Arrêt “ Ryñes ”: la vidéosurveillance à l’épreuve de la directive sur la protection des données à caractère personnel

Olivia Tambou

Commentaires

Arrêt « Ryneš » : la vidéosurveillance à l'épreuve de la directive sur la protection des données à caractère personnel[1]

Olivia Tambou(*)

- **Selon la Cour de justice, la vidéosurveillance constitue un traitement automatisé de données à caractère personnel réglementé par le droit de l'Union**
- **Ce traitement, dès lors qu'il permet de récolter des images de l'espace public, ne constitue pas une activité exclusivement personnelle ou domestique exclue du champ d'application des règles européennes**
- **Un tel traitement, même institué sans le consentement des personnes filmées, peut être légitimé s'il est nécessaire à la réalisation d'un intérêt légitime**

Introduction

La directive 95/46 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données[2] évoque simplement la vidéosurveillance au détour de son considérant 16, pour l'exclure lorsqu'elle est mise en œuvre « à des fins de sécurité publique, de défense, de sûreté de l'État ou pour l'exercice des activités de l'État relatives à des domaines n'entrant pas dans le champ du droit communautaire ».

Depuis l'adoption de cette directive, la vidéosurveillance et les traitements de données autour d'images se sont cependant fortement développés. L'affaire *Ryneš* fournit à la Cour de justice de l'Union européenne (ci-après : « la Cour ») l'occasion d'apporter, pour la première fois, d'utiles précisions sur la nature juridique de la vidéosurveillance.

1 Le champ d'application de la protection européenne des données à caractère personnel

La Cour rappelle que l'image d'une personne constitue une donnée personnelle dans la mesure où elle permet d'identifier la personne concernée[3]. En l'espèce, les enregistrements fournis par la caméra placée par M. Ryneš en façade de sa maison avait permis à la police de démasquer les auteurs de dégradations portées à celle-ci. La Cour en déduit que l'enregistrement d'une telle image par une caméra est un traitement automatisé de données personnelles au sens de l'article 2, sous b), de la directive 95/46.

La question centrale était de déterminer si ce traitement de données relevait des « activités exclusivement personnelles ou domestiques » susceptibles d'être exclues du champ d'application de la protection des données personnelles, sur le fondement de l'article 3, § 2, de la directive 95/46[4].

La Cour va répondre par la négative, en réaffirmant[5] la nécessité de se livrer à une interprétation stricte de l'article 3, § 2, et des exceptions à la protection des données à caractère personnel y inscrites. L'objectif de la directive 95/46 est d'assurer un niveau élevé de protection des droits et libertés fondamentaux, notamment de la vie privée à l'égard des traitements à caractère personnel[6]. Cette exigence se trouve renforcée depuis l'inscription du droit fondamental à la vie privée à l'article 7 de la Charte des droits fondamentaux voire même d'un droit autonome de la protection des données personnelles (article 8 de la Charte)[7]. Il en résulte que toute exception à cette protection des données personnelles doit être strictement interprétée[8].

La correspondance et la tenue de répertoires d'adresses sont les deux seuls exemples donnés par la directive pour illustrer l'exception relative aux activités exclusivement personnelles ou domestiques de l'article 3, § 2[9]. Selon l'avocat général, les activités personnelles constitueraient plutôt des activités manifestement privées et confidentielles destinées à un nombre limité voire identifié de personnes. Les activités domestiques recouvriraient des activités de la vie familiale ayant principalement lieu au domicile[10]. Dans tous les cas, la Cour souligne que ces activités ne rentrent dans le champ d'application de l'exception que si elles demeurent *exclusivement*[11] personnelles ou domestiques[12]. Le simple fait que la caméra enregistre même partiellement des images de la voie publique suffit à exclure l'application de l'article 3, § 2, de la directive 95/46[13].

---

(1) C.J., 11 décembre 2014, *František Ryneš*, C-212/13, EU:C:2014:2428. (*) L'auteure est maître de conférences en droit à l'Université Paris-Dauphine (France). Elle peut être contactée à l'adresse suivante : olivia.tambou@dauphine.fr. (2) 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 des données, *J.O.*, L 281, p. 31 (ci-après : « la directive 95/46 »). (3) Point 21 de l'arrêt annoté. (4) Point 26 de l'arrêt annoté. (5) C.J., 6 novembre 2003, *Bodil Lindqvist*, C-101/01, EU:C:2003:596. (6) Point 27 de l'arrêt annoté. (7) Points 28 et 29 de l'arrêt annoté. À cet égard, voy. également C.J., 13 mai 2014, *Google Spain et Google*, C-131/12, EU:C:2014:317. (8) Point 29 de l'arrêt annoté. (9) Considérant 12 de la directive 95/46. (10) Conclusions de l'avocat général Jääskinen, présentées le 10 juillet 2014, EU:C:2014:2072, point 51. (11) Nous soulignons. (12) Point 31 de l'arrêt annoté. (13) Point 33 de l'arrêt annoté.

Commentaires

2 L'intérêt légitime, un mécanisme dérogatoire

L'article 7, sous f), de la directive 95/46 autorise le traitement de données à caractère personnel s'« 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 1er, § 1er ».

L'application de cette disposition, au cas d'espèce est validée sans ambiguïté par l'avocat général[14], la Cour ayant préféré laisser la juridiction nationale vérifier elle-même la légalité du traitement[15].

L'article 7, sous f), de la directive 95/46 est une disposition ambiguë. D'application délicate, cet article réclame la mise en balance de l'intérêt légitime poursuivi par le responsable du traitement avec les droits et libertés fondamentaux de la personne concernée. Plusieurs critères doivent être pris en compte tels que la nature et la source de l'intérêt légitime du responsable de traitement, le caractère nécessaire ou non du traitement, l'impact sur la personne concernée[16]. En l'espèce, la jouissance de son droit de propriété et le respect à sa vie familiale étaient incontestablement les deux intérêts légitimes poursuivis par M. Ryneš. Ceux-ci semblent primer sur le droit à la protection des données personnelles de l'agresseur. En outre, la nécessité du traitement semblerait acquise, la caméra n'ayant été installée qu'à la suite d'incidents répétés et en présence d'une menace réelle.

L'article 7, sous f), de la directive 95/46 devrait donc permettre de légitimer de nombreux traitements dérogeant à la protection des données personnelles. Faut-il s'en alarmer, d'autant plus que cette disposition n'a fait l'objet d'aucune modification substantielle dans le cadre des discussions actuelles autour du règlement général de protection des données à caractère personnel[17] ? Faut-il y voir une source possible d'adaptation au regard du développement de nombreuses technologies utilisant l'exploitation d'images sur la voie publique par le biais de caméra embarquées (drone, dashcam, body-worm vidéo, Google Glass...) ? Rien n'est moins sûr. À ce stade, l'arrêt *Ryneš* semble surtout augurer d'un possible développement du contentieux autour de la prise d'images sur la voie publique.

Conclusion

L'affaire *Ryneš* impose aux particuliers ou installateurs de système de vidéosurveillance à domicile de veiller à ce que leur équipement n'enregistre aucune image de la voie publique sauf à se soumettre aux règles de la protection des données personnelles. Autrement dit, tout est une question d'orientation de la caméra.

Cette jurisprudence devrait avoir un impact sur l'encadrement actuel de la vidéosurveillance, domaine jusqu'alors régulé de façon extrêmement contrastée selon les États membres[18]. Au Royaume-Uni, pays européen dans lequel la vidéosurveillance est la plus développée, cette pratique fait l'objet d'un simple code de conduite. L'autorité de protection des données britannique avait déjà annoncé[19] qu'elle tirerait toutes les conséquences de l'affaire *Ryneš*. En effet, elle considérait jusqu'à peu que l'installation de caméra de surveillance dans les propriétés privées entrait dans l'exception de l'article 3, § 2, y compris si la caméra donnait sur l'espace public voire sur la propriété du voisin. C'est précisément cette position soutenue dans l'affaire *Ryneš* par le gouvernement britannique lors de son intervention, que la Cour a rejetée.

L'affaire *Ryneš* devrait ainsi relancer le débat sur la nécessité de clarifier l'encadrement européen et national de la vidéosurveillance alors que cette pratique tend à se banaliser. Au moment où la protection des données personnelles fait l'objet d'âpres discussions, l'arrêt *Ryneš* questionne la faculté du droit de l'Union européenne à mettre en place des catégories pertinentes susceptibles de ne pas être rapidement dépassées par les innovations technologiques et des règles dont le respect puisse être effectivement et facilement assuré dans vingt-huit États membres.

---

(14) Conclusions de l'avocat général Jääskinen, présentées le 10 juillet 2014, EU:C:2014:2072, points 64-67. **(15)** Point 34 de l'arrêt annoté. **(16)** Article 29, Data protection working party, Opinion 06/2014 on the notion of legitimate interests of the data controller under article 7 of Directive 95/46 EC. **(17)** F. Ferreti, « Data protection and the legitimate interest of data controllers : much ado about nothing or winter of rights ? », *C.M.L.R.*, 2014, n° 51, pp. 843-868. **(18)** *Cfr* groupe de travail de l'article 29, avis 4/2004 sur le traitement des données à caractère personnel au moyen de la vidéosurveillance. La Belgique s'est dotée d'une loi spécifique : la loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance. **(19)** Information Commissioner's Office, *In the picture : a data protection code of practice for surveillance cameras and personal information*, 15 octobre 2014, p. 7.