La protection des données à caractère personnel devant les juridictions européennes (I)

Van Gyseghem, Jean-Marc

Published in:
Journal européen des droits de l'homme

Publication date:
2023

Document Version
le PDF de l'éditeur

La protection des données à caractère personnel devant les juridictions européennes (I) – Chronique de jurisprudence (2022)

Personal Data Protection in European Law (I) – Column of Case Law (2022)

Jean-Marc Van Gyseghem[1]

Résumé

La chronique analyse la contribution du Tribunal et de la Cour de justice de l'Union européenne à la protection des données pour l'année 2022.

Les arrêts concernent diverses législations européennes qu'il s'agisse du RGPD, de la directive PNR, de la directive 2016/680 ou encore de la directive 2002/58. Cependant, les diverses questions analysées par les juridictions européennes et reprises dans la présente chronique concernent tant la primauté du droit européen que les divers principes qui régissent la protection de la vie privée et, de manière plus particulière, les données à caractère personnel.

La chronique montre également une inflation de nombre d'arrêts des juridictions européennes et, principalement, de la Cour qui concernent ces matières.

Abstract

The chronicle analyzes the contribution of the Tribunal and the Court of Justice of the European Union to data protection for the year 2022.

As far as they are concerned, the decisions deal with various European legislations as the RGPD, the PNR Directive, Directive 2016/680 or Directive 2002/58. However, the various issues analyzed by the European courts and taken up in this chronicle go from the primacy of European law to the rights of the rights of data subject. They go through the various principles governing the protection of privacy and, more specifically, personal data.

The chronicle also shows an inflation in the number of decisions handed down by the European courts, and, principally, by the European Court of Justice, dealing with these matters.

I. Principe de libre circulation des personnes et directive PNR

Dans le cadre de l'analyse de la loi belge transposant, entre autres, la directive PNR, la Cour s'attache à la question du « traitement, par les autorités compétentes, des données PNR des vols et des transports effectués par d'autres moyens à

[1] This work has been done with the financial support from the European Union's Digital Europe program under Grant Agreement 101100700 (TEF-Health). La publication ne reflète que l'opinion de son auteur et la Commission européenne ne peut être tenue responsable de l'usage qui en serait fait.

l'intérieur de l'Union, en provenance ou à destination de l'État membre ayant adopté ladite législation ou bien encore transitant par cet État membre ». En préambule de cette analyse, elle rappelle que la libre circulation des personnes constitue une des libertés fondamentales de l'Union européenne et qu'« une législation nationale qui désavantage certains ressortissants nationaux en raison du seul fait qu'ils ont exercé leur liberté de circuler et de séjourner dans un autre État membre constitue une restriction aux libertés reconnues par l'article 45, paragraphe 1, de la Charte [des droits fondamentaux de l'Union européenne] à tout citoyen de l'Union (voir en ce sens, en ce qui concerne l'article 21, paragraphe 1, TFUE, arrêts du 8 juin 2017, *Freitag*, C-541/15, EU:C:2017:432, point 35 et jurisprudence citée, ainsi que du 19 novembre 2020, *ZW*, C-454/19, EU:C:2020:947, point 30) »[2].

Elle complète son raisonnement en rappelant sa jurisprudence constante selon laquelle « une restriction à la libre circulation des personnes ne peut être justifiée que si elle se fonde sur des considérations objectives et est proportionnée à l'objectif légitimement poursuivi par le droit national. Une mesure est proportionnée lorsque, tout en étant apte à la réalisation de l'objectif poursuivi, elle ne va pas au-delà de ce qui est nécessaire pour l'atteindre (voir, en ce sens, arrêt du 5 juin 2018, *Coman e.a.*, C-673/16, EU:C:2018:385, point 41 ainsi que jurisprudence citée) » et qu'« il importe d'ajouter qu'une mesure nationale qui est de nature à entraver l'exercice de la libre circulation des personnes ne peut être justifiée que lorsque cette mesure est conforme aux droits fondamentaux garantis par la Charte dont la Cour assure le respect (arrêt du 14 décembre 2021, *Stolichna obshtina, rayon "Pancharevo"*, C-490/20, EU:C:2021:1008, point 58 et jurisprudence citée) »[3].

En conséquence, « s'agissant de la question de savoir si une législation nationale adoptée aux fins de transposer la directive PNR et qui étend le système prévu par cette directive aux vols intra-UE et à d'autres modes de transport intérieurs à l'Union est apte à la réalisation de l'objectif poursuivi, il ressort des indications figurant dans le dossier dont dispose la Cour que l'utilisation des données PNR permet d'identifier des personnes qui n'étaient pas soupçonnées de participation à des infractions terroristes ou à des formes graves de criminalité et qui devraient être soumises à un examen plus approfondi, de sorte qu'une telle législation paraît appropriée pour atteindre l'objectif de lutte contre les infractions terroristes et les formes graves de criminalité recherché »[4].

II. Effet immédiat du RGPD

Dans un dossier concernant Meta Platform Ireland, la Cour rappelle qu'« en vertu de l'article 288 TFUE et en raison même de la nature des règlements et de leur

[2] CJUE, 21 juin 2022, *Ligue des droits humains c. Conseil des ministres*, C-817/19, § 277.
[3] *Ibid.*, § 281.
[4] *Ibid.*, § 284.

fonction dans le système des sources du droit de l'Union, les dispositions des règlements ont, en général, un effet immédiat dans les ordres juridiques nationaux, sans que les autorités nationales aient besoin de prendre des mesures d'application. Néanmoins, certaines de ces dispositions peuvent nécessiter, pour leur mise en œuvre, l'adoption de mesures d'application par les États membres (arrêt du 15 juin 2021, *Facebook Ireland e.a.*, C-645/19, EU:C:2021:483, point 110 ainsi que jurisprudence citée) »[5].

III. Primauté du droit de l'Union européenne

Dans le cadre de l'analyse de la directive PNR sur question préjudicielle posée par la Cour constitutionnelle belge, la Cour a réaffirmé que « le principe de primauté du droit de l'Union consacre la prééminence du droit de l'Union sur le droit des États membres. Ce principe impose dès lors à toutes les instances des États membres de donner leur plein effet aux différentes dispositions du droit de l'Union, le droit des États membres ne pouvant affecter l'effet reconnu à ces dispositions sur le territoire desdits États. En vertu de ce principe, à défaut de pouvoir procéder à une interprétation de la législation nationale conforme aux exigences du droit de l'Union, le juge national chargé d'appliquer, dans le cadre de sa compétence, les dispositions du droit de l'Union a l'obligation d'assurer le plein effet de celles-ci en laissant au besoin inappliquée, de sa propre autorité, toute disposition contraire de la législation nationale, même postérieure, sans qu'il ait à demander ou à attendre l'élimination préalable de celle-ci par voie législative ou par tout autre procédé constitutionnel (arrêts du 15 juillet 1964, *Costa*, 6/64, EU:C:1964:66, p. 1159 et 1160 ; du 6 octobre 2020, *La Quadrature du Net e.a.*, C-511/18, C-512/18 et C-520/18, EU:C:2020:791, points 214 et 215, ainsi que du 5 avril 2022, *Commissioner of An Garda Síochána e.a.*, C-140/20, EU:C:2022:258, point 118) ». Il serait donc « porté atteinte à la primauté et à l'application uniforme du droit de l'Union si des juridictions nationales avaient le pouvoir de donner aux dispositions nationales la primauté par rapport au droit de l'Union auquel ces dispositions contreviennent, serait-ce même à titre provisoire (arrêt du 5 avril 2022, *Commissioner of An Garda Síochána e.a.*, C-140/20, EU:C:2022:258, point 119 ainsi que jurisprudence citée) »[6].

Ainsi et dans le cadre de la transposition de la directive PNR en droit belge, « le maintien des effets d'une législation nationale, telle que la loi [belge] du 25 décembre 2016 [transposant, entre autres, la directive PNR], signifierait que cette législation continue à imposer aux transporteurs aériens comme à d'autres transporteurs et aux opérateurs de voyage des obligations qui sont contraires au droit de l'Union et qui comportent des ingérences graves dans les droits fondamentaux des personnes dont les données ont été transférées, conservées

[5] CJUE, 28 avril 2022, *Meta Platforms Ireland Limited, anciennement Facebook Ireland Limited c. Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V.*, C-319/20, § 58.
[6] CJUE, 21 juin 2022, *Ligue des droits humains c. Conseil des ministres*, C-817/19, précité, § 294.

et traitées ainsi que des restrictions à la liberté de circulation de ces personnes allant au-delà de ce qui est nécessaire (voir, par analogie, arrêt du 5 avril 2022, *Commissioner of An Garda Síochána e.a.*, C-140/20, EU:C:2022:258, point 122 et jurisprudence citée) »[7].

Parallèlement, la Cour réaffirme son pouvoir « à titre exceptionnel et pour des considérations impérieuses de sécurité juridique [d']accorder une suspension provisoire de l'effet d'éviction exercé par une règle du droit de l'Union à l'égard du droit national contraire à celle-ci. Une telle limitation dans le temps des effets de l'interprétation de ce droit donnée par la Cour ne peut être accordée que dans l'arrêt même qui statue sur l'interprétation sollicitée ». Elle avait, par exemple, usé de ce pouvoir dans son arrêt du 29 juillet 2019[8]. Cependant une telle mesure exceptionnelle ne pouvait être envisagée dans la cause Ligue des droits humains contre Conseil des ministres[9].

IV. Règle d'interprétation du droit de l'Union

Dans un arrêt du 21 juin 2022 qui sera analysé plus précisément ci-après, la Cour a rappelé que « selon un principe général d'interprétation, un acte de l'Union doit être interprété, dans la mesure du possible, d'une manière qui ne remette pas en cause sa validité et en conformité avec l'ensemble du droit primaire et, notamment, avec les dispositions de la Charte. Ainsi, lorsqu'un texte du droit dérivé de l'Union est susceptible de plus d'une interprétation, il convient de donner la préférence à celle qui rend la disposition conforme au droit primaire plutôt qu'à celle conduisant à constater son incompatibilité avec celui-ci (arrêt du 2 février 2021, *Consob*, C-481/19, EU:C:2021:84, point 50 et jurisprudence citée) »[10].

De plus, « il est de jurisprudence constante que, lorsque les dispositions d'une directive laissent aux États membres une marge d'appréciation pour définir des mesures de transposition qui soient adaptées aux différentes situations envisageables, il leur incombe, lors de la mise en œuvre de ces mesures, non seulement d'interpréter leur droit national d'une manière conforme à la directive dont il s'agit, mais également de veiller à ne pas se fonder sur une interprétation de celle-ci qui entrerait en conflit avec les droits fondamentaux protégés par l'ordre juridique de l'Union ou avec les autres principes généraux reconnus dans cet ordre juridique [voir, en ce sens, arrêts du 15 février 2016, *N.*, C-601/15 PPU, EU:C:2016:84, point 60 et jurisprudence citée, ainsi que du 16 juillet 2020, *État belge (Regroupement familial – Enfant mineur)*, C-133/19, C-136/19 et C-137/19, EU:C:2020:577, point 33 et jurisprudence citée] »[11].

---

[7] *Ibid.*, § 295.
[8] CJUE, 27 juillet 2019, *Inter-Environnement Wallonie et Bond Beter Leefmilieu Vlaanderen*, C-411/17, §§ 175, 176, 179 et 181.
[9] CJUE, 21 juin 2022, *Ligue des droits humains c. Conseil des ministres*, C-817/19, précité, § 295.
[10] *Ibid.*, § 86.
[11] *Ibid.*, § 87.

V. Compétence de la Cour

Dans un arrêt du 20 octobre 2022, la Cour a rappelé qu'il lui appartient de donner une réponse utile aux juridictions nationales afin qu'elles puissent trancher les litiges. En conséquence, « il [lui] incombe, le cas échéant, de reformuler les questions qui lui sont soumises [voir, en ce sens, arrêt du 7 juillet 2022, *Pensionsversicherungsanstalt (Périodes d'éducation d'enfants à l'étranger)*, C-576/20, EU:C:2022:525, point 35 et jurisprudence citée]. À ces fins, la Cour peut extraire de l'ensemble des éléments fournis par la juridiction de renvoi, et notamment de la motivation de la décision de renvoi, les éléments dudit droit qui appellent une interprétation compte tenu de l'objet du litige au principal (voir, en ce sens, arrêt du 2 juin 2022, *HK/Danmark et HK/Privat*, C-587/20, EU:C:2022:419, point 18 ainsi que jurisprudence citée) »[12].

La Cour a également confirmé, dans un arrêt du 27 octobre 2023, que « les questions relatives à l'interprétation du droit de l'Union posées par le juge national dans le cadre réglementaire et factuel qu'il définit sous sa responsabilité, et dont il n'appartient pas à la Cour de vérifier l'exactitude, bénéficient d'une présomption de pertinence. Le refus de la Cour de statuer sur une demande de décision préjudicielle formée par une juridiction nationale n'est possible que s'il apparaît de manière manifeste que l'interprétation sollicitée du droit de l'Union n'a aucun rapport avec la réalité ou l'objet du litige au principal, lorsque le problème est de nature hypothétique ou encore lorsque la Cour ne dispose pas des éléments de fait et de droit nécessaires pour répondre de façon utile aux questions qui lui sont posées (arrêt du 1er août 2022, *Vyriausioji tarnybinės etikos komisija*, C-184/20, EU:C:2022:601, point 48 et jurisprudence citée) »[13].

VI. Recevabilité devant la CJUE

Dans un arrêt du 20 octobre 2022[14], la Cour, saisie sur question préjudicielle par la Cour de Budapest-Capitale (Hongrie), a rappelé qu'il résulte de sa jurisprudence constante « qu'il appartient au seul juge national, qui est saisi du litige et qui doit assumer la responsabilité de la décision juridictionnelle à intervenir, d'apprécier, au regard des particularités de l'affaire, tant la nécessité d'une décision préjudicielle pour être en mesure de rendre son jugement que la pertinence des questions qu'il pose à la Cour. En conséquence, dès lors que les questions posées portent sur l'interprétation ou la validité d'une règle du droit de l'Union, la Cour est, en principe, tenue de statuer. Il s'ensuit que les questions posées par les juridictions

[12] CJUE, 20 octobre 2022, *Komisia za zashtita na lichnite danni, Tsentralna izbiratelna komisia c. Koalitsia « Demokratichna Bulgaria – Obedinenie »*, C-306/21, §§ 43-44.
[13] CJUE, 20 octobre 2022, *Proximus c. Gegevensbeschermingsautoriteit*, C-129/21, § 38.
[14] CJUE, 20 octobre 2022, *Digi Távközlési és Szolgáltató Kft. c. Nemzeti Adatvédelmi és Információszabadság Hatóság*, C-77/21.

nationales bénéficient d'une présomption de pertinence. Le refus de la Cour de statuer sur une question préjudicielle posée par une juridiction nationale n'est possible que s'il apparaît que l'interprétation sollicitée n'a aucun rapport avec la réalité ou l'objet du litige au principal, si le problème est de nature hypothétique ou encore si la Cour ne dispose pas des éléments de fait et de droit nécessaires pour répondre de façon utile auxdites questions (arrêt du 16 juillet 2020, *Facebook Ireland et Schrems*, C-311/18, EU:C:2020:559, point 73 ainsi que jurisprudence citée) »[15].

VII. Champ d'application matériel du RGPD – interprétation des exceptions.

En matière d'exception au champ d'application matériel du RGPD, la Cour a rappelé, en réponse à la Commission européenne tendant à considérer que la conservation des données trafic et de localisation dans le domaine des télécommunications tendait à contrer la criminalité grave et devait donc être assimilée à une menace pour la sécurité nationale, qu'« une telle assimilation serait susceptible d'introduire une catégorie intermédiaire entre la sécurité nationale et la sécurité publique, aux fins d'appliquer à la seconde les exigences inhérentes à la première (arrêt du 5 avril 2022, *Commissioner of An Garda Síochána e.a.*, C-140/20, EU:C:2022:258, point 63) »[16].

En effet, « à la différence de la criminalité, même particulièrement grave, une menace pour la sécurité nationale doit être réelle et actuelle ou, à tout le moins, prévisible, ce qui suppose la survenance de circonstances suffisamment concrètes, pour pouvoir justifier une mesure de conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation, pendant une durée limitée. Une telle menace se distingue donc, par sa nature, sa gravité et le caractère spécifique des circonstances qui la constituent, du risque général et permanent qu'est celui de survenance de tensions ou de troubles, même graves, à la sécurité publique ou celui d'infractions pénales graves (arrêt du 5 avril 2022, *Commissioner of An Garda Síochána e.a.*, C-140/20, EU:C:2022:258, point 62 ainsi que jurisprudence citée) »[17].

Un mois plus tard, la Cour a rendu un arrêt[18] en réponse à une question préjudicielle posée par le Varhoven administrativen sad (Cour administrative suprême) bulgare relative à l'interprétation de la « notion de la notion d'activité qui ne relève pas du champ d'application du droit de l'Union »[19]. Le litige

[15] *Ibid.*, § 17.
[16] CJUE, 20 septembre 2022, *Bundesrepublik Deutschland c. SpaceNet AG et Telekom Deutschlend GmbH*, C-793/19 et C-794/19, § 94.
[17] *Ibid.*, § 93.
[18] CJUE, 20 octobre 2022, *Komisia za zashtita na lichnite danni, Tsentralna izbiratelna komisia c. Koalitsia « Demokratichna Bulgaria – Obedinenie »*, C-306/21, précité, §§ 43-44.
[19] Article 2.2.a) du RGPD.

à la base de cette question préjudicielle concernait une question d'enregistrement vidéo dans le cadre du processus électoral en Bulgarie et, plus particulièrement, l'interdiction pour les médias et d'autres participants au processus électoral de traiter des données à caractère personnel au moyen d'enregistrement d'images lors de l'ouverture des urnes contenant les bulletins de vote et lors de l'établissement des résultats des votes. Dans un premier temps, la Cour rappelle le principe selon lequel toute exception doit s'interpréter de manière restrictive[20].

Forte de ce rappel, elle circonscrit la notion d'« activité qui ne relève pas du champ d'application du droit de l'Union » en considérant que « l'article 2, paragraphe 2, sous a), du RGPD, lu à la lumière du considérant 16 de ce règlement, a pour seul objet d'exclure du champ d'application dudit règlement les traitements de données à caractère personnel effectués par les autorités étatiques dans le cadre d'une activité qui vise à préserver la sécurité nationale ou d'une activité pouvant être rangée dans la même catégorie, de telle sorte que le seul fait qu'une activité soit propre à l'État ou à une autorité publique ne suffit pas pour que cette exception soit automatiquement applicable à une telle activité [arrêt du 22 juin 2021, *Latvijas Republikas Saeima (Points de pénalité)*, C-439/19, EU:C:2021:504, point 66 et jurisprudence citée]. Les activités qui ont pour but de préserver la sécurité nationale visées à l'article 2, paragraphe 2, sous a), du RGPD couvrent, en particulier, celles ayant pour objet de protéger les fonctions essentielles de l'État et les intérêts fondamentaux de la société [voir, en ce sens, arrêt du 22 juin 2021, *Latvijas Republikas Saeima (Points de pénalité)*, C-439/19, EU:C:2021:504, point 67]. Or, les activités relatives à l'organisation d'élections dans un État membre ne poursuivent pas un tel objectif et ne sauraient, en conséquence, être rangées dans la catégorie des activités ayant pour but la préservation de la sécurité nationale, visées à l'article 2, paragraphe 2, sous a), du RGPD »[21].

Dans un arrêt du 8 décembre 2022[22], la Cour, analysant le champ d'application du RGPD, considère que « l'utilisation, par le parquet d'un État membre, des informations concernant une personne physique qu'il a collectées et traitées à des fins [de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces (article 1er, paragraphe 1, de la directive 2016/680)], en vue d'exercer ses droits de la défense dans le cadre d'une procédure civile, constitue un « traitement » de « données à caractère personnel », au sens de l'article 4, points 1 et 2, du RGPD »[23].

---

[20] CJUE, 20 octobre 2022, *Komisia za zashtita na lichnite danni, Tsentralna izbiratelna komisia c. Koalitsia « Demokratichna Bulgaria – Obedinenie »*, C-306/21, précité, § 35 ; voy. égal. CJUE, 22 juin 2021, *Latvijas Republikas Saeima*, C-439/19, § 62 et jurisprudence citée.

[21] *Ibid.*, §§ 39-41.

[22] CJUE, 8 décembre 2022, *VS c. Inspektor v Inspektorata kam Visshia sadeben savet*, C-180/21.

[23] *Ibid.*, § 69.

Ce litige donne ensuite l'occasion à la Cour de rappeler que « l'article 2, paragraphe 1, du RGPD définit de manière large le champ d'application matériel de ce règlement [arrêt du 22 juin 2021, *Latvijas Republikas Saeima (Points de pénalité)*, C-439/19, EU:C:2021:504, point 61], lequel inclut tout « traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu[e] [le] traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier ». Le corollaire de cette définition large est que les exceptions à l'application du RGPD, énumérées au paragraphe 2 de l'article 2 de celui-ci doivent recevoir une interprétation stricte »[24]. Pour ce qui concerne l'exception liée au « traitement de données à caractère personnel effectué par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales [voir, en ce sens, arrêt du 24 février 2022, *Valsts ieņēmumu dienests (Traitement des données personnelles à des fins fiscales)*, C-175/20, EU:C:2022:124, points 40 et 41 ainsi que jurisprudence citée] », la Cour rappelle qu'elle « est motivée par la circonstance que les traitements de données à caractère personnel par les autorités compétentes aux fins énoncées à l'article 2, paragraphe 2, sous d), du RGPD sont régis par un acte spécifique de l'Union, à savoir la directive 2016/680, laquelle a été adoptée le même jour que le RGPD [voir, en ce sens, arrêt du 24 février 2022, *Valsts ieņēmumu dienests (Traitement des données personnelles à des fins fiscales)*, C-175/20, EU:C:2022:124, point 42 et jurisprudence citée] »[25].

L'exception doit donc se lire au regard du champ d'application de la directive 2016/680 du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, à savoir le « traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces »[26]. En conclusion, la Cour estime que « le RGPD est applicable aux traitements de données à caractère personnel effectués par le parquet d'un État membre, aux fins d'exercer ses droits de la défense dans le cadre d'un recours en responsabilité de l'État, lorsque, d'une part, il informe la juridiction compétente de l'existence de dossiers concernant une personne physique partie à ce recours, ouverts aux fins énoncées à l'article 1er, paragraphe 1, de la directive 2016/680 et que, d'autre part, il transmet ces dossiers à cette juridiction »[27].

[24] *Ibid.*, § 73.
[25] *Ibid.*, § 74.
[26] Article 1.1 de la directive 2016/680.
[27] CJUE, 8 décembre 2022, *VS c. Inspektor v Inspektorata kam Visshia sadeben savet*, C-180/21, précité, § 82.

Dans un autre arrêt rendu le 21 juin 2022[28], la Cour a l'occasion de rappeler et préciser le champ d'application du RGPD dans un litige lié à la transposition des directives PNR[29], API[30] et 2010/64[31] (partiellement) en droit national par les états membre, la Belgique en l'espèce. Ainsi, elle relève que « deux conditions sont exigées pour qu'un traitement de données relève de l'exception [visée à l'article 2.2.d) du RGPD] prévoit. Si la première de ces conditions est relative aux finalités du traitement, à savoir la prévention et la détection des infractions pénales, les enquêtes et les poursuites en la matière ou l'exécution de sanctions pénales, y compris la protection contre des menaces pour la sécurité publique et la prévention de telles menaces, la seconde condition porte sur l'auteur de ce traitement, à savoir une « autorité compétente », au sens de ladite disposition »[32].

De plus, l'exception prévue à l'article 2.2.d) du RGPD doit recevoir une interprétation stricte[33]. La Cour rappelle également « qu'il ressort du considérant 19 dudit règlement [que] ladite exception est motivée par la circonstance que les traitements de données à caractère personnel effectués, par les autorités compétentes, aux fins, notamment, de prévention et de détection des infractions pénales, y compris de protection contre des menaces pour la sécurité publique et la prévention de telles menaces, sont régis par un acte plus spécifique de l'Union, à savoir la directive 2016/680, laquelle a été adoptée le même jour que le RGPD [arrêt du 22 juin 2021, *Latvijas Republikas Saeima (Points de pénalité)*, C-439/19, EU:C:2021:504, point 69] »[34].

En outre, en ses considérants 9 à 11, la directive 2016/680 « fixe des règles spécifiques relatives à la protection des personnes physiques à l'égard de ces traitements, en respectant la nature spécifique de ces activités relevant des domaines de la coopération judiciaire en matière pénale et de la coopération policière, tandis que le RGPD définit des règles générales concernant la protection de ces personnes qui ont vocation à s'appliquer auxdits traitements lorsque l'acte plus spécifique que constitue la directive 2016/680 n'est pas applicable. En particulier, selon le considérant 11 de cette directive, le RGPD s'applique au traitement de données à caractère personnel qui serait effectué par une « autorité compétente », au sens de l'article 3, paragraphe 7, de ladite directive, mais à des fins autres que celles prévues dans celle-ci [voir, en ce sens, arrêt du 22 juin 2021, *Latvijas Republikas Saeima (Points de pénalité)*, C-439/19, EU:C:2021:504, point 70] »[35].

---

[28] CJUE, 21 juin 2022, *Ligue des droits humains c. Conseil des ministres*, C-817/19, précité, § 277.
[29] Directive 2016/681 du 27 avril 2016 relative à l'utilisation des données des dossiers passagers (PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière.
[30] Directive 2004/82/CE du 29 avril 2004 concernant l'obligation pour les transporteurs de communiquer les données relatives aux passagers.
[31] Directive 2010/65/UE du 20 octobre 2010 concernant les formalités déclaratives applicables aux navires à l'entrée et/ou à la sortie des ports des États membres et abrogeant la directive 2002/6/CE.
[32] CJUE, 21 juin 2022, *Ligue des droits humains c. Conseil des ministres*, C-817/19, précité, § 67.
[33] *Ibid.*, § 70.
[34] *Ibid.*, § 71.
[35] *Ibid.*, § 72.

Au regard de ces considérations, la Cour considère que la directive PNR relève de l'exception prévue à l'article 2.2.d) du RGPD en ce que « les données PNR ne peuvent être traitées qu'à des fins de prévention et de détection des infractions terroristes et des formes graves de criminalité ainsi que d'enquêtes et de poursuites en la matière »[36].

Elle précise cependant que si les *Unités information passagers*[37] prévues par la directive PNR doivent être considérées comme autorité compétente au sens de la directive police et donc de l'article 2.2.d), du RGPD, il n'en va pas de même pour les opérateurs économiques, tels que des transporteurs aériens. En effet, ces derniers, « même s'ils sont tenus à une obligation légale de transfert des données PNR, ne sont ni chargés de l'exercice de l'autorité publique ni investis de prérogatives de puissance publique par cette directive, ne sauraient être regardés comme étant des autorités compétentes, au sens de l'article 3, paragraphe 7, de la directive 2016/680 et de l'article 2, paragraphe 2, sous d), du RGPD »[38].

Par contre, les directives API et 2010/65 ne peuvent être considérées comme entrant dans l'exception du champ d'application prévue à l'article 2.2.d), du RGPD dès lors que la première a pour objectif d'améliorer les contrôles aux frontières et à lutter contre l'immigration clandestine et la seconde « a pour objet de simplifier et d'harmoniser les procédures administratives appliquées aux transports maritimes par la généralisation de la transmission électronique des renseignements et la rationalisation des formalités déclaratives, afin de faciliter les transports maritimes et de réduire la charge administrative pesant sur les compagnies maritimes »[39]. Partant, elles entrent dans le champ d'application du RGPD.

Sur base de ces divers éléments, la Cour considère que « l'article 2, paragraphe 2, sous d), et l'article 23 du RGPD doivent être interprétés en ce sens que ce règlement est applicable aux traitements de données à caractère personnel prévus par une législation nationale visant à transposer, en droit interne, à la fois les dispositions de la directive API, de la directive 2010/65 et de la directive PNR pour ce qui est, d'une part, des traitements de données effectués par des opérateurs privés et, d'autre part, des traitements de données effectués par des autorités publiques relevant, uniquement ou également, de la directive API ou de la directive 2010/65. En revanche, ledit règlement n'est pas applicable aux traitements de données prévus par une telle législation ne relevant que de la directive PNR, qui sont effectués par l'UIP ou par les autorités compétentes aux fins visées à l'article 1er, paragraphe 2, de cette directive »[40].

---

[36] *Ibid.*, § 73.
[37] L'UIP est chargée : de la collecte, de la conservation et du traitement des données ainsi que du transfert des données ou des résultats du traitement aux autorités nationales compétentes ; de l'échange des données PNR et des résultats du traitement avec les autres États membres et l'Agence de l'Union européenne pour la coopération des services répressifs (https://eur-lex.europa.eu/FR/legal-content/summary/use-of-passenger-records-to-prevent-terrorism-and-serious-crime.html ; dernière consultation le 25 juin 2023).
[38] CJUE, 21 juin 2022, *Ligue des droits humains c. Conseil des ministres*, C-817/19, précité, § 81.
[39] *Ibid.*, § 76.
[40] *Ibid.*, § 84.

Jean-Marc Van Gyseghem

VIII. Notion de catégories particulières de données (article 9 du RGPD)

La Cour est interrogée par le tribunal administratif régional de Vilnius (Lituanie) qui est appelé à se prononcer dans un litige relatif à la loi lituanienne sur la conciliation des intérêts mettant en place un des déclarations d'intérêts des personnes travaillant dans le service public et leur contrôle. La déclaration d'intérêts doit également reprendre des données relatives au conjoint, concubin ou partenaire du déclarant sauf « s'ils vivent séparément, ne forment pas un ménage commun et qu'il n'est donc pas en possession de ces données »[41]. De plus, « sont publiques et publiées sur le site Internet de la Haute commission, conformément aux modalités définies par cette dernière, les données figurant dans les déclarations des élus et personnes occupant des postes politiques, des fonctionnaires et agents de l'État, des juges, des directeurs et directeurs adjoints d'institutions de l'État ou d'une collectivité locale [...] »[42]. Sont cependant exclues de cette publication, le numéro d'identification personnel, le numéro de sécurité sociale, des données à caractère personnel particulières ainsi que les autres renseignements dont la loi interdit la divulgation.

Une partie du litige porte sur la notion de catégories particulières de données à caractère personnel telles que visée à l'article 9 du RGPD et sur sa portée dès lors que le plaignant refuse de procéder à la déclaration d'intérêts alléguant qu'une telle déclaration porte atteinte à sa vie privée et à celle des personnes devant y être reprises. La Cour considère qu' « une interprétation large des notions de « catégories particulières de données à caractère personnel » et de « données sensibles » est confortée par l'objectif de la directive 95/46 et du RGPD [...], qui est de 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 les concernant (voir, en ce sens, arrêt du 6 novembre 2003, *Lindqvist*, C-101/01, EU:C:2003:596, point 50) »[43] et que « l'interprétation contraire irait, qui plus est, à l'encontre de la finalité de l'article 8, paragraphe 1, de la directive 95/46 et de l'article 9, paragraphe 1, du RGPD, consistant à assurer une protection accrue à l'encontre de traitements qui, en raison de la sensibilité particulière des données qui en sont l'objet, sont susceptibles de constituer, ainsi qu'il ressort du considérant 33 de la directive 95/46 et du considérant 51 du RGPD, une ingérence particulièrement grave dans les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel, garantis par les articles 7 et 8 de la Charte [voir, en ce sens, arrêt du 24 septembre 2019, *GC e.a. (Déréférencement de données sensibles)*, C-136/17, EU:C:2019:773, point 44] »[44].

[41] Article 6.2 de la loi n° VIII-371 du 2 juillet 1997 de la République de Lituanie sur la conciliation des intérêts publics et privés dans le service public (Žin., 1997, n° 67-1659).
[42] Article 10.1 de la loi n° VIII-371 du 2 juillet 1997, précitée.
[43] CJUE, 1er août 2022, *OT c. Vyriausioji tarnybinės etikos komisija*, C-184/20, § 125.
[44] *Ibid.*, § 126.

En conclusion de cette analyse, la Cour considère que « la publication, sur le site Internet de l'autorité publique chargée de collecter et de contrôler la teneur des déclarations d'intérêts privés, de données à caractère personnel susceptibles de divulguer indirectement l'orientation sexuelle d'une personne physique constitue un traitement portant sur des catégories particulières de données à caractère personnel, au sens de ces dispositions »[45]. À noter que la Cour porte son regard sur la question de la publication des données[46].

IX. Notion de responsable du traitement

Dans un litige relatif au référencement sur Google, la Cour a rappelé, dans un arrêt du 8 décembre 2022[47], que « dans la mesure où l'activité d'un moteur de recherche est susceptible d'affecter significativement et de manière additionnelle par rapport à celle des éditeurs de sites Internet les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel, l'exploitant de ce moteur en tant que personne déterminant les finalités et les moyens de cette activité doit assurer, dans le cadre de ses responsabilités, de ses compétences et de ses possibilités, que celle-ci satisfait aux exigences de la directive 95/46 et du RGPD pour que les garanties prévues par cette directive et ce règlement puissent développer leur plein effet et qu'une protection efficace et complète des personnes concernées, notamment de leur droit au respect de leur vie privée, puisse effectivement être réalisée [voir, en ce sens, arrêts du 13 mai 2014, *Google Spain et Google*, C-131/12, EU:C:2014:317, point 38, ainsi que du 24 septembre 2019, *GC e.a. (Déréférencement de données sensibles)*, C-136/17, EU:C:2019:773, point 37] »[48].

Elle ajoute que « s'agissant de l'étendue de la responsabilité et des obligations concrètes de l'exploitant d'un moteur de recherche, la Cour a déjà précisé que cet exploitant est responsable non pas du fait que des données à caractère personnel figurent sur une page Internet publiée par un tiers, mais du référencement de cette page et, tout particulièrement, de l'affichage du lien vers celle-ci dans la liste des résultats présentée aux internautes à la suite d'une recherche effectuée à partir du nom d'une personne physique, un tel affichage du lien dans une telle liste étant susceptible d'affecter significativement les droits fondamentaux de la personne concernée au respect de sa vie privée et à la protection des données à caractère personnel la concernant [voir, en ce sens, arrêts du 13 mai 2014, *Google Spain et Google*, C-131/12, EU:C:2014:317, point 80, ainsi que du 24 septembre 2019, *GC e.a. (Déréférencement de données sensibles)*, C-136/17, EU:C:2019:773, point 46] »[49].

---

[45] *Ibid.*, § 128.
[46] Pour une analyse approfondie, voy. F. Jacques, « Protection des données à caractère personnel : la Cour de justice a-t-elle transformé le RGPD en un instrument d'une sensibilité extrême ? », note sous C.J. (gde ch.), 1er août 2022, *R.D.T.I.*, 2023, à paraître.
[47] Si cet arrêt se réfère encore à la directive 95/46 du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, il est applicable sous l'empire du RGPD.
[48] CJUE, 8 décembre 2022, *TU et RE c. Google LLC*, C-460/20, § 51.
[49] *Ibid.*, § 52.

Jean-Marc Van Gyseghem

X. Notion de finalité de traitement

A. RGPD

1. *Notion de finalité*

Dans un arrêt du 20 octobre 2022[50], la Cour de justice saisie sur question préjudicielle par la Cour de Budapest-Capitale (Hongrie) analyse la question de notion de finalité dans un litige concernant la création, en avril 2018, d'une base de données dite « de test » par DIGI qui est un important fournisseur de services Internet et de télévision en Hongrie, et ce, suite à une défaillance technique d'un serveur. Cette base de données « de test » reprenant environ un tiers des clients particuliers de la société a été victime, en septembre 2019, d'une attaque opérée par un « pirate éthique » qui a ainsi réussi à avoir accès aux données de 322.000 personnes. DIGI a procédé aux corrections pour fermer la brèche de sécurité et, après effacement de la base de données « de test », a procédé à une notification auprès de l'autorité de protection hongroise. Cette dernière a cependant sanctionné DIGI au motif que, dès la défaillance technique corrigée, la base de données « de test » aurait dû être supprimée alors qu'elle a été maintenue durant 18 mois sans finalité. DIGI a contesté cette décision, devant la Cour de Budapest-Capitale, en considérant que la création de cette base de données « de test » et donc son maintien avait pour finalité la conclusion et de l'exécution des contrats d'abonnement et que la copie, dans une autre base de données, des données initialement collectées n'a pas modifié la finalité de la collecte initiale et du traitement des données.

Dans un premier temps, la Cour rappelle que « l'article 5, paragraphe 1, du [RGPD] fixe les principes relatifs au traitement des données à caractère personnel, qui s'imposent au responsable du traitement et dont ce dernier doit être en mesure de démontrer le respect, conformément au principe de responsabilité énoncé au paragraphe 2 de cet article »[51]. De plus, le libellé de l'article 5.1, b)[52] pose « l'exigence selon laquelle les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes [et] il résulte de la jurisprudence de la Cour que celle-ci implique, tout d'abord, que les finalités du traitement soient identifiées au plus tard lors de la collecte des données à caractère personnel, ensuite, que les finalités de ce traitement soient énoncées clairement et, enfin, que les finalités dudit traitement garantissent, notamment, la licéité du traitement de ces données, au sens de l'article 6, paragraphe 1, du règlement 2016/679 [voir, en ce sens, arrêt du 24 février 2022, *Valsts ieņēmumu dienests (Traitement des données personnelles à des fins fiscales)*, C-175/20, EU:C:2022:124, points 64 à 66] »[53].

---

[50] CJUE, 20 octobre 2022, *Digi Távközlési és Szolgáltató Kft. c. Nemzeti Adatvédelmi és Információszabadság Hatóság*, C-77/21, précité.
[51] *Ibid.*, § 24.
[52] « les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités [...] ».
[53] CJUE, 20 octobre 2022, *Digi Távközlési és Szolgáltató Kft. c. Nemzeti Adatvédelmi és Információszabadság Hatóság*, C-77/21, précité, § 27.

2. *Traitement ultérieur*

Par ailleurs, l'article 5.1.b) du RGPD prescrit que le traitement ultérieur doit être compatible avec les finalités du traitement initial sans donner d'indications permettant de déterminer si un traitement est compatible. Pour pallier ce déficit d'indications, la Cour tire d'une « lecture conjointe de l'article 5, paragraphe 1, sous b), de l'article 6, paragraphe 1, sous a), et de l'article 6, paragraphe 4, du règlement 2016/679 que la question de la compatibilité du traitement ultérieur des données à caractère personnel avec les finalités pour lesquelles ces données ont été initialement collectées ne se pose que dans l'hypothèse où les finalités dudit traitement ultérieur ne seraient pas identiques aux finalités de la collecte initiale »[54]. Elle poursuit son analyse en relevant qu'« il résulte de cet article 6, paragraphe 4, lu à la lumière du considérant 50 dudit règlement, que, lorsque le traitement à une fin autre que celle pour laquelle les données ont été collectées n'est pas fondé sur le consentement de la personne concernée ou sur le droit de l'Union ou le droit d'un État membre, il y a lieu, afin de déterminer si le traitement à une autre fin est compatible avec la finalité pour laquelle les données à caractère personnel ont été initialement collectées, de tenir compte, entre autres, premièrement, de l'existence éventuelle d'un lien entre les finalités pour lesquelles les données à caractère personnel ont été collectées et les finalités du traitement ultérieur envisagé ; deuxièmement, du contexte dans lequel les données à caractère personnel ont été collectées, en particulier en ce qui concerne la relation entre les personnes concernées et le responsable du traitement ; troisièmement, de la nature des données à caractère personnel ; quatrièmement, des conséquences possibles du traitement ultérieur envisagé pour les personnes concernées, et enfin, cinquièmement, de l'existence de garanties appropriées à la fois dans le cadre du traitement initial et du traitement ultérieur prévu »[55].

Après le rappel de ces critères et reprenant les conclusions de l'avocat général, la Cour relève qu'ils « traduisent la nécessité d'un lien concret, logique et suffisamment étroit entre les finalités de la collecte initiale des données à caractère personnel et le traitement ultérieur de ces données, et permettent de s'assurer que ce traitement ultérieur ne s'écarte pas des attentes légitimes des abonnés quant à l'utilisation ultérieure de leurs données »[56] et qu'ils « permettent, du reste, en troisième lieu […], d'encadrer la réutilisation de données à caractère personnel précédemment collectées en assurant un équilibre entre, d'une part, le besoin de prévisibilité et de sécurité juridique concernant les finalités du traitement de données à caractère personnel précédemment collectées et, d'autre part, la reconnaissance d'une certaine flexibilité au profit du responsable du traitement dans la gestion de ces données, et contribuent ainsi à la réalisation de l'objectif consistant à assurer un niveau cohérent et élevé de protection des personnes physiques, qui est énoncé au considérant 10 du [RGPD] »[57].

[54] *Ibid.*, § 34.
[55] *Ibid.*, § 34.
[56] *Ibid.*, § 36.
[57] *Ibid.*, § 37.

Cela étant précisé, la Cour considère que « la réalisation de tests et la correction d'erreurs qui affectent la base de données des abonnés présentent un lien concret avec l'exécution des contrats d'abonnement des clients particuliers, en ce que de telles erreurs sont susceptibles d'être dommageables pour la fourniture du service contractuellement prévu, et pour laquelle les données ont été initialement collectées. En effet, ainsi que M. l'avocat général l'a relevé au point 60 de ses conclusions, un tel traitement ne s'écarte pas des attentes légitimes de ces clients quant à l'utilisation ultérieure de leurs données à caractère personnel. Il ne ressort, du reste, pas de la décision de renvoi que tout ou partie de ces données auraient été sensibles ou que le traitement ultérieur en cause de celles-ci, en tant que tel, aurait eu des conséquences dommageables pour les abonnés ou n'aurait pas été accompagné de garanties appropriées, ce qu'il appartient, en tout état de cause, à la juridiction de renvoi de vérifier »[58].

En conséquence, « l'article 5, paragraphe 1, sous b), du règlement 2016/679 doit être interprété en ce sens que le principe de la "limitation des finalités", prévu à cette disposition, ne s'oppose pas à l'enregistrement et à la conservation par le responsable du traitement, dans une base de données créée aux fins de procéder à des tests et de corriger des erreurs, de données à caractère personnel préalablement collectées et conservées dans une autre base de données, lorsqu'un tel traitement ultérieur est compatible avec les finalités spécifiques pour lesquelles les données à caractère personnel ont été initialement collectées, ce qu'il convient de déterminer au regard des critères visés à l'article 6, paragraphe 4, de ce règlement »[59].

B. Directive PNR

Toujours quant à la notion de finalité mais dans le cadre de la directive PNR cette fois, la Cour a rappelé que « l'article 6 de la directive PNR, lu à la lumière des articles 7 et 8 ainsi que de l'article 52, paragraphe 1, de la Charte, doit être interprété en ce sens qu'il s'oppose à une législation nationale qui autorise le traitement de données PNR recueillies conformément à cette directive à des fins autres que celles expressément visées à l'article 1er, paragraphe 2, de ladite directive »[60]. En d'autres termes, tout État membre prenant une législation dans le cadre d'une directive doit en respecter la finalité. Sur base de ce principe et au regard de la loi belge de transposition de la directive PNR prévoyant que l'UIP « a également la qualité d'autorité nationale compétente habilitée à approuver la communication des données PNR à l'expiration de la période de six mois suivant le transfert de ces données à l'UIP »[61], cette dernière ne pourrait être considérée comme « disposant de toutes les qualités d'indépendance et d'impartialité requises pour exercer le contrôle préalable mentionné au point précédent du

[58] *Ibid.*, § 44.
[59] *Ibid.*, § 45.
[60] CJUE, 21 juin 2022, *Ligue des droits humains c. Conseil des ministres*, C-817/19, précité, § 237.
[61] *Ibid.*, § 238.

présent arrêt et vérifier si les conditions de communication de l'intégralité des données PNR sont remplies, tel que prévu à l'article 12, paragraphe 3, sous b), de la [directive PNR] »[62]. En conclusion et pour ce qui concerne la directive PNR, « l'article 12, paragraphe 3, sous b), de la directive PNR [réglant la communication de l'intégralité des données PNR au terme d'une période de conservation et dépersonnalisation des données] doit être interprété en ce sens qu'il s'oppose à une législation nationale selon laquelle l'autorité mise en place en tant qu'UIP a également la qualité d'autorité nationale compétente habilitée à approuver la communication des données PNR à l'expiration de la période de six mois suivant le transfert de ces données à l'UIP »[63].

XI. Principe de limitation de conservation des données

A. RGPD

Dans l'arrêt du 20 octobre 2022 déjà abordé, la Cour analyse la question de la conservation des données « sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées »[64]. Après avoir rappelé que le fait qu'un traitement soit licite ne permet pas une conservation des données à caractère personnel alors qu'une telle conservation n'est plus nécessaire, la Cour considère que « le principe de la "limitation de la conservation", prévu à [l'article 5.1.e) du RGPD], s'oppose à la conservation par le responsable du traitement, dans une base de données créée aux fins de procéder à des tests et de corriger des erreurs, de données à caractère personnel préalablement collectées pour d'autres finalités, pour une durée excédant celle qui est nécessaire à la réalisation de ces tests et à la correction de ces erreurs »[65].

B. Directive (UE) 2002/58 (directive vie privée et communications électroniques)

Dans un arrêt du 20 septembre 2022[66], la Cour rappelle que « la conservation des données relatives au trafic ou des données de localisation, susceptibles de fournir des informations sur les communications effectuées par un utilisateur d'un moyen de communication électronique ou sur la localisation des équipements terminaux qu'il utilise, présente en tout état de cause un caractère grave indépendamment de la durée de la période de conservation, de la quantité ou

[62] *Ibid.*, § 245.
[63] *Ibid.*, § 247.
[64] Article 5.1.e) du RGPD.
[65] CJUE, 20 octobre 2022, *Digi Távközlési és Szolgáltató Kft. c. Nemzeti Adatvédelmi és Információszabadság Hatóság*, C-77/21, précité, § 51.
[66] CJUE, 20 septembre 2022, *Bundesrepublik Deutschland c. SpaceNet AG et Telekom Deutschlend GmbH*, C-793/19 et C-794/19, § 94.

de la nature des données conservées, lorsque ledit ensemble de données est susceptible de permettre de tirer des conclusions très précises concernant la vie privée de la ou des personnes concernées [voir, en ce qui concerne l'accès à de telles données, arrêt du 2 mars 2021, *Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques)*, C-746/18, EU:C:2021:152, point 39] »[67]. Eu égard à ce caractère grave, « une législation nationale assurant le plein respect des conditions résultant de la jurisprudence ayant interprété la directive 2002/58 en matière d'accès aux données conservées ne saurait, par nature, être susceptible ni de limiter ni même de remédier à l'ingérence grave [dans les droits fondamentaux garantis aux articles 7 et 11 de la Charte], qui résulterait de la conservation généralisée de ces données prévue par cette législation nationale, dans les droits garantis aux articles 5 et 6 de cette directive et par les droits fondamentaux dont ces articles constituent la concrétisation (arrêt du 5 avril 2022, *Commissioner of An Garda Síochána e.a.*, C-140/20, EU:C:2022:258, point 47) »[68].

De plus, « l'existence éventuelle de difficultés pour définir précisément les hypothèses et les conditions dans lesquelles une conservation ciblée peut être effectuée ne saurait justifier que des États membres, en faisant de l'exception une règle, prévoient une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation (arrêt du 5 avril 2022, *Commissioner of An Garda Síochána e.a.*, C-140/20, EU:C:2022:258, point 84) »[69].

Par un arrêt du 17 novembre 2022, la Cour précise, toujours en matière de conservation de données trafic ou de données de localisation, que « l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, doit être interprété en ce sens qu'il s'oppose à une législation nationale prévoyant, à titre préventif, aux fins de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique, une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation, même si ladite législation limite cette conservation généralisée et indifférenciée à une période de six mois et prévoit un certain nombre de garanties en matière de conservation et d'accès aux données en cause »[70].

C. Directive PNR

En termes de conservation des données PNR, la directive du même nom rappelle que ces données « ne devraient être conservées que pour la durée nécessaire et proportionnée aux objectifs de prévention et de détection des infractions terroristes et des formes graves de criminalité, ainsi que d'enquêtes et de poursuites

[67] *Ibid.*, § 88.
[68] *Ibid.*, § 91.
[69] *Ibid.*, § 113.
[70] CJUE, 17 novembre 2022, *Spetsializirana prokuratura*, C-350/21, § 60.

en la matière »[71]. Cela implique que la conservation de telles données « en application de l'article 12, paragraphe 1, de la directive PNR ne saurait être justifiée en l'absence de rapport objectif entre cette conservation et les objectifs poursuivis par cette directive, à savoir la lutte contre les infractions terroristes et les formes graves de criminalité présentant un lien objectif, à tout le moins indirect, avec le transport aérien des passagers ». En d'autres termes, la conservation d'une durée de 5 ans, subdivisée en deux périodes aux paragraphes 2 et 3 de l'article 12, ne peut viser que le traitement effectué dans le cadre de l'objectif de la directive PNR et à nulle autre finalité.

Par ailleurs et si, selon la Cour, les données PNR doivent être conservées durant la période nécessaire à atteindre la finalité de la directive, une durée excédant la période initiale de 6 mois visée au paragraphe 2 de l'article 12 ne peut cependant être considérée comme conforme au principe de proportionnalité sauf s'il s'agit de « données PNR des passagers ayant donné lieu à une concordance positive vérifiée, qui permettent de considérer que certains passagers pourraient présenter un risque en matière d'infractions terroristes ou de formes graves de criminalité, un stockage de leurs données PNR paraît admissible au-delà de cette période initiale [voir, par analogie, avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, point 207 et jurisprudence citée] »[72].

En conclusion, « dans la mesure où [une législation] paraît prévoir une durée générale de conservation des données PNR de cinq ans, applicable indifféremment à tous les passagers, y compris à ceux pour lesquels ni l'évaluation préalable visée à l'article 6, paragraphe 2, sous a), de la directive PNR, ni les éventuelles vérifications effectuées au cours de la période initiale de six mois, ni aucune autre circonstance n'ont révélé l'existence d'éléments objectifs de nature à établir un risque en matière d'infractions terroristes ou de formes graves de criminalité, cette législation est susceptible de méconnaître l'article 12, paragraphe 1, de cette directive, lu à la lumière des articles 7 et 8 ainsi que de l'article 52, paragraphe 1, de la Charte, à moins qu'elle ne puisse faire l'objet d'une interprétation conforme à ces dispositions, ce qu'il incombe à la juridiction de renvoi de vérifier »[73].

XII. Principes de licéité et de minimisation des données

A. Article 6.1 du RGPD en lien avec le principe de minimisation

Dans son arrêt du 20 octobre 2022 précité concernant la création d'une base de données « de test » qui est riche en rappels et enseignements, la Cour a l'occasion

[71] Considérant 25 de la directive PNR.
[72] CJUE, 21 juin 2022, *Ligue des droits humains c. Conseil des ministres*, C-817/19, précité, § 259.
[73] *Ibid.*, § 261.

de préciser que « tout traitement de données à caractère personnel doit être conforme aux principes relatifs au traitement des données énoncés à l'article 5 dudit règlement et répondre à l'une des conditions relatives à la licéité du traitement énumérées à l'article 6 du même règlement »[74]. Sur base de ce principe, elle rappelle les principes de nécessité et de minimisation des données.

Ainsi, elle précise, d'une part, qu'« il ressort de cet article 6, lorsque la personne concernée n'a pas consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques, conformément à l'article 6, paragraphe 1, sous a), du [RGPD] [que] le traitement doit, ainsi qu'il ressort des points b) à f) dudit paragraphe, répondre à une exigence de nécessité »[75] et, d'autre part, que « une telle exigence de nécessité résulte également du principe de la « minimisation des données », prévu à l'article 5, paragraphe 1, sous c), de ce règlement, aux termes duquel les données à caractère personnel doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées »[76]. Cela permet ainsi d'« assurer un niveau élevé de protection des personnes physiques au sein de l'Union à l'égard du traitement des données à caractère personnel »[77].

B. Article 6.1.c) et e) du RGPD

Dans son second arrêt du 20 octobre 2022 relatif à l'enregistrement d'images dans les bureaux de dépouillement bulgare déjà analysé ci-dessus, la Cour rappelle que les conditions de licéité du traitement de données à caractère personnel sont fixées à l'article 6 du RGPD. Après ce rappel, elle s'attache à la base rendant licite le traitement « nécessaire aux fins de l'exécution d'une mission d'intérêt public ou d'une mission relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement »[78]. Après avoir précisé que l'article 6.1.e) du RGPD doit être lu conjointement avec l'article 6.3 du RGPD, la Cour précise que « les dispositions combinées de l'article 6, paragraphe 1, sous e), du RGPD et de l'article 6, paragraphe 3, de ce règlement permettent donc aux États membres d'adopter des règles sur le fondement desquelles les responsables du traitement peuvent traiter des données à caractère personnel dans le cadre de l'exécution d'une mission d'intérêt public ou d'une mission relevant de l'exercice de l'autorité publique »[79]. Par ailleurs et dès lors que l'article 6.3 du RGPD prescrit que le fondement du traitement « nécessaire aux fins de l'exécution d'une mission d'intérêt public ou d'une mission relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement » visé à l'article 6.1.e) du RGPD est défini par le droit

[74] CJUE, 20 octobre 2022, *Digi Távközlési és Szolgáltató Kft. c. Nemzeti Adatvédelmi és Információszabadság Hatóság*, C-77/21, précité, § 56.
[75] *Ibid.*, § 57.
[76] *Ibid.*, § 58.
[77] *Ibid.*, § 59.
[78] Article 6.1.e) du RGPD.
[79] CJUE, 20 octobre 2022, *Komisia za zashtita na lichnite danni, Tsentralna izbiratelna komisia c. Koalitsia « Demokratichna Bulgaria – Obedinenie »*, C-306/21, précité, § 50.

de l'Union ou le droit de l'État membre auquel le responsable du traitement est soumis[80], le traitement licite de données à caractère personnel par [certains des acteurs présents dans les locaux électoraux lors du dépouillement du scrutin] sur le fondement de l'article 6, paragraphe 1, sous e), du RGPD présuppose non seulement que ceux-ci puissent être considérés comme exécutant une mission d'intérêt publique, mais aussi que les traitements de données à caractère personnel aux fins de l'exécution d'une telle mission reposent sur une base légale visée à l'article 6, paragraphe 3, de ce règlement »[81]. La Cour établit donc deux conditions cumulatives dans l'application de l'article 6.1.e) du RGPD.

Par son arrêt du 8 décembre 2022, la Cour analysant l'articulation entre l'article 6.1.e) (« traitement de données à caractère personnel effectué par une autorité publique dans le cadre de l'exécution de ses missions ») et l'article 6.1 f) (intérêt légitime) a considéré qu'« il ressort clairement du libellé de l'article 6, paragraphe 1, second alinéa, du RGPD qu'un traitement de données à caractère personnel effectué par une autorité publique dans le cadre de l'exécution de ses missions ne peut pas relever du champ d'application de l'article 6, paragraphe 1, premier alinéa, sous f), du RGPD, relatif aux traitements de données à caractère personnel nécessaires aux fins des intérêts légitimes poursuivis par le responsable du traitement. Ainsi qu'il résulte du considérant 47 du RGPD et comme la Commission l'a fait valoir, cette dernière disposition ne saurait s'appliquer à de tels traitements de données, dès lors que la base juridique de ceux-ci doit être prévue par le législateur. Il s'ensuit que, lorsque le traitement effectué par une autorité publique est nécessaire à l'exécution d'une mission d'intérêt public, et que, partant, il relève des missions mentionnées à l'article 6, paragraphe 1, second alinéa, de ce règlement, l'application de l'article 6, paragraphe 1, premier alinéa, sous e), du RGPD et celle de l'article 6, paragraphe 1, premier alinéa, sous f), de celui-ci sont exclusives l'une de l'autre »[82].

Sur base de cette analyse et au terme d'un argumentaire concernant le traitement par le parquet d'un État membre de données – dont le traitement initial tombait dans le champ d'application de la directive 2016/680 – pour assurer la défense de l'État dans le cadre d'un recours en responsabilité, la Cour considère que ce traitement trouve sa base de licéité dans l'article 6.1.e) du RGPD. Elle ajoute que « par ailleurs, il ne saurait être exclu que, lorsque, aux fins d'assurer la défense de l'État dans le cadre d'un recours en responsabilité, le parquet d'un État membre transmet des données à caractère personnel à la juridiction compétente, à la demande de cette dernière, cette transmission soit également susceptible de relever du champ d'application de l'article 6, paragraphe 1, premier alinéa, sous c), du RGPD, lorsque, en vertu du droit national applicable, ledit parquet est tenu de donner suite à une telle demande »[83].

[80] *Ibid.*, § 52.
[81] *Ibid.*
[82] CJUE, 8 décembre 2022, *VS c. Inspektor v Inspektorata kam Visshia sadeben savet*, C-180/21, précité, § 85.
[83] *Ibid.*, § 94.

Dans l'arrêt du 1er août 2022 déjà repris ci-dessus, la Cour analyse également la compatibilité de la loi lituanienne sur la conciliation des intérêts avec l'article 6.1. c) et e) du RGPD et, plus précisément, la publication des informations figurant dans la déclaration d'intérêts privés sur le site Internet de la Haute commission (et non pas la déclaration elle-même). La Cour examine donc si l'article 6 du RGPD, lu à la lumière des articles 7 et 8 de la Charte, s'oppose « à la publication sur Internet d'une partie des données à caractère personnel figurant dans la déclaration d'intérêts privés qu'est tenu de déposer tout directeur d'un établissement percevant des fonds publics, telle que celle prévue à l'article 10 de la loi sur la conciliation des intérêts »[84]. La Cour analyse de manière plus particulière les points c) et e) de l'article 6.1 du RGPD.

Après avoir rappelé que « les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel, garantis aux articles 7 et 8 de la Charte, ne sont pas des prérogatives absolues, mais doivent être pris en considération par rapport à leur fonction dans la société et être mis en balance avec d'autres droits fondamentaux. Des limitations peuvent ainsi être apportées, pourvu que, conformément à l'article 52, paragraphe 1, de la Charte, elles soient prévues par la loi et qu'elles respectent le contenu essentiel des droits fondamentaux ainsi que le principe de proportionnalité. En vertu de ce dernier principe, des limitations ne peuvent être apportées que si elles sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et des libertés d'autrui. Elles doivent s'opérer dans les limites du strict nécessaire et la réglementation comportant l'ingérence doit prévoir des règles claires et précises régissant la portée et l'application de la mesure en cause [arrêt du 22 juin 2021, *Latvijas Republikas Saeima (Points de pénalité)*, C-439/19, EU:C:2021:504, point 105 et jurisprudence citée] »[85]. En l'espèce, la publication des informations reprises dans la déclaration d'intérêts est nécessaire au respect d'une obligation à laquelle est tenue la Haute commission et « l'ingérence qui en résulte doit être regardée comme étant prévue par la loi, au sens de l'article 52, paragraphe 1, de la Charte [voir, en ce sens, arrêt du 24 février 2022, *Valsts ieņēmumu dienests (Traitement des données personnelles à des fins fiscales)*, C-175/20, EU:C:2022:124, point 54] »[86]. Cette obligation légale, à savoir l'article 10 de la loi lituanienne sur la conciliation des intérêts, répond aux conditions fixées par l'article 52.1 de la Charte des droits fondamentaux de l'Union européenne[87] et de l'article 6.3 du RGPD parmi lesquelles figure l'exigence d'un « objectif d'intérêt public et de proportionnalité à l'objectif légitime poursuivi »[88].

---

[84] CJUE, 1er août 2022, *OT c. Vyriausioji tarnybinės etikos komisija*, C-184/20, précité, § 66.
[85] *Ibid.*, § 70.
[86] *Ibid.*, § 72.
[87] « Toute limitation de l'exercice des droits et libertés reconnus par la présente Charte doit être prévue par la loi et respecter le contenu essentiel desdits droits et libertés. Dans le respect du principe de proportionnalité, des limitations ne peuvent être apportées que si elles sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui ».
[88] CJUE, 1er août 2022, *OT c. Vyriausioji tarnybinės etikos komisija*, C-184/20, précité, § 73.

En l'espèce, la Cour relève que la loi lituanienne sur la conciliation des intérêts « vise à assurer la prévalence de l'intérêt public lors de la prise de décisions par les personnes travaillant dans le service public, à garantir l'impartialité de ces décisions et à prévenir les situations de conflits d'intérêts ainsi que l'apparition et l'essor de la corruption dans le service public. De tels objectifs, en ce qu'ils consistent à renforcer les garanties de probité et d'impartialité des décideurs du secteur public, à prévenir les conflits d'intérêts et à lutter contre la corruption dans le secteur public, sont incontestablement d'intérêt public et, par suite, légitimes. En effet, veiller à ce que les décideurs du secteur public exercent leurs fonctions de manière impartiale et objective, et éviter qu'ils soient influencés par des considérations tenant à des intérêts privés visent à garantir la bonne gestion des affaires publiques et des biens publics. En outre, la lutte contre la corruption constitue un objectif auquel les États membres ont souscrit tant au niveau international qu'au niveau de l'Union »[89]. Il y a cependant lieu de s'interroger sur la question de la proportionnalité d'une telle publication.

En d'autres termes, « s'agissant, ensuite, de l'exigence de nécessité, il ressort du considérant 39 du RGPD que celle-ci est remplie lorsque l'objectif d'intérêt général visé ne peut raisonnablement être atteint de manière aussi efficace par d'autres moyens moins attentatoires aux droits fondamentaux des personnes concernées, en particulier aux droits au respect de la vie privée et à la protection des données à caractère personnel garantis aux articles 7 et 8 de la Charte, les dérogations et les restrictions au principe de la protection de telles données devant s'opérer dans les limites du strict nécessaire [voir, en ce sens, arrêt du 22 juin 2021, *Latvijas Republikas Saeima (Points de pénalité)*, C-439/19, EU:C:2021:504, point 110 et jurisprudence citée] »[90]. La Cour précise que « cette appréciation doit être effectuée en tenant compte de l'ensemble des éléments de droit et de fait propres à l'État membre concerné, tels que l'existence d'autres mesures destinées à prévenir les conflits d'intérêts et à lutter contre la corruption, l'ampleur de tels conflits et du phénomène de corruption au sein du service public, ainsi que de la nature des informations en cause et de l'importance des fonctions exercées par le déclarant, notamment sa position hiérarchique, l'étendue des compétences d'administration publique dont il est éventuellement investi et les pouvoirs dont il dispose en matière d'engagement et de gestion de fonds publics »[91]. Au regard de ce critère, la Cour considère que « le manque de ressources allouées aux autorités publiques ne saurait en aucun cas constituer un motif légitime permettant de justifier une atteinte aux droits fondamentaux garantis par la Charte »[92].

Par ailleurs et « si, dans un objectif de prévention des conflits d'intérêts et de la corruption dans le secteur public, il peut être pertinent d'exiger que figurent, dans les déclarations d'intérêts privés, des informations permettant d'identifier la personne du déclarant ainsi que des informations relatives aux activités

[89] *Ibid.*, §§ 74-77 ; voy. égal. CJUE, 24 février, 2022, *« SS » SIA c. Valsts ieņēmumu dienests*, C-175/20, §§ 48 et s.
[90] CJUE, 1er août 2022, *OT c. Vyriausioji tarnybinės etikos komisija*, C-184/20, précité, § 85.
[91] *Ibid.*, § 86.
[92] *Ibid.*, § 89.

du conjoint, concubin ou partenaire du déclarant, la divulgation publique, en ligne, de données nominatives relatives au conjoint, concubin ou partenaire d'un directeur d'un établissement percevant des fonds publics ainsi qu'aux proches ou autres personnes connues de celui-ci susceptibles de donner lieu à un conflit d'intérêts paraît aller au-delà de ce qui est strictement nécessaire »[93]. Il est intéressant d'à nouveau relever le fait que la Cour porte une attention particulière sur la publication des données à caractère personnel[94].

En conclusion, « l'article 6, paragraphe 1, premier alinéa, sous c), et paragraphe 3, du RGPD, lus à la lumière des articles 7, 8 et 52, paragraphe 1, de la Charte, doivent être interprétés en ce sens qu'ils s'opposent à une législation nationale prévoyant la publication en ligne de la déclaration d'intérêts privés que tout directeur d'un établissement percevant des fonds publics est tenu de déposer, en tant, notamment, que cette publication porte sur des données nominatives relatives à son conjoint, concubin ou partenaire ainsi qu'aux personnes proches ou connues du déclarant susceptibles de donner lieu à un conflit d'intérêts, ou encore sur toute transaction conclue au cours des douze derniers mois civils dont la valeur excède 3.000 euros »[95].

XIII. Principe de minimisation

S'agissant du principe de minimisation, une société gérant un site Internet reprenant des annonces de vente de véhicules s'opposait à la communication de données telles que la marque, le modèle, le numéro de châssis et le prix du véhicule, ainsi que le numéro de téléphone du vendeur qui devaient communiquées par voie électronique et dans un format permettant leur filtrage ou sélection vers l'administration fiscale lettone au motif que la collecte était contraire aux principes du RGPD. Ainsi, la société considérait que les données dont la communication était demandée par l'administration étaient excessives[96].

Sur question préjudicielle d'une cour administrative régionale lettone, la Cour rappelle que tout traitement au sens du RGPD doit, « sous réserve des dérogations admises à l'article 23 du [RGPD], respecter les principes relatifs au traitement des données à caractère personnel énoncés à l'article 5 de ce règlement ainsi que les droits de la personne concernée figurant aux articles 12 à 22 de celui-ci »[97]. Parmi ces principes figure celui de la proportionnalité, appelé également minimisation, en vertu duquel « le responsable du traitement est également tenu de limiter au strict nécessaire, à l'aune de l'objectif du traitement envisagé, la période de collecte des données à caractère personnel en cause »[98].

---

[93] *Ibid.*, § 96.
[94] Pour une analyse approfondie, voy. F. Jacques, « Protection des données à caractère personnel : la Cour de justice a-t-elle transformé le RGPD en un instrument d'une sensibilité extrême ? », *op. cit.*
[95] *Ibid.*, § 116.
[96] CJUE, 24 février 2022, *« SS » SIA c. Valsts ieņēmumu dienests*, C-175/20, précité.
[97] *Ibid.*, § 61.
[98] *Ibid.*, § 79.

Par ailleurs, toute réglementation sur laquelle se fonde un traitement de données à caractère personnel « doit prévoir [pour satisfaire à l'exigence de proportionnalité] des règles claires et précises régissant la portée et l'application de la mesure en cause et imposant des exigences minimales, de telle sorte que les personnes dont les données à caractère personnel sont concernées disposent de garanties suffisantes permettant de protéger efficacement ces données contre les risques d'abus. Cette réglementation doit être légalement contraignante en droit interne et, en particulier, indiquer en quelles circonstances et sous quelles conditions une mesure prévoyant le traitement de telles données peut être prise, garantissant ainsi que l'ingérence soit limitée au strict nécessaire (arrêt du 6 octobre 2020, *Privacy International*, C-623/17, EU:C:2020:790, point 68 et jurisprudence citée) »[99].

En conclusion, la Cour considère que « les dispositions du règlement 2016/679 [RGPD] doivent être interprétées en ce sens qu'elles ne s'opposent pas à ce que l'administration fiscale d'un État membre impose à un prestataire de services d'annonces publiées sur Internet de lui communiquer des informations relatives aux contribuables ayant publié des annonces dans l'une des rubriques de son portail Internet pour autant, notamment, que ces données soient nécessaires au regard des finalités spécifiques pour lesquelles elles sont collectées et que la période sur laquelle porte la collecte desdites données n'excède pas la durée strictement nécessaire pour atteindre l'objectif d'intérêt général visé »[100].

XIV. Accès aux données par les autorités publiques

Dans l'arrêt du 17 novembre 2022 précité relatif à la directive 2002/58, la Cour a rappelé que « s'il appartient au droit national de déterminer les conditions dans lesquelles [un accès aux données relatives au trafic et aux données de localisation concernant les appels par téléphones mobiles de cinq personnes impliquées dans une activité criminelle] doit être accordé, une législation nationale doit, pour satisfaire à l'exigence de proportionnalité, prévoir des règles claires et précises régissant la portée et l'application de la mesure en cause et imposant des exigences minimales, de telle sorte que les personnes dont les données à caractère personnel sont concernées disposent de garanties suffisantes permettant de protéger efficacement ces données contre les risques d'abus. En particulier, une législation nationale régissant l'accès des autorités compétentes à des données relatives au trafic et à des données de localisation conservées, adoptée au titre de l'article 15, paragraphe 1, de la directive 2002/58, ne saurait se limiter à exiger que l'accès des autorités aux données réponde à la finalité poursuivie par cette législation, mais elle doit également prévoir les conditions matérielles et procédurales régissant cette utilisation (voir, en ce sens, arrêt du 5 avril 2022, *Commissioner*

[99] *Ibid.*, § 83 ; voy. égal. Trib. UE, *Leon Leonard Johan Veen c. Agence de l'Union européenne pour la coopération des services répressifs (Europol)*, T-436/21, § 46.
[100] CJUE, 24 février, 2022, *« SS » SIA c. Valsts ieņēmumu dienests*, C-175/20, précité, § 85.

of An Garda Síochána e.a., C-140/20, EU:C:2022:258, points 103 et 104 ainsi que jurisprudence citée) »[101].

Elle conclut en précisant donc que « l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, doit être interprété en ce sens qu'il s'oppose à une législation nationale ne prévoyant pas, de manière claire et précise, que l'accès aux données conservées est limité à ce qui est strictement nécessaire pour atteindre l'objectif poursuivi par cette conservation »[102].

XV. Droit de la personne concernée

A. Représentation des personnes concernées par une association à but non lucratif

Dans le cadre d'un litige porté contre Meta Platform Ireland par une association ayant qualité, en vertu de la législation allemande relative aux actions en cessation, la Cour a été interrogée, par question préjudicielle, sur la question de la représentation des personnes concernées telle que visée à l'article 80 du RGPD. La Cour rappelle, en préambule[103], que l'article 80 du RGPD vise deux situations distinctes, à savoir une première étant la personne concernée qui mandate « un organisme, une organisation ou une association à but non lucratif, qui a été valablement constitué conformément au droit d'un État membre »[104] et celle d'« un organisme, une organisation ou une association à but non lucratif, qui a été valablement constitué conformément au droit d'un État membre » qui agit sans mandat d'une personne concernée. La cour rappelle cependant que « des dispositions [du RGPD] ouvrent la possibilité pour les États membres de prévoir des règles nationales supplémentaires, plus strictes ou dérogatoires, qui laissent à ceux-ci une marge d'appréciation sur la manière dont ces dispositions peuvent être mises en œuvre ("clauses d'ouverture") »[105]. Il en va ainsi que l'article 80 du RGPD qui offre une possibilité de marge d'appréciation aux États membres. Ces derniers doivent cependant l'utiliser « dans les conditions et les limites prévues par les dispositions du RGPD et doivent ainsi légiférer de manière à ne pas porter atteinte au contenu et aux objectifs de ce règlement »[106].

Au terme de son analyse, entre autres du droit allemand en matière de représentation de consommateur et après avoir précisé que « la violation d'une règle relative à la protection des données à caractère personnel peut simultanément

[101] CJUE, 17 novembre 2022, *Spetsializirana prokuratura*, C-350/21, précité, § 60.
[102] *Ibid.*, § 67.
[103] CJUE, 28 avril 2022, *Meta Platforms Ireland Limited, anciennement Facebook Ireland Limited c. Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V.*, C-319/20, précité, § 49.
[104] Article 80.1 du RGPD.
[105] CJUE, 28 avril 2022, *Meta Platforms Ireland Limited, anciennement Facebook Ireland Limited c. Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V.*, C-319/20, précité, § 57.
[106] *Ibid.*, § 60 ; voy. égal. la partie dédiée à l'effet immédiat du RGPD.

entraîner la violation de règles relatives à la protection des consommateurs ou aux pratiques commerciales déloyales »[107], la Cour considère que « l'article 80, paragraphe 2, du RGPD doit être interprété en ce sens qu'il ne s'oppose pas à une réglementation nationale qui permet à une association de défense des intérêts des consommateurs d'agir en justice, en l'absence d'un mandat qui lui a été conféré à cette fin et indépendamment de la violation de droits concrets des personnes concernées, contre l'auteur présumé d'une atteinte à la protection des données à caractère personnel, en invoquant la violation de l'interdiction des pratiques commerciales déloyales, d'une loi en matière de protection des consommateurs ou de l'interdiction de l'utilisation de conditions générales nulles, dès lors que le traitement de données concerné est susceptible d'affecter les droits que des personnes physiques identifiées ou identifiables tirent de ce règlement »[108].

B. Droit à l'information

Dans le cadre de la directive (UE) 2016/680[109], la Cour s'est attachée au droit à l'information dans le chef des personnes concernées « lorsque cette information ne fait pas obstacle à la procédure pénale et disposent d'une voie de recours à l'encontre d'un accès illégal »[110] et, plus particulièrement dans le cadre de l'utilisation des données par les autorités compétentes en matière pénale. La Cour a relevé que l'article 13 de la directive 2016/680 confirme que « si les États membres peuvent adopter des mesures législatives visant à retarder, à limiter ou même à supprimer la fourniture des informations à la personne concernée, pour autant qu'une telle mesure soit conforme aux exigences énoncées au paragraphe 3 de cet article[111], une réglementation nationale qui exclurait, de manière générale, tout droit à l'information ne serait pas conforme au droit de l'Union »[112].

C. Droit de recours

Dans la directive 2016/680, l'article 54 prescrit le droit à un recours effectif au profit de la personne concernée et « 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, en vertu du principe d'autonomie procédurale, de régler

---

[107] *Ibid.*, § 78 ; voy. égal. le § 66.
[108] *Ibid.*, § 83.
[109] Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil.
[110] CJUE, 17 novembre 2022, *Spetsializirana prokuratura*, C-350/21, précité, § 68.
[111] « Les États membres peuvent adopter des mesures législatives visant à retarder ou limiter la fourniture des informations à la personne concernée en application du paragraphe 2, ou à ne pas fournir ces informations, dès lors et aussi longtemps qu'une mesure de cette nature constitue une mesure nécessaire et proportionnée dans une société démocratique, en tenant dûment compte des droits fondamentaux et des intérêts légitimes de la personne physique concernée pour : a) éviter de gêner des enquêtes, des recherches ou des procédures officielles ou judiciaires ; b) éviter de nuire à la prévention ou à la détection d'infractions pénales, aux enquêtes ou aux poursuites en la matière ou à l'exécution de sanctions pénales ; c) protéger la sécurité publique ; d) protéger la sécurité nationale ; e) protéger les droits et libertés d'autrui » (article 13.3 directive police).
[112] CJUE, 17 novembre 2022, *Spetsializirana prokuratura*, C-350/21, précité, § 71.

les modalités procédurales des recours en justice destinés à assurer la sauvegarde des droits que les justiciables tirent du droit de l'Union, à condition toutefois qu'elles ne soient pas 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) [arrêts du 6 octobre 2020, *La Quadrature du Net e.a.*, C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 223 ainsi que jurisprudence citée, ainsi que du 2 mars 2021, *Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques)*, C-746/18, EU:C:2021:152, point 42] »[113].

La Cour précise, en lien avec ce droit à un recours, que « dans le cas où l'accès aux données conservées requiert une autorisation délivrée par une juridiction nationale, le principe d'effectivité ne semble pas être respecté. En effet [...], une telle autorisation ne suffit pas, en tant que telle, à assurer la protection effective des personnes concernées contre les risques d'abus et d'accès illicite aux données qui les concernent lorsque, comme en l'occurrence, la réglementation nationale en cause prévoit que cette autorisation est octroyée sur le seul fondement d'une demande formée par les autorités nationales compétentes en matière d'enquêtes pénales, sans que les personnes concernées aient été entendues et, partant, sans que la juridiction compétente pour délivrer une telle autorisation ait été en mesure de prendre en compte les possibles objections de ces personnes »[114]. En effet, cette situation pourrait aboutir à ce que la personne concernée ne dispose pas d'une voie de recours à l'encontre d'un accès illégal aux données.

D. Droit à l'effacement

1. *Principe général*

La Cour est saisie d'une question préjudicielle posée dans le cadre d'un litige relatif à l'inscription d'un abonné d'un opérateur de service téléphonique, Telenet en l'espèce, dans l'annuaire d'un fournisseur d'annuaires, Proximus en l'occurrence, après transmission des données par la première à la seconde. Ledit abonné fait valoir son droit à l'effacement auprès de Proximus qui, à la réception de la demande, modifie le statut de l'abonné afin que les données le concernant ne soient plus rendues publiques. Cependant, lors d'une mise à jour périodique de ses abonnés, Telenet communique les nouvelles données concernant l'abonné sans qu'elles ne soient renseignées comme confidentielles. L'abonné, constatant que les données le concernant sont à nouveau accessibles au public, demande, une nouvelle fois, à Proximus de ne pas reprendre les données dans l'annuaire. Cette dernière lui confirme avoir supprimé l'accès au public et de l'avoir signalé tant à Google qu'aux autres fournisseurs d'annuaires auxquels elle avait transmis les

[113] *Ibid.*, § 74.
[114] *Ibid.*, § 75.

données. Nonobstant cela, l'abonné a porté plainte auprès de l'Autorité de protection des données belges.

Selon la Cour et, outre le fait que, le fournisseur d'annuaires comme Proximus « doit mettre en œuvre des mesures techniques et organisationnelles appropriées pour informer les autres fournisseurs d'annuaires auxquels il a fourni de telles données du retrait du consentement de la personne concernée qui lui a été adressé »[115], il « doit également veiller à informer l'opérateur de services téléphoniques qui lui a communiqué ces données à caractère personnel afin que ce dernier adapte la liste des données personnelles qu'il transmet automatiquement à ce fournisseur d'annuaires et isole les données de ses abonnés qui ont manifesté leur volonté de retirer leur consentement à ce que ces données soient rendues publiques »[116].

En effet, « l'absence d'une telle obligation d'information pour le responsable du traitement sur le retrait du consentement de la personne concernée pourrait rendre le retrait du consentement particulièrement difficile, dès lors que cette personne pourrait se croire tenue de s'adresser à chacun des opérateurs. Une telle approche serait ainsi contraire à l'article 7, paragraphe 3, du RGPD, selon lequel il doit être aussi simple de retirer que de donner son consentement au traitement de données à caractère personnel »[117]. Il convient de relever, en outre, que cette information doit également être effectuée à l'égard des fournisseurs de moteurs de recherche par des mesures raisonnables dont l'appréciation doit tenir compte « de la technologie disponible et les coûts de mise en œuvre »[118] ; « cette appréciation incombant principalement à l'autorité compétente en la matière et pouvant faire l'objet d'un contrôle juridictionnel »[119].

2. *Exception*

En matière de référencement sur des moteurs de recherche, la Cour a, dans son arrêt du 8 décembre 2022, traité de l'article 17.3 du RGPD relatif aux exceptions au droit à l'effacement prévu à l'article 17.1 et 2 du règlement et, plus particulièrement, l'exception liée à « l'exercice du droit à la liberté d'expression et d'information »[120].

En préambule, elle relève que cette exception « constitue une expression du fait que le droit à la protection des données à caractère personnel n'est pas un droit absolu, mais doit, ainsi que le souligne le considérant 4 du RGPD, 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 [voir, en ce

115 CJUE, 20 octobre 2022, *Proximus c. Gegevensbeschermingsautoriteit*, C-129/21, précité, § 83.
116 *Ibid*.
117 *Ibid*., § 87.
118 Article 17.2 du RGPD.
119 CJUE, 20 octobre 2022, *Proximus c. Gegevensbeschermingsautoriteit*, C-129/21, précité, § 96.
120 Article 17.3.a) du RGPD.

sens, arrêt du 24 septembre 2019, *GC e.a. (Déréférencement de données sensibles)*, C-136/17, EU:C:2019:773, point 57 ainsi que jurisprudence citée] »[121]. Elle précise ainsi que « le RGPD, et notamment son article 17, paragraphe 3, sous a), consacre ainsi explicitement l'exigence d'une mise en balance entre, d'une part, les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel, consacrés aux articles 7 et 8 de la Charte, et, d'autre part, le droit fondamental à la liberté d'information, garanti à l'article 11 de la Charte [arrêt du 24 septembre 2019, *GC e.a. (Déréférencement de données sensibles)*, C-136/17, EU:C:2019:773, point 59] »[122].

Ensuite, elle opère une comparaison avec la Convention européenne des droits de l'homme et la jurisprudence de la Cour européenne des droits de l'homme en relevant que « s'agissant de la publication de données, aux fins d'effectuer la mise en balance entre le droit au respect de la vie privée et le droit à la liberté d'expression et d'information, un certain nombre de critères pertinents doivent être pris en considération, tels que la contribution à un débat d'intérêt général, la notoriété de la personne visée, l'objet du reportage, le comportement antérieur de la personne concernée, le contenu, la forme et les répercussions de la publication, le mode et les circonstances dans lesquelles les informations ont été obtenues ainsi que leur véracité (voir, en ce sens, Cour EDH, 27 juin 2017, *Satakunnan Markkinapörssi Oy et Satamedia Oy c. Finlande*, CE:ECHR:2017:0627JUD000093113, § 165) »[123].

Revenant au niveau de l'exception du droit à l'effacement en cas de traitement nécessaire à l'exercice du droit à la liberté d'expression et d'information, elle opère une différenciation entre différents statuts de la personne concernée. Ainsi, « lorsque la personne concernée joue un rôle dans la vie publique, cette personne doit faire preuve d'un degré de tolérance accru, dès lors qu'elle est inévitablement et en pleine connaissance de cause exposée au regard du public (voir, en ce sens, Cour EDH, 6 octobre 2022, *Khural et Zeynalov c. Azerbaijan*, CE:ECHR:2022:1006JUD005506911, § 41 et jurisprudence citée) »[124]. Outre cela, « la question du caractère exact ou non du contenu référencé constitue également un élément pertinent dans le cadre de l'appréciation des conditions d'application prévues à l'article 17, paragraphe 3, sous a), du RGPD, en vue d'apprécier si le droit à l'information des internautes et la liberté d'expression du fournisseur de contenu peuvent prévaloir sur les droits du demandeur de déréférencement »[125].

Reprenant les conclusions de l'avocat général, la Cour précise que « si, dans certaines circonstances, le droit à la liberté d'expression et d'information peut prévaloir sur les droits à la protection de la vie privée et à la protection des données à caractère personnel, notamment lorsque la personne concernée joue un rôle dans la vie publique, ce rapport s'inverse en tout état de cause lorsque, à

[121] CJUE, 8 décembre 2022, *TU et RE c. Google LLC*, C-460/20, précité, § 56.
[122] *Ibid.*, § 57.
[123] *Ibid.*, § 58.
[124] *Ibid.*, § 63.
[125] *Ibid.*, § 64.

tout le moins, une partie des informations visées par la demande de déréférencement ne présentant pas un caractère mineur au regard de l'ensemble du contenu se révèlent inexactes. En effet, dans une telle hypothèse, le droit d'informer et le droit d'être informé ne sauraient être pris en compte, car ils ne peuvent inclure le droit de diffuser de telles informations et d'y avoir accès »[126].

Au niveau d'un moteur de recherche, « dans le cas où la personne ayant introduit une demande de déréférencement présente des éléments de preuve pertinents et suffisants, aptes à étayer sa demande et établissant le caractère manifestement inexact des informations figurant dans le contenu référencé ou, à tout le moins, d'une partie de ces informations qui ne présente pas un caractère mineur au regard de l'ensemble de ce contenu, l'exploitant du moteur de recherche est tenu de faire droit à cette demande de déréférencement. Il en va de même lorsque la personne concernée présente une décision de justice prise contre l'éditeur du site Internet et qui repose sur le constat que des informations figurant dans le contenu référencé, qui ne présentent pas un caractère mineur au regard de l'ensemble de celui-ci, sont, au moins à première vue, inexactes »[127].

La charge de la preuve reposant sur les épaules de la personne concernée ne peut cependant être excessive. Ainsi, « il lui incombe uniquement de fournir les éléments de preuve qu'il peut être, compte tenu des circonstances du cas d'espèce, raisonnablement exigé de celle-ci de rechercher en vue d'établir cette inexactitude manifeste. À cet égard, cette personne ne saurait être tenue, en principe, de produire, dès le stade précontentieux, à l'appui de sa demande de déréférencement auprès de l'exploitant du moteur de recherche, une décision juridictionnelle obtenue contre l'éditeur du site Internet en cause, même sous la forme d'une décision prise en référé. En effet, imposer une telle obligation à ladite personne aurait pour effet de faire peser sur celle-ci une charge déraisonnable »[128].

D'un autre côté, « il ne saurait être imposé à l'exploitant du moteur de recherche concerné une obligation d'enquêter sur les faits et, à cette fin, d'organiser un échange contradictoire avec le fournisseur de contenu visant à obtenir des éléments manquants concernant l'exactitude du contenu référencé. En effet, en ce qu'elle contraindrait l'exploitant du moteur de recherche à contribuer à établir lui-même le caractère exact ou non du contenu référencé, une telle obligation ferait peser sur cet exploitant une charge dépassant ce qui peut raisonnablement être attendu de lui au regard de ses responsabilités, compétences et possibilités, au sens de la jurisprudence rappelée au point 53 [de l'arrêt]. Ladite obligation comporterait ainsi un risque sérieux que des contenus qui répondent à un besoin d'information légitime et prépondérant du public soient déréférencés et qu'il devienne ainsi difficile de les trouver sur Internet. À cet égard, il existerait un risque réel d'effet dissuasif sur l'exercice de la liberté d'expression et d'information

[126] *Ibid.*, § 65.
[127] *Ibid.*, § 72.
[128] *Ibid.*, § 68.

si l'exploitant du moteur de recherche procédait à un tel déréférencement de manière quasi systématique, en vue d'éviter d'avoir à supporter la charge d'enquêter sur les faits pertinents pour établir le caractère exact ou non du contenu référencé »[129]. « Toutefois, dans le cas où une procédure administrative ou juridictionnelle portant sur le caractère prétendument inexact d'informations figurant dans un contenu référencé est engagée et où l'existence de cette procédure a été portée à la connaissance de l'exploitant du moteur de recherche concerné, il incombe à cet exploitant, aux fins notamment de donner aux internautes des informations toujours pertinentes et actualisées, d'ajouter, dans les résultats de la recherche, un avertissement portant sur l'existence d'une telle procédure »[130].

En conclusion, « l'article 17, paragraphe 3, sous a), du RGPD doit être interprété en ce sens que, dans le cadre de la mise en balance qu'il convient d'opérer entre les droits visés aux articles 7 et 8 de la Charte, d'une part, et ceux visés à l'article 11 de la Charte, d'autre part, aux fins de l'examen d'une demande de déréférencement adressée à l'exploitant d'un moteur de recherche et tendant à ce que soit supprimé de la liste de résultats d'une recherche le lien menant vers un contenu comportant des allégations que la personne ayant introduit la demande estime inexactes, ce déréférencement n'est pas soumis à la condition que la question de l'exactitude du contenu référencé ait été résolue, au moins à titre provisoire, dans le cadre d'un recours intenté par cette personne contre le fournisseur de contenu »[131].

XVI. Délégué à la protection des données (DPD ou DPO) – licenciement

Dans le cadre d'un litige lié au licenciement par une société privée allemande d'une DPO qui était également « cheffe du service des affaires juridiques »[132] suite à une décision d'externalisation de l'activité interne de conseil juridique et le service de protection des données, la Cour s'est prononcée sur la question de savoir si une législation nationale peut prévoir qu'un DPO ne peut être licencié que pour motif grave. En l'espèce, les juges du fond allemands saisis sur la validité du licenciement de la fonction de DPO ont, en effet, considéré, sur base de la loi fédérale allemande sur la protection des données, qu'un DPO ne pouvait être licencié que pour motif grave.

La Cour rappelle, dans un premier temps, que l'article 38.3 du RGPD prescrit que « le délégué à la protection des données ne peut être relevé de ses fonctions ou pénalisé par le responsable du traitement ou le sous-traitant pour l'exercice de ses missions ». Pour pallier l'absence de précision, par le législateur européen, des termes de « relevé de ses fonctions », « pénalisé » et « pour l'exercice de ses

[129] *Ibid.*, § 71.
[130] *Ibid.*, § 77.
[131] *Ibid.*, § 77.
[132] CJUE, 22 juin 2022, *Leistritz AG c. LH*, C-534/20, § 11.

missions », la Cour va chercher, dans le langage courant, le sens de ces mots pour en conclure que « l'interdiction faite au responsable du traitement ou au sous-traitant de relever un délégué à la protection des données de ses fonctions ou de le pénaliser signifie […] que ce délégué doit être protégé contre toute décision par laquelle il serait mis fin à ses fonctions, par laquelle il subirait un désavantage ou qui constituerait une sanction »[133]. Tel pourrait être le cas dans le cadre de la décision de licenciement prise par la société allemande à l'encontre de sa DPO.

La protection prévue par le RGPD vise à garantir l'indépendance du DPO dans l'exercice de ses missions sans, pour autant, avoir « pour objet de régir globalement les relations de travail entre un responsable du traitement ou un sous-traitant et des membres de son personnel, lesquelles ne sont susceptibles d'être affectées que de manière accessoire, dans la mesure strictement nécessaire à la réalisation de ces objectifs »[134].

Le RGPD « ne s'oppose [cependant] pas à une réglementation nationale prévoyant qu'un responsable du traitement ou un sous-traitant ne peut licencier un délégué à la protection des données qui est membre de son personnel que pour un motif grave, même si le licenciement n'est pas lié à l'exercice des missions de ce délégué, pour autant qu'une telle réglementation ne compromette pas la réalisation des objectifs du RGPD »[135].

À noter également que la Cour précise que la protection prévue pour le DPO est indépendante de la nature de la relation de travail avec le responsable du traitement ou le sous-traitant[136].

XVII. Compétence des autorités de protection des données nationales

L'article 55 du RGPD vise les compétences des autorités de contrôle et précise, en son paragraphe 3, que « les autorités de contrôle ne sont pas compétentes pour contrôler les opérations de traitement effectuées par les juridictions dans l'exercice de leur fonction juridictionnelle ».

Dans une affaire concernant l'accès par un journaliste à un dossier traité par le Conseil d'État hollandais, la Cour considère que « le fait pour une juridiction de mettre à la disposition temporaire de journalistes des pièces issues d'une procédure juridictionnelle, contenant des données à caractère personnel, afin de leur permettre de mieux rendre compte du déroulement de cette procédure relève de l'exercice, par cette juridiction, de sa "fonction juridictionnelle", au sens de [l'article 55.3 du RGPD] »[137].

133 *Ibid.*, § 21.
134 *Ibid.*, § 28.
135 *Ibid.*, § 36.
136 *Ibid.*, § 24.
137 CJUE, 24 mars 2022, *X et Z c. Autoriteit Persoonsgegevens*, C-245/20, § 39.

La Cour a ainsi précisé que « la détermination, eu égard à l'objet et au contexte d'une affaire donnée, des informations issues d'un dossier de procédure juridictionnelle pouvant être fournies à des journalistes dans le but de leur permettre de rendre compte du déroulement de la procédure juridictionnelle ou d'éclairer tel ou tel aspect d'une décision rendue se rattache clairement à l'exercice, par ces juridictions, de leur "fonction juridictionnelle", dont le contrôle par une autorité extérieure serait susceptible de porter atteinte, de manière générale, à l'indépendance du pouvoir judiciaire »[138].

Jean-Marc Van Gyseghem

Directeur adjoint du Centre de Recherches Information,
Droit et Société (www.crids.eu)
Avocat associé au barreau de Bruxelles (www.rawlingsgiles.be)

[138] *Ibid.*, § 38.