Сборник съдебна практика

ЗАКЛЮЧЕНИЕ НА ГЕНЕРАЛНИЯ АДВОКАТ
G. PITRUZZELLA
представено на 27 април 2023 година [1]

Дело C-340/21

V.B.
срещу
Национална агенция за приходите

(Преюдициално запитване, отправено от Върховен административен съд (България)

„Преюдициално запитване — Защита на личните данни — Регламент (ЕС) 2016/679 — Отговорност на администратора — Сигурност на обработването — Нарушение на сигурността на обработването на лични данни — Неимуществени вреди, претърпени поради бездействие от страна на администратора — Иск за обезщетение за вреди“

Може ли незаконното разпространение на съхранявани от публична агенция лични данни поради „хакерска атака“ да доведе до обезщетение за неимуществени вреди в полза на субекта на данните единствено на основание че последният се страхува от бъдеща злоупотреба с тях? Какви са критериите за вменяване на отговорност на администратора? Как се разпределя доказателствената тежест в рамките на производството? Какъв е обхватът на проверката от страна на съда?

I. Правна уредба

1. Член 4, озаглавен „Определения“, от Регламент 2016/679 [2] (наричан по-нататък „Регламентът“), гласи:

„За целите на настоящия регламент:

[…]

(12) „нарушение на сигурността на лични данни“ означава нарушение на сигурността, което води до случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до лични данни, които се предават, съхраняват или обработват по друг начин;

[1] Език на оригиналния текст: италиански.

[2] Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните).

[…]“.

2. Член 5, озаглавен „Принципи, свързани с обработването на лични данни“, предвижда:

„1. Личните данни са:

[…]

е) обработвани по начин, който гарантира подходящо ниво на сигурност на личните данни, включително защита срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане, като се прилагат подходящи технически или организационни мерки („цялостност и поверителност“);

2. Администраторът носи отговорност и е в състояние да докаже спазването на параграф 1 („отчетност“)“.

3. Член 24 от същия регламент, озаглавен „Отговорност на администратора“, гласи:

„1. Като взема предвид естеството, обхвата, контекста и целите на обработването, както и рисковете с различна вероятност и тежест за правата и свободите на физическите лица, администраторът въвежда подходящи технически и организационни мерки, за да гарантира и да е в състояние да докаже, че обработването се извършва в съответствие с настоящия регламент. Тези мерки се преразглеждат и при необходимост се актуализират.

2. Когато това е пропорционално на дейностите по обработване, посочените в параграф 1 мерки включват прилагане от страна на администратора на подходящи политики за защита на данните.

3. Придържането към одобрени кодекси за поведение, посочени в член 40 или одобрени механизми за сертифициране, посочени в член 42 може да се използва като елемент за доказване на спазването на задълженията на администратора.

4. Член 32, озаглавен „Сигурност на обработването“, предвижда:

„1. Като се имат предвид достиженията на техническия прогрес, разходите за прилагане и естеството, обхватът, контекстът и целите на обработването, както и рисковете с различна вероятност и тежест за правата и свободите на физическите лица, администраторът и обработващият лични данни прилагат подходящи технически и организационни мерки за осигуряване на съобразено с този риск ниво на сигурност, включително, inter alia, когато е целесъобразно:

[…]

2. При оценката на подходящото ниво на сигурност се вземат предвид по-специално рисковете, които са свързани с обработването, по-специално от случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до прехвърлени, съхранявани или обработени по друг начин лични данни.

3. Придържането към одобрен кодекс за поведение, посочен в член 40 или одобрен механизъм за сертифициране, посочен в член 42 може да се използва като доказателство за предоставянето на достатъчно гаранции съгласно параграф 1 от настоящия член.

[…]“.

5. Член 82 от същия регламент, озаглавен „Право на обезщетение и отговорност за причинени вреди“, гласи:

„1. Всяко лице, което е претърпяло материални или нематериални вреди в резултат на нарушение на настоящия регламент, има право да получи обезщетение от администратора или обработващия лични данни за нанесените вреди.

2. Администраторът, участващ в обработването на лични данни, носи отговорност за вреди, произтичащи от извършеното обработване, което нарушава настоящия регламент. […].

3. Администраторът или обработващият лични данни се освобождава от отговорност съгласно параграф 2, ако докаже, че по никакъв начин не е отговорен за събитието, причинило вредата.

II. Фактите, спорът в главното производство и преюдициалните въпроси

6. На 15 юли 2019 г. българските медии съобщават, че е имало неоторизиран достъп до ИТ системата на Националната агенция за приходите (наричана по-нататък „НАП“ [3]) и че различна данъчна и осигурителна информация на милиони хора, както български граждани, така и чужденци, е публикувана в интернет.

7. Следователно много лица, включително V.B., ищец в главното производство, завеждат дела срещу НАП, за да получат обезщетение за неимуществени вреди.

8. В конкретния случай ищцата в главното производство предявява иск пред Административен съд София-град (наричан по-нататък „АССГ“), като твърди, че НАП е нарушила националното право, както и задължението да обработва лични данни в качеството си на администратор по начин, който „да гарантира подходящо ниво на сигурност“, като се прилагат подходящи технически и организационни мерки, съгласно членове 24 и 32 от Регламент 2016/679. Ищцата твърди, че е претърпяла неимуществени вреди, които се изразяват в притеснения и опасения, че с личните ѝ данни може да бъде злоупотребено в бъдеще.

9. Ответникът обаче подчертава, че не е получил каквото и да било искане от страна на ищцата в главното производство за информация до какви точно лични данни е осъществен достъп. Също така, че след новината за пробива е свикал срещи с експерти на високо ниво с цел защита на правата и интересите на гражданите. Освен това според НАП няма причинна

[3] НАП е администратор съгласно член 4, точка 7 от Регламента. По националното право тя е специализиран държавен орган към министъра на финансите за установяване, обезпечаване и събиране на финанси, както и за установяване, обезпечаване и събиране на държавни вземания и определени със закон частни и публични вземания. В изпълнение на възложените ѝ публични функции тя обработва лични данни.

връзка между твърдените неимуществени вреди, тъй като агенцията е внедрила всички системи за управление на процесите и сигурността на информацията в съответствие с действащите международни стандарти в този област.

10. Първоинстанционният съд, АССГ, отхвърля иска, като приема, че агенцията не е отговорна за разкриването на данните, че доказателствената тежест на подходящия характер на приетите мерки е на ищцата и накрая, че няма неимуществени вреди, които да подлежат на обезщетяване.

11. Първоинстанционното решение е обжалвано пред Върховния административен съд. Сред изтъкнатите съображения ищцата в главното производство подчертава, че първоинстанционният съд е допуснал грешка при разпределянето на доказателствената тежест по отношение на неприемането на мерките за сигурност. Също така, че неимуществените вреди не трябва да бъдат предмет на доказателствената тежест, тъй като същите не са хипотетични, а реални.

12. От своя страна НАП настоява, че е предприела необходимите технически и организационни мерки в качеството си на администратор, и оспорва наличието на доказателства за действителни неимуществени вреди. В случая притесненията и страхът представляват емоционални състояния, които не полежат на обезщетяване.

13. Запитващата юрисдикция установява различни резултати от отделните производства, които ощетените страни са завели поотделно срещу НАП за обезщетяване на неимуществени вреди.

14. В този контекст запитващата юрисдикция спира производството и поставя на Съда следните преюдициални въпроси:

„1) Разпоредбите на член 24 и член 32 от Регламент (ЕС) 2016/679 [на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните)] могат ли да се тълкуват в смисъл, че е достатъчно да е осъществено неразрешено разкриване или достъп до лични данни по смисъла на член 4, точка 12 от Регламент (ЕС) 2016/679 от лица, които не са служители в администрацията на администратора на лични данни и не са под негов контрол, за да се приеме, че приложените технически и организационни мерки не са подходящи?

2) Ако отговорът на първия въпрос е отрицателен, какъв следва да е предметът и обхватът на съдебния контрол за законосъобразност при проверка дали приложените от администратора на лични данни технически и организационни мерки по член 32 от Регламент (ЕС) 2016/679 са подходящи?

3) Ако отговорът на първия въпрос е отрицателен, принципът на отчетност в член 5, параграф 2 и член 24 във връзка със съображение 74 от Регламент (ЕС) 2016/679 могат ли да се тълкуват в смисъл, че в исковото производство по член 82, параграф 1 от Регламент (ЕС) 2016/679 администраторът на лични данни носи доказателствена тежест относно обстоятелството, че приложените по член 32 от Регламента технически и организационни мерки са подходящи? Назначаването на съдебна експертиза може ли да се приеме като необходимо и достатъчно доказателствено средство, с което да се

установи дали приложените от администратора на лични данни технически и организационни мерки са подходящи в хипотеза като настоящата, в която неразрешеният достъп и разкриване на лични данни е резултат от „хакерска атака“?

4) Нормата на член 82, параграф 3 от Регламент (ЕС) 2016/679 може ли да се тълкува в смисъл, че неразрешено разкриване или достъп до лични данни по смисъла на член 4, точка 12 от Регламент (ЕС) 2016/679, в случая чрез „хакерска атака“, от лица, които не са служители в администрацията на администратора на лични данни и не са под негов контрол, е събитие, за което администраторът на лични данни по никакъв начин не е отговорен и е основание за освобождаване от отговорност?

5) Нормите на член 82, параграф 1 и параграф 2 във връзка със съображения 85 и 146 от преамбюла на Регламент (ЕС) 2016/679 могат ли да се тълкуват в смисъл, че в хипотеза като настоящата на нарушение на сигурността на личните данни, изразяващо се в неразрешен достъп и разпространение на лични данни, осъществено чрез „хакерска атака“, само преживените от субекта на лични данни опасения, притеснения и страх от евентуална, бъдеща злоупотреба с лични данни, без да е установена такава злоупотреба и/или да е настъпила друга вреда за субекта на данните, попадат в широкия смисъл на понятието нематериални вреди и [това] е основание за обезщетение?“.

III. Правен анализ

A. Предварителни бележки

15. Настоящият случай засяга интересни и отчасти неразглеждани въпроси относно тълкуването на различни разпоредби на Регламента [4].

16. Петте преюдициални запитвания се въртят около един и същ въпрос: условията за обезщетение за неимуществени вреди на лице, чиито лични данни, съхранявани от публична агенция, са били публикувани в интернет вследствие на хакерска атака.

17. За удобство на изложението ще предложа отделни кратки отговори на всички въпроси от акта за преюдициално запитване, макар и да съм наясно с известно концептуално припокриване, тъй като първите четири са насочени изцяло към определяне на условията за вменяване на отговорност за нарушение на разпоредбите на Регламента за администратора [5], а петият се отнася по-точно до понятието неимуществени вреди за целите на обезщетението [6].

[4] Член 5, параграф 2 (свързан с принципа на отчетност на всеки администратор на лични данни), член 24 (свързан с мерките, които този администратор е длъжен да въведе, за да гарантира, че обработването му е в съответствие с настоящия регламент), член 32 (свързан с това задължение конкретно по отношение на сигурността на обработването) и член 82, параграфи 1—3 (свързан с обезщетението за вреди, произтичащи от нарушение на регламента, и с възможността администраторът да предприеме мерки, за да гарантира спазването на регламента), както и съображения 74, 85 и 146, които са свързани с посочените по-горе членове.

[5] а) първият има за цел да отговори на въпроса дали неподходящият характер на въведените мерки може да бъде следствие само от пробив в системите; б) вторият се отнася до разширяването на съдебния контрол относно подходящия характер на горепосочените мерки; в) третият се отнася до тежестта на доказване на самата адекватност и до някои технически методи за търсене на доказателства; г) четвъртият се отнася до релевантността за целите на освобождаването от отговорност на обстоятелството, че атаката срещу системата идва отвън.

[6] По отношение на цитираните разпоредби от Регламента първите три въпроса засягат аспектите на отговорността на администратора във връзка с подходящия характер на мерките, които трябва да бъдат приети (членове 5, 24 и 32); четвъртият и петият — условията за освобождаване от отговорност и понятието за неимуществени вреди (член 82).

18. Бих искал да отбележа, че понастоящем в Съда се водят различни дела по член 82 от Регламента и по едно от тях вече бяха прочетени заключенията на генералния адвокат, които ще взема предвид в настоящия анализ [7].

19. Преди да разгледам поставените въпроси, считам за целесъобразно да изложа някои предварителни съображения относно принципите и целите на Регламента, които ще бъдат полезни за решаването на отделните преюдициални въпроси.

20. Член 24 от Регламента установява в общ план задължението на администратора да прилага подходящи технически и организационни мерки, за да гарантира, че обработването на лични данни е в съответствие със самия регламент, и да може да го докаже, докато член 32 конкретизира същото задължение по отношение на сигурността на обработването. В членове 24 и 32 се дефинира по-конкретно вече предвиденото в член 5, параграф 2, с който именно сред „принципите, свързани с обработването на лични данни“ се въвежда „принципът на отчетност“. Той следва логично и допълва „принципа на цялостност и поверителност“, посочен в член 5, параграф 1, буква е), като и двата следва да се четат в светлината на основания на риска подход, на който се основава Регламентът.

21. Принципът на отчетност е един от стълбовете на Регламента и едно от най-значимите му нововъведения. Той определя отговорността на администратора да предприеме проактивни действия, за да осигури съответствие с Регламента и да бъде в състояние да докаже това [8].

22. В доктрината се говори за истинска културна промяна като ефект от „глобалния обхват на задължението за отговорност“ [9]. Не става въпрос толкова за формалното изпълнение на правното задължение или точната мярка, колкото за цялостната корпоративна стратегия, възприета за освобождаване на администратора от отговорност поради спазването на разпоредбите за защита на данните.

23. Техническите и организационни мерки, изисквани от принципа на отчетност, трябва да бъдат „подходящи“ с оглед на факторите, посочени в член 24: естеството, обхвата, контекста и целите на обработването, както и рисковете с различна вероятност и тежест за правата и свободите на физическите лица.

24. Следователно член 24 налага подходящия характер на мерките, за да може да се докаже съответствието на обработването с принципите и разпоредбите на Регламента.

25. Член 32 от своя страна прилага принципа на отчетност към конкретните мерки, които следва да се предприемат, за да се гарантира „съобразено с риска ниво на сигурност“. И като прави това, той добавя достиженията на техническия прогрес и разходите за прилагане към факторите, които вече са предвидени като определящи при подготовката на техническите и организационни мерки.

[7] Вж. заключението на генерален адвокат Campos Sánchez-Bordona по дело Österreichische Post (Неимуществени вреди, свързани с обработването на лични данни) (C-300/21, EU:C:2022:756).

[8] *Docksey*, C. Article 24. Responsibility of the controller. — In: *Kuner*, C., *Bygrave*, L. A., *Docksey*, C., *Drechsler*. L. The EU General Data Protection Regulation (GDPR): A Commentary. Oxford University Press, 2020, p. 561. Принципите и задълженията на регламентите за защита на данните следва да проникнат в културната тъкан на организациите на всички нива, вместо да се разглеждат като набор от правни изисквания, които трябва да бъдат спазвани от правния отдел.

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

26. Понятието за адекватност изисква решенията, възприети за гарантиране на ИТ системите, да достигнат ниво на приемливост както от техническа гледна точка (уместност на мерките), така и от гледна точка на качеството (ефективност на защитата). За да се гарантира спазването на принципите на необходимост, целесъобразност и пропорционалност, операциите по обработването трябва да бъдат не само подходящи, но и задоволителни по отношение на преследваните цели. И в тази логика принципът на свеждане до минимум играе решаваща роля, по силата на който всички фази на обработката на данните трябва постоянно да се стремят към свеждане до минимум на рисковете за сигурността [10].

27. Целият регламент се основава на предотвратяването на риска и отчетността на администратора и следователно на телеологичен подход, който цели възможно най-добрия резултат по отношение на ефективността, т.е. далеч от формалистичната логика, свързана с простото задължение за изпълнение на конкретни процедури с цел освобождаване от отговорност [11].

28. Член 24 не съдържа изчерпателен списък на „подходящите“ мерки: ще трябва да се направи оценка за всеки отделен случай. Това е в съответствие с философията на Регламента, който разкрива как е било предпочетено процедурите, които трябва да бъдат възприети, да се избират въз основа на внимателна оценка на конкретната ситуация, така че да бъдат възможно най-ефективни [12].

Б. По първия преюдициален въпрос

29. С първия си въпрос запитващата юрисдикция по същество иска да се установи дали членове 24 и 32 от Регламента следва да се тълкуват в смисъл, че настъпването на „нарушение на сигурността на личните данни“, както е определено в член 4, параграф 12, само по себе си е достатъчно, за да се заключи, че прилаганите от администратора техническите и организационни мерки не са „подходящи“ за осигуряване на защитата на данните.

30. От текста на членове 24 и 32 от Регламента става ясно, че администраторът, когато избира техническите и организационни мерки, които е длъжен да приложи, за да гарантира спазването на самия Регламент, трябва да вземе предвид редица фактори за оценка, изброени в посочените членове и споменати по-горе.

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

[11] Поради тази причина, както ще видим, на първия и четвъртия преюдициален въпрос може да се даде само отрицателен отговор. От разпоредбите на Регламента не може да се извлече нищо автоматично: нито само фактът, че е имало разкриване на лични данни, е достатъчен, за да се смята, че приетите технически и организационни мерки не са подходящи, нито обстоятелството, че самото разкриване е извършено поради намеса на субекти извън организацията на администратора и извън сферата на контрол на същия, е достатъчно, за да го освободи от отговорност.

[12] *Bolognini*, L., *Pelino*, E. Codice della disciplina privacy. Giuffrè, 2019, p. 201. Следователно европейският законодател преодолява концепцията за сигурност на обработването, основана на наличието на предварително определени мерки за сигурност, и възприема методология, присъща на международните стандарти за управление на информационни системи, основаваща се на *риска*: тя предвижда определяне на мерки за намаляване на риска, които пренебрегват предварително конфигурирани и общи приложими *контролни списъци*. Следователно е необходимо да си послужим с международни насоки и стандарти. Следователно резултатът от тази оценка на риска става обвързващ в момента, в който организацията вземе решения за смекчаване на установените рискове, като поеме *отговорност*.

31. Администраторът разполага с известна свобода на действие по отношение на определянето на най-подходящите мерки с оглед на неговата конкретна ситуация, но този избор все още подлежи на евентуален съдебен контрол на съответствието на прилаганите мерки с всички задължения и цели на самия Регламент.

32. По-специално, по отношение на мерките за сигурност член 32, параграф 1 изисква администраторът да вземе предвид „достиженията на техническия прогрес“. Това предполага ограничаване на технологичното ниво на мерките, които трябва да бъдат приложени, до разумно възможното в момента на приемане на същите: следователно пригодността на мярката за предотвратяване на риска следва да бъде пропорционална на решенията, които достиженията на науката, техниката, текущите технологии и научни изследвания предлагат, при това като се вземат предвид, както ще видим, разходите за прилагане.

33. Мерките могат да бъдат „подходящи“ в даден момент и въпреки това да бъдат заобиколени от киберпрестъпници, които използват много сложни инструменти, способни да преодолеят дори най-съвременните мерки за сигурност.

34. От друга страна, изглежда нелогично да се смята, че намерението на законодателя на ЕС е било да наложи на администратора задължение за преодоляване на всяко нарушение на сигурността на личните данни, независимо от дължимата грижа при подготовката на мерките за сигурност [13].

35. Както беше посочено по-горе, Регламентът се развива в далечна от автоматизмите перспектива, като изисква високо ниво на отчетност на администратора, което обаче не може да води до невъзможност последният да докаже, че е изпълнил коректно наложените му задължения.

36. Освен това член 32, параграф 1 предвижда, че трябва да се вземат предвид, както беше споменато, „разходите за прилагане“ на въпросните технически и организационни мерки. От това следва, че оценката на подходящия характер на такива мерки трябва да се основава на баланс между интересите на субекта на данните, които обикновено клонят към по-високо ниво на защита, и икономическите интереси и технологичния капацитет на администратора, които понякога клонят към по-ниско ниво на защита. Този баланс трябва да отговаря на изискванията на общия принцип на пропорционалност.

37. Към това следва да се добави, с оглед на систематичното тълкуване, че законодателят предвижда възможността да възникнат нарушения на системите; член 32, параграф 1, буква в) включва сред предложените мерки способността за своевременно възстановяване на наличността и достъпа до личните данни в случай на физически или технически инцидент. Предвиждането на тази способност сред мерките за сигурност, които гарантират подходящо за риска ниво на сигурност, би било безполезно, ако се смята, че простото нарушение на системите само по себе си представлява доказателство за неадекватност на самите мерки.

[13] Концепцията за адекватност недвусмислено разкрива намерението да не се придава значение на всички теоретично възможни технически и организационни мерки. Вж. в този смисъл M. *Gambini*, Responsabilità e risarcimento nel trattamento dei dati personali. — In: *Cuffaro*, V., *D'Orazio*, R., *Ricciuto*, V. I dati personali nel diritto europeo. Giappichelli, 2019, p. 1059.

B. По втория преюдициален въпрос

38. С втория си въпрос запитващата юрисдикция по същество иска да се установи какъв следва да е предметът и обхватът на съдебния контрол при проверка дали приложените от администратора технически и организационни мерки по член 32 от Регламента са подходящи.

39. Предвид променливостта на ситуациите, които могат да възникнат на практика, Регламентът, както беше споменато, не установява обвързващи разпоредби за определяне на техническите и организационни мерки, които администраторът трябва да приложи, за да изпълни изискванията на самия Регламент. Следователно подходящият характер на приложените мерки ще трябва да бъде оценен конкретно, като се провери дали конкретните мерки са били подходящи за разумно предотвратяване на риска и свеждане до минимум на отрицателните последици от нарушението.

40. Ако несъмнено е вярно, че изборът и прилагането на тези мерки попада в обхвата на субективната оценка на администратора, тъй като посочените в Регламента мерки са само примерни, проверката от страна на съда не може да се ограничи до установяване на спазването от страна на администратора на задълженията, произтичащи от членове 24 и 32, т.е. до (формално) предвиждане на определени технически и организационни мерки. Той трябва да извърши конкретен анализ на съдържанието на тези мерки, начина на тяхното прилагане и практическите резултати от тях, въз основа на наличните доказателства и обстоятелствата по конкретния случай. Както успешно поддържа португалското правителство, „начинът на изпълнение на задълженията изглежда неделим от съдържанието на предприетите мерки, за да се докаже, че предвид специфичното обработване на данните (неговото естество, обхват, контекст и цели) достиженията на наличните технологии и съответните разходи, както и рисковете за правата и свободите на гражданите администраторът е взел всички необходими и подходящи мерки, за да гарантира ниво на сигурност, подходящо за съответния риск“ [14].

41. Следователно съдебният контрол ще трябва да вземе предвид всички фактори, съдържащи се в членове 24 и 32, които, както беше споменато, изброяват поредица от критерии за оценка на подходящия характер и предоставят примери за мерки, които могат да се считат за подходящи. Освен това, както е подчертано от Комисията и всички държави членки, които са представили коментари по втория въпрос, в член 32, параграфи 1—3 се подчертава необходимостта от „осигуряване на съобразено с [този] риск ниво на сигурност“, като се посочват други важни фактори за тази цел, като евентуалното приемане от администратора на одобрен кодекс за поведение или одобрена система за сертифициране, както е предвидено съответно в членове 40 и 42 от Регламента.

42. Приемането на кодекси за поведение или системи за сертифициране може да представлява полезен елемент за оценка за целите на изпълнението на доказателствената тежест и свързания съдебен контрол. С уточнението обаче, че не е достатъчно администраторът да се придържа към кодекс за поведение, но той има ангажимента да докаже, че действително е приложил предвидените в него мерки в съответствие с

[14] Писмено становище, точка 31.

принципа на отчетност. Сертифицирането, от друга страна, представлява „само по себе си доказателство за съответствие с регламента на операциите по обработване, макар и оспоримо от практическа гледна точка“ [15].

43. И накрая, следва да се отбележи, че тези мерки трябва да бъдат преразглеждани и при необходимост актуализирани съгласно член 24, параграф 1. Това също ще бъде предмет на оценка от страна на националния съд. Член 32, параграф 1 от Регламента [16] всъщност налага на администратора задължение за постоянен, превантивен и последващ контрол и наблюдение по отношение на дейностите по обработването, но също така и за поддръжка и евентуално актуализиране на прилаганите мерки с цел както предотвратяване на нарушенията, така и евентуално ограничаване на последиците от тях.

44. Склонен съм обаче да изключа възможността предстоящото решение да включва списък от съществени елементи, като този, предложен от португалското правителство [17]. Това би могло да предостави възможност за противоречиви тълкувания, тъй като списъкът очевидно не може да бъде изчерпателен.

Г. По третия преюдициален въпрос

45. С първата част на третия си въпрос запитващата юрисдикция по същество иска от Съда да установи дали, като се вземе предвид принципът на отчетност, посочен в член 5, параграф 2 и член 24 във връзка със съображение 74 [18] от Регламента, в контекста на иск за обезщетение по член 82, доказателствената тежест на подходящия характер на техническите и организационните мерки съгласно член 32 е задължение на администратора на лични данни.

46. Изложените по-горе съображения ми позволяват да дам кратък положителен отговор на този въпрос.

47. Наистина, буквата на закона, контекстът и целите на Регламента недвусмислено вменяват доказателствената тежест на администратора.

[15] *Gambini*, M. Responsabilità, op. cit., p. 1067. Следователно притежаването на сертификат води до обръщане на тежестта на доказване в полза на притежателя, който е улеснен да докаже, че е действал в съответствие с посочените в Регламента задължения.

[16] Като изрично предвижда в буква г), че преценката за адекватност обхваща ефективността на приетите мерки, т.е. процес на редовно изпитване, преценяване и оценка на ефективността на техническите и организационните мерки с оглед да се гарантира сигурността на обработването, независимо от нивото на риск; и отново, като изрично предвижда в буква в), че въведените технически и организационни мерки трябва да предоставят възможност за своевременно възстановяване на наличността и достъпа до личните данни в случай на физически или технически инцидент. Вж. *Gambini*, M. Responsabilità, op. cit., 1064—1065.

[17] Точка 30 от писменото становище: „администраторът ще трябва да докаже как е оценил всички фактори и обстоятелства, свързани с въпросното обработване, и по-специално резултата от извършения анализ на риска, установените рискове, конкретните мерки, определени за смекчаване на тези рискове, обосновката на избора на варианти с оглед наличните на пазара технологични решения, ефективността на мерките, връзката между техническите и организационните мерки, обучението на персонала, който обработва данните, наличието на външни изпълнители на операции по обработване на данни, включително разработване и поддържане на информационни технологии, както и наличието на надзор от страна на администратора и точни инструкции, предоставени на обработващите лични данни съгласно член 28 от GDPR, относно обработването на лични данни от последните; как е оценена инфраструктурата, поддържаща комуникационните и информационните системи и как е класифицирано нивото на риск за правата и свободите на субектите на данни“.

[18] Съгласно съображение 74: „Следва да бъдат установени отговорностите и задълженията на администратора за всяко обработване на лични данни, извършено от администратора или от негово име. По-специално, администраторът следва да е длъжен да прилага подходящи и ефективни мерки и да е в състояние да докаже, че дейностите по обработването са в съответствие с настоящия регламент, включително ефективността на мерките. Тези мерки следва да отчитат естеството, обхвата, контекста и целите на обработването, както и риска за правата и свободите на физическите лица“.

48. От формулировката на различни разпоредби на Регламента следва, че администраторът трябва да е „в състояние“ или да е „способен“ да „докаже“ спазването на предвидените в Регламента задължения, и по-специално да е приложил подходящи мерки за тази цел, както е посочено в съображение 74, член 5, параграф 2 и член 24, параграф 1. Както посочва португалското правителство, съображение 74 уточнява, че доказателствената тежест, вменена по този начин на отговорното лице, трябва да включва доказателство за „ефективността на въпросните мерки“.

49. Това буквално тълкуване ми изглежда подкрепено от следните практически и телеологични съображения.

50. Що се отнася до разпределението на доказателствената тежест, в контекста на иск за обезщетение по член 82, субектът на данни, който е завел делото срещу администратора, трябва, първо, да докаже, че е налице нарушение на Регламента, второ, че той е претърпял вреди и на трето място, че съществува причинно-следствена връзка между двата предходни елемента, както е отбелязано във всички писмени становища по петия преюдициален въпрос. Това са три кумулативни условия, както става ясно и от консолидираната постоянна практика на Съда и Общия съд в контекста на извъндоговорната отговорност на Съюза [19].

51. Считам обаче, че задължението на ищеца да докаже наличието на нарушение на Регламента, не може да стигне дотам, че да поиска да докаже, че приложените от администратора технически и организационни мерки не са подходящи, съгласно членове 24 и 32.

52. Както посочва Комисията, представянето на такива доказателства често би било почти невъзможно на практика, тъй като субектите на данни обикновено нямат достатъчно познания, за да могат да анализират подобни мерки, нито достъп до цялата информация, съхранявана от сезирания администратор, по-специално по отношение на прилаганите методи за гарантиране на сигурността на обработването. Освен това администраторът понякога може да изтъкне, че отказът му да разкрие тези факти на субектите на данните, се основава на законната причина да не разкрива своите вътрешни правила или също така елементи, обхванати от професионална тайна, наред с други неща, именно поради съображения за сигурност.

53. Следователно, ако се приеме, че доказателствената тежест е задължение на засегнатото лице, практическият резултат би бил, че правото на обжалване по член 82, параграф 1 ще загуби голяма част от обхвата си. Според мен това не би било в съответствие с намеренията на законодателя на ЕС, който с приемането на този Регламент се опита да засили правата на субектите на данни и задълженията на администраторите в сравнение с Директива 95/46, която замести. Следователно е по-логично и правно издържано да се изисква от администратора да докаже, в контекста на своята защита срещу иск за обезщетение, че е спазил задълженията, произтичащи от членове 24 и 32 от настоящия Регламент, като е приложил действително подходящи мерки.

[19] Вж. по-специално решения на Съда от 5 септември 2019 г., Европейски съюз/Guardian Europe и Guardian Europe/Европейски съюз (C-447/17 P и C479/17 P, EU:C:2019:672, т. 147) и от 28 октомври 2021 г., Vialto Consulting/Европейска комисия (C-650/19 P, EU:C:2021:879, т. 138), както и решенията на Общия съд от 13 януари 2021 г., Helbert/EUIPO (T-548/18, EU:T:2021:4, т. 116), и от 29 септември 2021 г., Kočner/Europol (T-528/20, непубликувано, EU:T:2021:631, т. 61), в които се припомня, че трябва да бъдат изпълнени три условия, а именно „незаконосъобразност на поведението, в което е обвинена институцията на Съюза, реалност на вредата и наличие на причинно-следствена връзка между поведението на тази институция и посочената вреда“.

54. С втората част на третия си въпрос запитващата юрисдикция по същество пита Съда дали евентуална съдебна техническа експертиза може да се счита за необходимо и достатъчно доказателство за оценка на подходящия характер на прилаганите от администратора технически и организационни мерки в ситуация, в която неоторизираният достъп и разкриването на лични данни са резултат от хакерска дейност.

55. Както (по същество) подчертаха и българското, и италианското правителство, Ирландия и Комисията, считам, че отговорът на тези въпроси трябва да се основава на постоянната практика на Съда, според която, съгласно принципа на процесуална автономия, при липса на правила на Съюза по този въпрос вътрешният правен ред на всяка държава членка урежда процедурните разпоредби за съдебни производства за защита на правата на лицата, при условие обаче, че тези правила не са, в ситуации, уредени от правото на Съюза, по-малко благоприятни от тези, които уреждат подобни ситуации в националното законодателство (принцип на равностойност), и не правят упражняването на правата, предоставени от правото на ЕС, невъзможно на практика или прекомерно трудно (принцип на ефективност).

56. В настоящия случай отбелязвам, че Регламентът не съдържа никаква разпоредба, насочена към определяне на допустимите методи за доказване и тяхната доказателствена стойност, по-специално по отношение на следствените действия (като експертно становище), които националните съдилища могат или трябва да разпоредят, за да се направи оценка дали администраторът е предприел подходящи мерки съгласно настоящия Регламент. Ето защо считам, че при липса на хармонизирани правила по въпроса вътрешната правна система на всяка държава членка следва да определи тези процедурни разпоредби, без да се засяга спазването на принципите на равностойност и ефективност.

57. Горепосоченият „принцип на ефективност“, който предполага, че независим съдия трябва да извърши безпристрастна оценка, може да бъде компрометиран, ако прилагателното „достатъчно“ трябва да се разбира в смисъла, който ми се струва, че е натоварено от запитващата юрисдикция, т.е. да може автоматично да са направи извод от експертно становище, че мерките, предприети от администратора, са подходящи [20].

Д. По четвъртия преюдициален въпрос

58. С четвъртия си въпрос запитващата юрисдикция по същество иска да се установи дали член 82, параграф 3 от Регламента трябва да се тълкува в смисъл, че в случай на нарушение на този регламент (състоящо се, както в настоящия случай, в „неразрешено разкриване“ или „неоторизиран достъп“ до лични данни по смисъла на член 4, параграф 12), извършено от лица, които не са служители на администратора на данните и не са под негов контрол, това представлява събитие, за което администраторът на личните данни по никакъв начин не е отговорен, и следователно основание за неговото освобождаване от отговорност съгласно член 82, параграф 3.

59. Отговорът на въпроса произтича линейно от изложеното по-горе относно общата философия на Регламента: няма автоматизми и следователно самият факт, че неразрешеното разкриване или достъп до лични данни е станал/о по вина на субекти извън сферата на контрол на администратора, не освобождава последния от отговорност.

[20] Писмено становище, точка 39.

60. На първо място, в буквален смисъл, следва да се отбележи, че нито член 82, параграф 3, нито съображение 146 определят специални условия, които могат да бъдат изпълнени, за да бъде освободен от отговорност администраторът, освен „ако докаже, че по никакъв начин не е отговорен за събитието, причинило вредата“. От тази формулировка следва, от една страна, че администраторът може да бъде освободен от отговорност само ако докаже, че не е отговорен за събитието, причинило въпросната вреда, и от друга страна, че изискваният стандарт за доказване от тази разпоредба е висок предвид използването на словосъчетанието „по никакъв начин“, както подчерта Комисията [21].

61. Режимът на отговорност, предвиден в член 82 и общо в целия регламент, е бил предмет на задълбочени дебати в доктрината на различните държави членки. Всъщност той съдържа традиционни елементи на извъндоговорната отговорност, но също и елементи, които в структурата на разпоредбите го доближават до договорната отговорност или дори до форма на обективна отговорност, поради присъщата опасност на дейността по обработване на данни. Тук не е мястото да обяснявам сложно формулирания дебат, но според мен член 82 не изглежда да определя режим на обективна отговорност [22].

62. Вредата от нарушаването на личните данни може да бъде конфигурирана като виновна последица от неприемането на разумни и във всички случаи подходящи технически и организационни мерки за нейното предотвратяване, като се вземат предвид рисковете за правата и свободите на лицата, свързани с дейността по обработването. Тези рискове правят по-строго задължението за предотвратяване и избягване на вредата, като разширяват задължението за полагане на грижи на администратора на лични данни. Следователно от тълкуването на задълженията за поведение на администраторите на лични данни във връзка с разпоредбата относно доказателството за освобождаване, възложено в тежест на причинителя на вредата, е възможно да се извлече аргумент в полза на признаването на характера на утежнената отговорност за предполагаема вина в случай на отговорност за неправомерно обработване на лични данни съгласно член 82 от Регламента [23].

63. От това произтича възможността администраторът да представи доказателство за освобождаване от отговорност (неразрешено при обективна отговорност). По отношение на формулирането на доказателствената тежест член 82, параграф 3 от Регламента диктува режим, благоприятен за увредената страна, като предвижда форма на обръщане на доказателствената тежест на вината към нейния причинител [24], изцяло в симетрия с горепосоченото обръщане на доказателствената тежест по отношение на подходящия характер на приетите мерки. По този начин законодателят показва, че съзнава

[21] В съответствие с постоянната съдебна практика на Съда, според която изключенията от общо правило трябва да се тълкуват ограничително, евентуалното освобождаване от отговорност, предвидено в член 82, параграф 3, трябва да се тълкува ограничително. Вж. по аналогия решения от 15 октомври 2020 г., Association française des usagers de banques (C-778/18, EU:C:2020:831, т. 53) и от 5 април 2022 г., Commissioner of An Garda Síochána и др. (C-140/20, EU:C:2022:258, т. 40).

[22] Съществува тенденция гражданската отговорност да се квалифицира като обективна, когато агентът е длъжен да предприеме всички абстрактно възможни мерки за избягване на вредата, независимо от действителните знания, с които е разполагал, или тяхната икономическа приемливост. Обратно, ако от агента се изисква да приеме мерки, които обикновено се наблюдават от оператор в референтния икономически сектор, за поддържане на безопасността и предотвратяване на вреди, които могат да произтекат от извършваната дейност, отговорността за тях е склонна да се насочва към режим на отговорност за конкретна вина. *Gambini*, M. Responsabilità, op. cit., p. 1055.

[23] M. Gambini, Responsabilità, op. cit., p. 1059. В подобен смисъл е становището, според което доказателството за предприемане на подходящи мерки се състои не в простото твърдение за необходимото най-голямо старание, а в доказването на генерирал вредата факт от трето лице с характеристиките на непредвидимост и неизбежност, характерни за случайността и непреодолимата сила, S. Sica, Sub art. 82. — In: *D'Orazio*, R., *Finocchiaro*, G., *Pollicino*, O., *Resta*, G. Codice della privacy e *data protection*. Giuffrè, 2021.

[24] „ако докаже, че по никакъв начин не е отговорен за събитието, причинило вредата“ (член 82, параграф 3).

опасностите, свързани с приемането на различно разпределение на доказателствената тежест; ако увредената страна — физическо лице, трябва да докаже вината на причинителя, това би довело до прекомерно утежняване на нейната позиция и следователно би компрометирало на практика ефективността на компенсаторната защита в контекста на правила, свързани с използването на новите технологии. Всъщност би могло да бъде особено обременително за заинтересованата страна да възстанови и да има достъп до методите на генериране на вредата и следователно да докаже вината на администратора. Обратно, администраторът на лични данни е в най-добра позиция да представи доказателство за освобождаване, за да докаже, че по никакъв начин не е отговорен за събитието, причинило вредата [25].

64. Администраторът също ще трябва да докаже в съответствие с описания по-горе принцип на отчетност, че е направил всичко възможно, за да възстанови своевременно наличността и достъпа до личните данни.

65. Връщайки се към въпроса на запитващата юрисдикция, въз основа на изложеното досега относно естеството на отговорността на администратора, ако, както беше споменато, администраторът може да бъде освободен от отговорност, като докаже, че по никакъв начин не е отговорен за причината на нарушението, самият факт, че събитието е причинено от субект извън неговата сфера на контрол, не може да се счита за такъв.

66. Когато администратор на данни е жертва на атака от страна на киберпрестъпници, би могло да се счита, че не е отговорен за събитието, което е довело до вредите, но не е изключено небрежност от негова страна да бъде в основата на въпросната атака, улеснявайки я поради липсата или неподходящия характер на мерките за сигурност на личните данни, които последното е задължено да прилага. Това са фактически оценки, специфични за всеки случай, които се оставят на сезирания национален съд в светлината на представените пред него доказателства.

67. Освен това обичаен опит е, че външните атаки срещу системите на публични или частни субекти, които притежават голямо количество лични данни, са много по-чести от вътрешните атаки. Следователно администраторът трябва да въведе подходящи мерки за справяне по-специално с външни атаки.

68. И накрая, от телеологична гледна точка следва да се отбележи, че Регламентът преследва целта за високо ниво на защита. В това отношение Съдът вече подчерта, че от член 1, параграф 2 от Регламента във връзка със съображения 10, 11 и 13 следва, че този регламент налага на институциите, органите, службите и агенциите на Съюза и компетентните органи на държавите членки задачата да осигурят високо ниво на защита на правата, свързани със защитата на личните данни, гарантирани от член 16 ДФЕС и от член 8 от Хартата [26].

69. Ако Съдът избере тълкуването, че когато нарушението на Регламента е извършено от трето лице, обработващият лични данни следва автоматично да бъде освободен от отговорност по член 82, параграф 3, такова тълкуване би имало ефект, несъвместим с целта за защита, преследвана от този инструмент, тъй като би подкопало правата на субектите на данни, ограничавайки тази отговорност до случаите, в които нарушението се дължи на лица, които са под властта и/или контрола на администратора на лични данни.

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

[26] Вж. в този смисъл решение от 15 юни 2021 г., Facebook Ireland и др. (C-645/19, EU:C:2021:483, т. 44 и 45).

E. По петия преюдициален въпрос

70. С петия въпрос националният съд по същество иска от Съда да тълкува понятието „неимуществени вреди“ (на езика на Регламента — „нематериални“) съгласно член 82 от Регламента. По-специално се пита дали разпоредбите на член 82, параграфи 1 и 2 от Регламента, във връзка със съображения 85 и 146 от него [27], следва да се тълкуват в смисъл, че в ситуация, в която нарушението на този регламент се състои при неоторизиран достъп до лични данни и неоторизирано разкриване на такива данни от киберпрестъпници, фактът, че субектът на данните се страхува от потенциална злоупотреба с личните му данни в бъдеще, може сам по себе си да представлява (неимуществена) вреда, даваща право на обезщетение.

71. Нито член 82, нито съображенията относно обезщетението за вреди дават ясен отговор на въпроса, но от тях могат да се извлекат някои полезни елементи за анализа: неимуществените (или нематериалните) вреди могат да бъдат предмет на обезщетение в допълнение към имуществените (или материалните); от нарушението на Регламента не следва автоматично, че „причинената“ от него вреда, или по-точно нарушението на личните данни, „може да причини“ физически, материални или нематериални щети на физически лица; понятието за вреда следва да се тълкува „в широк смисъл“ в светлината на съдебната практика на Съда по такъв начин, че да отразява напълно целите на Регламента; обезщетението за „претърпените“ вреди следва да бъде „пълно и ефективно“.

72. Буквалният смисъл на разпоредбите на Регламента вече изчиства полето за всяко възможно предположение за щети in re ipsa: основната цел на гражданската отговорност, предвидена от Регламента, е да даде удовлетворение на заинтересованата страна именно чрез „пълно и ефективно“ обезщетение за претърпените вреди и следователно възстановяване на баланса на правната ситуация, негативно променена от нарушението на правото [28].

73. От друга страна, дори от системна гледна точка, както в антитръстовото право, Регламентът предвижда два стълба на защита: единия от обществен характер, с предвиждане на санкции в случай на нарушения на разпоредбите на Регламента, и такъв от частен характер, по-точно осигуряващ гражданска отговорност от извъндоговорно

[27] Съгласно съображение 85: „Нарушаването на сигурността на лични данни може, ако не бъде овладяно по подходящ и навременен начин, да доведе до физически, материални или нематериални вреди за физическите лица […]“. Съгласно съображение 146: „Администраторът или обработващият лични данни следва да обезщети всички вреди, които дадено лице може да претърпи в резултат на обработване на данни, което нарушава настоящия регламент. Администраторът или обработващият лични данни следва да бъде освободен от отговорност, ако докаже, че по никакъв начин не е отговорен за вредите. Понятието „вреда“ следва да се тълкува в по-широк смисъл в контекста на съдебната практика на Съда по начин, който отразява напълно целите на настоящия регламент. Това не засяга евентуални искове за вреди, произтичащи от нарушаване на други правила на правото на Съюза или правото на държава членка. […]. Субектите на данни следва да получат пълно и действително обезщетение за претърпените от тях вреди. […]“.

[28] Вж. заключението на генерален адвокат Campos Sánchez-Bordona, посочено по-горе, точка 29 и бележка 11. В посоченото заключение генералният адвокат правилно завършва анализа си от буквална, историческа, контекстуална и телеологична гледна точка, като изключва „наказателния“ характер на обезщетението, дължимо на заинтересованите страни съгласно член 82 (т. 27—55), отбелязвайки, от една страна, че „държавите членки не трябва да избират (нито на практика имат право да направят това) измежду механизмите по глава VIII, за да гарантират защитата на данни. При наличието на нарушение, което не е причинило вреда, субектът на данните все още разполага с правото (най-малкото) да подаде жалба пред надзорния орган“, и от друга страна, че „възможността за получаване на обезщетение независимо от наличието на каквато и да била вреда вероятно би стимулирала образуването на гражданските производства в резултат от искове, които едва ли винаги ще бъдат основателни, и в този смисъл би могла да произведе възпиращ ефект по отношение на дейността по обработване на данни“ (т. 54 и 55).

естество, която може да бъде квалифицирана като утежнена поради предполагаема небрежност с посочените по-горе характеристики, включително по отношение на доказателството за освобождаване [29].

74. Следователно широкото тълкуване [30] на понятието (неимуществена) вреда не може да стигне дотам, че да предполага, че законодателят се е отказал от необходимостта реалната „щета“ да може да се конфигурира.

75. Истинският съществен проблем е дали, след като се установи наличието на нарушение и причинно-следствената връзка, правото на обезщетение може да възникне поради обикновени тревоги, безпокойства и страхове, изпитвани от засегнатото лице по отношение на евентуално бъдещо неправомерно използване на лични данни, ако такава злоупотреба не е установена и/или субектът на данните не е претърпял допълнителни щети.

76. Съгласно постоянната съдебна практика на Съда на понятията от разпоредбите от правото на ЕС, които не препращат изрично към правото на държавите членки за определяне на тяхното значение и обхват, обикновено трябва да се дава самостоятелно и еднакво тълкуване в целия Съюз, което трябва да се търси, като се вземе предвид буквалната формулировка на въпросната разпоредба, контекстът, в който е поставена, целите, преследвани от акта, част от който е тя, и генезисът на въпросната разпоредба [31].

77. Както беше напомнено от генерален адвокат Campos [32], Съдът не е установил едно общо определение за понятието „вреди“, което да е приложимо по еднакъв начин във всички области [33]. По отношение на неимуществените вреди от неговата съдебна практика може да се заключи, че: когато една от целите на разпоредбата, която трябва да се тълкува, е защитата на лицето или на определена категория лица [34], понятието за вреда трябва да бъде широко; в съответствие с този критерий, обезщетението обхваща нематериални вреди дори ако не е споменато в тълкуваната разпоредба [35].

[29] Следователно отказът на правото на обезщетение за леки и преходни чувства или емоции, свързани с нарушаването на правилата за обработване, не би оставил заинтересованата страна напълно без защита (в този смисъл вж. заключението на генерален адвокат Campos Sánchez-Bordona, посочено по-горе, т. 115).

[30] Или „в широк смисъл“ по думите на съображение 146.

[31] Вж. решения от 15 април 2021 г., The North of England P & I Association (C-786/19, EU:C:2021:276, т. 48) и от 10 юни 2021 г., KRONE — Verlag (C-65/20, EU:C:2021:471, т. 25).

[32] Вж. заключението на генерален адвокат Campos Sánchez-Bordona, посочено по-горе, точка 104.

[33] Нито е посочил предпочитан тълкувателен способ — самостоятелен или чрез препращане към националните правни системи: в зависимост от разглежданата област. Сравни решения от 10 май 2001 г., Veedfald (C-203/99, EU:C:2001:258, т. 27), относно дефектните продукти; от 6 май 2010 г., Walz (C-63/09, EU:C:2010:251, т. 21) относно отговорността на въздушните превозвачи и от 10 юни 2021 г., Van Ameyde España (C-923/19, EU:C:2021:475, т. 37 и сл.) относно режима на гражданска отговорност, приложим към произшествията, причинени при използването на моторни превозни средства.

[34] Например потребителите на стоки или жертвите на пътнотранспортни произшествия.

[35] В областта на комбинираните превози решение от 12 март 2002 г., Leitner (C-168/00, EU:C:2002:163), в областта на гражданската отговорност при използването на моторни превозни средства решения от 24 октомври 2013 г., Haasová (C-22/12, EU:C:2013:692, т. 47—50), от 24 октомври 2013 г., Drozdovs (C-277/12, EU:C:2013:685, т. 40), и от 23 януари 2014 г., Petillo (C-371/12, EU:C:2014:26, т. 35).

78. Дори практиката на Съда да допуска в този смисъл извода, че в правото на Съюза съществува принцип на обезщетяване на нематериалните вреди, съм съгласен с генерален адвокат Campos, че от тази практика не може да се изведе правило, че всяка нематериална вреда, независимо от нейната тежест, подлежи на обезщетяване [36].

79. В този смисъл предложеното на Съда разграничение между нематериални вреди, подлежащи на обезщетяване, и други неудобства, произтичащи от правонарушението, които поради незначителния им характер невинаги ще породят право на обезщетение, е обосновано [37].

80. Съдът допуска това разграничение, като приема безпокойството и неудобството за самостоятелна категория спрямо вредите в случаите, в които приема че същите трябва да бъдат обезщетени [38].

81. Емпирично може да се констатира, че всяко нарушение на правилата за защитата на личните данни ще предизвика някаква негативна реакция у субекта на данните. Обезщетението, дължимо само за чувството на безпокойство поради неспазването на закона от страна на друго лице, лесно би могло да се обърка с обезщетение без щети, което, както казахме, не изглежда да може да се конфигурира в случая, посочен в член 82 от Регламента.

82. Фактът, че при обстоятелства като тези в главното производство злоупотребата с лични данни е само потенциална, а не вече действителна, е достатъчен, за да се приеме, че субектът на данните може да е претърпял неимуществени вреди, причинени от нарушението на Регламента, при условие че заинтересованата страна докаже, че страхът от такава неправомерна употреба конкретно и действително му е причинил реални и сигурни емоционални вреди [39].

83. Границата между обикновеното раздразнение (неподлежащо на обезщетение) и действителната нематериална вреда (подлежаща на обезщетение) несъмнено е тънка, но националните съдилища, които имат задачата да определят тази граница за всеки отделен

[36] Вж. заключението на генерален адвокат Campos Sánchez-Bordona, посочено по-горе, точка 105. Съдът например е приел за съвместимо с европейските правила национално законодателство, което за целите на определяне на размера на обезщетението разграничава неимуществените вреди вследствие на телесни наранявания, причинени при произшествия, в зависимост от причината за настъпването на тези произшествия; вж. решение от 23 януари 2014 г., Petillo (C-371/12, EU:C:2014:26, диспозитив): правото на Съюза допуска „национално законодателство като разглежданото в главното производство, което предвижда особен режим на обезщетяване на неимуществените вреди вследствие на леки телесни наранявания, причинени при пътнотранспортни произшествия, който ограничава обезщетяването на тези вреди в сравнение с приетото относно обезщетяването на идентични вреди, настъпили при други обстоятелства, а не при такива произшествия“.

[37] Това разграничение се наблюдава в националните правни системи като неизбежна последица от социалния живот. Неотдавна в Италия във връзка със защитата на личните данни, Tribunale de Palermo, sez. I civile, решение от 05.10.2017 г. n. 5261, както и Cass Civ. Civ., Ord. sez. VI, n. 17383/2020. В Германия, наред с други, AG Diez, 07.11.2018 г. — 8 C 130/18; LG Karlsruhe, 02.08.2019 г. — 8 O 26/19, е AG Frankfurt am Main, 10.07.2020 г. — 385 C 155/19 (70). В Австрия, OGH 6 Ob 56/21k.

[38] Вж. решение от 23 октомври 2012 г., Nelson и др. (C-581/10 и C-629/10, EU:C:2012:657, т. 51) относно разграничението между „вреди“ по смисъла на член 19 от Конвенцията за уеднаквяване на някои правила за международния въздушен превоз, сключена в Монреал на 28 май 1999 г., и „неудобства“ по смисъла на Регламент № 261/2004, които дават право на обезщетение на основание член 7 от този регламент, съгласно решение от 19 ноември 2009 г., Sturgeon и др. (C-402/07 и C-432/07, EU:C:2009:716). В сектора на въздушния превоз, както и на превоза на пътници по море или по вътрешни водни пътища, за който се отнася Регламент № 1177/2010, законодателят е имал възможност да признае една абстрактна категория благодарение на това, че факторът, който създава безпокойството, и неговото естество са еднакви за всички засегнати лица. Не считам, че тази констатация е възможна в областта на защитата на данни.

[39] Според Ирландия тези съображения са особено важни в практиката и в контекста на киберпрестъпленията, тъй като ако всяко лице, дори минимално засегнато от нарушение, има право на обезщетение за нематериални вреди, това би имало голямо въздействие, особено върху администраторите в публичния сектор, които се финансират с ограничени публични средства и по-скоро трябва да служат на колективни интереси, включително подобряване на сигурността на личните данни (писмено становище, т. 72).

случай, следва да извършват внимателна оценка на всички елементи, предоставени от поискалата обезщетението заинтересована страна, която има задължението да представи точно, а не по общ начин, конкретни елементи, които могат да доведат до извода за „действително претърпени нематериални вреди“ поради нарушаване на личните данни, дори без те да достигат предварително определен праг на особена сериозност: важното е това да не бъде просто субективно възприятие, променливо и зависимо и от елементи на характера и личността, а обективиране на дискомфорт, макар и лек, но доказуем, на собствената физическа или психическа сфера или на собствения социален живот; естеството на засегнатите лични данни и значението, което те имат в живота на заинтересованата страна, и може би също възприятието, което към конкретния момент има обществото за този специфичен дискомфорт, свързан с нарушението на сигурността на данните [40].

IV. Заключение

84. Въз основа на всички гореизложени съображения предлагам на Съда да отговори на поставените преюдициални въпроси по следния начин:

„Членове 5, 24, 32 и 82 от Регламент 2016/679 трябва да се тълкуват в смисъл, че

самото наличие на „нарушение на сигурността на личните данни“, както е определено в член 4, параграф 12, само по себе си не е достатъчно, за да се заключи, че техническите и организационните мерки, приложени от администратора, не са били „подходящи“, за да гарантират защитата на въпросните данни;

когато проверява подходящия характер на техническите и организационните мерки, прилагани от администратора на лични данни, сезираният национален съд трябва да извърши проверка, която обхваща конкретен анализ както на съдържанието на тези мерки, така и на начина, по който са били приложени, и на техните практически ефекти;

в контекста на иск за обезщетение съгласно член 82 от GDPR, администраторът на лични данни има задължението да докаже, че мерките, които е приложил съгласно член 32 от настоящия регламент, са подходящи;

в съответствие с принципа на процесуална автономия вътрешният правен ред на всяка държава членка определя допустимите методи за доказване и тяхната доказателствена стойност, включително следствените действия, които националните съдилища могат или трябва да разпоредят, за да преценят дали администраторът на лични данни е приложил подходящи мерки съгласно настоящия регламент, в съответствие с принципите на равностойност и ефективност, определени от правото на Съюза;

фактът, че нарушението на този регламент, което е причинило въпросната вреда, е извършено от трето лице, само по себе си не представлява причина за освобождаване на администратора от отговорност и за да се възползва от предвиденото в разпоредбата освобождаване, той трябва да докаже, че по никакъв начин не е отговорен за нарушението;

[40] Вж. заключението на генерален адвокат Campos Sánchez-Bordona, посочено по-горе, точка 116.

вредата, състояща се в страх от потенциална бъдеща злоупотреба с личните данни на заинтересованата страна, чието съществуване тя е доказала, може да представлява неимуществена вреда, която дава право на обезщетение, при условие че заинтересованата страна докаже, че е претърпяла индивидуално реална и сигурна емоционална вреда, а задача на сезираната национална юрисдикция е да провери това във всеки отделен случай“.