ARRÊT DE LA COUR (troisième chambre)
14 décembre 2023 (*)

« Renvoi préjudiciel – Protection des personnes physiques à l'égard du traitement des données à caractère personnel – Règlement (UE) 2016/679 – Article 5 – Principes relatifs à ce traitement – Article 24 – Responsabilité du responsable du traitement – Article 32 – Mesures mises en œuvre pour garantir la sécurité du traitement – Appréciation du caractère approprié de telles mesures – Portée du contrôle juridictionnel – Administration des preuves – Article 82 – Droit à réparation et responsabilité – Exonération éventuelle de responsabilité du responsable du traitement en cas de violation commise par des tiers – Demande de réparation d'un préjudice moral fondée sur la crainte d'un potentiel usage abusif de données à caractère personnel »

Dans l'affaire C-340/21,

ayant pour objet une demande de décision préjudicielle au titre de l'article 267 TFUE, introduite par le Varhoven administrativen sad (Cour administrative suprême, Bulgarie), par décision du 14 mai 2021, parvenue à la Cour le 2 juin 2021, dans la procédure

VB

contre

Natsionalna agentsia za prihodite,

LA COUR (troisième chambre),

composée de M^me^ K. Jürimäe, présidente de chambre, MM. N. Piçarra, M. Safjan, N. Jääskinen (rapporteur) et M. Gavalec, juges,

avocat général : M. G. Pitruzzella,

greffier : M. A. Calot Escobar,

vu la procédure écrite,

considérant les observations présentées :

pour la Natsionalna agentsia za prihodite, par M. R. Spetsov,

pour le gouvernement bulgare, par M^mes^ M. Georgieva et L. Zaharieva, en qualité d'agents,

pour le gouvernement tchèque, par MM. O. Serdula, M. Smolek et J. Vláčil, en qualité d'agents,

pour l'Irlande, par M^me^ M. Browne, Chief State Solicitor, M. A. Joyce, M^me^ J. Quaney et M. M. Tierney, en qualité d'agents, assistés de M. D. Fennelly, BL,

pour le gouvernement italien, par M^me^ G. Palmieri, en qualité d'agent, assistée de M. E. De Bonis, avvocato dello Stato,

pour le gouvernement portugais, par M^mes^ P. Barros da Costa, A. Pimenta, M. J. Ramos et C. Vieira Guerra, en qualité d'agents,

pour la Commission européenne, par MM. A. Bouchagiar, H. Kranenborg et M^me^ N. Nikolova, en qualité d'agents,

ayant entendu l'avocat général en ses conclusions à l'audience du 27 avril 2023,

rend le présent

Arrêt

La demande de décision préjudicielle porte sur l'interprétation de l'article 5, paragraphe 2, des articles 24 et 32 ainsi que de l'article 82, paragraphes 1 à 3, 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) (JO 2016, L 119, p. 1, ci-après le « RGPD »).

Cette demande a été présentée dans le cadre d'un litige opposant VB, une personne physique, à la Natsionalna agentsia za prihodite (Agence nationale des recettes publiques, Bulgarie) (ci-après la « NAP ») au sujet de la réparation du préjudice moral que ladite personne affirme avoir subi en raison d'un prétendu manquement de cette autorité publique aux obligations légales lui incombant en sa qualité de responsable du traitement de données à caractère personnel.

Le cadre juridique

Les considérants 4, 10, 11, 74, 76, 83, 85 et 146 du RGPD sont libellés comme suit :

[...] Le présent règlement respecte tous les droits fondamentaux et observe les libertés et les principes reconnus par la [charte des droits fondamentaux de l'Union européenne], consacrés par les traités, en particulier le respect de la

vie privée et familiale, du domicile et des communications, la protection des données à caractère personnel, [...] le droit à un recours effectif et à accéder à un tribunal impartial [...]

Afin d'assurer un niveau cohérent et élevé de protection des personnes physiques et de lever les obstacles aux flux de données à caractère personnel au sein de l'Union [européenne], le niveau de protection des droits et des libertés des personnes physiques à l'égard du traitement de ces données devrait être équivalent dans tous les États membres. Il convient dès lors d'assurer une application cohérente et homogène des règles de protection des libertés et droits fondamentaux des personnes physiques à l'égard du traitement des données à caractère personnel dans l'ensemble de l'Union. [...]

Une protection effective des données à caractère personnel dans l'ensemble de l'Union exige de renforcer et de préciser les droits des personnes concernées et les obligations de ceux qui effectuent et déterminent le traitement des données à caractère personnel, [...]

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.

Il convient de déterminer la probabilité et la gravité du risque pour les droits et libertés de la personne concernée en fonction de la nature, de la portée, du contexte et des finalités du traitement. Le risque devrait faire l'objet d'une évaluation objective permettant de déterminer si les opérations de traitement des données comportent un risque ou un risque élevé.

Afin de garantir la sécurité et de prévenir tout traitement effectué en violation du présent règlement, il importe que le responsable du traitement ou le sous-traitant évalue les risques inhérents au traitement et mette en œuvre des mesures pour les atténuer, telles que le chiffrement. Ces mesures devraient assurer un niveau de sécurité approprié, y compris la confidentialité, compte tenu de l'état des connaissances et des coûts de mise en œuvre par rapport aux risques et à la nature des données à caractère personnel à protéger. Dans le cadre de l'évaluation des risques pour la sécurité des données, il convient de prendre en compte les risques que présente le traitement de données à caractère personnel, tels que la destruction, la perte ou 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, de manière accidentelle ou illicite, qui sont susceptibles d'entraîner des dommages physiques, matériels ou un préjudice moral.

Une 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 tels qu'une perte de contrôle sur leurs données à caractère personnel ou la limitation de leurs droits, une discrimination, un vol ou une usurpation d'identité, une perte financière, un renversement non autorisé de la procédure de pseudonymisation, une atteinte à la réputation, une perte de confidentialité de données à caractère personnel protégées par le secret professionnel ou tout autre dommage économique ou social important. En conséquence, dès que le responsable du traitement apprend qu'une violation de données à caractère personnel s'est produite, il convient qu'il le notifie à l'autorité de contrôle dans les meilleurs délais [...]

Le 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. Un traitement effectué en violation du présent règlement comprend aussi un traitement effectué en violation des actes délégués et d'exécution adoptés conformément au présent règlement et au droit d'un État membre précisant les règles du présent règlement. Les personnes concernées devraient recevoir une réparation complète et effective pour le dommage subi. [...] »

L'article 4 de ce règlement, intitulé « Définitions », dispose :

« Aux fins du présent règlement, on entend par :

"données à caractère personnel", toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée "personne concernée") ; [...]

"traitement", toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel [...]

[...]

"responsable du traitement", la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement ; [...]

"tiers", une personne physique ou morale, une autorité publique, un service ou un organisme autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, placées sous l'autorité directe du responsable du traitement ou du sous-traitant, sont autorisées à traiter les données à caractère personnel ;

"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 ;

L'article 5 dudit règlement, intitulé « Principes relatifs au traitement des données à caractère personnel », prévoit :
« 1. Les données à caractère personnel doivent être :
traitées de manière licite, loyale et transparente au regard de la personne concernée (licéité, loyauté, transparence) ;

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). »
Aux termes de l'article 24 du même règlement, intitulé « Responsabilité du responsable du traitement » :
« 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. »
L'article 32 du RGPD, intitulé « Sécurité du traitement », dispose :
« 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 :
la pseudonymisation et le chiffrement des données à caractère personnel ;
des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;
des moyens permettant 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 ;
une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.
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.
[...] »
L'article 79 de ce règlement, intitulé « Droit à un recours juridictionnel effectif contre un responsable du traitement ou un sous-traitant », énonce, à son paragraphe 1 :
« Sans préjudice de tout recours administratif ou extrajudiciaire qui lui est ouvert, y compris le droit d'introduire une réclamation auprès d'une autorité de contrôle au titre de l'article 77, chaque personne concernée a droit à un recours juridictionnel effectif si elle considère que les droits que lui confère le présent règlement ont été violés du fait d'un traitement de ses données à caractère personnel effectué en violation du présent règlement. »
L'article 82 dudit règlement, intitulé « Droit à réparation et responsabilité », prévoit, à ses paragraphes 1 à 3 :
« 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. »

Le litige au principal et les questions préjudicielles

La NAP est une autorité rattachée au ministre des Finances bulgare. Dans le cadre de ses missions, consistant, entre autres, en l'identification, la sécurisation et le recouvrement des créances publiques, elle est responsable du traitement de données à caractère personnel, au sens de l'article 4, point 7, du RGPD.

Le 15 juillet 2019, les médias ont révélé qu'un accès non autorisé au système informatique de la NAP avait eu lieu et que, à la suite de cette cyberattaque, des données à caractère personnel contenues dans ledit système avaient été publiées sur Internet.

Plus de six millions de personnes physiques, de nationalité bulgare ou étrangère, ont été concernées par ces évènements. Quelques centaines d'entre elles, dont la requérante au principal, ont introduit, contre la NAP, des actions en réparation de préjudices moraux qui auraient découlé de la divulgation de leurs données à caractère personnel.

C'est dans ce contexte que la requérante au principal a saisi l'Administrativen sad Sofia-grad (tribunal administratif de la ville de Sofia, Bulgarie) d'un recours visant à obtenir que la NAP lui verse la somme de 1 000 leva bulgares (BGN) (environ 510 euros) à titre de dommages-intérêts, sur le fondement de l'article 82 du RGPD et de dispositions du droit bulgare. À l'appui de cette demande, elle a soutenu avoir subi un préjudice moral résultant d'une violation de données à caractère personnel, au sens de l'article 4, point 12, du RGPD, plus particulièrement une violation de la sécurité qui aurait été causée par un manquement de la NAP aux obligations lui incombant en vertu, notamment, de l'article 5, paragraphe 1, sous f), ainsi que des articles 24 et 32 de ce règlement. Son préjudice moral consisterait en la crainte que ses données à caractère personnel ayant été publiées sans son consentement fassent l'objet d'une utilisation abusive, dans le futur, ou qu'elle-même subisse un chantage, une agression, voire un enlèvement.

En défense, la NAP, tout d'abord, a fait valoir que la requérante au principal ne lui avait pas demandé d'informations concernant les données précises ayant été divulguées. Ensuite, la NAP a produit des documents tendant à prouver qu'elle avait pris toutes les mesures nécessaires, en amont, pour prévenir la violation des données à caractère personnel contenues dans son système informatique ainsi que, en aval, pour limiter les effets de cette violation et pour rassurer les citoyens. En outre, selon la NAP, il n'existait pas de lien de causalité entre le préjudice moral allégué et ladite violation. Enfin, elle a avancé que, ayant elle-même subi une atteinte malveillante de la part de personnes qui n'étaient pas ses employés, elle ne saurait être tenue pour responsable des conséquences dommageables de cette atteinte.

Par décision du 27 novembre 2020, l'Administrativen sad Sofia-grad (tribunal administratif de la ville de Sofia) a rejeté le recours de la requérante au principal. Cette juridiction a considéré, d'une part, que l'accès non autorisé à la base de données de la NAP résultait d'un piratage informatique commis par des tiers et, d'autre part, que la requérante au principal n'avait pas prouvé de carence de la NAP quant à l'adoption de mesures de sécurité. En outre, elle a estimé que cette requérante n'avait pas subi de préjudice moral ouvrant droit à réparation.

La requérante au principal s'est pourvue en cassation contre ladite décision devant le Varhoven administrativen sad (Cour administrative suprême, Bulgarie), qui est la juridiction de renvoi dans la présente affaire. À l'appui de son pourvoi, elle soutient que la juridiction de première instance a commis une erreur de droit dans la répartition de la charge de la preuve relative aux mesures de sécurité prises par la NAP et que cette dernière n'a pas démontré son absence de carence à cet égard. En outre, la requérante au principal prétend que la crainte de possibles utilisations abusives de ses données à caractère personnel dans le futur constitue un préjudice moral réel, et non hypothétique. En défense, la NAP conteste chacun de ces arguments.

La juridiction de renvoi envisage, tout d'abord, la possibilité que le constat de la survenance d'une violation de données à caractère personnel permette, à lui seul, de conclure que les mesures mises en œuvre par le responsable du traitement de ces données n'étaient pas « appropriées », au sens des articles 24 et 32 du RGPD.

Cependant, dans l'hypothèse où ce constat serait insuffisant pour parvenir à une telle conclusion, elle s'interroge, d'une part, sur la portée du contrôle que les juges nationaux doivent opérer pour évaluer le caractère approprié des mesures concernées et, d'autre part, sur les règles relatives à l'administration des preuves qui doivent s'appliquer dans ce cadre, à la fois quant à la charge de la preuve et quant aux moyens de preuve, en particulier lorsque ces juges sont saisis d'une action en réparation fondée sur l'article 82 de ce règlement.

Ensuite, cette juridiction souhaite savoir si, au regard de l'article 82, paragraphe 3, dudit règlement, le fait que la violation de données à caractère personnel résulte d'un acte commis par des tiers, en l'occurrence d'une cyberattaque, constitue un facteur exonérant systématiquement le responsable du traitement de ces données de sa responsabilité pour le préjudice causé à la personne concernée.

Enfin, ladite juridiction se demande si la crainte ressentie par une personne que ses données à caractère personnel puissent faire l'objet d'un usage abusif dans le futur, en l'occurrence à la suite d'un accès non autorisé à celles-ci et de leur divulgation par des cybercriminels, est susceptible, à elle seule, de constituer un « dommage moral », au sens de l'article 82, paragraphe 1, du RGPD. Dans l'affirmative, cette personne serait dispensée d'établir que des tiers ont fait, antérieurement à sa demande de réparation, un usage illicite de ces données, tel qu'une usurpation de son identité.

Dans ces conditions, le Varhoven administrativen sad (Cour administrative suprême) a décidé de surseoir à statuer et de poser à la Cour les questions préjudicielles suivantes :

Les dispositions des articles 24 et 32 du [RGPD] 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, du [RGPD], 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 ?

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 [RGPD] sont appropriées ?

En cas de réponse négative à la première question, le principe de responsabilité, au sens de l'article 5, paragraphe 2, [du RGPD,] et l'article 24 [de ce règlement], lus en combinaison avec le considérant 74 [de celui-ci], peuvent-ils être interprétés en ce sens que, dans le cadre d'une action au titre de l'article 82, paragraphe 1, [dudit 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 [du même] 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" ?

La disposition de l'article 82, paragraphe 3, du [RGPD] 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, du [RGPD], en l'espèce par le biais d'une "attaque de hackers", 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 ?

Les dispositions de l'article 82, paragraphes 1 et 2, [du RGPD], lues en combinaison avec les considérants 85 et 146 [de ce règlement], 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 à caractère personnel, 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 à caractère personnel, 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 ? »

Sur les questions préjudicielles

Sur la première question

Par sa première question, la juridiction de renvoi s'interroge, en substance, sur le point de savoir si les articles 24 et 32 du RGPD doivent être interprétés en ce sens qu'une divulgation non autorisée de données à caractère personnel ou un accès non autorisé à de telles données par des « tiers », au sens de l'article 4, point 10, de ce règlement, suffisent, à eux seuls, pour considérer que les mesures techniques et organisationnelles mises en œuvre par le responsable du traitement en cause n'étaient pas « appropriées », au sens de ces articles 24 et 32.

À titre liminaire, il y a lieu de rappeler que, selon une jurisprudence constante, les termes d'une disposition du droit de l'Union qui, tels les articles 24 et 32 du RGPD, ne comporte aucun renvoi exprès au droit des États membres pour déterminer son sens et sa portée doivent normalement trouver, dans toute l'Union, une interprétation autonome et uniforme, laquelle doit être recherchée en tenant compte, notamment, du libellé de la disposition concernée, des objectifs poursuivis par cette dernière et du contexte dans lequel elle s'inscrit [voir, en ce sens, arrêts du 18 janvier 1984, Ekro, 327/82, EU:C:1984:11, point 11 ; du 1er octobre 2019, Planet49, C-673/17, EU:C:2019:801, points 47 et 48, ainsi que du 4 mai 2023, Österreichische Post (Préjudice moral lié au traitement de données personnelles), C-300/21, EU:C:2023:370, point 29].

En premier lieu, s'agissant du libellé des dispositions pertinentes, il convient de relever que l'article 24 du RGPD prévoit une obligation générale, pesant sur le responsable du traitement de données à caractère personnel, de mettre en œuvre des mesures techniques et organisationnelles appropriées afin de s'assurer que ledit traitement est effectué en conformité avec ce règlement et de pouvoir le démontrer.

À cette fin, cet article 24 énumère, à son paragraphe 1, un certain nombre de critères à prendre en compte pour évaluer le caractère approprié de telles mesures, à savoir la nature, la portée, le contexte et les finalités du traitement ainsi que les risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques. Cette disposition ajoute que lesdites mesures sont réexaminées et actualisées si nécessaire.

Dans cette perspective, l'article 32 du RGPD précise les obligations du responsable du traitement et d'un éventuel sous-traitant quant à la sécurité de ce traitement. Ainsi, le paragraphe 1 de cet article dispose que ces derniers doivent mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté aux risques mentionnés au point précédent du présent arrêt, en prenant en compte l'état des connaissances, les coûts de mise en œuvre ainsi que la nature, la portée, le contexte et les finalités du traitement concerné.

De même, le paragraphe 2 dudit article énonce que, lors de l'évaluation du niveau de sécurité approprié, il doit être 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 des données à caractère personnel, ou de l'accès non autorisé à de telles données, de manière accidentelle ou illicite.

En outre, tant l'article 24, paragraphe 3, de ce règlement que l'article 32, paragraphe 3, de celui-ci indiquent que le responsable du traitement ou le sous-traitant peut démontrer qu'il a respecté les exigences des paragraphes 1 respectifs de ces articles en s'appuyant sur le fait qu'il applique un code de conduite approuvé ou un mécanisme de certification approuvé, comme prévu aux articles 40 et 42 dudit règlement.

La référence, figurant à l'article 32, paragraphes 1 et 2, du RGPD, à « un niveau de sécurité adapté au risque » et à un « niveau de sécurité approprié » témoigne de ce que ce règlement instaure un régime de gestion des risques et qu'il ne prétend nullement éliminer les risques de violations des données à caractère personnel.

Ainsi, il ressort des libellés des articles 24 et 32 du RGPD que ces dispositions se bornent à imposer au responsable du traitement d'adopter des mesures techniques et organisationnelles destinées à éviter, dans toute la mesure du possible, toute violation de données à caractère personnel. Le caractère approprié de telles mesures doit être évalué de

manière concrète, en examinant si ces mesures ont été mises en œuvre par ce responsable en tenant compte des différents critères visés auxdits articles et des besoins de protection des données spécifiquement inhérents au traitement concerné ainsi qu'aux risques induits par ce dernier.

Partant, les articles 24 et 32 du RGPD ne sauraient être compris en ce sens qu'une divulgation non autorisée de données à caractère personnel ou un accès non autorisé à de telles données par un tiers suffisent pour conclure que les mesures adoptées par le responsable du traitement concerné n'étaient pas appropriées, au sens de ces dispositions, sans même permettre à ce dernier d'apporter la preuve contraire.

Une telle interprétation s'impose d'autant plus que l'article 24 du RGPD prévoit expressément que le responsable du traitement doit être en mesure de démontrer la conformité avec ce règlement des mesures qu'il a mises en œuvre, possibilité dont il serait privé si une présomption irréfragable était admise.

En second lieu, des éléments d'ordre contextuel et téléologique corroborent cette interprétation des articles 24 et 32 du RGPD.

S'agissant, d'une part, du contexte dans lequel s'inscrivent ces deux articles, il y a lieu de relever qu'il ressort de l'article 5, paragraphe 2, du RGPD que le responsable du traitement doit être en mesure de démontrer qu'il a respecté les principes relatifs au traitement des données à caractère personnel énoncés au paragraphe 1 dudit article. Cette obligation est reprise et précisée à l'article 24, paragraphes 1 et 3, ainsi qu'à l'article 32, paragraphe 3, de ce règlement, quant à l'obligation de mettre en œuvre des mesures techniques et organisationnelles pour protéger de telles données lors du traitement effectué par ce responsable. Or, une telle obligation de démontrer le caractère approprié de ces mesures n'aurait pas de sens si le responsable du traitement était obligé d'empêcher toute atteinte auxdites données.

En outre, le considérant 74 du RGPD met en exergue qu'il importe 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 ce règlement, y compris l'efficacité des mesures, lesquelles devraient tenir compte des critères, liés aux caractéristiques du traitement concerné et au risque présenté par celui-ci, qui sont aussi énoncés à ses articles 24 et 32.

De même, selon le considérant 76 de ce règlement, la probabilité et la gravité du risque dépendent des spécificités du traitement en cause et ce risque devrait faire l'objet d'une évaluation objective.

Par ailleurs, il découle de l'article 82, paragraphes 2 et 3, du RGPD que, si un responsable de traitement est responsable du dommage causé par le traitement qui constitue une violation de ce règlement, il est néanmoins exonéré de sa responsabilité s'il prouve que le fait qui a provoqué le dommage ne lui est nullement imputable.

D'autre part, l'interprétation dégagée au point 31 du présent arrêt est aussi accréditée par le considérant 83 du RGPD, qui énonce, à sa première phrase, que, « [a]fin de garantir la sécurité et de prévenir tout traitement effectué en violation du présent règlement, il importe que le responsable du traitement ou le sous-traitant évalue les risques inhérents au traitement et mette en œuvre des mesures pour les atténuer ». Ce faisant, le législateur de l'Union a manifesté son intention d'« atténuer » les risques de violation des données à caractère personnel, sans prétendre qu'il serait possible de les éliminer.

Eu égard aux motifs qui précèdent, il convient de répondre à la première question que les articles 24 et 32 du RGPD doivent être interprétés en ce sens qu'une divulgation non autorisée de données à caractère personnel ou un accès non autorisé à de telles données par des « tiers », au sens de l'article 4, point 10, de ce règlement, ne suffisent pas, à eux seuls, pour considérer que les mesures techniques et organisationnelles mises en œuvre par le responsable du traitement en cause n'étaient pas « appropriées », au sens de ces articles 24 et 32.

Sur la deuxième question

Par sa deuxième question, la juridiction de renvoi demande, en substance, si l'article 32 du RGPD doit être interprété en ce sens que le caractère approprié des mesures techniques et organisationnelles mises en œuvre par le responsable du traitement, au titre de cet article, doit être apprécié par les juridictions nationales de manière concrète, notamment en tenant compte des risques liés au traitement concerné.

À cet égard, il y a lieu de rappeler que, comme cela a été souligné dans le cadre de la réponse à la première question, l'article 32 du RGPD exige que le responsable du traitement et le sous-traitant, selon les cas de figure, mettent en œuvre des mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, compte tenu des critères d'appréciation qui sont énoncés à son paragraphe 1. En outre, le paragraphe 2 de cet article énumère, de manière non exhaustive, un certain nombre de facteurs qui sont pertinents pour évaluer le niveau de sécurité approprié au regard des risques que présente le traitement concerné.

Il ressort dudit article 32, paragraphes 1 et 2, que le caractère approprié de telles mesures techniques et organisationnelles doit s'apprécier en deux temps. D'une part, il convient d'identifier les risques de violation des données à caractère personnel induits par le traitement concerné et leurs éventuelles conséquences pour les droits et libertés des personnes physiques. Cette appréciation doit être conduite de manière concrète, en prenant en considération le degré de probabilité des risques identifiés et leur degré de gravité. D'autre part, il y a lieu de vérifier si les mesures mises en œuvre par le responsable du traitement sont adaptées à ces risques, compte tenu de l'état des connaissances, des coûts de mise en œuvre ainsi que de la nature, de la portée, du contexte et des finalités de ce traitement.

Certes, le responsable du traitement dispose d'une certaine marge d'appréciation pour déterminer les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, comme le requiert l'article 32, paragraphe 1, du RGPD. Il n'en reste pas moins qu'une juridiction nationale doit pouvoir évaluer l'appréciation complexe à laquelle s'est livré le responsable du traitement et, ce faisant, s'assurer que les mesures retenues par ce dernier sont aptes à garantir un tel niveau de sécurité.

Une telle interprétation est d'ailleurs de nature à assurer, d'une part, l'effectivité de la protection des données à caractère personnel que les considérants 11 et 74 de ce règlement mettent en exergue et, d'autre part, le droit à un recours juridictionnel effectif contre un responsable du traitement, tel que protégé par l'article 79, paragraphe 1, dudit règlement, lu en combinaison avec le considérant 4 du même règlement.

Partant, pour contrôler le caractère approprié de mesures techniques et organisationnelles mises en œuvre au titre de l'article 32 du RGPD, une juridiction nationale doit non pas se limiter à constater de quelle façon le responsable du traitement concerné a entendu satisfaire aux obligations lui incombant en vertu de cet article, mais se livrer à un examen de ces mesures sur le fond, au regard de tous les critères mentionnés audit article ainsi que des circonstances propres au cas d'espèce et des éléments de preuve dont cette juridiction dispose à ce sujet.

Un tel examen nécessite de procéder à une analyse concrète à la fois de la nature et de la teneur des mesures qui ont été mises en œuvre par le responsable du traitement, de la manière dont ces mesures ont été appliquées et de leurs effets pratiques sur le niveau de sécurité que celui-ci était tenu de garantir, eu égard aux risques inhérents à ce traitement.

Par conséquent, il convient de répondre à la deuxième question que l'article 32 du RGPD doit être interprété en ce sens que le caractère approprié des mesures techniques et organisationnelles mises en œuvre par le responsable du traitement au titre de cet article doit être apprécié par les juridictions nationales de manière concrète, en tenant compte des risques liés au traitement concerné et en appréciant si la nature, la teneur et la mise en œuvre de ces mesures sont adaptées à ces risques.

Sur la troisième question

Sur la première partie de la troisième question

Par la première partie de sa troisième question, la juridiction de renvoi demande, en substance, si le principe de responsabilité du responsable du traitement, énoncé à l'article 5, paragraphe 2, du RGPD et concrétisé à l'article 24 de celui-ci, doit être interprété en ce sens que, dans le cadre d'une action en réparation fondée sur l'article 82 de ce règlement, le responsable du traitement en cause supporte la charge de prouver le caractère approprié des mesures de sécurité qu'il a mises en œuvre au titre de l'article 32 dudit règlement.

À cet égard, il convient, en premier lieu, de rappeler que l'article 5, paragraphe 2, du RGPD pose un principe de responsabilité, en vertu duquel le responsable du traitement est responsable du respect des principes relatifs au traitement des données à caractère personnel énoncés au paragraphe 1 de cet article, et prévoit que ledit responsable doit être en mesure de démontrer que ces principes sont respectés.

En particulier, le responsable du traitement doit, conformément au principe d'intégrité et de confidentialité des données à caractère personnel qui est énoncé à l'article 5, paragraphe 1, sous f), de ce règlement, veiller à ce que de telles données soient traitées de façon à garantir une sécurité appropriée de celles-ci, 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, et doit être en mesure de démontrer que ce principe est respecté.

Il y a également lieu de relever que tant l'article 24, paragraphe 1**,** du RGPD, lu à la lumière du considérant 74 de celui-ci, que l'article 32, paragraphe 1, de ce règlement imposent au responsable du traitement, à l'égard de tout traitement de données à caractère personnel réalisé par lui-même ou pour son compte, de mettre en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué en conformité avec ledit règlement.

Il ressort sans ambiguïté des libellés de l'article 5, paragraphe 2, de l'article 24, paragraphe 1, et de l'article 32, paragraphe 1, du RGPD que la charge de prouver que les données à caractère personnel sont traitées de façon à garantir une sécurité appropriée de ces dernières, au sens de l'article 5, paragraphe 1, sous f), et de l'article 32 de ce règlement, incombe au responsable du traitement concerné [voir, par analogie, arrêts du 4 mai 2023, Bundesrepublik Deutschland (Boîte électronique judiciaire), C-60/22, EU:C:2023:373, points 52 et 53, ainsi que du 4 juillet 2023, Meta Platforms e.a. (Conditions générales d'utilisation d'un réseau social), C-252/21, EU:C:2023:537, point 95].

Ces trois articles énoncent ainsi une règle, d'application générale, qu'il convient, à défaut d'indication contraire dans le RGPD, d'appliquer également dans le cadre d'une action en réparation fondée sur l'article 82 de ce règlement.

En second lieu, il y a lieu de constater que l'interprétation littérale qui précède est confortée par la prise en compte des objectifs poursuivis par le RGPD.

D'une part, dès lors que le niveau de la protection visée par le RGPD est tributaire des mesures de sécurité adoptées par les responsables du traitement de données à caractère personnel, ceux-ci doivent être incités, moyennant le fait qu'ils supportent la charge de démontrer le caractère approprié de ces mesures, à tout mettre en œuvre pour prévenir la survenance d'opérations de traitement non conformes à ce règlement.

D'autre part, s'il devait être considéré que la charge de la preuve concernant le caractère approprié desdites mesures pèse sur les personnes concernées, telles que définies à l'article 4, point 1, du RGPD, il en résulterait que le droit à réparation prévu à l'article 82, paragraphe 1, de celui-ci serait privé d'une importante partie de son effet utile, alors même que le législateur de l'Union a entendu renforcer à la fois les droits de ces personnes et les obligations des responsables du traitement, par rapport aux dispositions antérieures à ce règlement, comme l'indique le considérant 11 de celui-ci.

Il convient donc de répondre à la première partie de la troisième question que le principe de responsabilité du responsable du traitement, énoncé à l'article 5, paragraphe 2, du RGPD et concrétisé à l'article 24 de celui-ci, doit être interprété en ce sens que, dans le cadre d'une action en réparation fondée sur l'article 82 de ce règlement, le responsable du traitement en cause supporte la charge de prouver le caractère approprié des mesures de sécurité qu'il a mises en œuvre au titre de l'article 32 dudit règlement.

Sur la seconde partie de la troisième question

Par la seconde partie de sa troisième question, la juridiction de renvoi cherche à savoir, en substance, si l'article 32 du RGPD et le principe d'effectivité du droit de l'Union doivent être interprétés en ce sens que, afin d'apprécier le caractère approprié des mesures de sécurité que le responsable du traitement a mises en œuvre au titre de cet article, une expertise judiciaire constitue un moyen de preuve nécessaire et suffisant.

À cet égard, il importe de rappeler qu'il est de jurisprudence constante que, en l'absence de règles de l'Union en la matière, il appartient à l'ordre juridique interne de chaque État membre de régler les aspects procéduraux des recours en justice destinés à assurer la sauvegarde des droits des justiciables, en vertu du principe de l'autonomie procédurale, à condition, toutefois, que ces modalités ne soient pas, dans les situations relevant du droit de l'Union, moins favorables que celles régissant des situations similaires soumises au droit interne (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) [arrêt du 4 mai 2023, Österreichische Post (Préjudice moral lié au traitement de données personnelles), C-300/21, EU:C:2023:370, point 53 et jurisprudence citée].

En l'occurrence, il y a lieu de relever que le RGPD n'énonce pas de règles relatives à l'admission et à la valeur probante d'un moyen de preuve, tel qu'une expertise judiciaire, qui doivent être appliquées par les juges nationaux saisis d'une action en réparation fondée sur l'article 82 de ce règlement et chargés d'apprécier, au regard de l'article 32 de celui-ci, le caractère approprié des mesures de sécurité que le responsable du traitement concerné a mises en œuvre. Partant, conformément à ce qui a été rappelé au point précédent du présent arrêt et à défaut de règles du droit de l'Union en la matière, il appartient à l'ordre juridique interne de chaque État membre de fixer les modalités des actions destinées à assurer la sauvegarde des droits que les justiciables tirent de cet article 82 et, en particulier, les règles afférentes aux moyens de preuve permettant d'évaluer le caractère approprié de telles mesures dans ce contexte, sous réserve du respect desdits principes d'équivalence et d'effectivité [voir, par analogie, arrêts du 21 juin 2022, Ligue des droits humains, C-817/19, EU:C:2022:491, point 297, ainsi que du 4 mai 2023, Österreichische Post (Préjudice moral lié au traitement de données personnelles), C-300/21, EU:C:2023:370, point 54].

Dans la présente procédure, la Cour ne dispose d'aucun élément de nature à susciter un doute sur le respect du principe d'équivalence. Il en va différemment s'agissant de la conformité au principe d'effectivité, dans la mesure où le libellé même de la seconde partie de la troisième question présente le recours à une expertise judiciaire comme un « moyen de preuve nécessaire et suffisant ».

En particulier, une règle de procédure nationale en vertu de laquelle il serait systématiquement « nécessaire » que les juridictions nationales ordonnent une expertise judiciaire serait susceptible de heurter le principe d'effectivité. En effet, le recours systématique à une telle expertise peut s'avérer superflu au vu des autres preuves détenues par la juridiction saisie, notamment, comme le gouvernement bulgare l'a indiqué dans ses observations écrites, au vu des résultats d'un contrôle du respect des mesures de protection des données à caractère personnel ayant été effectué par une autorité indépendante et établie par la loi, pour autant que ce contrôle soit récent, puisque lesdites mesures doivent, conformément à l'article 24, paragraphe 1, du RGPD, être réexaminées et actualisées si nécessaire.

En outre, ainsi que la Commission européenne l'a relevé dans ses observations écrites, le principe d'effectivité pourrait être enfreint dans l'hypothèse où le terme « suffisant » devrait être compris comme signifiant qu'une juridiction nationale doit déduire exclusivement ou automatiquement d'un rapport d'expertise judiciaire que les mesures de sécurité mises en œuvre par le responsable du traitement en cause sont « appropriées », au sens de l'article 32 du RGPD. Or, la sauvegarde des droits conférés par ce règlement, à laquelle tend ledit principe d'effectivité, et spécialement le droit à un recours juridictionnel effectif contre le responsable du traitement, qui est garanti par l'article 79, paragraphe 1, de celui-ci, requièrent qu'un tribunal impartial procède à une appréciation objective du caractère approprié des mesures concernées, au lieu de se limiter à une telle déduction (voir, en ce sens, arrêt du 12 janvier 2023, Nemzeti Adatvédelmi és Információszabadság Hatóság, C-132/21, EU:C:2023:2, point 50).

Eu égard aux motifs qui précèdent, il convient de répondre à la seconde partie de la troisième question que l'article 32 du RGPD et le principe d'effectivité du droit de l'Union doivent être interprétés en ce sens que, afin d'apprécier le caractère approprié des mesures de sécurité que le responsable du traitement a mises en œuvre au titre de cet article, une expertise judiciaire ne saurait constituer un moyen de preuve systématiquement nécessaire et suffisant.

Sur la quatrième question

Par sa quatrième question, la juridiction de renvoi demande, en substance, si l'article 82, paragraphe 3, du RGPD doit être interprété en ce sens que le responsable du traitement est exonéré de son obligation de réparer le dommage subi par une personne, au titre de l'article 82, paragraphes 1 et 2, de ce règlement, du seul fait que ce dommage résulte d'une divulgation non autorisée de données à caractère personnel ou d'un accès non autorisé à de telles données par des « tiers », au sens de l'article 4, point 10, dudit règlement.

À titre liminaire, il convient de préciser qu'il découle de l'article 4, point 10, du RGPD qu'ont la qualité de « tiers », notamment, les personnes autres que celles qui, placées sous l'autorité directe du responsable du traitement ou du sous-traitant, sont autorisées à traiter les données à caractère personnel. Cette définition couvre des personnes qui ne sont pas des employés du responsable du traitement et ne sont pas sous le contrôle de celui-ci, telles que celles visées dans la question posée.

Ensuite, il y a lieu de rappeler, en premier lieu, que l'article 82, paragraphe 2, du RGPD dispose que « tout responsable du traitement ayant participé au traitement est responsable du dommage causé par le traitement qui constitue une violation [de ce] règlement » et que le paragraphe 3 de cet article prévoit qu'un responsable du traitement, ou un sous-traitant selon les cas de figure, est exonéré d'une telle responsabilité « s'il prouve que le fait qui a provoqué le dommage ne lui est nullement imputable ».

En outre, le considérant 146 du RGPD, qui se rapporte spécifiquement à l'article 82 de celui-ci, énonce, à ses première et deuxième phrases, que « [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 [de ce] règlement » et « devrait être exonéré de sa responsabilité s'il prouve que le dommage ne lui est nullement imputable ».

Il résulte de ces dispositions, d'une part, que le responsable du traitement en cause doit en principe réparer un dommage causé par une violation de ce règlement liée à ce traitement et, d'autre part, qu'il ne peut être exonéré de sa responsabilité que s'il apporte la preuve que le fait qui a provoqué ce dommage ne lui est nullement imputable.

Ainsi, comme le révèle l'ajout exprès de l'adverbe « nullement » au cours de la procédure législative, les circonstances dans lesquelles le responsable du traitement peut prétendre à être exonéré de la responsabilité civile qu'il encourt au titre de l'article 82 du RGPD doivent être strictement limitées à celles où ce responsable est en mesure de démontrer une absence d'imputabilité du dommage dans son propre chef.

Lorsque, comme en l'occurrence, une violation de données à caractère personnel, au sens de l'article 4, point 12, du RGPD, a été commise par des cybercriminels, et donc par des « tiers », au sens de l'article 4, point 10, de ce règlement, cette violation ne saurait être imputée au responsable du traitement, sauf si celui-ci a rendu possible ladite violation en méconnaissant une obligation prévue par le RGPD, et notamment l'obligation de protection des données à laquelle il est tenu en vertu de l'article 5, paragraphe 1, sous f), et des articles 24 et 32 du même règlement.

Ainsi, en cas de violation de données à caractère personnel commise par un tiers, le responsable du traitement peut s'exonérer de sa responsabilité, sur le fondement de l'article 82, paragraphe 3, du RGPD, en prouvant qu'il n'y a aucun lien de causalité entre son éventuelle violation de l'obligation de protection des données et le dommage subi par la personne physique.

En second lieu, l'interprétation qui précède de cet article 82, paragraphe 3, est également conforme à l'objectif du RGPD consistant à assurer un niveau élevé de protection des personnes physiques à l'égard du traitement de leurs données à caractère personnel, énoncé aux considérants 10 et 11 de ce règlement.

Eu égard à l'ensemble de ces considérations, il y a lieu de répondre à la quatrième question que l'article 82, paragraphe 3, du RGPD doit être interprété en ce sens que le responsable du traitement ne saurait être exonéré de son obligation de réparer le dommage subi par une personne, au titre de l'article 82, paragraphes 1 et 2, de ce règlement, du seul fait que ce dommage résulte d'une divulgation non autorisée de données à caractère personnel ou d'un accès non autorisé à de telles données par des « tiers », au sens de l'article 4, point 10, dudit règlement, ledit responsable devant alors prouver que le fait qui a provoqué le dommage concerné ne lui est nullement imputable.

Sur la cinquième question

Par sa cinquième question, la juridiction de renvoi demande, en substance, si l'article 82, paragraphe 1, du RGPD doit être interprété en ce sens que la crainte d'un potentiel usage abusif de ses données à caractère personnel par des tiers qu'une personne concernée éprouve à la suite d'une violation de ce règlement est susceptible, à elle seule, de constituer un « dommage moral », au sens de cette disposition.

S'agissant, en premier lieu, du libellé de l'article 82, paragraphe 1, du RGPD, il y a lieu d'observer que celui-ci prévoit que « [t]oute 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 ».

À cet égard, la Cour a relevé qu'il ressort clairement du libellé de l'article 82, paragraphe 1, du RGPD que l'existence d'un « dommage » ou d'un « préjudice » ayant été « subi » constitue l'une des conditions du droit à réparation prévu à ladite disposition, tout comme l'existence d'une violation de ce règlement et d'un lien de causalité entre ce dommage et cette violation, ces trois conditions étant cumulatives [arrêt du 4 mai 2023, Österreichische Post (Préjudice moral lié au traitement de données personnelles), C-300/21, EU:C:2023:370, point 32].

Par ailleurs, en se fondant sur des considérations d'ordre à la fois littéral, systémique et téléologique, la Cour a interprété l'article 82, paragraphe 1, du RGPD en ce sens qu'il s'oppose à une règle ou une pratique nationale subordonnant la réparation d'un « dommage moral », au sens de cette disposition, à la condition que le préjudice subi par la personne concernée ait atteint un certain degré de gravité [arrêt du 4 mai 2023, Österreichische Post (Préjudice moral lié au traitement de données personnelles), C-300/21, EU:C:2023:370, point 51].

Cela étant rappelé, il importe de souligner, en l'occurrence, que l'article 82, paragraphe 1, du RGPD n'opère pas de distinction entre des cas de figure où, à la suite d'une violation avérée de dispositions de ce règlement, le « dommage moral » allégué par la personne concernée, d'une part, est relié à un usage abusif par des tiers de ses données à caractère personnel qui s'est déjà produit, à la date de sa demande de réparation, ou bien, d'autre part, est rattaché à la peur ressentie par cette personne qu'un tel usage puisse se produire, à l'avenir.

Dès lors, le libellé de l'article 82, paragraphe 1, du RGPD n'exclut pas que la notion de « dommage moral » figurant à cette disposition englobe une situation, telle que celle visée par la juridiction de renvoi, où la personne concernée invoque, en vue d'obtenir une réparation sur le fondement de cette disposition, sa crainte que ses données à caractère personnel fassent l'objet d'un futur usage abusif par des tiers, du fait de la violation de ce règlement qui est advenue.

Cette interprétation littérale est corroborée, en deuxième lieu, par le considérant 146 du RGPD, qui porte spécifiquement sur le droit à réparation prévu à l'article 82, paragraphe 1, de ce dernier et qui mentionne, à sa troisième phrase, que « 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 » de ce règlement. Or, une interprétation de la notion de « dommage moral », au sens de cet article 82, paragraphe 1, qui n'inclurait pas les situations où la personne concernée par une violation dudit règlement se prévaut de la crainte qu'elle éprouve que ses propres données à caractère personnel fassent l'objet d'un usage abusif dans le futur ne répondrait pas à une conception large de cette notion, telle que voulue par le législateur de l'Union [voir, par analogie, arrêt du 4 mai 2023,

Österreichische Post (Préjudice moral lié au traitement de données personnelles), C-300/21, EU:C:2023:370, points 37 et 46].

Par ailleurs, le considérant 85, première phrase, du RGPD indique qu'« une 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 tels qu'une perte de contrôle sur leurs données à caractère personnel ou la limitation de leurs droits, une discrimination, un vol ou une usurpation d'identité, une perte financière, [...] ou tout autre dommage économique ou social important ». Il ressort de cette liste exemplative des « dommages » ou des « préjudices » susceptibles d'être subis par les personnes concernées que le législateur de l'Union a entendu inclure dans ces notions, en particulier, la simple « perte de contrôle » sur leurs propres données, à la suite d'une violation de ce règlement, quand bien même un usage abusif des données en cause ne se serait pas produit concrètement au détriment desdites personnes.

En troisième et dernier lieu, l'interprétation figurant au point 80 du présent arrêt est confortée par les objectifs du RGPD, dont il convient de tenir pleinement compte pour définir la notion de « dommage », comme l'indique le considérant 146, troisième phrase, de ce règlement. Or, une interprétation de l'article 82, paragraphe 1, du RGPD selon laquelle la notion de « dommage moral », au sens de cette disposition, n'inclurait pas les situations où une personne concernée se prévaut uniquement de sa crainte que ses données fassent l'objet d'un usage abusif par des tiers, à l'avenir, ne serait pas conforme à la garantie d'un niveau élevé de protection des personnes physiques à l'égard du traitement des données à caractère personnel au sein de l'Union, qui est visée par cet instrument.

Cependant, il importe de souligner qu'une personne concernée par une violation du RGPD ayant eu des conséquences négatives à son encontre est tenue de démontrer que ces conséquences sont constitutives d'un dommage moral, au sens de l'article 82 de ce règlement [voir, en ce sens, arrêt du 4 mai 2023, Österreichische Post (Préjudice moral lié au traitement de données personnelles), C-300/21, EU:C:2023:370, point 50].

En particulier, lorsqu'une personne demandant réparation sur ce fondement invoque la crainte qu'une utilisation abusive de ses données à caractère personnel survienne dans le futur en raison de l'existence d'une telle violation, la juridiction nationale saisie doit vérifier que cette crainte peut être considérée comme étant fondée, dans les circonstances spécifiques en cause et au regard de la personne concernée.

Eu égard aux motifs qui précèdent, il convient de répondre à la cinquième question que l'article 82, paragraphe 1, du RGPD doit être interprété en ce sens que la crainte d'un potentiel usage abusif de ses données à caractère personnel par des tiers qu'une personne concernée éprouve à la suite d'une violation de ce règlement est susceptible, à elle seule, de constituer un « dommage moral », au sens de cette disposition.

Sur les dépens

La procédure revêtant, à l'égard des parties au principal, le caractère d'un incident soulevé devant la juridiction de renvoi, il appartient à celle-ci de statuer sur les dépens. Les frais exposés pour soumettre des observations à la Cour, autres que ceux desdites parties, ne peuvent faire l'objet d'un remboursement.

Par ces motifs, la Cour (troisième chambre) dit pour droit :

Les articles 24 et 32 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 :

une divulgation non autorisée de données à caractère personnel ou un accès non autorisé à de telles données par des « tiers », au sens de l'article 4, point 10, de ce règlement, ne suffisent pas, à eux seuls, pour considérer que les mesures techniques et organisationnelles mises en œuvre par le responsable du traitement en cause n'étaient pas « appropriées », au sens de ces articles 24 et 32.

L'article 32 du règlement 2016/679

doit être interprété en ce sens que :

le caractère approprié des mesures techniques et organisationnelles mises en œuvre par le responsable du traitement au titre de cet article doit être apprécié par les juridictions nationales de manière concrète, en tenant compte des risques liés au traitement concerné et en appréciant si la nature, la teneur et la mise en œuvre de ces mesures sont adaptées à ces risques.

Le principe de responsabilité du responsable du traitement, énoncé à l'article 5, paragraphe 2, du règlement 2016/679 et concrétisé à l'article 24 de celui-ci,

doit être interprété en ce sens que :

dans le cadre d'une action en réparation fondée sur l'article 82 de ce règlement, le responsable du traitement en cause supporte la charge de prouver le caractère approprié des mesures de sécurité qu'il a mises en œuvre au titre de l'article 32 dudit règlement.

L'article 32 du règlement 2016/679 et le principe d'effectivité du droit de l'Union

doivent être interprétés en ce sens que :

afin d'apprécier le caractère approprié des mesures de sécurité que le responsable du traitement a mises en œuvre au titre de cet article, une expertise judiciaire ne saurait constituer un moyen de preuve systématiquement nécessaire et suffisant.

L'article 82, paragraphe 3, du règlement 2016/679

doit être interprété en ce sens que :

le responsable du traitement ne saurait être exonéré de son obligation de réparer le dommage subi par une personne, au titre de l'article 82, paragraphes 1 et 2, de ce règlement, du seul fait que ce dommage

résulte d'une divulgation non autorisée de données à caractère personnel ou d'un accès non autorisé à de telles données par des « tiers », au sens de l'article 4, point 10, dudit règlement, ledit responsable devant alors prouver que le fait qui a provoqué le dommage concerné ne lui est nullement imputable.

L'article 82, paragraphe 1, du règlement 2016/679

doit être interprété en ce sens que :

la crainte d'un potentiel usage abusif de ses données à caractère personnel par des tiers qu'une personne concernée éprouve à la suite d'une violation de ce règlement est susceptible, à elle seule, de constituer un « dommage moral », au sens de cette disposition.

Signatures

---

* Langue de procédure : le bulgare.