



samsara

Commentaires de Samsara Inc. en réponse à consultation publique de la CNIL sur son projet de position relative aux conditions de déploiement des caméras dites « intelligentes » ou « augmentées » dans les espaces publics.

Résumé

Samsara Inc. (« **Samsara** ») soumet les commentaires suivants en réponse à la consultation publique de la CNIL sur son projet de position (le « **Projet** ») visant à clarifier le cadre juridique de l'utilisation de caméras dites « intelligentes » ou « augmentées » dans les espaces publics (la « **Technologie** »). Comme le reconnaît la CNIL, la Technologie peut être déployée dans une variété de contextes, servant différents intérêts publics et privés. Certains usages favorisent la sécurité opérationnelle, l'efficacité et le développement durable, et sont capables de répondre à des défis sociétaux importants, comme l'amélioration de la sécurité routière. Samsara encourage la CNIL à soutenir une utilisation de la Technologie qui contribuera à concrétiser ces avantages sociétaux, pour autant que des garanties appropriées répondent de manière adéquate aux considérations de protection des données personnelles et de la vie privée.

Nos commentaires portent spécifiquement sur trois principes qui devraient guider toute réglementation régissant l'utilisation de la Technologie. *Premièrement*, la réglementation doit permettre à chaque responsable de traitement de procéder à sa propre évaluation des risques et des avantages afin de déterminer la Technologie qui répondra le mieux à son cas d'utilisation particulier tout en respectant la vie privée des personnes concernées. *Deuxièmement*, la réglementation ne doit pas empêcher les responsables de traitement d'invoquer des intérêts légitimes comme base juridique pour le traitement des données personnelles dans le cadre de l'utilisation de la Technologie. La réalisation d'évaluations spécifiques de l'intérêt légitime en plus des évaluations d'impact sur la protection des données devrait permettre aux utilisateurs de trouver un équilibre entre la légitimité de leur(s) cas d'utilisation particulier(s) et les droits des personnes concernées potentiellement touchées. *Troisièmement*, la réglementation doit prendre en compte la manière dont les obligations de protection des données dès la conception et par défaut peuvent aider les utilisateurs de la Technologie dans l'atténuation des préoccupations en matière de respect de la vie privée. Ces principes sont expliqués plus en détail ci-dessous et permettraient à la CNIL d'avoir une approche nuancée, neutre et holistique de la réglementation de la Technologie.

Au sujet de Samsara

Samsara est l'un des principaux fournisseurs de solutions de l'Internet des Objets qui combinent matériels, logiciels et capacités du cloud en vue d'accroître l'efficacité, la sécurité et le développement durable des opérations qui alimentent notre économie mondiale. La technologie de Samsara comprend la sécurité par la vidéo, des solutions télématiques pour les véhicules et des outils de coaching des conducteurs pour les flottes commerciales, ainsi que la surveillance et la visibilité des équipements en temps réel pour les sites industriels.

Fondée en 2015, Samsara compte plus de 25 000 clients.

Commentaires de Samsara sur le Projet

Samsara estime que les principes suivants devraient guider tout effort visant à élaborer un cadre légal spécifique concernant l'utilisation de la Technologie :

1. Mettre l'accent sur une approche fondée sur les risques et les faits de l'utilisation de la Technologie

La CNIL devrait affirmer clairement qu'en utilisant la Technologie, chaque responsable de traitement est habilité à adopter une approche fondée sur les risques et les faits pour déterminer la base juridique appropriée pour le traitement des données. Cette détermination doit tenir compte de la nature des données, de la capacité de l'utilisateur à contrôler leur traitement, des risques et des avantages d'un tel traitement, et de toute protection des données dès la conception et par défaut, telles que documentées dans un cadre approprié comme une étude d'impact sur la protection des données (AIPD). La consultation préalable ou la soumission préalable d'une AIPD à la CNIL ne devrait pas être une condition préalable à l'utilisation de la Technologie (point 4.2.8.1 du Projet), si des mesures technologiques et organisationnelles appropriées assurent la protection des données.

2. Reconnaître les intérêts légitimes comme base légale pour utiliser la Technologie

La CNIL devrait considérer que l'utilisation de la Technologie avec des garanties appropriées devrait permettre un équilibre entre les intérêts légitimes des utilisateurs (responsables du traitement) et les droits et libertés des personnes concernées potentiellement affectées (par exemple, les conducteurs ou autres usagers de la route). Le Projet peut sembler porter atteinte au critère de mise en balance des intérêts légitimes du fait de l'exclusion, *par principe*, de l'intérêt légitime comme base juridique pour toute Technologie qui analyserait le comportement d'une personne sur la base de ses gestes et expressions, ou de son interaction avec un objet (point 4.2.5.3 du Projet). Une telle approche ne tient pas compte du fait que certaines Technologies basées sur la vidéo qui analysent le comportement d'une personne peuvent servir des objectifs importants en matière de sécurité sans pour autant mettre en péril les droits des personnes concernées. Par exemple, les caméras intelligentes déployées dans les véhicules d'une flotte commerciale peuvent contribuer à alerter les conducteurs des risques et des incidents potentiels en temps réel (par exemple, lorsqu'un conducteur utilise un téléphone au volant), contribuant ainsi à réduire la fréquence et la gravité des accidents de la route, tout en offrant des garanties pour protéger la vie privée des autres usagers de la route. Cela permet non seulement de sauver des vies, mais aussi d'aider les flottes à économiser de l'argent en réduisant les coûts d'exploitation (par exemple, en diminuant les primes d'assurance), en réduisant les réclamations juridiques (par exemple, les réclamations frauduleuses) et en améliorant les programmes d'encadrement et de fidélisation des conducteurs. Une approche qui ne prendrait pas correctement en compte ces types d'avantages serait disproportionnée et pourrait étouffer les améliorations en matière de sécurité qu'offrent ces Technologies.

3. Renforcer les obligations de protection de la vie privée dès la conception et par défaut

Le Groupe de Travail Article 29 sur la protection des données, dans ses orientations sur la notion d'intérêt légitime, a souligné « *le rôle essentiel que les garanties peuvent jouer pour réduire les incidences injustifiées sur les personnes concernées et, partant, modifier l'équilibre des droits et des intérêts, au point que ceux de ces personnes ne prévalent plus sur l'intérêt légitime poursuivi par le responsable du traitement des données* »¹. La protection des données dès la conception et par défaut est une obligation légale établie à la charge des responsables du traitement d'intégrer la protection des données dans leurs activités de traitement et leurs pratiques commerciales, dès la conception et tout au long du cycle de vie. De nombreuses technologies de sécurité basées sur la vidéo intègrent la protection et la sécurité des données grâce à des fonctions paramétrables qui offrent aux responsables une maîtrise de leur mise en œuvre pour remplir leurs obligations et objectifs particuliers en matière de protection de la vie privée. Ces fonctions permettent notamment aux utilisateurs d'anonymiser les personnes concernées dans les données vidéo (par exemple, via la pixellisation/l'obscurcissement/le floutage de l'image), de contrôler le type de données collectées et la manière dont elles sont collectées (par exemple, via l'utilisation de caches physiques, ou des restrictions sur l'enregistrement audio), de configurer le volume de données stockées/accessibles et leur durée de conservation, de restreindre l'accès aux données (par exemple, via des contrôles d'accès et journaux d'audit) et de vérifier la manière dont les données sont protégées (par exemple, via le cryptage et la sécurité physique et environnementale des serveurs). L'objectif de toute nouvelle réglementation devrait être de veiller à ce que les responsables du traitement de données soient habilités à adopter une Technologie qui dès la conception inclut des mesures appropriées de protection des données et de la vie privée en fonction de leur situation spécifique.

¹ [Avis 06/2014 sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE](#)

Ces principes contribueront à garantir que toute réglementation s'adapte au rythme de l'innovation, permettant à la société de profiter des avantages de la Technologie en termes de sécurité, d'efficacité et de développement durable, tout en préservant la vie privée des personnes concernées. Toute nouvelle réglementation devrait souligner l'importance des mesures de protection de la vie privée dans toute nouvelle Technologie, sans étouffer ou interdire une telle Technologie en tant que telle.

* * *

Compte tenu de ces principes, Samsara invite la CNIL à adopter une approche nuancée, neutre et globale quant à la définition d'un cadre légal spécifique pour la Technologie. Spécifiquement, lors de l'analyse des risques (point 3 du Projet), la CNIL devrait prendre en compte les avantages démontrés de la Technologie et les mesures de protection existantes. Des études montrent que lorsqu'ils sont associés à l'accompagnement du conducteur et à la télématique, les systèmes de sécurité basés sur la vidéo utilisés dans les véhicules commerciaux peuvent réduire les événements liés à la sécurité (par exemple, les freinages brusques et les collisions) de plus de 50%², et l'utilisation de systèmes de sécurité basés sur la vidéo à double face peut conduire à une réduction de 60%³ des accidents. Cette augmentation significative de la sécurité s'accompagne d'un autre avantage : contrairement aux caméras embarquées de base, bon nombre de ces systèmes ne téléchargent pas et ne stockent pas de manière continue ou permanente toutes les données qu'ils enregistrent. Au contraire, les solutions de sécurité vidéo plus avancées ne téléchargent que les séquences *pertinentes* (par exemple, la vidéo d'une distraction au volant ou d'un accident), ce qui est conforme au principe de minimisation des données du RGPD et permet d'éviter spécifiquement une « surveillance systématique et à grande échelle ».

Samsara apprécie les efforts de la CNIL pour aborder ces questions importantes. Nous espérons que nos commentaires, basés sur notre expertise technologique en tant que fournisseur de solutions de sécurité par vidéo, seront utiles. Si vous avez des questions ou souhaitez obtenir plus de précisions, Samsara se réjouira de poursuivre le dialogue sur ces questions importantes et je vous invite à me contacter.

Bien cordialement,

² [Matthew C. Camden et al., Effective Use of Commercially Available Onboard Safety Monitoring Technologies: Guidance for Commercial Motor Vehicle Carriers, Nat'l Surface Transp. Safety Ctr. for Excellence, \(2015\), Accessed November 7, 2021.](#)

³ [Jennifer L. Bell et al., Evaluation of an in-vehicle monitoring system \(IVMS\) to reduce risky driving behaviors in commercial drivers: Comparison of in-cab warning lights and supervisory coaching with videos of driving behavior, Dep't Health Hum. Serv., \(](#)