Recueil de la jurisprudence

CONCLUSIONS DE L'AVOCAT GÉNÉRAL
M. GIOVANNI PITRUZZELLA
présentées le 27 avril 2023 [1]

Affaire C-340/21

VB
contre
Natsionalna agentsia za prihodite

[demande de décision préjudicielle formée par le Varhoven administrativen sad (Cour administrative suprême, Bulgarie)]

« Renvoi préjudiciel – Protection des données à caractère personnel – Règlement (UE) 2016/679 – Responsabilité du responsable du traitement – Sécurité du traitement – Violation de la sécurité du traitement des données à caractère personnel – Préjudice moral subi du fait d'une inaction du responsable du traitement – Action en réparation »

La diffusion illicite, en raison d'une attaque pirate, de données à caractère personnel détenues par une agence publique peut-elle donner lieu à réparation du préjudice moral au profit de la personne concernée par les données traitées, du seul fait que celle-ci redoute que ses données fassent l'objet d'une utilisation future abusive ? Quels sont les critères permettant d'imputer la responsabilité au responsable du traitement des données ? Comment les obligations en matière de charge de la preuve se répartissent-elles dans le cadre du contentieux ? Quelle est l'étendue du contrôle du juge ?

I. Le cadre juridique

1. L'article 4, intitulé « Définitions », du règlement (UE) 2016/679 [2] dispose :

« Aux fins du présent règlement, on entend par :

[...]

12) "violation de données à caractère personnel", une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données ;

[1] Langue originale : l'italien.

[2] Règlement du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (JO 2016, L 119, p. 1).

[…] »

2. L'article 5 de ce règlement, intitulé « Principes relatifs au traitement des données à caractère personnel », énonce :

«1. Les données à caractère personnel doivent être :

[…]

f) traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (intégrité et confidentialité).

2. Le responsable du traitement est responsable du respect du paragraphe 1 et est en mesure de démontrer que celui-ci est respecté (responsabilité). »

3. L'article 24 dudit règlement, intitulé « Responsabilité du responsable du traitement », dispose :

« 1. Compte tenu de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement met en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au présent règlement. Ces mesures sont réexaminées et actualisées si nécessaire.

2. Lorsque cela est proportionné au regard des activités de traitement, les mesures visées au paragraphe 1 comprennent la mise en œuvre de politiques appropriées en matière de protection des données par le responsable du traitement.

3. L'application d'un code de conduite approuvé comme le prévoit l'article 40 ou de mécanismes de certification approuvés comme le prévoit l'article 42 peut servir d'élément pour démontrer le respect des obligations incombant au responsable du traitement. »

4. L'article 32 de ce même règlement, intitulé « Sécurité du traitement », prévoit :

« 1. Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris entre autres, selon les besoins :

[…]

2. Lors de l'évaluation du niveau de sécurité approprié, il est tenu compte en particulier des risques que présente le traitement, résultant notamment de la destruction, de la perte, de l'altération, de la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou de l'accès non autorisé à de telles données, de manière accidentelle ou illicite.

3. L'application d'un code de conduite approuvé comme le prévoit l'article 40 ou d'un mécanisme de certification approuvé comme le prévoit l'article 42 peut servir d'élément pour démontrer le respect des exigences prévues au paragraphe 1 du présent article.

[...] »

5. L'article 82 du règlement 2016/679, intitulé « Droit à réparation et responsabilité », dispose :

« 1. Toute personne ayant subi un dommage matériel ou moral du fait d'une violation du présent règlement a le droit d'obtenir du responsable du traitement ou du sous-traitant réparation du préjudice subi.

2. Tout responsable du traitement ayant participé au traitement est responsable du dommage causé par le traitement qui constitue une violation du présent règlement. [...]

3. Un responsable du traitement ou un sous-traitant est exonéré de responsabilité, au titre du paragraphe 2, s'il prouve que le fait qui a provoqué le dommage ne lui est nullement imputable.

[...] »

II. Les faits, le litige et les questions préjudicielles

6. Le 15 juillet 2019, les médias bulgares ont rendu publique l'information selon laquelle un accès non autorisé au système informatique de la Natsionalna agentsia za prihodite (Agence nationale des recettes publiques, Bulgarie, ci-après la « NAP »)[3] avait été constaté et diverses informations publiées sur Internet, en matière de fiscalité et d'assurances sociales, concernant des millions d'individus tant ressortissants nationaux qu'étrangers.

7. De nombreuses personnes, parmi lesquelles VB, la requérante au principal, ont alors assigné la NAP devant les tribunaux pour obtenir réparation de leur préjudice moral.

8. En l'espèce, la requérante au principal a saisi l'Administrativen sad Sofia-grad (tribunal administratif de la ville de Sofia, Bulgarie, ci-après l'« ASSG »), faisant valoir que la NAP avait violé la réglementation nationale ainsi que l'obligation, en sa qualité de responsable du traitement des données, de traiter les données à caractère personnel de façon à « garantir un niveau de sécurité approprié » en adoptant des mesures techniques et organisationnelles appropriées conformément aux articles 24 et 32 du règlement 2016/679. La requérante a affirmé en outre avoir subi un préjudice moral se manifestant par une inquiétude et des craintes que ses données à caractère personnel puissent faire l'objet d'une utilisation future abusive.

9. La défenderesse a fait valoir, pour sa part, qu'elle n'avait reçu aucune demande de la requérante au principal visant à s'enquérir des données à caractère personnel précises auxquelles il avait été accédé. En outre, une fois informée de l'intrusion, elle indique avoir organisé des réunions avec les experts afin de protéger les droits et les intérêts des citoyens. Selon la NAP, le lien de causalité

[3] La NAP est responsable du traitement de données à caractère personnel au sens de l'article 4, point 7, du règlement 2016/679. Il s'agit, selon le droit national, d'un organisme administratif doté de compétences spécifiques, soumis à la tutelle du ministre des Finances, et chargé de la constatation, la préservation et la récupération des créances de l'État, publiques et privées, définies par la loi. Dans l'exercice des prérogatives de puissance publique qui lui sont dévolues, elle traite des données personnelles.

entre la cyberattaque et le préjudice allégué serait inexistant, l'agence ayant mis en œuvre tous les systèmes de gestion des processus et de la sécurité des informations conformément aux normes internationales en vigueur en la matière.

10. La juridiction de première instance, l'ASSG, a rejeté le recours, estimant que la diffusion des données n'était pas imputable à l'agence, que c'était à la requérante qu'incombait la charge de prouver le caractère (in)approprié des mesures adoptées et, enfin, qu'il n'existait pas de préjudice moral indemnisable.

11. Le jugement de première instance a ensuite fait l'objet d'un pourvoi en cassation devant le Varhoven administrativen sad (Cour administrative suprême, Bulgarie). Parmi les moyens soulevés, la requérante au principal a fait valoir que la juridiction de première instance aurait commis une erreur au sujet de la répartition de la charge de la preuve du défaut d'adoption de mesures de sécurité. Le préjudice moral ne devrait pas non plus constituer l'objet d'une preuve à administrer, dès lors qu'il s'agit d'un dommage moral réel et non purement potentiel.

12. De son côté, la NAP a maintenu avoir pris les mesures techniques et organisationnelles nécessaires en sa qualité de responsable du traitement et a contesté l'existence de la preuve d'un préjudice moral réel. L'anxiété et les craintes seraient, en effet, des états émotionnels n'ouvrant pas droit à réparation.

13. La juridiction de renvoi a constaté que les actions intentées par les personnes lésées à l'encontre de la NAP en vue d'obtenir réparation de leur dommage moral avaient abouti à des résultats disparates.

14. C'est dans ce contexte que le Varhoven administrativen sad (Cour administrative suprême) a sursis à statuer et a saisi la Cour des questions préjudicielles suivantes :

« 1) Les dispositions des articles 24 et 32 du [règlement 2016/679] peuvent-elles être interprétées en ce sens qu'une divulgation ou un accès non autorisés à des données à caractère personnel, au sens de l'article 4, point 12, [de ce règlement], par des personnes qui ne sont pas des employés de l'administration du responsable du traitement des données à caractère personnel et ne sont pas sous le contrôle de celui-ci, suffit pour considérer que les mesures techniques et organisationnelles mises en œuvre n'étaient pas appropriées ?

2) En cas de réponse négative à la première question, quels doivent être l'objet et l'étendue du contrôle juridictionnel de légalité lors de l'examen du point de savoir si les mesures techniques et organisationnelles mises en œuvre par le responsable du traitement des données à caractère personnel en vertu de l'article 32 du [règlement 2016/679] sont appropriées ?

3) En cas de réponse négative à la première question, le principe de responsabilité au sens de l'article 5, paragraphe 2, et de l'article 24, lus en combinaison avec le considérant 74 du [règlement 2016/679], peut-il être interprété en ce sens que, dans le cadre d'une action au titre de l'article 82, paragraphe 1, [de ce règlement], le responsable du traitement des données à caractère personnel supporte la charge de la preuve que les mesures techniques et organisationnelles mises en œuvre en vertu de l'article 32 dudit règlement sont appropriées ? Si la juridiction ordonne une expertise judiciaire, cela peut-il être considéré comme un moyen de preuve nécessaire et suffisant pour établir si les mesures techniques et

organisationnelles mises en œuvre par le responsable du traitement des données à caractère personnel étaient appropriées dans un cas de figure comme celui de l'espèce, où l'accès et la divulgation non autorisés résultent d'une "attaque de hackers" ?

4) La disposition de l'article 82, paragraphe 3, du [règlement 2016/679] peut-elle être interprétée en ce sens qu'une divulgation ou un accès non autorisés à des données à caractère personnel au sens de l'article 4, point 12, [de ce règlement], en l'espèce par une "attaque de hackers" commise par des personnes qui ne sont pas des employés de l'administration du responsable du traitement des données à caractère personnel et ne sont pas sous le contrôle de celui-ci, constitue un fait qui n'est nullement imputable au responsable du traitement des données à caractère personnel et représente un motif d'exonération de responsabilité ?

5) Les dispositions de l'article 82, paragraphes 1 et 2, lues en combinaison avec les considérants 85 et 146 du [règlement 2016/679], peuvent-elles être interprétées en ce sens que, dans un cas de figure comme celui de l'espèce, de violation de la sécurité de données à caractère personnel, se traduisant par un accès et une diffusion non autorisés de données personnelles, dans le cadre d'une "attaque de hackers", les préoccupations, les craintes et la peur, en tant que telles, de la personne concernée, d'un éventuel usage abusif futur de données personnelles, sans que soit établi un tel usage abusif et/ou que la personne concernée ait subi un autre dommage, relèvent du sens large de la notion de préjudice moral et justifient une indemnisation ? »

III. L'analyse juridique

A. Observations préliminaires

15. La présente affaire soulève des questions intéressantes et en partie inédites ayant trait à l'interprétation de plusieurs dispositions du règlement 2016/679 [4].

16. Les cinq questions préjudicielles s'articulent autour de la même interrogation : les conditions dans lesquelles le préjudice moral peut ouvrir droit à réparation en faveur d'une personne dont les données à caractère personnel, détenues par une agence publique, ont fait l'objet d'une publication sur Internet à la suite d'une attaque de hackers.

17. Pour la clarté de l'exposé, je proposerai des réponses synthétiques distinctes à l'ensemble des questions préjudicielles de la décision de renvoi, tout en étant conscient de l'existence de quelques recoupements conceptuels dès lors que les quatre premières questions visent toutes à identifier les

[4] L'article 5, paragraphe 2 (relatif au principe de responsabilité de tout responsable du traitement des données personnelles), l'article 24 (relatif aux mesures que ce responsable du traitement est tenu de mettre en œuvre pour garantir que le traitement soit conforme au règlement), l'article 32 (relatif à cette obligation en ce qui concerne spécifiquement la sécurité du traitement) et l'article 82, paragraphes 1 à 3 (relatif à la réparation des dommages résultant d'une violation de ce règlement et à la possibilité pour le responsable du traitement d'adopter des mesures pour garantir le respect de ce règlement), outre les considérants 74, 85 et 146 qui sont liés aux articles susdits.

conditions d'imputabilité au responsable du traitement de la violation des dispositions du règlement 2016/679 [5] et que la cinquième concerne plus spécifiquement la notion de dommage moral aux fins de la réparation [6].

18. Il est à signaler que plusieurs affaires relatives à l'article 82 du règlement 2016/679 sont actuellement pendantes devant la Cour et que, dans l'une d'elles, l'avocat général a déjà présenté ses conclusions, dont je tiendrai compte dans le cadre de la présente analyse [7].

19. Avant d'examiner les questions soulevées, il me semble opportun de formuler quelques remarques liminaires à propos des principes et des objectifs du règlement 2016/679, qui s'avèreront utiles pour résoudre chacune des questions préjudicielles.

20. L'article 24 du règlement 2016/679 instaure à titre général l'obligation pour le responsable du traitement de mettre en œuvre les mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement des données à caractère personnel est effectué conformément à ce règlement, tandis que l'article 32 dudit règlement instaure la même obligation de façon plus spécifique à l'égard de la sécurité du traitement. Ces articles 24 et 32 sont des déclinaisons plus détaillées de ce qui a d'abord été prévu à l'article 5, paragraphe 2, du règlement 2016/679, qui énonce, au nombre des « principes relatifs au traitement des données à caractère personnel », le principe de « responsabilité ». Ce principe vient logiquement à la suite et en complément du principe d'« intégrité et confidentialité », prévu à l'article 5, paragraphe 1, sous f), de ce règlement et les deux principes doivent se comprendre à la lumière de l'approche fondée sur les risques qui est à la base dudit règlement.

21. Le principe de responsabilité est l'un des piliers du règlement 2016/679 et l'une de ses innovations les plus significatives. Il assigne au responsable du traitement la responsabilité de prendre des mesures proactives pour assurer la conformité du traitement à ce règlement et être en mesure de démontrer cette conformité [8].

22. Dans la doctrine, des auteurs ont parlé d'un véritable changement de culture, en tant que conséquence de la « portée globale de l'obligation de responsabilité » [9]. Ce n'est pas tant le respect formel de l'obligation légale ou de la mesure ponctuelle que la stratégie d'ensemble adoptée par l'entreprise qui libère le responsable de sa responsabilité, en tant qu'entité *respectueuse* de la réglementation relative à la protection des données.

[5] a) La première vise à répondre à la question de savoir si l'on peut déduire de la simple violation le caractère inapproprié des mesures prescrites ; b) la deuxième concerne l'étendue du contrôle juridictionnel portant sur le caractère approprié de ces mesures ; c) la troisième se réfère à la charge de la preuve du caractère approprié proprement dit et à certaines modalités techniques d'obtention de la preuve ; d) la quatrième porte sur la pertinence, aux fins de l'exonération de la responsabilité, du fait que l'attaque lancée sur le système provient de l'extérieur.

[6] Quant aux dispositions du règlement 2016/679 citées, les trois premières questions concernent les aspects de la responsabilité du responsable du traitement liés au caractère approprié des mesures à adopter (articles 5, 24 et 32), la quatrième et la cinquième, les conditions d'exonération de la responsabilité et la notion de dommage moral ouvrant droit à réparation (article 82).

[7] Voir conclusions de l'avocat général Campos Sánchez-Bordona dans l'affaire Österreichische Post (préjudice moral lié au traitement de données à caractère personnel) (C-300/21, EU:C:2022:756).

[8] Docksey, C., « Article 24 : Responsability of the controller », dans Kuner, C., Bygrave, L. A., Docksey, C., Dreschler, L., *The EU General Data Protection Regulation (GRPD) : A Commentary*, Oxford University Press, 2020, p. 561. Les principes et les obligations issues des réglementations sur la protection des données devraient imprégner le tissu culturel des organisations, à tous les niveaux, plutôt que d'être considérés comme une série d'exigences devant être imposées par le service juridique.

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

23. Les mesures techniques et organisationnelles exigées par le principe de responsabilité doivent être « appropriées » au regard des éléments spécifiques mentionnés à l'article 24 du règlement 2016/679, à savoir la nature, la portée, le contexte et les finalités du traitement ainsi que la probabilité et la gravité des risques pour les droits et libertés des personnes physiques.

24. Cet article 24 requiert par conséquent que ces mesures présentent un caractère approprié pour que puisse être démontrée la conformité du traitement aux principes et aux dispositions du règlement 2016/679.

25. L'article 32 de ce règlement projette, quant à lui, le principe de responsabilité sur les mesures concrètes à prendre afin de garantir « un niveau de sécurité adapté au risque ». Et ce faisant, il ajoute l'état des connaissances et les coûts de mise en œuvre aux éléments déjà prévus, à prendre en compte dans l'élaboration des mesures techniques et organisationnelles.

26. La notion de caractère approprié suppose l'acceptabilité tant technique (la pertinence des mesures) que qualitative (l'efficacité de la protection) des solutions adoptées pour protéger les systèmes informatiques. Afin de garantir le respect des principes de nécessité, de pertinence et de proportionnalité, les traitements doivent être non seulement appropriés, mais aussi satisfaisants au regard des objectifs poursuivis. Et, dans cette logique, le principe de minimisation, en vertu duquel toutes les étapes du traitement des données doivent constamment tendre à réduire à leur plus bas niveau les risques pour la sécurité, joue un rôle déterminant [10].

27. L'idée qui imprègne le règlement 2016/679 tout entier est la prévention du risque ainsi que la responsabilité du responsable du traitement et, par conséquent, une démarche de type téléologique visant à atteindre le meilleur résultat possible en termes d'efficacité, ce qui signifie que l'on est loin des logiques formalistes liées à une simple obligation de respecter des procédures spécifiques pour se libérer de la responsabilité [11].

28. L'article 24 de ce règlement ne contient pas de liste exhaustive des mesures « appropriées » : il faudra procéder à une appréciation au cas par cas. Cela est conforme à la philosophie dudit règlement, qui explique que l'on ait préféré que les procédures à adopter soient choisies sur la base d'une évaluation minutieuse de la situation spécifique, de manière à ce qu'elles puissent être aussi efficaces que possible [12].

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

[11] Pour cette raison, comme nous le verrons, la première et la quatrième question ne peuvent recevoir une réponse autre que négative. Aucun automatisme ne peut être déduit des dispositions du règlement 2016/679 : le seul fait qu'il y ait eu une divulgation des données à caractère personnel ne suffit pas pour que l'on en conclue que les mesures techniques et organisationnelles adoptées ne sont pas appropriées, et la circonstance que la divulgation a eu lieu par suite de l'intervention de sujets étrangers à la structure du responsable du traitement et échappant à son contrôle ne suffit pas non plus pour exonérer celui-ci de sa responsabilité.

[12] Bolognini, L., Pelino, E., *Codice della disciplina privacy*, Giuffrè, 2019, p. 201. Le législateur européen ne s'en tient donc pas à une conception de la sécurité du traitement basée sur l'existence de mesures de sécurité prédéterminées, il adopte la méthodologie propre aux normes internationales en matière de gestion des systèmes d'information, basée sur le risque : celle-ci prévoit l'identification des mesures visant à réduire les risques, ne dépendant pas de check-lists préétablies et d'application générale. Il convient donc de se référer à des lignes directrices et à des normes internationales. Le fruit de cette évaluation des risques prend ensuite une valeur contraignante au moment où l'entité met en œuvre des décisions afin de réduire les risques identifiés, s'en rendant ainsi responsable.

B. Sur la première question préjudicielle

29. Par sa première question, la juridiction de renvoi demande, en substance, si les articles 24 et 32 du règlement 2016/679 doivent être interprétés en ce sens que l'existence d'une « violation de données à caractère personnel », telle que définie à l'article 4, paragraphe 12, de ce règlement, est suffisante pour conclure que les mesures techniques et organisationnelles mises en œuvre par le responsable du traitement n'étaient pas « appropriées » aux fins de la protection des données.

30. Il ressort du libellé des articles 24 et 32 du règlement 2016/679 que, lorsqu'il réfléchit aux mesures techniques et organisationnelles qu'il est tenu de mettre en œuvre afin d'assurer le respect de ce règlement, le responsable du traitement doit tenir compte d'un ensemble de paramètres d'évaluation, énumérés dans ces articles et rappelés ci-dessus.

31. Le responsable du traitement dispose d'une certaine marge de manœuvre pour déterminer quelles sont les mesures les plus appropriées au regard de sa situation spécifique, mais ce choix n'en est pas moins soumis à un éventuel contrôle juridictionnel quant à la conformité des mesures appliquées à l'ensemble des obligations et des objectifs du règlement 2016/679.

32. En particulier, pour ce qui est des mesures de sécurité, l'article 32, paragraphe 1, de ce règlement impose au responsable du traitement de tenir compte de l'« état des connaissances ». Cela implique que le niveau technologique des mesures à mettre en œuvre ne saurait aller au-delà de ce qui est raisonnablement possible à la date d'adoption des mesures : l'aptitude de la mesure à prévenir le risque devra donc être fonction des solutions offertes par l'état contemporain d'avancement de la science, de la technique, de la technologie et de la recherche, compte tenu également, comme on le verra, des coûts de mise en œuvre.

33. Des mesures peuvent être « appropriées » à un moment donné et être, malgré tout, contournées par des cybercriminels recourant à des outils très sophistiqués capables de violer aussi des mesures de sécurité conformes à l'état des connaissances.

34. Par ailleurs, il serait illogique de considérer que l'intention du législateur de l'Union a été d'imposer au responsable du traitement l'obligation d'empêcher toute violation de données à caractère personnel indépendamment de la diligence ayant présidé à l'élaboration des mesures de sécurité [13].

35. Comme on l'a vu, le règlement 2016/679 s'inscrit dans une optique éloignée des automatismes, exigeant du responsable du traitement une responsabilité importante, mais qui ne saurait conduire à l'impossibilité pour celui-ci de démontrer qu'il s'est correctement acquitté des obligations lui incombant.

36. En outre, l'article 32, paragraphe 1, de ce règlement prévoit la prise en compte, comme il a été dit, des « coûts de mise en œuvre » des mesures techniques et organisationnelles en cause. Il s'ensuit que l'appréciation du caractère approprié de ces mesures doit reposer sur une mise en balance des intérêts de la personne concernée, qui cibleront en général un niveau de protection

[13] L'expression « caractère approprié » montre sans équivoque l'intention de ne pas considérer comme pertinentes toutes les mesures techniques et organisationnelles abstraitement concevables. Voir, en ce sens, Gambini, M., « Responsabilità e risarcimento nel trattamento dei dati personali », dans Cuffaro, V., D'Orazio, R., Ricciuto, V., *I dati personali nel diritto europeo*, Giappichelli, 2019, p. 1059.

plus élevé, et des intérêts économiques ainsi que de la capacité technologique du responsable du traitement, qui pointent parfois vers un niveau de protection moindre. Cette mise en balance doit respecter les exigences du principe général de proportionnalité.

37. Il convient d'ajouter à cela, dans une optique d'interprétation systématique, que le législateur envisage la possibilité que surviennent des violations des systèmes ; en effet, cet article 32, paragraphe 1, sous c), inclut, parmi les mesures suggérées, la capacité de rétablir en temps utile la disponibilité et l'accès des données à caractère personnel en cas d'incident physique ou technique. Il n'y aurait aucun intérêt à prévoir une telle capacité au nombre des mesures de sécurité garantissant un niveau de sécurité adapté au risque si l'on considérait que la seule violation des systèmes représente en soi la preuve du caractère inapproprié des mesures.

C. Sur la deuxième question préjudicielle

38. Par sa deuxième question, la juridiction de renvoi demande, en substance, quels doivent être l'objet et l'étendue du contrôle juridictionnel quant au caractère approprié des mesures techniques et organisationnelles mises en œuvre par le responsable du traitement des données à caractère personnel au sens de l'article 32 du règlement 2016/679.

39. Étant donné la variété des situations pouvant se rencontrer dans la pratique, ce règlement ne prescrit pas, comme nous l'avons vu, de dispositions contraignantes en ce qui concerne la détermination des mesures techniques et organisationnelles que le responsable du traitement est tenu d'adopter pour respecter les exigences dudit règlement. Le caractère approprié des mesures adoptées devra donc être apprécié in concreto, il s'agira de vérifier si les mesures spécifiques étaient aptes à prévenir raisonnablement le risque et à minimiser les effets négatifs de la violation.

40. S'il est vrai que le choix et la mise en œuvre de ces mesures relèvent de l'appréciation subjective du responsable du traitement, puisque les mesures mentionnées dans le règlement 2016/679 ne sont que des exemples, le contrôle du juge ne peut pas se limiter à constater un respect, de la part du responsable du traitement, des obligations découlant des articles 24 et 32 de ce règlement se traduisant par la prévision (formelle) de certaines mesures techniques et organisationnelles. La juridiction doit procéder à une analyse concrète du contenu de ces mesures, de la façon dont elles ont été appliquées et de leurs effets pratiques, sur la base des éléments de preuve dont elle dispose et des circonstances du cas d'espèce. Comme l'a fait observer avec justesse le gouvernement portugais, « la manière dont [le responsable] a rempli ses obligations apparaît indissociable de la teneur des mesures adoptées, afin de démontrer que, compte tenu du traitement spécifique des données (sa nature, sa portée, son contexte et ses finalités), de l'état de l'art des technologies disponibles et de leurs coûts, tout comme des risques pour les droits et libertés des citoyens, le responsable du traitement a pris toutes les mesures nécessaires et appropriées pour assurer un niveau de sécurité adapté au risque sous-jacent » [14].

41. Le contrôle juridictionnel devra donc tenir compte de tous les paramètres indiqués aux articles 24 et 32 du règlement 2016/679 qui, comme nous l'avons dit, énumèrent une série de critères permettant d'évaluer le caractère approprié et fournissent des exemples de mesures pouvant être considérées comme appropriées. En outre, comme l'ont relevé la Commission et tous les États membres ayant présenté des observations à propos de la deuxième question, l'article 32, paragraphes 1 à 3, souligne la nécessité de « garantir un niveau de sécurité adapté au

[14] Observations écrites, point 31.

risque » en citant d'autres éléments pertinents à cet effet, tels que l'adoption éventuelle par le responsable du traitement d'un code de conduite approuvé ou d'un système de certification approuvé, ainsi que le prévoient respectivement les articles 40 et 42 dudit règlement.

42. L'adoption de codes de conduite ou de systèmes de certification peut fournir un élément d'appréciation utile, aux fins de la preuve à apporter et du contrôle juridictionnel y afférent, étant précisé toutefois qu'il ne suffit pas au responsable du traitement d'adhérer à un code de conduite, mais qu'il lui appartient de prouver qu'il a pris concrètement les mesures que ce code prévoit, conformément au principe de responsabilité. La certification constitue, en revanche, « en soi une preuve de la conformité au règlement des traitements effectués même si elle est susceptible d'être démentie sur le plan pratique » [15].

43. Enfin, il convient d'observer que ces mesures doivent être réexaminées et actualisées si nécessaire, ainsi que le prévoit l'article 24, paragraphe 1, du règlement 2016/679. Cela fera aussi l'objet d'une appréciation de la part de la juridiction nationale. L'article 32, paragraphe 1, de ce règlement [16] impose en effet au responsable du traitement un devoir de contrôle et de surveillance constante, préalable et postérieure aux activités de traitement, mais aussi de maintenance et d'actualisation éventuelle des mesures prises, dans le but à la fois de prévenir les violations et, le cas échéant, d'en limiter les effets.

44. J'aurais tendance à penser cependant qu'il n'est pas opportun que l'arrêt à intervenir inclue une énumération d'éléments de fond telle que celle suggérée par le gouvernement portugais [17]. Cela pourrait laisser place à des interprétations contradictoires, puisqu'il est évident que l'énumération ne peut jamais être exhaustive.

D. Sur la troisième question préjudicielle

45. Dans la première partie de sa troisième question, la juridiction de renvoi demande en substance à la Cour de préciser si, compte tenu du principe de responsabilité énoncé à l'article 5, paragraphe 2, ainsi qu'à l'article 24, lu conjointement avec le considérant 74 [18] du règlement 2016/679, la charge de la preuve du caractère approprié des mesures techniques et

[15] Gambini, M., op. cit., p. 1067. Le fait de disposer d'une certification a par conséquent pour effet de renverser la charge de la preuve, en faveur du responsable, lequel peut plus facilement démontrer qu'il a agi dans le respect des obligations prévues par le règlement 2016/679.

[16] En prévoyant expressément au point d) que le contrôle du caractère approprié s'étend à l'efficacité des mesures adoptées, devant être régulièrement testée, analysée et évaluée, tant au stade initial que périodiquement, afin d'assurer la sécurité effective de tous les types de traitement, quel que soit le niveau de risque qu'ils présentent, et en prévoyant explicitement au point c) que les mesures techniques et organisationnelles mises en œuvre doivent avoir la capacité de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique. Voir Gambini, M., op. cit., p. 1064 et 1065.

[17] Point 30 des observations écrites : « [I]l incombera au responsable du traitement de démontrer comment il a évalué l'ensemble des facteurs et circonstances liés au traitement en question, et, notamment, le résultat de l'analyse des risques effectuée, les risques identifiés, les mesures concrètes trouvées pour atténuer ces risques, la justification des options retenues compte tenu des solutions technologiques disponibles sur le marché, l'efficacité des mesures, la corrélation entre les mesures techniques et organisationnelles, la formation du personnel traitant les données, l'existence d'une sous-traitance des opérations de traitement des données, y compris le développement et la maintenance informatique, et l'existence d'un contrôle par le responsable du traitement et d'instructions précises données aux sous-traitants, conformément à l'article 28 du [règlement 2016/679], sur le traitement des données par ces derniers; comment l'infrastructure de support des systèmes d'information et de communication et d'information a été évaluée et comment le niveau de risque pour les droits et libertés des personnes concernées a été classé. »

[18] En vertu du considérant 74 : « Il y a lieu d'instaurer la responsabilité du responsable du traitement pour tout traitement de données à caractère personnel qu'il effectue lui-même ou qui est réalisé pour son compte. Il importe, en particulier, que le responsable du traitement soit tenu de mettre en œuvre des mesures appropriées et effectives et soit à même de démontrer la conformité des activités de traitement avec le présent règlement, y compris l'efficacité des mesures. Ces mesures devraient tenir compte de la nature, de la portée, du contexte et des finalités du traitement ainsi que du risque que celui-ci présente pour les droits et libertés des personnes physiques. »

organisationnelles visées à l'article 32 de ce règlement pèse sur le responsable du traitement des données à caractère personnel dans le cadre d'une action en réparation au titre de l'article 82 dudit règlement.

46. Les considérations qui précèdent me permettent de répondre succinctement à cette question par l'affirmative.

47. La lettre de la loi, le contexte et la finalité du règlement 2016/679 plaident, en effet, de manière univoque en faveur de la solution consistant à faire supporter la charge de la preuve au responsable du traitement.

48. De la formulation de diverses dispositions de ce règlement il résulte que le responsable du traitement doit être « à même de » ou « capable » de « démontrer » le respect des obligations prévues par le règlement, et, en particulier, la mise en œuvre des mesures appropriées à cette fin, comme indiqué au considérant 74, à l'article 5, paragraphe 2, et à l'article 24, paragraphe 1, dudit règlement. Ainsi que le souligne le gouvernement portugais, le considérant 74 précise que la preuve ainsi mise à la charge du responsable doit comprendre la preuve de l'« efficacité des mesures » en question.

49. Cette interprétation littérale me semble confortée par les considérations d'ordre pratique et téléologique suivantes.

50. En ce qui concerne la répartition de la charge de la preuve dans le cadre d'une action en réparation fondée sur l'article 82 du règlement 2016/679, celui qui a intenté l'action contre le responsable du traitement doit établir, premièrement, qu'il y a eu violation du règlement, deuxièmement, qu'il a subi un préjudice et, troisièmement, qu'il existe un lien de causalité entre les deux éléments précédents, ainsi qu'il a été relevé dans toutes les observations écrites présentées à propos de la cinquième question préjudicielle. Il s'agit de trois conditions cumulatives, comme l'indiquent également la jurisprudence constante de la Cour et du Tribunal, dans le contexte de la responsabilité extracontractuelle de l'Union [19].

51. J'estime toutefois que l'obligation qui pèse sur le requérant de démontrer l'existence d'une violation du règlement 2016/679 ne peut pas aller jusqu'à requérir qu'il démontre en quoi les mesures techniques et organisationnelles mises en œuvre par le responsable du traitement ne sont pas appropriées au regard des articles 24 et 32 de ce règlement.

52. Ainsi que le souligne la Commission, il serait souvent quasi impossible de rapporter de telles preuves dans la pratique, les personnes concernées n'ayant généralement ni une connaissance suffisante pour pouvoir analyser ces mesures, ni un accès à toutes les informations qui sont en possession du responsable du traitement contesté, en particulier pour ce qui est des méthodes appliquées afin d'assurer la sécurité de ce traitement. En outre, le responsable du traitement pourrait parfois soutenir que son refus de révéler ces éléments aux personnes concernées repose sur le motif légitime de ne pas rendre publics ses affaires internes ou des éléments couverts par le secret professionnel, notamment pour des raisons de sécurité.

[19] Voir, en particulier, arrêts du 5 septembre 2019, Union européenne/Guardian Europe et Guardian Europe/Unione europea (C-447/17 P et C-479/17 P, EU:C:2019:672, point 147), du 28 octobre 2021, Vialto Consulting/Commission (C-650/19 P, EU:C:2021:879, point 138), du 13 janvier 2021, Helbert/EUIPO (T-548/18, EU:T:2021:4, point 116), et du 29 septembre 2021, Kočner/Europol (T-528/20, non publié, EU:T:2021:631, point 61), où il est rappelé que trois conditions doivent être remplies, à savoir « l'illégalité du comportement reproché à l'institution de l'Union, la réalité du dommage et l'existence d'un lien de causalité entre le comportement de cette institution et le dommage invoqué ».

53. C'est pourquoi, s'il était considéré que la charge de la preuve pèse sur la personne concernée, le résultat pratique serait que le droit de recours prévu à l'article 82, paragraphe 1, du règlement 2016/679 se verrait en grande partie vidé de sa substance. À mon avis, cela ne serait pas conforme aux intentions du législateur de l'Union qui, avec l'adoption de ce règlement, a cherché à renforcer les droits des personnes concernées ainsi que les obligations des responsables du traitement, par rapport à la directive 95/46 que ledit règlement a remplacée. Il est donc plus logique, et juridiquement défendable, que ce soit au responsable du traitement de démontrer, lorsqu'il se défend face à une action en réparation, qu'il a respecté les obligations découlant des articles 24 et 32 de ce même règlement en prenant des mesures effectivement appropriées.

54. Dans la seconde partie de sa troisième question, la juridiction de renvoi interroge la Cour, en substance, sur le point de savoir si une expertise judiciaire peut être considérée comme une preuve nécessaire et suffisante, aux fins de l'appréciation du caractère approprié des mesures techniques et organisationnelles mises en œuvre par le responsable du traitement des données à caractère personnel, dans un cas où l'accès aux données à caractère personnel et leur diffusion non autorisés sont le résultat d'une activité de piratage.

55. Je suis d'avis que la réponse à ces questions doit, comme l'ont souligné (en substance) également les gouvernements bulgare et italien, ainsi que l'Irlande et la Commission, se fonder sur notre jurisprudence constante en vertu de laquelle, conformément au principe d'autonomie procédurale, il appartient à l'ordre juridique interne de chaque État membre, en l'absence de règles de l'Union en la matière, de régler les modalités procédurales des procédures judiciaires destinées à sauvegarder les droits des personnes, à condition toutefois que ces règles ne soient pas, dans les situations régies par le droit de l'Union, moins favorables que celles régissant des situations similaires soumises au droit national (principe d'équivalence) et qu'elles ne rendent pas impossible en pratique ou excessivement difficile l'exercice des droits conférés par le droit de l'Union (principe d'effectivité).

56. En l'espèce, on observe que le règlement 2016/679 ne contient aucune disposition visant à définir les moyens de preuve admissibles et leur force probante, notamment pour ce qui est des mesures d'instruction (telles qu'une expertise judiciaire) que les juridictions nationales peuvent ou doivent ordonner pour apprécier si un responsable du traitement des données à caractère personnel a pris des mesures appropriées au sens de ce règlement. Je considère donc que, en l'absence de règles harmonisées en la matière, il appartient à l'ordre juridique interne de chaque État membre de déterminer ces modalités procédurales, sous réserve du respect des principes d'équivalence et d'effectivité.

57. Le « principe d'effectivité », qui présuppose l'obligation pour un juge indépendant de procéder à une appréciation impartiale, pourrait être remis en cause si l'adjectif « suffisant » devait être compris dans le sens que semble lui attribuer la juridiction de renvoi, à savoir que la juridiction pourrait déduire automatiquement d'une expertise la conclusion que les mesures prises par le responsable du traitement sont appropriées [20].

E. Sur la quatrième question préjudicielle

58. Dans sa quatrième question, la juridiction de renvoi demande, en substance, si l'article 82, paragraphe 3, du règlement 2016/679 doit être interprété en ce sens que, en cas de violation de ce règlement (consistant, comme en l'espèce, en la « divulgation non autorisée » ou en l'« accès non

[20] Observations écrites, point 39.

autorisé » à des données à caractère personnel au sens de l'article 4, paragraphe 12, dudit règlement), de la part de personnes qui ne sont pas des employés du responsable du traitement de ces données et ne sont pas sous le contrôle de celui-ci, on est en présence d'un événement nullement imputable au responsable du traitement et, partant, d'une cause d'exonération de sa responsabilité au sens dudit article 82, paragraphe 3.

59. La réponse à cette question découle directement de ce qui a été expliqué plus haut concernant la philosophie générale du règlement 2016/679 : aucun automatisme n'est prévu et, par voie de conséquence, le seul fait que la divulgation ou l'accès non autorisés à des données à caractère personnel se sont produits à cause de personnes étrangères au périmètre de contrôle du responsable du traitement n'exonère pas ce dernier de sa responsabilité.

60. Tout d'abord, du point de vue littéral, il convient de noter que pas plus l'article 82, paragraphe 3, que le considérant 146 ne prévoient de conditions particulières pouvant être remplies pour que le responsable du traitement soit exonéré de sa responsabilité, si ce n'est celle de démontrer que « le fait dommageable ne lui est nullement imputable ». Il ressort de cette formulation, d'une part, que le responsable du traitement ne peut s'exonérer de sa responsabilité que s'il démontre que le fait ayant entraîné le dommage en cause ne lui est pas imputable et, d'autre part, que cette disposition requiert un niveau de preuve élevé, en raison de l'emploi du terme « nullement », comme l'a souligné la Commission [21].

61. Le régime de responsabilité prévu par l'article 82 et, plus généralement, par l'ensemble du règlement 2016/679, a fait l'objet de débats extensifs dans la doctrine des divers États membres. En effet, il inclut des éléments traditionnels propres à la responsabilité extracontractuelle, mais aussi des éléments qui, dans l'architecture des dispositions, le rapprochent de la responsabilité contractuelle, voire d'une forme de responsabilité objective, en raison de la dangerosité intrinsèque de l'activité de traitement des données. Ce n'est pas le lieu adéquat pour rendre compte du débat en détail, mais, à mon avis, cet article 82 ne paraît pas instituer un régime de responsabilité sans faute [22].

62. Le préjudice résultant d'une violation de données à caractère personnel peut être défini comme la conséquence fautive de l'absence d'adoption des mesures techniques et organisationnelles raisonnables et, en tout cas, appropriées pour prévenir ce préjudice, compte tenu des risques pour les droits et libertés des personnes liés à l'activité de traitement. De tels risques rendent plus stricte l'obligation de prévenir et d'éviter le dommage, le devoir de diligence incombant au responsable du traitement se voyant ainsi renforcé. C'est pourquoi une lecture coordonnée des obligations de conduite incombant aux responsables du traitement et de la disposition relative à la preuve libératoire pour l'auteur du dommage pourrait inciter à

[21] Conformément à la jurisprudence constante de la Cour en vertu de laquelle les exceptions à une règle générale doivent être interprétées de façon restrictive, l'éventuelle exonération de responsabilité prévue par l'article 82, paragraphe 3, doit être interprétée de façon stricte. Voir, par analogie, arrêts du 15 octobre 2020, Association française des usagers de banques (C-778/18, EU:C:2020:831, point 53), et du 5 avril 2022, Commissioner of An Garda Síochána e.a. (C-140/20, EU:C:2022:258, point 40).

[22] La responsabilité civile tend à être qualifiée d'objective chaque fois que l'auteur est tenu d'adopter toutes les mesures abstraitement possibles pour éviter le préjudice, indépendamment de la connaissance effective qu'il en avait ou de leur faisabilité économique. Inversement, lorsque l'auteur se voit imposer d'adopter les mesures devant normalement être respectées par un opérateur du secteur économique de référence pour maintenir la sécurité et prévenir les préjudices pouvant découler de l'activité exercée, l'imputation du dommage a tendance à s'axer sur un régime de responsabilité pour faute spécifique. Gambini, M., op. cit., p. 1055.

reconnaître la nature de responsabilité aggravée, pour faute présumée, au régime de responsabilité découlant du traitement illicite de données à caractère personnel prévue par l'article 82 du règlement 2016/679 [23].

63. Il en découle que le responsable du traitement a la possibilité de fournir une preuve libératoire (non admise dans le cadre d'une responsabilité objective). En ce qui concerne la répartition du fardeau de la preuve, l'article 82, paragraphe 3, du règlement 2016/679 prévoit un système favorable à la victime, en instituant une sorte de renversement de la charge de la preuve de la faute de l'auteur du dommage [24], dans un rapport de parfaite symétrie avec le renversement, évoqué plus haut, de la charge de la preuve du caractère approprié des mesures adoptées. Le législateur montre ainsi qu'il est conscient des dangers inhérents à l'admission d'une répartition différente de la charge de la preuve qui, si l'on faisait peser l'obligation de prouver la faute de l'auteur du dommage sur la personne physique lésée, aboutirait à obérer excessivement la position de celle-ci et, partant, à compromettre, dans les faits, l'efficacité de la protection résidant dans l'action en réparation, dans un contexte de règles liées à l'emploi des nouvelles technologies. En effet, il pourrait s'avérer particulièrement onéreux pour la personne concernée d'identifier les modalités de production du dommage et d'y avoir accès, et, partant, de démontrer la faute du responsable. À l'inverse, le responsable du traitement est le mieux placé pour offrir la preuve libératoire visant à établir que le fait dommageable ne lui est nullement imputable [25].

64. Le responsable du traitement devra également démontrer, conformément au principe de responsabilité décrit ci-dessus, qu'il a fait tout son possible pour rétablir en temps utile la disponibilité et l'accès aux données à caractère personnel.

65. Pour en venir à la question de la juridiction de renvoi, sur la base de ce qui vient d'être exposé quant à la nature de la responsabilité du responsable du traitement, si, comme nous l'avons vu, le responsable du traitement peut être exonéré de sa responsabilité en démontrant que la violation est due à une cause qui ne lui est nullement imputable, le seul fait que l'événement a été causé par une personne échappant à son contrôle ne saurait être considéré comme une telle cause.

66. Lorsqu'un responsable du traitement est victime d'une attaque de la part de cybercriminels, l'événement qui a donné naissance au dommage pourrait être considéré comme n'étant pas imputable au responsable du traitement des données, mais il n'est pas exclu que la négligence de celui-ci ait été à l'origine de l'attaque en question, en la facilitant du fait de l'absence ou du caractère inapproprié des mesures de sécurité des données à caractère personnel qu'il est tenu de mettre en œuvre. Il s'agit d'appréciations de fait, propres à chaque cas, qui sont laissées à la juridiction nationale saisie, au vu des preuves produites devant elle.

67. En outre, l'expérience commune montre que les attaques externes vis-à-vis des systèmes d'entités publiques ou privées détentrices d'une grande quantité de données à caractère personnel sont bien plus fréquentes que les attaques internes. Le responsable du traitement doit donc mettre en place des mesures appropriées pour faire face tout particulièrement aux attaques externes.

[23] Gambini, M., op. cit., p. 1059. Il en va de même de l'opinion selon laquelle la preuve de l'adoption des mesures idoines consiste non pas dans la simple allégation de la plus grande diligence exigible, mais dans la démonstration d'un évènement extérieur, générateur du dommage, présentant les caractères d'imprévisibilité et d'inévitabilité propres au cas fortuit ou à la force majeure, Sica, S, « Sub art. 82 », dans D'Orazio, R., Finocchiaro, G., Pollicino, O., Resta, G., *Codice della privacy e data protection*, Giuffrè, 2021.

[24] « [S]'il *prouve* que le fait qui a provoqué le dommage ne lui est nullement imputable. » Mise en italique par mes soins.

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

68. Enfin, d'un point de vue téléologique, il convient de noter que le règlement 2016/679 se fixe pour objectif de conférer un niveau élevé de protection. À cet égard, la Cour a déjà souligné qu'il ressort de l'article 1er, paragraphe 2, de ce règlement, lu conjointement avec ses considérants 10, 11 et 13, que ledit règlement impose aux institutions, aux organes, organismes et agences de l'Union et aux autorités compétentes des États membres d'assurer un niveau élevé de protection des droits relatifs à la protection des données à caractère personnel garantis par l'article 16 TFUE et l'article 8 de la charte des droits fondamentaux de l'Union européenne [26].

69. Si la Cour devait opter pour l'interprétation en vertu de laquelle, dans le cas où la violation du règlement 2016/679 a été commise par un tiers, le responsable du traitement doit être automatiquement exonéré de sa responsabilité en vertu de l'article 82, paragraphe 3, de ce règlement, une telle interprétation produirait un effet incompatible avec l'objectif de protection poursuivi par cet instrument, car elle affaiblirait les droits des personnes concernées, en ce qu'elle limiterait cette responsabilité aux seuls cas dans lesquels la violation est due à des personnes placées sous l'autorité et/ou le contrôle du responsable du traitement.

F. Sur la cinquième question préjudicielle

70. Par sa cinquième question, la juridiction nationale demande à la Cour, en substance, d'interpréter la notion de « dommage moral » au sens de l'article 82 du règlement 2016/679. En particulier, elle demande si les dispositions de l'article 82, paragraphes 1 et 2, de ce règlement, lues conjointement avec les considérants 85 et 146 de celui-ci [27], doivent être interprétées en ce sens que, dans un cas où la violation dudit règlement a consisté en un accès non autorisé à des données à caractère personnel et en une divulgation non autorisée de ces données par des cybercriminels, le fait que la personne concernée craigne une éventuelle utilisation future abusive de ses données à caractère personnel peut constituer en soi un préjudice (moral) ouvrant droit à réparation.

71. Ni l'article 82 ni les considérants relatifs à la réparation du dommage ne fournissent une réponse claire à la question, mais il est possible d'en retirer certains éléments utiles pour l'analyse de la question : le dommage moral peut faire l'objet d'une indemnisation en plus du dommage matériel (ou patrimonial) ; de la violation du règlement 2016/679 ne découle pas automatiquement le dommage qu'elle a « causé » ou, plus précisément, la violation de données à caractère personnel « peut causer » des dommages physiques, matériels ou moraux aux personnes physiques ; la notion de dommage devrait être interprétée « au sens large » à la lumière de la jurisprudence de la Cour, d'une manière qui tienne pleinement compte des objectifs du règlement 2016/679, et la réparation du dommage « subi » devrait être « complète et effective ».

[26] Voir, en ce sens, arrêt du 15 juin 2021, Facebook Ireland e.a (C-645/19, EU:C:2021:483, points 44 et 45).

[27] En vertu du considérant 85, « [u]ne violation de données à caractère personnel risque, si l'on n'intervient pas à temps et de manière appropriée, de causer aux personnes physiques concernées des dommages physiques, matériels ou un préjudice moral ». En vertu du considérant 146, « [l]e responsable du traitement ou le sous-traitant devrait réparer tout dommage qu'une personne peut subir du fait d'un traitement effectué en violation du présent règlement. Le responsable du traitement ou le sous-traitant devrait être exonéré de sa responsabilité s'il prouve que le dommage ne lui est nullement imputable. La notion de dommage devrait être interprétée au sens large, à la lumière de la jurisprudence de la Cour de justice, d'une manière qui tienne pleinement compte des objectifs du présent règlement. Cela est sans préjudice de toute action en dommages-intérêts fondée sur une infraction à d'autres règles du droit de l'Union ou du droit d'un État membre. [...] Les personnes concernées devraient recevoir une réparation complète et effective pour le dommage subi ».

72. La teneur littérale des dispositions du règlement 2016/679 élimine d'emblée l'idée éventuelle de dommage in re ipsa : l'objectif principal de la responsabilité civile instituée par ce règlement est de donner satisfaction à la personne concernée, précisément par le biais d'une réparation « complète et effective » du dommage subi, et donc de rétablir l'équilibre de la situation juridique négativement affectée par la violation du droit [28].

73. Par ailleurs, d'un point de vue systématique également, tout comme en matière de droit de la concurrence et des ententes, le règlement 2016/679 prévoit deux axes de protection : l'un est de nature publique avec la prévision de sanctions en cas de violation des dispositions de ce règlement, l'autre de nature privée, avec précisément la prévision d'une responsabilité civile de nature extracontractuelle, susceptible d'être qualifiée d'aggravée, pour faute présumée, présentant les caractéristiques évoquées ci-dessus, y compris en ce qui concerne la preuve libératoire [29].

74. Dès lors, une interprétation large [30] de la notion de dommage (moral) ne saurait conduire à juger envisageable l'idée que le législateur a renoncé à la nécessité d'un véritable « dommage ».

75. Le problème de fond est de savoir si, une fois que l'existence de la violation et du lien de causalité est établie, un droit à réparation peut exister du fait de simples inquiétudes, d'anxiété et de craintes ressenties par la personne concernée quant à une éventuelle utilisation abusive future de ses données à caractère personnel, lorsque aucune utilisation abusive n'a été constatée et/ou que la personne concernée n'a subi aucun autre préjudice.

76. Selon une jurisprudence constante de la Cour, les notions d'une disposition du droit de l'Union, qui ne renvoie pas expressément au droit des États membres pour déterminer son sens et sa portée, doivent normalement recevoir une interprétation autonome et uniforme dans toute l'Union, qui doit être recherchée en tenant compte des termes de la disposition en cause, du contexte dans lequel elle s'insère, des objectifs poursuivis par l'acte dont elle fait partie et de la genèse de cette disposition [31].

[28] Voir conclusions de l'avocat général Campos Sánchez-Bordona dans l'affaire Österreichische Post (préjudice moral lié au traitement de données à caractère personnel) (C-300/21, EU:C:2022:756, point 29 et note 11). Dans ces conclusions, l'avocat général conclut avec raison son analyse abordant les aspects littéral, historique, contextuel et téléologique, en excluant la nature « punitive » des dommages et intérêts susceptibles d'être alloués aux personnes concernées sur le fondement de l'article 82 du règlement 2016/679 (points 27 à 55), relevant, d'une part, que les États membres « n'ont pas à choisir parmi les mécanismes du chapitre VIII de ce règlement pour garantir la protection des données (et, de fait, ne le peuvent pas). En présence d'une violation qui ne cause pas de dommage, la personne concernée conserve (au moins) le droit d'introduire une réclamation auprès d'une autorité de contrôle » et, d'autre part, que « la perspective d'obtenir réparation en l'absence de tout dommage encouragerait probablement les litiges civils et l'introduction de demandes qui ne seraient peut-être pas toujours justifiées, et pourrait, dans cette mesure, décourager l'activité de traitement de données » (points 54 et 55).

[29] Refuser un droit à réparation pour les émotions ou sentiments passagers ou de faible intensité liés à la violation de règles relatives au traitement ne laisse pas la personne concernée complètement démunie [voir, en ce sens, conclusions de l'avocat général Campos Sánchez-Bordona dans l'affaire Österreichische Post (préjudice moral lié au traitement de données à caractère personnel) (C-300/21, EU:C:2022:756, point 115)].

[30] Ou « au sens large » selon les termes du considérant 146 du règlement 2016/679.

[31] Voir arrêts du 15 avril 2021, The North of England P & I Association (C-786/19, EU:C:2021:276, point 48), et du 10 juin 2021, KRONE – Verlag (C-65/20, EU:C:2021:471, point 25).

77. Il est de fait que, comme l'a rappelé l'avocat général Campos Sánchez-Bordona [32], la Cour n'a pas élaboré de définition générale de la notion de « dommage » applicable indistinctement dans n'importe quel domaine [33]. Pour ce qui nous intéresse ici (les dommages moraux), il peut être déduit de sa jurisprudence que : lorsque l'un des objectifs de la disposition à interpréter est la protection de l'individu ou d'une certaine catégorie particulière d'individus [34], la notion de dommage doit être large ; conformément à ce critère, la réparation s'étend aux dommages moraux, même s'ils ne sont pas mentionnés dans la disposition interprétée [35].

78. Si la jurisprudence de la Cour autorise à soutenir que, dans les conditions précédemment décrites, il existe en droit de l'Union un principe de réparation du préjudice moral, je ne crois pas, en accord avec l'avocat général Campos Sánchez-Bordona, que l'on puisse en déduire, en revanche, une règle selon laquelle *tout* préjudice moral, quelle que soit sa gravité, est indemnisable [36].

79. Dans ce contexte, la distinction entre un préjudice moral indemnisable et d'autres *inconvénients résultant du non-respect de la légalité* qui, en raison de leur faible importance, n'ouvriraient pas nécessairement droit à réparation, est pertinente [37].

80. La Cour n'ignore pas cette distinction qu'elle admet lorsqu'elle se réfère aux difficultés et aux désagréments en tant que catégorie autonome par rapport à celle des dommages, dans des domaines où elle estime que ceux-ci doivent être réparés [38].

[32] Voir conclusions de l'avocat général Campos Sánchez-Bordona, dans l'affaire Österreichische Post (préjudice moral lié au traitement de données à caractère personnel) (C-300/21, EU:C:2022:756, point 104).

[33] Et n'a pas non plus indiqué une méthode d'interprétation – autonome ou par renvoi aux droits des États membres – qui serait préférable : cela dépend de la matière objet de l'examen. Voir arrêts du 10 mai 2001, Veedfald (C-203/99, EU:C:2001:258, point 27), en matière de produits défectueux, du 6 mai 2010, Walz (C-63/09, EU:C:2010:251, point 21), en matière de responsabilité des transports aériens, et du 10 juin 2021, Van Ameyde España (C-923/19, EU:C:2021:475, points 37 et suiv.), concernant la responsabilité civile pour les accidents résultant de la circulation automobile

[34] Par exemple, les consommateurs de produits ou les victimes d'accidents de la route.

[35] En matière de voyages « tout compris », voir arrêt du 12 mars 2002, Leitner (C-168/00, EU:C:2002:163) ; dans le cadre de la responsabilité civile résultant de la circulation automobile, voir arrêts du 24 octobre 2013, Haasová (C-22/12, EU:C:2013:692, points 47 à 50) ; du 24 octobre 2013, Drozdovs (C-277/12, EU:C:2013:685, point 40), et du 23 janvier 2014, Petillo (C-371/12, EU:C:2014:26, point 35).

[36] Voir conclusions de l'avocat général Campos Sánchez-Bordona, dans l'affaire Österreichische Post (préjudice moral lié au traitement de données à caractère personnel) (C-300/21, EU:C:2022:756, point 105). La Cour a, par exemple, reconnu la compatibilité avec les règles européennes d'une réglementation nationale qui, pour le calcul de l'indemnisation, distingue les dommages immatériels liés à des lésions corporelles causées par un accident en fonction de l'origine de ce dernier ; voir arrêt du 23 janvier 2014, Petillo (C-371/12, EU:C:2014:26, dispositif) : le droit de l'Union ne fait pas obstacle « à une législation nationale telle que celle en cause au principal, qui prévoit un régime particulier d'indemnisation des préjudices immatériels résultant de lésions corporelles de faible gravité causées par les accidents de la circulation routière limitant l'indemnisation de ces préjudices par rapport à ce qui est admis en matière d'indemnisation de préjudices identiques résultant de causes autres que ces accidents ».

[37] Cette dichotomie est présente dans certains ordres juridiques nationaux, en tant que corollaire inévitable de la vie en société. Récemment, en matière de protection des données, en Italie, Tribunale di Palermo, sez. I civile, jugement du 5 octobre 2017, n° 5261, ainsi que Cass. Civ. Ord. Sez VI, n° 17383/2020. En Allemagne, notamment, AG Diez, 7 novembre 2018 – 8 C 130/18 ; LG Karlsruhe, 2 août 2019 – 8 O 26/19, et AG Frankfurt am Main, 10 juillet 2020 – 385 C 155/19 (70). En Autriche, OHG 6 Ob 56:21k.

[38] Voir arrêt du 23 octobre 2012, Nelson e.a (C-581/10 et C-629/10, EU:C:2012:657, point 51), sur la distinction entre « dommages », au sens de l'article 19 de la convention pour l'unification de certaines règles relatives au transport aérien international, conclue à Montréal le 28 mai 1999, et les « désagréments », au sens du règlement (CE) n° 261/2004 du Parlement européen et du Conseil, du 11 février 2004, établissant des règles communes en matière d'indemnisation et d'assistance des passagers en cas de refus d'embarquement et d'annulation ou de retard important d'un vol, et abrogeant le règlement (CEE) n° 295/91 (JO 2004, L 46, p. 1), qui sont indemnisables en vertu de l'article 7 de ce dernier, conformément à l'arrêt du 19 novembre 2009, Sturgeon e.a (C-402/07 et C-432/07, EU:C:2009:716). Dans ce secteur, tout comme dans celui du transport des passagers par mer et par voie de navigation intérieure, auquel se réfère le règlement (UE) n° 1177/2010 du Parlement européen et du Conseil, du 24 novembre 2010, concernant les droits des passagers voyageant par mer ou par voie de navigation intérieure et modifiant le règlement (CE) n° 2006/2004 (JO 2010, L 334, p. 1), le législateur a pu admettre une catégorie abstraite, dans la mesure où l'élément qui entraîne l'inconvénient et l'essence de celui-ci sont identiques pour tous les intéressés. Je ne crois pas qu'il soit possible d'inférer la même chose en matière de protection des données.

81. De façon empirique, l'on peut observer que toute violation d'une règle relative à la protection des données à caractère personnel suscitera une réaction négative de la personne concernée. Une réparation fondée sur un simple désagrément ressenti face au non-respect de la loi par autrui pourrait aisément être confondue avec une réparation sans dommage, ce qui, comme nous l'avons vu, ne semble pas envisageable dans la situation prévue par l'article 82 du règlement 2016/679.

82. Le fait que, dans des circonstances telles que celles de l'affaire au principal, l'utilisation abusive des données à caractère personnel soit seulement potentielle, et non effective, est suffisant pour que la personne concernée puisse être considérée comme ayant subi un préjudice moral causé par la violation du règlement 2016/679, à la condition qu'elle établisse que la crainte d'une telle utilisation abusive lui a concrètement et spécifiquement causé un préjudice émotionnel réel et certain [39].

83. La frontière entre un simple mécontentement (non indemnisable) et de véritables dommages moraux (indemnisables) est ténue, mais les juridictions nationales, auxquelles il appartient de tracer au cas par cas cette ligne de partage, devraient procéder à une appréciation attentive de tous les éléments produits par la personne concernée demandant réparation, à qui il incombera de fournir de façon précise, et non générique, des éléments concrets susceptibles de conduire à la reconnaissance d'un « préjudice moral effectivement subi » du fait de la violation de données à caractère personnel, sans toutefois que ce préjudice atteigne un seuil de gravité particulière prédéterminé : ce qui importe, c'est qu'il ne s'agisse pas d'une simple perception subjective, fluctuante et dépendant également d'éléments liés au tempérament et à la personne, mais d'un trouble de nature objective, même de faible intensité, pourvu qu'il soit démontrable, causé à son intimité physique ou psychique ou sa vie relationnelle ; la nature des données à caractère personnel concernées et l'importance qu'elles revêtent pour la vie de la personne concernée et peut-être aussi la perception qu'a la société, à ce moment-là, de ce trouble particulier lié à la violation des données [40].

IV. Conclusion

84. Eu égard à l'ensemble des considérations qui précèdent, je propose à la Cour de répondre aux questions préjudicielles posées par le Varhoven administrativen sad (Cour administrative suprême, Bulgarie) en ces termes :

Les articles 5, 24, 32 et 82 du règlement (UE) 2016/679 du Parlement européen et du Conseil, du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), doivent être interprétés en ce sens que :

la simple existence d'une « violation de données à caractère personnel », telle que définie à l'article 4, paragraphe 12, de ce règlement, ne suffit pas en soi pour conclure que les mesures techniques et organisationnelles mises en œuvre par le responsable du traitement n'étaient pas « appropriées » aux fins d'assurer la protection des données en question ;

[39] Selon l'Irlande, ces considérations sont particulièrement importantes en pratique, dans le contexte de la cybercriminalité, parce que, si toute personne affectée – même de façon minime – par une violation avait droit à une réparation pour un dommage moral, cela aurait des conséquences graves, en particulier, pour les responsables du traitement des données agissant dans l'intérêt public, qui sont financés par des fonds publics limités, qui devraient plutôt servir les intérêts de la collectivité, y compris le renforcement de la sécurité des données à caractère personnel (observations écrites, point 72).

[40] Voir conclusions de l'avocat général Campos Sánchez-Bordona dans l'affaire Österreichische Post (préjudice moral lié au traitement de données à caractère personnel) (C-300/21, EU:C:2022:756, point 116).

lorsqu'elle vérifie le caractère approprié des mesures techniques et organisationnelles mises en œuvre par le responsable du traitement des données à caractère personnel, la juridiction nationale saisie doit procéder à un contrôle s'étendant à une analyse concrète tant du contenu de ces mesures que de la manière dont elles ont été appliquées et de leurs effets pratiques ;

dans le cadre d'une action en réparation fondée sur l'article 82 dudit règlement, c'est au responsable du traitement des données à caractère personnel qu'il incombe de démontrer le caractère approprié des mesures qu'il a mises en œuvre en vertu de l'article 32 de ce même règlement ;

conformément au principe d'autonomie procédurale, il appartient à l'ordre juridique interne de chaque État membre de déterminer quels sont les moyens de preuve recevables ainsi que leur force probante, y compris les mesures d'instruction que les tribunaux nationaux peuvent ou doivent ordonner afin d'apprécier si un responsable du traitement des données à caractère personnel a mis en œuvre des mesures appropriées au titre du règlement 2016/679, dans le respect des principes d'équivalence et d'efficacité définis par le droit de l'Union ;

le fait que la violation de ce règlement ayant causé le dommage en question a été commise par un tiers ne constitue pas en soi une cause d'exonération pour le responsable du traitement et, pour pouvoir se prévaloir de l'exonération de responsabilité prévue par cette disposition, le responsable du traitement doit démontrer que la violation ne lui est nullement imputable ;

le préjudice consistant dans la crainte d'une future utilisation abusive potentielle de ses données à caractère personnel, dont la personne concernée a démontré l'existence, peut constituer un préjudice moral ouvrant droit à réparation, à condition que la personne concernée démontre avoir subi individuellement un préjudice émotionnel réel et certain, circonstance qu'il appartient à la juridiction nationale saisie de vérifier dans chaque cas d'espèce.