Jurisprudentie

CONCLUSIE VAN ADVOCAAT-GENERAAL
G. PITRUZZELLA
van 27 april 2023[1]

Zaak C-340/21

VB
tegen
Natsionalna agentsia za prihodite

[verzoek van de Varhoven administrativen sad (Bulgarije) om een prejudiciële beslissing]

„Prejudiciële verwijzing – Bescherming van persoonsgegevens – Verordening (EU) 2016/679 – Verantwoordelijkheid van de verwerkingsverantwoordelijke – Beveiliging van de verwerking – Inbreuk op de beveiliging van de verwerking van persoonsgegevens – Immateriële schade die is geleden als gevolg van nalatigheid van de verwerkingsverantwoordelijke – Vordering tot schadevergoeding”

Kan de onrechtmatige verspreiding, als gevolg van een hackaanval, van persoonsgegevens die in het bezit zijn van een overheidsinstantie, aanleiding geven tot vergoeding van immateriële schade aan degene op wie de gegevens betrekking hebben alleen omdat hij vreest dat zijn gegevens in de toekomst eventueel worden misbruikt? Op basis van welke criteria kan de verwerkingsverantwoordelijke aansprakelijk worden gehouden? Hoe is de bewijslast verdeeld in de procedure? Wat is de omvang van de rechterlijke toetsing?

I. Toepasselijke bepalingen

1. Artikel 4 van verordening 2016/679[2] (hierna: „AVG”), met als opschrift „Definities”, luidt als volgt:

„Voor de toepassing van deze verordening wordt verstaan onder:

[…]

12) ‚inbreuk in verband met persoonsgegevens’: een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens;

[1] Oorspronkelijke taal: Italiaans.

[2] Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van richtlijn 95/46/EG (algemene verordening gegevensbescherming).

[…]”

2. Artikel 5, met als opschrift „Beginselen inzake verwerking van persoonsgegevens”, bepaalt het volgende:

„1. Persoonsgegevens moeten:

[…]

f) door het nemen van passende technische of organisatorische maatregelen op een dusdanige manier worden verwerkt dat een passende beveiliging ervan gewaarborgd is, en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging (‚integriteit en vertrouwelijkheid’).

2. De verwerkingsverantwoordelijke is verantwoordelijk voor de naleving van lid 1 en kan deze aantonen (‚verantwoordingsplicht’).”

3. Artikel 24 van deze verordening, „Verantwoordelijkheid van de verwerkingsverantwoordelijke”, luidt als volgt:

„1. Rekening houdend met de aard, de omvang, de context en het doel van de verwerking, alsook met de qua waarschijnlijkheid en ernst uiteenlopende risico’s voor de rechten en vrijheden van natuurlijke personen, treft de verwerkingsverantwoordelijke passende technische en organisatorische maatregelen om te waarborgen en te kunnen aantonen dat de verwerking in overeenstemming met deze verordening wordt uitgevoerd. Die maatregelen worden geëvalueerd en indien nodig geactualiseerd.

2. Wanneer zulks in verhouding staat tot de verwerkingsactiviteiten, omvatten de in lid 1 bedoelde maatregelen een passend gegevensbeschermingsbeleid dat door de verwerkingsverantwoordelijke wordt uitgevoerd.

3. Het aansluiten bij goedgekeurde gedragscodes als bedoeld in artikel 40 of goedgekeurde certificeringsmechanismen als bedoeld in artikel 42 kan worden gebruikt als element om aan te tonen dat de verplichtingen van de verwerkingsverantwoordelijke zijn nagekomen.”

4. Artikel 32, „Beveiliging van de verwerking”, luidt als volgt:

„1. Rekening houdend met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico’s voor de rechten en vrijheden van personen, treffen de verwerkingsverantwoordelijke en de verwerker passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen, die, waar passend, onder meer het volgende omvatten:

[…]

2. Bij de beoordeling van het passende beveiligingsniveau wordt met name rekening gehouden met de verwerkingsrisico’s, vooral als gevolg van de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens, hetzij per ongeluk hetzij onrechtmatig.

3. Het aansluiten bij een goedgekeurde gedragscode als bedoeld in artikel 40 of een goedgekeurd certificeringsmechanisme als bedoeld in artikel 42 kan worden gebruikt als element om aan te tonen dat de in lid 1 van dit artikel bedoelde vereisten worden nageleefd.

[…]"

5. Artikel 82 van deze verordening, „Recht op schadevergoeding en aansprakelijkheid", bepaalt het volgende:

„1. Eenieder die materiële of immateriële schade heeft geleden ten gevolge van een inbreuk op deze verordening, heeft het recht om van de verwerkingsverantwoordelijke of de verwerker schadevergoeding te ontvangen voor de geleden schade.

2. Elke verwerkingsverantwoordelijke die bij verwerking is betrokken, is aansprakelijk voor de schade die wordt veroorzaakt door verwerking die inbreuk maakt op deze verordening. […].

3. Een verwerkingsverantwoordelijke of verwerker wordt van aansprakelijkheid op grond van lid 2 vrijgesteld indien hij bewijst dat hij op geen enkele wijze verantwoordelijk is voor het schadeveroorzakende feit."

II. Feiten, procedure en prejudiciële vragen

6. Op 15 juli 2019 maakten Bulgaarse media bekend dat ongeoorloofde toegang tot het informatiesysteem van de Natsionalna agentsia za prihodite (nationale belastingdienst; hierna: „NAP")[3] was verkregen en dat diverse fiscale gegevens en socialezekerheidsgegevens van miljoenen mensen, zowel Bulgaarse als buitenlandse staatsburgers, op internet waren geplaatst.

7. Talrijke personen, onder wie VB, verzoekster in het hoofdgeding, hebben de NAP vervolgens gedagvaard om een vergoeding voor immateriële schade te verkrijgen.

8. In het onderhavige geval heeft verzoekster in het hoofdgeding zich gewend tot de Administrativen sad Sofia-grad (bestuursrechter in eerste aanleg van de stad Sofia, Bulgarije; hierna: „ASSG") en aangevoerd dat de NAP de nationale regels had geschonden evenals de verplichting om als verwerkingsverantwoordelijke persoonsgegevens zodanig te verwerken dat door het treffen van passende technische en organisatorische maatregelen in de zin van de artikelen 24 en 32 van verordening 679/2016 „een passend veiligheidsniveau gegarandeerd" is. Voorts heeft verzoekster gesteld dat zij immateriële schade heeft geleden, aangezien zij zich zorgen maakt over en vreest voor misbruik van haar persoonsgegevens in de toekomst.

9. De wederpartij heeft daarentegen benadrukt dat verzoekster in het hoofdgeding niet heeft verzocht om aan te geven tot welke persoonsgegevens precies toegang was verkregen, en heeft voorts naar aanleiding van de inbraakmelding bijeenkomsten met deskundigen belegd ter bescherming van de rechten en belangen van de burgers. Volgens de NAP was er ook geen

[3] De NAP is verwerkingsverantwoordelijke in de zin van artikel 4, punt 7, AVG. Naar nationaal recht is de NAP een bestuurslichaam met specifieke bevoegdheden onder het gezag van de minister van Financiën en belast met het vaststellen, veiligstellen en invorderen van openbare gelden en met het vaststellen, veiligstellen en invorderen van wettelijk vastgestelde openbare en particuliere overheidsvorderingen. In het kader van de uitoefening van de aan hem verleende openbare bevoegdheden verwerkt de NAP persoonsgegevens.

causaal verband tussen de cyberaanval en de beweerde schade aangezien de NAP in overeenstemming met de geldende internationale normen op dat gebied alle procesbeheer- en managementsystemen voor informatiebeveiliging had geïmplementeerd.

10. De rechter in eerste aanleg, de ASSG, heeft het verzoek afgewezen daar hij van oordeel was dat de NAP niet verantwoordelijk was voor de verspreiding van de gegevens, dat de bewijslast ten aanzien van de vraag of de getroffen maatregelen passend waren op verzoekster rustte en tot slot dat er geen immateriële schade voor vergoeding in aanmerking kwam.

11. De uitspraak in eerste aanleg is vervolgens aangevochten bij de Varhoven administrativen sad (hoogste bestuursrechter, Bulgarije). Verzoekster in het hoofdgeding heeft onder andere opgemerkt dat de rechter in eerste aanleg de last om te bewijzen dat er geen beveiligingsmaatregelen waren getroffen, niet correct had verdeeld. De bewijslast moest volgens haar ook niet gelden voor de immateriële schade, aangezien het gaat om daadwerkelijke en niet om louter potentiële immateriële schade.

12. De NAP stelde daarentegen dat hij als verwerkingsverantwoordelijke de noodzakelijke technische en organisatorische maatregelen had getroffen en betwistte dat er bewijs was voor daadwerkelijke immateriële schade. Ongerustheid en vrees zijn immers emotionele toestanden die niet in aanmerking komen voor vergoeding.

13. De verwijzende rechter heeft vastgesteld dat de procedures die benadeelden afzonderlijk tegen de NAP hadden aangespannen ter vergoeding van immateriële schade tot uiteenlopende uitkomsten hadden geleid.

14. In deze omstandigheden heeft de verwijzende rechter de behandeling van de zaak geschorst en het Hof de volgende prejudiciële vragen gesteld:

„1) Moeten de artikelen 24 en 32 van verordening (EU) 2016/679 [van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van richtlijn 95/46/EG (algemene verordening gegevensbescherming)] aldus worden uitgelegd dat het feit dat de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot persoonsgegevens in de zin van artikel 4, punt 12, van verordening (EU) 2016/679 heeft plaatsgevonden door personen die geen medewerkers van de verwerkingsverantwoordelijke zijn en niet onder zijn toezicht staan, volstaat om aan te nemen dat de getroffen technische en organisatorische maatregelen niet passend zijn?

2) Ingeval de eerste vraag ontkennend wordt beantwoord: waarop moet de rechterlijke toetsing van de rechtmatigheid bij het onderzoek van de vraag of de door de verwerkingsverantwoordelijke getroffen technische en organisatorische maatregelen passend zijn in de zin van artikel 32 van verordening (EU) 2016/679 betrekking hebben en welke omvang moet die toetsing hebben?

3) Ingeval de eerste vraag ontkennend wordt beantwoord: moet het beginsel van de verantwoordingsplicht op grond van artikel 5, lid 2, en artikel 24 juncto overweging 74 van verordening (EU) 2016/679 aldus worden uitgelegd dat in het kader van een beroep op grond van artikel 82, lid 1, van die verordening de bewijslast voor het feit dat de getroffen technische en organisatorische maatregelen passend zijn in de zin van artikel 32 van de verordening, op de verwerkingsverantwoordelijke rust? Kan een deskundigenrapport als een noodzakelijk en

toereikend bewijsmiddel worden beschouwd om vast te stellen dat de door de verwerkingsverantwoordelijke getroffen technische en organisatorische maatregelen in een geval zoals het onderhavige passend waren, wanneer de ongeoorloofde toegang tot en de ongeoorloofde verstrekking van persoonsgegevens het gevolg zijn van een ‚hackaanval'?

4) Moet artikel 82, lid 3, van verordening (EU) 2016/679 aldus worden uitgelegd dat de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot persoonsgegevens in de zin van artikel 4, punt 12, van die verordening, in casu door middel van een ‚hackaanval' door personen die geen medewerkers van de verwerkingsverantwoordelijke zijn en niet onder zijn toezicht staan, een feit is waarvoor de verwerkingsverantwoordelijke niet verantwoordelijk is en dat bijgevolg een vrijstelling van aansprakelijkheid rechtvaardigt?

5) Moet artikel 82, leden 1 en 2, junctis de overwegingen 85 en 146 van verordening (EU) 2016/679 aldus worden uitgelegd dat wanneer er zoals in casu sprake is van een inbreuk op persoonsgegevens die bestaat in de ongeoorloofde toegang tot en de verspreiding van persoonsgegevens door middel van een ‚hackaanval', alleen al de bezorgdheid en ongerustheid van de betrokkene over en zijn vrees voor mogelijk misbruik van zijn persoonsgegevens in de toekomst, zonder dat een dergelijk misbruik is vastgesteld en/of de betrokkene verdere schade heeft geleden, onder het ruim uit te leggen begrip ‚immateriële schade' vallen en een recht op schadevergoeding doen ontstaan?"

III. Juridische analyse

A. Opmerkingen vooraf

15. De onderhavige zaak heeft betrekking op interessante en deels nieuwe vragen over de uitlegging van verschillende bepalingen van de AVG. [4]

16. Alle vijf de prejudiciële vragen draaien om dezelfde kwestie: de voorwaarden waaronder de immateriële schade kan worden vergoed aan een persoon wiens persoonsgegevens die in het bezit zijn van een overheidsinstantie, na een hackaanval zijn gepubliceerd op internet.

17. Gemakshalve zal ik bondige en afzonderlijke antwoorden voorstellen voor alle prejudiciële vragen in de verwijzingsbeslissing. Ik ben mij evenwel bewust van een zekere conceptuele overlapping, aangezien de eerste vier vragen alle betrekking hebben op de voorwaarden

[4] Artikel 5, lid 2 (over het beginsel van de verantwoordingsplicht van elke verwerkingsverantwoordelijke van persoonsgegevens), artikel 24 (over de maatregelen die deze verwerkingsverantwoordelijke moet treffen om te waarborgen dat de verwerking door hem in overeenstemming met deze verordening wordt uitgevoerd), artikel 32 (over die verplichting in het bijzonder wat de beveiliging van de verwerking betreft) en artikel 82, leden 1 tot en met 3 (over de vergoeding van schade ten gevolge van een inbreuk op deze verordening en de mogelijkheid voor de verwerkingsverantwoordelijke om maatregelen te treffen om de naleving van deze verordening te waarborgen), evenals de overwegingen 74, 85 en 146 die betrekking hebben op bovengenoemde artikelen.

waaronder de verwerkingsverantwoordelijke verantwoordelijk kan worden gehouden voor de inbreuk op de bepalingen van de AVG[5] en de vijfde vraag meer in het bijzonder gaat over het begrip „immateriële schade" in het kader van schadevergoeding.[6]

18. Ik merk op dat thans verschillende zaken over artikel 82 AVG bij het Hof aanhangig zijn en dat in een van die zaken de conclusie van de advocaat-generaal reeds beschikbaar is. Bij deze analyse zal ik hiermee rekening houden.[7]

19. Alvorens op de gestelde vragen in te gaan, acht ik het zinvol vooraf enige opmerkingen over de beginselen en doelstellingen van de AVG te maken die nuttig zijn voor de beantwoording van de afzonderlijke prejudiciële vragen.

20. In artikel 24 AVG is in algemene bewoordingen bepaald dat de verwerkingsverantwoordelijke verplicht is om passende technische en organisatorische maatregelen te treffen om te waarborgen dat de verwerking van persoonsgegevens in overeenstemming met de verordening wordt uitgevoerd en dat hij dit moet kunnen aantonen, terwijl in artikel 32 diezelfde verplichting is opgenomen meer bepaald wat betreft de beveiliging van de verwerking. In de artikelen 24 en 32 is hetgeen in artikel 5, lid 2, reeds is bepaald verder uitgewerkt. In laatstgenoemde bepaling is als een van de „beginselen inzake verwerking van persoonsgegevens" het „beginsel van de verantwoordingsplicht" opgenomen. Dit beginsel is een logisch uitvloeisel van en vormt een aanvulling op het „beginsel van integriteit en vertrouwelijkheid" van artikel 5, lid 1, onder f), en beide beginselen moeten worden gelezen in het licht van de risicobenadering waarop de AVG is gebaseerd.

21. Het beginsel van de verantwoordingsplicht is een van de pijlers van de AVG en een van de belangrijkste vernieuwingen ervan. Volgens dit beginsel is de verwerkingsverantwoordelijke ervoor verantwoordelijk dat hij proactieve stappen neemt om te waarborgen dat de AVG wordt nageleefd en dat hij kan aantonen dat hij dat heeft gedaan.[8]

22. In de rechtsleer is er gesproken van een reële culturele omslag als gevolg van „de algehele omvang van de verantwoordingsplicht".[9] Het is niet zozeer de formele naleving van een wettelijke verplichting of van een individuele maatregel als wel de algehele bedrijfsstrategie om de verwerkingsverantwoordelijke vrij te stellen van aansprakelijkheid omdat hij voldoet aan de regelgeving inzake gegevensbescherming.

[5] a) Met de eerste vraag moet worden beantwoord of louter vanwege een inbreuk op de systemen kan worden aangevoerd dat de getroffen maatregelen niet passend zijn; b) de tweede vraag gaat over de uitbreiding van de rechterlijke toetsing naar de vraag of de genoemde maatregelen passend zijn; c) de derde vraag heeft betrekking op de bewijslast voor het feit dat de maatregelen passend zijn en op enkele technische methoden voor het onderzoek van het bewijs; d) de vierde vraag gaat, met het oog op de vrijstelling van aansprakelijkheid, over de relevantie van het feit dat het systeem van buitenaf werd aangevallen.

[6] Wat de aangehaalde bepalingen van de AVG betreft, hebben de eerste drie vragen betrekking op de verantwoordelijkheid van de verwerkingsverantwoordelijke ten opzichte van de te treffen passende maatregelen (artikelen 5, 24 en 32); de vierde en de vijfde vraag hebben betrekking op de voorwaarden voor vrijstelling van aansprakelijkheid en op het begrip immateriële schade die voor vergoeding in aanmerking komt (artikel 82).

[7] Zie de conclusie van advocaat-generaal Campos Sánchez-Bordona in de zaak Österreichische Post (Immateriële schade als gevolg van de verwerking van persoonsgegevens) (C-300/21, EU:C:2022:756).

[8] Docksey C., „Article 24. Responsibility of the controller", Kuner C., Bygrave L.A., Docksey C., Drechsler L., *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford University Press, 2020, blz. 561. De beginselen en verplichtingen in de regelgeving inzake gegevensbescherming zouden moeten doordringen in de cultuur van organisaties op alle niveaus en niet worden gezien als een reeks wettelijke eisen die door een afdeling juridische zaken moeten worden afgevinkt.

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

23. De technische en organisatorische maatregelen die op grond van het beginsel van de verantwoordingsplicht vereist zijn, moeten „passend" zijn gelet op de in artikel 24 genoemde factoren: de aard, de omvang, de context en het doel van de verwerking, evenals de waarschijnlijkheid en ernst van de risico's voor de rechten en vrijheden van natuurlijke personen.

24. In artikel 24 is dus bepaald dat de maatregelen passend moeten zijn om te kunnen aantonen dat de verwerking in overeenstemming met de beginselen en bepalingen van de AVG wordt uitgevoerd.

25. In artikel 32 daarentegen is het beginsel van de verantwoordingsplicht gericht op de concrete maatregelen die moeten worden getroffen om „een op het risico afgestemd beveiligingsniveau" te waarborgen. En daarbij zijn de stand van de techniek en de uitvoeringskosten toegevoegd aan de reeds genoemde factoren waarmee rekening moet worden gehouden bij het opstellen van de technische en organisatorische maatregelen.

26. Het begrip „passend" vereist dat de oplossingen voor de beveiliging van informatiesystemen een bepaald niveau van aanvaardbaarheid hebben, zowel in technisch opzicht (relevantie van de maatregelen) als in kwalitatief opzicht (doeltreffendheid van de bescherming). Een verwerking moet, om te waarborgen dat de beginselen van noodzakelijkheid, relevantie en evenredigheid worden nageleefd, niet alleen geschikt zijn, maar ook beantwoorden aan de beoogde doelen. En volgens deze logica is een beslissende rol weggelegd voor het beginsel van minimale gegevensverwerking op grond waarvan in alle fasen van gegevensverwerking voortdurend moet worden gestreefd naar zo min mogelijk beveiligingsrisico's. [10]

27. De AVG is geheel gericht op het voorkomen van risico's en op de verantwoordingsplicht van de verwerkingsverantwoordelijke en heeft derhalve een teleologische benadering die het best mogelijke resultaat qua doeltreffendheid nastreeft en dus verre blijft van een formalistische logica waarbij het louter gaat om de verplichting om te voldoen aan specifieke procedures teneinde niet aansprakelijk te worden gesteld. [11]

28. In artikel 24 is geen uitputtende opsomming van „passende" maatregelen opgenomen: een beoordeling van geval tot geval is noodzakelijk. Dit strookt met de filosofie van de AVG waaruit blijkt dat de te volgen procedures moeten worden gekozen op basis van een zorgvuldige beoordeling van de situatie in kwestie zodat zij zo doeltreffend mogelijk zijn. [12]

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

[11] Daarom kunnen de eerste en de vierde prejudiciële vraag, zoals ik hierna uiteen zal zetten, alleen maar ontkennend worden beantwoord. Uit de bepalingen van de AVG kan geen enkel automatisme worden afgeleid: het loutere feit dat persoonsgegevens zijn verstrekt, volstaat niet om aan te nemen dat de getroffen technische en organisatorische maatregelen niet passend waren, maar de omstandigheid dat die verstrekking heeft plaatsgevonden door toedoen van personen buiten de organisatie van de verwerkingsverantwoordelijke en buiten zijn toezicht volstaat evenmin om hem vrij te stellen van aansprakelijkheid.

[12] Bolognini L., Pelino E., *Codice della disciplina privacy*, Giuffrè, 2019, blz. 201. De Europese wetgever gaat dus verder dan de definitie van beveiliging van de verwerking die is gebaseerd op het bestaan van vooraf vastgestelde beveiligingsmaatregelen en hanteert een methode die kenmerkend is voor internationale normen inzake het beheer van *risk-based* informatiesystemen: maatregelen ter beperking van risico's worden vastgesteld waarbij vooraf opgestelde en breed toepasbare *checklists* buiten beschouwing worden gelaten. Het is dan ook noodzakelijk zich te baseren op internationale richtsnoeren en normen. Het resultaat van die risicobeoordeling wordt dus bindend wanneer de organisatie beslissingen neemt om de vastgestelde risico's te beperken en *accountable* is.

B. Eerste prejudiciële vraag

29. Met zijn eerste vraag wenst de verwijzende rechter in wezen te vernemen of de artikelen 24 en 32 AVG aldus moeten worden uitgelegd dat een „inbreuk in verband met persoonsgegevens", zoals gedefinieerd in artikel 4, punt 12, op zichzelf volstaat om te concluderen dat de door de verwerkingsverantwoordelijke genomen technische en organisatorische maatregelen niet „passend" waren om de bescherming van de gegevens te garanderen.

30. Uit de tekst van de artikelen 24 en 32 AVG blijkt dat de verwerkingsverantwoordelijke bij zijn keuze voor de technische en organisatorische maatregelen die hij moet treffen om te waarborgen dat de AVG wordt nageleefd, rekening moet houden met een reeks beoordelingsfactoren die in die artikelen zijn genoemd en hierboven zijn aangehaald.

31. De verwerkingsverantwoordelijke heeft een zekere vrijheid om te bepalen welke maatregelen in het licht van zijn specifieke situatie het meest geschikt zijn, maar die keuze kan niettemin worden onderworpen aan een rechterlijke toetsing of de gehanteerde maatregelen voldoen aan alle verplichtingen en doelstellingen van de AVG.

32. In artikel 32, lid 1, wordt in het bijzonder ten aanzien van de beveiligingsmaatregelen aan de verwerkingsverantwoordelijke de verplichting opgelegd om rekening te houden met de „stand van de techniek". Dit impliceert dat het technologische niveau van maatregelen die moeten worden getroffen, beperkt is tot hetgeen redelijkerwijs haalbaar is op het moment dat zij worden getroffen: de geschiktheid van de maatregel om risico's te voorkomen moet dan ook in verhouding staan tot de oplossingen die mogelijk zijn op basis van de huidige stand van de wetenschap, de techniek, de technologie en het onderzoek, mede gelet op, zoals hierna zal worden uiteengezet, de uitvoeringskosten.

33. Maatregelen kunnen op een bepaald moment „passend" zijn en desondanks worden omzeild door cybercriminelen die zeer geavanceerde middelen gebruiken waarmee ook inbreuk kan worden gemaakt op beveiligingsmaatregelen die in overeenstemming zijn met de stand van de techniek.

34. Het lijkt daarentegen niet logisch om aan te nemen dat de Uniewetgever de bedoeling had om de verwerkingsverantwoordelijke te verplichten om iedere inbreuk in verband met persoonsgegevens te voorkomen, los van de zorgvuldigheid bij het opstellen van beveiligingsmaatregelen. [13]

35. Zoals hierboven uiteengezet, is in de optiek van de AVG geen ruimte voor automatismen en heeft de verwerkingsverantwoordelijke een grote verantwoordingsplicht die er echter niet toe kan leiden dat het voor hem onmogelijk is om aan te tonen dat hij zijn verplichtingen naar behoren is nagekomen.

36. Voorts is in artikel 32, lid 1, bepaald dat rekening moet worden gehouden met, zoals gezegd, de „uitvoeringskosten" van de betreffende technische en organisatorische maatregelen. Hieruit volgt dat bij de beoordeling of die maatregelen passend zijn, een afweging moet worden gemaakt tussen de belangen van de betrokkene, die doorgaans gericht zijn op een hoger niveau van

[13] Het begrip „passend" toont ondubbelzinnig aan dat het niet de bedoeling was dat aan alle technische en organisatorische maatregelen die in theorie mogelijk zijn, belang werd gehecht. Zie in die zin Gambini M., „Responsabilità e risarcimento nel trattamento dei dati personali", Cuffaro V., D'Orazio R., Ricciuto V., *I dati personali nel diritto europeo*, Giappichelli, 2019, blz. 1059.

bescherming, en de economische belangen en technologische capaciteiten van de verwerkingsverantwoordelijke, die soms gericht zijn op een lager niveau van bescherming. Bij die afweging moet worden voldaan aan de vereisten van het algemene evenredigheidsbeginsel.

37. Hieraan moet nog worden toegevoegd dat de wetgever, volgens een systematische uitlegging, voorziet in de mogelijkheid dat zich inbreuken op de systemen voordoen; artikel 32, lid 1, onder c), noemt als een van de voorgestelde maatregelen het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen. Indien wordt aangenomen dat een inbreuk op de systemen op zichzelf al het bewijs vormt dat de maatregelen niet passend zijn, zou deze maatregel als een van de beveiligingsmaatregelen die een op het risico afgestemd beveiligingsniveau waarborgen, zinloos zijn.

C. Tweede prejudiciële vraag

38. Met de tweede vraag wenst de verwijzende rechter in wezen te vernemen waarop de rechterlijke toetsing betrekking moet hebben en welke omvang die toetsing moet hebben bij het onderzoek van de vraag of de door de verwerkingsverantwoordelijke getroffen technische en organisatorische maatregelen passend zijn in de zin van artikel 32 AVG.

39. Gelet op het feit dat zich in de praktijk verschillende situaties kunnen voordoen, zijn in de AVG, zoals gezegd, geen bindende bepalingen opgenomen voor de vaststelling van de technische en organisatorische maatregelen die de verwerkingsverantwoordelijke moet treffen om aan de vereisten van de AVG te voldoen. De vraag of de getroffen maatregelen passend zijn, moet derhalve in de praktijk worden beoordeeld door te toetsen of de maatregelen in kwestie geschikt zijn om het risico redelijkerwijs te voorkomen en om de negatieve gevolgen van de inbreuk tot een minimum te beperken.

40. Hoewel de keuze en de uitvoering van deze maatregelen aan de subjectieve beoordeling van de verwerkingsverantwoordelijke zijn overgelaten, aangezien de in de AVG genoemde maatregelen slechts voorbeelden zijn, kan het onderzoek door de rechter zich niet beperken tot de toetsing of de verwerkingsverantwoordelijke de verplichtingen van de artikelen 24 en 32 heeft nageleefd, dat wil zeggen of hij (formeel) bepaalde technische en organisatorische maatregelen heeft getroffen. Die rechter moet de inhoud van deze maatregelen, de wijze waarop zij zijn toegepast en de gevolgen ervan in de praktijk concreet analyseren op basis van het bewijs waarover hij beschikt en de omstandigheden van het specifieke geval. Zoals de Portugese regering terecht heeft opgemerkt, „lijkt de wijze waarop hij heeft voldaan aan zijn verplichtingen niet los te kunnen worden gezien van de inhoud van de getroffen maatregelen om aan te tonen – rekening houdend met de specifieke gegevensverwerking (de aard, de omvang, de context en de doeleinden), met de stand van de beschikbare technologieën en de kosten ervan, alsook met de risico's voor de rechten en vrijheden van burgers – dat de verwerkingsverantwoordelijke alle maatregelen heeft getroffen die noodzakelijk en passend zijn om een op het onderliggende risico afgestemd beveiligingsniveau te waarborgen". [14]

41. Bij de rechterlijke toetsing moet derhalve rekening worden gehouden met alle factoren die zijn genoemd in de artikelen 24 en 32 waarin, zoals gezegd, diverse criteria zijn opgesomd om te beoordelen of maatregelen passend zijn en waarin voorbeelden van maatregelen zijn gegeven die als passend kunnen worden beschouwd. Zoals is benadrukt door de Commissie en door alle lidstaten die opmerkingen bij de tweede vraag hebben ingediend, is voorts in artikel 32, leden 1

[14] Schriftelijke opmerkingen, punt 31.

tot en met 3, de nadruk gelegd op de noodzaak om „een op het risico afgestemd beveiligingsniveau te waarborgen" en zijn nog andere daartoe relevante factoren genoemd, zoals de vraag of de verwerkingsverantwoordelijke een goedgekeurde gedragscode of een goedgekeurd certificeringsmechanisme als bedoeld in respectievelijk artikel 40 en artikel 42 AVG heeft vastgesteld.

42. Een gedragscode of een certificeringsmechanisme kan een nuttig beoordelingselement zijn met het oog op de vervulling van de bewijslast en de rechterlijke toetsing in verband daarmee. Hierbij moet echter worden opgemerkt dat het niet volstaat dat de verwerkingsverantwoordelijke zich heeft aangesloten bij een gedragscode, maar dat hij moet kunnen bewijzen dat hij de betreffende maatregelen concreet heeft getroffen overeenkomstig het beginsel van de verantwoordingsplicht. Certificering daarentegen vormt „op zichzelf het bewijs dat de verwerking wordt uitgevoerd in overeenstemming met de verordening hoewel dit in de praktijk kan worden weerlegd". [15]

43. Tot slot moet worden opgemerkt dat deze maatregelen op grond van artikel 24, lid 1, moeten worden geëvalueerd en indien nodig geactualiseerd. En ook dit zal door de nationale rechter worden beoordeeld. Krachtens artikel 32, lid 1, AVG [16] rust op de verwerkingsverantwoordelijke immers de verplichting tot voortdurende toetsing en monitoring, zowel voor als na de verwerkingsactiviteiten, maar ook de verplichting tot het onderhouden en eventueel actualiseren van de getroffen maatregelen teneinde niet alleen inbreuken te voorkomen, maar ook eventuele gevolgen ervan te beperken.

44. Mijns inziens moet echter de mogelijkheid worden uitgesloten dat in het te geven arrest een opsomming van essentiële elementen wordt gegeven, zoals de door de Portugese regering voorgestelde opsomming. [17] Dit zou ruimte laten voor tegenstrijdige uitleggingen aangezien de opsomming uiteraard nooit volledig kan zijn.

[15] Gambini M., „Responsabilità", op. cit., blz. 1067. Certificering vertaalt zich derhalve in een omkering van de bewijslast ten gunste van de houder van het certificaat die daarmee kan aantonen dat hij heeft gehandeld met inachtneming van de verplichtingen van de AVG.

[16] Onder d) is uitdrukkelijk bepaald dat het oordeel over de vraag of de maatregelen passend zijn zich ook uitstrekt tot de doeltreffendheid van de getroffen maatregelen die op gezette tijden moet worden getest, beoordeeld en geëvalueerd, zowel in de beginfase als op periodieke basis, om te waarborgen dat alle soorten verwerkingen daadwerkelijk zijn beveiligd, ongeacht het risiconiveau daarvan. Voorts is onder c) nog expliciet bepaald dat de technische en organisatorische maatregelen het vermogen moeten omvatten om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen. Zie Gambini M., „Responsabilità", op. cit., blz. 1064-1065.

[17] Punt 30 van de schriftelijke opmerkingen: „het is aan de verwerkingsverantwoordelijke om aan te tonen hoe hij alle factoren en omstandigheden met betrekking tot de verwerking in kwestie heeft beoordeeld, in het bijzonder het resultaat van de uitgevoerde risicoanalyse, de vastgestelde risico's, de concrete maatregelen die zijn gevonden om die risico's te beperken, de rechtvaardiging opties die hij heeft gekozen in het licht van de op de markt beschikbare technologische mogelijkheden, de doeltreffendheid van de maatregelen, de correlatie tussen de technische en organisatorische maatregelen, de opleiding van het personeel dat de gegevens verwerkt, de eventuele uitbesteding van de gegevensverwerkingen, met inbegrip van de ontwikkeling en het onderhoud van de informatietechnologie, en het al dan niet bestaan van toezicht door de verwerkingsverantwoordelijke en van exacte instructies die worden gegeven aan degenen die belast zijn met de verwerking, in de zin van artikel 28 AVG, met betrekking tot de verwerking van persoonsgegevens door laatstgenoemden; de wijze waarop de ondersteunende infrastructuur voor de communicatie- en informatiesystemen is beoordeeld en waarop het risiconiveau is bepaald voor de rechten en vrijheden van de betrokkenen".

D. Derde prejudiciële vraag

45. Met het eerste onderdeel van zijn derde vraag wenst de verwijzende rechter in wezen van het Hof te vernemen of, gelet op het beginsel van de verantwoordingsplicht van artikel 5, lid 2, en van artikel 24 juncto overweging 74[18] AVG, in het kader van een vordering tot schadevergoeding in de zin van artikel 82, de bewijslast voor het feit dat de technische en organisatorische maatregelen passend zijn in de zin van artikel 32, op de verwerkingsverantwoordelijke rust.

46. Op basis van de bovenstaande argumenten kan ik deze vraag bevestigend en bondig beantwoorden.

47. De bewoordingen, de context en de doelstellingen van de AVG wijzen er immers ondubbelzinnig op dat de bewijslast berust bij de verwerkingsverantwoordelijke.

48. Uit de bewoordingen van verschillende bepalingen van de AVG blijkt dat de verwerkingsverantwoordelijke moet „kunnen aantonen" dat de verplichtingen uit de AVG zijn nageleefd en in het bijzonder dat hij daartoe passende maatregelen heeft getroffen, zoals is vermeld in overweging 74, in artikel 5, lid 2, en in artikel 24, lid 1. Zoals de Portugese regering heeft benadrukt, blijkt uit bovengenoemde overweging 74 dat de bewijslast die dus bij de verwerkingsverantwoordelijke is gelegd, zich ook moet uitstrekken tot de „doeltreffendheid van de maatregelen" in kwestie.

49. Mijns inziens vindt deze letterlijke uitlegging steun in de volgende praktische en teleologische overwegingen.

50. Wat betreft de verdeling van de bewijslast in het kader van een vordering tot schadevergoeding op grond van artikel 82, moet de betrokkene die de vordering heeft ingesteld tegen de verwerkingsverantwoordelijke ten eerste aantonen dat sprake is van een inbreuk op de verordening, ten tweede dat hij schade heeft geleden en ten derde dat er een causaal verband tussen beide voornoemde elementen bestaat, zoals in alle schriftelijke opmerkingen over de vijfde prejudiciële vraag naar voren is gebracht. Het gaat om drie cumulatieve voorwaarden, zoals tevens blijkt uit de vaste rechtspraak van het Hof en van het Gerecht in het kader van de niet-contractuele aansprakelijkheid van de Unie.[19]

51. Mijns inziens kan de verplichting van de verzoeker om aan te tonen dat er sprake is van een inbreuk op de AVG niet zover gaan dat van hem wordt geëist dat hij aantoont in welk opzicht de door de verwerkingsverantwoordelijke getroffen technische en organisatorische maatregelen niet passend zijn in de zin van de artikelen 24 en 32.

[18] Overweging 74 luidt als volgt: „De verantwoordelijkheid en aansprakelijkheid van de verwerkingsverantwoordelijke moeten worden vastgesteld voor elke verwerking van persoonsgegevens die door of namens hem wordt uitgevoerd. Meer bepaald dient de verwerkingsverantwoordelijke te worden verplicht passende en effectieve maatregelen uit te voeren en te kunnen aantonen dat elke verwerkingsactiviteit overeenkomstig deze verordening geschiedt, ook wat betreft de doeltreffendheid van de maatregelen. Bij die maatregelen moet rekening worden gehouden met de aard, de omvang, de context en het doel van de verwerking en het risico voor de rechten en vrijheden van natuurlijke personen."

[19] Zie met name de arresten van het Hof van 5 september 2019, Europese Unie/Guardian Europe en Guardian Europe/Europese Unie (C-447/17 P en C-479/17 P, EU:C:2019:672, punt 147), en 28 oktober 2021, Vialto Consulting/Commissie (C-650/19 P, EU:C:2021:879, punt 138), en de arresten van het Gerecht van 13 januari 2021, Helbert/EUIPO (T-548/18, EU:T:2021:4, punt 116), en 29 september 2021, Kočner/EUROPOL (T-528/20, niet gepubliceerd, EU:T:2021:631, punt 61), waarin eraan is herinnerd dat moet worden voldaan aan drie voorwaarden, namelijk „de onrechtmatigheid van de aan de instelling van de Unie verweten gedraging, het daadwerkelijk bestaan van schade en het bestaan van een causaal verband tussen de gedraging van die instelling en de gestelde schade".

52. Zoals de Commissie heeft benadrukt, is het in de praktijk vaak bijna onmogelijk om dat bewijs te leveren, aangezien betrokkenen doorgaans over onvoldoende kennis beschikken om die maatregelen te kunnen analyseren en geen toegang hebben tot alle gegevens die in het bezit zijn van de betrokken verwerkingsverantwoordelijke, met name wat betreft de methoden die zijn gebruikt om de beveiliging van die verwerking te waarborgen. Voorts zou de verwerkingsverantwoordelijke daarbij kunnen aanvoeren dat zijn weigering om deze feiten aan de betrokkenen bekend te maken gerechtvaardigd is omdat hij zijn interne zaken of gegevens die onder een beroepsgeheim vallen niet openbaar wil maken, onder meer juist om veiligheidsredenen.

53. Indien wordt aangenomen dat de bewijslast berust op de betrokkene, zou dit derhalve in de praktijk tot gevolg hebben dat het recht op beroep van artikel 82, lid 1, grotendeels zijn inhoud zou verliezen. Naar mijn mening is dit niet in overeenstemming met de bedoelingen van de Uniewetgever die met de vaststelling van de AVG heeft getracht de rechten van betrokkenen en de verplichtingen van verwerkingsverantwoordelijken te versterken ten opzichte van richtlijn 95/46 die door de AVG is vervangen. Derhalve is het logischer en is het juridisch te verdedigen dat de verwerkingsverantwoordelijke, in het kader van zijn verweer tegen een vordering tot schadevergoeding, moet aantonen dat hij de verplichtingen van de artikelen 24 en 32 AVG heeft nageleefd door daadwerkelijk passende maatregelen te treffen.

54. Met het tweede onderdeel van zijn derde vraag wenst de verwijzende rechter in wezen van het Hof te vernemen of een gerechtelijk deskundigenonderzoek als een noodzakelijk en toereikend bewijsmiddel kan worden beschouwd om vast te stellen dat de door de verwerkingsverantwoordelijke getroffen technische en organisatorische maatregelen passend waren, wanneer de ongeoorloofde toegang tot en de ongeoorloofde verstrekking van persoonsgegevens het gevolg zijn van een hackaanval.

55. Ik ben van mening dat, zoals ook de Bulgaarse en de Italiaanse regering, Ierland en de Commissie (in wezen) hebben benadrukt, het antwoord op deze vragen gebaseerd moet zijn op de vaste rechtspraak van het Hof volgens welke het op basis van het beginsel van de procedurele autonomie, bij gebreke van Unievoorschriften ter zake, een zaak van de interne rechtsorde van elke lidstaat is om de procesregels te geven voor rechtsvorderingen ter bescherming van de rechten van justitiabelen, op voorwaarde evenwel dat die regels in situaties waarop het Unierecht van toepassing is, niet ongunstiger zijn dan die welke gelden voor soortgelijke situaties die onder het nationale recht vallen (gelijkwaardigheidsbeginsel) en dat zij de uitoefening van de door het Unierecht verleende rechten in de praktijk niet onmogelijk of uiterst moeilijk maken (doeltreffendheidsbeginsel).

56. In casu merk ik op dat de AVG geen enkele bepaling bevat voor de vaststelling van toelaatbare bewijsmethoden en de bewijskracht ervan, met name wat betreft maatregelen van instructie (zoals een deskundigenonderzoek) waartoe nationale rechters opdracht kunnen of moeten geven om te beoordelen of een verwerkingsverantwoordelijke passende maatregelen heeft getroffen in de zin van de AVG. Derhalve is het mijns inziens, bij gebreke van geharmoniseerde regels, een zaak van de interne rechtsorde van elke lidstaat om die procesregels vast te stellen, met eerbiediging van de beginselen van gelijkwaardigheid en doeltreffendheid.

57. Het hierboven genoemde „doeltreffendheidsbeginsel” dat impliceert dat een onafhankelijke rechter een onpartijdige toetsing moet verrichten, zou kunnen worden ondermijnd indien het bijvoeglijk naamwoord „toereikend” moet worden opgevat in de betekenis die de verwijzende rechter daar volgens mij aan toekent, namelijk dat op basis van een deskundigenonderzoek

automatisch kan worden geconcludeerd dat de door de verwerkingsverantwoordelijke getroffen maatregelen passend zijn. [20]

E. Vierde prejudiciële vraag

58. Met de vierde vraag wenst de verwijzende rechter in wezen te vernemen of artikel 82, lid 3, AVG aldus moet worden uitgelegd dat een inbreuk op de AVG (die, zoals in casu, bestaat in de „ongeoorloofde verstrekking" van of de „ongeoorloofde toegang" tot persoonsgegevens in de zin van artikel 4, punt 12) door personen die geen medewerkers van de verwerkingsverantwoordelijke zijn en niet onder zijn toezicht staan, een feit is waarvoor de verwerkingsverantwoordelijke op geen enkele wijze verantwoordelijk is en dat bijgevolg rechtvaardigt dat hij wordt vrijgesteld van aansprakelijkheid in de zin van artikel 82, lid 3.

59. Het antwoord op deze vraag volgt rechtstreeks uit hetgeen hierboven is uiteengezet met betrekking tot de algemene filosofie van de AVG: er is geen sprake van automatismen en de verwerkingsverantwoordelijke kan dan ook niet worden vrijgesteld van aansprakelijkheid op grond van het enkele feit dat de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot persoonsgegevens heeft plaatsgevonden door toedoen van personen die niet onder zijn toezicht staan.

60. Allereerst moet worden opgemerkt dat noch uit de tekst van artikel 82, lid 3, noch uit die van overweging 146 volgt dat de verwerkingsverantwoordelijke wordt vrijgesteld van aansprakelijkheid indien aan bepaalde voorwaarden is voldaan, tenzij hij bewijst dat „hij op geen enkele wijze verantwoordelijk is voor het schadeveroorzakende feit". Uit die bewoordingen blijkt ten eerste dat de verwerkingsverantwoordelijke slechts kan worden vrijgesteld van aansprakelijkheid indien hij bewijst dat hij niet verantwoordelijk is voor het betreffende schadeveroorzakende feit en ten tweede, dat de in die bepaling verlangde bewijsstandaard hoog is gelet op het gebruik van de uitdrukking „op geen enkele wijze", zoals de Commissie heeft benadrukt. [21]

61. De aansprakelijkheidsregeling van artikel 82 en meer in het algemeen van de gehele AVG heeft aanleiding gegeven tot een breed debat in de rechtsleer van verschillende lidstaten. Die regeling bevat namelijk traditionele elementen die kenmerkend zijn voor niet-contractuele aansprakelijkheid, maar ook elementen die volgens de structuur van de bepalingen in de buurt liggen van contractuele aansprakelijkheid of zelfs van een vorm van objectieve aansprakelijkheid vanwege het intrinsiek risicovolle karakter van gegevensverwerking. Dit is niet de plek om dieper in te gaan op dat debat, maar naar mijn mening lijkt in artikel 82 geen sprake te zijn van een regeling van objectieve aansprakelijkheid. [22]

[20] Schriftelijke opmerkingen, punt 39.

[21] Overeenkomstig de vaste rechtspraak van het Hof op grond waarvan uitzonderingen op een algemene regel restrictief moeten worden uitgelegd, moet de eventuele vrijstelling van aansprakelijkheid van artikel 82, lid 3, restrictief worden uitgelegd. Zie naar analogie de arresten van 15 oktober 2020, Association française des usagers de banques (C-778/18, EU:C:2020:831, punt 53), en 5 april 2022, Commissioner of An Garda Síochána e.a. (C-140/20, EU:C:2022:258, punt 40).

[22] Wettelijke aansprakelijkheid wordt doorgaans als objectief aangemerkt wanneer de handelende persoon verplicht is tot het treffen van alle maatregelen die theoretisch gezien mogelijk zijn ter voorkoming van schade, ongeacht of hij er feitelijk kennis van droeg of ongeacht de economische houdbaarheid ervan. Indien daarentegen aan de handelende persoon wordt opgelegd dat hij maatregelen treft die normaliter door een marktdeelnemer in de betrokken economische sector worden getroffen teneinde de veiligheid te garanderen en eventuele uit de activiteit voortvloeiende schade te voorkomen, lijkt de verantwoordelijkheid voor de schade te verschuiven in de richting van schuldaansprakelijkheid. Gambini M., „Responsabilità", op. cit., blz. 1055.

62. Schade als gevolg van een inbreuk in verband met persoonsgegevens kan ontstaan indien – niet-opzettelijk, maar uit nalatigheid – geen technische en organisatorische maatregelen zijn getroffen die redelijk en in elk geval passend zijn om die schade te voorkomen, gelet op de risico's voor de rechten en vrijheden van de personen wier gegevens verwerkt worden. Deze risico's leiden tot een striktere verplichting om schade te voorkomen en te vermijden en tot een grotere zorgvuldigheidsplicht voor de verwerkingsverantwoordelijke. Op basis van de gedragsverplichtingen voor verwerkingsverantwoordelijken en de bepaling inzake bevrijdend bewijs ten laste van de schadeveroorzaker, in onderlinge samenhang gelezen, kan derhalve worden geconcludeerd dat wordt erkend dat aansprakelijkheid in het geval van onrechtmatige verwerking van persoonsgegevens in de zin van artikel 82 AVG het karakter heeft van verruimde aansprakelijkheid voor veronderstelde schuld. [23]

63. Hieruit volgt de mogelijkheid voor de verwerkingsverantwoordelijke om bevrijdend bewijs te leveren (wat niet mogelijk is bij objectieve aansprakelijkheid). Met betrekking tot de verdeling van de bewijslast is in artikel 82, lid 3, AVG een regeling ten gunste van de benadeelde uiteengezet, waarbij is bepaald dat voor de schuld van de schadeveroorzaker een omgekeerde bewijslast geldt [24], geheel in lijn met de hiervoor genoemde omgekeerde bewijslast wat betreft het feit dat de getroffen maatregelen passend zijn. De wetgever toont op die manier aan dat hij zich bewust is van de gevaren wanneer een andere verdeling van de bewijslast zou worden toegestaan en dat, wanneer hij de bewijslast voor de schuld van de schadeveroorzaker bij de natuurlijke persoon/benadeelde zou leggen, dit uiteindelijk een buitensporige belasting voor diens positie zou betekenen en dus in feite de doeltreffendheid van het recht op schadevergoeding zou aantasten in het kader van regels met betrekking tot het gebruik van nieuwe technologieën. Het kan voor de betrokkene bijzonder bezwaarlijk blijken te zijn om de wijze waarop de schade is ontstaan te reconstrueren en daarvan kennis te hebben en bijgevolg om de schuld van de verwerkingsverantwoordelijke aan te tonen. De verwerkingsverantwoordelijke daarentegen kan beter het bevrijdende bewijs leveren om aan te tonen dat hij op geen enkele wijze verantwoordelijk is voor het schadeveroorzakende feit. [25]

64. In lijn met het hiervoor genoemde beginsel van de verantwoordingsplicht moet de verwerkingsverantwoordelijke ook aantonen dat hij al het mogelijke heeft ondernomen om de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen.

65. Terugkomend op de vraag van de verwijzende rechter of de verwerkingsverantwoordelijke, op basis van de voorgaande overwegingen over de aard van de aansprakelijkheid van de verwerkingsverantwoordelijke, zoals gezegd, kan worden vrijgesteld van aansprakelijkheid wanneer hij bewijst dat de inbreuk is veroorzaakt door een feit waarvoor hij op geen enkele wijze verantwoordelijk is, kan de enkele omstandigheid dat dit feit is veroorzaakt door een persoon die niet onder zijn toezicht staat, niet als zodanig worden aangemerkt.

66. Wanneer een verwerkingsverantwoordelijke slachtoffer is van een aanval door cybercriminelen, kan het schadeveroorzakende feit niet aan de verwerkingsverantwoordelijke worden toegerekend, maar is het niet uitgesloten dat aan de betreffende aanval nalatigheid van de verwerkingsverantwoordelijke ten grondslag heeft gelegen en dat de aanval is vergemakkelijkt

[23] Gambini M., „Responsabilità", op. cit., blz. 1059. Zie naar analogie voor het standpunt volgens welke het bewijs dat passende maatregelen zijn getroffen, niet alleen wordt geleverd door aan te tonen dat de vereiste grootst mogelijke zorgvuldigheid is betracht, maar ook door bewijs te leveren van een extern schadeveroorzakend feit met de kenmerken van onvoorzienbaarheid en onvermijdelijkheid die typisch zijn voor toeval en overmacht, Sica S., „Sub artikel 82", D'Orazio R., Finocchiaro G., Pollicino O., Resta G., *Codice della privacy e data protection*, Giuffrè, 2021.

[24] „[…] indien hij *bewijst* dat hij op geen enkele wijze verantwoordelijk is voor het schadeveroorzakende feit" (artikel 82, lid 3).

[25] Gambini M., „Responsabilità", op. cit., blz. 1060.

doordat de beveiligingsmaatregelen die laatstgenoemde voor de persoonsgegevens had moeten treffen, ontbraken of niet passend waren. Het gaat om feitelijke beoordelingen die per geval verschillen en die aan de betrokken nationale rechter worden overgelaten in het licht van het voor hem aangevoerde bewijs.

67. Voorts is het algemeen bekend dat externe aanvallen op systemen van publieke of private entiteiten die in het bezit zijn van grote hoeveelheden persoonsgegevens, veel vaker voorkomen dan interne aanvallen. Derhalve moet de verwerkingsverantwoordelijke beschikken over passende maatregelen om zich met name tegen externe aanvallen te wapenen.

68. In de laatste plaats moet vanuit teleologisch oogpunt worden opgemerkt dat de AVG een hoog niveau van bescherming nastreeft. In dit verband heeft het Hof reeds onderstreept dat uit artikel 1, lid 2, AVG, gelezen in samenhang met de overwegingen 10, 11 en 13 ervan, blijkt dat deze verordening de instellingen, organen en instanties van de Unie en de bevoegde autoriteiten van de lidstaten de verplichting oplegt om een hoog niveau van bescherming van de door artikel 16 VWEU en artikel 8 van het Handvest gewaarborgde rechten ten aanzien van de bescherming van persoonsgegevens te waarborgen. [26]

69. Mocht het Hof kiezen voor de uitlegging waarbij de verwerkingsverantwoordelijke, ingeval een derde inbreuk maakt op de AVG, automatisch moet worden vrijgesteld van aansprakelijkheid in de zin van artikel 82, lid 3, dan zou een dergelijke uitlegging onverenigbaar zijn met het door deze verordening nagestreefde doel van bescherming gelet op het feit dat de rechten van de betrokkenen zouden worden verzwakt, aangezien die aansprakelijkheid dan beperkt zou zijn tot de gevallen waarin de inbreuk toe te rekenen is aan personen die onder het gezag en/of het toezicht van deze verwerkingsverantwoordelijke staan.

F. Vijfde prejudiciële vraag

70. Met de vijfde vraag verzoekt de nationale rechter het Hof in wezen om een uitlegging van het begrip „immateriële schade” in de zin van artikel 82 AVG. Hij wenst in het bijzonder te vernemen of de bepalingen van artikel 82, leden 1 en 2, AVG junctis de overwegingen 85 en 146 ervan [27], aldus moeten worden uitgelegd dat bij een inbreuk op deze verordening in de vorm van de ongeoorloofde toegang tot persoonsgegevens en van de ongeoorloofde verstrekking van die gegevens door cybercriminelen, het feit dat de betrokkene vreest voor mogelijk misbruik van zijn persoonsgegevens in de toekomst op zich (immateriële) schade kan opleveren waarvoor recht op schadevergoeding bestaat.

71. Noch artikel 82 noch de overwegingen met betrekking tot schadevergoeding geven een duidelijk antwoord op de vraag, maar voor de analyse kunnen daaruit wel enkele nuttige elementen worden gehaald: immateriële (of morele) schade kan naast materiële schade (of vermogensschade) voor vergoeding in aanmerking komen; een inbreuk op de verordening wordt niet automatisch gevolgd door schade die daardoor wordt „veroorzaakt” of, meer bepaald, een

[26] Zie in die zin arrest van 15 juni 2021, Facebook Ireland e.a. (C-645/19, EU:C:2021:483, punten 44 en 45).

[27] Overweging 85 luidt als volgt: „Een inbreuk in verband met persoonsgegevens kan, wanneer dit probleem niet tijdig en op passende wijze wordt aangepakt, resulteren in lichamelijke, materiële of immateriële schade voor natuurlijke personen […]”. Overweging 146 luidt als volgt: „De verwerkingsverantwoordelijke of de verwerker moeten alle schade vergoeden die iemand kan lijden ten gevolge van een verwerking die inbreuk maakt op deze verordening. De verwerkingsverantwoordelijke of de verwerker moet van zijn aansprakelijkheid worden vrijgesteld indien hij bewijst dat hij niet verantwoordelijk is voor de schade. Het begrip „schade” moet ruim worden uitgelegd in het licht van de rechtspraak van het Hof van Justitie, op een wijze die ten volle recht doet aan de doelstellingen van deze verordening. Dit laat eventuele eisen tot schadeloosstelling wegens inbreuken op andere regels in het Unierecht of het lidstatelijke recht onverlet. […]. De betrokkenen dienen volledige en daadwerkelijke vergoeding van door hen geleden schade te ontvangen. […]”

inbreuk in verband met persoonsgegevens „kan resulteren in" lichamelijke, materiële of immateriële schade voor natuurlijke personen; het begrip „schade" moet „ruim" worden uitgelegd in het licht van de rechtspraak van het Hof, op een wijze die ten volle recht doet aan de doelstellingen van de AVG; de „geleden" schade moet „volledig en daadwerkelijk" worden vergoed.

72. Elke mogelijke suggestie dat er vanzelfsprekend sprake is van schade, wordt door de bewoordingen van de bepalingen van de AVG reeds uit de wereld geholpen: de primaire doelstelling van de wettelijke aansprakelijkheid waarin de AVG voorziet, is het geven van genoegdoening aan de betrokkene, en wel precies door middel van een „volledige en daadwerkelijke" vergoeding van de schade die hij heeft geleden, en dus het herstellen van het evenwicht van de rechtssituatie die door de inbreuk op het recht in negatieve zin is gewijzigd (geschaad). [28]

73. Echter ook vanuit systematisch oogpunt, zoals in de antitrustwetgeving, biedt de AVG twee pijlers van bescherming: één van publieke aard, waarbij sancties gelden indien inbreuk wordt gemaakt op de bepalingen van de AVG, en één van particuliere aard die juist voorziet in wettelijke aansprakelijkheid van niet-contractuele aard, die kan worden aangemerkt als verruimde aansprakelijkheid voor veronderstelde schuld met de bovengenoemde kenmerken, mede in verband met het leveren van bevrijdend bewijs. [29]

74. Derhalve kan een brede uitlegging [30] van het begrip (morele) schade niet zover strekken dat de wetgever zou hebben afgezien van het vereiste van reële „schade".

75. Het werkelijke probleem is de vraag of er, zodra de inbreuk en het causale verband zijn vastgesteld, een recht op schadevergoeding kan ontstaan louter vanwege de bezorgdheid en ongerustheid van de betrokkene over en zijn vrees voor mogelijk misbruik van zijn persoonsgegevens in de toekomst, zonder dat een dergelijk misbruik is vastgesteld en/of de betrokkene verdere schade heeft geleden.

76. Volgens vaste rechtspraak van het Hof moeten begrippen in een bepaling van Unierecht die voor de betekenis en de draagwijdte ervan niet uitdrukkelijk naar het recht van de lidstaten verwijst, normaliter in de gehele Unie autonoom en uniform worden uitgelegd, rekening houdend met de bewoordingen van de betreffende bepaling, met de context waarin zij is geplaatst, met de doelstellingen van de regeling waarvan zij deel uitmaakt en met de ontstaansgeschiedenis van die bepaling. [31]

[28] Zie de reeds aangehaalde conclusie van advocaat-generaal Campos Sánchez-Bordona, punt 29 en voetnoot 11. In diezelfde conclusie rondt de advocaat-generaal zijn analyse correct af met een letterlijke, historische, contextuele en teleologische uitlegging waarbij hij uitsluit dat op grond van artikel 82 aan betrokkenen schadevergoeding met een „punitief" karakter kan worden toegekend (punten 27-55). Enerzijds merkt hij op dat lidstaten „[niet] hoeven […] te kiezen (en […] dat trouwens ook niet [kunnen]) tussen de mechanismen van hoofdstuk VIII om de bescherming van gegevens te waarborgen. In het geval van een inbreuk die niet tot schade leidt, heeft de betrokkene nog steeds (ten minste) het recht om een klacht in te dienen bij een toezichthoudende autoriteit". Anderzijds merkt hij op dat „het vooruitzicht op het verkrijgen van een schadevergoeding zonder dat er sprake is van schade, waarschijnlijk [zou] leiden tot meer civielrechtelijke zaken, met vorderingen die misschien niet altijd gerechtvaardigd zijn, en aldus een rem kunnen zetten op de activiteiten in verband met gegevensverwerking" (punten 54 en 55).

[29] Dat er geen recht op schadevergoeding voor zwakke en voorbijgaande gevoelens of emoties wordt toegekend waar het gaat om de inbreuk op verwerkingsregels, betekent nog niet dat de betrokkene in het geheel niet wordt beschermd (zie in die zin de reeds aangehaalde conclusie van advocaat-generaal Campos Sánchez-Bordona, punt 115).

[30] Ofwel „ruim" in de bewoordingen van overweging 146.

[31] Zie arresten van 15 april 2021, The North of England P & I Association (C-786/19, EU:C:2021:276, punt 48), en 10 juni 2021, KRONE – Verlag (C-65/20, EU:C:2021:471, punt 25).

77. Zoals advocaat-generaal Campos in herinnering heeft gebracht [32], heeft het Hof geen algemene definitie van „schade" uitgewerkt die zonder onderscheid op elk gebied kan worden toegepast. [33] Wat immateriële schade betreft, kan uit zijn rechtspraak worden afgeleid dat, wanneer een van de doelen van de uit te leggen bepaling bestaat in de bescherming van het individu, of van een bepaalde categorie individuen [34], het begrip „schade" ruim moet worden opgevat, en dat de schadevergoeding zich in overeenstemming met dit criterium uitstrekt tot immateriële schade, ook al wordt dit soort schade niet in de uitgelegde bepaling genoemd. [35]

78. Gelet op de rechtspraak van het Hof kan er weliswaar voor worden gepleit dat er in het Unierecht op de aangegeven wijze een beginsel bestaat dat immateriële schade wordt vergoed, maar ik sluit mij aan bij advocaat-generaal Campos dat daaruit geen regel kan worden afgeleid volgens welke *alle* immateriële schade, ongeacht de ernst ervan, in aanmerking komt voor vergoeding. [36]

79. In dit verband is een relevant aanknopingspunt het onderscheid tussen immateriële schade die in aanmerking komt voor vergoeding, en andere *ongemakken die voortvloeien uit de niet-nakoming van de wet* maar die wegens hun geringe belang niet noodzakelijkerwijs recht op schadevergoeding zouden geven. [37]

80. Het Hof erkent dit verschil door moeilijkheden en ongemakken als een zelfstandige categorie – die van de categorie schade losstaat – aan te merken op gebieden waarop het van oordeel is dat die moeilijkheden en ongemakken moeten worden vergoed. [38]

[32] Zie de reeds aangehaalde conclusie van advocaat-generaal Campos Sánchez-Bordona, punt 104.

[33] Het heeft ook niet aangegeven dat een bepaalde methode van uitlegging – autonoom of onder verwijzing naar de nationale rechtsstelsels – de voorkeur verdient: dit hangt af van welk onderwerp er aan de orde is. Vergelijk de arresten van 10 mei 2001, Veedfald (C-203/99, EU:C:2001:258, punt 27), over producten met gebreken; 6 mei 2010, Walz (C-63/09, EU:C:2010:251, punt 21), over de aansprakelijkheid van luchtvervoerders, en 10 juni 2021, Van Ameyde España (C-923/19, EU:C:2021:475, punten 37 e.v.), over de wettelijke aansprakelijkheid voor ongevallen ten gevolge van de deelneming aan het verkeer van motorrijtuigen.

[34] Bijvoorbeeld consumenten van producten of slachtoffers van verkeersongevallen.

[35] Zie, op het gebied van pakketreizen, arrest van 12 maart 2002, Leitner (C-168/00, EU:C:2002:163), alsmede, op het gebied van de wettelijke aansprakelijkheid waartoe deelneming aan het verkeer van motorrijtuigen aanleiding kan geven, de arresten van 24 oktober 2013, Haasová (C-22/12, EU:C:2013:692, punten 47-50); 24 oktober 2013, Drozdovs (C-277/12, EU:C:2013:685, punt 40), en 23 januari 2014, Petillo (C-371/12, EU:C:2014:26, punt 35).

[36] Zie de reeds aangehaalde conclusie van advocaat-generaal Campos Sánchez-Bordona, punt 105. Het Hof heeft bijvoorbeeld erkend dat een nationale regeling waarbij er voor de berekening van de schadevergoeding in geval van immateriële schade die voortvloeit uit letselschade door een ongeval, een onderscheid wordt gemaakt afhankelijk van de oorzaak van het ongeval, verenigbaar is met de Europese regels. Zie arrest van 23 januari 2014, Petillo (C-371/12, EU:C:2014:26, dictum), waaruit blijkt dat het Unierecht zich niet verzet tegen „een nationale wettelijke regeling […] die een bijzonder stelsel inhoudt voor de vergoeding van immateriële schade die voortvloeit uit lichte verwondingen ten gevolge van verkeersongevallen op de weg en waarin de vergoeding van deze schade is beperkt ten opzichte van de vergoeding die kan worden toegewezen voor identieke schade die voortvloeit uit andere oorzaken dan [verkeers]ongevallen".

[37] Dit onderscheid wordt in de nationale rechtsstelsels beschouwd als een onvermijdelijk uitvloeisel van het samenleven. Zie recentelijk op het gebied van gegevensbescherming, in Italië Tribunale di Palermo, sez. I civile (rechter in eerste aanleg, civiele kamer nr. 1, Palermo, Italië), vonnis nr. 5261 van 5 oktober 2017, alsook Cass. Civ. Sez. 6 (hoogste rechter in civiele en strafzaken, kamer nr. 6, Italië), beschikking nr. 17383/2020. In Duitsland onder meer Amtsgericht Diez (rechter in eerste aanleg Diez, Duitsland), 7 november 2018 – 8 C 130/18; Landgericht Karlsruhe (rechter in eerste aanleg Karlsruhe, Duitsland), 2 augustus 2019 – 8 O 26/19, en Amtsgericht Frankfurt am Main (rechter in eerste aanleg Frankfurt am Main, Duitsland), 10 juli 2020 – 385 C 155/19 (70). In Oostenrijk, Oberster Gerichtshof, 6 Ob 56/21k.

[38] Zie arrest van 23 oktober 2012, Nelson e.a. (C-581/10 en C-629/10, EU:C:2012:657, punt 51), over het onderscheid tussen „schade" in de zin van artikel 19 van het op 28 mei 1999 te Montreal gesloten Verdrag tot het brengen van eenheid in enige bepalingen inzake het internationale luchtvervoer en „ongemak" in de zin van verordening nr. 261/2004, dat kan worden vergoed op grond van artikel 7 van die verordening, gelet op het arrest van 19 november 2009, Sturgeon e.a. (C-402/07 en C-432/07, EU:C:2009:716). In deze sector heeft de wetgever, net als in het geval van het passagiersvervoer over zee en over binnenwateren, dat onder verordening nr. 1177/2010 valt, een abstracte categorie kunnen vaststellen omdat de aan die moeilijkheden ten grondslag liggende factor en de essentie van de moeilijkheden voor alle benadeelden identiek zijn. Volgens mij is een dergelijke gevolgtrekking niet mogelijk op het gebied van gegevensbescherming.

81. Op basis van ervaring kan worden gesteld dat elke inbreuk op een regel inzake de bescherming van persoonsgegevens kan leiden tot een negatieve reactie van de betrokkene. Schadevergoeding die louter voortvloeit uit een gevoel van onbehagen over het feit dat een ander de wet niet eerbiedigt, wordt gemakkelijk verward met schadevergoeding zonder schade, die, zoals gezegd, in het in artikel 82 AVG bedoelde geval niet mogelijk is.

82. Het feit dat in omstandigheden als die van het hoofdgeding misbruik van persoonsgegevens slechts een mogelijkheid is die nog geen werkelijkheid is geworden, volstaat om aan te nemen dat de betrokkene immateriële schade kan hebben geleden als gevolg van de inbreuk op de AVG, op voorwaarde dat de betrokkene bewijst dat de vrees voor dat misbruik hem in concreet en specifiek opzicht reële en zekere emotionele schade heeft berokkend. [39]

83. De scheidslijn tussen louter ergernis (geen vergoeding mogelijk) en reële immateriële schade (wel vergoeding mogelijk) is zeker dun, maar de nationale rechters, die tot taak hebben om die scheidslijn in elk afzonderlijk geval te trekken, moeten alle gegevens die zijn aangeleverd door de betrokkene die om schadevergoeding verzoekt, zorgvuldig beoordelen. Op laatstgenoemde rust de verplichting om nauwkeurig en niet in algemene termen aan te voeren welke concrete gegevens kunnen leiden tot „daadwerkelijk geleden immateriële schade" als gevolg van de inbreuk in verband met persoonsgegevens, zonder dat voor die schade echter een vooraf bepaalde graad van ernst geldt: wat telt is niet een louter subjectieve beleving die veranderlijk en ook afhankelijk is van karakter- en persoonlijke eigenschappen, maar de objectivering van de voor de eigen fysieke of psychische toestand of voor het eigen sociale leven bestaande moeilijkheden, zelfs als zij gering maar wel aantoonbaar zijn, de aard van de betreffende persoonsgegevens en het belang daarvan in het leven van de betrokkene en misschien ook de immer aanwezige maatschappelijke perceptie omtrent die specifieke moeilijkheden ten opzichte van de gegevensinbreuk. [40]

IV. Conclusie

84. In het licht van het bovenstaande geef ik het Hof in overweging om de prejudiciële vragen te beantwoorden als volgt:

„De artikelen 5, 24, 32 en 82 van verordening 2016/679 moeten aldus worden uitgelegd dat:

louter een ‚inbreuk in verband met persoonsgegevens', zoals gedefinieerd in artikel 4, punt 12, op zichzelf niet volstaat om te concluderen dat de door de verwerkingsverantwoordelijke getroffen technische en organisatorische maatregelen niet ‚passend' waren om de bescherming van de betreffende gegevens te waarborgen;

de betrokken nationale rechter bij de beoordeling of de door de verwerkingsverantwoordelijke getroffen technische en organisatorische maatregelen passend zijn, een toetsing moet verrichten die een concrete analyse omvat van zowel de inhoud van die maatregelen als de wijze waarop zij zijn toegepast en de gevolgen ervan in de praktijk;

[39] Volgens Ierland zijn deze overwegingen in de praktijk in het kader van cybercriminaliteit bijzonder belangrijk, omdat wanneer iedereen die, ook slechts minimaal, wordt getroffen door een inbreuk, recht op vergoeding van immateriële schade zou hebben, dit grote gevolgen zou hebben en wel met name voor de verwerkingsverantwoordelijken in de publieke sector die met beperkte openbare middelen worden gefinancierd en vooral het collectieve belang moeten dienen, daaronder begrepen de verbetering van de beveiliging van persoonsgegevens (schriftelijke opmerkingen, punt 72).

[40] Zie de reeds aangehaalde conclusie van advocaat-generaal Campos Sánchez-Bordona, punt 116.

in het kader van een vordering tot schadevergoeding in de zin van artikel 82 AVG de verwerkingsverantwoordelijke verplicht is om te bewijzen dat de door hem getroffen maatregelen passend zijn in de zin van artikel 32 van deze verordening;

het in overeenstemming met het beginsel van de procedurele autonomie een zaak is van de interne rechtsorde van elke lidstaat om toelaatbare bewijsmethoden en de bewijskracht ervan vast te stellen, met inbegrip van maatregelen van instructie waartoe nationale rechters opdracht kunnen of moeten geven, teneinde te beoordelen of een verwerkingsverantwoordelijke van persoonsgegevens passende maatregelen heeft getroffen in de zin van deze verordening, met inachtneming van de in het Unierecht vastgelegde beginselen van gelijkwaardigheid en doeltreffendheid;

het feit dat de schadeveroorzakende inbreuk op deze verordening door toedoen van een derde heeft plaatsgevonden, op zichzelf geen reden is om de verwerkingsverantwoordelijke vrij te stellen van aansprakelijkheid en dat de verwerkingsverantwoordelijke, om in aanmerking te komen voor de vrijstelling in die bepaling, moet bewijzen dat hij op geen enkele wijze verantwoordelijk is voor de inbreuk;

de schade in de vorm van vrees voor mogelijk misbruik van de eigen persoonsgegevens in de toekomst, waarvan het bestaan door de betrokkene is aangetoond, immateriële schade kan opleveren waarvoor een recht op schadevergoeding bestaat, op voorwaarde dat de betrokkene bewijst dat hijzelf reële en zekere emotionele schade heeft geleden en dat de betrokken nationale rechter dit in elk afzonderlijk geval toetst.”