Rättsfallssamlingen

FÖRSLAG TILL AVGÖRANDE AV GENERALADVOKAT
GIOVANNI PITRUZZELLA
föredraget den 27 april 2023 [1]

Mål C-340/21

VB
mot
Natsionalna agentsia za prihodite

(begäran om förhandsavgörande från Varhoven administrativen sad (Högsta förvaltningsdomstolen, Bulgarien))

”Begäran om förhandsavgörande – Skydd av personuppgifter – Förordning (EU) 2016/679 – Den personuppgiftsansvariges ansvar – Säkerhet i samband med behandlingen – Personuppgiftsincident – Ideell skada på grund av den personuppgiftsansvariges passivitet – Skadeståndstalan”

Kan den omständigheten att personuppgifter som finns hos en myndighet blir föremål för olaglig spridning genom ett it-angrepp ge rätt till ersättning för den ideella skada som en registrerad gör gällande enbart av det skälet att den registrerade är rädd för att dennes personuppgifter kan komma att missbrukas i framtiden? På grundval av vilka kriterier kan den personuppgiftsansvarige hållas ansvarig? Hur ska bevisbördan fördelas mellan parterna i målet? Vilken är omfattningen av domstolsprövningen?

I. Tillämpliga bestämmelser

1. I artikel 4, som har rubriken ”Definitioner”, i förordning 2016/679 [2] (nedan kallad förordningen) stadgas följande:

”I denna förordning avses med

…

12. *personuppgiftsincident*: en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats,

[1] Originalspråk: italienska.

[2] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).

…”

2. I artikel 5, som har rubriken ”Principer för behandling av personuppgifter”, föreskrivs följande:

”1. Vid behandling av personuppgifter ska följande gälla:

…

f) De ska behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna, inbegripet skydd mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse, med användning av lämpliga tekniska eller organisatoriska åtgärder (*integritet och konfidentialitet*).

2. Den personuppgiftsansvarige ska ansvara för och kunna visa att punkt 1 efterlevs (*ansvarsskyldighet*).”

3. I artikel 24 i samma förordning, som har rubriken ”Den personuppgiftsansvariges ansvar”, fastställs följande:

”1. Med beaktande av behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att behandlingen utförs i enlighet med denna förordning. Dessa åtgärder ska ses över och uppdateras vid behov.

2. Om det står i proportion till behandlingen, ska de åtgärder som avses i punkt 1 omfatta den personuppgiftsansvariges genomförande av lämpliga strategier för dataskydd.

3. Tillämpningen av godkända uppförandekoder som avses i artikel 40 eller godkända certifieringsmekanismer som avses i artikel 42 får användas för att visa att den personuppgiftsansvarige fullgör sina skyldigheter.”

4. I artikel 32, som har rubriken ”Säkerhet i samband med behandlingen”, föreskrivs följande:

”1. Med beaktande av den senaste utvecklingen, genomförandekostnaderna och behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige och personuppgiftsbiträdet vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken, inbegripet, när det är lämpligt

…

2. Vid bedömningen av lämplig säkerhetsnivå ska särskild hänsyn tas till de risker som behandling medför, i synnerhet från oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.

3. Anslutning till en godkänd uppförandekod som avses i artikel 40 eller en godkänd certifieringsmekanism som avses i artikel 42 får användas för att visa att kraven i punkt 1 i den här artikeln följs.

…”

5. I artikel 82 i samma förordning, som har rubriken ”Ansvar och rätt till ersättning”, stadgas följande:

”1. Varje person som har lidit materiell eller immateriell skada till följd av en överträdelse av denna förordning ska ha rätt till ersättning från den personuppgiftsansvarige eller personuppgiftsbiträdet för den uppkomna skadan.

2. Varje personuppgiftsansvarig som medverkat vid behandlingen ska ansvara för skada som orsakats av behandling som strider mot denna förordning. …

3. Den personuppgiftsansvarige eller personuppgiftsbiträdet ska undgå ansvar enligt punkt 2 om den visar att den inte på något sätt är ansvarig för den händelse som orsakade skadan.”

II. De faktiska omständigheterna, det nationella målet och tolkningsfrågorna

6. Den 15 juli 2019 avslöjades i de bulgariska medierna att det hade skett obehörig åtkomst till informationssystemet hos Natsionalna agentsia za prihodite (Nationella skattemyndigheten, Bulgarien) (nedan kallad skattemyndigheten [3]) och att uppgifter om skatter och avgifter och socialförsäkring avseende flera miljoner personer, både bulgariska och utländska medborgare, hade publicerats på internet.

7. Ett stort antal personer, däribland VB som är klagande i det nationella målet, väckte talan mot skattemyndigheten och yrkade ersättning för ideell skada.

8. I det nu aktuella fallet väckte VB talan mot skattemyndigheten vid Administrativen sad Sofia-grad (Förvaltningsdomstolen i Sofia, Bulgarien) (nedan kallad ASSG). VB gjorde gällande att skattemyndigheten hade överträtt de nationella bestämmelserna och åsidosatt sin skyldighet som personuppgiftsansvarig att behandla personuppgifterna på ett sätt som ”säkerställer lämplig säkerhet” genom att vidta lämpliga tekniska och organisatoriska åtgärder i enlighet med artiklarna 24 och 32 i förordning 2016/679. VB gjorde vidare gällande att hon hade lidit ideell skada som yttrade sig i oro och farhågor för att hennes personuppgifter skulle komma att missbrukas i framtiden.

9. Skattemyndigheten påpekade å sin sida att VB inte hade begärt någon information om exakt vilka personuppgifter som hade utsatts för intrång. Efter avslöjandet av intrånget hade skattemyndigheten dessutom sammankallat till möten med experter för att skydda medborgarnas rättigheter och intressen. Enligt skattemyndigheten fanns det inget orsakssamband mellan it-angreppet och den påstådda skadan, eftersom skattemyndigheten hade infört alla processhanteringssystem och ledningssystem för informationssäkerhet i enlighet med de gällande internationella standarderna på området.

[3] Den nationella skattemyndigheten är personuppgiftsansvarig i den mening som avses i artikel 4.7 i förordningen. Enligt nationell rätt är skattemyndigheten en specialiserad myndighet som är underordnad finansministern och har ansvar för att fastställa, säkerställa och driva in offentliga fordringar och privatpersoners i lag föreskrivna skulder till staten. Skattemyndigheten behandlar personuppgifter när den utövar sina offentliga befogenheter.

10. ASSG ogillade talan med den motiveringen att skattemyndigheten inte på något sätt var ansvarig för spridningen av uppgifterna, att VB hade bevisbördan för att de vidtagna åtgärderna inte var lämpliga och slutligen att VB inte hade lidit någon ersättningsgill ideell skada.

11. VB överklagade denna dom till den hänskjutande domstolen, Varhoven administrativen sad (Högsta förvaltningsdomstolen, Bulgarien). Till stöd för sitt överklagande gjorde hon gällande att ASSG hade gjort en felaktig uppdelning av bevisbördan när det gällde att bevisa att det inte hade vidtagits säkerhetsåtgärder. Hon anförde vidare att det inte borde vara nödvändigt att bevisa en ideell skada, eftersom denna skada är faktisk och inte bara hypotetisk.

12. Skattemyndigheten gjorde i sin tur gjort gällande att den i egenskap av personuppgiftsansvarig hade vidtagit de nödvändiga tekniska och organisatoriska åtgärderna. Skattemyndigheten anförde dessutom att VB inte hade styrkt att hon faktiskt hade lidit ideell skada. Oro och farhågor är nämligen känslomässiga tillstånd som inte är ersättningsgilla.

13. Den hänskjutande domstolen har i sin begäran om förhandsavgörande angett att varje enskild talan som de skadelidande, var och en för sig, väckte mot skattemyndigheten med yrkande om ersättning för ideell skada gav skilda resultat.

14. Mot denna bakgrund har den hänskjutande domstolen beslutat att vilandeförklara målet och hänskjuta följande tolkningsfrågor till EU-domstolen för förhandsavgörande:

”1. Ska artiklarna 24 och 32 i [Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning)] tolkas på så sätt att det är tillräckligt att personer som inte är anställda vid den personuppgiftsansvariga myndigheten och inte står under dennas kontroll har gjort sig skyldiga till obehörigt röjande av eller obehörig åtkomst till personuppgifter i den mening som avses i artikel 4 led 12 i förordning (EU) 2016/679, för att de tekniska och organisatoriska åtgärderna ska anses inte vara lämpliga?

2. Om fråga 1 besvaras nekande, vad ska vara föremål för domstolens laglighetsprövning och i vilken omfattning ska prövningen göras när domstolen undersöker huruvida de tekniska och organisatoriska åtgärder som den personuppgiftsansvariga myndigheten har vidtagit är lämpliga enligt artikel 32 i förordning (EU) 2016/679?

3. Om fråga 1 besvaras nekande, ska principen om ansvarsskyldighet enligt artiklarna 5.2 och 24 jämförda med skäl 74 i förordning (EU) 2016/679 tolkas på så sätt att när en talan väcks enligt artikel 82.1 i förordning (EU) 2016/679 har den personuppgiftsansvariga myndigheten bevisbördan för att de tekniska och organisatoriska åtgärder enligt artikel 32 i förordningen som har vidtagits är lämpliga? Kan ett sakkunnigutlåtande anses utgöra nödvändig och tillräcklig bevisning för att fastställa huruvida de tekniska och organisatoriska åtgärder som den personuppgiftsansvariga myndigheten vidtagit varit lämpliga i ett sådant fall som det förevarande, om den obehöriga åtkomsten till och det obehöriga röjandet av personuppgifter är en följd av ett ’it-angrepp’?

4. Ska artikel 82.3 i förordning (EU) 2016/679 tolkas på så sätt att det obehöriga röjandet av eller den obehöriga åtkomsten till personuppgifter i den mening som avses i artikel 4 led 12 i förordning (EU) 2016/679, så som i förevarande fall genom ett it-angrepp som utförts av personer som inte är anställda vid den personuppgiftsansvariga myndigheten och inte står

under dess kontroll, utgör en omständighet för vilken den personuppgiftsansvariga myndigheten inte på något sätt är ansvarig och vilken gör det möjligt att undanta denna från ersättningsansvar?

5. Ska artikel 82.1 och 82.2 jämförd med skälen 85 och 146 i förordning (EU) 2016/679 tolkas på så sätt att, i ett sådant fall som det förevarande där det skett en kränkning av skyddet av personuppgifter, vilken tar sig uttryck i obehörig åtkomst till och spridning av personuppgifter genom ett it-angrepp, enbart den berörda personens oro, farhågor och rädsla för att personuppgifter kan missbrukas i framtiden omfattas av begreppet immateriell skada, vilket ska tolkas extensivt och därmed ger rätt till skadeersättning, om sådant missbruk inte har fastställts och/eller ingen ytterligare skada har åsamkats den berörda personen?”

III. Rättslig bedömning

A. Inledande överväganden

15. Förevarande mål gäller intressanta och till viss del nya frågor om tolkningen av flera bestämmelser i förordningen. [4]

16. De fem tolkningsfrågorna rör alla samma frågeställning, närmare bestämt under vilka förutsättningar en person har rätt till ersättning för ideell skada om dennes personuppgifter, som finns hos en myndighet, har publicerats på internet till följd av ett it-angrepp.

17. För att underlätta bedömningen kommer jag att föreslå ett kortfattat separat svar på varje tolkningsfråga i begäran om förhandsavgörande, även om jag är medveten om att en viss begreppsmässig överlappning förekommer, i och med att de första fyra frågorna alla syftar till att identifiera under vilka förutsättningar den personuppgiftsansvarige kan hållas ansvarig för överträdelsen av bestämmelserna i förordningen, [5] medan den femte frågan närmare bestämt gäller begreppet ersättningsgill ideell skada. [6]

18. Jag vill påpeka att flera mål som rör artikel 82 i förordningen för närvarande pågår vid EU-domstolen. I ett av dessa mål har generaladvokaten redan föredragit sitt förslag till avgörande, som jag kommer att beakta i min bedömning. [7]

[4] Artikel 5.2 (angående principen om personuppgiftsbiträdens ansvarsskyldighet), artikel 24 (om de åtgärder som den personuppgiftsansvarige ska vidta för att säkerställa att behandlingen utförs i enlighet med förordningen), artikel 32 (om nämnda skyldighet med specifikt avseende på säkerhet i samband med behandlingen) och artikel 82.1–82.3 (om ersättning för skada på grund av en överträdelse av denna förordning och om möjligheten för den personuppgiftsansvarige att vidta åtgärder för att säkerställa att förordningen efterlevs), utöver skälen 74, 85 och 146 som har samband med de nämnda artiklarna.

[5] a) Den första frågan gäller huruvida den omständigheten att systemen blir föremål för intrång räcker för att de vidtagna åtgärderna inte ska anses vara lämpliga. b) Den andra frågan avser i vilken omfattning prövningen ska göras när en domstol undersöker huruvida nämnda åtgärder är lämpliga. c) Den tredje frågan gäller bevisbördan med avseende på frågan huruvida nämnda åtgärder är lämpliga och vissa tekniska bestämmelser för bevisupptagning. d) Den fjärde frågan avser huruvida den omständigheten att systemangreppet sker utifrån är av relevans för ansvarsfrihet.

[6] Vad gäller de anförda bestämmelserna i förordningen rör de första tre frågorna aspekterna om den personuppgiftsansvariges ansvar för att de åtgärder som vidtas är lämpliga (artiklarna 5, 24 och 32), medan den fjärde och den femte frågan rör förutsättningarna för ansvarsfrihet respektive begreppet ersättningsgill ideell skada (artikel 82).

[7] Se förslag till avgörande av generaladvokaten Campos Sánchez-Bordona i målet Österreichische Post (Ideell skada på grund av behandling av personuppgifter) (C-300/21, EU:C:2022:756).

19. Innan tolkningsfrågorna prövas finner jag det vara angeläget att göra några inledande anmärkningar om principerna i och syftena med förordningen som kommer att vara av betydelse för svaret på de enskilda tolkningsfrågorna.

20. I artikel 24 i förordningen fastställs det i allmänna ordalag att den personuppgiftsansvarige ska genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att personuppgifter behandlas i enlighet med förordningen, medan samma skyldighet vad gäller säkerheten i samband med behandlingen specificeras mer i detalj i artikel 32. I artiklarna 24 och 32 behandlas artikel 5.2 mer ingående, vilken bland ”principerna för behandling av personuppgifter” inför just ”principen om ansvarsskyldighet”. Denna princip kompletterar och följer logiskt av ”principen om integritet och konfidentialitet” i artikel 5.1 f. Båda dessa principer ska läsas mot bakgrund av det riskbaserade förhållningssätt som förordningen bygger på.

21. Principen om ansvarsskyldighet är en av förordningens hörnstenar och en av dess mest betydelsefulla förnyelser. Enligt denna princip ska den personuppgiftsansvarige vidta proaktiva åtgärder för att säkerställa och kunna visa att behandlingen utförs i enlighet med förordningen. [8]

22. I doktrinen har detta beskrivits som en reell kulturell förändring till följd av den ”allmänna räckvidden av ansvarsskyldigheten”. [9] Det är inte det formella uppfyllandet av ett lagstadgat krav eller av en specifik åtgärd, utan snarare hela den strategi som organisationen har infört som kan undanta den personuppgiftsansvarige från ansvar, förutsatt att den aktuella strategin är i överensstämmelse med bestämmelserna om dataskydd.

23. De tekniska och organisatoriska åtgärder som krävs enligt principen om ansvarsskyldighet ska vara ”lämpliga” med beaktande av de faktorer som nämns i artikel 24: behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter.

24. Enligt artikel 24 ska åtgärderna därför vara lämpliga när det gäller att kunna visa att behandlingen utförs i enlighet med principerna och bestämmelserna i förordningen.

25. Artikel 32 projicerar emellertid principen om ansvarsskyldighet på de konkreta åtgärder som ska vidtas för att säkerställa ”en säkerhetsnivå som är lämplig i förhållande till risken”. De faktorer som ska beaktas vid fastställande av de tekniska och organisatoriska åtgärderna utvidgas därvidlag till att även omfatta den senaste utvecklingen och genomförandekostnaderna.

26. Begreppet lämpliga åtgärder erfordrar att de lösningar som används för att skydda informationssystem uppnår en acceptabel nivå både tekniskt sett (åtgärdernas relevans) och kvalitativt sett (skyddets effektivitet). För att säkerställa iakttagandet av principerna om nödvändighet, relevans och proportionalitet ska behandlingen inte bara vara lämplig, utan även tillfredsställande i förhållande till de eftersträvade syftena. Utifrån ett sådant synsätt spelar principen om uppgiftsminimering en avgörande roll. Enligt denna princip ska alla faser av behandlingen av personuppgifter ständigt sträva efter att minimera datasäkerhetsrisken. [10]

[8] C. Docksey, Article 24. Responsibility of the controller, i C. Kuner, L.A. Bygrave, C. Docksey, L. Drechsler, *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford University Press, 2020, s. 561. De principer och skyldigheter som fastställs i bestämmelserna om skydd av personuppgifter bör kännetecknа den kulturella strukturen hos organisationerna på alla nivåer, snarare än uppfattas som en rad lagstadgade krav som deras juridikavdelning ska bocka av.

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

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

27. Hela förordningen präglas av riskförebyggande och den personuppgiftsansvariges ansvarsskyldighet och därmed av ett teleologiskt synsätt som eftersträvar det bästa möjliga resultatet ur effektivitetssynpunkt. Med andra ord långt ifrån ett formalistiskt synsätt enligt vilket det räcker att det finns en skyldighet att iaktta specifika procedurer för att undgå ansvar. [11]

28. Artikel 24 innehåller ingen uttömmande förteckning över ”lämpliga” åtgärder. Bedömningen ska således göras i varje enskilt fall. Detta är helt i linje med tanken bakom förordningen, enligt vilken valet av de förfaranden som ska tillämpas helst ska ske mot bakgrund av en noggrann bedömning av den specifika situationen, så att dessa förfaranden är så effektiva som möjligt. [12]

B. Den första tolkningsfrågan

29. Den hänskjutande domstolen har ställt den första tolkningsfrågan i huvudsak för att få klarhet i huruvida artiklarna 24 och 32 i förordningen ska tolkas på så sätt att den omständigheten att det har inträffat en ”personuppgiftsincident” enligt definitionen i artikel 4.12 i sig är tillräcklig för att dra slutsatsen att de tekniska och organisatoriska åtgärder som den personuppgiftsansvarige har vidtagit inte var ”lämpliga” för att säkerställa dataskyddet.

30. Det framgår av artiklarna 24 och 32 i förordningen att den personuppgiftsansvarige ska beakta en rad bedömningsfaktorer som nämns i dessa artiklar, och som jag har anfört ovanför, när denne väljer de tekniska och organisatoriska åtgärder som denne ska vidta för att säkerställa att behandlingen utförs i enlighet med förordningen.

31. Den personuppgiftsansvarige förfogar över ett visst utrymme för skönsmässig bedömning vad gäller att fastställa vilka åtgärder som är lämpligast mot bakgrund av dennes specifika situation. Detta val kan dock under alla omständigheter vara föremål för domstolsprövning av huruvida de tillämpade åtgärderna är i överensstämmelse med alla skyldigheter enligt förordningen och förordningens syften.

32. Vad gäller bland annat säkerhetsåtgärder är den personuppgiftsansvarige enligt artikel 32.1 skyldig att beakta ”den senaste utvecklingen”. Detta innebär att den teknologiska nivån på de åtgärder som ska vidtas begränsas till vad som rimligen är möjligt vid den tidpunkt då åtgärderna genomförs. En åtgärds förmåga att förebygga en viss risk ska därför vara anpassad till de lösningar som den senaste utvecklingen inom vetenskap, teknik, teknologi och forskning erbjuder, varvid det även tas hänsyn till genomförandekostnaderna, såsom kommer att framgå bättre i det följande.

33. Vissa åtgärder kan vara ”lämpliga” vid en given tidpunkt men trots detta kringgås av cyberbrottslingar som använder väldigt sofistikerade instrument i stånd till att även komma förbi säkerhetsåtgärder som är i överensstämmelse med den senaste utvecklingen.

[11] Såsom kommer att framgå bättre i det följande kan den första och den fjärde tolkningsfrågan av detta skäl inte besvaras på annat sätt än nekande. Ingen automatisk mekanism kan härledas ur bestämmelserna i förordningen: enbart det faktum att personuppgifter har röjts är inte tillräckligt för att de tekniska och organisatoriska åtgärder som har vidtagits inte ska anses vara lämpliga, men inte heller den omständigheten att röjandet är en följd av handlingar som har utförts av personer som befinner sig utanför den personuppgiftsansvariges organisation och inte står under dennes kontroll är tillräcklig för att undanta denne från ansvar.

[12] L. Bolognini, E. Pelino, *Codice della disciplina privacy*, Giuffrè, 2019, s. 201. Unionslagstiftaren tog således avstånd från tanken om att säkerhet i samband med behandlingen ska vara baserad på att det finns förutbestämda säkerhetsåtgärder och valde en metod som tillämpas i internationella standarder om riskbaserad styrning av informationssystem. Denna metod går ut på att det fastställs åtgärder för att dämpa riskerna som inte är bundna till förkonfigurerade och allmänt tillämpliga kontrollistor. Det är således nödvändigt att ta utgångspunkt i internationella riktlinjer och standarder. Resultatet av denna riskbedömning blir därför bindande när organisationen fattar beslut i syfte att dämpa de identifierade riskerna och därmed åtar sig ett ansvar.

34. Vidare förefaller det vara ologiskt att anta att unionslagstiftaren hade för avsikt att ålägga den personuppgiftsansvarige skyldigheten att förebygga alla sorters personuppgiftsincidenter, oberoende av den omsorg som denne har visat i samband med fastställandet av säkerhetsåtgärder. [13]

35. Förordningen tillämpar ett synsätt som tar avstånd från automatiska mekanismer och ålägger den personuppgiftsansvarige en hög ansvarsskyldighet, vilket dock inte får medföra att denne fråntas möjligheten att visa att denne har fullgjort sina skyldigheter på ett korrekt sätt.

36. Enligt artikel 32.1 är det dessutom nödvändigt att beakta ”genomförandekostnaderna” för de aktuella tekniska och organisatoriska åtgärderna. Därav följer att bedömningen av huruvida dessa åtgärder är lämpliga ska grunda sig på en avvägning mellan å ena sidan den registrerades intressen, som i allmänhet tenderar att gå mot en högre skyddsnivå, och å andra sidan den personuppgiftsansvariges ekonomiska intressen och teknologiska kapacitet, som ibland tenderar att gå mot en lägre skyddsnivå. I samband med denna avvägning ska kraven enligt den allmänna proportionalitetsprincipen iakttas.

37. Inom ramen för en systematisk tolkning ska det vidare påpekas att lagstiftaren var medveten om att intrång i system trots allt kan inträffa. Bland de åtgärder som föreslås i artikel 32.1 c finns förmågan att återställa tillgängligheten och tillgången till personuppgifter i rimlig tid vid en fysisk eller teknisk incident. Det skulle vara meningslöst att räkna upp denna förmåga bland de säkerhetsåtgärder som säkerställer en säkerhetsnivå som är lämplig i förhållande till risken, för det fall intrång i system i sig självt ansågs utgöra tillräckligt bevis för att åtgärderna inte är lämpliga.

C. Den andra tolkningsfrågan

38. Genom den andra tolkningsfrågan önskar den hänskjutande domstolen närmare bestämt få klarhet i vad som ska vara föremål för domstolsprövning och i vilken omfattning prövningen ska göras när en domstol undersöker huruvida de tekniska och organisatoriska åtgärder som den personuppgiftsansvarige har vidtagit är lämpliga enligt artikel 32 i förordningen.

39. Med tanke på de många olika situationer som kan uppstå i praktiken innehåller förordningen inga bindande bestämmelser om fastställandet av de tekniska och organisatoriska åtgärder som den personuppgiftsansvarige ska vidta för att uppfylla kraven i förordningen. Bedömningen av huruvida åtgärderna är lämpliga ska således göras i varje enskilt fall. Det ska följaktligen undersökas om de specifika åtgärderna var lämpliga för att rimligen förebygga den aktuella risken och minimera de negativa konsekvenserna av personuppgiftsincidenten.

40. Det stämmer visserligen att valet och tillämpningen av dessa åtgärder har överlåtits åt den personuppgiftsansvariges subjektiva bedömning, eftersom de åtgärder som nämns i förordningen enbart tjänar som exempel, men domstolsprövningen får inte vara begränsad till att undersöka om den personuppgiftsansvarige har fullgjort de skyldigheter som följer av artiklarna 24 och 32, det vill säga om denne (formellt) har fastställt vissa tekniska och organisatoriska åtgärder. Den handläggande domstolen ska genomföra en konkret bedömning av innehållet av dessa åtgärder, av det sätt på vilka de har tillämpats och av deras praktiska konsekvenser mot bakgrund av

[13] Begreppet lämpliga åtgärder visar otvetydigt att avsikten inte var att tillmäta alla abstrakt möjliga tekniska och organisatoriska åtgärder betydelse. Se, för ett liknande resonemang, M. Gambini, Responsabilità e risarcimento nel trattamento dei dati personali, i V. Cuffaro, R. D’Orazio, V. Ricciuto, *I dati personali nel diritto europeo*, Giappichelli, 2019, s. 1059.

tillgänglig bevisning och omständigheterna i det specifika fallet. Såsom den portugisiska regeringen med fog har påpekat ”förefaller det sätt på vilket den personuppgiftsansvarige har fullgjort sina skyldigheter inte kunna skiljas från innehållet av de vidtagna åtgärderna, när nämnda personuppgiftsbiträde, mot bakgrund av den specifika behandlingen av personuppgifter (behandlingens art, omfattning, sammanhang och ändamål), den senaste utvecklingen av de tillgängliga teknologierna och deras kostnader samt de tänkbara riskerna för medborgarnas rättigheter och friheter, vill visa att denne har vidtagit alla åtgärder som är nödvändiga och passande för att säkerställa en säkerhetsnivå som är lämplig i förhållande till den bakomliggande risken”. [14]

41. I samband med domstolsprövningen ska därför alla faktorer beaktas som anges i artiklarna 24 och 32 vilka, som nämnts ovan, listar en rad kriterier för att bedöma huruvida åtgärderna är lämpliga och ger exempel på åtgärder som kan anses vara lämpliga. Såsom påpekats av kommissionen och alla medlemsstater som har inkommit med yttranden till domstolen angående den andra frågan, understryks i artikel 32.1–32.3 dessutom behovet att ”säkerställa en säkerhetsnivå som är lämplig i förhållande till risken” och anges andra faktorer som är relevanta i detta sammanhang, däribland den omständigheten att den personuppgiftsansvarige kan ansluta sig till en godkänd uppförandekod eller en godkänd certifieringsmekanism som avses i artikel 40 respektive artikel 42 i förordningen.

42. Anslutningen till uppförandekoder eller certifieringsmekanismer kan utgöra en användbar bedömningsfaktor med avseende på uppfyllande av bevisbördan och den förknippade domstolsprövningen. Det ska dock preciseras att det inte är tillräckligt att den personuppgiftsansvarige ansluter sig till en uppförandekod, utan denne har bevisbördan för att denne konkret har vidtagit de åtgärder som föreskrivs i denna kod, i enlighet med principen om ansvarsskyldighet. Certifiering utgör däremot ”i sig själv ett bevis för att behandlingen har utförts i enlighet med förordningen, även om sådan bevisning kan motsägas i praktiken”. [15]

43. Slutligen ska det påpekas att dessa åtgärder ska ses över och uppdateras vid behov i enlighet med artikel 24.1. Även dessa aspekter ska vara föremål för domstolsprövning. Enligt artikel 32.1 i förordningen [16] har den personuppgiftsansvarige nämligen en skyldighet att ständigt, det vill säga både före, under och efter, kontrollera och övervaka behandlingen, men även att se över och uppdatera de vidtagna åtgärderna i syfte att både förebygga intrång och eventuellt att begränsa konsekvenserna av intrång.

[14] Skriftligt yttrande, punkt 31.

[15] M. Gambini, *Responsabilità e risarcimento nel trattamento dei dati* personali, nämnd ovan, s. 1067. Innehav av en certifiering leder därför till en omvänd bevisbörda till fördel för den personuppgiftsansvarige, som lättare kan visa att denne har fullgjort de skyldigheter som föreskrivs i förordningen.

[16] I led d föreskrivs det uttryckligen att bedömningen av huruvida åtgärderna är lämpliga även omfattar effektiviteten hos de vidtagna åtgärderna, som regelbundet ska testas, undersökas och utvärderas, både i den inledande fasen och med jämna mellanrum, i syfte att säkerställa den faktiska säkerheten hos alla sorters behandling, oavsett deras risknivå. Vidare föreskrivs det uttryckligen i led c att de vidtagna tekniska och organisatoriska åtgärderna ska utvisa förmågan att återställa tillgängligheten och tillgången till personuppgifter i rimlig tid vid en fysisk eller teknisk incident. Se M. Gambini, Responsa*bilità e risarcimento nel trattamento dei dati personali*, a.a., s. 1064 och 1065.

44. Jag är dock benägen att utesluta att domstolen i sin dom ska inkludera en förteckning över materiella uppgifter såsom den som den portugisiska regeringen har föreslagit.[17] I och med att en sådan förteckning aldrig kan vara uttömmande, skulle det ge utrymme för motstridiga tolkningar.

D. Den tredje tolkningsfrågan

45. Genom den första delen av den tredje frågan önskar den hänskjutande domstolen närmare bestämt få klarhet i huruvida den personuppgiftsansvarige, mot bakgrund av principen om ansvarsskyldighet enligt artiklarna 5.2 och artikel 24 jämförda med skäl 74[18] i förordningen, när en skadeståndstalan väcks enligt artikel 82 har bevisbördan för att de tekniska och organisatoriska åtgärder enligt artikel 32 som har vidtagits är lämpliga.

46. Mot bakgrund av vad jag redan anfört ovan kan jag kortfattat svara jakande på denna fråga.

47. Förordningens ordalydelse, sammanhang och syften talar nämligen otvetydigt för att den personuppgiftsansvarige har bevisbördan.

48. Det framgår av formuleringen av flera bestämmelser i förordningen att den personuppgiftsansvarige ska ”kunna” eller ”ha förmåga” att ”visa” att denne har fullgjort de skyldigheter som fastställs i förordningen, och i synnerhet vidtagit åtgärder som är lämpliga i detta hänseende, såsom anförs i skäl 74, artikel 5.2 och artikel 24.1. Som den portugisiska regeringen har påpekat specificeras det i ovannämnda skäl 74 att personuppgiftsansvariga även har bevisbördan för att visa de aktuella ”åtgärdernas effektivitet”.

49. Denna bokstavstolkning understöds enligt min mening av följande praktiska och teleologiska överväganden.

50. Vad gäller fördelningen av bevisbördan när en skadeståndstalan väcks enligt artikel 82 ska den registrerade som har väckt talan mot den personuppgiftsansvarige påvisa för det första att det har skett en överträdelse av förordningen, för det andra att han eller hon har lidit skada och för det tredje att det finns ett orsakssamband mellan de två föregående omständigheterna, såsom det har betonats i alla skriftliga yttranden om den femte tolkningsfrågan. Det rör sig om tre kumulativa villkor, såsom även framgår av domstolens och tribunalens fasta praxis om unionens utomobligatoriska skadeståndsansvar.[19]

[17] Punkt 30 i det skriftliga yttrandet: ”Det ankommer på den personuppgiftsansvarige att visa att denne har bedömt alla faktorer och omständigheter som kännetecknar den aktuella behandlingen, särskilt resultatet av den utförda riskanalysen, de identifierade riskerna, de konkreta åtgärder som har fastställts för att dämpa dessa risker, motiveringen av valet av åtgärderna mot bakgrund av de teknologiska lösningar som är tillgängliga på marknaden, åtgärdernas effektivitet, sambandet mellan tekniska och organisatoriska åtgärder, utbildningen av personal som deltar i behandling, eventuell utlokalisering av behandling av personuppgifter, inklusive utveckling och underhåll av informationstekniken, eventuell kontroll som genomförs av den personuppgiftsansvarige och noggranna instruktioner som ges till de personer som anlitas för behandlingen i enlighet med artikel 28 i förordningen om hur de sistnämnda ska behandla personuppgifter, bedömningen av stödinfrastrukturen för kommunikations- och informationssystem och klassificeringen av risknivån för registrerades rättigheter och friheter.”

[18] I skäl 74 anges följande: ”Personuppgiftsansvariga bör åläggas ansvaret för all behandling av personuppgifter som de utför eller som utförs på deras vägnar. Personuppgiftsansvariga bör särskilt vara skyldiga att vidta lämpliga och effektiva åtgärder och kunna visa att behandlingen är förenlig med denna förordning, även vad gäller åtgärdernas effektivitet. Man bör inom dessa åtgärder beakta behandlingens art, omfattning, sammanhang och ändamål samt risken för fysiska personers rättigheter och friheter.”

[19] Se, bland annat, domstolens dom av den 5 september 2019, Europeiska unionen/Guardian Europe (C-447/17 P och C-479/17 P, EU:C:2019:672, punkt 147), och dom av den 28 oktober 2021, Vialto Consulting/kommissionen (C-650/19 P, EU:C:2021:879, punkt 138), samt tribunalens dom av den 13 januari 2021, Helbert/EUIPO (T-548/18, EU:T:2021:4, punkt 116), och dom av den 29 september 2021, Kočner/Europol (T-528/20, ej publicerad, EU:T:2021:631, punkt 61), där det påpekades att tre villkor ska vara uppfyllda, nämligen ”att det handlande som läggs unionens institution till last är rättsstridigt, att den åberopade skadan är faktisk och att det finns ett orsakssamband mellan institutionens rättsstridiga handlande och den åberopade skadan”.

51. Jag finner emellertid att kärandens skyldighet att visa att det har skett en överträdelse av förordningen inte kan sträcka sig så långt att denne ska visa att de tekniska och organisatoriska åtgärder som den personuppgiftsansvarige har vidtagit inte är lämpliga i den mening som avses i artiklarna 24 och 32.

52. Som kommissionen har understrukit skulle det i praktiken vara så gott som omöjligt att lägga fram sådan bevisning, eftersom de registrerade i allmänhet varken förfogar över tillräckliga kunskaper för att analysera dessa åtgärder eller har tillgång till all information som den ansvarige för den omtvistade behandlingen innehar, däribland vad gäller de metoder som har tillämpats för att säkerställa behandlingens säkerhet. Dessutom skulle den personuppgiftsansvarige ibland kunna hävda att dennes vägran att yppa dessa omständigheter för de registrerade bygger på det berättigade skälet att inte vilja offentliggöra sina interna angelägenheter eller uppgifter som omfattas av tystnadsplikt, däribland just av säkerhetsskäl.

53. För det fall den registrerade ansågs ha bevisbördan skulle den praktiska följden bli att rätten att väcka talan enligt artikel 82.1 skulle mista en stor del av sin räckvidd. Enligt min uppfattning skulle detta inte vara i linje med unionslagstiftarens avsikter, som antog denna förordning för att stärka de registrerades rättigheter och personuppgiftsbiträdenas skyldigheter jämfört med direktiv 95/46, som förordningen ersatte. Det är därför mer logiskt, och rättsligt försvarbart, att den personuppgiftsansvarige, för sitt försvar i samband med en skadeståndstalan, ska visa att denne har fullgjort de skyldigheter som föreskrivs i artiklarna 24 och 32 i denna förordning genom att vidta åtgärder som verkligen är lämpliga.

54. Genom den andra delen av den tredje frågan önskar den hänskjutande domstolen närmare bestämt få klarhet i huruvida ett sakkunnigutlåtande kan anses utgöra nödvändig och tillräcklig bevisning för att fastställa huruvida de tekniska och organisatoriska åtgärder som den personuppgiftsansvarige har vidtagit varit lämpliga i ett fall där den obehöriga åtkomsten till och det obehöriga röjandet av personuppgifter är en följd av ett it-angrepp.

55. Som den bulgariska regeringen, den italienska regeringen, Irland och kommissionen (i allt väsentligt) har understrukit anser jag att svaret på dessa frågor ska baseras på EU-domstolens fasta praxis, enligt vilken det i avsaknad av unionsbestämmelser på området ankommer på varje medlemsstat att i enlighet med principen om medlemsstaternas processuella autonomi i sin rättsordning fastställa de processuella regler som gäller för talan som syftar till att säkerställa skyddet av enskildas rättigheter. Dessa regler får emellertid varken vara mindre förmånliga än dem som avser liknande situationer som grundas på nationell rätt (likvärdighetsprincipen) eller medföra att det i praktiken blir omöjligt eller svårt att utöva de rättigheter som följer av unionens rättsordning (effektivitetsprincipen).

56. I förevarande fall vill jag betona att förordningen inte innehåller någon bestämmelse där det fastställs vilka bevismedel som är tillåtna och deras bevisvärde, däribland i fråga om den bevisning (exempelvis ett sakkunnigutlåtande) som de nationella domstolarna kan eller måste inhämta för att bedöma huruvida en personuppgiftsansvarig har vidtagit lämpliga åtgärder i enlighet med förordningen. Jag anser därför att, eftersom det saknas unionsbestämmelser på området, ankommer det på varje medlemsstat att i sin interna rättsordning fastställa dessa processuella regler, under förutsättning att principerna om likvärdighet och effektivitet iakttas.

57. Ovannämnda ”effektivitetsprincip”, som innebär att en oavhängig domstol ska genomföra en opartisk bedömning, skulle kunna undermineras om adjektivet ”tillräcklig” gavs den betydelse som den hänskjutande domstolen tycks tillmäta det, det vill säga att det automatiskt av ett

sakkunnigutlåtande går att dra slutsatsen att de åtgärder som den personuppgiftsansvarige har vidtagit var lämpliga. [20]

E. Den fjärde tolkningsfrågan

58. Den hänskjutande domstolen har ställt den fjärde tolkningsfrågan i huvudsak för att få klarhet i huruvida artikel 82.3 i förordningen ska tolkas på så sätt att en överträdelse av förordningen (bestående, såsom i förevarande fall, i ”obehörigt röjande av” eller ”obehörig åtkomst” till personuppgifter i den mening som avses i artikel 4.12) som har begåtts av personer som inte är anställda av den personuppgiftsansvarige och inte står under dennes kontroll utgör en omständighet som inte kan tillskrivas den personuppgiftsansvarige och därmed utgör en ansvarsfrihetsgrund enligt artikel 82.3.

59. Svaret på frågan följer linjärt av ovanstående överväganden rörande den allmänna tanken bakom förordningen. Det finns inga automatiska mekanismer och enbart den omständigheten att obehörigt röjande av eller obehörig åtkomst till personuppgifter är en följd av handlingar som har utförts av personer som inte står under den personuppgiftsansvariges kontroll undantar inte denne från ansvar.

60. För det första ska det ur en bokstavlig synvinkel påpekas att det varken i artikel 82.3 eller skäl 146 anges särskilda villkor som medför att den personuppgiftsansvarige kan undgå ansvar om de är uppfyllda, bortsett från att den personuppgiftsansvarige visar att ”den inte på något sätt är ansvarig för den händelse som orsakade skadan”. Ur denna formulering härleds det dels att den personuppgiftsansvarige endast kan undgå ansvar om personuppgiftsbiträdet visar att denne inte på något sätt är ansvarig för den händelse som orsakade den aktuella skadan, dels att den bevisnivå som krävs enligt denna bestämmelse är hög, eftersom det däri används uttrycket ”inte på något sätt”, såsom kommissionen har understrukit. [21]

61. Ansvarssystemet enligt artikel 82, och mer allmänt enligt förordningen i sin helhet, har varit föremål för livlig debatt inom flera medlemsstaters doktrin. Detta system utvisar nämligen särdrag som är typiska för utomobligatoriskt skadeståndsansvar, men även kännetecken som i bestämmelsernas uppbyggnad kan jämföras med ansvar i avtalsförhållanden eller till och med en typ av strikt ansvar mot bakgrund av de inneboende riskerna med behandling av personuppgifter. Detta är inte rätt plats för att redogöra för diskussionen på området, men enligt min uppfattning fastställs det i artikel 82 inte något system för strikt ansvar. [22]

62. Den skada som uppkommer vid en personuppgiftsincident kan följa av oaktsamhet i form av att de tekniska och organisatoriska åtgärder inte har vidtagits som rimligen och under alla omständigheter var lämpliga för att undvika skadan, med hänsyn tagen till de risker för personers rättigheter och friheter som behandlingen medför. Dessa risker gör att skyldigheten att förebygga

[20] Skriftligt yttrande, punkt 39.

[21] I överensstämmelse med domstolens fasta praxis, enligt vilken undantag från en allmän regel ska tolkas restriktivt, ska eventuell ansvarsfrihet som följer av artikel 82.3 likaledes tolkas restriktivt. Se, analogt, dom av den 15 oktober 2020, Association française des usagers de banques (C-778/18, EU:C:2020:831, punkt 53), och dom av den 5 april 2022, Commissioner of An Garda Síochána m.fl. (C-140/20, EU:C:2022:258, punkt 40).

[22] Skadeståndsansvar tenderar att kvalificeras som strikt ansvar i alla de fall då den person som gör en viss handling är skyldig att vidta alla åtgärder som på ett abstrakt plan är möjliga för att undvika en skada, oberoende av om denne faktiskt kände till dessa eller av deras ekonomiska hållbarhet. Om den person som gör en viss handling däremot åläggs att vidta åtgärder som i normala fall ska tillämpas av en operatör i den aktuella ekonomiska sektorn för att upprätthålla säkerheten och förebygga de skador som kan uppstå vid den utförda verksamheten, tenderar åläggandet av ansvaret för skadan att röra sig mot ett ansvarssystem för specifik oaktsamhet. M. Gambini, *Responsabilità e risarcimento nel trattamento dei dati personali*, a.a., s. 1055.

och undvika skadan stärks och utvidgar omsorgsplikten för den personuppgiftsansvarige. Om de skyldigheter som åläggs personuppgiftsansvariga tolkas i kombination med bestämmelsen om friande bevis som ska läggas fram av den person som orsakar skadan kan det leda till argument som talar för att ansvaret för olaglig behandling av personuppgifter enligt artikel 82 i förordningen ska anses ha karaktär av skärpt ansvar för förmodad oaktsamhet. [23]

63. Av detta följer att den personuppgiftsansvarige får lägga fram friande bevis (vilket inte är tillåtet vid strikt ansvar). Vad gäller fördelningen av bevisbördan fastställs det ett system i artikel 82.3 i förordningen som är till förmån för den skadelidande, i och med att det tillämpas en sorts omvänd bevisbörda för den skadevållande personens oaktsamhet, [24] fullt symmetriskt med ovannämnda omvända bevisbörda för att de vidtagna åtgärderna är lämpliga. Lagstiftaren tycks således ha varit medveten om de faror som är förknippade med en annorlunda fördelning av bevisbördan. För det fall den fysiska person som har lidit skada skulle vara skyldig att lägga fram bevis för den skadevållande personens oaktsamhet, skulle den skadelidandes ställning betungas i för stor omfattning och effektiviteten av skyddet i form av ersättning därigenom i praktiken undergrävas, i ett sammanhang med bestämmelser som rör användning av nya teknologier. Det skulle i själva verket vara ytterst betungande för den registrerade att rekonstruera och få tillgång till uppgifter om hur skadan har uppkommit och, följaktligen, att påvisa den personuppgiftsansvariges oaktsamhet. Däremot är den personuppgiftsansvarige mest lämpad att lägga fram friande bevis för att denne inte på något sätt är ansvarig för den händelse som orsakade skadan. [25]

64. I linje med den ovan beskrivna principen om ansvarsskyldighet ska den personuppgiftsansvarige även visa att denne har gjort allt denne har kunnat för att återställa tillgängligheten och tillgången till personuppgifter i rimlig tid.

65. För att återgå till den hänskjutande domstolens fråga kan det mot bakgrund av ovanstående överväganden angående karaktären av den personuppgiftsansvariges ansvar – i och med att den personuppgiftsansvarige kan undgå ansvar genom att visa att överträdelsen följer av en omständighet som den personuppgiftsansvarige inte på något sätt är ansvarig för – inte anses att denne kan undgå ansvar enbart av det skälet att händelsen har förorsakats av en person som inte står under dennes kontroll.

66. När en personuppgiftsansvarig blir utsatt för ett angrepp av cyberbrottslingar skulle det kunna antas att den skadevållande händelsen inte kan tillskrivas den personuppgiftsansvarige, men det är inte uteslutet att det var den personuppgiftsansvariges oaktsamhet som låg till grund för det aktuella angreppet och underlättade angreppet till följd av att denne inte hade vidtagit de nödvändiga säkerhetsåtgärderna för att säkerställa skyddet av personuppgifterna eller att dessa åtgärder inte var lämpliga. Det rör sig om en bedömning av de faktiska omständigheterna som det ankommer på den nationella domstol som prövar en talan att göra i varje enskilt fall mot bakgrund av tillgänglig bevisning.

[23] M. Gambini, *Responsabilità e risarcimento nel trattamento dei dati personali*, a.a., s. 1059. Se analogt, vad gäller uppfattningen att det för att bevisa att det har vidtagits lämpliga åtgärder inte räcker att påstå att det har visats prov på nödvändig omsorg, utan ska påvisas en skadevållande handling av tredje parter med de särdrag om oförutsebarhet och oundviklighet som kännetecknar tillfälligheter och force majeure, S. Sica, Sub art. 82, i R. D'Orazio, G. Finocchiaro, O. Pollicino, G. Resta, *Codice della privacy e data protection*, Giuffrè, 2021.

[24] ”om den *visar* att den inte på något sätt är ansvarig för den händelse som orsakade skadan” (artikel 82.3).

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

67. Erfarenheten visar att externa angrepp mot system tillhörande offentliga eller privata organisationer som behandlar stora mängder personuppgifter är mycket vanligare än interna angrepp. Den personuppgiftsansvarige ska därför vidta lämpliga åtgärder för att motverka i synnerhet externa angrepp.

68. Avslutningsvis ska det ur en teleologisk synvinkel noteras att förordningen eftersträvar en hög skyddsnivå. I detta hänseende har domstolen redan betonat att unionens institutioner, organ och byråer samt medlemsstaternas behöriga myndigheter genom förordningen ges i uppgift – vilket följer av artikel 1.2 jämförd med skälen 10, 11 och 13 i förordningen – att säkerställa en hög skyddsnivå för de rättigheter som har samband med skydd av personuppgifter och garanteras i artikel 16 FEUF och artikel 8 i stadgan. [26]

69. Om domstolen skulle föredra en tolkning enligt vilken den personuppgiftsansvarige automatiskt undgår ansvar enligt artikel 82.3 i fall där överträdelsen av förordningen har begåtts av tredje parter, skulle en sådan tolkning ha en verkan som är oförenlig med det skyddsmål som eftersträvas med förordningen, eftersom de registrerades rättigheter i så fall försvagas, i och med att det aktuella ansvaret begränsas till de fall där överträdelsen kan tillskrivas personer som står under nämnda den personuppgiftsansvariges ledning och/eller kontroll.

F. Den femte tolkningsfrågan

70. Genom den femte tolkningsfrågan har EU-domstolen i huvudsak ombetts att tolka begreppet ideell skada (som i förordningen benämns ”immateriell” skada) i den mening som avses i artikel 82 i förordningen). Närmare bestämt ska det klargöras huruvida artikel 82.1 och 82.2, jämförd med skälen 85 och 146 i förordningen [27], ska tolkas på så sätt att, i ett sådant fall där överträdelsen av förordningen tar sig uttryck i obehörig åtkomst till och obehörigt röjande av personuppgifter från cyberbrottslingars sida, kan den registrerades rädsla för att dennes personuppgifter kan komma missbrukas i framtiden i sig utgöra en ersättningsgill (ideell) skada.

71. Varken artikel 82 eller skälen i förordningen angående ersättning för skada ger ett klart svar på frågan, men ur dessa kan flera faktorer härledas som är till hjälp vid bedömningen, nämligen följande: att ersättning för ideell skada kan utgå vid sidan av ersättning för ekonomisk skada, att överträdelsen av förordningen inte automatiskt ”ger upphov” till en skada, eller närmare bestämt att personuppgiftsincidenten ”kan leda till” fysisk, ekonomisk eller ideell skada för fysiska personer, att begreppet skada bör tolkas ”brett” mot bakgrund av domstolens rättspraxis på ett sätt som fullt ut återspeglar förordningens mål och att ersättningen för den skada som dessa personer har ”lidit” ska vara ”full och effektiv”.

72. Ordalydelsen i förordningens bestämmelser innebär i sig att man kan avfärda eventuella påståenden om att det skulle vara fråga om presumerad skada (*in re ipsa*). Det främsta syftet med det skadeståndsansvar som införs genom förordningen är nämligen att gottgöra den registrerade,

[26] Se, för ett liknande resonemang, dom av den 15 juni 2021, Facebook Ireland m.fl. (C-645/19, EU:C:2021:483, punkterna 43 och 44).

[27] I skäl 85 anges följande: ”En personuppgiftsincident som inte snabbt åtgärdas på lämpligt sätt kan för fysiska personer leda till fysisk, materiell eller immateriell skada …” Av skäl 146 framgår följande: ”Den personuppgiftsansvarige eller personuppgiftsbiträdet bör ersätta all skada som en person kan komma att lida till följd av behandling som strider mot denna förordning. Den personuppgiftsansvarige eller personuppgiftsbiträdet bör dock befrias från skadeståndsskyldighet om den kan visa att den inte på något sätt är ansvarig för skadan. Begreppet skada bör tolkas brett mot bakgrund av domstolens rättspraxis på ett sätt som fullt ut återspeglar denna förordnings mål. Detta påverkar inte skadeståndsanspråk till följd av överträdelser av andra bestämmelser i unionsrätten eller i medlemsstaternas nationella rätt. … Registrerade bör få full och effektiv ersättning för den skada de lidit …”

just genom en ”full och effektiv” ersättning för den skada som han eller hon har lidit och följaktligen att återställa jämvikten i den rättsliga situation som rubbats på ett negativt sätt på grund av överträdelsen av lagstiftningen. [28]

73. Även ur en systematisk synvinkel fastställs det i förordningen, på samma sätt som i konkurrensrätten, två hörnstenar som skyddet bygger på. Skyddssystemets effektivitet säkerställs genom å ena sidan offentlig tillämpning, där överträdelse av bestämmelserna i förordningen leder till påföljder, och å andra sidan privat tillämpning, som just föreskriver ett utomobligatoriskt skadeståndsansvar, som kan betecknas som skärpt för förmodad oaktsamhet med ovannämnda särdrag, och där det bereds tillfälle att lägga fram friande bevis. [29]

74. För det fall begreppet (ideell) skada tolkas extensivt [30] kan denna tolkning emellertid inte sträcka sig så långt att det antas att lagstiftaren ville frångå kravet på att det är fråga om en faktisk ”skada”.

75. Den egentliga materiella frågeställningen är huruvida den registrerade, när det har fastställts att en överträdelse har skett och det har konstaterats ett orsakssamband, har rätt till ersättning enbart på grund av den registrerades oro, farhågor och rädsla för att dennes personuppgifter kan komma att missbrukas i framtiden, om sådant missbruk inte har fastställts och/eller ingen ytterligare skada har åsamkats den registrerade.

76. När det gäller tolkningen av begreppen i en unionsbestämmelse framgår det av domstolens fasta praxis att ordalydelsen i en unionsbestämmelse som inte innehåller någon uttrycklig hänvisning till medlemsstaternas rättsordningar för fastställandet av bestämmelsens innebörd och tillämpningsområde i regel ska ges en självständig och enhetlig tolkning inom hela unionen, varvid inte bara lydelsen ska beaktas, utan också sammanhanget och de mål som eftersträvas med de föreskrifter som bestämmelsen ingår i samt bestämmelsens tillkomsthistoria. [31]

77. Som generaladvokaten Campos Sánchez-Bordona har erinrat om [32] har domstolen inte utvecklat någon allmän definition av begreppet skada som är tillämplig inom alla områden. [33] Vad beträffar ideell skada följer följande av domstolens praxis: När ett av syftena med den bestämmelse

[28] Se ovannämnda förslag till avgörande av generaladvokaten Campos Sánchez-Bordona (punkt 29 och fotnot 11). I samma förslag till avgörande drog generaladvokaten med fog, efter sin bedömning ur en bokstavlig, historisk, systematisk och teleologisk synvinkel, slutsatsen att ersättningsgill skada för de registrerade enligt artikel 82 inte är av ”straffliknande” karaktär (punkterna 27–55). Generaladvokaten påpekade dels att ”[d]et finns ingen anledning för medlemsstaterna att välja mellan mekanismerna i kapitel VIII för att säkerställa skyddet av uppgifter (och de får i själva verket inte heller göra det). Vid en överträdelse som inte ger upphov till skada, har den registrerade fortfarande (åtminstone) rätt att lämna in ett klagomål till en tillsynsmyndighet”, dels att ”[e]n möjlighet att erhålla ersättning oavsett eventuella skador skulle sannolikt främja civilrättsliga tvister där en talan kanske inte alltid är motiverad. Samtidigt skulle det kunna avskräcka från att behandla personuppgifter” (punkterna 54 och 55).

[29] Att ersättning nekas för svaga och övergående känslor till följd av överträdelser av regler om behandling innebär därför inte att den registrerade blir helt skyddslös (se, för ett liknande resonemang, ovannämnda förslag till avgörande av generaladvokaten Campos Sánchez-Bordona, punkt 115).

[30] Eller ”brett” enligt lydelsen i skäl 146.

[31] Se dom av den 15 april 2021, The North of England P & I Association (C-786/19, EU:C:2021:276, punkt 48), och dom av den 10 juni 2021, KRONE – Verlag (C-65/20, EU:C:2021:471, punkt 25).

[32] Se ovannämnda förslag till avgörande av generaladvokat Campos Sánchez-Bordona (punkt 104).

[33] Domstolen har heller inte angett någon tolkningsmetod – självständig eller genom hänvisning till de nationella rättsordningarna – som i första hand bör tillämpas, utan denna är beroende av vilket område som är föremål för prövning. Se dom av den 10 maj 2001, Veedfald (C-203/99, EU:C:2001:258, punkt 27), rörande produkter med säkerhetsbrister, dom av den 6 maj 2010, Walz (C-63/09, EU:C:2010:251, punkt 21), rörande lufttrafikföretags skadeståndsansvar, eller dom av den 10 juni 2021, Van Ameyde España (C-923/19, EU:C:2021:475, punkt 37 och följande punkter), rörande civilrättsligt skadeståndsansvar som ska tillämpas vid trafikolyckor.

som tolkas är att skydda individen, eller en viss kategori av individer,[34] bör begreppet skada ges en vid definition. I överensstämmelse med detta kriterium omfattar skadeståndet ideell skada, även om sådan skada inte nämns i den tolkade bestämmelsen.[35]

78. Trots att domstolens rättspraxis gör det möjligt att mot denna bakgrund hävda att det föreligger en princip om ersättning för ideell skada i unionsrätten, delar jag generaladvokaten Campos Sánchez-Bordonas uppfattning om att det ur detta inte kan härledas en regel som innebär att *all* ideell skada är ersättningsgill, oavsett svårighetsgrad.[36]

79. I detta sammanhang är det lämpligt att göra skillnad mellan ideell skada som är ersättningsgill och *andra olägenheter som är en följd av bristande respekt för vad som är lagligt*, vilka på grund av sin ringa omfattning inte nödvändigtvis ger rätt till ersättning.[37]

80. Domstolen har godtagit denna skillnad när den har tagit upp problem och olägenheter som utgör en kategori som är självständig i förhållande till kategorin skador, inom områden där den anser att dessa ska kompenseras.[38]

81. Empiriskt kan det noteras att varje överträdelse av en bestämmelse om skydd av personuppgifter som regel ger upphov till en negativ reaktion från den registrerades sida. En ersättning som enbart grundar sig på en känsla av missnöje på grund av att någon annan inte har efterlevt lagen är lätt att förväxla med en ersättning utan skada, vilket, såsom har nämnts, inte förefaller föreskrivas med avseende på den situation som avses i artikel 82 i förordningen.

82. Under de omständigheter som föreligger i det nationella målet är den omständigheten att missbruket av personuppgifter enbart är hypotetiskt, och inte faktiskt, tillräcklig för att anse att den registrerade kan ha lidit en ideell skada till följd av överträdelsen av förordningen, under förutsättning att den registrerade visar att rädslan för detta missbruk konkret och specifikt har vållat honom eller henne en faktisk och säker emotionell skada.[39]

[34] Till exempel konsumenter av produkter eller skadelidande i trafikolyckor.

[35] Inom området paketresor, dom av den 12 mars 2002, Leitner (C-168/00, EU:C:2002:163), inom området civilrättsligt ansvar för motorfordon, dom av den 24 oktober 2013, Haasová (C-22/12, EU:C:2013:692, punkterna 47–50), dom av den 24 oktober 2013, Drozdovs (C-277/12, EU:C:2013:685, punkt 40), och dom av den 23 januari 2014, Petillo (C-371/12, EU:C:2014:26, punkt 35).

[36] Se ovannämnda förslag till avgörande av generaladvokaten Campos Sánchez-Bordona (punkt 105). Domstolen har exempelvis slagit fast att unionsrätten inte utgör hinder för en nationell lagstiftning som vid beräkningen av ersättningen gör skillnad mellan olika typer av ideell skada som är följden av personskador orsakade av olyckor beroende på vad som orsakat olyckan. Se dom av den 23 januari 2014, Petillo (C-371/12, EU:C:2014:26, domslutet): Unionsrätten utgör inte hinder för ”en nationell lagstiftning … enligt vilken ett särskilt system för ersättning för immateriella skador som är följden av lindriga personskador, vilka orsakats av trafikolyckor, begränsar ersättningen för dessa skador i förhållande till den ersättning som beviljas för identiska skador som är följden av andra händelser än trafikolyckor”.

[37] En sådan åtskillnad finns i vissa nationella rättsordningar, som en oundviklig följd av samhällslivet. Se nyligen, när det gäller området dataskydd, i Italien, Tribunale di Palermo, sez. I civile, sentenza 05/10/2017 nr. 5261, samt Cass Civ. Ord. Sez 6, nr. 17383/2020. I Tyskland bland annat AG Diez, 07.11.2018-8 C-130/18; LG Karlsruhe, 02.08.2019-8 O 26/19; och AG Frankfurt am Main, 10.07.2020 -385 C-155/19 (70). I Österrike, OGH 6 Ob 56/21k.

[38] Se dom av den 23 oktober 2012, Nelson m.fl. (C-581/10 och C-629/10, EU:C:2012:657, punkt 51), rörande skillnaden mellan ”skador” i den mening som avses i artikel 19 i konventionen om vissa enhetliga regler för internationella lufttransporter, som ingicks i Montreal den 28 maj 1999, och ”olägenheter” i den mening som avses i förordning nr 261/2004, vilka är ersättningsgilla enligt artikel 7 i den förordningen, enligt dom av den 19 november 2009, Sturgeon m.fl. (C-402/07 och C-432/07, EU:C:2009:716). Inom detta område, liksom inom området passagerartrafik till sjöss eller på inre vattenvägar som förordning nr 1177/2010 handlar om, har lagstiftaren kunnat identifiera en abstrakt kategori tack vare att den faktor som ger upphov till problemet, och dess väsentliga innehåll, är identiska för alla som berörs. Jag anser inte att det går att dra en sådan slutsats när det gäller området dataskydd.

[39] Enligt Irlands uppfattning är dessa överväganden särskilt viktiga i praktiken med avseende på it-brottslighet. Om var och en som – även i en begränsad omfattning – blir föremål för en överträdelse hade rätt till ersättning för ideell skada skulle det nämligen ha en kraftig effekt, i synnerhet på personuppgiftsansvariga inom den offentliga sektorn som finansieras med begränsade offentliga medel och snarare borde eftersträva kollektiva intressen, däribland förbättrad säkerhet för personuppgifter (skriftligt yttrande, punkt 72).

83. Gränsen mellan ren irritation (som inte är ersättningsgill) och verklig ideell skada (som är ersättningsgill) är subtil, men de nationella domstolarna, som har i uppgift att i varje enskilt fall sätta denna gräns, bör genomföra en noggrann bedömning av alla uppgifter som har lagts fram av den registrerade som har yrkat ersättning, som då är skyldig att i detalj, och inte bara rent generellt, inkomma med konkreta uppgifter som leder till slutsatsen att personuppgiftsincidenten har vållat en ”faktisk ideell skada”, dock utan att denna skyldighet når upp till en särskild förhandbestämd betungande tröskel. Det väsentliga är att det inte rör sig om en rent subjektiv känsla som är föränderlig och även avhänger av personlighetsmässiga och individuella drag, utan att det är fråga om en möjligen ringa, men påvisbar, objektiv olägenhet för personens fysiska eller psykiska sfär eller sociala liv och där de aktuella personuppgifternas karaktär och deras betydelse i den registrerades liv och kanske även den rådande uppfattningen i samhället om den specifika olägenhet som följer av personuppgiftsincidenten är av vikt. [40]

IV. Förslag till avgörande

84. Mot bakgrund av samtliga ovanstående överväganden föreslår jag att domstolen besvarar tolkningsfrågorna på följande sätt:

Artiklarna 5, 24, 32 och 82 i förordning 2016/679 ska tolkas på följande sätt:

Enbart den omständigheten att det har skett en ”personuppgiftsincident” enligt definitionen i artikel 4.12 räcker inte i sig för att anse att de tekniska och organisatoriska åtgärder som den personuppgiftsansvarige har vidtagit inte är ”lämpliga” för att säkerställa skyddet av de aktuella personuppgifterna.

Vid bedömningen av huruvida de tekniska och organisatoriska åtgärder som den personuppgiftsansvarige har vidtagit är lämpliga ska den nationella domstol som har att pröva det aktuella målet genomföra en undersökning som även omfattar en konkret bedömning av innehållet av dessa åtgärder, av det sätt på vilket de har tillämpats och av deras praktiska konsekvenser.

När en skadeståndstalan väcks med stöd av artikel 82 i förordningen är den personuppgiftsansvarige skyldig att visa att denne har vidtagit åtgärder som är lämpliga i den mening som avses i artikel 32 i denna förordning.

I enlighet med principen om medlemsstaternas processuella autonomi ankommer det på varje medlemsstat att i sin rättsordning fastställa vilka bevismedel som är tillåtna och deras bevisvärde, däribland den bevisning som de nationella domstolarna kan eller måste inhämta för att bedöma huruvida en personuppgiftsansvarig har vidtagit lämpliga åtgärder i enlighet med förordningen, under förutsättning att likvärdighets- och effektivitetsprinciperna i unionsrätten iakttas.

Den omständigheten att den överträdelse av denna förordning som har vållat den aktuella skadan har vållats av tredje man utgör i sig inte någon grund för att undanta den personuppgiftsansvarige från ansvar. För att kunna frånsäga sig ansvaret med stöd av denna bestämmelse måste den personuppgiftsansvarige visa att denne inte på något sätt bär ansvar för överträdelsen.

[40] Se ovannämnda förslag till avgörande av generaladvokaten Campos Sánchez-Bordona (punkt 116).

Olägenheten bestående i den registrerades rädsla för att dennes personuppgifter kan komma att missbrukas i framtiden, för det fall den registrerade har påvisat denna olägenhet, kan utgöra en ersättningsgill ideell skada, under förutsättning att den registrerade visar att han eller hon har lidit en faktisk och säker emotionell skada, vilket det ankommer på den nationella domstol som har att pröva målet att i varje enskilt fall undersöka.