RGPD

Réutilisation de données et changement de finalité : test de compatibilité

Comme chaque mois, Alexandre Fievée tente d'apporter des réponses aux questions que tout le monde se pose en matière de protection des données personnelles, en s'appuyant sur les décisions rendues par les autorités nationales de contrôle au niveau européen et les juridictions européennes. Ce mois-ci, il se penche sur la problématique de l'exploitation par le responsable du traitement d'images obtenues grâce à un dispositif de vidéosurveillance, mais pour une finalité différente que celle initialement prévue.

Il ressort des termes de l'article 5 du RGPD que les données sont notamment collectées et traitées, d'une part, de manière loyale et licite et, d'autre part, « *pour des finalités déterminées, explicites et légitimes* ». Le texte ajoute que ces données ne peuvent être traitées « *ultérieurement de manière incompatible avec ces finalités* ». En d'autres termes, le responsable du traitement ne peut, en principe, exploiter les données qu'il a initialement collectées que pour la finalité pour laquelle il a opéré la collecte desdites données. Il ne peut donc utiliser les données pour un autre but que celui qui a été fixé. Ainsi, un fichier de recrutement de candidats pour une offre d'embauche ne peut pas être utilisé pour proposer à ces candidats des offres commerciales.

Toutefois, et comme l'indique l'article 5 susvisé, ce principe de limitation doit être nuancé, lorsque la finalité ultérieure est compatible avec la finalité initiale, ce que confirme le considérant 50 du RGPD : « *le traitement de données à caractère personnel pour d'autres finalités que celles pour lesquelles les données à caractère personnel ont été collectées initialement ne devrait être autorisé que s'il est compatible avec les finalités pour lesquelles les données à caractère personnel ont été collectées initialement* ».

Il appartient donc au responsable du traitement qui souhaite réutiliser les données collectées pour une autre finalité, de réaliser un test de compatibilité. Pour ce faire, il doit notamment tenir compte: (i) de l'existence éventuelle d'un lien entre les finalités pour lesquelles les données personnelles ont été collectées et les finalités du traitement ultérieur envisagé ; (ii) du contexte dans lequel les données personnelles ont été collectées, en particulier en ce qui concerne la relation entre les personnes concernées et le responsable du traitement ; (iii) de la nature des données personnelles, en particulier si le traitement porte sur des données sensibles ou des données personnelles relatives à des condamnations pénales et à des infractions ; (iv) des conséquences possibles du traitement ultérieur envisagé pour les personnes concernées ; (v) de l'existence de garanties appropriées.

L'affaire[1]

Un particulier avait été signalé pour avoir enfreint les règles de confinement mises en œuvre pour lutter contre la propagation du COVID-19. Ce signalement avait été réalisé grâce aux images issues du dispositif de vidéosurveillance installé dans les rues de la municipalité de Salento.

Considérant que ce traitement était contraire à la règlementation sur la protection des données personnelles, le particulier a déposé une plainte auprès de l'autorité de contrôle italienne (la « *GPDP* »). Rappelant que si une municipalité est en droit, en application des textes, d'utiliser un dispositif de vidéosurveillance installé sur la voie publique « *à des fins de sécurité urbaine* », ce dispositif ne peut être exploité pour un autre objectif, en application du principe de limitation des finalités. Or, en l'espèce, la municipalité avait traité les images litigieuses dans un but qui n'était pas la sécurité publique, mais la répression des comportements contraires aux mesures d'endiguement de la pandémie.

La question se posait alors de la compatibilité des deux finalités, étant précisé qu'il ne peut y avoir, en principe, une relation entre la finalité initiale et la finalité du traitement ultérieur que si ce dernier est déjà, dans une certaine mesure, « *implicite* » ou peut être considéré comme une « *suite logique* » du traitement initial. La GPDP a considéré que ce n'était pas le cas en l'espèce, expliquant que le traitement visant à constater une infraction aux règles de confinement « *ne peut en aucun cas être considéré comme logiquement lié ou dérivant du traitement mis en place par la municipalité aux fins de sécurité urbaine, qui vise à prévenir et combattre les phénomènes de criminalité généralisée* ».

Par ailleurs, l'autorité de protection des données a souligné que : « *le recours à la vidéosurveillance sur la voie publique en tant que mesure visant à contenir la pandémie (...) est également contraire aux attentes des citoyens concernant le traitement de leurs données, qui, compte tenu également des dispositions du règlement municipal sur la vidéosurveillance adopté par la municipalité, étaient convaincus que les images capturées par les caméras installées sur la voie publique seraient traitées exclusivement aux fins de la sécurité urbaine susmentionnée* ».

Enfin, la GPDP a relevé que la municipalité n'avait adopté aucune « *garantie spécifique* » afin de réduire l'impact du traitement sur les citoyens et d'assurer la loyauté dudit traitement, dès lors qu'elle n'a fourni aux personnes concernées « *aucune information spécifique sur la finalité du traitement poursuivie* » à savoir la détection des violations administratives des règles d'urgence pour le confinement.

Dans ces conditions, le traitement des images litigieuses par la municipalité a été considéré comme illicite car réalisé en violation notamment des dispositions de l'article 5 du RGPD.

Quelles recommandations ?

La première recommandation serait d'identifier, pour un traitement donné, toutes les finalités « *légitimes* » du dit traitement afin d'étendre son périmètre, sous réserve (i) que ces finalités soient « *déterminées, explicites* » et (ii) que les données soient traitées de manière « *loyale et transparente* ». La seconde recommandation serait, dans le cas où le responsable du traitement souhaiterait traiter les données pour une finalité différente de la ou des finalité(s) initialement prévue(s), de réaliser un test de compatibilité. Cet exercice est fondamental car, en cas d'incompatibilité, le nouveau traitement serait considéré comme illicite et les éléments de preuve obtenus au moyen dudit traitement (par exemple : un dispositif de vidéosurveillance) pourraient être considérés, devant une juridiction civile, comme déloyaux et donc inopposables à la personne concernée.

Alexandre FIEVEE
Avocat associé
DERRIENNIC Associés

Notes

(1) GPDP, ordonnance d'injonction, 20 octobre 2022.

Vous avez envie de vous exprimer sur un sujet qui vous tient à cœur, de partager votre analyse avec la communauté des lecteurs d'Expertises, d'exposer un point de vue différent sur un article déjà publié, de lancer un débat sur un thème émergent, ou simplement de commenter l'actualité du droit du numérique ?

Contactez la rédactrice en chef d'Expertises Sylvie Rozenfeld sr@expertises.info