PROTECTION DES DONNÉES

Comment sécuriser les projets locaux impliquant les nouvelles technologies

De plus en plus régulièrement, les collectivités territoriales sont sollicitées par leurs satellites locaux pour les accompagner dans le portage de projets innovants impliquant le maniement de nouvelles technologies et le traitement de données parfois sensibles. Ce qui implique des problématiques nouvelles qu'un récent cas d'école a illustrées. Ce qu'il faut en retenir.

1 L'INSTRUCTION DES PROJETS PORTÉS PAR LES SATELLITES LOCAUX

Les projets locaux impliquant les nouvelles technologies et leurs usages se multiplient avec l'essor du numérique. Les collectivités locales, particulièrement concernées par ces évolutions, doivent percevoir les bonnes pratiques pour se prémunir des risques juridiques et mésusages. Ainsi, lorsqu'elles sont sollicitées pour intervenir, matériellement ou financièrement, dans la mise en place d'un tel projet, les collectivités doivent être en mesure d'instruire les demandes de façon sécurisée, qu'il s'agisse d'installer un système de captation d'images sur un équipement municipal, de mettre en œuvre un dispositif de reconnaissance faciale à l'entrée des services publics ou encore de transmettre voire de vendre des bases de données.

Car de plus en plus de start-up se penchent sur le développement d'outils innovants intégrant des nouvelles technologies. Ces produits sont désormais largement proposés aux collectivités et à leurs satellites locaux, dont les sociétés publiques locales, les associations ou les groupements d'intérêt public. Ces dispositifs innovants peuvent améliorer la qualité d'un service public, contribuer à garantir la sécurité des administrés, aider les collectivités dans la gestion quotidienne de leurs compétences locales et assurer la performance de leurs satellites locaux au regard de leur objet social.

Un projet qui doit être lié aux compétences de la collectivité

A cet égard, si le recours à ces outils présente un intérêt indéniable pour les collectivités et leurs satellites locaux, il n'en demeure pas moins que leur mise en place doit répondre à un process savamment orchestré afin de s'assurer de la sécurité juridique du projet soumis. En effet, les collectivités sont garantes de la bonne gestion des deniers publics et leurs interventions, financières comme matérielles, sont largement encadrées par le législateur. Rappelons à ce titre que l'octroi de subventions publiques, telles qu'elles sont définies à l'article 9-1 de la loi du 12 avril 2000, doit être justifié par un intérêt public local et viser la réalisation d'une action déterminée. Or, si l'appréciation de l'intérêt public local justifiant l'octroi d'une subvention est discrétionnaire et souveraine, il n'en demeure pas moins que le projet soumis à la collectivité doit pouvoir être rattaché à l'une des compétences qu'elle exerce. Il est plus facile de démontrer ce lien lorsque c'est une commune qui est sollicitée puisqu'elle jouit encore de la clause générale de compétences.

S'assurer du respect de l'ordre public… et du RGPD

Dès lors que la subvention est fléchée, et qu'il est indéniable que la solution innovante proposée peut se rattacher à une compétence exercée par la collectivité, celle-ci peut participer à son déploiement. A cet égard, on peut envisager que soit financée directement l'entreprise qui apporte l'outil ou son satellite local qui se dote d'un tel outil dans le cadre de son activité.

Si les conditions d'attribution de la subvention sont remplies, il convient encore de s'assurer que l'innovation proposée n'est pas de nature à contrevenir à l'ordre public et au RGPD dont les collectivités assurent la mise en conformité dans leur fonctionnement quotidien. Il en va de même si le concours n'est pas financier.

A titre d'exemple, s'agissant de l'octroi d'une autorisation d'occupation du domaine public soumis aux articles L.2122-1 et L.2125-1 du code général de la propriété des personnes publiques (CG3P), il appartient à la collectivité de s'assurer que le projet remplit les conditions pour se voir délivrer une autorisation mais aussi qu'il respecte la réglementation en matière de protection des données.

Partant, la participation d'une collectivité territoriale à la mise en

place d'un outil innovant doit s'accompagner d'une analyse combinée pour déterminer si les conditions du concours sont remplies mais aussi si le dispositif est conforme au RGPD.

2 COLLECTIVITÉS, FOOT ET VIDÉOS : LE CAS D'ÉCOLE

A titre d'exemple, une société proposant la mise à disposition d'une plateforme de scouting vidéos (travail sur enregistrements) a démarché des clubs de football amateurs afin de leur proposer une solution innovante. Il s'agissait de l'installation d'un dispositif de captation d'images leur permettant de filmer les matchs, d'analyser les performances et de créer une base de données complète avec les matchs et les joueurs.

Partant, la société collecte des informations personnelles, notamment relatives aux caractéristiques biométriques ou à la santé des joueurs, telles que la taille, le poids et le pied fort des joueurs. En parallèle, la société propose aux recruteurs de clubs de football professionnel de leur faciliter l'accès aux images captées via une plateforme.

Notons que la majorité des clubs de football amateur sont constitués sous forme associative dont les statuts sont régis par la loi de 1901 . A cet égard, il est fréquent que les associations locales concluent des partenariats avec les collectivités locales qui peuvent concourir, matériellement ou financièrement, à leur activité.

La délicate captation d'images

En l'occurrence, l'association sportive concernée a conclu avec la commune une convention pluriannuelle d'objectifs et de moyens au terme de laquelle elle bénéficie d'avantages en nature, tels que la mise à disposition à titre gracieux d'équipements sportifs et de subventions publiques versées annuellement. Or, en pratique, le dispositif proposé par la société à l'association nécessite l'installation d'un système de captation d'images qui passe par l'implantation, en bord de terrain, d'un poteau, sur lequel est fixée une caméra.

Un dispositif de captation d'images, stocké dans un dispositif d'enregistrement continu, à savoir le disque dur, doit respecter les prescriptions du RGPD.

C'est dans ces conditions que la société a sollicité de l'association sportive qu'elle se rapproche de la commune, propriétaire des équipements sportifs, afin de disposer d'une autorisation d'occupation du domaine public. A cet égard, la commune s'est donc interrogée, d'une part, sur les modalités d'octroi d'une telle autorisation et, d'autre part, sur la légalité du dispositif innovation proposé par la société.

En effet, et en tout état de cause, si la commune peut octroyer une autorisation d'occupation du domaine public dans le respect des principes légaux et jurisprudentiels, elle doit aussi s'assurer que l'activité qui se déploiera grâce à cette autorisation ne contrevient pas à l'ordre public.

Redevance imposée, mise en concurrence préférable

Ainsi, au regard des dispositions du CG3P, la commune peut délivrer une telle autorisation mais à la condition de fixer une redevance. Contrairement à l'association sportive, la société ne peut pas bénéficier des dérogations légales pour jouir d'une autorisation à titre gracieux. En outre, si la commune a pu envisager d'actionner certaines dérogations légalement prévues, afin de sécuriser le projet, dès lors que la société a une activité économique dans un secteur concurrentiel, il est apparu préférable de soumettre la délivrance de l'autorisation à la procédure de mise en concurrence et de publicité prévue à l'article L. 2122-1-1 du CG3P.

Reste à déterminer pour la commune la manière dont elle peut contrôler l'activité réalisée grâce à cette autorisation. A cet égard, plusieurs préconisations, transposables à d'autres projets, sont apportées.

3 LA SÉCURISATION JURIDIQUE DES CONCOURS APPORTÉS PAR LES COLLECTIVITÉS

La qualification juridique des traitements au regard du RGPD

Rappelons que dès qu'une collecte concerne toute information se rapportant à une personne physique identifiée ou identifiable, il s'agira de données personnelles. De plus, toute utilisation de données à caractère personnel sera qualifiée de traitement de données. Or un traitement de données doit respecter les dispositions relatives à la législation issue du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et au règlement général sur la protection des données (ci-après « RGPD ») du 27 avril 2016. A cet égard, un visage reconnaissable est une donnée à caractère ●●●

RÉFÉRENCES

- 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.
- Arrêt de la Cour de justice de l'Union européenne C-212/13 du 11 décembre 2014, František Ryneš contre Úrad pro ochranu osobních údaj.
- 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.

personnel puisqu'elle permet l'identification indirecte d'une personne physique au travers d'un élément spécifique propre à son identité physique.
La CJUE, interrogée au travers d'une question préjudicielle des juridictions tchèques en 2014, a rendu une décision soumettant l'ensemble des systèmes de vidéoprotection et vidéosurveillance aux dispositions de la directive de 1995 (l'ancêtre du RGPD), puisque ce système de surveillance comprenait bien des données à caractère personnelles, qu'elles étaient bien identifiantes et qu'il y avait bien une activité de traitement.

L'enregistrement en continu relève bien du RGPD. Lorsque l'on évoque le concept d'activité de traitement de données, tous les procédés sont pris en compte. Il peut s'agir d'une action de collecte, d'enregistrement, d'organisation, de conservation, d'adaptation, de modification, d'extraction, de consultation, d'utilisation, de communication par transmission ou toute autre forme de mise à disposition, de rapprochement ou d'interconnexion, de verrouillage, d'effacement ou de destruction de données à caractère personnel.
Dans ces conditions, et dans notre exemple, un dispositif de captation d'images, stocké dans un dispositif d'enregistrement continu, à savoir le disque dur, constitue un traitement de données à caractère personnel automatisé. Par conséquent, cet outil doit respecter les prescriptions du RGPD.
Notons ainsi que, pour déterminer si les obligations fixées par le RGPD sont applicables, la question liminaire est celle de savoir si l'outil innovant réalise un traitement de données à caractère personnel.

Les points juridiques à contrôler

La mise en œuvre d'un tel traitement entraîne l'application de formalités administratives.

La prise de contact avec le délégué à la protection des données du prestataire. Le délégué à la protection des données (DPD) est chargé de mettre en œuvre la conformité au RGPD au sein de l'organisme qui l'a désigné. Sa désignation est obligatoire dans certains cas, notamment lorsque le traitement est effectué par une autorité publique ou un organisme public ou alors que les activités de base du responsable du traitement ou du sous-traitant consistent en un traitement à grande échelle de catégories particulières de données sensibles. De plus, la Cnil considère généralement qu'un traitement à large échelle s'entend du traitement de données personnelles de plusieurs centaines de personnes.
Dans notre exemple, une entreprise ayant pour objet de collecter des données relatives à l'âge, à la technique mais aussi à la santé de joueurs afin de constituer une banque de données accessible pour différents recruteurs a l'obligation de désigner un DPD dès lors qu'il s'agit de brasser des données sensibles.
Aussi, eu égard aux circonstances de l'espèce, il appartient à la collectivité de prendre attache avec la société ou le satellite local proposant la solution innovante afin de s'assurer de la nomination d'un délégué interne ou externe pour traiter des problématiques issues du RGPD.

La communication du registre des traitements. Ensuite, afin de vérifier le respect du droit des données, il est possible de demander la communication du registre des activités de traitement.
Ces éléments permettent d'obtenir des informations très précises sur le traitement réalisé (notamment les finalités, les catégories de destinataires, les descriptions de personnes concernées, les délais prévus pour l'effacement des données). Cela permet de s'assurer du bon usage des données collectées.
Toutefois, l'obligation de tenir un registre ne s'applique pas à une entreprise ou à une organisation comptant moins de 250 em-

ployés, sauf si le traitement porte notamment sur les catégories particulières de données visées à l'article 9 du RGPD précité. Ainsi, si une entreprise a moins de 250 salariés mais qu'elle collecte des données de santé, ce qui est le cas dans notre exemple, alors la société a l'obligation de tenir un registre des activités de traitements. La collectivité devrait donc en demander la communication pour vérifier la qualité des renseignements inscrits et repérer un éventuel manquement à la législation européenne.

Le recueil du consentement. Ensuite, il est possible de demander par quel moyen la société collecte le consentement des personnes visées par le traitement et d'en demander la communication. En effet, tous les traitements de données à caractère personnel doivent être fondés sur une base légale. S'agissant d'un dispositif de captation d'images, comme c'est le cas dans notre exemple, il apparaît que seul le consentement des joueurs permet la collecte de leurs données.
Au-delà, tous les joueurs devront être informés des données que l'entreprise va collecter sur eux au moment du recueil du consentement.
A ce titre, il serait possible de solliciter de la société la communication du questionnaire de consentement transmis aux joueurs. Il en va de même lorsqu'il s'agit de mettre en place un outil innovant ou de procéder à la collecte de données pour créer de la data.

L'analyse d'impact relative à la protection des données. Enfin, il est possible de demander si une analyse d'impact a été réalisée. En effet, cette nouvelle obligation a été pensée pour assurer un niveau de protection plus élevé des données à caractère personnel des individus, et donc un respect accru de leurs droits et libertés.
Le Comité européen de la protection des données (CEPD) a identifié neuf critères permettant de caractériser un traitement susceptible d'engendrer un risque élevé :
– données traitées à grande échelle ;
– données sensibles (origine raciale ou ethnique, opinions politiques, convictions religieuses ou philosophiques, appartenance syndicale, données génétiques ou de santé, données biométriques et données concernant la vie ou l'orientation sexuelle) ou données à caractère hautement personnel (données relatives à des communications électroniques, données de localisation, données financières, etc.) ;
– données concernant des personnes vulnérables ;
– croisement ou combinaison de données ;
– évaluation / scoring (y compris le profilage) ;
– prise de décision automatisée avec un effet juridique ou similaire ;
– surveillance systématique de personnes ;
– traitement pouvant exclure du bénéfice d'un droit, d'un service ou d'un contrat ;
– utilisation innovante ou application de solutions technologiques ou organisationnelles.

Il est possible de demander si une analyse d'impact sur la protection des données a été réalisée, une nouvelle obligation visant à renforcer les libertés et droits individuels.

Dans ses différentes délibérations, la Cnil considère qu'un traitement qui est caractérisé par au moins deux des critères susmentionnés doit faire l'objet d'une analyse d'impact relative à la protection des données (AIPD).
Dans l'exemple précité, le traitement mis en œuvre par la société concerne des données à large échelle (plusieurs centaines de personnes, de différents clubs), il va concerner des personnes vulnérables (enfants par exemple), il concerne des données sensibles, il permettra du scoring et l'on peut enfin considérer qu'il s'agit d'une solution technique innovante.
Ainsi, trois à cinq critères seraient réunis, entraînant ainsi la nécessité d'une analyse d'impact. Il convient alors de demander la transmission de l'AIPD.

En conclusion, l'application du régime juridique des données à caractère personnel entraîne de nombreuses conséquences pour les entreprises proposant des outils innovants. Le respect de ces obligations pourra être contrôlé par les collectivités territoriales sollicitées pour concourir au développement des outils proposés et vérifier la conformité du traitement au RGPD.

Par Alexandra Aderno et David Conerardy, avocats à la Cour, SCP Seban & associés