ARTICLE d'ISABELLE DUBOIS, AD HOC RESOLUTION PARU IN PIXEL, 2018, p. 126-128

RGPD, quel impact pour les acteurs de la vidéo protection ?[1]

Préambule

Comme déjà évoqué, l'objectif du règlement est de renforcer les droits des personnes physiques en matière de protection des données, et de faciliter la libre circulation des données à caractère personnel dans le marché unique numérique, notamment par une réduction de la charge administrative. Comme personne ne peut plus l'ignorer, il s'applique de plein droit sur tout le territoire de l'Union européenne depuis le 25 mai dernier. Il permet d'uniformiser les droits et obligations et d'organiser de manière cohérente le traitement des litiges par les autorités de surveillance.

Le citoyen est au cœur de cette réglementation, dont le fondement est le respect de tous les droits fondamentaux et principes reconnus par la Charte des droits fondamentaux de l'Union européenne, consacrés par les traités, et en particulier le droit au respect de la vie privée et familiale, du domicile et des communications, le droit à la protection des données à caractère personnel, et le droit à la liberté d'expression et d'information.

L'évolution technologique et la mondialisation imposaient la mise en place d'un cadre de protection des données solide et cohérent dans l'Union accompagné d'une application rigoureuse des règles, de manière à susciter la confiance indispensable au développement de l'économie numérique.

Pour les pays tiers, comme la Suisse, le Règlement s'applique, d'une part, au traitement de données à caractère personnel relatives à des personnes concernées qui se trouvent dans l'Union, lorsque les activités de traitement sont liées à *l'offre de biens ou de services* à ces personnes, qu'un paiement soit exigé ou non ; d'autre part, lorsque ledit traitement est lié à l'observation du comportement de ces personnes, dans la mesure où il s'agit de leur comportement au sein de l'Union européenne.

Les activités de vidéo protection et le RGPD

Lorsque j'installe un système de vidéo surveillance dans mon entreprise, dans mon usine, dans mon quartier , mon centre commercial ou plus largement ma ville, je mets en place un système qui conduit au traitement de données à caractère personnel, possiblement de catégories particulières, au sens du Règlement , car par l'image , lorsqu'elle est de qualité et vise l'identification des personnes, il me sera possible de détecter des origines raciales ou ethniques , des données de santé voire des opinions politiques ou des convictions religieuses si de tels lieux (partis politiques, manifestations politiques, manifestations et cérémonies religieuses) sont inclus dans les lieux sous vidéosurveillance. En dehors d'autorisations spécifiques à obtenir cas échéant, il y a lieu de respecter les principes applicables à tout traitement de données personnelles, que l'on peut rappeler ici :

---

1 http://eur-lex.europa.eu/search.html?textScope0=title&qid=1469976055573&DTS_DOM=EU_LAW&type=advanced&lang=fr&andText0=R%C3%88GLEMENT%20(UE)%202016/679&SUBDOM_INIT=LEGISLATION&DTS_SUBDOM=LEGISLATION

- Tout traitement doit être licite et loyal.
- Les personnes doivent être informées « en toute transparence » de la collecte, de l'utilisation, de la consultation, du traitement actuel ou futur. L'information doit être accessible, facile à comprendre, exprimée en termes simples et clairs. L'identité du responsable de traitement et la finalité doivent être connus.
- Les finalités précises du traitement doivent être explicites et légitimes, et déterminées lors de la collecte. Un traitement à d'autres fins est admissible s'il est « compatible » avec la finalité initiale (comme l'archivage).
- Les données doivent être adéquates, pertinentes, limitées à ce qui est nécessaire au vu des finalités. En particulier, la durée de conservation doit être « limitée au strict minimum », de sorte que des délais devront être fixés par les responsables de traitement. Le traitement ne doit avoir lieu que si la finalité ne peut être atteinte autrement.
- Les données inexactes doivent être rectifiées ou supprimées.
- Une sécurité et une confidentialité « appropriées » des données doit être garantie, l'accès non autorisé à ces données et à l'équipement servant à leur traitement doit être prévenu.

Plusieurs obligations de faire sont nouvelles ou renforcées, et ont un impact en matière de vidéosurveillance :

- Protection des données dès la conception et par défaut : cela implique que les outils, applications, logiciels doivent être conçus dès l'origine de manière à respecter ou permettre de respecter les principes qui prévalent au traitement de données personnelles. En particulier, vu le droit d'accès des personnes concernées, le système de vidéosurveillance doit permettre d'isoler une personne dans une séquence enregistrée, en masquant ou floutant les tiers. Il faut aussi rappeler l'obligation de limiter la conservation des données à la période nécessaire à la mission ou prévue par la loi. De même la confidentialité, mais aussi la disponibilité et l'intégrité devront être garanties ;
- Analyse d'impact : une évaluation de l'impact attendu ou supposé devra être effectuée lorsqu'un nouveau traitement envisagé est susceptible d'enfreindre les droits de la personnalité ou les droits fondamentaux des personnes concernées. Ce sera le cas de nouvelles technologies comme de tout traitement de données de catégories particulières, et des traitements impliquant une surveillance du comportement à large échelle, par exemple d'un système de vidéosurveillance de l'espace public. Cette obligation d'évaluation est à prendre, de mon point de vue, comme l'opportunité de décrire clairement le projet et ses implications, et de s'interroger sur les mesures techniques et organisationnelles à mettre en place. Vous trouverez ci-dessous certains outils existants testés :
    - La CNIL propose un outil gratuit, très utile pour les entreprises qui sont uniquement ou également par le biais de filiales par exemple, soumises au RGPD

      https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-2-fr-modeles.pdf

    - L'équivalent est proposé pour les organes fédéraux et les entreprises soumises à la loi suisse (dont le projet de modification reprend l'analyse d'impact)

https://www.apps.edoeb.admin.ch/dsfa/fr/evaluation.html

- Un outil en ligne, payant car le résultat de l'analyse est délivré avec un avis d'expert, et destiné aux petites et moyennes entreprises suisses et françaises :
- https://www.pragmatic-consulting.ch/evaluation-impact/

- Registre des traitements : Les fichiers de vidéosurveillance devront être listés dans un registre, au même titre que tout autre traitement, avec l'indication du nom, du but du traitement, des catégories de données traitées, des destinataires et des personnes ayant les accès en visionnement direct ou différé et en extraction, du lieu et de la durée de conservation. On peut y adjoindre des indications sur la mise en œuvre des principes, comme par exemple les mesures techniques et organisationnelles qui sont prises. Le registre des traitements est un bon outil de gestion.
- Annonce des violations de données à caractère personnel : le responsable du traitement doit annoncer les failles de sécurité à l'autorité de contrôle compétente, dans les 72 heures au plus tard après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques. Si au contraire le risque pour ces personnes est élevé elles devront également être informées. Le sous-traitant doit être mesure d'informer le responsable de traitement dans les mêmes délais.
- Désignation d'un délégué à la protection des données : pour les institutions publiques, il est désormais obligatoire de désigner une telle personne, interne ou externe, sachant que la fonction peut être mutualisée. Les entreprises privées ont le choix sauf si elles traitent un volume important de données ou des catégories particulières de données.

Comme le FGS (Forum genevois de la sécurité, voir www.fgsonline.ch) que je préside depuis peu aime à le relever dans ses recommandations, l'essentiel en matière de vidéosurveillance est de considérer celle-ci comme un moyen de sécurité à intégrer dans un concept global de sécurité, et non de considérer celle-ci *per se.*

C'et donc avec l'accompagnement d'experts que la mise en place d'un tel système a le plus de chance d'être efficient, conforme à la législation et respectueux des citoyens.

*

ID, juin 2018