RATP

NOTE

10 mars 2022

OBSERVATIONS RELATIVES A LA CONSULTATION PUBLIQUE DE LA CNIL SUR LES CAMERAS INTELLIGENTES DANS LES ESPACES PUBLICS

L'objectif de cette note est de proposer à la CNIL des axes de réflexion pour assouplir et préciser la position soumise à consultation publique.

La RATP a déjà proposé plusieurs cas d'usage en essayant d'adapter les conditions de gestion du droit d'opposition, mais les conditions de réalisation sont difficilement gérables dans une phase de généralisation.

Par ailleurs les cas d'usage encadrés par la directive Police Justice nécessitent une analyse particulière sur laquelle la RATP, en partenariat avec l'autorité régulatrice des transports, souhaite apporter là aussi des axes de propositions d'application plus souple des exigences législatives et réglementaires dans le strict respect des libertés publiques.

I. L'utilisation de la vidéo intelligente dans le cadre de finalités régies par le RGPD

A - La nécessité d'une norme autorisant et encadrant la plupart des dispositifs

1. *La position de la CNIL*

La CNIL estime que la plupart des dispositifs de vidéo intelligente « *nécessitaient, pour pouvoir être légalement mis en œuvre, l'existence ou l'intervention d'un texte de nature législative ou réglementaire les encadrant* » notamment car ils « *se heurtent généralement en pratique à l'obligation prévue par le RGPD de garantir aux personnes concernées la possibilité de s'opposer au traitement de leurs données* ».

En effet, les conditions d'exercice du droit d'opposition lui « *apparaissent la plupart du temps, difficilement acceptables* », « *font souvent peser une contrainte trop lourde sur les personnes* » ou bien impliquent un « *traitement de données supplémentaire potentiellement plus intrusif* ». « *Par ailleurs, l'existence même d'un droit d'opposition pourrait, dans certains cas, apparaître antinomique avec l'objectif poursuivi par le traitement : il en va ainsi de toutes les fois où il s'agit, pour des gestionnaires de lieux ouverts au public, de détecter des comportements anormaux, suspects ou dangereux à des fins de sécurisation des personnes et des biens* ».

2. *La position de la RATP*

Pour rappel, le réseau RATP s'étend, actuellement, sur l'ensemble de la région Île-de-France, avec 16 lignes de métro, 2 lignes de RER, 8 lignes de tram, 354 lignes de bus et fonctionne 24h/24, et permet le transport de plus de 3,3 milliards de passagers par an.

La RATP qui a des obligations contractuelles vis-à-vis d'IDFM, autorité organisatrice des transports en Île-de-France (comme ses filiales avec d'autres autorités en France et dans l'Europe), en matière de régularité, de sécurité, d'information voyageurs, met en œuvre des expérimentations, qui pourraient potentiellement être généralisées en cas de bilan positif, afin d'améliorer l'information, la sécurité et le confort des voyageurs, généralement les personnes concernées.

Ces traitements sont mis en œuvre par la RATP dans le cadre de son activité d'opérateur de transport multimodal et donc dans le cadre de sa mission de service public, sur des thématiques qui correspondent à des préoccupations des usagers. De plus, ils n'ont pas de finalités qui seraient susceptibles d'affecter les garanties fondamentales apportées aux citoyens pour l'exercice des libertés publiques. Ils sont mis en œuvre dans l'intérêt de toutes les parties prenantes et, en premier lieu, des personnes concernées par ces traitements, les voyageurs qui utilisent les transports en communs.

Ainsi les cas d'usage de caméras filmant la voie publique, pour participer à la sécurité de circulation des véhicules autonomes (totalement ou partiellement) qui répondent à des finalités couvertes par les textes de la loi LOM et de la loi PACTE[1] sur l'exploitation de ce type de véhicule, n'ont pas de caractère intrusif bien au contraire. Par contre à la lecture de la position de la CNIL, il subsiste un flou sur les critères applicables aux cas d'usages associés qui participent à la sécurisation de la circulation du véhicule mais aussi à la gestion du domaine public : entretien des trottoirs, type de véhicules légers partageant la voie (vélo, voiture, trottinette...). La compatibilité des finalités au sens du considérant 50 du RGPD doit pouvoir se mesurer clairement, notamment à l'aide d'une position de droit souple de la CNIL.

[1] La base légale (LOI PACTE) : décret rectificatif de l'article 125 de la PACTE sur les expérimentations de Véhicules à délégation Totale ou Partielle de Conduite.
Article 31 de la Loi LOM, ordonnance 2021-443 du 14 avril 2021 et décret d'application 2021-873 du 29 juin 2021

De même des systèmes de comptage de voyageur dans les matériels roulant (Bus principalement) pourraient être utilisés pour réaliser des analyses statistiques sur la connaissance de trajets origine/destination, afin d'améliorer l'offre de transport, en utilisant une caméra avec IA. Le projet de proposition permet, a priori, de clarifier les conditions de réalisations de ce type de comptage statistique, qui peut permettre d'adapter l'offre de transport en fonction des types de trajets (scolaires, travail, jours de marché...). Les critères énoncés, notamment le délai entre la production et l'exploitation opérationnelle de la statistique, sont applicables.

La RATP, dans la conception de ces traitements, est soucieuse de mettre en œuvre des modalités de traitement les moins intrusives possible, par exemple en jouant sur la position de la caméra et/ou sur la résolution des images captées et analysées par l'algorithme, et d'apporter des garanties fortes aux personnes concernées, notamment l'anonymisation des données collectées à très bref délai, la mise en place d'une information claire et spécifique, et le respect des droits de personnes. Dans le cadre de futures expérimentations , il est également prévu de mettre en place un comité éthique pour la prise en compte de ces enjeux dans le cadre des expérimentations envisagées.

Cependant, concernant le droit d'opposition, si dans le cadre de certains traitements, il est possible de l'organiser en prévoyant par exemple, un itinéraire de substitution permettant aux usagers de ne pas être exposés à la zone d'expérimentation[2], il peut en effet être difficile, dans d'autres cas de répondre à l'exigence de ce droit d'opposition, notamment lorsque la généralisation du traitement est envisagée et dans un contexte où la participation des personnes est nécessaire à l'efficacité du dispositif ayant pour finalité l'amélioration de l'information ou du confort des voyageurs.

L'acceptation par les voyageurs de ce type d'expérimentation est assez satisfaisante comme le montre le retour d'expérience sur l'expérimentation X.

Le projet X

Le projet X vise à permettre de détecter et d'alerter en temps réel les patrouilleurs vidéo, via l'utilisation d'un système de vidéoprotection augmenté, lorsqu'un bagage est abandonné, puis de retrouver et suivre le ou les propriétaires du bagage abandonné, et de coordonner les équipes opérationnelles pour retrouver le propriétaire s'il est toujours en gare.

A ce titre, il illustre bien les enjeux de la mise en œuvre d'un dispositif de vidéo augmentée.

Un tel traitement, avec la finalité de retrouver le propriétaire d'un bagage abandonné le plus rapidement possible pour ne pas impacter le trafic voyageur, relève du RGPD.

La captation des données personnelles est déjà prévue et encadrée par un texte de nature législative (le code de la sécurité intérieure). C'est l'algorithme, visant à analyser la donnée captée afin de détecter le fait de sûreté, qui n'est prévu par aucun texte. Pour autant, il s'inscrit dans une finalité compatible (Considérant 50 RGPD) avec celle ayant permis initialement de capter la donnée. L'algorithme vient simplement procéder à un pré-tri en vue de l'analyse humaine du flux vidéo par l'agent en charge de la surveillance des images.

Dans ce contexte, la CNIL estime qu'il est nécessaire d'avoir un texte législatif ou a minima réglementaire pour mettre en œuvre ce type de traitement, en l'absence de mise en œuvre d'un droit d'opposition adapté. Cependant, il apparait difficilement envisageable pour la RATP, et les opérateurs de transport public de manière générale, de pouvoir bénéficier d'un texte encadrant de manière spécifique chacun des nouveaux traitements ou expérimentations envisagés.

---

[2] Comme dans le cadre du projet X (dispositif expérimental d'analyse en temps réel de flux vidéo par des algorithmes d'intelligence artificielle afin de calculer le taux d'affluence des usagers et leur répartition sur un quai de métro) présenté par la RATP à la CNIL dans le courant de l'année 2021.

A minima, les expérimentations, conçues dans le respect des règles de protection des données et à certaines conditions (par exemple, la présentation préalable de l'expérimentation à la CNIL qui pourrait vérifier la qualité des garanties pour les droits et libertés des personnes), pourraient être dispensées de l'exigence d'un cadre législatif ou réglementaire préalable car ces expérimentations permettent justement de nourrir la réflexion du législateur sur la façon d'encadrer de manière pertinente les traitements qui seraient mis en œuvre de manière durable, en prenant en compte les bilans et retours d'expérience.

Par ailleurs, la RATP estime que la CNIL pourrait assouplir sa position concernant les traitements mettant en œuvre des garanties fortes comme l'anonymisation à bref délai des données collectées et permettant ainsi de minimiser les risques pour les personnes concernées. Elle pourrait considérer que ce type de traitements pourrait, sous certaines conditions (notamment le respect des règles de *Privacy by Design* et *by Default bien sûr, mais aussi imposer un délai d'expérimentation limité à quelques mois*), bénéficier d'un régime dérogatoire permettant d'exclure le droit d'opposition.

Une interprétation souple et limitative fut d'ailleurs appliquée, certes avant l'entrée en vigueur du RGPD, pour les dispositifs de mesure d'audience proposant une anonymisation à bref délai des données. En effet, la CNIL avait publié le 19 août 2014 sa doctrine sur la « Mesure de fréquentation et analyse du comportement des consommateurs dans les magasins ». Elle avait ainsi considéré que, pour les dispositifs décrits (caméras placées sur des panneaux publicitaires pour mesurer leur audience), et sous réserve de traiter les images à la volée pour produire des données anonymes et de fournir une information claire aux personnes dans les lieux concernés, « l'exercice du droit d'accès, de rectification et d'opposition ne peut pas s'appliquer ». Elle avait une analyse similaire pour les dispositifs de mesure de fréquentation des magasins via des boîtiers captant les adresses MAC des téléphones portables pour établir des statistiques de fréquentation : sous réserve que des mesures soient prises pour garantir l'anonymat des personnes (données supprimées à bref délai) et d'une information claire des personnes, « lorsque les données sont anonymisées, l'exercice du droit d'accès, de rectification et d'opposition ne peut pas s'appliquer ».

Cette doctrine avait notamment trouvé à s'appliquer dans la délibération n° 2015-255 du 16 juillet 2015 (JC Decaux) : « ***Dès lors, les données n'étant pas anonymisées, le traitement*** *de données à caractère personnel qui serait mis en œuvre par la société JCDecaux* ***doit respecter les droits*** *des personnes concernées* », et dans la délibération n° 2017-145 du 09 mai 2017 (Retency) : « *La Commission précise sur ce point que* ***dans la mesure où les données collectées ne permettent pas d'individualiser une personne,*** *les dispositions des articles 38 à 40, à savoir* ***l'exercice des droits d'accès, de modification et d'opposition, ne trouvent pas à s'appliquer*** ».

B - L'exception des traitements à des fins statistiques

1. *La position de la CNIL*

La CNIL ne fait exception à l'exigence de prévoir un droit d'opposition que pour les traitements de données à des fins statistiques au sens du RGPD et de la Loi Informatique et Libertés. Ces traitements peuvent en effet bénéficier sous conditions d'un régime dérogatoire permettant d'exclure le droit d'opposition des personnes concernées.

« *Pour que ces traitements algorithmiques constituent un traitement de données à des fins statistiques, la CNIL considère qu'ils devront répondre aux conditions cumulatives suivantes :*

- *En premier lieu,* ***les résultats statistiques obtenus*** *à partir du traitement de données* ***ne doivent pas constituer des données à caractère personnel mais des données agrégées et anonymes*** *au sens de la réglementation sur la protection des données.*

- *En second lieu, le traitement n'a une finalité statistique que **s'il tend à la production de ces données agrégées pour elles-mêmes, afin de permettre éventuellement leur utilisation dans un second temps**. Le fait, pour un dispositif qui se fonde sur une donnée agrégée, d'avoir une portée opérationnelle, pour **permettre une réaction concrète en temps réel, lui fait généralement perdre sa qualification de « statistique »** et donc le bénéfice du régime dérogatoire afférent. En principe, **la CNIL considère qu'il doit exister un délai entre la captation des données par le dispositif permettant la production des résultats statistiques et leur exploitation** par le responsable du traitement ».*

Par ailleurs la CNIL précise que « en cas d'utilisation de caméras augmentées pour calculer des statistiques sur un flux de personnes, **l'éventuelle mesure prise par le responsable de traitement s'applique à un groupe de personnes nécessairement différent du groupe sur lequel porte l'information** (la « statistique »). En outre, ainsi que le rappelle le considérant 162 du RGPD, les **résultats statistiques ne sont en principe pas utilisés en tant que tels à l'appui d'une décision ou mesure** concernant une personne physique en particulier ».

2. La position de la RATP

A la suite de l'expérimentation X, une autre expérimentation, présentée également à la CNIL dans le courant de l'année 2021, est envisagée pour mesurer la densité à bord d'une ligne de métro via une caméra qui capture des images du train après son départ de la station. La mesure de densité est réalisée depuis l'extérieur du train au travers des fenêtres afin de fournir aux usagers des statistiques liées à cette affluence : affichage à quai de l'affluence de chaque voiture de la prochaine rame et éventuellement, suggestion à l'utilisateur d'une heure de départ différente lors des recherches d'itinéraires dans l'application mobile. Pour la RATP, il s'agit également d'optimiser ainsi la régulation du trafic et de gérer au mieux les incidents.

Dans le cadre de cette expérimentation projetée, les personnes concernées par le traitement (celles qui sont comptées à bord du train) ne sont pas celles qui reçoivent l'information (personnes à l'entrée de la station, sur le quai précédent de la ligne ou bien personnes qui consultent des recherches d'itinéraires dans l'application mobile). Par ailleurs, les personnes qui seront impactées par les mesures de régulation et de gestion des incidents ne seront pas les personnes qui ont été soumises au traitement de production des données statistiques.

La CNIL considère également qu'un certain délai doit exister entre la captation des données pour produire la statistique et l'exploitation de cette statistique par le responsable de traitement. Elle donne l'exemple de la mesure de fréquentation par les centres commerciaux pour l'affichage ultérieur (et non en temps réel) de publicités adaptées à cette fréquentation, en indiquant un délai d'une semaine (adaptation des publicités chaque week-end en fonction des statistiques de fréquentation des week-ends précédents). Si ce délai d'une semaine est pertinent dans le contexte de la fréquentation des centres commerciaux où les consommateurs restent exposés pendant de longues durées aux caméras dans l'enceinte des centres, du fait de la présence de nombreux commerces, il n'en va pas de même pour la fréquentation des espaces de la RATP (notamment les quais et trains) où les usagers ne font que transiter. Ils sont de passage et n'ont pas vocation à rester de manière longue dans ces espaces.

De plus la finalité d'information ou d'amélioration des conditions transports publics ne sont pas aussi intrusives que la finalité marketing d'un centre commercial.

De fait, les personnes qui reçoivent les informations liées à l'affluence ne sont pas celles qui ont été concernées par le traitement de captation et de comptage, quelques minutes précédemment. Ainsi dans le contexte d'un transporteur, un délai raisonnable entre le traitement de production de la statistique via les images captées et l'exploitation de cette statistique, à savoir l'affichage de l'information à d'autres usagers, serait davantage pertinent.

Ce délai, variable selon la finalité d'exploitation de la statistique, devrait être en cohérence et en adéquation avec la dynamique d'un réseau de transport urbain permettant de produire l'information voyageur en juste temps.

Enfin si la finalité est exclusivement liée à l'information voyageur, cette production de statistiques n'a pas d'autres but que de partager le résultat agrégé avec le voyageur (comme pour SYTADIN et l'information routière par exemple), et la notion de délai à respecter parait excessive au regard de la notion de statistique.

Dans le cadre de l'expérimentation X et d'une expérimentation de mesure de l'affluence à bord, la finalité du traitement est d'obtenir à partir des images vidéo des statistiques et de partager ces statistiques sur l'affluence avec les voyageurs par le biais d'affichage afin qu'ils puissent prendre leurs dispositions. Aucune décision concernant les personnes concernées n'est prise par la RATP dans le cadre de ces traitements, sur la base des données collectées et agrégées.

Ainsi, la RATP estime que les traitements ayant pour but de fournir des données agrégées statistiques qui seront partagées avec les usagers (qui ne sont pas les personnes concernées) et qui ne servent pas à prendre des mesures concernant ces personnes, pourraient bénéficier d'un régime dérogatoire permettant d'exclure le droit d'opposition, à la condition de respecter les dispositions de l'article 116 du décret n° 2019-536 du 29 mai 2019, et notamment dans les cas où l'exercice du droit d'opposition risque « de rendre impossible ou d'entraver sérieusement la réalisation des finalités spécifiques et où de telles dérogations sont nécessaires pour atteindre ces finalités ».

C - L'exception des traitements à des fins de recherche

Ce point n'est pas évoqué dans la position proposée par la CNIL, mais le périmètre de cette exception définie à l'article 21 6 du RGPD peut correspondre à des cas d'usage pour lesquels la RATP est en partenariat avec des organismes de recherche ou des start-ups.

Il est en effet possible qu'après les premières étapes d'apprentissage d'un algorithme en laboratoire, La RATP soit intéressée par une phase d'expérimentation et de mise au point de l'apprentissage de l'algorithme en situation réelle.

Même si le résultat peut être parfois la production de statistiques, ce qui rejoint le point précédent, les phases d'apprentissage peuvent correspondre à des besoins d'expérimentation répondant à la notion de traitement de recherche, au sens du considérant 159[3].pour lesquels la gestion du droit d'opposition fausserait l'apprentissage.

Ce type d'exception et de situation ne pourrait correspondre bien évidemment donc à des expérimentations temporaires ayant mis en place des garanties appropriées par ailleurs, déjà évoquée dans les points précédents (anonymisation, minimisation...).

[3] « développement et la démonstration de technologies, la recherche fondamentale, la recherche appliquée et la recherche financée par le secteur privé. Il devrait, en outre, tenir compte de l'objectif de l'Union mentionné à l'article 179, paragraphe 1, du traité sur le fonctionnement de l'Union européenne, consistant à réaliser un espace européen de la recherche » (considérant 159, RGPD).

II. L'utilisation de vidéo intelligente dans le cadre de finalités régies par la directive police-justice

La CNIL indique au 4.1.4 que le CSI « *n'a pas d'effet limitatif sur les projets poursuivant des finalités sans lien direct avec la préservation de l'ordre et de la sécurité publics* » et que le régime de vidéoprotection prévu par le CSI, y compris ses dispositions pénales, n'interdit pas, par lui-même, toute utilisation de la vidéo augmentée.

Elle considère également au 4.1.6 que « *les caméras encadrées par le CSI ne sont pas non plus de facto « autorisées » à utiliser des technologies de vidéo « augmentée » pour les finalités ayant permis leur implantation : le législateur n'a clairement entendu régir et autoriser que des dispositifs de vidéo « simples », qui ne captent pas le son et ne sont pas équipés d'algorithmes d'analyse automatique.* »

La CNIL considère ainsi que les vidéos augmentées doivent respecter l'ensemble de la réglementation applicable en matière de données à caractère personnel (c'est-à-dire le RGPD et la loi informatique et libertés).

Notre objectif est de proposer à la CNIL des axes d'assouplissement de sa position afin de permettre de mettre en place des expérimentations pour des finalités d'amélioration des conditions de transport des usagers dans un cadre moins contraint et de déployer, sans avoir à légiférer, les expérimentations à finalité sécuritaire, dans le cadre du Lab_IA.

A – Des traitements mis en œuvre par le service interne de sécurité (SIS) de la RATP

La vidéoprotection augmentée exploitée par le service interne de sécurité de la RATP (SIS) entrerait dans le cadre de la **Directive police-justice** :

- Elle vise un traitement des données à caractère personnel à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales ;
- Le SIS de la RATP constitue une autorité publique compétente au sens de la loi informatique et libertés, comme cela est d'ailleurs précisé par votre doctrine ;

L'utilisation d'une vidéoprotection intelligente par le SIS ne serait donc pas soumise au RGPD, et notamment au droit d'opposition.

Le traitement devra néanmoins respecter les obligations suivantes :

- mettre en œuvre des mesures techniques et organisationnelles appropriées pour que le traitement soit conforme à la directive (article 19)
- mettre en œuvre une protection des données dès la conception et par défaut : *privacy by design and by default* (article 20)
- faire appel à des sous-traitants qui présentent des garanties suffisantes et qui ne pourront agir que sur instruction du responsable du traitement (article 22)
- tenir un registre des activités de traitement (article 24)
- mettre en œuvre des mesures de journalisation (article 25)

- coopérer avec l'autorité de contrôle, à la demande de celle-ci, dans l'exécution de ses missions (article 26)
- **réaliser une analyse d'impact relative à la protection des données lorsque le traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques (article 27)**
- consulter préalablement l'autorité de contrôle dans les cas énumérés à l'article 28 de la directive
- mettre en œuvre les mesures appropriées afin de garantir un niveau de sécurité adapté au risque, en particulier pour les données dites sensibles (article 29)
- notifier à l'autorité de contrôle les violations de données à caractère personnel dans les meilleurs délais, et si possible au plus tard dans un délai de 72h après en avoir pris connaissance, en cas de risques pour les droits et libertés d'une personne physique (article 30)
- communiquer à la personne concernée la violation de ses données à caractère personnel lorsqu'il y a un risque élevé pour les droits et libertés de celle-ci (article 31)
- désigner un délégué à la protection des données dans les conditions prévues à l'article 32 de la directive
- respecter les conditions définies pour le transfert de données à caractère personnel vers des pays tiers ou à des organisations internationales (articles 35 et suivants)
- établir, le cas échéant et dans la mesure du possible, une distinction claire entre les données à caractère personnel de différentes catégories de personnes concernées, comme par exemple les personnes reconnues coupables d'une infraction pénale, les personnes victimes d'une infraction pénale, les tiers à une infraction pénale etc (article 6)
- distinguer entre les données à caractère personnel (données fondées sur des faits/données fondées sur des appréciations personnelles) et vérifier la qualité des données (article 7)
- le **traitement doit être licite**, c'est-à-dire **nécessaire à l'exécution d'une mission effectuée par une autorité compétente**, pour les finalités prévues aux fins de la présente directive, et fondé sur le droit de l'Union ou le droit d'un Etat membre (article 8)
- le traitement portant sur des données sensibles ne peut être autorisé qu'en cas de **nécessité absolue** (article 10)
- informer les usagers du caractère augmenté des caméras de vidéoprotection et des finalités poursuivies dans des termes clairs et simples

L'article 8 de la directive police-justice, relatif à la licéité du traitement prévoit que :

« 1. Les États membres prévoient que le traitement n'est licite que si et dans la mesure où il est nécessaire à l'exécution d'une mission effectuée par une autorité compétente, pour les finalités énoncées à l'article 1er, paragraphe 1, et où il est fondé sur le droit de l'Union ou le droit d'un État membre.

2. Une disposition du droit d'un État membre qui réglemente le traitement relevant du champ d'application de la présente directive précise au moins les objectifs du traitement, les données à caractère personnel devant faire l'objet d'un traitement et les finalités du traitement. »

Il apparaît dès lors que les articles L.223-1 et L.251-2 du code de la sécurité intérieure répondent à cette obligation dans la mesure où ces dispositions de nature législative fixent :

- L'objectif du traitement : la transmission et l'enregistrement des images ;
- Les données personnelles objets du traitement : les images des personnes captées par une caméra dans des lieux et établissements ouverts au public ;
- Finalité du traitement : assurer la sécurité des personnes et des biens dans les lieux et établissements particulièrement exposés à des risques d'agression, de vol ou d'actes de terrorisme ;

De même, la partie réglementaire du code de la sécurité intérieure (article R.251-7 et suiv.) détermine les conditions d'exploitation des systèmes de vidéoprotection installés sur le fondement des articles L.223-

1 et L.251-2, pose les conditions de contrôle de ces systèmes ainsi qu'elle règlemente le droit d'accès afin de garantir une information claire et permanente des personnes filmées.

En adéquation avec cette réglementation, la mission du SIS, prévue par l'article L.2251-1 du code des transports, est bien de *veiller à la sécurité des personnes et des biens, de protéger les agents de l'entreprise et son patrimoine et de veiller au bon fonctionnement du service.*

Comme indiqué précédemment, le réseau RATP s'étend, actuellement, sur l'ensemble de la région Ile-de-France, avec 16 lignes de métro, 2 lignes de RER, 8 lignes de tram, 354 lignes de bus et fonctionne 24h/24, et permet le transport de plus de 3,3 milliards de passagers par an.

Afin d'assurer plus efficacement la sécurité des personnes et des biens sur le réseau et d'agir en complémentarité avec les agents du GPSR qui patrouillent dans nos espaces et matériels roulants, la RATP a déployé plus de 50 000 caméras sur son réseau.

Demain, avec les prolongements de lignes et le réseau du Grand Paris Express dont le SIS RATP doit assurer la sécurisation en vertu de la loi n°2019-1428 du 24 décembre 2019 d'orientation des mobilités (article L.2251-1-2 code des transports), l'utilisation de la vidéo augmentée rendra plus efficiente encore la mission du SIS RATP.

L'identification de faits de sécurité par les agents du PC sûreté sur l'ensemble du réseau relève avant tout d'alertes humaines, ce qui peut retarder la prise en charge effective de ces faits par les équipes du GPSR en coordination avec le PC sûreté.

Ainsi, la mise en place d'algorithmes sur les dispositifs de vidéoprotection classiques existants, permet d'alerter plus rapidement les agents du PC SUR au regard de la détection de faits de sûreté. Elle constitue ainsi une nécessité afin d'exercer encore plus efficacement la mission dévolue au SIS RATP par le code des transports, et donc afin de préserver la sécurité des personnes et des biens sur ce réseau.

Il est important de s'interroger véritablement sur la nature de ces caméras dites intelligentes.
L'utilisation d'algorithmes dans le cadre de la vidéo augmenté n'implique pas une prise de décision automatique, mais vise à alerter un opérateur, afin qu'il effectue une levée de doute et coordonne l'action des agents implantés à proximité du lieu de l'évènement de sûreté.

En cela, la vidéo augmentée n'engendre pas davantage de risque pour la liberté des citoyens que le cadre actuel de vidéoprotection du CSI.

De ce fait, la mise en place d'une vidéo intelligente par le SIS RATP dans le cadre exclusif des finalités prévues par le CSI n'apparaît pas incompatible avec les prescriptions de la loi informatique et libertés en ce qu'elle reprend les dispositions de la directive police-justice.

B - Les bases légales et réglementaires de la vidéo intelligente des espaces de transport

1. *La nécessité d'une loi*

Au 4.3.8, la CNIL considère « ***que, dans le prolongement de la jurisprudence du Conseil d'État (caméras piétons : INT 390313 23/09/2015), certains de ces dispositifs, et tout particulièrement ceux mis en oeuvre à des fins de police administrative ou judiciaire – donc de prévention ou de répression d'atteintes à l'ordre public -, soient susceptibles d'affecter les garanties fondamentales apportées aux citoyens pour l'exercice des libertés publiques. La mise en oeuvre de tels dispositifs relève à ce titre des domaines constitutionnellement réservés à la loi (article 34 de la Constitution).***

Il apparaît néanmoins que si, s'agissant des caméras piétons, il n'existait effectivement pas de texte de nature législative, ce cadre existe pour la vidéoprotection à travers les articles L.251-2 et L.223-1 du code de la sécurité intérieure, qui prévoient des finalités limitatives permettant d'assurer une proportionnalité entre la nécessité de la mesure à des fins de police administrative et les atteintes aux libertés fondamentales (droit à la vie privée, liberté d'aller et venir, de se réunir et de manifester).

De ce fait, les exigences constitutionnelles rappelées par la CNIL sont satisfaites par le cadre légal actuel.

2. Sur la nécessité d'un encadrement législatif spécifique au traitement algorithmique des images de vidéoprotection

« 4.3.9. La CNIL considère que la légalité du recours à des analyses algorithmiques d'images de caméras de vidéoprotection, réalisées en temps réel en vue d'une intervention immédiate ou de l'enclenchement de procédures, administratives ou judiciaires par les services de police, est subordonnée à l'existence d'une autorisation et d'un encadrement législatifs spécifiques. »

La RATP considère que les images de vidéoprotection, dont l'exploitation est autorisée sur le fondement des dispositions actuelles du code de la sécurité intérieure, visent notamment à permettre l'analyse en temps réel de ces images par des opérateurs de vidéoprotection en vue de diligenter une intervention immédiate du SIS RATP ou des forces de sécurité intérieure, ou de l'enclenchement de procédures administratives ou judiciaires par les services de police.
L'arrêté préfectoral vaut autorisation de mise en œuvre du système de vidéoprotection conformément au cadre légal prévu par le code de la sécurité intérieure.

La RATP tient également à rappeler que les dispositifs de vidéo augmentée déployés sur la base des images de vidéoprotection « simples » n'impliquent aucunement la captation et l'analyse des sons.

Ainsi, un encadrement législatif supplémentaire serait nécessairement redondant avec les dispositions existantes, dès lors qu'il porterait sur la captation des mêmes images de vidéoprotection et pour les mêmes finalités.

Dès lors, la mise en place d'une analyse algorithmique de l'image dans le cadre des finalités autorisées des systèmes de vidéoprotection conformément aux dispositions des articles L.221-3 et L.251-2 du code de la sécurité intérieure, s'inscrit dans le cadre prévu par les articles 87 et 90 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, ne nécessitant qu'une analyse d'impact relative à la protection des données avec une consultation préalable obligatoire de la CNIL avant mise en place du traitement.

3. Sur le changement de nature et de degré du dispositif de surveillance

« 4.3.10. À cet égard, même en étant limités à la protection de certains événements ou à des finalités de prévention de troubles graves à l'ordre public, ce type de traitements - même temporaires - sont susceptibles de modifier par principe et tellement profondément, la façon dont l'action des services de police influe sur l'exercice par les citoyens de leurs libertés et droits fondamentaux, qu'ils ne peuvent dès lors trouver un fondement juridique suffisant dans les dispositions générales de la loi Informatique et Libertés ou dans le seul pouvoir réglementaire du gouvernement ou, a fortiori, des maires. »

« 4.3.11. Les algorithmes de détection de comportements « suspects » ou infractionnels, au profit de services publics bénéficiant de prérogatives de puissance publique particulières (et notamment de pouvoirs de contrainte et d'engagement de poursuites), emportent un changement de degré et de nature dans la surveillance à distance de la voie publique que le législateur a encadrée pour les caméras « simples ». Ces dispositifs engendrent des risques accrus pour les personnes dépassant la seule problématique de la

protection de leurs données, en touchant à la fois à la sphère pénale (logique répressive) et aux conditions d'exercice de leurs libertés fondamentales (droit à la vie privée, liberté d'aller et venir, de se réunir et de manifester, etc.). »

La RATP estime, qu'il s'agisse de vidéo augmentée ou de vidéoprotection « simple », que les données personnelles faisant l'objet du traitement, ainsi que les atteintes aux libertés qui en découlent, sont identiques.
L'usage d'un algorithme de détection de comportements suspects ou infractionnels ne fait que rendre plus efficient l'objectif initial du traitement par vidéoprotection et l'intervention des services publics bénéficiant de prérogatives de puissance publique particulières, et s'inscrit ainsi dans les intentions du législateur quant à l'encadrement de la vidéoprotection.

L'amélioration de la puissance d'analyse d'un système de vidéo protection ne dénature ni ne change la portée de la vidéo que nous exploitons depuis de nombreuses années.

En effet, que la détection du fait de sûreté soit d'origine humaine ou algorithmique, l'action des services de police, ou du service interne de sécurité de la RATP, sera identique dès lors qu'ils en auront été alertés.
Par ailleurs, l'intervention des autorités compétentes sera nécessairement conditionnée à la confirmation du fait de sûreté par l'opérateur de vidéoprotection, et donc par une analyse humaine postérieure au traitement algorithmique.

De fait, les atteintes aux libertés et droits fondamentaux sont identiques à celles induites par le système de vidéoprotection, seul le canal d'alerte de l'opérateur de vidéoprotection diffère.

Il paraît également pertinent de s'intéresser à l'analyse des différentes typologies de lieux susceptibles de faire l'objet d'une vidéoprotection.

Pour rappel, conformément à l'article L.251-2 du code de la sécurité intérieure, seules les préfectures et les collectivités locales ont qualité pour vidéoprotéger la voie publique. Ces mêmes autorités autorisées à visualiser la voie publique ne pourront déployer un dispositif de vidéo augmentée que dans le cadre de l'article 89 I. de la loi informatique et libertés, et donc sur la base d'une disposition législative ou réglementaire, permettant ainsi, par ce texte, de limiter les atteintes à l'exercice des libertés fondamentales.

A l'inverse, les opérateurs de transport public et le service interne de sécurité de la RATP ne peuvent visualiser que leurs espaces et véhicules, particulièrement exposés à des risques d'actes de terrorisme, d'agressions ou de vols, et dans la seule finalité d'y assurer la sécurité des personnes et des biens, ce qui limite drastiquement les risques d'atteintes aux libertés fondamentales susmentionnés par la CNIL.

Par ailleurs, le déploiement d'un algorithme à des fins de prévention de ces troubles à l'ordre public sera nécessairement conditionné à une analyse d'impact relative à la protection des données à caractère personnel (AIPD) avec consultation préalable de la CNIL conformément à l'article 90 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, interdisant de fait, toutes atteintes disproportionnées auxdites libertés.
Pour rappel, le Conseil constitutionnel considère que *« la prévention d'atteintes à l'ordre public, notamment d'atteintes à la sécurité des personnes et des biens, et la recherche des auteurs d'infractions, sont nécessaires à la sauvegarde de principes et droits de valeur constitutionnelle* [4]».

[4] Décision n°80-127 DC du 20 janvier 1981 « *Loi renforçant la sécurité et protégeant la liberté des personnes* », considérant 56

De ce fait, c'est le rôle de l'AIPD de s'assurer que l'usage d'un algorithme pour analyser les images de vidéoprotection, permette de contribuer à prévenir les atteintes à l'ordre public, tout en préservant les libertés, sous le contrôle et l'arbitrage de la CNIL.

La conciliation équilibrée entre l'objectif de sauvegarde de l'ordre public et l'impératif de protection des droits et libertés fondamentaux est avérée en l'espèce puisqu'un socle législatif et réglementaire encadre le système de vidéoprotection « simple » et que l'AIPD , qui sera nécessairement réalisée, porte une description détaillée du traitement mis en œuvre, comprenant tant les aspects techniques qu'opérationnels, évalue la nécessité et de la proportionnalité concernant les principes et droits fondamentaux et étudie les risques sur la sécurité des données (confidentialité, intégrité et disponibilité) ainsi que leurs impacts potentiels sur la vie privée, ce qui permet de déterminer les mesures techniques et organisationnelles nécessaires pour protéger les données.

4. Sur les garanties minimales des dispositifs de vidéo augmentée

«4.3.12. *Leur nécessité réelle, en fonction de circonstances précises, doit impérativement être évaluée à un niveau plus général que les collectivités publiques décidant de leur mise en place : l'éventuel déploiement de tels dispositifs intrusifs ne doit pas résulter d'une addition d'initiatives, nécessairement sans cohérence. Pour la CNIL,* ***seule une loi spécifique, adaptée aux caractéristiques techniques et aux enjeux en cause, pourrait, à l'issue d'un débat démocratique, décider de leur légitimité et, par la fixation de garanties minimales, prévoir une conciliation équilibrée entre l'objectif de sauvegarde de l'ordre public et l'impératif de protection des droits et libertés fondamentaux.*** »

Il revient à la CNIL, dans le cadre de sa mission prévue par l'article 8 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, de fixer les lignes directrices, les recommandations et les référentiels permettant aux algorithmes de respecter les libertés tout en poursuivant les finalités des systèmes de vidéoprotection prévues par le législateur.

La CNIL pourrait ainsi conditionner le déploiement de tout dispositif de vidéo augmentée à une vérification humaine systématique pour tout fait de sûreté, détecté par un algorithme, et s'assurer ainsi que les traitements respectent scrupuleusement les finalités prévues par le code de la sécurité intérieure.

La CNIL pourrait également prescrire que certains éléments soient expressément exclus du traitement algorithmique, comme la détection d'émotions, la reconnaissance faciale, ou toute donnée personnelle qui n'apparaîtrait pas indispensable au fonctionnement de l'algorithme, à charge pour le législateur, le cas échéant, de les autoriser explicitement.

En effet, les algorithmes de vidéo augmentée pour des finalités de sûreté peuvent présenter des niveaux de risques distincts. Un algorithme qui aurait pour seule finalité de détecter la survenance d'une rixe dans un lieu spécifique, en vue de permettre l'intervention de personnes légalement missionnées, sur vérification d'un opérateur de vidéoprotection, serait tout à fait conforme au droit positif, et strictement proportionné au but recherché, à savoir assurer la sécurité des personnes dans un lieu particulièrement exposé à un risque d'agression.

La RATP sollicite donc de la CNIL la mise en place de recommandations plus spécifiques et adaptées au cas par cas, permettant de distinguer des algorithmes de vidéo augmentée considérés comme étant excessifs au regard des finalités prévues par le code de la sécurité intérieure, et les algorithmes acceptables sous certaines conditions, à charge pour le législateur d'encadrer les algorithmes les plus attentatoires aux libertés (notamment ceux basés sur des technologies de reconnaissance faciale, sur la détection d'émotions...).

La mise en place de telles recommandations permettrait d'établir un socle de caractéristiques communes assurant la cohérence des différents dispositifs, disposant d'un fondement textuel, mis en place dans les différentes collectivités et établissements publics relevant de la directive police – justice.

Enfin, toute utilisation d'un algorithme de vidéo intelligente pour des finalités de sûreté non prévues par le code de la sécurité intérieure, y compris par une autorité publique permettant l'application de la directive police-justice, ne pourra être mise en œuvre que sur la base d'un texte légal ou réglementaire spécifique (par ex : l'expérimentation pour prévenir les suicides).

C. Une illustration dans le cadre des projets de la RATP

La RATP prévoit d'expérimenter l'utilisation de la vidéo augmentée dans certains cas d'usage déterminés

L'expérimentation, puis le déploiement, de tels dispositifs apparaît particulièrement urgente à court terme, au regard de l'échéance des Jeux Olympiques de Paris 2024, qui vont nécessiter la mise en œuvre d'un système de sécurité extrêmement efficace face aux risques, notamment terroristes, induits par l'organisation d'un tel événement, et la sécurisation du déplacement des millions de personnes transitant sur le réseau de transport de la RATP afin de prendre part à cet événement de portée internationale.

La nécessité d'adopter une nouvelle loi spécifique, comme demandé par la CNIL, semble disproportionnée, alors que la captation de données personnelles pour des finalités de sûreté fait déjà l'objet d'un encadrement législatif approprié s'il est assorti d'une AIPD.

De fait, la mise en place d'une AIPD sur la base des dispositions actuelles du code de la sécurité intérieure permettrait de légitimer de tels dispositifs au regard des exigences de la loi informatique et libertés, tout en permettant leur déploiement dans des délais compatibles avec les exigences de sécurité requises par l'organisation des JO de 2024.

- Le X

Le X est un projet d'expérimentation de vidéo augmentée en matière de sûreté réalisé par le service interne de sécurité de la RATP et Ile-de-France Mobilités.

Il vise à pouvoir expérimenter divers cas d'usage de vidéo augmentée dans les infrastructures et véhicules de transport sur le réseau RATP, tels que la détection de rixe ou la détection de vol.

Ces comportements sont systématiquement constitutifs d'un délit dès lors qu'ils sont commis dans les transports collectifs de voyageurs :

- le vol commis dans un véhicule affecté au transport collectif de voyageurs ou dans un lieu destiné à l'accès à un moyen de transport collectif de voyageurs (art. 311-4-7° code pénal) ;
- les violences ayant entraîné une incapacité de travail inférieure ou égale à huit jours ou n'ayant entraîné aucune incapacité de travail dans un moyen de transport collectif de voyageurs ou dans un lieu destiné à l'accès à un moyen de transport collectif de voyageurs (art. 222-13 code pénal).

De ce fait, la prévention et la détection de ces comportements par le SIS RATP par un outil de vidéo augmentée entre bien dans le cadre prévu par la directive police-justice.

Ces cas d'usage s'intègrent aux finalités d'un système de vidéoprotection prévu par l'article L.251-2 du code de la sécurité intérieure :

- Assurer la sécurité des personnes et des biens lorsque ces lieux et établissements sont particulièrement exposés à des risques d'agression ou de vol

Multiplier et automatiser, sous couvert d'un ultime regard d'un opérateur du sûreté, les capacités des dispositifs vidéo classiques pour les cas d'usage prévus ci-dessus, ne modifie pas la nature du système ni ne remet en cause la finalité du système autorisé, qui est d'assurer la sécurité des personnes et des biens dans des lieux et établissements exposés à des risques d'agression ou de vol.

De fait, les mêmes données sont traitées dans le cadre de la vidéoprotection, et de l'algorithme, et pour la même finalité.

Dès lors, le fondement législatif ou réglementaire spécifique exigé par la CNIL pour les finalités poursuivies par le X existe déjà, et apparaît suffisant au regard des finalités envisagées par la RATP, pour permettre le déploiement de telles expérimentations.

L'AIPD qui accompagnera systématiquement ce type de traitement viendra quant à elle rappeler la nécessité et la proportionnalité du dispositif, et encadrer le respect des droits des personnes concernées tels que prévus par les points 4.2.6 et 4.2.7 et 8 de la présente recommandation.

II. Remarques conclusives

La présente note constitue la contribution de la RATP à la consultation de la CNIL sur son projet de position sur les conditions de déploiement des caméras intelligentes dans les espaces publics. La RATP se tient à la disposition des services la CNIL pour exposer plus avant ses arguments en les illustrant dans le cadre d'expérimentations et projets menés ou projetés, seule ou en collaboration avec d'autres transporteurs ou avec IDFM.

Sans un assouplissement de la doctrine actuelle de la CNIL notamment sur l'exigence du droit d'opposition, un certain nombre de traitements projetés par la RATP dans le cadre de sa mission de service public et ayant pour finalité d'améliorer les conditions de transports dans l'intérêt premier des usagers ne pourront être expérimentés ou mis en œuvre du fait de l'impossibilité pour elle et pour les transporteurs de pouvoir s'appuyer sur une diversité de textes législatifs ou règlementaires encadrant de manière précise ou spécifique ces traitements.

À tout le moins la position officielle de la CNIL devrait pouvoir dans sa forme définitive poser des critères plus précis pour pouvoir structurer les cas d'usage qui serait clairement interdits où autorisés selon les conditions définies dans la position. Nous rejoignons en ce sens la SNCF dans sa proposition liminaire sur l'élaboration d'une grille d'analyse en fonction des finalités, des cas d'usage, de la nature des données traitées et de la typologie des traitements envisagés.

Par ailleurs concernant la précision de la CNIL au § 4.2.6.1 selon lequel le choix entre une technologie alternative au système de caméras intelligentes devrait être systématiquement privilégié à partir du moment où celle-ci est moins intrusive, il serait utile de préciser si et comment ce choix doit aussi tenir compte du coût de la technologie de remplacement en question, dans la logique des considérants 83-84 et 94 du RGPD. Ainsi s'il existe une technologie de substitution moins intrusive à l'emploi des caméras intelligentes, le dédoublement de la vidéoprotection existante va s'avérer beaucoup plus couteux en possession, et contraire aux objectifs de maitrise de l'argent public.
Au-delà des axes de réflexion proposés précédemment, la RATP souhaite qu'il soit possible de prolonger cette réflexion après le délai du 11 mars avec la CNIL et les autres partenaires des transports publics car le sujet nécessite des échanges complémentaires pour arriver à finaliser une méthodologie applicable par chacun d'entre nous.

Ces échanges pourraient prendre la forme de bac-à-sable sur le sujet organisé par la CNIL et son laboratoire LINC, la systématisation de l'étude des analyses d'impact avec l'avis des associations de voyageurs pour mesurer l'acceptation sociétale de ce type de projet avec intelligence artificielle.

Il faut aussi relever que le paradoxe du projet de position en l'état permettrait aux centres commerciaux de déployer des traitements avec IA pour des finalités beaucoup plus intrusives que celles que les transporteurs publics dans le cadre des missions de service public cherchent à mettre en place pour le confort et la sécurité des voyageurs.

La plupart de nos actions en matière d'utilisation des caméras intelligentes, s'inscrivent dans un cadre contractuel, sous l'égide d'une autorité publique d'organisation des transports (en Ile de France, et plus généralement en France et en Europe) et que de ce fait, elles visent avant tout à l'amélioration du bien-être social (optimisation de l'offre de transport, amélioration de la régularité, du confort, de l'information voyageurs, de la sécurité ...) et que de ce fait les externalités positives qu'elles génèrent pour la collectivité vont très au-delà des externalités négatives que pourraient leur opposer certains particuliers.