



Recueil de la jurisprudence

ARRÊT DE LA COUR (troisième chambre)

11 décembre 2019*

« Renvoi préjudiciel – Protection des personnes physiques à l’égard du traitement des données à caractère personnel – Charte des droits fondamentaux de l’Union européenne – Articles 7 et 8 – Directive 95/46/CE – Article 6, paragraphe 1, sous c), et article 7, sous f) – Légitimation du traitement de données à caractère personnel – Réglementation nationale permettant la vidéosurveillance aux fins d’assurer la sécurité et la protection des personnes, biens et valeurs et la réalisation d’intérêts légitimes, sans le consentement de la personne concernée – Mise en place d’un système de vidéosurveillance dans les parties communes d’un immeuble à usage d’habitation »

Dans l’affaire C-708/18,

ayant pour objet une demande de décision préjudicielle au titre de l’article 267 TFUE, introduite par le Tribunalul București (tribunal de grande instance de Bucarest, Roumanie), par décision du 2 octobre 2018, parvenue à la Cour le 6 novembre 2018, dans la procédure

TK

contre

Asociația de Proprietari bloc M5A-ScaraA,

LA COUR (troisième chambre),

composée de M^{me} A. Prechal (rapporteuse), présidente de chambre, M^{me} L. S. Rossi, MM. J. Malenovský, F. Biltgen et N. Wahl, juges,

avocat général : M. G. Pitruzzella,

greffier : M. A. Calot Escobar,

vu la procédure écrite,

considérant les observations présentées :

- pour le gouvernement roumain, par M. C.-R. Canțăr ainsi que par M^{mes} O.-C. Ichim et A. Wellman, en qualité d’agents,
- pour le gouvernement tchèque, par MM. M. Smolek, J. Vláčil et O. Serdula, en qualité d’agents,
- pour le gouvernement danois, par M. J. Nymann-Lindgren ainsi que par M^{mes} M. Wolff et P. Z. L. Ngo, en qualité d’agents,

* Langue de procédure : le roumain.

- pour l'Irlande, par M^{mes} M. Browne et G. Hodge ainsi que par M. A. Joyce, en qualité d'agents, assistés de M. D. Fenelly, BL,
- pour le gouvernement autrichien, initialement par M. G. Hesse et M^{me} J. Schmoll, puis par M^{me} J. Schmoll, en qualité d'agents,
- pour le gouvernement portugais, par M. L. Inez Fernandes ainsi que par M^{mes} P. Barros da Costa, L. Medeiros, I. Oliveira et M. Cancela Carvalho, en qualité d'agents,
- pour la Commission européenne, par MM. H. Kranenborg et D. Nardi ainsi que par M^{me} L. Nicolae, en qualité d'agents,

vu la décision prise, l'avocat général entendu, de juger l'affaire sans conclusions,

rend le présent

Arrêt

- 1 La demande de décision préjudicielle porte sur l'interprétation de l'article 6, paragraphe 1, sous e), et de l'article 7, sous f), de la directive 95/46/CE du Parlement européen et du Conseil, 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 (JO 1995, L 281, p. 31), ainsi que des articles 8 et 52 de la charte des droits fondamentaux de l'Union européenne (ci-après la « Charte »).
- 2 Cette demande a été présentée dans le cadre d'un litige opposant TK à l'Asociația de Proprietari bloc M5A-Scara A (association des copropriétaires de l'immeuble M5A-escalier A, Roumanie, ci-après l'« association des copropriétaires »), au sujet de la demande de TK d'enjoindre cette association de mettre hors service le système de vidéosurveillance de cet immeuble et de retirer les caméras installées dans des parties communes de celui-ci.

Le cadre juridique

Le droit de l'Union

- 3 La directive 95/46 a été abrogée et remplacée, avec effet au 25 mai 2018, par le règlement (UE) 2016/679 du Parlement européen et du Conseil, du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (JO 2016, L 119, p. 1). Cependant, compte tenu de la date des faits en cause dans le litige au principal, ce dernier demeure régi par les dispositions de cette directive.
- 4 La directive 95/46 avait, selon son article 1^{er}, pour objet la 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, ainsi que l'élimination des obstacles à la libre circulation de ces données.
- 5 L'article 3 de cette directive prévoyait, à son paragraphe 1 :

« La présente directive s'applique au traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier. »

6 Le chapitre II de ladite directive comprenait une section I, intitulée « Principes relatifs à la qualité des données », composée de l'article 6 de cette même directive, qui disposait :

« 1. Les États membres prévoient que les données à caractère personnel doivent être :

- a) traitées loyalement et licitement ;
- b) collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités. Un traitement ultérieur à des fins historiques, statistiques ou scientifiques n'est pas réputé incompatible pour autant que les États membres prévoient des garanties appropriées ;
- c) adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement ;
- d) exactes et, si nécessaire, mises à jour ; toutes les mesures raisonnables doivent être prises pour que les données inexactes ou incomplètes, au regard des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement, soient effacées ou rectifiées ;
- e) conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement. Les États membres prévoient des garanties appropriées pour les données à caractère personnel qui sont conservées au-delà de la période précitée, à des fins historiques, statistiques ou scientifiques.

2. Il incombe au responsable du traitement d'assurer le respect du paragraphe 1. »

7 À la section II de ce chapitre II, intitulée « Principes relatifs à la légitimation des traitements de données », l'article 7 de la directive 95/46 était libellé comme suit :

« Les États membres prévoient que le traitement de données à caractère personnel ne peut être effectué que si :

- a) la personne concernée a indubitablement donné son consentement
ou
- b) il est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci
ou
- c) il est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis
ou
- d) il est nécessaire à la sauvegarde de l'intérêt vital de la personne concernée
ou
- e) il est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, dont est investi le responsable du traitement ou le tiers auquel les données sont communiquées

ou

- f) il est nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le ou les tiers auxquels les données sont communiquées, à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée, qui appellent une protection au titre de l'article 1^{er} paragraphe 1. »

Le droit roumain

- 8 La Legea nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date (loi n° 677/2001 relative à la protection des personnes à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données) (*Monitorul Oficial*, partie I, n° 790 du 12 décembre 2001), telle que modifiée par la loi n° 102/2005 et l'ordonnance d'urgence du gouvernement n° 36/2007, applicable *ratione temporis* au litige au principal, a été adoptée afin de transposer en droit roumain la directive 95/46.
- 9 L'article 5 de cette loi disposait :
- « 1. Tout traitement de données à caractère personnel, sauf s'il vise des données appartenant aux catégories mentionnées à l'article 7, paragraphe 1, et aux articles 8 et 10, peut être effectué uniquement si la personne concernée a expressément et indubitablement donné son consentement à ce traitement.
2. Le consentement de la personne concernée n'est pas requis dans les cas suivants :
- a) lorsque le traitement est nécessaire à l'exécution d'un contrat ou d'un avant-contrat auquel la personne concernée est partie ou à l'adoption de mesures, à la demande de celle-ci, avant la conclusion d'un contrat ou d'un avant-contrat ;
- b) lorsque le traitement est nécessaire à la protection de la vie, de l'intégrité physique ou de la santé de la personne concernée ou d'une autre personne menacée ;
- c) lorsque le traitement est nécessaire au respect d'une obligation légale du responsable du traitement ;
- d) lorsque le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou visant l'exercice des prérogatives de puissance publique dont est investi le responsable du traitement ou le tiers auquel les données sont divulguées ;
- e) lorsque le traitement est nécessaire à la réalisation d'un intérêt légitime du responsable du traitement ou du tiers auquel les données sont divulguées, à condition que cet intérêt ne porte pas atteinte à l'intérêt ou aux droits et libertés fondamentaux de la personne concernée ;
- f) lorsque le traitement concerne des données tirées de documents accessibles au public, conformément à la loi ;
- g) lorsque le traitement est effectué à des fins exclusivement statistiques, de recherche historique ou scientifique, et les données demeurent anonymes tout au long du traitement.
3. Les dispositions du paragraphe 2 sont sans préjudice des dispositions légales régissant l'obligation des autorités publiques de respecter et de protéger la vie intime, familiale et privée. »

10 La décision n° 52/2012 de l’Autoritate Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (Autorité nationale de surveillance du traitement des données à caractère personnel, Roumanie, ci-après l’« ANSPDCP ») concernant le traitement des données à caractère personnel par le recours à des moyens de vidéosurveillance, dans sa version applicable au litige au principal, prévoyait, à son article 1^{er} :

« La collecte, l’enregistrement, le stockage, l’utilisation, la transmission, la divulgation ou toute autre opération de traitement des images par des moyens de vidéosurveillance, qui permettent directement ou indirectement d’identifier des personnes physiques, constituent des opérations de traitement de données à caractère personnel qui entrent dans le champ d’application de la [loi n° 677/2001]. »

11 L’article 4 de cette décision disposait :

« La vidéosurveillance peut principalement être effectuée dans les buts suivants :

- a) la prévention des infractions et la lutte contre celles-ci ;
- b) la surveillance de la circulation routière et la constatation des infractions aux règles de circulation routière ;
- c) la garde et la protection des personnes, des biens et des actifs, des immeubles et des installations d’utilité publique ainsi que de leurs enceintes ;
- d) l’exécution de mesures d’intérêt public ou l’exercice de prérogatives de puissance publique ;
- e) la réalisation d’intérêts légitimes, à condition de ne pas porter atteinte aux droits et libertés fondamentales des personnes concernées. »

12 Aux termes de l’article 5, paragraphes 1 à 3, de ladite décision :

« 1. La vidéosurveillance peut être effectuée dans les lieux et espaces ouverts ou destinés au public, y compris sur les voies publiques d’accès situées sur le domaine public ou privé, dans les conditions prévues par la loi.

2. Les caméras de vidéosurveillance sont installées visiblement.

3. L’utilisation de moyens de vidéosurveillance dissimulés est interdite, sauf dans les cas prévus par la loi. »

13 L’article 6 de la même décision énonçait :

« Le traitement des données à caractère personnel au moyen de systèmes de vidéosurveillance est effectué avec le consentement exprès et indubitable de la personne concernée ou dans les cas visés à l’article 5, paragraphe 2, de la loi n° 677/2001[...] »

Le litige au principal et les questions préjudicielles

14 TK réside dans un appartement, dont il est propriétaire, situé dans l’immeuble M5A. À la demande de certains copropriétaires de cet immeuble, l’association des copropriétaires a, lors d’une assemblée générale qui s’est tenue le 7 avril 2016, adopté une décision approuvant l’installation de caméras de vidéosurveillance dans celui-ci.

- 15 En exécution de cette décision, trois caméras de vidéosurveillance ont été installées dans des parties communes de l'immeuble M5A. La première caméra était orientée vers la façade de l'immeuble, alors que les deuxième et troisième caméras étaient installées, respectivement, dans le hall du rez-de-chaussée et dans l'ascenseur de l'immeuble.
- 16 TK s'est opposé à l'installation de ce système de vidéosurveillance, au motif qu'elle constituait une violation du droit au respect de la vie privée.
- 17 Ayant constaté que, en dépit de ses nombreuses démarches et de la reconnaissance écrite par l'association des copropriétaires de l'illégalité du système de vidéosurveillance mis en place, ce système continuait à fonctionner, TK a saisi la juridiction de renvoi afin d'enjoindre ladite association de retirer les trois caméras et de mettre celles-ci définitivement hors service sous peine de l'imposition d'une astreinte.
- 18 Devant cette juridiction, TK a fait valoir que le système de vidéosurveillance en cause violait le droit primaire et dérivé de l'Union, en particulier le droit au respect de la vie privée, ainsi que le droit national relatif au droit au respect de la vie privée. Il a par ailleurs indiqué que l'association des copropriétaires avait assumé la fonction de responsable du traitement des données à caractère personnel sans avoir suivi la procédure d'enregistrement prévue à cette fin par la loi.
- 19 L'association des copropriétaires a indiqué que la décision d'installer un système de vidéosurveillance avait été prise afin de contrôler aussi efficacement que possible les allées et venues dans l'immeuble, en raison du fait que l'ascenseur avait été vandalisé à de nombreuses reprises et que plusieurs appartements ainsi que les parties communes avaient fait l'objet de cambriolages et de vols.
- 20 Elle a également précisé que d'autres mesures qu'elle avait préalablement prises, à savoir l'installation d'un système d'entrée dans l'immeuble avec interphone et carte magnétique, n'avaient pas empêché la commission répétée d'infractions de même nature.
- 21 L'association des copropriétaires a en outre transmis à TK le procès-verbal qu'elle avait dressé avec la société qui avait installé les caméras du système de vidéosurveillance, indiquant qu'il avait été procédé, le 21 octobre 2016, à l'effacement et à la déconnexion du disque dur du système, que celui-ci avait été mis hors service et que les images enregistrées avaient été supprimées.
- 22 Elle lui a également communiqué un autre procès-verbal, daté du 18 mai 2017, duquel il ressort que les trois caméras de vidéosurveillance avaient été désinstallées. Ce procès-verbal précisait que l'association des copropriétaires avait, dans l'intervalle, accompli la procédure lui permettant d'être enregistrée en tant que responsable du traitement de données à caractère personnel.
- 23 TK a toutefois fait observer devant la juridiction de renvoi que les trois caméras de vidéosurveillance étaient toujours en place.
- 24 La juridiction de renvoi relève que l'article 5 de la loi n° 677/2001 prévoit, d'une manière générale, qu'un traitement de données à caractère personnel, tel que l'enregistrement d'images au moyen d'un système de vidéosurveillance, ne peut être effectué que si la personne concernée a expressément et indubitablement donné son consentement. Le paragraphe 2 du même article énoncerait toutefois une série d'exceptions à cette règle, au nombre desquelles figure celle selon laquelle le traitement de données à caractère personnel est nécessaire à la protection de la vie, de l'intégrité physique ou de la santé de la personne concernée ou d'une autre personne menacée. La décision n° 52/2012 de l'ANSPDCP prévoirait une exception de même nature.
- 25 La juridiction de renvoi se réfère ensuite, notamment, à l'article 52, paragraphe 1, de la Charte consacrant le principe selon lequel il doit exister un rapport de proportionnalité entre le but poursuivi par l'ingérence dans les droits et libertés des citoyens et les moyens utilisés.

- 26 Or, selon cette juridiction, le système de vidéosurveillance en cause devant elle ne semble pas avoir été utilisé d'une manière ou dans un but qui ne correspondait pas à l'objectif déclaré par l'association des copropriétaires, à savoir celui de protéger la vie, l'intégrité physique et la santé des personnes concernées, soit les copropriétaires de l'immeuble dans lequel ce système a été installé.
- 27 Dans ces conditions, le Tribunalul București (tribunal de grande instance de Bucarest, Roumanie) a décidé de surseoir à statuer et de poser à la Cour les questions préjudicielles suivantes :
- « 1) Les articles 8 et 52 de la Charte ainsi que l'article 7, sous f), de la directive 95/46 doivent-ils être interprétés en ce sens qu'ils s'opposent à des dispositions nationales telles que celles en cause en l'espèce, à savoir l'article 5, paragraphe 2, de la [loi n° 677/2001] et l'article 6 de la [décision n° 52/2012 de l'ANSPDCP], qui autorisent la mise en place d'une vidéosurveillance pour assurer la garde et la protection des personnes, des biens et des actifs et pour la réalisation d'intérêts légitimes, sans le consentement de la personne concernée ?
- 2) Les articles 8 et 52 de la Charte doivent-ils être interprétés en ce sens que la limitation des droits et des libertés engendrée par la vidéosurveillance respecte le principe de proportionnalité ainsi que l'exigence d'être "nécessaire" et de "répondre à des objectifs d'intérêt général ou au besoin de protection des droits et libertés d'autrui", lorsque le responsable du traitement a la possibilité de prendre d'autres mesures pour protéger l'intérêt légitime poursuivi ?
- 3) L'article 7, sous f), de la directive 95/46 doit-il être interprété en ce sens que l'"intérêt légitime" du responsable du traitement doit être prouvé et être né et actuel au moment du traitement ?
- 4) L'article 6, paragraphe 1, sous e), de la directive 95/46 doit-il être interprété en ce sens qu'un traitement (vidéosurveillance) est excessif ou n'est pas adéquat, lorsque le responsable du traitement a la possibilité de prendre d'autres mesures pour protéger l'intérêt légitime poursuivi ? »

Sur les questions préjudicielles

- 28 À titre liminaire, il y a lieu de constater, en premier lieu, que, si la juridiction de renvoi se réfère, par sa quatrième question, à l'article 6, paragraphe 1, sous e), de la directive 95/46, elle ne fournit aucune explication quant à la pertinence de cette disposition aux fins de la solution du litige en cause au principal.
- 29 En effet, ladite disposition concerne uniquement les exigences auxquelles doit répondre la conservation de données à caractère personnel. Or, rien dans le dossier dont dispose la Cour ne permet de considérer que le litige au principal porte sur cet aspect.
- 30 En revanche, dans la mesure où, par cette question, la juridiction de renvoi demande, en substance, si la mise en place d'un système de vidéosurveillance, tel que celui en cause devant elle, est proportionnée aux buts poursuivis, il convient de relever que la question de savoir si les données à caractère personnel collectées par ce système répondent à l'exigence de proportionnalité se rapporte à l'interprétation de l'article 6, paragraphe 1, sous c), de la directive 95/46.
- 31 Or, cette dernière disposition doit être prise en compte lors de la vérification de la deuxième condition d'application posée à l'article 7, sous f), de la directive 95/46, selon laquelle le traitement des données à caractère personnel doit être « nécessaire » à la réalisation de l'intérêt légitime poursuivi.
- 32 En second lieu, par ses première et deuxième questions, la juridiction de renvoi se réfère aux articles 8 et 52 de la Charte, pris de manière isolée ou lus en combinaison avec l'article 7, sous f), de la directive 95/46. Or, la Cour a déjà précisé que l'appréciation de la condition posée à cette disposition, relative à

l'existence de droits et de libertés fondamentaux de la personne concernée par la protection des données qui prévaudraient sur l'intérêt légitime poursuivi par le responsable du traitement des données ou par le ou les tiers auxquels les données sont communiquées, nécessite qu'il soit procédé à une pondération des droits et des intérêts opposés en cause en fonction des circonstances concrètes du cas particulier concerné, dans le cadre de laquelle il doit être tenu compte de l'importance des droits de la personne concernée résultant des articles 7 et 8 de la Charte (arrêt du 24 novembre 2011, Asociación Nacional de Establecimientos Financieros de Crédito, C-468/10 et C-469/10, EU:C:2011:777, point 40). Il s'ensuit que ces articles 8 et 52 ne doivent pas, en l'occurrence, être appliqués de manière isolée.

- 33 Au vu de ce qui précède, il y a lieu de considérer que, par ses questions, qu'il convient d'examiner ensemble, la juridiction de renvoi demande, en substance, si l'article 6, paragraphe 1, sous c), et l'article 7, sous f), de la directive 95/46, lus à la lumière des articles 7 et 8 de la Charte, doivent être interprétés en ce sens qu'ils s'opposent à des dispositions nationales qui autorisent la mise en place d'un système de vidéosurveillance, tel que le système en cause au principal, installé dans les parties communes d'un immeuble à usage d'habitation, aux fins de poursuivre des intérêts légitimes consistant à assurer la garde et la protection des personnes et des biens, sans le consentement des personnes concernées.
- 34 Il y a lieu de rappeler qu'une surveillance effectuée par un enregistrement vidéo des personnes, stocké dans un dispositif d'enregistrement continu, à savoir un disque dur, constitue, conformément à l'article 3, paragraphe 1, de la directive 95/46, un traitement de données à caractère personnel automatisé (arrêt du 11 décembre 2014, Ryneš, C-212/13, EU:C:2014:2428, point 25).
- 35 Partant, un système de vidéosurveillance par caméra doit être qualifié de traitement de données à caractère personnel automatisé, au sens de ladite disposition, lorsque le dispositif mis en place permet d'enregistrer et de stocker des données à caractère personnel telles des images permettant d'identifier des personnes physiques. Il incombe à la juridiction de renvoi de vérifier si le système en cause au principal présente de telles caractéristiques.
- 36 En outre, tout traitement de données à caractère personnel doit, d'une part, être conforme aux principes relatifs à la qualité des données, énoncés à l'article 6 de la directive 95/46, et, d'autre part, répondre à l'un des principes relatifs à la légitimation des traitements de données énumérés à l'article 7 de cette directive (arrêt du 13 mai 2014, Google Spain et Google, C-131/12, EU:C:2014:317, point 71 ainsi que jurisprudence citée).
- 37 L'article 7 de la directive 95/46 établit une liste exhaustive et limitative des cas dans lesquels un traitement de données à caractère personnel peut être considéré comme étant licite. Les États membres ne sauraient ni ajouter de nouveaux principes relatifs à la légitimation des traitements de données à caractère personnel audit article ni prévoir des exigences supplémentaires qui viendraient modifier la portée de l'un des six principes prévus à cet article (arrêt du 19 octobre 2016, Breyer, C-582/14, EU:C:2016:779, point 57).
- 38 Il s'ensuit que, pour qu'il puisse être considéré comme étant légitime, un traitement de données à caractère personnel doit relever de l'un des six cas prévus à l'article 7 de la directive 95/46.
- 39 Les questions que pose la juridiction de renvoi concernent en particulier le principe relatif à la légitimation des traitements de données visé à l'article 7, sous f), de la directive 95/46, disposition qui a été transposée dans l'ordre juridique roumain par l'article 5, paragraphe 2, sous e), de la loi n° 677/2001, auquel renvoie également l'article 6 de la décision n° 52/2012 de l'ANSPDCP pour ce qui concerne spécifiquement le traitement de données à caractère personnel par le recours à des moyens de vidéosurveillance.

- 40 À cet égard, l'article 7, sous f), de la directive 95/46 prévoit trois conditions cumulatives pour qu'un traitement de données à caractère personnel soit licite, à savoir, premièrement, la poursuite d'un intérêt légitime par le responsable du traitement ou par le ou les tiers auxquels les données sont communiquées, deuxièmement, la nécessité du traitement des données à caractère personnel pour la réalisation de l'intérêt légitime poursuivi et, troisièmement, la condition tenant à ce que les droits et les libertés fondamentaux de la personne concernée par la protection des données ne prévalent pas sur l'intérêt légitime poursuivi (arrêt du 4 mai 2017, Rīgas satiksme, C-13/16, EU:C:2017:336, point 28).
- 41 Il y a lieu de souligner que l'article 7, sous f), de la directive 95/46 ne requiert pas le consentement de la personne concernée. Un tel consentement figure cependant, en tant que condition à laquelle le traitement des données à caractère personnel est subordonné, uniquement à l'article 7, sous a), de cette directive.
- 42 En l'occurrence, l'objectif que vise, en substance, le responsable du traitement des données lorsqu'il met en place un système de vidéosurveillance tel que celui en cause au principal, à savoir la protection des biens, de la santé et de la vie des copropriétaires d'un immeuble, est susceptible d'être qualifié d'« intérêt légitime », au sens de l'article 7, sous f), de la directive 95/46. La première condition fixée à cette disposition apparaît donc, en principe, remplie (voir, par analogie, arrêt du 11 décembre 2014, Ryneš, C-212/13, EU:C:2014:2428, point 34).
- 43 La juridiction de renvoi se pose toutefois la question de savoir si la première des conditions prévues à cet article 7, sous f), doit être comprise en ce sens que l'intérêt poursuivi par le responsable en cause doit, d'une part, être « prouvé » et, d'autre part, être « né et actuel au moment du traitement ».
- 44 À cet égard, il y a lieu de relever que, comme l'ont également fait valoir les gouvernements roumain et tchèque, l'Irlande, le gouvernement autrichien, le gouvernement portugais ainsi que la Commission, dès lors que, conformément à l'article 7, sous f), de la directive 95/46, le responsable du traitement de données à caractère personnel ou le tiers à qui les données sont communiquées doit poursuivre un intérêt légitime justifiant ce traitement, cet intérêt doit être né et actuel à la date du traitement et ne pas présenter de caractère hypothétique à cette date. Il ne saurait cependant être nécessairement exigé, lors de l'appréciation de l'ensemble des circonstances du cas d'espèce, qu'il ait été porté antérieurement atteinte à la sécurité des biens et des personnes.
- 45 En l'occurrence, dans une situation telle que celle en cause au principal, la condition relative à l'existence d'un intérêt né et actuel semble en tout état de cause être satisfaite, dès lors que la juridiction de renvoi relève que des vols, des cambriolages et des actes de vandalisme s'étaient produits avant la mise en place du système de vidéosurveillance et ce malgré l'installation, dans l'entrée de l'immeuble, d'un système sécurisé composé d'un interphone et d'une carte magnétique.
- 46 S'agissant de la deuxième condition posée à l'article 7, sous f), de la directive 95/46, relative à la nécessité du recours à un traitement des données à caractère personnel pour la réalisation de l'intérêt légitime poursuivi, la Cour a rappelé que les dérogations et les restrictions au principe de la protection des données à caractère personnel doivent s'opérer dans les limites du strict nécessaire (arrêt du 4 mai 2017, Rīgas satiksme, C-13/16, EU:C:2017:336, point 30 et jurisprudence citée).
- 47 Cette condition impose à la juridiction de renvoi de vérifier que l'intérêt légitime du traitement des données poursuivi par la vidéosurveillance en cause au principal, lequel consiste, en substance, à assurer la sécurité des biens et des personnes et à prévenir la survenance d'infractions, ne peut raisonnablement être atteint de manière aussi efficace par d'autres moyens moins attentatoires aux libertés et 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 par les articles 7 et 8 de la Charte.

- 48 En outre, ainsi que l'a soutenu la Commission, la condition tenant à la nécessité du traitement doit être examinée conjointement avec le principe dit de la « minimisation des données » consacré à l'article 6, paragraphe 1, sous c), de la directive 95/46, selon lequel les données à caractère personnel doivent être « adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement ».
- 49 Il résulte du dossier dont dispose la Cour que les exigences liées à la proportionnalité du traitement de données en cause au principal semblent avoir été prises en compte. Il est constant en effet que des mesures alternatives consistant en un système sécurisé, installé dans l'entrée de l'immeuble, composé d'un interphone et d'une carte magnétique, ont initialement été mises en place, mais se sont révélées insuffisantes. En outre, le dispositif de vidéosurveillance en cause est limité aux seules parties communes de la copropriété et aux voies d'accès à celle-ci.
- 50 Toutefois, la proportionnalité du traitement des données par la voie d'un dispositif de vidéosurveillance doit être appréciée en tenant compte des modalités concrètes de mise en place et de fonctionnement de ce dispositif, lesquelles doivent en limiter l'incidence sur les droits et libertés des personnes concernées tout en garantissant l'efficacité du système de vidéosurveillance en cause.
- 51 Ainsi, comme l'a fait valoir la Commission, la condition tenant à la nécessité du traitement implique que le responsable du traitement doit examiner, par exemple, s'il est suffisant que la vidéosurveillance ne fonctionne que la nuit ou en dehors des heures de travail normales et bloquer ou rendre floues les images prises dans des zones où la surveillance n'est pas nécessaire.
- 52 Enfin, quant à la troisième condition posée à l'article 7, sous f), de la directive 95/46, relative à l'existence de droits et de libertés fondamentaux de la personne concernée par la protection des données qui prévaudraient sur l'intérêt légitime poursuivi par le responsable du traitement des données ou par le ou les tiers auxquels les données sont communiquées, il y a lieu de rappeler, comme il a déjà été mentionné au point 32 du présent arrêt, que l'appréciation de cette condition nécessite qu'il soit procédé à une pondération des droits et des intérêts opposés en cause en fonction des circonstances concrètes du cas particulier concerné, dans le cadre de laquelle il doit être tenu compte de l'importance des droits de la personne concernée résultant des articles 7 et 8 de la Charte.
- 53 Dans ce contexte, la Cour a jugé que l'article 7, sous f), de la directive 95/46 s'oppose à ce qu'un État membre exclue de façon catégorique et généralisée la possibilité pour certaines catégories de données à caractère personnel d'être traitées, sans permettre une pondération des droits et des intérêts opposés en cause dans un cas particulier. Un État membre ne saurait ainsi prescrire, pour ces catégories, de manière définitive, le résultat de la pondération des droits et des intérêts opposés, sans permettre un résultat différent en raison de circonstances particulières d'un cas concret (arrêt du 19 octobre 2016, Breyer, C-582/14, EU:C:2016:779, point 62).
- 54 Il ressort également de la jurisprudence de la Cour qu'il est possible de prendre en considération, aux fins de procéder à cette pondération, le caractère variable, en fonction de la possibilité d'accéder aux données en cause dans des sources accessibles au public, de la gravité de l'atteinte aux droits fondamentaux de la personne concernée par ledit traitement (voir, en ce sens, arrêt du 4 mai 2017, Rîgas satiksme, C-13/16, EU:C:2017:336, point 32).
- 55 À la différence des traitements de données émanant de sources accessibles au public, les traitements de données émanant de sources non accessibles au public impliquent que des informations sur la vie privée de la personne concernée seront désormais connues par le responsable du traitement et, le cas échéant, par le ou les tiers auxquels les données sont communiquées. Cette atteinte plus grave aux droits de la personne concernée, consacrés aux articles 7 et 8 de la Charte, doit être prise en compte et être mise en balance avec l'intérêt légitime poursuivi par le responsable du traitement ou par le ou

les tiers auxquels les données sont communiquées (voir, en ce sens, arrêt du 24 novembre 2011, Asociación Nacional de Establecimientos Financieros de Crédito, C-468/10 et C-469/10, EU:C:2011:777, point 45).

- 56 Le critère tenant à la gravité de l'atteinte aux droits et aux libertés de la personne concernée constitue un élément essentiel de l'exercice de pondération ou de mise en balance au cas par cas, exigé par l'article 7, sous f), de la directive 95/46.
- 57 À ce titre, il doit notamment être tenu compte de la nature des données à caractère personnel en cause, en particulier de la nature éventuellement sensible de ces données, ainsi que de la nature et des modalités concrètes du traitement des données en cause, en particulier du nombre de personnes qui ont accès à ces données et des modalités d'accès à ces dernières.
- 58 Sont également pertinentes aux fins de cette pondération les attentes raisonnables de la personne concernée à ce que ses données à caractère personnel ne seront pas traitées lorsque, dans les circonstances de l'espèce, cette personne ne peut raisonnablement s'attendre à un traitement ultérieur de celles-ci.
- 59 Enfin, ces éléments doivent être mis en balance avec l'importance, pour l'ensemble des copropriétaires de l'immeuble concerné, de l'intérêt légitime poursuivi en l'espèce par le système de vidéosurveillance en cause, en ce que celui-ci vise essentiellement à assurer la protection des biens, de la santé et de la vie desdits copropriétaires.
- 60 Eu égard à ce qui précède, il y a lieu de répondre aux questions posées que l'article 6, paragraphe 1, sous c), et l'article 7, sous f), de la directive 95/46, lus à la lumière des articles 7 et 8 de la Charte, doivent être interprétés en ce sens qu'ils ne s'opposent pas à des dispositions nationales qui autorisent la mise en place d'un système de vidéosurveillance, tel que le système en cause au principal installé dans les parties communes d'un immeuble à usage d'habitation, aux fins de poursuivre des intérêts légitimes consistant à assurer la garde et la protection des personnes et des biens, sans le consentement des personnes concernées, si le traitement de données à caractère personnel opéré au moyen du système de vidéosurveillance en cause répond aux conditions posées audit article 7, sous f), ce qu'il incombe à la juridiction de renvoi de vérifier.

Sur les dépens

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

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

L'article 6, paragraphe 1, sous c), et l'article 7, sous f), de la directive 95/46/CE du Parlement européen et du Conseil, 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, lus à la lumière des articles 7 et 8 de la charte des droits fondamentaux de l'Union européenne, doivent être interprétés en ce sens qu'ils ne s'opposent pas à des dispositions nationales qui autorisent la mise en place d'un système de vidéosurveillance, tel que le système en cause au principal installé dans les parties communes d'un immeuble à usage d'habitation, aux fins de poursuivre des intérêts légitimes consistant à assurer la garde et la protection des personnes et des biens, sans le consentement des personnes concernées, si le traitement de données à caractère personnel opéré au moyen du système de vidéosurveillance en cause répond aux conditions posées audit article 7, sous f), ce qu'il incombe à la juridiction de renvoi de vérifier.

Signatures