

Affaire C-563/23

Demande de décision préjudicielle

Date de dépôt :

12 septembre 2023

Juridiction de renvoi :

Sofiyski rayonen sad (Bulgarie)

Date de la décision de renvoi :

11 septembre 2023

Requérant dans la procédure principale :

Teritorialna direksia na Natsionalna agentsia za prihodite – Sofia

ORDONNANCE

N° 31722

Sofia, le 11 septembre 2023

Le **SOFIYSKI RAYONEN SAD** (tribunal d'arrondissement de Sofia, Bulgarie),
section civile [OMISSIS] :

[OMISSIS]

Après avoir examiné l'affaire civile privée n° **50078** inscrite au rôle pour **2023**, vu ce qui suit :

- 1 La procédure est celle régie par l'article 267, premier alinéa, TFUE.
- 2 Renvoie aux questions concernant l'étendue du contrôle du juge en tant qu'autorité autorisant la divulgation de données à caractère personnel en présence d'une obligation de vérifier les conditions formelles, qui sont identiques à celles posées dans les affaires C-313/23, C-316/23 et C-332/23.

LES PARTIES AU LITIGE :

3 **Partie requérante :**

4 **Natsionalna agentsia za prihodite** (agence nationale des revenus, ci-après la « NAP ») – organe étatique ayant pour adresse [OMISSIS] BULGARIE, [OMISSIS] Sofia [OMISSIS].

5 Représentée dans la présente affaire par [OMISSIS], directeur territorial de la direction territoriale de Sofia.

6 La personne contrôlée n'est pas partie à la procédure sur laquelle la juridiction statue à huis clos et confidentiellement à son égard.

7 **Conclusions des parties**

8 En vertu de l'article 62, paragraphe 6, de la Zakon za kreditnite institutsii (loi sur les établissements de crédit), la NAP, dans l'exercice de ses pouvoirs de contrôle fiscal et d'obtention d'informations, demande également à la juridiction de lui donner accès aux données bancaires confidentielles du contribuable.

LES FAITS DU LITIGE :

9 Le 15 juillet 2019, des informations sont apparues dans de nombreux médias bulgares selon lesquelles des données personnelles, y compris des informations fiscales et de sécurité sociale de 6 074 140 personnes, dont 4 104 786 ressortissants bulgares et étrangers vivants, et de 1 959 598 personnes décédées, figurant dans la base de données de la NAP avaient été divulguées. Conséquence de cette fuite, la NAP a donné accès à une base de données spéciale des personnes affectées par la fuite de données.

10 Selon une communication de l'autorité bulgare visée à l'article 51, paragraphe 1 du règlement (UE) 2016/679 (« règlement général sur la protection des données », ci-après le « RGPD »), la Komisija za zashtita na lichnite danni (Commission de la protection des données à caractère personnel, ci-après la « KZLD »), publiée le 29 juillet 2019 sur son site internet, disponible à l'adresse : https://www.cdpd.bg/index.php?p=news_view&aid=1519, la NAP a été condamnée à une amende et 20 décisions lui ont été adressées lui imposant, en vertu de l'article 58, paragraphe 2, sous d), lu en combinaison avec l'article 57, paragraphe 1, sous a), RGPD, de prendre dans un délai de 6 mois des mesures techniques et organisationnelles afin d'éviter de futures fuites de données.

11 Dans l'arrêt n° 565/02.02.2023 dans l'affaire administrative n° 10477/2019, l'Administrativen sad (tribunal administratif) de Sofia a confirmé 18 des 20 décisions contraignantes de la KZLD, deux ayant été annulées partiellement. L'arrêt est disponible à l'adresse <https://search-sofia-adms-g.justice.bg/Acts/GetActContent?BlobID=662f36cf-7076-4247-bbd5-9d9f7c0fb7>.

- 12 Le texte de l'arrêt est le suivant : « Selon la première expertise judiciaire technique, la NAP dispose d'un centre de stockage de données qui est utilisé pour stocker les informations provenant des principaux systèmes d'information de la NAP, y compris les données à caractère personnel traitées par l'agence. Ce centre permet de garantir que les systèmes de la NAP soient remis en état de fonctionnement dans les délais prévus dans le plan de continuité des activités de la NAP. En ce qui concerne la mise en place d'un centre de récupération des systèmes en temps réel (DRC) pour soutenir la pleine fonctionnalité des systèmes d'information et des services de la NAP en temps réel, l'agence a pris des mesures organisationnelles, l'une des options étant la mise en place d'un centre de stockage de données commun pour les structures de l'administration publique sous la gestion du Darzhavna agentsia "Elektronno upravlenie" (agence étatique "contrôle électronique").
- 13 Selon la deuxième expertise judiciaire technique, la NAP dispose d'un DRC pour le stockage des données qui est utilisé pour stocker des informations provenant des principaux systèmes d'information de la NAP, y compris des données à caractère personnel traitées à la NAP. Il assure la récupération des systèmes de la NAP dans les délais prévus dans le plan de continuité des activités de la NAP, la synchronisation des données étant effectuée toutes les deux minutes et l'activité étant transférée sur les serveurs de secours en cas de défaillance critique des serveurs primaires. *Selon le recours, la NAP ne conteste pas l'absence de construction d'un centre de récupération des systèmes en temps réel dans le délai de 6 mois prévu à cet effet. Au vu de ces circonstances, l'ordonnance doit être considérée comme légale, étant précisé, en ce qui concerne le délai, qu'au moment où les examens ont été effectués, la NAP s'était déjà conformée à l'injonction de mettre en place un centre de récupération des systèmes en temps réel ».*
- 14 L'arrêt de la juridiction a été attaqué devant le Varhoven Administrativen sad (Cour administrative suprême), où l'affaire administrative n° 3781/2023 a été introduite et programmée pour une audience le 14 décembre 2023 (des données accessibles au public sur l'évolution de l'affaire sont disponibles sur https://info-adc.justice.bg/courts/portal/edis.nsf/e_case.xsp?id=472354&code=vas&guid=1541050632).
- 15 Dans le même temps, selon les données accessibles au public par une recherche dans les moteurs de recherche généraux sur Internet on constate que par l'arrêt n° 837/12.01.2022 dans l'affaire administrative n° 9546/2020, de l'Administrativen sad (tribunal administratif) de Sofia, que la KZLD a publié (à l'adresse https://www.cpdp.bg/userfiles/file/ASSG_2020_2021/Reshenie_ASSG-837_12_02_2021.pdf), devenu définitif en vertu de l'arrêt n° 8431/12.07.2021 dans l'affaire administrative n° 5165/2021 du Varhoven Administrativen sad (Cour administrative suprême) (publié sur Internet à l'adresse : https://info-adc.justice.bg/courts/portal/edis.nsf/e_act.xsp?id=1718161&code=vas&guid=2135386076) il est établi que par une autre décision n° PPN-02-507/2019, du 18 août 2020, la KZLD a adressé d'autres injonctions à la NAP concernant la protection des données à caractère personnel en relation avec la fuite identifiée de ces

données due aux employés de l'administration fiscale elle-même, en recommandant des mesures pour contrôler l'accès électronique.

- 16 La juridiction de céans ne dispose d'aucune information permettant de savoir si les problèmes ayant conduit à la divulgation illégale de données à caractère personnel ont été corrigés ni quelles mesures ont été prises par la NAP pour prévenir des risques futurs. Jusqu'à présent, il n'existe pas non plus de jurisprudence sur la recherche de telles informations.
- 17 En l'espèce, la NAP affirme avoir démarré le 13 juin 2023 un contrôle d'un ressortissant bulgare, personne physique, pour fraude à l'impôt sur le revenu.
- 18 Elle affirme avoir transmis au contribuable personne physique, le 19 juillet 2023, par voie électronique, une demande datée du 15 juin 2023, l'invitant à fournir les données sur les soldes disponibles sur ses comptes bancaires au 1^{er} janvier 2020 et au 31 décembre 2021, ou à soumettre une déclaration de consentement à la levée de son secret bancaire.
- 19 La NAP a établi que le contribuable possédait sept comptes bancaires dans diverses institutions financières bulgares et demande donc à la juridiction d'autoriser la levée du secret bancaire concernant les soldes présents sur ces comptes.

LES DISPOSITIONS PERTINENTES DU DROIT BULGARE :

A) Zakon za zashtita na lichnite danni [loi sur la protection des données à caractère personnel, ci-après la « ZZLD », Darzhaven Vestik (journal officiel, ci-après le « DV ») n° 1, du 4 janvier 2002 [OMISSIS]]

- 20 « **Article 6** (1) [OMISSIS] La Commission de protection des données à caractère personnel, ci-après dénommée "la commission", est une autorité permanente et indépendante de contrôle qui assure la protection des personnes lors du traitement de leurs données à caractère personnel et lors de l'accès à ces données, ainsi que le contrôle du respect du règlement (UE) 2016/679 et de la présente loi.
- 21 **Article 12a** [OMISSIS] (1) Sur demande, le responsable du traitement et le sous-traitant coopèrent avec la commission dans l'exécution de ses tâches et l'exercice de ses pouvoirs.
- 22 **Article 17** [OMISSIS] (1) L'Inspection près le Conseil supérieur de la magistrature – ci-après, "l'Inspection" – surveille et contrôle le respect du règlement (UE) 2016/679, de la présente loi et des actes en matière de protection des données à caractère personnel, lorsque des données à caractère personnel sont traitées par :
 1. la juridiction dans l'exercice de ses fonctions d'autorité du pouvoir judiciaire, et

2. le parquet et les autorités d'enquête dans l'exercice de leurs fonctions d'autorités du pouvoir judiciaire aux fins de la prévention, de la détection, de l'instruction ou de la poursuite d'infractions pénales ou de l'exécution de sanctions pénales.

(2) Les modalités de mise en œuvre de l'activité visée au paragraphe 1, y compris la réalisation de contrôles et l'examen des procédures devant l'Inspection, sont fixées par le règlement visé à l'article 55, paragraphe 8, de la loi relative au pouvoir judiciaire.

(3) Lors de l'exercice de la surveillance visée au paragraphe 1, l'article 12a s'applique également.

23 **Article 17a** [OMISSIS] (1) Lorsqu'elle contrôle le traitement de données à caractère personnel par une juridiction dans l'exercice de ses fonctions d'autorité judiciaire, sauf dans les cas de traitement de données à caractère personnel aux fins de l'article 42, paragraphe 1, l'Inspection :

1. accomplit les missions visées à l'article 57, paragraphe 1, points a) à i), l), u) et v), et paragraphes 2 et 3, du règlement (UE) 2016/679 ;

2. exerce les pouvoirs conférés par l'article 58, paragraphe 1, sous a), b), d), e), f), paragraphe 2, sous a) à g), i) et j), et paragraphe 3, sous a), b) et c), du règlement (UE) 2016/679 ;

3. applique la liste établie par la commission, conformément à l'article 35, paragraphe 4, du règlement (UE) 2016/679 lu en combinaison avec l'exigence d'une analyse d'impact relative à la protection des données ;

4. saisit la juridiction en cas de violation du règlement (UE) 2016/679.

(2) Outre les tâches et les compétences visées au paragraphe 1, l'Inspection :

1. participe à la coopération internationale, avec d'autres autorités de protection des données à caractère personnel et organisations internationales, sur les questions de protection des données personnelles ;

2. émet des instructions, des recommandations et des bonnes pratiques en matière de protection des données à caractère personnel.

(3) Dans le cadre du contrôle du traitement des données à caractère personnel effectué, aux fins de l'article 42, paragraphe 1, par le tribunal, le ministère public et les autorités d'enquête dans l'exercice de leurs fonctions d'autorités judiciaires, l'Inspection s'acquitte des tâches et exerce les pouvoirs visés au chapitre huit.

24 **Article 20** [OMISSIS] L'inspecteur général, les inspecteurs et les fonctionnaires de justice de l'administration de l'Inspection sont tenus de ne pas divulguer ou tirer profit, pour eux-mêmes ou pour autrui, des informations constituant un secret

protégé par la loi dont ils ont eu connaissance dans le cadre de leurs activités au titre de la présente loi, tant que le délai de protection n'a pas expiré. »

25 **B) Danachno-osiguriteln protsesualen kodeks** (code de procédure fiscale et des assurances sociales, ci-après le « DOPK », promulgué au DV n° 105, du 29 décembre 2005 [OMISSIS])

26 « **Suspension de la procédure**

Article 34 (1) La procédure est suspendue : (...)

2. si une procédure administrative, pénale ou autre procédure juridictionnelle, pertinente pour l'issue du litige, est en cours – sur présentation d'un certificat délivré par l'autorité devant laquelle ladite procédure se déroule (...).

(3) [OMISSIS] Dans le cas d'un motif visé aux paragraphes (1) ou (2), l'appréciation est effectuée par l'autorité qui a ordonné la procédure et, en cas de recours administratif, par l'autorité statuant. La procédure est suspendue par une injonction signifiée aux personnes concernées.

(4) [OMISSIS] L'absence de décision dans les 7 jours à compter de la réception de la demande de suspension déposée par la personne partie à la procédure vaut refus implicite.

(5) [OMISSIS] L'injonction et le refus de suspendre la procédure sont susceptibles de recours dans un délai de 14 jours à compter de la signification de l'injonction, ou de l'expiration du délai pour statuer visé au paragraphe 4, par l'autorité dont l'acte est attaqué. Le recours est formé devant le tribunal administratif du domicile du requérant.

(6) [OMISSIS] Dans un délai de 14 jours à compter de la réception de l'acte introductif d'instance, la juridiction rend une ordonnance de rejet ou annulant l'injonction ou le refus de surseoir à statuer.

(7) [OMISSIS] L'ordonnance rendue par la juridiction en vertu du paragraphe (6) est définitive.

(8) [OMISSIS] Lorsque la procédure est suspendue dans le cadre d'une procédure d'échange d'informations avec un autre État pendante, la durée de la suspension ne peut excéder 8 mois.

27 **Collecte et appréciation des preuves**

Article 37 (1) Dans les procédures administratives, les preuves sont collectées d'office par l'autorité fiscale ou à l'initiative de l'intéressé. Tous les éléments de preuve recueillis font l'objet d'une appréciation et d'une analyse objectives.

(2) Une personne est tenue de produire toutes les données, informations, documents, papiers, supports et autres éléments de preuve relatifs à ses droits et

obligations, de présenter les faits et circonstances à établir dans le cadre de la procédure concernée, et d'identifier toutes les personnes, autorités publiques ou municipales en possession de ces éléments.

(3) L'autorité fiscale peut demander par écrit à la personne de fournir les preuves visées au paragraphe 2 dans le délai qu'elle impartit.

(4) Dans le cas où l'intéressé ne fournit pas les informations demandées en vertu de l'article 3, l'autorité fiscale peut considérer qu'elles n'existent pas et décider de n'apprecier que les preuves recueillies dans la procédure. (...)

28 Audits et inspections

Article 110 (1) Les autorités fiscales exercent un contrôle fiscal et de sécurité sociale en effectuant des audits et des inspections.

(2) L'audit est un ensemble d'actions des autorités fiscales visant à établir les obligations fiscales et de sécurité sociale.

(3) L'inspection est un ensemble d'actions menées par les autorités fiscales concernant le respect de la législation en matière de fiscalité et de sécurité sociale. Certains faits et circonstances pertinents pour fonder les obligations fiscales et de sécurité sociale peuvent être établis moyennant une inspection. Les obligations fiscales et de sécurité sociale de la personne contrôlée ne peuvent pas être établies moyennant une inspection.

(4) Les autorités fiscales réalisent l'inspection sans qu'une mission expresse écrite soit nécessaire. Les règles visées à l'article 8 ne s'appliquent pas si la mission est ordonnée par le directeur exécutif ou son délégué. Le résultat de l'inspection fait l'objet d'un rapport lorsque la loi ne prévoit pas d'acte clôturant l'inspection.

(5) [OMISSIS] Sauf disposition légale contraire, le délai pour effectuer les inspections ne peut être supérieur à six mois à compter de la date du premier acte de procédure, qui doit être attesté par un rapport ou une demande notifiés en vertu de l'article 37, paragraphe 3. Si le délai de six mois s'avère insuffisant, il peut être porté à six mois par décision de l'autorité qui a ordonné l'inspection. Lorsqu'un rapport est établi sur les résultats de l'inspection, il doit être communiqué à la personne dans les sept jours suivant sa clôture.

(6) [OMISSIS] En cas d'inspection, l'article 116 s'applique le cas échéant. »

C) Zakon za kreditnite instituitsii (loi sur les établissements de crédit, promulguée au DV n° 59, du 21 juillet 2006 [OMISSIS])

29 « **Article 62** (1) [OMISSIS] Il est interdit aux employés de banque, aux membres des organes de gestion et de surveillance des banques, aux agents de la Banque nationale de Bulgarie (BNB), aux employés et aux membres du conseil

d'administration du Fonds de garantie des dépôts, aux liquidateurs, aux administrateurs provisoires et aux syndics, ainsi qu'à toutes autres personnes travaillant pour une banque, de divulguer ou utiliser à leur profit personnel ou au profit des membres de leur famille des informations constituant un secret bancaire.

(2) Le secret bancaire est constitué par les faits et circonstances affectant les soldes et les opérations des comptes et dépôts des clients de la banque.

(3) [OMISSIS] Les personnes visées au paragraphe 1 signent à leur entrée en fonction, ou avant d'entamer l'exécution de la mission qui leur est confiée, une déclaration de respect du secret bancaire.

(4) La disposition du paragraphe 1 s'applique également aux cas dans lesquels la relation de ces personnes avec la banque a été rompue ou leur activité a cessé.

(5) [OMISSIS] Sauf à la BNB et aux fins et dans les conditions de l'article 56, la banque ne peut fournir les informations visées au paragraphe 2 concernant des clients individuels que :

1. avec leur consentement ;
2. en vertu d'une décision d'une juridiction, prise conformément aux paragraphes 6 et 7 ;
3. [OMISSIS] sur ordonnance d'une juridiction, lorsque cela est nécessaire pour clarifier les circonstances d'une affaire dont elle est saisie ;
4. [OMISSIS] dans les situations visées au paragraphe 12, dans le cas d'une banque faisant l'objet d'une procédure d'insolvabilité ; ou
5. [OMISSIS] dans le cadre d'une procédure arbitrale internationale en cours, à laquelle la République de Bulgarie est partie.

(6) La juridiction peut également ordonner la divulgation des informations visées au paragraphe 2, à la demande :

3. du directeur de la direction territoriale de l'Agence nationale des revenus, lorsque :
 - a) est apportée la preuve que la personne contrôlée a empêché la réalisation d'une inspection ou d'un audit ou n'a pas tenu les registres nécessaires ou que ces registres sont incomplets ou non fiables ;
 - b) est constatée par acte de l'autorité étatique compétente la survenance d'un événement ayant entraîné la destruction des livres comptables de la personne contrôlée ; (...)

(7) Le juge du Rayonen sad (tribunal d'arrondissement) statue en chambre du conseil par décision motivée sur la demande visée au paragraphe 6, au plus tard

dans les 24 heures suivant la réception de la demande, en précisant la période à laquelle se rapportent les renseignements visés au paragraphe 1. La décision du tribunal est insusceptible de recours. »

LIEN AVEC LE DROIT DE L'UNION EUROPÉENNE. NÉCESSITÉ D'UNE INTERPRÉTATION :

- 30 La juridiction de céans a été saisie par la NAP d'une demande de levée du secret bancaire (concernant les soldes des comptes bancaires) d'un contribuable qui aurait uniquement refusé de fournir ces données.
- 31 Sur le rôle de la juridiction dans le processus de divulgation des données à caractère personnel de contribuables**
- 32 Le rôle de la juridiction en tant qu'autorité autorisant la NAP à accéder aux données à caractère personnel des personnes contrôlées n'est pas clair. La situation juridique et les obligations d'une telle institution publique – qui n'a pas d'accès direct aux données à caractère personnel, mais doit donner une autorisation formelle à l'organisme qui les traitera, afin que celui-ci puisse y accéder – ne sont pas directement réglementées par le RGPD.
- 33 Il convient donc de déterminer si les juridictions qui accordent une telle autorisation ont la qualité de « responsable du traitement » au sens de l'article 4, point 7, du RGPD, dans la mesure où elles accordent un accès à ces données qui ne peut être obtenu sans leur autorisation.
- 34 Il convient ici de souligner que, selon l'interprétation qui prévaut, dans la présente procédure les juridictions exercent un contrôle purement formel, lequel se limite à déterminer si les personnes dont le secret bancaire est levé ont la qualité de contribuables et si en l'espèce ils n'ont pas fourni les données pertinentes pour un contrôle fiscal qui leur avaient été demandées. Il apparaît que, si le droit national bulgare devait s'appliquer sans aucun sens critique, les juridictions devraient toujours autoriser la levée du secret bancaire dans ces situations. En revanche, tel ne serait pas le cas si la juridiction pouvait être considérée comme le responsable du traitement des données à caractère personnel auxquelles elle donne accès, puisque le responsable du traitement a un certain nombre de responsabilités pour assurer la sécurité des données en vertu des articles 32 à 34 du RGPD, y compris des vérifications minimales de l'existence de moyens permettant de garantir la sécurité.
- 35 Aux termes de la définition donnée à l'article 4, point 7, du RGPD, le « responsable du traitement » est celui « qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement » ; par ailleurs, une règle spéciale a été introduite en vertu de laquelle « 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 ».

- 36 Le droit bulgare ne définit pas qui est le responsable du traitement des données aux fins de cette procédure. Les articles 17 et suivants du *Zakon za sadebnata vlast* (loi sur le pouvoir judiciaire) régissent les fonctions de l'Inspection près le Conseil supérieur de la magistrature en tant qu'autorité de contrôle de la protection des données à caractère personnel dans les procédures judiciaires, conformément à l'article 23, paragraphe 1, sous f), du RGPD, lu en combinaison avec son considérant 20. Or, tel n'est pas le cas en l'espèce – ce n'est pas la juridiction qui est contrôlée au sujet des modalités du traitement des données à caractère personnel. Les juridictions contrôlent cette activité en accordant ou en refusant l'accès aux données.
- 37 En ce sens, bien que les autorités judiciaires n'aient pas un accès direct aux données à caractère personnel dont la divulgation est demandée (ce qui ne constitue pas une condition nécessaire pour désigner une personne comme « responsable de traitement » de données à caractère personnel – voir arrêt de la Cour de justice du 10 juillet 2018, *Jehovan todistajat*, C-25/17, EU:C:2018:551, point 3), elles déterminent dans une certaine mesure les finalités du traitement en autorisant ou en interdisant l'accès à des données à caractère personnel constitutives d'un secret bancaire. À cet égard, il semble que la juridiction puisse, selon une certaine interprétation de la loi, être considérée comme l'autorité qui détermine les finalités pour lesquelles les données sont traitées.
- 38 Il convient également de souligner que le législateur bulgare n'a pas fait usage de son pouvoir d'indiquer dans cette situation spéciale, où les finalités du traitement des données à caractère personnel sont précisées dans la loi, quelle autorité a les droits et obligations d'un responsable du traitement des données à caractère personnel. Dans ces conditions, il y a lieu de fixer des critères d'interprétation de cette disposition afin de déterminer si la juridiction autorisant l'accès peut elle aussi être considérée, au même titre que la NAP, comme un responsable du traitement des données à caractère personnel.
- 39 Compte tenu du manque de clarté des règles nationales, il est également nécessaire de répondre à la question de savoir si une autorité judiciaire, laquelle détermine les conditions d'accès d'une autre autorité étatique à des données à caractère personnel constituant un secret bancaire, ne peut pas également être considérée comme une autorité de contrôle exerçant une partie des pouvoirs prévus par le RGPD dans le domaine étroit du contrôle de l'accès aux données.

Sur les obligations en matière de protection des données à caractère personnel pesant sur la juridiction donnant l'autorisation

- 40 En l'espèce, il existe des informations publiques selon lesquelles la NAP a commis une violation de la sécurité des données à caractère personnel en divulguant des données sur plus de cinq millions de personnes vivantes, ainsi que

des données publiques concernant des déficiences techniques et organisationnelles en matière d'autorisations d'accès aux données. Les autorités de contrôle l'ont enjoint à 21 reprises au moins à prendre des mesures spécifiques dont il n'y a pas de preuve de la mise en œuvre. En outre, le *

- 41 Selon les communiqués de la principale autorité de contrôle en Bulgarie au sens de l'article 51 du RGPD (la Commission de protection des données à caractère personnel), pour ce manquement, une amende a été infligée à la NAP. Il convient toutefois de vérifier si une telle violation justifie que la juridiction qui accorde la levée du secret bancaire vérifie, comme une sorte d'autorité de contrôle, si des mesures supplémentaires de protection des données ont été prises.
- 42 Si la juridiction a un rôle de responsable du traitement ou d'autorité de contrôle, il semblerait qu'un tel contrôle soit nécessaire pour s'assurer que le pouvoir judiciaire ne fonctionne pas comme une simple chambre d'enregistrement en accordant des autorisations d'accès aux données, mais qu'il vérifie au contraire si des mesures ont été prises pour que les données soient traitées et protégées conformément à la loi, compte tenu notamment du fait que des informations ont été rendues publiques selon lesquelles la NAP attaque toute décision l'enjoignant à prendre des mesures de protection des données.
- 43 Dans ce contexte, il apparaît que la juridiction ne devra accorder la levée du secret bancaire qu'après avoir demandé des informations sur les procédures de sécurité applicables et après s'être assurée que ces procédures garantissent, du moins à première vue, une protection contre une violation ultérieure de la sécurité des données à caractère personnel. Il est donc nécessaire de répondre à la question de savoir si la juridiction nationale aurait de tels pouvoirs en tant qu'autorité accordant l'accès.
- 44 Toutefois, il convient également de répondre à la question de savoir si, même si elle n'a pas la qualité de responsable du traitement des données à caractère personnel ou d'autorité de contrôle, la juridiction à laquelle le droit national confère le pouvoir d'autoriser l'accès aux données à caractère personnel couvertes par le secret bancaire peut procéder à de tels contrôles en vertu de l'obligation de protection juridictionnelle effective prévue à l'article 79 du RGPD.
- 45 En effet, cette disposition a été édictée pour les cas dans lesquels c'est par une saisine expresse du juge que la personne concernée par les données demande une protection. Or, lorsque la procédure de divulgation des données est menée sans la participation de l'intéressé et que le droit national a expressément instauré un contrôle juridictionnel préalable, il semble qu'une obligation similaire doive s'appliquer d'office. Cela semble également découler du droit de chaque personne concernée à un recours juridictionnel effectif, tel que consacré à l'article 47 de la charte des droits fondamentaux de l'Union européenne. En l'absence d'une telle obligation, le juge se limitera toujours à un examen formel et à une confirmation

* Ndt : il manque la suite de la phrase.

de l'action de l'administration, ce qui apparaît contraire aux objectifs de l'article 79 du RGPD.

- 46 A la lumière de ce qui précède, il convient également de préciser les obligations de la juridiction en matière de protection des données à caractère personnel dans le cadre d'une procédure d'autorisation d'accès à ces données, même en supposant que la juridiction nationale n'agit alors pas en qualité de responsable du traitement ou d'autorité de contrôle.
- 47 Au vu de ce qui précède, le tribunal de céans se voit dans l'obligation de soumettre à la Cour de justice de l'Union européenne des questions relatives à l'interprétation du droit de l'Union. Par ces motifs, le Sofiyski rayonnen sad (tribunal d'arrondissement de Sofia) [OMISSIS]

ORDONNE :

- 48 [OMISSIS]
- 49 **RENVOIE** conformément à l'article 267, premier alinéa, TFUE, les questions préjudicielles suivantes à la **COUR DE JUSTICE DE L'UNION EUROPÉENNE** :
- 50 1. Convient-il d'interpréter l'article 4, point 7, du règlement (UE) 2016/679 (le « règlement général sur la protection des données ») en ce sens que :
- une autorité judiciaire, laquelle autorise une autre autorité étatique à accéder aux données relatives aux soldes des comptes bancaires de contribuables, détermine les finalités ou les moyens du traitement des données à caractère personnel et constitue donc un « responsable du traitement » des données à caractère personnel ?
- 51 2. S'il est répondu par la négative à la première question, convient-il d'interpréter l'article 51 du règlement général sur la protection des données en ce sens qu'une autorité judiciaire, laquelle autorise une autre autorité étatique à accéder aux données relatives aux soldes des comptes bancaires de contribuables est chargée de surveiller l'application de ce règlement et la qualité d'« autorité de contrôle » en ce qui concerne ces données ?
- 52 3. S'il est répondu par l'affirmative à l'une des questions précédentes, convient-il d'interpréter l'article 32, paragraphe 1, sous b), du règlement général sur la protection des données, respectivement son article 57, paragraphe 1, sous a), en ce sens qu'une autorité judiciaire, laquelle autorise une autre autorité étatique à accéder aux données relatives aux soldes des comptes bancaires de contribuables est tenue, lorsqu'il existe des informations sur une violation antérieure de la sécurité des données à caractère personnel par l'autorité à laquelle l'accès doit être accordé, de demander des informations sur les mesures qui ont été prises en matière de protection des données et d'examiner l'adéquation de ces mesures lorsqu'elle décide d'accorder ou non l'accès ?

- 53 4. Indépendamment des réponses aux [deuxième] et [troisième] questions, convient-il d'interpréter l'article 79, paragraphe 1, du règlement général sur la protection des données, lu en combinaison avec l'article 47 de la charte des droits fondamentaux de l'Union européenne, en ce sens que, lorsque le droit national de l'un des États de l'Union prévoit que certaines catégories de données ne peuvent être divulguées qu'après autorisation judiciaire, la juridiction qui accorde cette autorisation est tenue d'assurer d'office la protection des personnes dont elle divulgue les données en exigeant de l'autorité étatique qui demande l'accès aux données, et dont il est notoire qu'elle s'est vue imposer des dispositions contraignantes par l'autorité visée à l'article 51, paragraphe 1, RGPD après avoir commis une violation de la sécurité de données à caractère personnel, de fournir des informations sur la mise en œuvre des mesures qui lui ont été imposées moyennant une décision administrative au titre de l'article 58, paragraphe 2, sous d), RGPD ?

[OMISSIS]

DOCUMENT DE TRAVAIL