Samling af Afgørelser

FORSLAG TIL AFGØRELSE FRA GENERALADVOKAT
G. PITRUZZELLA
fremsat den 27. april 2023 [1]

Sag C-340/21

VB
mod
Natsionalna agentsia za prihodite

(anmodning om præjudiciel afgørelse indgivet af Varhoven administrativen sad (øverste forvaltningsdomstol, Bulgarien))

»Præjudiciel forelæggelse – beskyttelse af personoplysninger – forordning (EU) 2016/679 – den dataansvarliges ansvar – behandlingssikkerhed – brud på persondatasikkerheden – ikke-økonomisk skade som følge af den dataansvarliges passivitet – erstatningssøgsmål«

Kan det forhold, at personoplysninger, som et offentligt agentur er i besiddelse af, bliver genstand for ulovlig formidling gennem et cyberangreb, give ret til erstatning for den ikke-økonomiske skade, som en registreret gør gældende alene af den grund, at denne nærer frygt for et muligt fremtidigt misbrug af dennes personoplysninger? På baggrund af hvilke kriterier skal den dataansvarlige tilregnes ansvaret? Hvordan skal bevisbyrden fordeles mellem parterne i sagen? Hvilket omfang skal rettens legalitetskontrol have?

I. Retsforskrifter

1. Artikel 4 med overskriften »Definitioner« i forordning 2016/679 [2] (herefter »forordningen«) bestemmer følgende:

»I denne forordning forstås ved:

[…]

12) »brud på persondatasikkerheden«: et brud på sikkerheden, der fører til hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet

[…]«

[1] – Originalsprog: italiensk.

[2] – Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27.4.2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse).

2. Artikel 5 med overskriften »Principper for behandling af personoplysninger« foreskriver følgende:

»1. Personoplysninger skal:

[…]

f) behandles på en måde, der sikrer tilstrækkelig sikkerhed for de pågældende personoplysninger, herunder beskyttelse mod uautoriseret eller ulovlig behandling og mod hændeligt tab, tilintetgørelse eller beskadigelse, under anvendelse af passende tekniske eller organisatoriske foranstaltninger (»integritet og fortrolighed«).

2. Den dataansvarlige er ansvarlig for og skal kunne påvise, at stk. 1 overholdes (»ansvarlighed«).«

3. Samme forordnings artikel 24 med overskriften »Den dataansvarliges ansvar« bestemmer følgende:

»1. Under hensyntagen til den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder gennemfører den dataansvarlige passende tekniske og organisatoriske foranstaltninger for at sikre og for at være i stand til at påvise, at behandling er i overensstemmelse med denne forordning. Disse foranstaltninger skal om nødvendigt revideres og ajourføres.

2. Hvis det står i rimeligt forhold til behandlingsaktiviteter, skal de foranstaltninger, der er omhandlet i stk. 1, omfatte den dataansvarliges implementering af passende databeskyttelsespolitikker.

3. Overholdelse af godkendte adfærdskodekser som omhandlet i artikel 40 eller godkendte certificeringsmekanismer som omhandlet i artikel 42 kan bruges som et element til at påvise overholdelse af den dataansvarliges forpligtelser.«

4. Artikel 32 med overskriften »Behandlingssikkerhed« fastsætter følgende:

»1. Under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder gennemfører den dataansvarlige og databehandleren passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til disse risici, herunder bl.a. alt efter hvad der er relevant:

[…]

2. Ved vurderingen af, hvilket sikkerhedsniveau der er passende, tages der navnlig hensyn til de risici, som behandling udgør, navnlig ved hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.

3. Overholdelse af en godkendt adfærdskodeks som omhandlet i artikel 40 eller en godkendt certificeringsmekanisme som omhandlet i artikel 42 kan bruges som et element til at påvise overholdelse af kravene i nærværende artikels stk. 1.

[…]«

5. Samme forordnings artikel 82, som har overskriften »Ret til erstatning og erstatningsansvar«, bestemmer følgende:

»1. Enhver, som har lidt materiel eller immateriel skade som følge af en overtrædelse af denne forordning, har ret til erstatning for den forvoldte skade fra den dataansvarlige eller databehandleren.

2. Enhver dataansvarlig, der er involveret i behandling, hæfter for den skade, der er forvoldt af behandling, der overtræder denne forordning. […]

3. En dataansvarlig eller databehandler er fritaget for erstatningsansvar i henhold til stk. 2, hvis det bevises, at den pågældende ikke er skyld i den begivenhed, der medførte skaden.«

II. Faktiske omstændigheder, hovedsagen og de præjudicielle spørgsmål

6. Den 15. juli 2019 offentliggjorde de bulgarske medier, at der var sket en uautoriseret adgang til informationssystemet hos Natsionalna agentsia za prihodite (det nationale agentur for indtægter, Bulgarien, herefter »agenturet« [3]), og at skatte-, afgifts- og socialforsikringsoplysninger vedrørende flere millioner personer, både bulgarske og udenlandske statsborgere, var blevet offentliggjort på internettet.

7. Mange personer, herunder VB, som er kassationsappellanten i hovedsagen, anlagde sag mod agenturet med påstand om betaling af erstatning for ikke-økonomisk skade.

8. I den konkrete situation anlagde kassationsappellanten i hovedsagen sag mod agenturet ved Administrativen sad Sofia-grad (forvaltningsdomstolen i Sofia by, Bulgarien, herefter »ASSG«) og gjorde gældende, at agenturet havde tilsidesat de nationale bestemmelser og ikke opfyldt sin forpligtelse til i sin egenskab af dataansvarlig at behandle personoplysninger på en måde, der »yder en passende sikkerhed«, ved at gennemføre passende tekniske og organisatoriske foranstaltninger i henhold til artikel 24 og 32 i forordning 2016/679. Kassationsappellanten gjorde desuden gældende, at hun var blevet påført en ikke-økonomisk skade, der bestod i bekymringer og frygt for fremtidigt misbrug af hendes personoplysninger.

9. Agenturet påpegede derimod, at kassationsappellanten i hovedsagen ikke havde anmodet agenturet om nogen informationer om, nøjagtig hvilke personoplysninger der var blevet opnået adgang til. Efter offentliggørelsen af nyheden om angrebet havde agenturet desuden afholdt møder med eksperter med det formål at beskytte borgernes rettigheder og interesser. Ifølge agenturet var der ikke nogen årsagssammenhæng mellem cyberangrebet og den påståede skade, eftersom agenturet havde indført alle processtyringssystemer og styringssystemer vedrørende informationssikkerhed i overensstemmelse med de gældende internationale standarder på området.

[3] – Agenturet er dataansvarligt som omhandlet i forordningens artikel 4, nr. 7). I henhold til national lovgivning er det en faglig myndighed, som er underlagt finansministeren og har kompetence til at fastslå, sikre og inddrive offentlige og lovbestemte private statsfordringer. Ved udøvelsen af de offentlige beføjelser, som det er blevet overdraget, behandler det personoplysninger.

10. Retten i første instans – ASSG (forvaltningsdomstolen i Sofia by) – tog ikke søgsmålet til følge, med den begrundelse, at formidling af oplysninger ikke kunne tilregnes agenturet, at bevisbyrden for, at de trufne foranstaltninger ikke var passende, påhvilede kassationsappellanten, og endelig at kassationsappellanten ikke var blevet påført nogen ikke-økonomisk skade, som kunne give ret til erstatning.

11. Dommen i første instans er blevet genstand for appel ved Varhoven administrativen sad (øverste forvaltningsdomstol, Bulgarien). Blandt anbringenderne har kassationsappellanten i hovedsagen gjort gældende, at retten i første instans fordelte bevisbyrden for at påvise undladelsen af at træffe passende sikkerhedsforanstaltninger ukorrekt. Det burde heller ikke være nødvendigt at påvise en ikke-økonomisk skade, fordi denne skade er faktisk og ikke alene hypotetisk.

12. Agenturet har gjort gældende, at det i sin egenskab af dataansvarlig havde gennemført de nødvendige tekniske og organisatoriske foranstaltninger, og bestridt, at en faktisk ikke-økonomisk skade var blevet påvist. Bekymringer og angst er nemlig følelsesmæssige tilstande, der ikke giver ret til erstatning.

13. Den forelæggende ret har konstateret, at sager anlagt af skadelidte mod agenturet med påstand om erstatning for ikke-økonomisk skade har fået divergerende udfald.

14. På denne baggrund har den forelæggende ret besluttet at udsætte sagen og forelægge Domstolen følgende præjudicielle spørgsmål:

»1) Skal artikel 24 og 32 i [Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse)] fortolkes således, at det forhold, at en uautoriseret videregivelse eller en uautoriseret adgang til personoplysninger som omhandlet i artikel 4, nr. 12), i forordning (EU) 2016/679 er blevet foretaget af personer, som ikke er ansatte i den dataansvarliges administration og ikke er undergivet dennes kontrol, er tilstrækkeligt til at lægge til grund, at de iværksatte tekniske og organisatoriske foranstaltninger ikke er passende?

2) Såfremt det første spørgsmål besvares benægtende, hvilken genstand og hvilket omfang skal rettens legalitetskontrol da have ved vurderingen af, om de tekniske og organisatoriske foranstaltninger, som den dataansvarlige har truffet som omhandlet i artikel 32 i forordning (EU) 2016/679, er passende?

3) Såfremt det første spørgsmål besvares benægtende, skal ansvarlighedsprincippet som omhandlet i artikel 5, stk. 2, og artikel 24 i forordning (EU) 2016/679, sammenholdt med 74. betragtning hertil, da fortolkes således, at bevisbyrden for, at de iværksatte tekniske og organisatoriske foranstaltninger som omhandlet i artikel 32 i forordning (EU) 2016/679 er passende, påhviler den dataansvarlige i forbindelse med et søgsmål i henhold til forordningens artikel 82, stk. 1? Kan indhentningen af en sagkyndig udtalelse anses for et bevismiddel, der er nødvendigt for og tilstrækkeligt til at fastslå, om de tekniske og organisatoriske foranstaltninger, som den dataansvarlige har truffet, i en sag som den foreliggende var passende, hvis den uautoriserede adgang til og den uautoriserede videregivelse af personoplysninger skyldtes et »hackerangreb«?

4) Skal artikel 82, stk. 3, i forordning (EU) 2016/679 fortolkes således, at den uautoriserede videregivelse af eller den uautoriserede adgang til personoplysninger som omhandlet i artikel 4, nr. 12), i forordning (EU) 2016/679 som i den foreliggende sag gennem et »hackerangreb« udført af personer, der ikke er ansatte i den dataansvarliges administration og ikke er undergivet dennes kontrol, udgør en omstændighed, som den dataansvarlige ikke er skyld i, og som kan begrunde en fritagelse for erstatningsansvar?

5) Skal artikel 82, stk. 1 og 2, i forordning (EU) 2016/679, sammenholdt med 85. og 146. betragtning hertil, fortolkes således, at det i en sag som den foreliggende, hvor tilsidesættelsen af beskyttelsen af personoplysninger kommer til udtryk ved en uautoriseret adgang til og formidling af personoplysninger gennem et »hackerangreb«, kun er den berørte persons bekymringer, frygt og angst for et muligt fremtidigt misbrug af personoplysninger, der er omfattet af begrebet immateriel skade, som skal fortolkes bredt, og dermed berettiger til erstatning, hvis der ikke er blevet konstateret et sådant misbrug og/eller den berørte person ikke er blevet påført nogen yderligere skade?«

III. Bedømmelse

A. Indledende betragtninger

15. Den foreliggende sag vedrører interessante og i en vis grad nye spørgsmål om fortolkningen af flere bestemmelser i forordningen [4].

16. De fem præjudicielle spørgsmål angår alle den samme problemstilling, nærmere bestemt de betingelser, under hvilke en person har ret til erstatning for ikke-økonomisk skade, såfremt dennes personoplysninger, som et offentligt agentur er i besiddelse af, er blevet offentliggjort på internettet som følge af et hackerangreb.

17. For enkelthedens skyld vil jeg foreslå kortfattede særskilte svar på de enkelte spørgsmål i forelæggelsesafgørelsen, selv om jeg finder, at der er begrebsmæssige overlap, idet de første fire spørgsmål alle sigter mod at fastlægge, under hvilke betingelser den dataansvarlige skal tilregnes overtrædelsen af forordningens bestemmelser [5], mens det femte spørgsmål mere præcist vedrører begrebet »ikke-økonomisk skade, der giver ret til erstatning« [6].

[4] – Artikel 5, stk. 2 (angående princippet om den dataansvarliges ansvarlighed), artikel 24 (angående de foranstaltninger, som den dataansvarlige skal træffe for at sikre, at behandlingen er i overensstemmelse med forordningen), artikel 32 (om den nævnte forpligtelse med specifikt hensyn til behandlingssikkerhed) og artikel 82, stk. 1-3 (om erstatning for skader, der er resultatet af en overtrædelse af denne forordning, og om den dataansvarliges mulighed for at træffe foranstaltninger til at sikre overholdelsen af forordningen), ud over 74., 85. og 146. betragtning, som er knyttet til de nævnte artikler.

[5] – a) Det første spørgsmål vedrører, hvorvidt det forhold, at systemerne er genstand for angreb, er tilstrækkeligt til at lægge til grund, at de iværksatte foranstaltninger ikke er passende; b) det andet spørgsmål angår, hvilket omfang rettens legalitetskontrol skal have ved vurderingen af, om de nævnte foranstaltninger er passende; c) det tredje spørgsmål angår bevisbyrden med hensyn til, hvorvidt de nævnte foranstaltninger er passende, og visse tekniske bestemmelser vedrørende bevisoptagelse; d) det fjerde spørgsmål angår, hvorvidt det forhold, at systemangrebet finder sted udefra, er relevant for ansvarsfrihed.

[6] – Hvad angår de anførte bestemmelser i forordningen vedrører de første tre spørgsmål aspekterne om den dataansvarliges ansvar for, at de trufne foranstaltninger er passende (artikel 5, 24 og 32), mens det fjerde og det femte spørgsmål angår dels betingelserne for ansvarsfrihed, dels begrebet »ikke-økonomisk skade, der giver ret til erstatning« (artikel 82).

18. Jeg skal oplyse, at flere sager netop nu verserer ved Domstolen angående forordningens artikel 82, og i en af disse har generaladvokaten allerede fremsat sit forslag til afgørelse, hvortil jeg vil tage hensyn i min bedømmelse [7].

19. Inden prøvelsen af de rejste spørgsmål finder jeg det hensigtsmæssigt at foretage nogle indledende betragtninger vedrørende principperne i og formålene med forordningen, som vil være af betydning for besvarelsen af de enkelte præjudicielle spørgsmål.

20. Forordningens artikel 24 fastsætter i generelle vendinger, at den dataansvarlige skal gennemføre passende tekniske og organisatoriske foranstaltninger for at sikre og for at være i stand til at påvise, at personoplysninger behandles i overensstemmelse med forordningen, mens den samme pligt er specificeret mere detaljeret i artikel 32 med hensyn til behandlingssikkerheden. Artikel 24 og 32 udvikler bestemmelserne i artikel 5, stk. 2, som netop under »principperne for behandling af personoplysninger« indfører »ansvarlighedsprincippet«. Dette princip følger logisk af og supplerer »princippet om integritet og fortrolighed« i artikel 5, stk. 1, litra f), og begge disse principper skal læses i lyset af den risikobaserede tilgang, som forordningen bygger på.

21. Ansvarlighedsprincippet er en af forordningens grundpiller og en af dens mest betydningsfulde fornyelser. Dette princip pålægger den dataansvarlige ansvaret for at træffe proaktive foranstaltninger for at sikre og for at være i stand til at påvise, at behandlingen er i overensstemmelse med forordningen [8].

22. I litteraturen er dette blevet beskrevet som en egentlig kulturel forandring, som er en følge af »ansvarlighedens almindelige rækkevidde« [9]. Det er ikke den formelle opfyldelse af et lovbestemt krav eller af en præcis foranstaltning, men snarere den samlede strategi, som organisationen har gennemført, som kan fritage den dataansvarlige for erstatningsansvar, når denne strategi er i overensstemmelse med databeskyttelsesbestemmelserne.

23. De tekniske og organisatoriske foranstaltninger, som er påkrævet ifølge ansvarlighedsprincippet, skal være »passende« under hensyntagen til de i artikel 24 nævnte faktorer, dvs. den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder.

24. I henhold til artikel 24 skal foranstaltningerne derfor være passende i forhold til at påvise, at behandlingen er i overensstemmelse med principperne og bestemmelserne i forordningen.

25. Artikel 32 overfører imidlertid ansvarlighedsprincippet til de konkrete foranstaltninger, som skal gennemføres for at sikre »et sikkerhedsniveau, der passer til disse risici«. Viften af de faktorer, som skal tages i betragtning i forbindelse med udvælgelsen af de tekniske og organisatoriske foranstaltninger, udvides således til også at omfatte det aktuelle tekniske niveau og implementeringsomkostningerne.

7 – Jf. generaladvokat Campos Sánchez-Bordonas forslag til afgørelse Österreichische Post (Ikke-økonomisk skade som følge af behandling af personoplysninger) (C-300/21, EU:C:2022:756).

8 – C. Docksey, *Article 24. Responsibility of the controller*, i C. Kuner, L.A. Bygrave, C. Docksey og L. Drechsler, *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford University Press, 2020, s. 561. De principper og forpligtelser, som er fastsat i databeskyttelsesbestemmelserne, bør kendetegne den kulturelle struktur i organisationerne på alle niveauer, snarere end at blive opfattet som en række lovbestemte krav, som deres juridiske afdeling skal opfylde et efter et.

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

26. Begrebet »passende foranstaltninger« kræver, at de løsninger, som er anvendt til at beskytte informationssystemer, når et acceptabelt niveau både teknisk set (foranstaltningernes relevans) og kvalitativt set (beskyttelsens effektivitet). For at sikre overholdelsen af nødvendighedsprincippet, relevansprincippet og proportionalitetsprincippet skal behandlingen ikke alene være passende, men også tilfredsstillende i forhold til de forfulgte formål. Ifølge denne logik spiller princippet om dataminimering en afgørende rolle, i kraft af hvilket alle faser af behandlingen af personoplysninger konstant skal tendere mod at minimere datasikkerhedsrisikoen [10].

27. Forordningen i sin helhed er baseret på forebyggelse af risiko og på den dataansvarliges ansvarlighed og således på en teleologisk tilgang, som sigter mod det ud fra et effektivitetssynspunkt bedst mulige resultat, hvilket står klart langt fra en formalistisk tilgang, som er knyttet til den simple pligt til at opfylde givne procedurer for at være fritaget for erstatningsansvar [11].

28. Artikel 24 indeholder ingen udtømmende fortegnelse over »passende« foranstaltninger, og vurderingen skal således foretages i hvert enkelt tilfælde. Dette er helt på linje med den filosofi, der ligger til grund for forordningen, ifølge hvilken det foretrækkes, at de gennemførte procedurer vælges med udgangspunkt i en nøje vurdering af den specifikke situation, således at disse procedurer er så effektive som muligt [12].

B. Det første præjudicielle spørgsmål

29. Med det første præjudicielle spørgsmål ønsker den forelæggende ret nærmere bestemt oplyst, om forordningens artikel 24 og 32 skal fortolkes således, at det forhold, at der indtræffer et »brud på persondatasikkerheden« som omhandlet i artikel 4, nr. 12), i sig selv er tilstrækkeligt til at lægge til grund, at de af den dataansvarlige iværksatte tekniske og organisatoriske foranstaltninger ikke var »passende« til at sikre databeskyttelsen.

30. Det fremgår af forordningens artikel 24 og 32, at den dataansvarlige skal tage hensyn til en række vurderingsfaktorer, som er nævnt i disse artikler, og som jeg har erindret om ovenfor, når denne vælger de tekniske og organisatoriske foranstaltninger, som denne skal gennemføre for at sikre, at behandlingen er i overensstemmelse med forordningen.

31. Den dataansvarlige råder over en vis skønsmargen med hensyn til udvælgelsen af de foranstaltninger, som er mest passende på baggrund af dennes specifikke situation, men denne udvælgelse kan under alle omstændigheder være genstand for legalitetskontrol af, hvorvidt de trufne foranstaltninger er i overensstemmelse med alle forpligtelser, som er foreskrevet i forordningen, og formålene med forordningen.

[10] – E. Belisario, G. Riccio og G. Scorza, *GDPR e Normativa Privacy – Commentario*, nævnt ovenfor, s. 380.

[11] – Som jeg vil uddybe i det følgende, kan det første og det fjerde præjudicielle spørgsmål af denne grund kun besvares benægtende. Ingen automatisk mekanisme kan udledes af forordningens bestemmelser: Det forhold, at personoplysninger er blevet videregivet, er i sig selv ikke tilstrækkeligt til at lægge til grund, at de iværksatte tekniske og organisatoriske foranstaltninger ikke er passende, men heller ikke det forhold, at videregivelsen er en følge af handlinger udført af personer, der ikke er en del af den dataansvarliges organisation og ikke er undergivet dennes kontrol, er tilstrækkeligt til at fritage denne for erstatningsansvar.

[12] – L. Bolognini og E. Pelino, *Codice della disciplina privacy*, Giuffrè, 2019, s. 201. EU-lovgiver fjernede sig således fra tanken om, at behandlingssikkerheden skal være baseret på, at der findes forhåndsbestemte sikkerhedsforanstaltninger, og valgte en metode, som benyttes i internationale standarder for risikobaseret styring af informationssystemer, og som går ud på, at der udvælges foranstaltninger til at mindske risici, som ikke er bundet til forhåndskonfigurerede og generelt anvendelige checklister. Det er således nødvendigt at tage udgangspunkt i internationale retningslinjer og standarder. Resultatet af denne risikovurdering bliver derfor bindende, når organisationen træffer beslutninger med henblik på at mindske de identificerede risici og dermed påtager sig et ansvar.

32. Hvad angår bl.a. sikkerhedsforanstaltninger har den dataansvarlige ifølge artikel 32, stk. 1, pligt til at tage hensyn til »det aktuelle tekniske niveau«. Dette indebærer, at det teknologiske niveau af de foranstaltninger, som skal gennemføres, er begrænset til det, som med rimelighed er muligt på det tidspunkt, hvor foranstaltningerne træffes, i den forstand, at en foranstaltnings evne til at forebygge en given risiko derfor skal være afpasset de løsninger, som det aktuelle videnskabelige, tekniske, teknologiske og forskningsmæssige niveau tilbyder, idet der også tages højde for implementeringsomkostningerne, sådan som jeg vil uddybe i det følgende.

33. Bestemte foranstaltninger kan være »passende« på et givet tidspunkt og alligevel omgås af cyberkriminelle, som benytter meget sofistikerede instrumenter, der også er i stand til at omgå sikkerhedsforanstaltninger, der er i overensstemmelse med det aktuelle tekniske niveau.

34. I øvrigt synes det ulogisk at antage, at EU-lovgiver havde til hensigt at pålægge den dataansvarlige at forebygge alle former for brud på persondatasikkerheden, uafhængigt af den omhu, som denne har udvist i forbindelse med udvælgelsen af sikkerhedsforanstaltninger [13].

35. Som anført ovenfor anvender forordningen en tilgang, som fjerner sig fra automatiske mekanismer og pålægger den dataansvarlige en høj ansvarlighed, hvilket dog ikke kan føre til, at denne afskæres fra at påvise, at denne har opfyldt sine forpligtelser på korrekt vis.

36. Ifølge artikel 32, stk. 1, er det endvidere nødvendigt, som sagt, at tage hensyn til »implementeringsomkostningerne« for de konkrete tekniske og organisatoriske foranstaltninger. Heraf følger, at vurderingen af, om disse foranstaltninger er passende, skal være baseret på en afvejning mellem på den ene side den registreredes interesser, som generelt tenderer mod et højere beskyttelsesniveau, og på den anden side den dataansvarliges økonomiske interesser og tekniske kapacitet, der nogle gange tenderer mod et lavere beskyttelsesniveau. Denne afvejning skal opfylde kravene ifølge det almindelige proportionalitetsprincip.

37. På grundlag af en systematisk fortolkning skal det endvidere påpeges, at lovgiver var bekendt med, at angreb på systemer kan finde sted, idet de i artikel 32, stk. 1, litra c), foreslåede foranstaltninger omfatter evnen til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse. Det ville være meningsløst at opregne denne evne blandt de sikkerhedsforanstaltninger, som sikrer et sikkerhedsniveau, der passer til de konkrete risici, hvis det blev antaget, at angreb på systemer i sig selv udgør et bevis for, at foranstaltningerne ikke er passende.

C. Det andet præjudicielle spørgsmål

38. Med det andet præjudicielle spørgsmål ønsker den forelæggende ret nærmere bestemt afklaring af, hvilken genstand og hvilket omfang rettens legalitetskontrol skal have ved vurderingen af, om de tekniske og organisatoriske foranstaltninger, som den dataansvarlige har truffet som omhandlet i forordningens artikel 32, er passende.

39. Henset til de mange forskellige situationer, som kan opstå i virkeligheden, fastsætter forordningen som sagt ingen bindende bestemmelser om udvælgelsen af de tekniske og organisatoriske foranstaltninger, som den dataansvarlige skal træffe for at opfylde kravene i

[13] – Begrebet »passende foranstaltninger« viser utvetydigt, at hensigten ikke var at give alle på et abstrakt plan mulige tekniske og organisatoriske foranstaltninger betydning. Jf. i denne retning M. Gambini, *Responsabilità e risarcimento nel trattamento dei dati personali*, i V. Cuffaro, R. D'Orazio og V. Ricciuto, *I dati personali nel diritto europeo*, Giappichelli, 2019, s. 1059.

forordningen. Vurderingen af, om foranstaltningerne er passende, skal således foretages i hvert enkelt tilfælde, dvs. ved at undersøge, om de specifikke foranstaltninger var passende for med rimelighed at forebygge en given risiko og minimere de negative konsekvenser af det indtrufne brud på persondatasikkerheden.

40. Om end det uden tvivl er sandt, at udvælgelsen og anvendelsen af disse foranstaltninger er overladt til den dataansvarliges subjektive vurdering, fordi de i forordningen nævnte foranstaltninger kun tjener som eksempler, kan rettens legalitetskontrol ikke være begrænset til at undersøge, om den dataansvarlige har opfyldt de forpligtelser, som følger af artikel 24 og 32, dvs. om denne (formelt) har fastsat visse tekniske og organisatoriske foranstaltninger. Retten skal foretage en konkret vurdering af indholdet af disse foranstaltninger, af den måde, hvorpå de er blevet gennemført, og af deres praktiske konsekvenser på grundlag af de fremlagte beviser og omstændighederne i det specifikke tilfælde. Sådan som den portugisiske regering med rette har påpeget, »synes den måde, hvorpå den dataansvarlige har opfyldt sine forpligtelser, ikke at kunne adskilles fra indholdet af de trufne foranstaltninger, når denne på baggrund af den pågældende behandling af personoplysninger (dens karakter, omfang, sammenhæng og formål), det aktuelle tekniske niveau af de tilgængelige teknologier og deres omkostninger samt de potentielle risici for borgernes rettigheder og frihedsrettigheder vil påvise at have gennemført alle foranstaltninger, som er nødvendige og passende for at sikre et sikkerhedsniveau, der passer til den underliggende risiko« [14].

41. Legalitetskontrollen skal derfor tage alle de i artikel 24 og 32 nævnte faktorer i betragtning, idet disse artikler som sagt opregner en række kriterier for at vurdere, om foranstaltningerne er passende, og giver eksempler på foranstaltninger, der kan opfattes som passende. Som understreget af Kommissionen og alle de medlemsstater, der har fremlagt bemærkninger vedrørende det andet spørgsmål, fremhæver artikel 32, stk. 1-3, endvidere behovet for at »sikre et sikkerhedsniveau, der passer til disse risici«, og angiver andre faktorer, som er relevante i denne sammenhæng, herunder den omstændighed, at den dataansvarlige kan overholde en godkendt adfærdskodeks eller en godkendt certificeringsmekanisme som omhandlet i henholdsvis forordningens artikel 40 og artikel 42.

42. Overholdelse af adfærdskodekser eller certificeringsmekanismer kan udgøre en nyttig vurderingsfaktor med henblik på at løfte bevisbyrden og den respektive legalitetskontrol. Det skal dog præciseres, at det ikke er tilstrækkeligt, at den dataansvarlige overholder en adfærdskodeks, men denne skal påvise konkret at have gennemført de i kodeksen fastsatte foranstaltninger i overensstemmelse med ansvarlighedsprincippet. Certificering udgør derimod »i sig selv et bevis for, at behandlingen er i overensstemmelse med forordningen, selv hvis der er mulighed for, at dette bevis kan afkræftes på et praktisk plan« [15].

43. Afslutningsvis skal det påpeges, at disse foranstaltninger om nødvendigt skal revideres og ajourføres i henhold til artikel 24, stk. 1. Også disse aspekter skal være genstand for den nationale rets legalitetsprøvelse. Ifølge forordningens artikel 32, stk. 1 [16], har den dataansvarlige nemlig pligt

[14] – Skriftligt indlæg, punkt 31.

[15] – M. Gambini, *Responsabilità e risarcimento nel trattamento dei dati personali*, nævnt ovenfor, s. 1067. Besiddelse af en certificering fører derfor til omvendt bevisbyrde til gavn for den dataansvarlige, som nemmere kan påvise at have opfyldt de i forordningen fastsatte forpligtelser.

[16] – Litra d) foreskriver udtrykkeligt, at vurderingen af, om foranstaltningerne er passende, også omfatter effektiviteten af de iværksatte foranstaltninger, som skal være genstand for regelmæssig afprøvning, vurdering og evaluering, både i den indledende fase og med jævne mellemrum, med henblik på at sikre den reelle sikkerhed af alle former for behandling uafhængigt af deres risikoniveau, og desuden fastsætter litra c) udtrykkeligt, at de iværksatte tekniske og organisatoriske foranstaltninger skal udvise evnen til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse. Jf. M. Gambini, *Responsabilità e risarcimento nel trattamento dei dati personali*, nævnt ovenfor, s. 1064 og 1065.

til kontinuerligt – dvs. både før, under og efter – at kontrollere og overvåge behandlingen, men også til at revidere og ajourføre de trufne foranstaltninger med henblik på både at forebygge overtrædelser og eventuelt at begrænse konsekvenserne af overtrædelser.

44. Jeg vil dog udelukke, at Domstolen i sin dom skal inkludere en fortegnelse over materielle elementer såsom den af den portugisiske regering foreslåede [17]. Eftersom en sådan fortegnelse aldrig kan være udtømmende, ville dette give plads til modsatrettede fortolkninger.

D. Det tredje præjudicielle spørgsmål

45. Med den første del af det tredje spørgsmål ønsker den forelæggende ret nærmere bestemt oplyst, om bevisbyrden for, at de iværksatte tekniske og organisatoriske foranstaltninger som omhandlet i forordningens artikel 32 er passende, på baggrund af ansvarlighedsprincippet i artikel 5, stk. 2, og artikel 24, sammenholdt med 74. betragtning hertil [18], påhviler den dataansvarlige i forbindelse med et erstatningssøgsmål i henhold til artikel 82.

46. På baggrund af ovenstående overvejelser kan jeg kortfattet besvare dette spørgsmål bekræftende.

47. Forordningens ordlyd, sammenhæng og formål taler nemlig utvetydigt for, at bevisbyrden påhviler den dataansvarlige.

48. Det følger af formuleringen af flere bestemmelser i forordningen, at den dataansvarlige skal »være i stand til at«, dvs. »kunne«, »påvise« at have opfyldt de i forordningen fastsatte forpligtelser, og navnlig at have truffet foranstaltninger, som er passende i denne henseende, sådan som det fremgår af 74. betragtning, artikel 5, stk. 2, og artikel 24, stk. 1. Som den portugisiske regering har påpeget, specificerer ovennævnte 74. betragtning, at den dataansvarlige også skal løfte bevisbyrden for »foranstaltningernes effektivitet«.

49. Denne ordlydsfortolkning understøttes efter min opfattelse af følgende praktiske og teleologiske betragtninger.

50. Hvad angår fordelingen af bevisbyrden i forbindelse med et erstatningssøgsmål i henhold til artikel 82 skal den registrerede, som har anlagt søgsmål mod den dataansvarlige, godtgøre for det første, at forordningen er blevet tilsidesat, for det andet at have lidt skade, og for det tredje, at der findes en årsagssammenhæng mellem disse to omstændigheder, sådan som påpeget i alle skriftlige

[17] – Punkt 30 i det skriftlige indlæg: »Det påhviler den dataansvarlige at påvise at have vurderet alle faktorer og omstændigheder, som kendetegner den pågældende behandling, og navnlig resultatet af den foretagne risikovurdering, de identificerede risici, de konkrete foranstaltninger, som er udvalgt til at mindske disse risici, begrundelsen for udvælgelsen af foranstaltningerne i lyset af de på markedet tilgængelige teknologiske løsninger, foranstaltningernes effektivitet, sammenhængen mellem tekniske og organisatoriske foranstaltninger, uddannelsen af det personale, der medvirker ved behandlingsaktiviteter, den eventuelle outsourcing af behandling af personoplysninger, herunder udvikling og vedligeholdelse af informationsteknologien, den eventuelle kontrol, som foretages af den dataansvarlige, og nøjagtige instrukser til de i medfør af […] artikel 28 [i forordning 2016/679] benyttede personer om, hvordan behandlingen skal udføres, vurderingen af støtteinfrastrukturen for kommunikations- og informationssystemerne samt klassificeringen af risikoniveauet for de registreredes rettigheder og frihedsrettigheder.«

[18] – 74. betragtning anfører: »Der bør fastsættes bestemmelser om den dataansvarliges ansvar, herunder erstatningsansvar, for enhver behandling af personoplysninger, der foretages af den dataansvarlige eller på den dataansvarliges vegne. Den dataansvarlige bør navnlig have pligt til at gennemføre passende og effektive foranstaltninger og til at påvise, at behandlingsaktiviteter overholder denne forordning, herunder foranstaltningernes effektivitet. Disse foranstaltninger bør tage højde for behandlingens karakter, omfang, sammenhæng og formål og risikoen for fysiske personers rettigheder og frihedsrettigheder.«

bemærkninger vedrørende det femte præjudicielle spørgsmål. Det drejer sig om tre kumulative betingelser, sådan som det også fremgår af Domstolens og Rettens faste praksis vedrørende Unionens ansvar uden for kontraktforhold [19].

51. Jeg mener imidlertid, at sagsøgerens pligt til at godtgøre en overtrædelse af forordningen ikke kan gå så langt, at sagsøgeren skal godtgøre, at de af den dataansvarlige gennemførte tekniske og organisatoriske foranstaltninger ikke er passende som omhandlet i artikel 24 og 32.

52. Som Kommissionen har understreget, ville det i virkeligheden være så godt som umuligt at fremlægge sådanne beviser, fordi de registrerede generelt hverken råder over tilstrækkelige kundskaber til at analysere disse foranstaltninger eller har adgang til al den information, som den ansvarlige for den omtvistede behandling er i besiddelse af, navnlig hvad angår de anvendte metoder til sikring af behandlingssikkerheden. Desuden ville den dataansvarlige undertiden kunne hævde, at dennes nægtelse af, at de registrerede modtager oplysninger om disse omstændigheder, er baseret på den legitime grund om ikke at ville offentliggøre interne anliggender eller oplysninger, der er omfattet af tavshedspligt, herunder netop af sikkerhedsgrunde.

53. Såfremt det blev antaget, at bevisbyrden påhviler den registrerede, ville den praktiske konsekvens derfor være, at søgsmålsretten i medfør af artikel 82, stk. 1, ville miste en stor del af sin rækkevidde. Efter min opfattelse ville dette ikke være på linje med EU-lovgivers hensigt, som i forbindelse med vedtagelsen af denne forordning sigtede mod at styrke de registreredes rettigheder og databehandlernes forpligtelser i forhold til direktiv 95/46, som forordningen erstattede. Det er derfor mere logisk, og juridisk holdbart, at den dataansvarlige, når denne vil forsvare sig mod et erstatningssøgsmål, skal påvise at have opfyldt de forpligtelser, som er fastsat i denne forordnings artikel 24 og 32, ved at gennemføre faktisk passende foranstaltninger.

54. Med den anden del af det tredje spørgsmål ønsker den forelæggende ret nærmere bestemt oplyst, om indhentningen af en sagkyndig udtalelse kan anses for et bevismiddel, der er nødvendigt for og tilstrækkeligt til at fastslå, om de tekniske og organisatoriske foranstaltninger, som den dataansvarlige har truffet, var passende i en situation, hvor den uautoriserede adgang til og den uautoriserede videregivelse af personoplysninger skyldtes et »hackerangreb«.

55. Som også den bulgarske regering, den italienske regering, Irland og Kommissionen (i det væsentlige) har understreget, mener jeg, at svaret på disse spørgsmål skal være baseret på Domstolens faste praksis, ifølge hvilken det, når der ikke findes EU-retlige bestemmelser på området, i overensstemmelse med princippet om medlemsstaternes procesautonomi tilkommer den nationale retsorden i hver enkelt medlemsstat at fastsætte de processuelle regler for sagsanlæg til sikring af beskyttelsen af borgernes rettigheder, dog på den betingelse, at disse ikke må være mindre gunstige end dem, som regulerer tilsvarende situationer, der er underlagt national ret (ækvivalensprincippet), og at de i praksis ikke umuliggør eller uforholdsmæssigt vanskeliggør udøvelsen af rettigheder, der er tillagt ved EU-retten (effektivitetsprincippet).

56. Med hensyn til den foreliggende situation skal det konstateres, at forordningen ikke indeholder bestemmelser, der fastsætter, hvilke beviser der er antagelige, og deres bevisværdi, navnlig hvad angår de bevismidler (eksempelvis en sagkyndig udtalelse), som de nationale retter

[19] – Jf. bl.a. Domstolens dom af 5.9.2019, Den Europæiske Union mod Guardian Europe og Guardian Europe mod Den Europæiske Union (C-447/17 P og C-479/17 P, EU:C:2019:672, præmis 147), og af 28.10.2021, Vialto Consulting mod Kommissionen (C-650/19 P, EU:C:2021:879, præmis 138), samt Rettens dom af 13.1.2021, Helbert mod EUIPO (T-548/18, EU:T:2021:4, præmis 116), og af 29.9.2021, Kočner mod Europol (T-528/20, ikke trykt i Sml., EU:T:2021:631, præmis 61), hvor det blev erindret om, at tre betingelser skal være opfyldt, nemlig »at den adfærd, som Unionens institution lægges til last, har været retsstridig, at der foreligger et virkeligt tab, og at der er en årsagssammenhæng mellem denne adfærd og det hævdede tab«.

kan eller skal indhente for at undersøge, om en dataansvarlig har iværksat passende foranstaltninger i overensstemmelse med forordningen. Jeg finder derfor, at det, når der ikke findes EU-retlige bestemmelser på området, tilkommer den nationale retsorden i hver enkelt medlemsstat at fastsætte disse processuelle regler, idet ækvivalensprincippet og effektivitetsprincippet overholdes.

57. Det ovennævnte »effektivitetsprincip«, hvorefter en uafhængig domstol skal foretage en upartisk vurdering, ville kunne undergraves, såfremt adjektivet »tilstrækkelig« blev givet den betydning, som den forelæggende ret tilsyneladende giver det, dvs. at det automatisk på baggrund af en sagkyndig udtalelse kan udledes, at de af den dataansvarlige trufne foranstaltninger var passende [20].

E. Det fjerde præjudicielle spørgsmål

58. Med det fjerde præjudicielle spørgsmål ønsker den forelæggende ret nærmere bestemt oplyst, om forordningens artikel 82, stk. 3, skal fortolkes således, at en overtrædelse af forordningen [bestående som i den konkrete situation i »den uautoriserede videregivelse af« eller »den uautoriserede adgang til« personoplysninger som omhandlet i artikel 4, nr. 12)], som er blevet begået af personer, der ikke er ansatte i den dataansvarliges administration og ikke er undergivet dennes kontrol, udgør en omstændighed, som den dataansvarlige ikke er skyld i, og som kan begrunde en fritagelse for erstatningsansvar i henhold til artikel 82, stk. 3.

59. Svaret på spørgsmålet følger direkte af ovenstående betragtninger om den generelle filosofi, der ligger til grund for forordningen, dvs. at der ikke findes automatiske mekanismer, og at det forhold, at den uautoriserede videregivelse af eller den uautoriserede adgang til personoplysninger er en følge af handlinger udført af personer, der ikke er undergivet den dataansvarliges kontrol, ikke fritager denne fra erstatningsansvar.

60. For det første skal det ud fra en ordlydsmæssig synsvinkel påpeges, at hverken artikel 82, stk. 3, eller 146. betragtning anfører særlige betingelser, som skal være opfyldt, for at den dataansvarlige skal kunne fritages for erstatningsansvar, ud over det forhold, at den pågældende påviser, at denne »ikke er skyld i den begivenhed, der medførte skaden«. Af denne formulering udledes dels, at den dataansvarlige alene kan fritages for erstatningsansvar, såfremt den pågældende påviser, at denne ikke er skyld i den begivenhed, der medførte den konkrete skade, dels, at det i denne bestemmelse påkrævede bevisniveau er højt, fordi der anvendes udtrykket »ikke [på nogen måde] er skyld i« [(o.a.: »in alcun modo«)], sådan som Kommissionen har understreget [21].

61. Ansvarsordningen ifølge artikel 82 og mere generelt ifølge forordningen i sin helhed har været genstand for en intens debat i litteraturen i flere medlemsstater. Denne ordning udviser nemlig særtræk, som er typiske for ansvar uden for kontraktforhold, men også elementer, som ved bestemmelsernes opbygning får den til at nærme sig ansvar i kontraktforhold eller endog en form

[20] – Skriftligt indlæg, punkt 39.

[21] – I overensstemmelse med Domstolens faste praksis, ifølge hvilken undtagelser til en hovedregel skal fortolkes strengt, skal den eventuelle ansvarsfrihed, som følger af artikel 82, stk. 3, ligeledes fortolkes strengt. Jf. analogt dom af 15.10.2020, Association française des usagers de banques (C-778/18, EU:C:2020:831, præmis 53), og af 5.4.2022, Commissioner of An Garda Síochána m.fl. (C-140/20, EU:C:2022:258, præmis 40).

for objektivt ansvar på baggrund af de iboende risici med behandling af personoplysninger. Dette er ikke stedet til at redegøre for denne artikulerede debat, men efter min opfattelse fastsætter artikel 82 ingen ordning for objektivt ansvar [22].

62. Den skade, der er resultatet af et brud på persondatasikkerheden, kan være konsekvensen af uagtsomhed i form af manglende gennemførelse af de tekniske og organisatoriske foranstaltninger, som med rimelighed og under alle omstændigheder var passende for at undgå skaden, under hensyntagen til de risici, som behandlingen medførte for personers rettigheder og frihedsrettigheder. Disse risici bevirker, at pligten til at forebygge og undgå skaden bliver strengere, og udvider pligten for den dataansvarlige til at udvise omhu. Hvis forpligtelserne for de dataansvarlige læses kombineret med bestemmelsen om diskulperende bevis, som kan fremlægges af den person, som har forvoldt skade, er der grundlag for at udlede argumenter, som taler for, at ansvar for ulovlig behandling af personoplysninger i henhold til forordningens artikel 82 har karakter af skærpet ansvar ved formodet uagtsomhed [23].

63. Heraf følger, at den dataansvarlige kan fremlægge et diskulperende bevis (hvilket ikke er tilladt i tilfælde af objektivt ansvar). Hvad angår fordelingen af bevisbyrden fastsætter forordningens artikel 82, stk. 3, en ordning, som er til gavn for den skadelidte, idet der anvendes en form for omvendt bevisbyrde for uagtsomheden udvist af den person, som har forvoldt skade [24], som er fuld ud symmetrisk med den ovennævnte omvendte bevisbyrde for, at de trufne foranstaltninger er passende. Lovgiver var således tilsyneladende bekendt med de farer, som er knyttet til en anderledes fordeling af bevisbyrden i den forstand, at såfremt den fysiske person, som har lidt skade, var forpligtet til at fremlægge bevis for uagtsomheden udvist af den person, som har forvoldt skade, ville den skadelidtes stilling belastes i for høj grad, og effektiviteten af beskyttelsen i form af erstatning i virkeligheden udhules, i en sammenhæng med bestemmelser, som vedrører anvendelsen af nye teknologier. Det ville nemlig være yderst byrdefuldt for den registrerede at rekonstruere og opnå adgang til oplysninger om, hvordan skaden fandt sted, og følgelig at godtgøre den dataansvarliges uagtsomhed. Omvendt er den dataansvarlige bedst i stand til at fremlægge diskulperende bevis for, at den pågældende ikke er skyld i den begivenhed, der medførte skaden [25].

64. På linje med det ovenfor beskrevne ansvarlighedsprincip skal den dataansvarlige også påvise, at den pågældende har gjort, hvad der er muligt for rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger.

65. For at vende tilbage til den forelæggende rets spørgsmål kan det på baggrund af ovenstående overvejelser om karakteren af den dataansvarliges ansvar – idet den dataansvarlige som anført kan fritages for erstatningsansvar, hvis den pågældende påviser, at overtrædelsen følger af en

[22] – Erstatningsansvar kvalificeres tendentielt som objektivt i alle de tilfælde, hvor den person, som udøver en vis handling, har pligt til at træffe alle på et abstrakt plan mulige foranstaltninger for at undgå en skade, uafhængigt af, om denne reelt var bekendt med disse, og uafhængigt af deres økonomiske bæredygtighed. Såfremt den person, som udøver en vis handling, derimod pålægges at iværksætte foranstaltninger, som under normale forhold skal træffes af en erhvervsdrivende i den konkrete økonomiske sektor for at opretholde sikkerheden og for at forebygge de skader, som kan følge af den udførte aktivitet, bevæger tilskrivning af ansvar sig tendentielt mod en ordning for ansvar for specifik uagtsomhed. M. Gambini, *Responsabilità e risarcimento nel trattamento dei dati personali*, nævnt ovenfor, s. 1055.

[23] – M. Gambini, *Responsabilità e risarcimento nel trattamento dei dati personali*, nævnt ovenfor, s. 1059. Jf. analogt hvad angår synspunktet om, at bevis for at have truffet passende foranstaltninger ikke består simpelthen i at hævde at have udvist den fornødne omhu, men i at godtgøre en særskilt skadevoldende begivenhed, som en tredjepart er skyld i, og som udviser de særtræk af uforudsigelighed og uundgåelighed, som kendetegner hændelige omstændigheder og force majeure, S. Sica, *Sub art. 82*, i R. D'Orazio, G. Finocchiaro, O. Pollicino og G. Resta, *Codice della privacy e data protection*, Giuffrè, 2021.

[24] – »[H]vis det *bevises*, at den pågældende ikke er skyld i den begivenhed, der medførte skaden« (artikel 82, stk. 3).

[25] – M. Gambini, *Responsabilità e risarcimento nel trattamento dei dati personali*, nævnt ovenfor, s. 1060.

omstændighed, som denne ikke er skyld i – ikke antages, at den pågældende kan fritages for erstatningsansvar alene af den grund, at begivenheden skyldes en person, der ikke er undergivet dennes kontrol.

66. Når en dataansvarlig er offer for et angreb fra cyberkriminelle, er det muligt, at den skadevoldende begivenhed ikke kan tilregnes den dataansvarlige, men det er ikke udelukket, at det var den dataansvarliges uagtsomhed, der gav anledning til det konkrete angreb, idet det gjorde angrebet lettere, at den dataansvarlige ikke havde gennemført de nødvendige foranstaltninger for at sikre personoplysningssikkerheden, eller at disse foranstaltninger ikke var passende. Det drejer sig om vurderinger af de faktiske omstændigheder, som det tilkommer den nationale ret, ved hvilken søgsmålet er anlagt, i hvert enkelt tilfælde at foretage på grundlag af de fremlagte beviser.

67. Erfaringsmæssigt er eksterne angreb på systemer, der tilhører offentlige eller private organisationer, som behandler store mængder af personoplysninger, langt mere hyppige end interne angreb. Den dataansvarlige skal derfor gennemføre passende foranstaltninger for at modvirke i særdeleshed eksterne angreb.

68. Afslutningsvis skal det ud fra en teleologisk synsvinkel påpeges, at forordningen forfølger et højt beskyttelsesniveau. I denne henseende har Domstolen allerede bemærket, at som det følger af forordningens artikel 1, stk. 2, sammenholdt med 10., 11. og 13. betragtning til denne forordning, pålægger denne forordning EU's institutioner, organer, kontorer og agenturer samt medlemsstaternes kompetente myndigheder at sikre et højt beskyttelsesniveau for de rettigheder, der er knyttet til beskyttelse af alle personoplysninger og er sikret ved artikel 16 TEUF og chartrets artikel 8 [26].

69. Hvis Domstolen foretrak en fortolkning, ifølge hvilken den dataansvarlige automatisk blev fritaget for erstatningsansvar i henhold til artikel 82, stk. 3, såfremt overtrædelsen af forordningen blev begået af en tredjepart, ville en sådan fortolkning have en virkning, som er uforenelig med det med forordningen forfulgte beskyttelsesmål, fordi de registreredes rettigheder i givet fald ville svækkes, idet det omhandlede ansvar ville begrænses til de tilfælde, hvor overtrædelsen blev tilregnet personer, der er undergivet den nævnte dataansvarliges ledelse og/eller kontrol.

F. Det femte præjudicielle spørgsmål

70. Med det femte præjudicielle spørgsmål har den forelæggende ret nærmere bestemt anmodet Domstolen om at fortolke begrebet »ikke-økonomisk skade« (eller »immateriel skade« som omhandlet i forordningens artikel 82). Navnlig skal det afklares, om bestemmelserne i forordningens artikel 82, stk. 1 og 2, sammenholdt med 85. og 146. betragtning hertil [27], skal fortolkes således, at den registreredes frygt for et muligt fremtidigt misbrug af dennes

[26] – Jf. i denne retning dom af 15.6.2021, Facebook Ireland m.fl. (C-645/19, EU:C:2021:483, præmis 44 og 45).

[27] – 85. betragtning anfører: »Et brud på persondatasikkerheden kan, hvis det ikke håndteres på en passende og rettidig måde, påføre fysiske personer fysisk, materiel eller immateriel skade […].« 146. betragtning anfører: »Den dataansvarlige eller databehandleren bør yde erstatning for enhver skade, som en person måtte lide som følge af behandling, der overtræder denne forordning. Den dataansvarlige eller databehandleren bør være fritaget for erstatningsansvar, hvis den pågældende beviser ikke at være ansvarlig for den forvoldte skade. Begrebet »skade« bør fortolkes bredt i lyset af retspraksis ved Domstolen, således at det fuldt ud afspejler formålene for denne forordning. Dette berører ikke eventuelle erstatningskrav for skade som følge af overtrædelse af andre bestemmelser i EU-retten eller medlemsstaternes nationale ret. […] Registrerede bør have fuld erstatning for den skade, som de har lidt. […]«

personoplysninger i sig selv kan udgøre en (ikke-økonomisk) skade, der giver ret til erstatning i et tilfælde, hvor overtrædelsen af forordningen kommer til udtryk ved cyberkriminelles uautoriserede adgang til og uautoriserede videregivelse af personoplysninger.

71. Hverken artikel 82 eller de betragtninger til forordningen, som omhandler erstatning for skade, giver et klart svar på spørgsmålet, men af disse er det muligt at udlede flere elementer, som kan være nyttige i forbindelse med vurderingen, dvs. at den immaterielle (eller ikke-økonomiske) skade kan give ret til erstatning i tillæg til erstatningen for den materielle (eller økonomiske) skade, at overtrædelsen af forordningen ikke automatisk »giver anledning« til en skade, eller nærmere bestemt at bruddet på persondatasikkerheden »kan […] påføre« fysiske personer fysisk, materiel eller immateriel skade, at begrebet »skade« bør fortolkes bredt i lyset af praksis ved Domstolen, således at det fuldt ud afspejler formålene med forordningen, og at disse personer bør have »fuld« erstatning for den skade, som de har »lidt«.

72. Ordlyden af forordningens bestemmelser eliminerer i sig selv antagelsen om, at skaden er indtrådt automatisk og implicit (in re ipsa), idet det primære mål med det erstatningsansvar, som forordningen indfører, nemlig er at fyldestgøre den registrerede, netop gennem en »fuld erstatning« for den skade, som denne har lidt, og herved at genoprette ligevægten i den retsstilling, der blev ændret i negativ retning (skadet) som følge af overtrædelsen af loven [28].

73. Også ud fra en systematisk synsvinkel fastsætter forordningen, lige som kartellovgivningen, to grundpiller for beskyttelse: Beskyttelsesordningens effektivitet sikres ved på den ene side offentlig håndhævelse, hvor overtrædelsen af forordningens bestemmelser medfører sanktioner, og på den anden side privat håndhævelse, som tager udgangspunkt i et erstatningsansvar uden for kontraktforhold, som kan betragtes som skærpet ved formodet uagtsomhed med de ovennævnte særtræk, og hvor der gives mulighed for at fremlægge diskulperende bevis [29].

74. Såfremt begrebet (ikke-økonomisk) »skade« fortolkes udvidende [30], kan denne fortolkning imidlertid ikke gå så langt, at det antages, at lovgiver ville afstå fra behovet for, at det drejer sig om en faktisk »skade«.

75. Den reelle materielle problemstilling er, hvorvidt den registrerede, når det er fastlagt, at en overtrædelse har fundet sted, og der er blevet konstateret en årsagssammenhæng, har ret til erstatning alene på grundlag af den registreredes bekymringer, frygt og angst for et muligt fremtidigt misbrug af dennes personoplysninger, hvis der ikke er blevet konstateret et sådant misbrug, og/eller den registrerede ikke er blevet påført nogen yderligere skade.

76. Hvad angår fortolkningen af begreberne i en EU-retlig bestemmelse følger det i henhold til Domstolens faste praksis, at indholdet af en EU-retlig bestemmelse, som ikke indeholder nogen udtrykkelig henvisning til medlemsstaternes ret med henblik på at fastlægge dens betydning og

[28] – Jf. generaladvokat Campos Sánchez-Bordonas ovennævnte forslag til afgørelse, punkt 29 og fodnote 11. I samme forslag til afgørelse konkluderede generaladvokaten med føje, efter sin bedømmelse ud fra en ordlydsmæssig, historisk, kontekstuel og teleologisk synsvinkel, at de skader for de registrerede, der giver ret til erstatning i henhold til artikel 82, ikke har »karakter af straf« (punkt 27-55), idet generaladvokaten påpegede, at medlemsstaterne »[ikke skal] (og kan reelt heller ikke) vælge mellem mekanismerne i kapitel VIII med henblik på at sikre beskyttelsen af oplysninger. I tilfælde af en overtrædelse, der ikke giver anledning til en skade, har den registrerede stadig (som minimum) ret til at indgive klage til en tilsynsmyndighed«, og at »[u]dsigten til at opnå erstatning uden nogen form for skade [sandsynligvis vil] tilskynde til flere civile søgsmål med krav, som måske ikke altid er begrundede, og kan i denne forbindelse bremse behandlingen af oplysninger« (punkt 54 og 55).

[29] – Såfremt den registrerede nægtes ret til erstatning for svage og forbigående følelser i forbindelse med overtrædelsen af regler om behandlingen, står den pågældende ikke fuldstændig uden retsbeskyttelse (jf. i denne retning generaladvokat Campos Sánchez-Bordonas ovennævnte forslag til afgørelse, punkt 115).

[30] – Eller »bredt« som omhandlet i 146. betragtning.

rækkevidde, normalt i hele EU skal undergives en selvstændig og ensartet fortolkning, som skal søges under hensyntagen til ikke alene bestemmelsens ordlyd, men ligeledes til dens kontekst, det formål, der forfølges med den ordning, som den udgør en del af, og bestemmelsens tilblivelseshistorie [31].

77. Som generaladvokat Campos Sánchez-Bordona erindrede om [32], har Domstolen ikke udarbejdet en generel definition af begrebet »skade«, der finder anvendelse uden forskel på ethvert område [33]. For så vidt angår ikke-økonomiske skader kan følgende udledes af Domstolens praksis: Når et af formålene med den bestemmelse, der fortolkes, er at beskytte enkeltpersoner eller en bestemt kategori af enkeltpersoner [34], bør begrebet skade defineres bredt. Sammenholdt med dette kriterium ydes der også erstatning for immateriel skade, selv om denne skade ikke er nævnt i den bestemmelse, der fortolkes [35].

78. Selv om det i henhold til Domstolens praksis kan gøres gældende, at der i EU-retten som beskrevet ovenfor findes et princip om erstatning for immateriel skade, er jeg enig med generaladvokat Campos Sánchez-Bordona i, at der derimod ikke kan udledes en regel heraf, hvorefter *al* immateriel skade, uanset hvor alvorlig den er, giver ret til erstatning [36].

79. I denne forbindelse er sondringen mellem immateriel skade, der giver ret til erstatning, og andre *ulemper som følge af den manglende overholdelse af loven*, som på grund af deres ubetydelige karakter ikke nødvendigvis giver ret til erstatning, relevant [37].

80. Domstolen har tiltrådt denne sondring, når den har henvist til problemer og gener som en selvstændig kategori i forhold til skader på områder, hvor der efter Domstolens opfattelse bør ydes erstatning for disse [38].

[31] – Jf. dom af 15.4.2021, The North of England P & I Association (C-786/19, EU:C:2021:276, præmis 48), og af 10.6.2021, KRONE – Verlag (C-65/20, EU:C:2021:471, præmis 25).

[32] – Jf. generaladvokat Campos Sánchez-Bordonas ovennævnte forslag til afgørelse, punkt 104.

[33] – Domstolen har heller ikke fastlagt en foretrukken fortolkningsmetode – selvstændig fortolkning eller en fortolkning med henvisning til de nationale lovgivninger: Det afhænger af det område, der er genstand for undersøgelsen. Jf. dom af 10.5.2001, Veedfald (C-203/99, EU:C:2001:258, præmis 27), vedrørende defekte produkter, af 6.5.2010, Walz (C-63/09, EU:C:2010:251, præmis 21), vedrørende luftfartsselskabers erstatningsansvar, eller af 10.6.2021, Van Ameyde España (C-923/19, EU:C:2021:475, præmis 37 ff.), vedrørende erstatningsansvarsordningen for skader, der forvoldes ved færdsel med motorkøretøjer.

[34] – F.eks. forbrugere af produkter eller ofre for trafikulykker.

[35] – Med hensyn til »pakkerejser« dom af 12.3.2002, Leitner (C-168/00, EU:C:2002:163); med hensyn til erstatningsansvar for motorkøretøjer dom af 24.10.2013, Haasová (C-22/12, EU:C:2013:692, præmis 47-50), af 24.10.2013, Drozdovs (C-277/12, EU:C:2013:685, præmis 40), og af 23.1.2014, Petillo (C-371/12, EU:C:2014:26, præmis 35).

[36] – Jf. generaladvokat Campos Sánchez-Bordonas ovennævnte forslag til afgørelse, punkt 105. Domstolen har eksempelvis fastslået, at EU-retten er forenelig med en national lovgivning, der med henblik på beregning af erstatning sondrer mellem immateriel skade i forbindelse med legemsbeskadigelse som følge af en ulykke alt efter ulykkens årsag, jf. dom af 23.1.2014, Petillo (C-371/12, EU:C:2014:26, domskonklusionen): EU-retten er ikke til hinder for »en national lovgivning […], der fastsætter en særlig ordning med erstatning for ikke-økonomiske skader i forbindelse med mindre legemsbeskadigelse som følge af færdselsulykker, og hvorved erstatningen for disse skader er begrænset sammenlignet med den erstatning, der indrømmes for identiske skader, som følger af andre årsager end disse ulykker«.

[37] – Denne sondring findes i nogle nationale lovgivninger som en uundgåelig følgevirkning af samfundslivet. Senest, med hensyn til databeskyttelse, i Italien, Tribunale di Palermo, sez. I civile, sentenza 05/10/2017 n. 5261, samt Cass. Civ., Ord. sez VI, n. 17383/2020. I Tyskland bl.a. AG Diez, 7.11.2018 – 8 C 130/18, LG Karlsruhe, 2.8.2019 – 8 O 26/19, og AG Frankfurt am Main, 10.7.2020 – 385 C 155/19 (70). I Østrig OGH 6 Ob 56/21k.

[38] – Jf. dom af 23.10.2012, Nelson m.fl. (C-581/10 og C-629/10, EU:C:2012:657, præmis 51), med hensyn til sondringen mellem »skader« som omhandlet i artikel 19 i konventionen om indførelse af visse ensartede regler for international luftbefordring, indgået i Montreal den 28.5.1999, og »gener« som omhandlet i forordning nr. 261/2004, som er omfattet af en kompensationsret i henhold til sidstnævntes artikel 7; jf. dom af 19.11.2009, Sturgeon m.fl. (C-402/07 og C-432/07, EU:C:2009:716). Ligesom inden for passagerbefordring til søs og på indre vandveje, som er omhandlet i forordning nr. 1177/2010, har EU-lovgiver på dette område kunnet anerkende en abstrakt kategori, eftersom det element, der skaber problemet, og dets essens er det samme for alle de berørte parter. Denne følgeslutning er efter min opfattelse ikke mulig på området for databeskyttelse.

81. Empirisk kan det konstateres, at enhver overtrædelse af en bestemmelse om beskyttelse af personoplysninger som regel skaber en negativ reaktion hos den registrerede. En erstatning, der alene er baseret på en følelse af ubehag i forbindelse med andres manglende overholdelse af loven, kan let forveksles med en erstatning uden skade, hvilket som sagt ikke synes at være omfattet af den i forordningens artikel 82 omhandlede situation.

82. Under de i hovedsagen foreliggende omstændigheder er det forhold, at misbruget af personoplysninger kun er hypotetisk og ikke faktisk, tilstrækkeligt til at lægge til grund, at den registrerede har lidt en ikke-økonomisk skade som følge af overtrædelsen af forordningen, forudsat at denne godtgør, at angsten for dette misbrug reelt og specifikt har forvoldt denne en faktisk og reel følelsesmæssig skade [39].

83. Grænsen mellem simpel utilfredshed (som ikke er erstatningsberettiget) og reel immateriel skade (som er erstatningsberettiget) er vag, men de nationale retter, som har til opgave i hvert enkelt tilfælde at opstille denne grænse, bør foretage en nøje vurdering af alle elementer fremlagt af den registrerede, som har fremsat erstatningskravet, og som da har pligt til – i detaljer og ikke alene på generel vis – at frembringe konkrete elementer, hvoraf det kan konkluderes, at bruddet på persondatasikkerheden har givet anledning til en »faktisk ikke-økonomisk skade«, dog uden at denne pligt antager karakteren af en forhåndsbestemt tærskel for særlig belastning, idet det væsentlige er, at det ikke drejer sig om en simpel subjektiv følelse, der er foranderlig og også afhænger af personlighedsmæssige og individuelle særtræk, men at det drejer sig om en objektiv gene, som godt kan være let, men som skal kunne godtgøres, for personens fysiske eller psykiske sfære eller sociale liv, hvor karakteren af de omfattede personoplysninger og deres betydning i den registreredes liv og endog den opfattelse, der til enhver tid hersker i samfundet hvad angår den specifikke gene, som følger af bruddet på persondatasikkerheden, er af betydning [40].

IV. Forslag til afgørelse

84. På baggrund af alle ovenstående betragtninger foreslår jeg Domstolen at besvare de præjudicielle spørgsmål på følgende måde:

»Artikel 5, 24, 32 og 82 i Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse) skal fortolkes således, at

det forhold, at et »brud på persondatasikkerheden« som omhandlet i denne forordnings artikel 4, nr. 12), har fundet sted, i sig selv ikke er tilstrækkeligt til at lægge til grund, at de af den dataansvarlige iværksatte tekniske og organisatoriske foranstaltninger ikke er »passende« til at sikre beskyttelsen af de omfattede personoplysninger.

Ved vurderingen af, om de af den dataansvarlige trufne tekniske og organisatoriske foranstaltninger er passende, skal den nationale ret, ved hvilken søgsmålet er anlagt, foretage en bedømmelse, som inkluderer en konkret vurdering af indholdet af disse foranstaltninger, af den måde, hvorpå de er blevet gennemført, og af deres praktiske konsekvenser.

[39] – Efter Irlands opfattelse er disse overvejelser særlig vigtige i virkeligheden med hensyn til cyberkriminalitet, for hvis enhver, der – om end i et begrænset omfang – bliver genstand for en overtrædelse, skulle have ret til erstatning for immaterielle skader, ville dette øve en kraftig indflydelse, navnlig på de dataansvarlige inden for den offentlige sektor, som finansieres med begrænsede offentlige midler og snarere burde forfølge kollektive interesser, herunder forbedringen af personoplysningssikkerheden (skriftligt indlæg, punkt 72).

[40] – Jf. generaladvokat Campos Sánchez-Bordonas ovennævnte forslag til afgørelse, punkt 116.

I forbindelse med et erstatningssøgsmål i henhold til forordningens artikel 82 har den dataansvarlige pligt til at påvise, at den pågældende har iværksat foranstaltninger, som er passende som omhandlet i denne forordnings artikel 32.

I overensstemmelse med princippet om medlemsstaternes procesautonomi tilkommer det den nationale retsorden i hver enkelt medlemsstat at fastsætte, hvilke beviser der er antagelige, og deres bevisværdi, herunder de bevismidler, som de nationale retter kan eller skal indhente for at undersøge, om en dataansvarlig har iværksat passende foranstaltninger i henhold til forordningen, idet ækvivalensprincippet og effektivitetsprincippet i EU-retten overholdes.

Det forhold, at den overtrædelse af denne forordning, som har givet anledning til den konkrete skade, er blevet begået af en tredjepart, udgør i sig selv ingen grund til at fritage den dataansvarlige for erstatningsansvar, og for at kunne fraskrive sig erstatningsansvar i medfør af denne bestemmelse har den dataansvarlige pligt til at påvise, at den pågældende ikke er skyld i overtrædelsen.

Den af den registrerede godtgjorte gene, der består i angst for et muligt fremtidigt misbrug af dennes personoplysninger, kan udgøre en ikke-økonomisk skade, der giver ret til erstatning, forudsat at denne godtgør at have lidt en faktisk og reel følelsesmæssig skade, hvilket det tilkommer den nationale ret, ved hvilken søgsmålet er anlagt, i hvert enkelt tilfælde at undersøge.«