filarów rozporządzenia i jedną z jego najistotniejszych innowacji. Nakłada ona na administratora odpowiedzialność za podejmowanie proaktywnych działań w celu zapewnienia zgodności z rozporządzeniem i udowodnienie zgodności z rozporządzeniem [8].

22. W doktrynie mowa była o rzeczywistej zmianie kulturowej jako efekcie „ogólnego zakresu obowiązku odpowiedzialności" [9]. To nie formalne przestrzeganie obowiązku prawnego lub jednorazowego środka, lecz cała przyjęta strategia przedsiębiorstwa zwalnia administratora z odpowiedzialności ze względu na przestrzeganie przepisów o ochronie danych.

23. Środki techniczne i organizacyjne wymagane zgodnie z zasadą rozliczalności muszą być „odpowiednie" w świetle czynników określonych w art. 24, a mianowicie charakteru, zakresu stosowania, kontekstu i celów przetwarzania oraz prawdopodobieństwa i wagi ryzyka naruszenia praw i wolności osób fizycznych.

24. Artykuł 24 ustanawia zatem obowiązek, zgodnie z którym środki muszą być odpowiednie, aby móc wykazać zgodność przetwarzania z zasadami i przepisami rozporządzenia.

25. Z kolei art. 32 odnosi zasadę rozliczalności do konkretnych środków, które należy przyjąć, aby zapewnić „stopień bezpieczeństwa odpowiadający temu ryzyku". W ten sposób w przepisie tym wprowadzono oprócz już przewidzianych czynników, które należy uwzględnić przy wdrażaniu środków technicznych i organizacyjnych, stan wiedzy technicznej i koszt wdrażania.

26. Pojęcie odpowiedniego charakteru wymaga, aby rozwiązania przyjęte w celu zabezpieczenia systemów informatycznych osiągnęły poziom akceptowalności zarówno pod względem technicznym (istotność środków), jak i jakościowym (skuteczność ochrony). W celu zapewnienia

[7] Zobacz opinia rzecznika generalnego M. Camposa Sáncheza-Bordony w sprawie Österreichische Post (Szkoda niemajątkowa wynikająca z niezgodnego z prawem przetwarzania danych) (C-300/21, EU:C:2022:756).

[8] C. Docksey, Article 24. Responsibility of the controller, w: C. Kuner, L.A. Bygrave, C. Docksey, L. Drechsler, *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford University Press, 2020, s. 561. Zasady i obowiązki wynikające z przepisów o ochronie danych powinny raczej przenikać strukturę kulturową organizacji na wszystkich poziomach, a nie być traktowane jako szereg wymogów prawnych, które muszą być spełnione przez dział prawny.

[9] E. Belisario, G. Riccio, G. Scorza, *GDPR e Normativa Privacy – Commentario*, Wolters Kluwer, 2022, s. 301.

poszanowania zasad konieczności, istotności i proporcjonalności operacje przetwarzania muszą być nie tylko odpowiednie, lecz również zadowalające w odniesieniu do zamierzonych celów. Decydującą rolę w tej logice odgrywa zasada minimalizacji, zgodnie z którą na wszystkich etapach przetwarzania danych należy stale dążyć do zminimalizowania ryzyka dla bezpieczeństwa [10].

27. Całe rozporządzenie opiera się na zapobieganiu ryzyku i rozliczalności administratora, a zatem na podejściu celowościowym, które ma na celu osiągnięcie jak najlepszego wyniku pod względem skuteczności, to znaczy znacznie odbiega od logiki formalistycznej związanej z samym obowiązkiem przestrzegania konkretnych procedur w celu uwolnienia się od odpowiedzialności [11].

28. Artykuł 24 nie zawiera wyczerpującego wykazu „odpowiednich" środków i w związku z tym konieczne jest dokonanie oceny każdego przypadku z osobna. Jest to zgodne z filozofią rozporządzenia, z której wynika, że preferowane jest, by procedury, które mają zostać przyjęte, były wybierane na podstawie dokładnej oceny konkretnej sytuacji, tak by mogły być jak najskuteczniejsze [12].

B. W przedmiocie pierwszego pytania prejudycjalnego

29. Poprzez pytanie pierwsze sąd odsyłający zmierza zasadniczo do ustalenia, czy art. 24 i 32 rozporządzenia należy interpretować w ten sposób, że wystąpienie „naruszenia danych osobowych", zdefiniowanego w art. 4 pkt 12, jest wystarczające samo w sobie do stwierdzenia, że wdrożone przez administratora środki techniczne i organizacyjne nie były „odpowiednie" w celu zapewnienia ochrony danych.

30. Z brzmienia art. 24 i 32 rozporządzenia wynika, że administrator, dokonując wyboru środków technicznych i organizacyjnych, które jest zobowiązany wdrożyć w celu zapewnienia zgodności z samym rozporządzeniem, musi wziąć pod uwagę szereg czynników oceny wymienionych w tych artykułach i przywołanych powyżej.

31. Administrator ma pewien zakres swobody, jeśli chodzi o określenie najbardziej odpowiednich środków w świetle jego konkretnej sytuacji, jednak taki wybór podlega ewentualnej kontroli sądowej zgodności zastosowanych środków ze wszystkimi obowiązkami i celami samego rozporządzenia.

32. W szczególności, w odniesieniu do środków bezpieczeństwa w art. 32 ust. 1 nakłada się na administratora obowiązek uwzględnienia „stanu wiedzy technicznej". Oznacza to ograniczenie poziomu technologicznego wdrażanych środków do tego, co jest racjonalnie możliwe w chwili

[10] E. Belisario, G. Riccio, G. Scorza, op.cit., s. 380.

[11] Dlatego też, jak zostanie to wykazane poniżej, na pytania prejudycjalne pierwsze i czwarte należy udzielić odpowiedzi przeczącej. Z przepisów rozporządzenia nie można wywieść żadnego automatyzmu: ani sam fakt, że doszło do ujawnienia danych osobowych, nie jest wystarczający, aby stwierdzić, że przyjęte środki techniczne i organizacyjne są nieodpowiednie, ani również okoliczność, że samo ujawnienie miało miejsce w wyniku interwencji podmiotów niezwiązanych z organizacją administratora i niepodlegających jego kontroli, nie jest wystarczająca, aby zwolnić administratora z odpowiedzialności.

[12] L. Bolognini, E. Pelino, *Codice della disciplina privacy*, Giuffrè, 2019, s. 201. Prawodawca Unii wykracza zatem poza koncepcję bezpieczeństwa przetwarzania opartą na istnieniu z góry określonych środków bezpieczeństwa i przyjmuje metodologię właściwą dla norm międzynarodowych dotyczących zarządzania systemami informatycznymi opartymi na ryzyku: przewiduje ona określenie środków ograniczających ryzyko, które są niezależne od z góry ustalonych i powszechnie stosowanych list kontrolnych. Należy zatem zastosować wytyczne i normy międzynarodowe. Wynik tej oceny ryzyka staje się zatem wiążący z chwilą, gdy organizacja podejmuje decyzje w celu ograniczenia zidentyfikowanego ryzyka, czyniąc siebie odpowiedzialną.

przyjęcia środków, co znaczy, że zdolność środka do zapobiegania ryzyku musi być zatem proporcjonalna do rozwiązań, jakie oferuje obecny stan zaawansowania nauki, techniki, technologii i badań, przy uwzględnieniu również, jak zostanie to wyjaśnione, kosztów wdrażania.

33. Środki mogą być „odpowiednie" w danym momencie, a mimo to mogą być obchodzone przez cyberprzestępców stosujących bardzo zaawansowane narzędzia, które mogą naruszyć również środki bezpieczeństwa zgodne ze stanem wiedzy technicznej.

34. Ponadto nielogiczne wydaje się założenie, że zamiarem prawodawcy Unii było nałożenie na administratora obowiązku zapobiegania wszelkim naruszeniom danych osobowych, niezależnie od staranności we wprowadzaniu środków bezpieczeństwa [13].

35. Jak wskazano powyżej, rozporządzenie odchodzi od automatyzmu, wymagając wysokiego poziomu rozliczalności administratora, co nie może jednak prowadzić do tego, że nie będzie on w stanie udowodnić, iż prawidłowo wykonał nałożone na niego obowiązki.

36. Co więcej art. 32 ust. 1 stanowi, że należy uwzględnić, jak już wspomniano, „koszt wdrażania" rozpatrywanych środków technicznych i organizacyjnych. Wynika z tego, że ocena odpowiedniości takich środków musi być oparta na wyważeniu interesów osoby, której dane dotyczą, które ogólnie zmierzają do wyższego poziomu ochrony, z interesami finansowymi i możliwościami technologicznymi administratora, które niekiedy zmierzają do niższego poziomu ochrony. Wyważenie to musi być zgodne z wymogami ogólnej zasady proporcjonalności.

37. Ponadto należy dodać w świetle wykładni systemowej, że prawodawca przewiduje możliwość wystąpienia naruszeń systemów. W art. 32 ust. 1 lit. c) wymieniono wśród sugerowanych środków zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego. Zapewnienie takiej zdolności wśród środków bezpieczeństwa gwarantujących poziom bezpieczeństwa odpowiedni do ryzyka byłoby bezcelowe, gdyby uznać, że samo naruszenie systemów stanowi samo w sobie dowód świadczący o nieodpowiednim charakterze takich środków.

C. W przedmiocie drugiego pytania prejudycjalnego

38. Poprzez pytanie drugie sąd odsyłający zmierza zasadniczo do ustalenia, jaki powinien być przedmiot i zakres kontroli sądowej przy weryfikacji, czy wdrożone przez administratora danych osobowych środki techniczne i organizacyjne w rozumieniu art. 32 rozporządzenia są odpowiednie.

39. Biorąc pod uwagę zmienność sytuacji, które mogą wystąpić w praktyce, rozporządzenie, jak wspomniano, nie ustanawia wiążących przepisów dotyczących określenia środków technicznych i organizacyjnych, jakie administrator musi przyjąć, aby spełnić wymogi wynikające z samego rozporządzenia. Odpowiedni charakter przyjętych środków będzie zatem musiał być oceniany in concreto poprzez zbadanie, czy konkretne środki były odpowiednie, aby zapobiec w racjonalny sposób ryzyku i zminimalizować negatywne skutki naruszenia.

[13] Pojęcie odpowiedniego charakteru wskazuje jednoznacznie na zamiar nienadawania znaczenia wszystkim teoretycznie możliwym środkom technicznym i organizacyjnym. Zobacz podobnie M. Gambini, Responsabilità e risarcimento nel trattamento dei dati personali, w: V. Cuffaro, R. D'Orazio, V. Ricciuto, *I dati personali nel diritto europeo, Giappichelli*, 2019, s. 1059.

40. O ile niewątpliwie prawdą jest, że wybór i wdrożenie takich środków należy do subiektywnej oceny administratora, ponieważ środki wymienione w rozporządzeniu są jedynie przykładami, o tyle kontrola sądu nie może ograniczać się do sprawdzenia, czy administrator wykonuje obowiązki wynikające z art. 24 i 32, to znaczy czy przewidział (formalnie) określone środki techniczne i organizacyjne. Sąd musi dokonać konkretnej analizy treści takich środków, sposobu, w jaki zostały one zastosowane, oraz ich praktycznych skutków na podstawie dowodów, którymi dysponuje, i okoliczności danej sprawy. Jak słusznie zauważył rząd portugalski, „sposób, w jaki administrator wykonał swoje obowiązki, wydaje się nierozerwalnie związany z treścią przyjętych środków, aby wykazać, że biorąc pod uwagę konkretną operację przetwarzania danych (jej charakter, zakres, kontekst i cele), stan wiedzy technicznej o dostępnych technologiach i ich kosztach, a także ryzyko naruszenia praw i wolności obywateli, administrator przyjął wszelkie niezbędne i odpowiednie środki w celu zapewnienia poziomu bezpieczeństwa odpowiedniego do podstawowego ryzyka” [14].

41. W ramach kontroli sądowej konieczne będzie zatem uwzględnienie wszystkich czynników zawartych w art. 24 i 32, w których, jak wspomniano, wymieniono szereg kryteriów oceny odpowiedniego charakteru i wskazano przykłady środków, które mogą być uznane za odpowiednie. Ponadto, jak podkreśliły Komisja i wszystkie państwa członkowskie, które przedstawiły uwagi dotyczące pytania drugiego, w art. 32 ust. 1–3 zwrócono uwagę konieczność „zapewni[enia] stop[nia] bezpieczeństwa odpowiadając[ego] temu ryzyku”, wskazując w tym celu inne istotne czynniki, takie jak ewentualne przyjęcie przez administratora zatwierdzonego kodeksu postępowania lub zatwierdzonego systemu certyfikacji, jak przewidziano odpowiednio w art. 40 i 42 rozporządzenia.

42. Przyjęcie kodeksów postępowania lub systemów certyfikacji może stanowić przydatny element oceny w celu wywiązania się z ciężaru dowodu i związanej z tym kontroli sądowej. Należy jednak uściślić, że nie wystarczy, by administrator przestrzegał kodeksu postępowania, gdyż spoczywa na nim ciężar udowodnienia, że przyjął konkretnie przewidziane przez siebie środki zgodnie z zasadą rozliczalności. Natomiast certyfikacja stanowi „sama w sobie dowód zgodności z rozporządzeniem dokonanych operacji przetwarzania, nawet jeśli w praktyce dowód ten może zostać podważony” [15].

43. Wreszcie należy zauważyć, że środki te muszą być w razie potrzeby poddawane przeglądom i uaktualniane zgodnie z art. 24 ust. 1. I to również będzie podlegało ocenie sądu krajowego. Artykuł 32 ust. 1 rozporządzenia [16] nakłada bowiem na administratora obowiązek stałej kontroli i monitorowania przed rozpoczęciem i po zakończeniu czynności przetwarzania, lecz także utrzymania i ewentualnej aktualizacji przyjętych środków zarówno w celu zapobiegania naruszeniom, jak i, w stosownych przypadkach, ograniczenia ich skutków.

[14] Uwagi na piśmie, pkt 31.

[15] M. Gambini, Responsabilità…, op.cit., s. 1067. Posiadanie certyfikacji powoduje zatem odwrócenie ciężaru dowodu na korzyść administratora, któremu ułatwia się wykazanie, że działał z poszanowaniem obowiązków wynikających z rozporządzenia.

[16] Stanowiąc wyraźnie w lit. d), że ocena odpowiedniego charakteru obejmuje skuteczność przyjętych środków, która musi być regularnie testowana, mierzona i oceniana zarówno na etapie początkowym, jak i w regularnych odstępach czasu w celu zapewnienia skutecznego bezpieczeństwa wszystkich rodzajów przetwarzania, niezależnie od ich poziomu ryzyka; ponadto stanowiąc wyraźnie w lit. c), że wdrożone środki techniczne i organizacyjne muszą być zdolne do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego. Zobacz M. Gambini, Responsabilità…, op.cit., s. 1064, 1065.

44. Skłaniałbym się jednak do wykluczenia możliwości, że następny wyrok będzie zawierał wykaz istotnych elementów, taki jak ten zaproponowany przez rząd portugalski [17]. Mogłoby to prowadzić do sprzecznych wykładni, ponieważ wykaz oczywiście nigdy nie może być wyczerpujący.

D. W przedmiocie trzeciego pytania prejudycjalnego

45. Poprzez pierwszą część pytania trzeciego sąd odsyłający zwraca się zasadniczo do Trybunału o ustalenie, czy, przy uwzględnieniu zasady rozliczalności ustanowionej w art. 5 ust. 2 i art. 24 w związku z motywem 74 [18] rozporządzenia, w ramach powództwa o odszkodowanie na podstawie art. 82 na administratorze danych osobowych spoczywa ciężar udowodnienia okoliczności, że środki techniczne i organizacyjne w rozumieniu art. 32 są odpowiednie.

46. Wcześniejsze rozważania pozwalają mi na udzielenie na to pytanie krótkiej odpowiedzi twierdzącej.

47. Brzmienie prawa, kontekst i cele rozporządzenia przemawiają bowiem w sposób jednoznaczny za tym, że ciężar dowodu spoczywa na administratorze.

48. Z brzmienia szeregu przepisów rozporządzenia wynika, że administrator musi być „w stanie" lub być „zdolny" „wykazać", że przestrzega obowiązków wynikających z rozporządzenia, w szczególności że wdrożył w tym celu odpowiednie środki, jak wskazano w motywie 74, art. 5 ust. 2 i art. 24 ust. 1. Jak podkreśla rząd portugalski, rzeczony motyw 74 wskazuje, że nałożony w ten sposób na administratora ciężar dowodu powinien obejmować dowód na to, „że [dane środki] są skuteczne".

49. Wydaje mi się, że za taką literalną wykładnią przemawiają następujące względy praktyczne i celowościowe.

50. W odniesieniu do rozkładu ciężaru dowodu w ramach powództwa o odszkodowanie opartego na art. 82 osoba, której dane dotyczą, która wytoczyła powództwo przeciwko administratorowi, musi udowodnić, po pierwsze, że miało miejsce naruszenie rozporządzenia, po drugie, że poniosła szkodę, i po trzecie, że istnieje związek przyczynowy między dwoma poprzednimi elementami, jak

[17] Punkt 30 uwag na piśmie: „[A]dministrator będzie musiał wykazać, w jaki sposób ocenił wszystkie czynniki i okoliczności dotyczące danej operacji przetwarzania, w szczególności wynik przeprowadzonej analizy ryzyka, zidentyfikowane ryzyko, konkretne środki zastosowane w celu ograniczenia tego ryzyka, uzasadnienie wybranych możliwości w świetle dostępnych na rynku rozwiązań technologicznych, skuteczność środków, korelację pomiędzy środkami technicznymi i organizacyjnymi, szkolenie personelu przetwarzającego dane, istnienie outsourcingu operacji przetwarzania danych, w tym rozwój i utrzymanie technologii informatycznych, a także istnienie kontroli prowadzonej przez administratora oraz dokładnych instrukcji udzielanych podmiotom przetwarzającym zgodnie z art. 28 RODO, dotyczących przetwarzania danych osobowych przez podmioty przetwarzające; w jaki sposób oceniono infrastrukturę wspierającą systemy komunikacyjne i informacyjne oraz w jaki sposób sklasyfikowano poziom ryzyka dla praw i wolności osób, których dane dotyczą".

[18] Zgodnie z motywem 74 „[n]ależy 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".

wskazano we wszystkich uwagach na piśmie dotyczących piątego pytania prejudycjalnego. Są to trzy przesłanki kumulatywne, jak wynika również z utrwalonego orzecznictwa Trybunału i Sądu w kontekście odpowiedzialności pozaumownej Unii [19].

51. Uważam jednak, że obowiązek udowodnienia przez skarżącą, że doszło do naruszenia rozporządzenia, nie może iść tak daleko, by wymagać wykazania, że wdrożone przez administratora środki techniczne i organizacyjne nie są odpowiednie w rozumieniu art. 24 i 32.

52. Jak podkreśla Komisja, przedstawienie takich dowodów byłoby często prawie niemożliwe w praktyce, ponieważ osoby, których dane dotyczą, nie mają na ogół ani wystarczającej wiedzy, aby móc przeanalizować takie środki, ani dostępu do wszystkich informacji będących w posiadaniu administratora kwestionowanego przetwarzania, w szczególności w odniesieniu do metod stosowanych w celu zapewnienia bezpieczeństwa takiego przetwarzania. Ponadto administrator mógłby niekiedy twierdzić, że odmowa przez niego ujawnienia tych okoliczności faktycznych osobom, których dane dotyczą, opiera się na uzasadnionej podstawie nieujawniania jego spraw wewnętrznych lub nawet elementów objętych tajemnicą zawodową, między innymi właśnie ze względów bezpieczeństwa.

53. Gdyby zatem uznać, że ciężar dowodu spoczywa na osobie, której dane dotyczą, praktyczną konsekwencją byłoby to, że przewidziane w art. 82 ust. 1 prawo do wniesienia powództwa straciłoby w znacznym stopniu swoje znaczenie. Moim zdaniem byłoby to niezgodne z zamiarem prawodawcy Unii, który, przyjmując to rozporządzenie, dążył do wzmocnienia praw osób, których dane dotyczą, oraz obowiązków administratorów w porównaniu z dyrektywą 95/46, którą rozporządzenie to zastąpiło. Jest zatem bardziej logiczne i prawnie uzasadnione, by administrator był zobowiązany do wykazania w ramach obrony przed powództwem o odszkodowanie, iż przestrzegał obowiązków wynikających z art. 24 i 32 tego rozporządzenia poprzez przyjęcie rzeczywiście odpowiednich środków.

54. Poprzez drugą część pytania trzeciego sąd odsyłający zwraca się zasadniczo do Trybunału o ustalenie, czy opinia biegłego sądowego może zostać uznana za niezbędny i wystarczający dowód w celu oceny odpowiedniości środków technicznych i organizacyjnych wdrożonych przez administratora danych osobowych w sytuacji, w której nieuprawniony dostęp do danych osobowych i ich ujawnienie jest wynikiem ataku hakerskiego.

55. Uważam, że – jak podkreśliły również (co do istoty) rządy bułgarski i włoski, Irlandia oraz Komisja – odpowiedź na te pytania powinna opierać się na utrwalonym orzecznictwie Trybunału, zgodnie z którym, na mocy zasady autonomii proceduralnej, w braku przepisów prawa Unii w tej dziedzinie do wewnętrznego porządku prawnego każdego państwa członkowskiego należy uregulowanie szczegółowych zasad proceduralnych dotyczących postępowań sądowych mających na celu ochronę praw jednostek, pod warunkiem jednak, by zasady te nie były mniej korzystne w sytuacjach objętych prawem Unii niż zasady odnoszące się do podobnych sytuacji podlegających prawu krajowemu (zasada równoważności) oraz by w praktyce nie uniemożliwiały lub nie czyniły nadmiernie uciążliwym wykonywania uprawnień przyznanych w prawie Unii (zasada skuteczności).

[19] Zobacz w szczególności wyroki Trybunału: z dnia 5 września 2019 r., Unia Europejska/Guardian Europe i Guardian Europe/Unia Europejska (C-447/17 P i C-479/17 P, EU:C:2019:672, pkt 147); z dnia 28 października 2021 r., Vialto Consulting/Komisja (C-650/19 P, EU:C:2021:879, pkt 138); a także wyroki Sądu: z dnia 13 stycznia 2021 r., Helbert/EUIPO (T-548/18, EU:T:2021:4, pkt 116); z dnia 29 września 2021 r., Kočner/Europol (T-528/20, niepublikowany, EU:T:2021:631, pkt 61), w których przypomniano, że muszą być spełnione trzy przesłanki, a mianowicie „bezprawność[ć] zachowania zarzucanego instytucjom Unii, rzeczywistość[ć] szkody oraz istnieni[e] związku przyczynowego pomiędzy tym zachowaniem a podniesioną szkodą”.

56. W niniejszej sprawie pragnę zauważyć, że rozporządzenie nie zawiera żadnego przepisu mającego na celu określenie dopuszczalnych metod dowodowych i ich mocy dowodowej, w szczególności w odniesieniu do czynności dowodowych (takich jak opinia biegłego), które sądy krajowe mogą lub muszą zarządzić w celu dokonania oceny, czy administrator danych osobowych przyjął odpowiednie środki w rozumieniu tego rozporządzenia. Uważam zatem, że w braku zharmonizowanych przepisów w tej dziedzinie do wewnętrznego porządku prawnego każdego państwa członkowskiego należy określenie tych zasad proceduralnych, z zastrzeżeniem przestrzegania zasad równoważności i skuteczności.

57. Wspomniana „zasada skuteczności", z której wynika, że niezależny sąd musi dokonać bezstronnej oceny, mogłaby zostać naruszona, gdyby przymiotnik „wystarczający" miał być rozumiany w znaczeniu, jakie moim zdaniem nadaje mu sąd odsyłający, to znaczy, że z opinii biegłego można automatycznie wywnioskować, iż środki przyjęte przez administratora są odpowiednie [20].

E. W przedmiocie czwartego pytania prejudycjalnego

58. Poprzez pytanie czwarte sąd odsyłający zmierza zasadniczo do ustalenia, czy art. 82 ust. 3 rozporządzenia należy interpretować w ten sposób, że w przypadku gdy naruszenie tego rozporządzenia (polegające, jak ma to miejsce w niniejszej sprawie, na „nieuprawnionym ujawnieniu" lub „nieuprawnionym dostępie" do danych osobowych w rozumieniu art. 4 pkt 12) zostało popełnione przez osoby, które nie są pracownikami administratora tych danych i nie podlegają jego kontroli, okoliczność ta stanowi zdarzenie, za które administrator nie ponosi w żaden sposób winy i które w związku z tym jest podstawą zwolnienia go z odpowiedzialności zgodnie z art. 82 ust. 3.

59. Odpowiedź na to pytanie wynika liniowo z tego, co zostało przedstawione powyżej w odniesieniu do ogólnej filozofii rozporządzenia: nie przewidziano automatyzmu, a zatem sama okoliczność, że nieuprawnione ujawnienie danych osobowych lub nieuprawniony dostęp do nich miały miejsce z powodu osób niepodlegających kontroli administratora, nie zwalnia administratora z odpowiedzialności.

60. Po pierwsze, w odniesieniu do brzmienia przepisów należy zauważyć, że ani art. 82 ust. 3, ani motyw 146 nie ustanawiają żadnych szczególnych przesłanek, które mogą być spełnione, aby administrator został zwolniony z odpowiedzialności, poza udowodnieniem, że „w żaden sposób nie ponos[i] winy za zdarzenie, które doprowadziło do powstania szkody". Ze sformułowania tego wynika z jednej strony, że administrator może zostać zwolniony z odpowiedzialności tylko wtedy, gdy wykaże, że nie ponosi winy za zdarzenie, które doprowadziło do rozpatrywanej szkody, a z drugiej strony, że wymagany w tym przepisie standard dowodu jest wysoki, biorąc pod uwagę użycie wyrażenia „w żaden sposób", jak podkreśliła Komisja [21].

61. System odpowiedzialności przewidziany w art. 82 oraz ogólniej w całym rozporządzeniu był przedmiotem szerokiej debaty w doktrynie różnych państw członkowskich. Zawiera on bowiem tradycyjne elementy właściwe dla odpowiedzialności deliktowej, lecz także elementy, które w strukturze przepisów zbliżają go do odpowiedzialności umownej lub nawet do formy

[20] Uwagi na piśmie, pkt 39.

[21] Zgodnie z utrwalonym orzecznictwem Trybunału, w myśl którego wyjątki od zasady ogólnej należy interpretować w sposób ścisły, ewentualne zwolnienie z odpowiedzialności przewidziane w art. 82 ust. 3 należy interpretować w sposób ścisły. Zobacz analogicznie wyroki: z dnia 15 października 2020 r., Association française des usagers de banques (C-778/18, EU:C:2020:831, pkt 53); z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in. (C-140/20, EU:C:2022:258, pkt 40).

odpowiedzialności obiektywnej ze względu na nieodłączny niebezpieczny charakter działalności polegającej na przetwarzaniu danych. Celem niniejszej opinii nie jest przedstawienie szczegółowej debaty, ale moim zdaniem art. 82 nie wydaje się wskazywać na system odpowiedzialności obiektywnej [22].

62. Szkoda wynikająca z naruszenia danych osobowych może być zawinionym następstwem braku przyjęcia racjonalnych i w każdym przypadku odpowiednich środków technicznych i organizacyjnych w celu zapobieżenia tej szkodzie, biorąc pod uwagę ryzyko naruszenia praw i wolności osób związane z czynnością przetwarzania. Ryzyko to powoduje zaostrzenie obowiązku zapobiegania szkodzie i unikania jej, rozszerzając obowiązek staranności spoczywający administratorze. W związku z tym argumentację przemawiającą za uznaniem zaostrzonego charakteru odpowiedzialności z tytułu domniemanej winy w przypadku odpowiedzialności za niezgodne z prawem przetwarzanie danych osobowych, o którym mowa w art. 82 rozporządzenia, można opierać na łącznym odczytaniu obowiązków dotyczących zachowania się spoczywających na administratorze oraz przepisu dotyczącego dowodu zwalniającego z odpowiedzialności, którego ciężar spoczywa na sprawcy szkody [23].

63. Wynika z tego możliwość przedstawienia przez administratora dowodu zwalniającego z odpowiedzialności (niedopuszczalnego w przypadku odpowiedzialności obiektywnej). W odniesieniu do struktury ciężaru dowodu art. 82 ust. 3 rozporządzenia ustanawia system korzystny dla poszkodowanego, przewidując formę odwrócenia ciężaru dowodu winy sprawcy szkody [24] w sposób w pełni zgodny ze wspomnianym odwróceniem ciężaru dowodu w odniesieniu do odpowiedniości przyjętych środków. Prawodawca wskazuje w ten sposób, że jest świadomy niebezpieczeństw, jakie wiążą się z przyjęciem innego rozkładu ciężaru dowodu, oraz że gdyby nałożył ciężar dowodu winy sprawcy szkody na poszkodowaną osobę fizyczną, doprowadziłby do nadmiernego obciążenia jej pozycji, a tym samym do naruszenia de facto skuteczności ochrony odszkodowawczej w ramach przepisów związanych z wykorzystaniem nowych technologii. Odtworzenie warunków powstania szkody i uzyskanie do nich dostępu, a w konsekwencji udowodnienie winy administratora, mogłoby być bowiem szczególnie uciążliwe dla osoby, której dane dotyczą. I odwrotnie, administrator znajduje się w najlepszej sytuacji, aby przedstawić dowód zwalniający z odpowiedzialności w celu wykazania, że nie ponosi w żaden sposób winy za zdarzenie, które doprowadziło do powstania szkody [25].

64. Administrator będzie musiał również wykazać zgodnie z opisaną powyżej zasadą rozliczalności, że uczynił wszystko, co możliwe, aby szybko przywrócić dostępność danych osobowych i dostęp do nich.

[22] Odpowiedzialność cywilna kwalifikowana jest jako obiektywna w każdym przypadku, gdy podmiot działający jest zobowiązany do przyjęcia wszelkich teoretycznie możliwych środków w celu uniknięcia szkody, niezależnie od rzeczywistej wiedzy, jaką o nich posiadał, lub ich efektywności finansowej. Natomiast w sytuacji, gdy nakłada się na podmiot działający obowiązek przyjęcia środków zwykle przestrzeganych przez podmiot gospodarczy w danym sektorze gospodarki w celu utrzymania bezpieczeństwa i zapobieżenia szkodom, które mogą wyniknąć z wykonywanej działalności, przypisanie samej szkody jest objęte systemem odpowiedzialności na zasadzie winy. M. Gambini, Responsabilità…, op.cit., s. 1055.

[23] M. Gambini, Responsabilità…, op.cit. s. 1059. Podobnie, w odniesieniu do poglądu, zgodnie z którym dowód przyjęcia odpowiednich środków nie polega na samym twierdzeniu, że zachowana została najwyższa wymagana staranność, lecz na wykazaniu czynu osoby trzeciej powodującego szkodę, cechującego się nieprzewidywalnością i nieuchronnością właściwymi dla nieprzewidywalnej okoliczności i siły wyższej, zob. S. Sica, Sub art. 82, w: R. D'Orazio, G. Finocchiaro, O. Pollicino, G. Resta, *Codice della privacy e data protection*, Giuffrè, 2021.

[24] „[J]eżeli *udowodn*[*i*], że w żaden sposób nie ponos[i] winy za zdarzenie, które doprowadziło do powstania szkody" (art. 82 ust. 3).

[25] M. Gambini, *Responsabilità*…, op.cit., s. 1060.

65. Wracając do pytania sądu odsyłającego w oparciu o powyższe rozważania dotyczące charakteru odpowiedzialności administratora: jeżeli, jak już wspomniałem, administrator może zostać zwolniony z odpowiedzialności poprzez wykazanie, że naruszenie nastąpiło z przyczyny, za którą w żaden sposób nie ponosi on winy, to sam fakt, iż zdarzenie zostało spowodowane przez osobę niepodlegającą jego kontroli, nie może być za taką przyczynę uznany.

66. W przypadku gdy administrator jest ofiarą ataku ze strony cyberprzestępców, można by uznać, że administrator nie ponosi winy za zdarzenie, które doprowadziło do powstania szkody, ale nie jest wykluczone, że zaniedbanie administratora mogło doprowadzić do danego ataku, ułatwiając jego sytuację z powodu braku lub nieodpowiedniego charakteru środków bezpieczeństwa danych osobowych, które ten ostatni jest zobowiązany wdrożyć. Chodzi o oceny okoliczności faktycznych każdego przypadku z osobna, które pozostawia się sądowi krajowemu rozpatrującemu sprawę w świetle przedstawionych mu dowodów.

67. Ponadto z doświadczenia powszechnego wynika, że zewnętrzne ataki na systemy podmiotów publicznych lub prywatnych będących administratorami dużej ilość danych osobowych są znacznie częstsze niż ataki wewnętrzne. Administrator musi zatem wdrożyć odpowiednie środki, aby poradzić sobie w szczególności z atakami zewnętrznymi.

68. Wreszcie z celowościowego punktu widzenia należy zauważyć, że rozporządzenie dąży do osiągnięcia celu, jakim jest wysoki poziom ochrony. W tym względzie Trybunał podkreślił już, że z art. 1 ust. 2 w związku z motywami 10, 11 i 13 rozporządzenia wynika, że rozporządzenie to nakłada na instytucje, organy i jednostki organizacyjne Unii oraz na właściwe organy państw członkowskich obowiązek zapewnienia wysokiego poziomu ochrony praw związanych z ochroną danych osobowych zagwarantowanych w art. 16 TFUE i w art. 8 karty[26].

69. Gdyby Trybunał przyjął wykładnię, zgodnie z którą w sytuacji, gdy naruszenie rozporządzenia zostało popełnione przez osobę trzecią, administrator powinien być automatycznie zwolniony z odpowiedzialności na podstawie art. 82 ust. 3, taka wykładnia miałaby skutek niezgodny z celem ochrony realizowanym przez ten instrument, ponieważ osłabiłaby prawa osób, których dane dotyczą, ze względu na to, że ograniczyłaby tę odpowiedzialność do przypadków, w których naruszenie zostało spowodowane przez osoby podlegające nadzorowi lub kontroli tego administratora.

F. W przedmiocie piątego pytania prejudycjalnego

70. Poprzez pytanie piąte sąd krajowy zwraca się zasadniczo do Trybunału o dokonanie wykładni pojęcia „szkody niematerialnej” (używając języka rozporządzenia – szkody „niemajątkowej”) w rozumieniu art. 82 rozporządzenia. W szczególności sąd krajowy zwraca się z pytaniem, czy przepisy art. 82 ust. 1 i 2 w związku z motywami 85 i 146 rozporządzenia[27] należy interpretować w ten sposób, że w sytuacji, w której naruszenie tego rozporządzenia polegało na

[26] Zobacz podobnie wyrok z dnia 15 czerwca 2021 r., Facebook Ireland i in. (C-645/19, EU:C:2021:483, pkt 44, 45).

[27] Zgodnie z motywem 85 „[p]rzy braku odpowiedniej i szybkiej reakcji naruszenie ochrony danych osobowych może skutkować powstaniem uszczerbku fizycznego, szkód majątkowych lub niemajątkowych u osób fizycznych […]”. W myśl motywu 146 „[z]a 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 […]. Osoby, których dane dotyczą, powinny uzyskać pełne i skuteczne odszkodowanie za poniesione szkody […]”.

nieuprawnionym dostępie do danych osobowych i nieuprawnionym ujawnieniu tych danych przez cyberprzestępców, okoliczność, że osoba, której dane dotyczą, obawia się potencjalnego nieuczciwego wykorzystania jej danych osobowych w przyszłości, może sama w sobie stanowić szkodę (niemajątkową) uprawniającą do odszkodowania.

71. Ani art. 82, ani motywy dotyczące odszkodowania nie dają wyraźnej odpowiedzi na to pytanie, ale można z nich wywnioskować pewne elementy przydatne dla analizy: szkoda niemajątkowa (lub niematerialna) może być podstawą odszkodowania oprócz szkody majątkowej (lub materialnej); z naruszenia rozporządzenia nie wynika automatycznie szkoda, która jest przez to naruszenie „spowodowana", lub, dokładniej rzecz ujmując, naruszenie danych osobowych „może skutkować" powstaniem uszczerbku fizycznego, szkód majątkowych lub niemajątkowych u osób fizycznych; pojęcie szkody należy interpretować „szeroko" w świetle orzecznictwa Trybunału, w sposób w pełni odzwierciedlający cele rozporządzenia; odszkodowanie za „poniesioną" szkodę powinno być „pełne i skuteczne".

72. Brzmienie przepisów rozporządzenia wyklucza wszelkie ewentualne sugestie dotyczące szkód in re ipsa: głównym celem odpowiedzialności cywilnej przewidzianej w rozporządzeniu jest zadośćuczynienie osobie, której dane dotyczą, właśnie poprzez „pełne i skuteczne" odszkodowanie za poniesioną przez nią szkodę, a zatem przywrócenie równowagi w sytuacji prawnej negatywnie zmienionej wskutek naruszenia prawa [28].

73. Z drugiej strony, również z systemowego punktu widzenia, podobnie jak w prawie ochrony konkurencji rozporządzenie przewiduje dwa filary ochrony: jeden o charakterze publicznoprawnym, obejmujący sankcje w przypadku naruszenia przepisów rozporządzenia, i jeden o charakterze prywatnoprawnym, obejmujący właśnie odpowiedzialność cywilną o charakterze deliktowym, którą można uznać za zaostrzoną z powodu domniemanej winy o wspomnianych powyżej cechach, również w odniesieniu do dowodu zwalniającego z odpowiedzialności [29].

74. W związku z tym rozszerzająca [30] wykładnia pojęcia szkody (niemajątkowej) nie może prowadzić do uznania, że prawodawca zrezygnował z wymogu wystąpienia rzeczywistej „szkody".

75. Rzeczywista kwestia merytoryczna dotyczy tego, czy po stwierdzeniu istnienia naruszenia i związku przyczynowego prawo do odszkodowania może powstać jedynie z powodu obaw, niepokojów i lęków odczuwanych przez osobę, której dane dotyczą, dotyczących ewentualnego nieuczciwego wykorzystania danych osobowych w przyszłości, w przypadku gdy takie nieuczciwe wykorzystanie nie zostało stwierdzone lub osoba, której dane dotyczą, nie poniosła żadnej innej szkody.

[28] Zobacz ww. opinia rzecznika generalnego M. Camposa Sáncheza-Bordony, pkt 29 i przypis 11. W tej samej opinii rzecznik generalny słusznie kończy swoją analizę z literalnego, historycznego, kontekstowego i celowościowego punktu widzenia wykluczeniem „karnego" charakteru szkód podlegających naprawieniu na rzecz osób, których dane dotyczą, na podstawie art. 82 (pkt 27–55), zauważając, po pierwsze, że państwa członkowskie „nie muszą (i w rzeczywistości nie mogą) wybierać spośród mechanizmów przewidzianych w rozdziale VIII w celu zapewnienia ochrony danych. W przypadku naruszenia, które nie powoduje szkody, osoba, której dane dotyczą, jest jeszcze (co najmniej) uprawniona do wniesienia skargi do organu nadzorczego", a po drugie, że „perspektywa uzyskania odszkodowania bez względu na jakąkolwiek szkodę prawdopodobnie przyczyniłaby się do sporów cywilnych i pozwów, które nie zawsze mogą być uzasadnione, i w tym zakresie mogłaby zniechęcić do działalności polegającej na przetwarzaniu danych" (pkt 54, 55).

[29] Odmówienie prawa do odszkodowania za słabe i przejściowe odczucia czy emocje związane z naruszeniem przepisów dotyczących przetwarzania danych nie pozostawiałoby osoby, której dane dotyczą, całkowicie pozbawionej ochrony (zob. podobnie ww. opinia rzecznika generalnego M. Camposa Sáncheza-Bordony, pkt 115).

[30] Lub „szeroka" zgodnie ze sformułowaniem użytym w motywie 146.

76. Zgodnie z utrwalonym orzecznictwem Trybunału pojęciom w danym przepisie prawa Unii, który nie zawiera żadnego wyraźnego odesłania do prawa państw członkowskich w celu określenia ich znaczenia i zakresu, należy zazwyczaj nadawać w całej Unii autonomiczną i jednolitą wykładnię, której należy dokonywać z uwzględnieniem nie tylko treści tego przepisu, ale także jego kontekstu i celów realizowanych przez uregulowanie, którego stanowi on część, oraz genezy tego przepisu [31].

77. Jak przypomniał rzecznik generalny M. Campos Sánchez-Bordona [32], Trybunał nie opracował ogólnej definicji „szkody", która mogłaby być stosowana bez rozróżnienia w każdej dziedzinie [33]. W odniesieniu do szkód niemajątkowych z orzecznictwa Trybunału można wywnioskować, że w przypadku gdy jednym z celów przepisu, którego wykładni się dokonuje, jest ochrona jednostki lub pewnej kategorii jednostek [34], pojęcie szkody musi być szerokie; zgodnie z tym kryterium odszkodowanie rozciąga się na szkodę niemajątkową, nawet jeśli nie jest ona wymieniona w przepisie, którego wykładni się dokonuje [35].

78. Chociaż orzecznictwo Trybunału pozwala bronić stanowiska, że w przedstawionych powyżej warunkach w prawie Unii istnieje zasada odszkodowania za szkody niemajątkowe, zgadzam się z rzecznikiem generalnym M. Camposem Sánchezem-Bordoną, że nie można z niego wywieść zasady, zgodnie z którą *każda* szkoda niemajątkowa, niezależnie od jej wagi, podlega odszkodowaniu [36].

79. W tym kontekście istotne jest rozróżnienie między szkodami niemajątkowymi podlegającymi naprawieniu a innymi *niedogodnościami wynikającymi z nieprzestrzegania prawa*, które ze względu na swój niewielki rozmiar niekoniecznie rodziłyby prawo do odszkodowania [37].

[31] Zobacz wyroki: z dnia 15 kwietnia 2021 r., The North of England P & I Association (C-786/19, EU:C:2021:276, pkt 48); z dnia 10 czerwca 2021 r., KRONE – Verlag (C-65/20, EU:C:2021:471, pkt 25).

[32] Zobacz ww. opinia rzecznika generalnego M. Camposa Sáncheza-Bordony, pkt 104.

[33] Trybunał nie wskazał również preferowanej metody wykładni – autonomicznej lub poprzez odniesienie do krajowych porządków prawnych: zależy to od dziedziny będącej przedmiotem badania. Porównaj wyroki: z dnia 10 maja 2001 r., Veedfald (C-203/99, EU:C:2001:258, pkt 27) – w dziedzinie produktów wadliwych; z dnia 6 maja 2010 r., Walz (C-63/09, EU:C:2010:251, pkt 21), dotyczący odpowiedzialności przewoźników lotniczych; z dnia 10 czerwca 2021 r., Van Ameyde España (C-923/19, EU:C:2021:475, pkt 37 i nast.) – w odniesieniu do odpowiedzialności cywilnej za szkody powstałe w związku z ruchem pojazdów mechanicznych.

[34] Na przykład konsumentów produktów lub osób poszkodowanych w wypadkach drogowych.

[35] W dziedzinie imprez turystycznych – zob. wyrok z dnia 12 marca 2002 r., Leitner (C-168/00, EU:C:2002:163); w dziedzinie odpowiedzialności cywilnej za szkody powstałe w związku z ruchem pojazdów mechanicznych – wyroki: z dnia 24 października 2013 r., Haasová (C-22/12, EU:C:2013:692, pkt 47–50); z dnia 24 października 2013 r., Drozdovs (C-277/12, EU:C:2013:685, pkt 40); z dnia 23 stycznia 2014 r., Petillo (C-371/12, EU:C:2014:26, pkt 35).

[36] Zobacz ww. opinia rzecznika generalnego M. Camposa Sáncheza-Bordony, pkt 105. Trybunał uznał na przykład, że przepis krajowy, który dla celów obliczenia wysokości odszkodowania rozróżnia szkody niemajątkowe związane z obrażeniami ciała w wyniku wypadku w zależności od ich źródła, jest zgodny z przepisami prawa Unii; zob. wyrok z dnia 23 stycznia 2014 r., Petillo (C-371/12, EU:C:2014:26), sentencja: prawo Unii nie stoi na przeszkodzie „ustawodawstwu krajowemu […], które przewiduje szczególny system zadośćuczynienia za szkody niemajątkowe powstałe w wyniku lekkich obrażeń cielesnych spowodowanych wypadkami drogowymi ograniczający zadośćuczynienie za wspomniane szkody niemajątkowe w stosunku do tego, co jest przyjęte w dziedzinie zadośćuczynień za identyczne szkody wynikłe z przyczyn innych niż wspomniane wypadki".

[37] Rozróżnienie to jest postrzegane w niektórych krajowych porządkach prawnych jako nieuniknione następstwo życia w społeczeństwie. Zobacz w dziedzinie ochrony danych, we Włoszech, niedawny wyrok Tribunale di Palermo, sez. I civile (sądu w Palermo, pierwsza izba cywilna, Włochy) nr 5261 z dnia 5 października 2017 r., a także orzeczenie Cass. Civ., Ord. sez. VI (sądu kasacyjnego, szósta izba cywilna, Włochy) nr 17383/2020. W Niemczech między innymi AG Diez, 07.11.2018-8 C 130/18; LG Karlsruhe, 02.08.2019-8 O 26/19; AG Frankfurt am Main, 10.07.2020-385 C 155/19 (70). W Austrii – OGH 6 Ob. 56/21k.

80. Trybunał uznaje tę różnicę, gdy odnosi się do trudności i niedogodności jako autonomicznej kategorii w stosunku do kategorii szkód w dziedzinach, w odniesieniu do których uważa, że powinny one zostać naprawione [38].

81. Z punktu widzenia empirycznego można zauważyć, że każde naruszenie przepisu dotyczącego ochrony danych osobowych wywołuje jakąś negatywną reakcję osoby, której dane dotyczą. Odszkodowanie wynikające z samego poczucia niezadowolenia z powodu braku poszanowania prawa przez inną osobę można łatwo pomylić z odszkodowaniem bez szkody, które, jak już wspomniałem, nie wydaje się mieć miejsca w przypadku, o którym mowa w art. 82 rozporządzenia.

82. Fakt, że w okolicznościach takich jak w postępowaniu głównym nieuczciwe wykorzystanie danych osobowych jest jedynie potencjalne, a nie rzeczywiste, jest wystarczający, aby uznać, że osoba, której dane dotyczą, mogła ponieść szkodę niemajątkową spowodowaną naruszeniem rozporządzenia, pod warunkiem że osoba ta wykaże, że obawa przed takim nieuczciwym wykorzystaniem rzeczywiście i konkretnie wyrządziła jej rzeczywistą i pewną szkodę emocjonalną [39].

83. Granica między zwykłymi niedogodnościami (niepodlegającymi odszkodowaniu) a rzeczywistymi szkodami niemajątkowymi (podlegającymi odszkodowaniu) jest niewątpliwie subtelna, ale sądy krajowe, których zadaniem jest wyznaczenie tej granicy w każdym przypadku z osobna, powinny dokonać dokładnej oceny wszystkich dowodów przedstawionych przez wnoszącą roszczenie odszkodowawcze osobę, której dane dotyczą, na której będzie spoczywał ciężar przedstawienia w sposób dokładny, a nie ogólny, konkretnych dowodów, które mogą świadczyć o „rzeczywiście poniesionej szkodzie niemajątkowej" z powodu naruszenia danych osobowych, nawet jeśli szkoda ta nie osiągnie z góry określonego progu szczególnej wagi: istotne jest to, że nie chodzi tu o zwykłe subiektywne odczucie, które jest zmienne i zależne również od cech charakteru i elementów osobistych, lecz o obiektywizm trudności, choćby niewielkich, lecz możliwych do wykazania, dla czyjejś sfery fizycznej lub psychicznej lub dla życia rodzinnego, charakter odnośnych danych osobowych i znaczenie, jakie mają one w życiu osoby, której dane dotyczą, oraz być może również postrzeganie przez społeczeństwo w danym momencie tych konkretnych trudności związanych z naruszeniem danych [40].

[38] Zobacz wyrok z dnia 23 października 2012 r., Nelson i in. (C-581/10 i C-629/10, EU:C:2012:657, pkt 51), dotyczący rozróżnienia między „szkodą" w rozumieniu art. 19 Konwencji o ujednoliceniu niektórych zasad dotyczących międzynarodowego przewozu lotniczego, zawartej w Montrealu w dniu 28 maja 1999 r., a „niedogodnościami" w rozumieniu rozporządzenia nr 261/2004, które podlegają odszkodowaniu na podstawie art. 7 tego rozporządzenia zgodnie z wyrokiem z dnia 19 listopada 2009 r., Sturgeon i in. (C-402/07 i C-432/07, EU:C:2009:716). W tym sektorze, podobnie jak w sektorze przewozu pasażerskiego drogą morską i drogą wodną śródlądową objętym rozporządzeniem nr 1177/2010, prawodawca mógł uznać kategorię abstrakcyjną dzięki temu, że czynnik powodujący trudności, jak i istota trudności są identyczne dla wszystkich poszkodowanych. Nie uważam, aby takie wnioskowanie było możliwe w dziedzinie ochrony danych.

[39] Zdaniem Irlandii względy te są w praktyce szczególnie ważne w kontekście cyberprzestępczości, ponieważ gdyby każda osoba dotknięta – nawet w minimalnym stopniu – naruszeniem była uprawniona do odszkodowania za szkody niemajątkowe, miałoby to silny wpływ w szczególności na administratorów danych sektora publicznego, którzy są finansowani z ograniczonych środków publicznych i powinni raczej służyć interesom zbiorowym, w tym poprawie bezpieczeństwa danych osobowych (uwagi na piśmie, pkt 72).

[40] Zobacz ww. opinia rzecznika generalnego M. Camposa Sáncheza-Bordony, pkt 116.

IV. Wnioski

84. Na podstawie wszystkich powyższych rozważań proponuję, aby na pytania prejudycjalne Trybunał udzielił następujących odpowiedzi:

Artykuły 5, 24, 32 i 82 rozporządzenia 2016/679 należy interpretować w ten sposób, że:

samo istnienie »naruszenia ochrony danych osobowych«, zgodnie z jego definicją zawartą w art. 4 pkt 12, nie jest samo w sobie wystarczające do stwierdzenia, że wdrożone przez administratora środki techniczne i organizacyjne nie były »odpowiednie« w celu zapewnienia ochrony rozpatrywanych danych;

oceniając, czy wdrożone przez administratora danych osobowych środki techniczne i organizacyjne są odpowiednie, sąd krajowy rozpatrujący sprawę musi przeprowadzić kontrolę, która obejmuje konkretną analizę zarówno treści tych środków, jak i sposobu ich wdrożenia oraz ich praktycznych skutków;

w ramach powództwa o odszkodowanie na podstawie art. 82 RODO na administratorze danych osobowych spoczywa ciężar udowodnienia, że środki, które wdrożył on na podstawie art. 32 tego rozporządzenia, są odpowiednie;

zgodnie z zasadą autonomii proceduralnej do wewnętrznego porządku prawnego każdego państwa członkowskiego należy określenie dopuszczalnych metod dowodowych i ich mocy dowodowej, w tym środków dowodowych, jakie sądy krajowe mogą lub muszą zarządzić w celu dokonania oceny, czy administrator danych osobowych wdrożył odpowiednie środki w rozumieniu tego rozporządzenia, z poszanowaniem zasad równoważności i skuteczności ustanowionych w prawie Unii;

okoliczność, że naruszenie tego rozporządzenia, które spowodowało daną szkodę, zostało popełnione przez osobę trzecią, nie stanowi sama w sobie podstawy zwolnienia administratora z odpowiedzialności, a w celu skorzystania ze zwolnienia przewidzianego w tym przepisie administrator musi udowodnić, że nie ponosi w żaden sposób winy za naruszenie;

szkoda polegająca na obawie przed potencjalnym nieuczciwym wykorzystaniem w przyszłości jej danych osobowych, której istnienie wykazała osoba, której dane dotyczą, może stanowić szkodę niemajątkową uprawniającą do odszkodowania, pod warunkiem że osoba, której dane dotyczą, wykaże, że poniosła indywidualnie rzeczywistą i pewną szkodę emocjonalną, czego ustalenie należy do sądu krajowego rozpatrującego sprawę w każdym konkretnym przypadku.