Contribution NEPSIS Engineering à la consultation publique de la CNIL sur les caméras intelligentes dans les espaces publics

NEPSIS engineering est une jeune startup dédiée au développement et à la commercialisation de systèmes de vidéo protection et de vidéo surveillance à base d'intelligence artificielle. Le système NASLE que nous développons est destiné à détecter de potentielles situations d'agressions, de situations violentes entre individus et de comportements dangereux sur la voie publique ou dans des espaces fermés.

Nos clients sont principalement des municipalités (centres de surveillance urbains) et des entreprises privées.

S'agissant de la partie "1. Observations préalables" du projet de position, notre analyse de la situation est que, la multiplication des caméras sur l'espace public génère un flux d'information en très forte augmentation. L'exploitation de ces flux vidéo nécessite de plus en plus de moyens humains pour les visionner et pour détecter des situations nécessitant l'intervention des forces de l'ordre ou de vigiles. Les systèmes automatisés permettent de scruter en temps réel un grand nombre de caméras, d'identifier des situations critiques et de les signaler à un opérateur humain qui sera chargé de les analyser et de déclencher une intervention si nécessaire.

Nous sommes donc confrontés au paradoxe suivant :
Le taux d'incident est extrêmement faible en moyenne. Le travail de surveillance manuelle est très monotone et réparti sur des équipes réduites pour des raisons de coût d'exploitation.
Cependant, en cas d'incident avéré, les opérateurs présents peuvent être confrontés à une charge de travail significative (analyse, déclenchement d'interventions, coordination, …), surtout si les incidents interviennent simultanément.

Le système que nous développons a pour objet d'assister les équipes humaines chargées de la surveillance, de les décharger des tâches monotones et de leur présenter des situations potentiellement dangereuses pour lesquelles leur analyse critique est requise.

Les systèmes d'intelligence artificielle utilisés par NEPSIS reposent sur l'apprentissage profond.
Cette technologie permet de détecter avec une forte acuité des situations complexes et des situations nouvelles pour lesquelles elle n'avait pas été entrainée.
Cependant, les résultats produits reposent principalement sur les données utilisées pour entrainer le système (datasets).

Notre analyse de la situation est d'apporter une grande vigilance concernant les données utilisées pour l'entrainement.

Ainsi, s'agissant de la partie 3 « *Une technologie porteuse de risques gradués pour les droits et libertés des personnes* » (notamment 3.1.11) du projet de position, il nous semble que les

datasets utilisés ne devraient pas créer de biais entre individus : représentation équilibrée entre sexe, classe d'âge, origine ethnique, taille, corpulence, …
Nous travaillons actuellement sur des datasets synthétiques générés automatiquement depuis des développements logiciels NEPSIS à partir de classes d'individus représentatifs. Cette approche permet de prouver statistiquement la parfaite représentativité des différentes catégories de personnes.

En outre, s'agissant de la partie 4 « *Des conditions de légalité différenciées en fonction des objectifs, des conditions de mise en œuvre et des risques des dispositifs de vidéo « augmentée* », nous recommandons que les personnes figurant dans les datasets d'entrainement aient préalablement données leur consentement de manière libre, éclairée, spécifique et univoque, pour l'utilisation de leurs données personnelles aux fins d'alimenter un système de détection de potentielles situations d'agressions entre individus sur la voie publique ou dans des espaces fermés. Cela permettrait d'une part, de s'assurer de disposer d'une base légale appropriée, non déjà au stade de la collecte des données nécessaires à la constitution des datasets permettant d'entraîner le système et d'autre part, d'éviter d'éventuels recours pouvant invalider des procédures de contrôles et susceptibles de rendre nécessaire un nouvel entraînement des systèmes d'apprentissage profonds (ce qui nécessite des ressources informatiques et énergétiques importantes).

Ces deux recommandations représentent à nos yeux une voie possible pour le développement de systèmes d'apprentissage profonds sécurisés, respectant des règles d'équité objective, et les principes de la règlementation relative à la protection des données à caractère personnel.