

Affaire C-683/21

Demande de décision préjudicielle

Date de dépôt :

12 novembre 2021

Jurisdiction de renvoi :

Vilniaus apygardos administracinis teismas (Lituanie)

Date de la décision de renvoi :

22 octobre 2021

Partie demanderesse :

Nacionalinis visuomenės sveikatos centras prie Sveikatos apsaugos ministerijos

Partie défenderesse :

Valstybinė duomenų apsaugos inspekcija

VILNIAUS APYGARDOS ADMINISTRACINIS TEISMAS

ORDONNANCE

[OMISSIS]

22 octobre 2021

Vilnius

La chambre du Vilniaus apygardos administracinis teismas (tribunal administratif régional de Vilnius, Lituanie) [OMISSIS] [formation de jugement et dispositions procédurales], dans l'affaire administrative engagée par le pourvoi formé par la partie requérante, le Centre national de la santé publique auprès du ministère de la santé (Nacionalinis visuomenės sveikatos centras prie Sveikatos apsaugos ministerijos, ci-après le « requérant » ou le « CNSP ») en vue de l'annulation d'une décision de la partie défenderesse, l'Inspection nationale de la protection des données (Valstybinė duomenų apsaugos inspekcija, ci-après l'« Inspection »), des tiers intéressés, la société par actions (UAB) IT sprendimai sėkmei (ci-après la « société ITSS ») et le ministère de la santé lituanien (Lietuvos Respublikos

sveikatos apsaugos ministerija, ci-après le « ministère de la santé ») participant à la procédure,

Constate :

L'affaire concerne un litige entre la partie requérante, le CNSP, et l'Inspection relatif à la décision de l'Inspection du 24 février 2021 [OMISSIS], par laquelle une amende a été infligée au requérant, le CNSP, au titre de violations des dispositions des articles 5, 13, 24, 32, 35 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, ci-après le [OMISSIS] « RGPD »). Cette décision a également imposé une amende à la société ITSS en sa qualité de responsable conjoint du traitement des données.

Le litige entre les parties relève du cadre réglementaire direct du RGPD.

[OMISSIS] [Fondement juridique du renvoi]

La juridiction de céans se voit dans la nécessité de saisir la Cour de justice parce que le contenu des règles du droit positif de l'Union applicables au présent litige n'est pas totalement clair. Les actes du droit de l'Union doivent être interprétés de manière autonome et uniforme dans toute l'Union, [OMISSIS]. [OMISSIS] Les réponses de la Cour aux questions énoncées dans le dispositif de la présente ordonnance revêtent par conséquent une importance essentielle pour la présente affaire, car [OMISSIS] le contenu de la notion de responsable du traitement, la reconnaissance d'une personne comme responsable du traitement et (ou) responsable conjoint du traitement des données personnelles collectées dans l'application mobile « Karantinas » (« Quarantaine », ci-après « Karantinas ») et, par conséquent, l'établissement de l'entité responsable au titre des infractions prévues par le RGPD dépendent de l'interprétation du droit de l'Union.

Fondement juridique.

Droit de l'Union

Le quatrième considérant du préambule du RGPD prévoit que le droit à la protection des données à caractère personnel n'est pas un droit absolu ; il doit être considéré par rapport à sa fonction dans la société et être mis en balance avec d'autres droits fondamentaux, conformément au principe de proportionnalité. Le présent règlement respecte tous les droits fondamentaux et observe les libertés et les principes reconnus par la Charte, 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, la liberté de pensée, de conscience et de religion, la liberté d'expression et d'information, la liberté d'entreprise, le droit

à un recours effectif et à accéder à un tribunal impartial, et la diversité culturelle, religieuse et linguistique.

Le dixième considérant du préambule du RGPD précise qu'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, 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.

Le considérant 74 du préambule du RGPD indique qu'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.

L'article 4, point 7, du RGPD dispose qu'on entend par « 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 ; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre.

L'article 4, point 2, du RGPD dispose qu'on entend par « 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, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.

L'article 26, paragraphe 1, du RGPD dispose que lorsque deux responsables du traitement ou plus déterminent conjointement les finalités et les moyens du traitement, ils sont les responsables conjoints du traitement. Les responsables conjoints du traitement définissent de manière transparente leurs obligations respectives aux fins d'assurer le respect des exigences du présent règlement, notamment en ce qui concerne l'exercice des droits de la personne concernée, et leurs obligations respectives quant à la communication des informations visées

aux articles 13 et 14, par voie d'accord entre eux, sauf si, et dans la mesure, où leurs obligations respectives sont définies par le droit de l'Union ou par le droit de l'État membre auquel les responsables du traitement sont soumis. Un point de contact pour les personnes concernées peut être désigné dans l'accord.

L'article 26, paragraphe 2, du RGPD dispose que l'accord visé au paragraphe 1 reflète dûment les rôles respectifs des responsables conjoints du traitement et leurs relations vis-à-vis des personnes concernées. Les grandes lignes de l'accord sont mises à la disposition de la personne concernée.

L'article 83, paragraphe 1, du RGPD dispose que chaque autorité de contrôle veille à ce que les amendes administratives imposées en vertu du présent article pour des violations du présent règlement visées aux paragraphes 4, 5 et 6 soient, dans chaque cas, effectives, proportionnées et dissuasives.

Droit national pertinent

En vertu de [OMISSIS] l'article 72, paragraphe 2, de la loi lituanienne relative aux marchés publics (Viešųjų pirkimų įstatymas, ci-après la « loi sur les marchés publics »), le pouvoir adjudicateur mène des négociations non publiées par les étapes suivantes : 1) il invite par écrit les fournisseurs sélectionnés à présenter leurs offres ; 2) il contrôle l'absence des motifs d'inéligibilité des fournisseurs prévus dans le cahier des charges et que les fournisseurs satisfont aux exigences de qualification imposées et, le cas échéant, aux normes du système de gestion de la qualité exigées, et (ou) du système de gestion de la protection de l'environnement ; 3) il se concerte avec les soumissionnaires selon les modalités prévues à l'article 66 de la présente loi et leur demande de présenter les offres définitives. Le pouvoir adjudicateur n'est pas tenu de demander de présenter l'offre définitive lorsqu'un seul fournisseur participe à des négociations non publiées ; et 4) apprécie les offres définitives et désigne le lauréat.

L'article 29, paragraphe 3, de la loi sur les marchés publics dispose qu'à tout moment avant la conclusion du marché public (ou du contrat préliminaire) ou la détermination du lauréat du concours, le pouvoir adjudicateur a le droit de retirer à son initiative les procédures d'appel d'offres ou de concours engagées, s'il apparaît des circonstances qu'il n'était pas possible de prévoir, et est tenu de procéder ainsi si les principes établis à l'article 17, paragraphe 1, de la présente loi ont été violés et s'il n'est pas possible de remédier à la situation concernée.

[OMISSIS]

L'article 2.133, paragraphe 9, du code civil lituanien prévoit que dans l'hypothèse où un agent a agi en outrepassant ses compétences mais d'une manière qui a donné à un tiers de sérieuses raisons de penser qu'il concluait un contrat avec un agent dûment autorisé, le contrat est obligatoire pour le commettant, sauf lorsque l'autre partie au contrat a été avisée ou devait être avisée qu'un agent avait outrepassé ses compétences.

L'article 2.136, paragraphe 1, du code civil lituanien prévoit qu'un contrat, qui a été conclu par une personne au nom d'une autre personne sans autorisation expresse ou en outrepassant ses compétences, crée, modifie et annule les droits et les obligations d'un commettant seulement dans les cas où, à une date ultérieure, le commettant approuve l'ensemble du contrat ou la partie de ce dernier qui a outrepassé ses compétences [OMISSIS].

[OMISSIS] [disposition de droit national sans importance pour l'affaire]

Circonstances factuelles

L'entreprise privée UAB ITSS a créé l'application mobile « Karantinas ».

Il ressort du dossier de l'affaire que le ministre de la santé lituanien a décidé par décision n° V-519 du 24 mars 2020, en sa qualité de responsable de l'action de l'État dans une situation extrême d'importance nationale [OMISSIS] et dans le but gérer de manière appropriée la situation extrême d'importance nationale liée au risque de propagation de la COVID-19 (infection au coronavirus), de confier au directeur du CNSP la mission d'organiser immédiatement l'acquisition d'une plate-forme informatique (un système) de gestion des situations extrêmes (destinée à enregistrer des données des personnes déclarés porteuses de la COVID-19 [OMISSIS] et à constater leur exposition, qui seront utilisées à des fins de suivi épidémiologique de la COVID-19 [OMISSIS] pour que le virus ne se répande pas dans le pays).

La société ITSS s'est vue adresser le 27 mars 2020 par une personne physique se présentant comme un représentant du CNSP – A. S. – un courriel présentant les caractéristiques des courriels officiellement utilisés par le CNSP (@CNSP.lt ; A. S. n'ayant pas conclu un contrat de travail ou d'une autre nature avec le CNSP), par lequel la société ITSS a été informée que le CNSP l'avait sélectionnée pour créer une application. A. S. a ensuite envoyé à plusieurs reprises des courriels à l'entreprise, en se présentant comme représentant du CNSP, relatifs à divers aspects de la création de l'application mobile. Une copie du courriel a été portée à la connaissance du directeur du CNSP.

Au cours des négociations et de la coopération entre la société et le CNSP, certains employés du CNSP ont de même adressé des courriels à la société au sujet de l'ajustement du libellé des questions posées dans l'application.

La politique de protection de la vie privée de l'application a été élaborée à l'étape de la création de l'application, lors de laquelle la société ITSS et le CNSP ont été désignés comme responsables du traitement.

Le directeur de CNSP a envoyé le 3 avril 2020 un courriel, dans lequel il a indiqué qu'il existe des irrégularités dans l'application, justifiant de modifier les libellés.

Il était possible de télécharger l'application à partir de la boutique en ligne « Google Playstore » à partir du 4 avril 2020, et de la boutique en ligne « Apple

App store » – à partir du 6 avril 2020. L'application mentionne la société ITSS et le CNSP.

L'application « Karantinas » collecte les informations suivantes : le numéro d'identité, les coordonnées (latitude et longitude), le pays, la ville, la commune, le code postal, le nom de rue, le numéro de l'immeuble, le nom, le prénom, le code personnel, le numéro de téléphone, l'adresse, une deuxième adresse, si le lieu déclaré est en Lituanie, si la personne doit s'isoler, si elle s'est enregistrée, s'il apparaît qu'une photo est nécessaire, l'identifiant universel unique, l'identifiant d'utilisateur, quand le consentement a été donné, quand il a été créé, quand il a été modifié, quand la personne s'est enregistrée, quand une photo a été demandée, jusqu'à quand une photo est nécessaire et quand la personne s'est enregistrée la dernière fois. La collecte des données de l'application a été opérée non seulement sur le territoire de la Lituanie, mais aussi en Europe (notamment en Estonie et en Suisse) et au-delà (notamment en Inde et aux États-Unis).

Le ministre de la santé lituanien [OMISSIS] a décidé par décision n°V-821 du 10 avril 2020 [OMISSIS] de confier [OMISSIS] au directeur [du CNSP] la mission d'organiser rapidement l'acquisition de l'application mobile « Karantinas ».

Il a été envisagé d'acquérir l'application auprès du fournisseur, la société ITSS, par un des moyens prévus par la loi sur les marchés publics, celui des négociations sans publication.

Le 15 mai 2020, le CNSP a informé l'entreprise de l'exigence de ne pas utiliser des indications du CNSP ou d'autres liens avec le CNSP dans l'application « Karantinas ».

L'enquête relative au traitement des données à caractère personnel a débuté à l'Inspection à partir du 18 mai 2020, sur décision du directeur de l'Inspection.

En vue d'apporter des explications, le CNSP a indiqué par sa lettre n° (06 1.12E) 2-28797) du 4 juin 2020 [OMISSIS] adressée à la société ITSS (et en copie à l'Inspection) que la procédure d'appel d'offres avait été engagée par décision du directeur du CNSP [OMISSIS], mais comme le financement nécessaire à l'acquisition de l'objet de l'appel d'offres n'avait pas été reçu, celle-ci a été annulée. La poursuite de la procédure d'appel d'offres sans posséder des possibilités financières à cette fin est objectivement impossible et il n'est pas pertinent de conclure une transaction en sachant d'avance que celle-ci ne pourra pas être exécutée et devra être annulée. Ces circonstances importantes n'ayant pas été connues du pouvoir adjudicateur et n'ayant pas pu être raisonnablement prévues, le CNSP a clôturé la procédure d'appel d'offres conformément à l'article 29, paragraphe 3, de la loi sur les marchés publics après les avoir découvertes.

La société ITSS a communiqué à l'Inspection la lettre du 3 juin 2020, dans laquelle elle a indiqué qu'avant la suspension provisoire du fonctionnement de

l'application en vertu de l'instruction de l'Inspection du 26 mai 2020, 3802 utilisateurs avaient fourni leurs données à caractère personnel dans l'application.

Les spécialistes de l'inspection ont établi dans leurs conclusions n° 4R-333(2.14.E) du 3 novembre 2020 que les données à caractère personnel ont été recueillies à l'aide de l'application Karantinas. Il a été également demandé aux utilisateurs ayant choisi l'application comme méthode de suivi de l'isolement obligatoire de répondre tous les jours aux questions mentionnées ci-après, impliquant le traitement des données à caractère personnel fournies dans les réponses : « Avez-vous pris votre température aujourd'hui ? Si oui, quelle est-elle ? Si non, veuillez la mesurer maintenant et l'inscrire. Ressentez-vous au moins un des symptômes suivants : toux, difficultés respiratoires ? Ressentez-vous d'autres symptômes ? Si oui, lesquels (les inscrire) ? Respectez-vous les exigences d'auto-isolement (il est possible de joindre une mention des règles d'isolement) ? Avez-vous besoin d'une aide sociale ? Si oui, laquelle (l'inscrire) ? Avez-vous besoin d'une aide psychologique ? »

De même, les spécialistes de l'Inspection ont établi que UAB Juvare Lithuania, qui est la gérante du système informatique de suivi et de contrôle des maladies transmissibles présentant un risque de propagation, (ci-après le « système ULSKIS ») en vertu du programme prévu par le CNSP, devait recevoir les copies des données recueillies par l'application Karantinas. Dans la lettre adressée à l'Inspection par la société Juvare Lithuania, les données [OMISSIS] ont été fournies pour la période du 7 mai 2020 au 10 mai 2020, 51 enregistrements de données ont été fournis à l'Inspection, des informations étant recueillies dans chaque enregistrement : la date d'introduction, le numéro de téléphone, le code personnel, quand cet enregistrement a été modifié et quand il a été créé, si la personne a des difficultés à respirer, si elle respecte les exigences d'auto-isolement, si elle tousse, quels symptômes spécifiques elle ressent, si elle a de la température, si elle a besoin d'une aide psychologique ou d'une assistance sociale. Les données sont fausses (destinées aux essais de l'application Karantinas), mis à part les numéros de téléphone des employés de Juvare, qui ont été également utilisés à des fins d'essais de l'application Karantinas. Le CNSP a été désigné ultérieurement responsable du système ULSKIS.

Lors d'une audience, les représentants de CNSP ont expliqué qu'il était envisagé, après son acquisition, de l'intégrer l'application concernée (la relier) au système ULSKIS dirigé par le CNSP.

Sur le fond du litige

Le litige porte en substance sur l'interprétation de la notion de personne responsable du traitement prévue par le RGPD : sur le point de savoir si cette notion doit être interprétée largement, c'est-à-dire en ce sens qu'une personne doit être considérée comme responsable du traitement des données personnelles pour avoir seulement établi les objectifs du traitement des données et les mesures de

traitement des données, si cette notion doit être interprétée de manière plus étroite, après avoir apprécié la procédure d'organisation des marchés publics et son résultat. Il est établi en l'espèce que la société ITSS a créé l'application mobile Karantinas, et que le CNSP, en tant que pouvoir adjudicateur, a aidé par des conseils sur le contenu des questions posées (les informations collectées), mais le CNSP n'a pas conclu le contrat public, l'acte de transmission et de réception relatif à la transmission du produit informatique créé n'a pas été signé, les droits de propriété sur l'application mobile Karantinas n'a pas été transféré et il n'existe pas de données selon lesquelles un consentement ou une autorisation officiels de diffuser l'application mobile par diverses boutiques en ligne (Google Play Store, App Store) aurait été donné.

[OMISSIS]

La réglementation des marchés publics et le fait qu'une entité d'administration publique, à laquelle s'applique aussi un des principes essentiels de l'administration publique en vertu du droit de l'Union, le principe de légalité, a engagé sa responsabilité au titre d'infractions au RGPD, sont de même pertinents dans la présente affaire. L'institution des marchés publics relève tant du droit national que du droit de l'Union, mais le droit de l'Union ne réglemente pas tous les aspects des marchés publics, certains d'entre eux relevant toujours du droit national. Selon le droit national, une procédure de passation de marché public est considérée close après la conclusion d'un contrat public. Les modalités et conditions des négociations non publiées sont réglementées aux articles 71 et 72 de la loi sur les marchés publics. Cet acte de droit national met en œuvre, notamment, aussi la directive 2014/24/UE du Parlement européen et du Conseil, du 26 février 2014, sur la passation des marchés publics et abrogeant la directive 2004/18/CE, dans laquelle l'utilisation des négociations sans publication préalable sur le marché est également prévue comme procédure de marché public (article 32). En vertu de [OMISSIS] l'article 72, paragraphe 2, de la loi sur les marchés publics, le pouvoir adjudicateur mène des négociations non publiées par les étapes suivantes : 1) il invite par écrit les fournisseurs sélectionnés à présenter leurs offres ; 2) il contrôle l'absence des motifs d'inéligibilité des fournisseurs prévus dans le cahier des charges et que les fournisseurs satisfont aux exigences de qualification imposées et, le cas échéant, aux normes du système de gestion de la qualité exigées, et (ou) du système de gestion de la protection de l'environnement ; 3) il se concerte avec les soumissionnaires selon les modalités prévues à l'article 66 de la présente loi et leur demande de présenter les offres définitives. Le pouvoir adjudicateur n'est pas tenu de demander de présenter l'offre définitive lorsqu'un seul fournisseur participe à des négociations non publiées ; et 4) il apprécie les offres définitives et désigne le lauréat. Il ressort de la réglementation nationale, telle que prévue par les dispositions susmentionnées de la loi sur les marchés publics, que le législateur a clairement défini les modes d'exécution d'un appel d'offres réalisé au moyen de négociations non publiées, le moment du début de cet appel d'offres et le moment où les négociations sont considérées comme ayant eu lieu. Toute procédure de marché public ne prend pas fin par la conclusion d'un contrat public et l'acquisition des services ou des

produits concernés. L'article 29, paragraphe 3, de la loi sur les marchés publics prévoit qu'à tout moment avant la conclusion du marché (du contrat préliminaire) ou la désignation du lauréat du concours, le pouvoir adjudicateur a le droit de retirer à son initiative une procédure d'appel d'offres ou de concours commencée, s'il apparaît des circonstances qu'il n'était pas possible de prévoir, et doit procéder ainsi si les principes établis à l'article 17, paragraphe 1, de cette loi ont été violés et qu'il n'est pas possible de rétablir la situation concernée. Dans la présente affaire, la position du CNSP s'appuie en fait aussi sur des arguments selon lesquels la procédure de marché public n'étant pas clôturée par la conclusion du contrat public, l'exploitation de l'application mobile n'a pas été transférée et le CNSP ne saurait être considéré comme responsable des données personnelles collectées avec cette application.

La Cour a précisé la notion de responsable du traitement en rappelant que compte tenu de l'objectif de la directive 95/46 (à partir du 25 mai 2018, la directive 95/46 a été abrogée et remplacée par le RGPD), qui vise à garantir un niveau élevé de protection des libertés et des droits fondamentaux des personnes physiques, notamment de leur vie privée, à l'égard du traitement des données à caractère personnel, l'article 2, sous d), de cette directive définit de manière large la notion de « responsable du traitement » comme visant la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel (voir, sur cette question, arrêt du 5 juin 2018, *Wirtschaftsakademie Schleswing-Holstein*, C-210/16, EU:C:2018:388, points 26 et 27). L'objectif de l'article 2, sous d), de la directive 95/46 étant d'assurer, par une définition large de la notion de « responsable », une protection efficace et complète des personnes concernées, l'existence d'une responsabilité conjointe ne se traduit pas nécessairement par une responsabilité équivalente, pour un même traitement de données à caractère personnel, des différents acteurs. Au contraire, ces acteurs peuvent être impliqués à différents stades de ce traitement et selon différents degrés, de telle sorte que le niveau de responsabilité de chacun d'entre eux doit être évalué en tenant compte de toutes les circonstances pertinentes du cas d'espèce (sur cette question, voir arrêt du 10 juillet 2018, *Jehovan todistajat*, C-25/17, EU:C:2018:551, point 66).

L'Inspection a indiqué que la notion de responsable du traitement est une notion pratique, dont l'objet est d'imputer la responsabilité à la personne ayant une réelle influence, sur le fondement d'une analyse des faits concrets, et qu'une personne devient responsable du traitement en ayant décidé de traiter dans une situation spécifique les données à caractère personnel en poursuivant ses objectifs. L'inspection souligne que le responsable fixe, et non valide, l'objectif et les modes de traitement des données. L'Inspection souligne les précisions apportées par l'avis n° 1/2010 du groupe de travail « article 29 » sur les notions de « responsable du traitement » et de « sous-traitant », ainsi que l'explication fournie par les lignes directrices 07/2020, du 2 septembre 2020, adoptées par le Comité européen de la protection des données (CEPD) sur les notions de responsable du traitement et de sous-traitant dans la version 1.0 du RGPD,

desquelles il ressort que les responsables conjoints doivent se compléter mutuellement par leurs décisions et que les décisions de chacun d'entre eux doivent en fait avoir un effet tangible sur la détermination des objectifs du traitement des données et des mesures de traitement des données. En outre, en cas de responsables conjoints des données, les objectifs que ceux-ci poursuivent doivent être étroitement liés ou se compléter mutuellement.

La société ITSS a indiqué qu'elle surveillait en tant que sous-traitante le fonctionnement de l'application sur le plan technique (de la programmation), mais dans l'application, les données à caractère personnel ont été traitées exclusivement en fonction des objectifs fixés par le CNSP et selon les indications du CNSP.

Il ressort de la correspondance entre la société et le CNSP que la création de l'application visait la mise en œuvre de l'objectif assigné par le CNSP (en vue de la gestion de la pandémie par la création d'une décision en matière informatique) et il était prévu à cette fin de traiter les données à caractère personnel. Il existe également des données dans l'affaire selon lesquelles les décisions techniques ont été modifiées en fonction des besoins du pouvoir adjudicateur (du client) (notamment les questions posées et leur formulation). Il n'est pas prévu que la société poursuive d'autres objectifs que celui de percevoir une rémunération au titre du produit informatique créé.

La juridiction nationale se pose la question de l'interprétation de la notion de « responsable du traitement » prévue à l'article 4, point 7, du RGPD : la notion de « responsable du traitement » peut-elle être interprétée en ce sens que l'on doit aussi considérer comme responsable du traitement une personne qui prévoit d'acquérir au moyen d'un marché public un outil de collecte des données (une application mobile), car celle-ci présente dans le cahier des charges la description du produit qu'elle a prévu d'acquérir, notamment les paramètres techniques et l'objectif ? La circonstance que le contrat de marché public n'avait pas été conclu et que le produit créé (l'application mobile), pour l'acquisition duquel la procédure de marché public a été utilisée, n'a pas été transféré n'est-elle pas en ce cas déterminante pour interpréter la notion de responsable du traitement ? La juridiction demande donc qu'il lui soit précisé si la notion de « responsable du traitement » prévue à l'article 4, point 7, du RGPD peut être interprétée en ce sens que dans la situation factuelle examinée, une personne qui a prévu d'acquérir au moyen d'un marché public un outil de collecte des données (une application mobile), alors que le créateur du produit informatique (l'entreprise) a opéré un traitement de données à caractère personnel à l'aide de l'application créée avant la clôture de l'appel d'offres doit aussi être considérée comme responsable du traitement ? Un traitement des données inapproprié de la part du sous-traitant engage-t-il toujours la responsabilité du responsable du traitement, ou est-ce que la notion de « responsable du traitement » ne devrait pas être interprétée en ce sens qu'il est nécessaire d'établir au moins des actions minimales d'autorisation ou de consentement de la part de la personne désignée responsable du traitement pour le traitement réel des données ?

Le « traitement des données à caractère personnel » est défini suffisamment largement, comme signifiant en substance toute opération ou groupe d'opérations, réalisé par des moyens automatiques ou non automatiques avec des données à caractère personnel. Il ressort de cette définition que le traitement des données à caractère personnel peut se composer d'une ou plusieurs actions, dont chacune peut être liée à différentes étapes du traitement des données à caractère personnel. Sur cet aspect, l'article 4, point 2, du RGPD peut-il être interprété en ce sens que lors du processus d'acquisition de l'application mobile, l'utilisation de copies des données personnelles destinées aux essais des systèmes informatiques (vraies et fausses) doit être considérée comme un traitement de données à caractère personnel ?

Du fait que le CNSP est reconnu comme étant conjointement responsable du traitement des données à caractère personnel, les questions de l'interprétation de l'article 4, point 7, et de l'article 26, paragraphe 1, du RGPD, liées à la responsabilité conjointe des données sont également soulevées en l'espèce. Il est demandé à la Cour de préciser si la responsabilité conjointe des données doit être interprétée comme une harmonisation volontaire des actions relatives à la fixation de l'objet du traitement des données et des mesures de traitement des données, ou si celle-ci peut être interprétée en ce sens que la responsabilité conjointe est possible en l'absence d'accord sur l'objet du traitement des données à caractère personnel et des mesures du traitement de ces données et d'une coordination des actions entre les entités. L'établissement d'un « accord » entre personnes, la clarté et la certitude de son contenu, sont-ils en ce cas importants pour interpréter la responsabilité conjointe des données ? Une circonstance relative à l'identification d'une étape de la création d'une mesure de traitement des données à caractère personnel (d'une application informatique), lors de laquelle les données à caractère personnel ont été traitées, ainsi qu'à l'objectif de la création de l'application (exclusivement destinée aux besoins du pouvoir adjudicateur de maîtriser la pandémie) est-elle juridiquement importante pour l'interprétation de la notion de responsabilité conjointe des données ?

Pour se prononcer sur la responsabilité de plusieurs entités selon le RGPD, la juridiction de renvoi se pose aussi la question de savoir si, en vertu de l'article 83, paragraphe 1, du RGPD, la disposition selon laquelle « les amendes administratives [sont] effectives, proportionnées et dissuasives » comprend aussi les cas d'engagement de la responsabilité du « responsable du traitement » dans lesquels le créateur réalise des actions de traitement des données à caractère personnel lors de la procédure de création du produit informatique. Les actions inappropriées de traitement des données à caractère personnel réalisées par le sous-traitant engagent-elles toujours aussi automatiquement la responsabilité juridique du responsable du traitement ? L'application d'une responsabilité en vertu du RGPD comprend-elle aussi les cas de responsabilité sans faute ou l'établissement d'une faute minimale au moins (par exemple, de négligence) est-il nécessaire ?

[OMISSIS] [questions de droit procédural national]

La chambre, sur le fondement de ce qui précède et de l'article 267, paragraphe 2, TFUE [OMISSIS], [mentions de disposition du droit national]

Décide :

La Cour de justice de l'Union européenne est saisie d'une demande de décision préjudicielle sur les questions suivantes [OMISSIS] :

1. Convient-il d'interpréter la notion de « responsable du traitement » prévue à l'article 4, point 7, du RGPD en ce sens qu'une personne qui prévoit d'acquérir au moyen d'un marché public un outil de collecte des données (une application mobile) doit être également considérée comme responsable du traitement, en dépit du fait que le contrat de marché public n'a pas été conclu et que le produit créé (l'application mobile), pour l'acquisition duquel la procédure de marché public a été utilisée, n'a pas été transféré ?

2. Convient-il d'interpréter la notion de « responsable du traitement » prévue à l'article 4, point 7, du RGPD en ce sens qu'un pouvoir adjudicateur, qui n'a pas acquis de droit de propriété sur le produit informatique créé et n'a pas repris sa gestion, doit également être considéré comme étant responsable du traitement lorsque des mentions de cette entité publique ou de liens vers celle-ci sont opérées dans la dernière version de l'application créée et (ou) lorsque cette entité publique est indiquée comme étant le responsable du traitement dans la politique de protection de la vie privée de l'application, qui n'a pas été officiellement confirmée ou reconnue par l'entité publique concernée ?

3. La notion de « responsable du traitement » prévue à l'article 4, point 7, du RGPD doit-elle être interprétée en ce sens qu'une personne, qui n'a pas réalisé des actions réelles de traitement des données, définies à l'article 4, point 2, du RGPD, et (ou) n'a pas donné une autorisation ou un consentement clairs à leur réalisation doit être également considérée responsable du traitement ? Est-ce que la circonstance que le produit informatique à l'aide duquel des données à caractère personnel ont été traitées a été créé selon une instruction formulée par le pouvoir adjudicateur serait importante pour l'interprétation de la notion de responsable du traitement ?

4. Si la détermination des actions réelles du traitement des données est importante pour l'interprétation de la notion de responsable du traitement, l'article 4, point 2, du RGPD (« traitement des données à caractère personnel ») doit-il être interprété comme couvrant aussi les situations dans lesquelles les copies de données à caractère personnel sont utilisées pour les essais des systèmes informatiques lors de la procédure d'acquisition de l'application mobile ?

5. La responsabilité conjointe des données en vertu de l'article 4, point 7, et de l'article 26, paragraphe 1, du RGPD peut-elle être exclusivement interprétée comme impliquant une harmonisation volontaire des actions relatives à la fixation de l'objet du traitement des données et des mesures de traitement des données, ou peut-elle être interprétée également en ce sens que la responsabilité conjointe

comprend aussi les situations dans lesquelles il n'existe pas d'« accord » clair relatif à l'objet du traitement des données à caractère personnel et des mesures de traitement de ces données et (ou) les actions ne sont pas coordonnées entre les entités ? Une circonstance relative à une étape de la création d'une mesure de traitement des données à caractère personnel (d'une application informatique), lors de laquelle les données à caractère personnel ont été traitées, ainsi qu'à l'objectif de la création de l'application est-elle juridiquement importante pour l'interprétation de la notion de responsabilité conjointe des données ? Un « accord » entre les responsables conjoints peut-il être interprété comme impliquant nécessairement la fixation claire et définie de conditions relatives à la responsabilité conjointe du traitement des données ?

6. Les dispositions de l'article 83, paragraphe 1, du RGPD, prévoyant que « les amendes administratives [sont] effectives, proportionnées et dissuasives » doivent-elles être interprétées en ce sens que celles-ci comprennent également les cas d'engagement de la responsabilité du « responsable du traitement », lorsque le créateur réalise des actions de traitement des données à caractère personnel lors du processus de création du produit informatique, et les actions de traitement des données à caractère personnel inappropriées réalisées par le sous-traitant engagent-elles toujours automatiquement la responsabilité juridique du responsable du traitement ? Ces dispositions doivent-elles également être interprétées en ce sens qu'elles comprennent aussi les cas de responsabilité sans faute du responsable du traitement ?

[OMISSIS] [mention des documents joints à l'ordonnance de renvoi]

[OMISSIS] [questions de droit procédural national et noms des juges]