LA PROTECTION DES DONNÉES PERSONNELLES A L'EPREUVE DU CONFINEMENT : BILAN, LEÇONS ET PERSPECTIVES

ANTOINE BÉGUIN, *MAÎTRE DE CONFÉRENCES - UNIVERSITÉ ANGERS*

AVOCAT AU BARREAU D'ANGERS

L'UTILISATION ET LE TRAITEMENT DE DONNÉES PERSONNELLES DANS LE CONTEXTE DE LA PANDÉMIE DU COVID-19 SUSCITENT BEAUCOUP D'INTERROGATIONS LÉGITIMES

- Objectif des autorités : RASSURER !

  - Rassurer sur le fait que la législation en matière de protection des données personnelles ne fait pas obstacle à la mise en œuvre de traitements destinés à gérer la pandémie, y compris lorsque des données de santé ou de localisation sont concernées,

  - Rassurer sur le fait que le respect des principes de protection des données personnelles est nécessaire pour garantir les droits et libertés des personnes.

OBJECTIF ATTEINT ?

- Pas certain…
- …car le cadre légal applicable reste assez largement méconnu ou incompris.
- Pourquoi ?
  - Depuis le début de la crise générée par le Covid-19, nombre de mesures envisagées pour prévenir ou contenir la pandémie, **sont signalées ou dénoncées comme contraires au RGPD**.

QUELQUES RAPPELS :

- Quelles sont les données personnelles protégées ?
  - Les données personnelles regroupent toutes les informations se rapportant à une personne physique identifiée ou identifiable (l'article 4 du RGPD + article 2 de la loi informatique et libertés du 6 Janvier 1978).
  - Il s'agit donc du nom/prénom, adresse, numéro de carte d'identité, adresse IP etc…
  - Certaines données sont dites sensibles : données de santé.

- Encore faut-il que ces données personnelles soient l'objet d'un traitement

- Quels sont les textes applicables ?
  - Dans un premier temps, la protection des données personnelles de chaque citoyen français était couverte par une loi du 6 janvier 1978 dite « informatique et liberté ».

INFLUENCE DU DROIT EUROPÉEN

- « Directive police justice » du 27 avril 2016 relatives aux traitements des données personnelles en matière pénale.

→ Elle a conduit à renforcer les droits de chaque citoyen européen sur la protection des données personnelles et responsabilise les acteurs à l'origine de ces données.

- Règlement Général sur la Protection des Données Personnelles entré en application du 25 mai 2018 qui couvre l'ensemble des résidents de l'Union Européenne.

CONCLUSIONS SUR LE SUBSTRAT LÉGAL

- **Nous disposons du cadre juridique le plus strict au monde concernant le traitement et la circulation des données à caractère personnel.**

- En France, la CNIL, en tant qu'autorité administrative indépendante est chargée de contrôler l'application de cette législation, ce qui implique de donner des avis, de contrôler en amont et en aval, voire de sanctionner.

- Elle oblige toutes les entreprises et administrations à respecter certaines règles concernant le traitement informatisé ou écrit des données à caractère personnel. Ce cadre européen a été un précieux outil afin de réguler la récolte des données personnelles au vu de l'installation de la pandémie en France.

POINT ESSENTIEL : LE DROIT À LA PROTECTION DES DONNÉES N'EST PAS UN DROIT ABSOLU

- Il connaît comme les autres droits fondamentaux des limites qui sont posées par l'interaction de ce droit avec les autres droits et libertés.

- Le 4ème considérant du RGPD nous rappelle qu'il n'est pas absolu et qu'il doit être considéré « *par rapport à sa fonction dans la société et être mis en balance avec d'autres droits fondamentaux, conformément au principe de proportionnalité* ».

→ Ce droit est « *conçu pour servir l'humanité* ». Ainsi, dans le contexte de la pandémie du Covid-19, le droit à la santé et le droit à la protection des données personnelles vont de pair.

= Il faut concilier libertés personnelles et la récolte nécessaire des données personnelles.

POINT DE VUE DE LA CNIL

- En France, la CNIL s'est auto-saisie avant le début du confinement pour rappeler les grands principes gouvernant la collecte des données = démarche de prévention.

- Le but de cette autorité était clair : la protection des données ne doit aucunement être un frein aux traitements des données nécessaires à la lutte contre le virus.

- Le risque tient qu'avec le motif d'une crise sanitaire, l'autorité publique cherche à récolter le maximum de données sur l'état de santé de chaque citoyen français.

LA SOUPLESSE OFFERTE PAR LE RGDP

- Le RGPD offre de la souplesse pour mettre en œuvre la collecte de données liées à la pandémie.

- Cependant, il ne faut pas oublier que la collecte des données doit respecter différents principes figurant dans le RGPD tels que la proportionnalité ou encore la transparence.

- Classiquement, le traitement des données personnelles en droit français se soumet à de nombreuses obligations, toutes remplissant le même objectif : celui de protéger la vie privée et les libertés individuelles des citoyens.

QUELLES SONT LES CONDITIONS DE LÉGALITÉ DES TRAITEMENTS DE DONNÉES À CARACTÈRE PERSONNEL DANS LE CONTEXTE DE LA PANDÉMIE DU COVID-19 ?

- En principe, au visa de l'article 5 du RGPD, les données à caractère personnel doivent être *traitées de manière licite, loyale et transparente* et *collectées pour des finalités déterminées* ; *explicites* et *légitimes* ; *adéquates, pertinentes et limitées aux finalités du traitement* ; *exactes* et *tenues à jour* ; *conservées de façon temporaire* et *sécurisée*.

- Pourtant, ce règlement prévoit un certain nombre d'exceptions aux principes de protection susmentionnés.

→ En effet, certains motifs impérieux, reposant pour leur grande majorité sur une nécessité d'intérêt public, impliquent le traitement des données personnelles et ce, même en l'absence de consentement de l'individu.

POURQUOI CETTE SOUPLESSE ?

- Cette exception à la protection des données traduit la consécration d'un principe fondamental

→ la protection de la santé publique = évidemment applicable au contexte d'épidémie qu'a connu la France

- Vigilance nécessaire car la collecte et plus précisément le traitement des données personnelles des citoyens français, serait donc justifiée par la crise sanitaire actuelle, qui, indéniablement, constitue une menace grave pour les intérêts vitaux de la population.

UNE PRÉCISION : L'ÉTAT D'URGENCE SANITAIRE ÉCARTE-T-IL L'APPLICATION DU RGPD ?

- La promulgation par l'article 4 de la loi du 23 mars 2020 d'un nouveau régime d'exception, **l'état d'urgence sanitaire**, mis en œuvre pour une période reconductible de deux mois, a pu susciter des doutes sur l'applicabilité du RGPD aux traitements décidés dans ce cadre.

- Question : les mesures décidées par les autorités sur le fondement de la loi du 23 mars 2020 pour gérer la pandémie, sont-elles considérées comme de simples mesures mises en œuvre à des fins de « santé publique » telle que définie au RGPD ou faut-il considérer qu'elles relèvent d'un régime dérogatoire relevant de la sécurité publique ?

- Réponse : même si ces traitements sont souvent mis en œuvre dans l'urgence, il n'en demeure pas moins qu'ils restent soumis à la réglementation en matière de protection des données personnelles, dont notamment le RGPD.

QUELLES SONT LES CONDITIONS DE MISE EN ŒUVRE DES TRAITEMENTS DE DONNÉES À CARACTÈRE PERSONNEL DANS LE CADRE D'UNE CRISE SANITAIRE ?

- Avant toute chose, la collecte de données à caractère personnel doit obéir à un strict principe de légalité et reposer par conséquent sur une base juridique admissible = il faut une loi.

- De plus, il existe des exigences résultant de deux principes :
  - la finalité et la minimisation
  - = il s'agit d'avoir recours à des traitements les moins **immisçant et intrusifs** possible afin de collecter le minimum de données nécessaires au regard de l'objectif poursuivi.

DEUX IMPÉRATIFS À RESPECTER DANS LE CADRE DU CONFINEMENT ET DU DÉCONFINEMENT

- Il est indispensable que les responsables de traitement gardent à l'esprit le respect des principes directeurs du RGPD qui peuvent être résumés par :
  - le respect du **principe de finalité** = les raisons pour lesquelles les données personnelles traitées doivent légitimes, explicites et déterminées.

    Il est donc important de ne pas succomber à la tentation de collecter précipitamment des données sans but précis en pensant que celles-ci pourraient présenter un intérêt futur

  - Le respect du **principe de proportionnalité** = seules les données permettant la poursuite des finalités préalablement identifiées peuvent être traitées, et ce, uniquement pendant le temps nécessaire à leur accomplissement.

LE PARADOXE…

- Ces deux principes s'apprécient à l'aulne des bénéfices sociaux qui découlent de la mesure.
  - Or les bénéfices sociaux dépendent de leur efficacité.
  - Ainsi, s'il est démontré qu'une application mobile est efficace dans la lutte contre le coronavirus, l'ingérence avec le droit de la protection des données personnelles sera plus facile à justifier, à condition d'accompagner cette ingérence de mesures techniques et organisationnelles de protection.

  - Or, on sait que l'efficacité d'un dispositif du type application sur mobile nécessite une adoption par plus de 60 % de la population

- Paradoxalement, un dispositif d'application mobile sur la base du volontariat se révélera moins proportionné (et donc moins justifié au regard du RGPD) qu'un dispositif obligatoire !

Focus sur quelques mesures mises en œuvre

FOCUS SUR LA CAMÉRA THERMIQUE

- **Décision du Conseil d'Etat du 26 juin 2020 (n° 441065, Ligue des droits de l'homme, Lebon)**

- Installation d'une caméra thermique dans des locaux municipaux :
  - Légale si :
    - La personne se place volontairement dans son champ d'action pour savoir si sa température excède ou non la normale ;
    - Elle ne doit pas constituer une condition d'accès ;
  - Illégale si :
    - La personne dont la température excède la normale est « invitée » à quitter l'établissement = traitement automatisé de données personnes au sens du RGPD
    - = atteinte manifestement illégale à une liberté fondamentale.

FOCUS SUR LA SURVEILLANCE PAR DRONE

- **Décision du Conseil d'Etat du 18 mai 2020 (n° 440442)**

- Le préfet de police avait mis en place un dispositif de drones pour apprécier à distance le respect des conditions de confinement (un appel d'offre avait été lancé par le Ministère de l'intérieur pour acquérir 650 drones !).

→ = illégalité de la mesure en raison de l'absence de garanties techniques de nature à éviter que les drones ne collectent des données à caractère personnel

→ = Il existe donc un risque qu'un opérateur puisse activer le zoom, ou baisser l'altitude de vol, de manière à individualiser des personnes

- En l'absence de telles garanties techniques, le dispositif doit être considéré comme traitant des données à caractère personnel et être autorisé par un arrêté après avis de la CNIL, ce qui n'a pas été le cas.

FOCUS SUR LA GÉOLOCALISATION INDIVIDUALISÉE

Exemple de Taïwan :

- les personnes malades ou suspectées d'être contaminées étaient contrôlées plusieurs fois par jour.
- Les autorités surveillaient la localisation du téléphone en temps réel.
- Si une personne en quarantaine s'éloignait de son lieu de résidence, la police recevait immédiatement une alerte et intervenait, de même si quelqu'un éteignait son téléphone.
- Pour vérifier que la personne n'était pas sortie en laissant le mobile à la maison, les fonctionnaires appellaient également plusieurs fois par jour. Les contrevenants s'exposaient à de sévères amendes, pouvant dépasser 30. 000 euros.

En Russie :

Plus de 100.000 caméras de vidéosurveillance de Moscou ont été couplées à un système de reconnaissance faciale permettant d'identifier les personnes qui violaient leur quarantaine.

En Pologne :

- Les autorités proposaient aux personnes qui revenaient de l'étranger d'installer une application mobile appelée « La quarantaine à domicile ».
- La personne devait se prendre initialement en photo. Pour vérifier le respect de sa quarantaine, le système lui demandait de manière inopinée de prendre des selfies géolocalisés, plusieurs fois par jour. Le système était facultatif, mais ceux qui ne l'installaient pas s'exposaient à des visites surprises de la police à domicile. La violation de la quarantaine était passible d'une amende de 1.000 euros.

FOCUS SUR LE TRAÇAGE STATISTIQUE

- Choix Français (inspiré de ce qui a été pratiqué dans d'autres pays) :
  - Orange a fourni à l'INSERM (Institut national de la santé et de la recherche médicale) des données mobiles de géolocalisation afin de modéliser la diffusion du virus et l'impact du confinement.

  - Les données fournies par Orange ont été utilisées de deux manières.
    - Dans un premier temps, l'INSERM a analysé la mobilité avant et après le confinement.
    - Elle s'est intéressée aux changements spontanés dans la mobilité des personnes = l'objectif est de mieux appréhender comment les personnes changent elles-mêmes leurs comportements en réponse à une épidémie.
    - Dans un deuxième temps, les données ont aussi été intégrées dans des modèles de diffusion de la pandémie développés par l'équipe, afin de mieux prévoir la propagation du virus en tenant compte de la mobilité des personnes mais aussi d'identifier les régions à risque de devenir un foyer épidémique et de modéliser l'impact sur le système sanitaire.
    - Conclusions : l'étude a permis de montrer que près d'un million de Franciliens ont quitté la région parisienne juste avant le début du confinement et au début de celui-ci = « *Disposer de ces données est très important afin de mieux conseiller les décideurs publics sur la manière dont ils doivent allouer les ressources de santé et pour les informer sur les régions les plus vulnérables* ».

- <u>Toutes ces études statistiques étant agrégées et anonymes, elles échappent aux règles s'appliquant aux traitements de données personnelles : en effet, le propre d'une donnée personnelle est d'être rattachable à une personne physique identifiée ou identifiable</u>.

FOCUS SUR LA RECONSTITUTION DE LA CHAÎNE DE CONTAMINATION = STOPCOVID / TOUSANTICOVD

Attention, il ne s'agit pas de *contact tracking* parfois utilisé dans le débat public mais d'un *contact tracing* :

l'application ne permet pas la géolocalisation des personnes : il s'agit d'établir, grâce à la technologie Bluetooth, un historique de proximité entre différentes personnes équipées de l'application, auquel nul n'a accès, pas même le propriétaire du téléphone

- Concrètement : une fois l'application téléchargée, celle-ci enregistre, de façon anonyme, le nom de code des personnes croisées : si l'une d'elles est testée positive au Covid-19, elle le déclare dans l'application, qui envoie une notification et invite le destinataire à se faire tester. On ne peut pas savoir qui a est à l'origine de la contamination et nul n'aura accès à la liste des personnes contaminées.

- AVIS préventif de la CNIL : la collecte et le traitement des données opérés par l'application doivent revêtir une durée limitée à l'utilité du dispositif au regard de ses finalités, les données devant être supprimées dès lors que l'utilité de l'application ne sera plus avérée.

AVIS DE LA CNIL du 20 juillet 2020

- L'application respecte les principes essentiels du traitement de données personnelles mais…

→ Mise en demeure adressée au ministère de l'intérieur car :

- Caractère incomplet :
  - du contrat de sous-traitance,
  - de l'analyse d'impact,
  - de l'information fournie aux utilisateurs concernant les destinataires des données,
  - des opérations de lecture des informations présentes sur les équipements terminaux,
  - le droit de les refuser.

- Demande la généralisation de la nouvelle version de l'application dans laquelle le filtrage de l'historique de contacts est opéré au niveau du téléphone de l'utilisateur et non plus du serveur central

→ Prise en compte des remarques par le ministère = clôture de la mise en demeure

ET APRES LE COVID ?

Quelques chiffres :

15 millions de visiteurs attendus en Ile-de-France, 600.000 spectateurs munis de billets…
Les Jeux Olympiques du 26 juillet au 11 août 2024 vont rassembler un nombre record de sportifs, officiels, spectateurs, touristes…

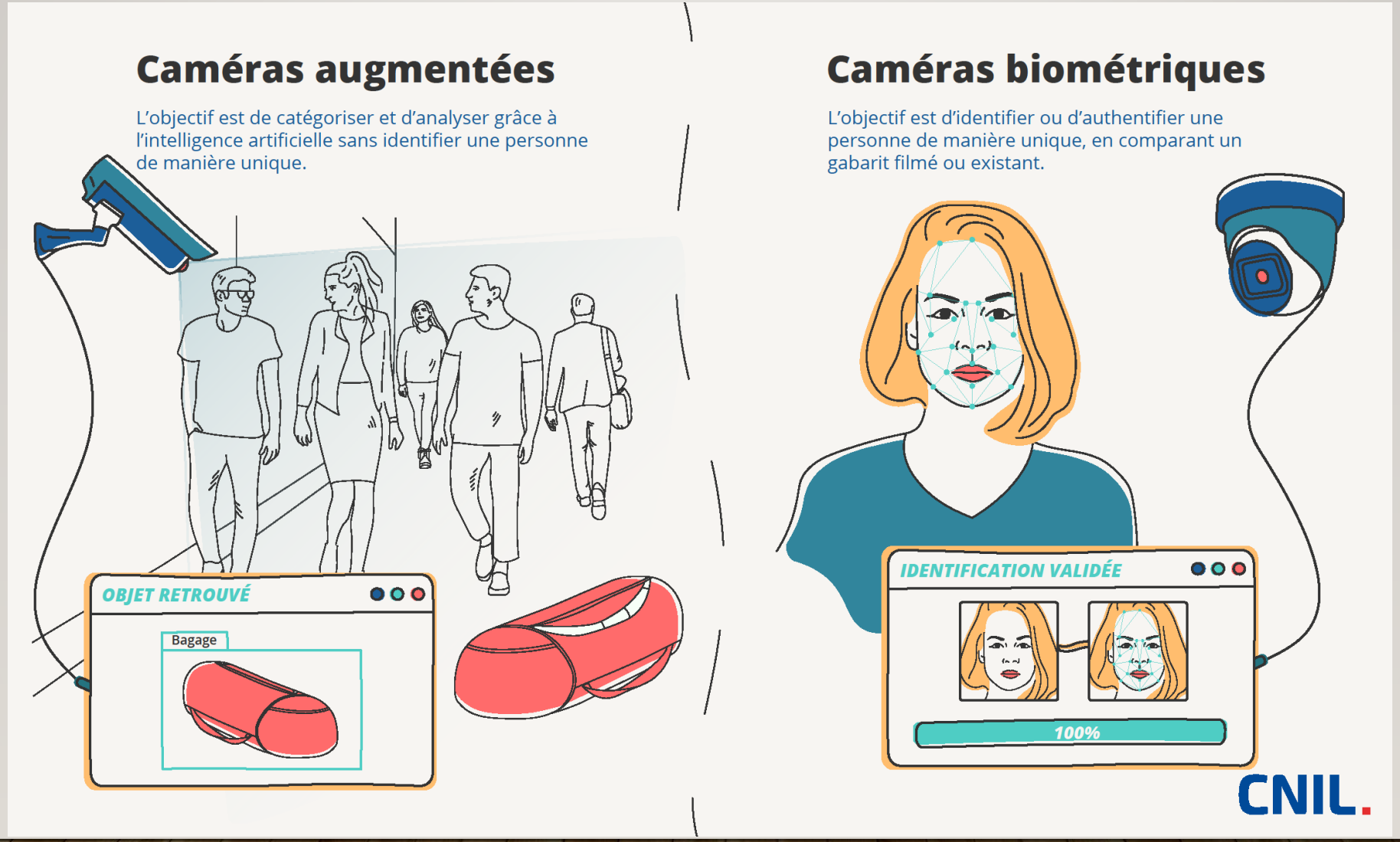
Question centrale : comment gérer la sécurité de l'événement ?

Position du ministère de l'intérieur :

- les Jeux olympiques impliquent la mise en place de mesures de sécurisation accrues de certains lieux ;
- la multiplicité des lieux concernés et le niveau de sécurité attendu rendent nécessaire l'optimisation de l'emploi des forces de sécurité intérieure et des forces de sécurité civile ;
- Seul le traitement en temps réel, par des traitements algorithmiques, des images issues des dispositifs de vidéoprotection et des drones sont de nature à permettre cette optimisation ;
- Il est nécessaire de permettre l'utilisation des dispositifs de *caméras augmentées* pour sécuriser l'ensemble des manifestations sportives, récréatives et culturelles.

D'où la loi relative aux jeux Olympiques et Paralympiques de 2024 **promulguée le 19 mai 2023**.

Une mesure attire tout particulièrement l'attention dans le texte (article 10) :
le recours à des caméras dites augmentées pour assurer la sécurité des grands évènements.



Objectif de ces caméras : « *détecter, en temps réel, des évènements prédéterminés susceptibles de révéler des risques ou de les signaler* ».

Exemples : détecter des mouvements de foules, un sac abandonné, une personne isolée et statique ou des comportements suspects dans des lieux accueillant des manifestations, à leurs abords et dans les transports en commun…

Interdiction d'utiliser une technique de reconnaissance faciale, ni aucun système d'identification biométrique

Mais le recours à cette nouvelle technologie à des fins de prévention du terrorisme et d'atteinte à la sécurité des personnes est inédit en France

Position d'alerte de la CNIL : « *Le déploiement dans l'espace public de « caméras augmentées » présente* ***des risques nouveaux pour la vie privée.*** *En effet, une généralisation non maîtrisée de ces dispositifs, par nature intrusifs, conduirait à un risque de surveillance et d'analyse généralisée dans l'espace public susceptible de modifier, en réaction, les comportements des personnes circulant dans la rue ou se rendant dans des magasins* ».

Position de la CNIL = il est nécessaire de **fixer des lignes rouges**.

Avis de la CNIL du 8 décembre 2022

La CNIL a validé le dispositif aux conditions suivantes :

- un déploiement expérimental ;
- limité dans le temps et l'espace ;
- pour certaines finalités spécifiques et correspondant à des risques graves pour les personnes ;
- l'absence de traitement de données biométriques ;
- l'absence de rapprochement avec d'autres fichiers ;
- l'absence de décision automatique : les algorithmes ne servent qu'à signaler des situations potentiellement problématiques à des personnes qui procèdent ensuite à une analyse humaine.

La loi a été validée par le Conseil constitutionnel (décision n° 2023-850 DC du 17 mai 2023)

« *D'autre part, les dispositions contestées prévoient que les traitements algorithmiques ne mettent en oeuvre aucune technique de reconnaissance Faciale* »

« *Par ailleurs, les traitements ne peuvent procéder à aucun rapprochement, à aucune interconnexion ni à aucune mise en relation automatisée avec d'autres traitements de données à caractère personnel.* »

« *En dernier lieu, d'une part, les traitements algorithmiques procèdent exclusivement à un signalement d'attention* »

« *Les dispositions contestées prévoient que les traitements ne peuvent fonder, par eux-mêmes, aucune décision individuelle ni aucun acte de poursuite et demeurent en permanence sous le contrôle des personnes chargées de leur mise en œuvre* »

Pourquoi faut-il rester vigilants ?

La vigilance demeure car :

Si les garde-fous instaurés par la loi existent, leur mise en pratique devra être surveillée.

Quel sont les risques ?

Le recours à des dispositifs de caméras augmentées et d'intelligence artificielle sera immanquablement confié à des prestataires externes (sous-traitants), experts dans ces domaines.

Attention à l'externalisation qui implique le recours à des sous-traitants extérieurs.

Ils sont potentiellement les maillons faibles de la chaine (et quid de la localisation des données ?).

Attention aux chaines de sous-traitance et aux personnes autorisées à accéder !

Mise en place par la CNIL d’un accompagnement renforcé :

Les prestataires qui seront sélectionnés par les pouvoirs publics pour assurer cette gestion des foules, devront passer par un **accompagnent dit renforcé** de la CNIL, une sorte de contrôle permanent.

En théorie, cette expérimentation ne saurait en aucun cas préjuger d’une éventuelle pérennisation de ces systèmes.

L’autorisation de la vidéosurveillance algorithmique courre jusqu’au 31 mars 2025, soit plus de sept mois après la clôture des JO.

Tout événement « *particulièrement exposé à des risques d’actes de terrorisme ou d’atteintes graves à la sécurité des personnes* » pourrait donc être surveillé par la vidéoprotection intelligente jusqu’en 2025.

La Commission travaille actuellement à l’élaboration d’une doctrine générale en matière d’intelligence artificielle afin d’accompagner les responsables de traitement, et qui se traduira notamment par la publication de recommandations dans le courant de l’année 2023.

Et après les JO ?

Rédaction d'un rapport d'évaluation de la loi avec deux conclusions possibles :

soit on décide de tout stopper soit on prolonge l'expérimentation.

Il est tout à fait possible que ce régime d'exception devienne le droit commun = on pourrait également l'assouplir ou le rendre plus strict si des failles sont identifiées.

Quelle sont les lignes rouges à ne pas franchir ?

1- Il ne peut y avoir de décision automatisée prise par l'algorithme. L'algorithme doit se contenter de faire remonter les images aux humains qui prendront une décision

2- Interdiction de la reconnaissance faciale et de la biométrie

3- Interdiction de croiser les traitements par algorithme avec les fichiers de police, de gendarmerie ou de renseignement.

Bibliographie

Antoine Béguin, « La protection des données personnelles pendant le confinement et le déconfinement », Les Cahiers de l'Association Française des Auditeurs de l'Académie Internationale de Droit constitutionnel, 2021.