David Libeau

Le 17 avril 2023 à Paris

Conseil constitutionnel
2 Rue de Montpensier
75001 Paris

Objet : contribution extérieure concernant l'affaire 2023-850 DC

J'ai alerté le Conseil constitutionnel dans une contribution extérieure datée du 18 janvier 2022 du risque que portait l'article 1 du projet de loi renforçant les outils de gestion de la crise sanitaire et modifiant le code de la santé publique concernant la protection des données personnelles et le respect du droit à la vie privée des Français. Dans sa décision n° 2022-835 DC du 21 janvier 2022, le Conseil a jugé que les principales mesures étaient conformes à la constitution. Dans les contributions extérieures publiées par le Conseil, ce dernier a diffusé le QR code d'un pass sanitaire lisible alors que la greffe doit occulter les données personnelles sensibles. **Cette diffusion d'informations de santé a démontré la méconnaissance du Conseil sur le sujet.** Ainsi, je vous propose cette nouvelle contribution extérieure qui concerne cette fois l'article 7 du projet de loi relatif aux jeux Olympiques et Paralympiques de 2024.

Ce projet de loi porte gravement atteinte au respect du droit à la vie privée des citoyens français et étrangers se rendant sur le sol français. L'article 7 introduit la surveillance algorithmique par vidéosurveillance. Sous couvert d'expérimentation, les dispositions précitées sont une première étape, un pied dans la porte, du traitement à grande échelle de données biométriques et de la mise en place de la reconnaissance faciale dans l'espace public. Soumettre toute personne se baladent dans l'espace public à ce type de traitement de données personnelles porte gravement atteinte aux droits fondamentaux de liberté de circulation et droit au respect de la vie privée. Les droits humains sont également bafoués à cause de l'impact environnemental et du micro-travail qu'impliquent ces algorithmes.

Le respect de la vie privée

L'importance du respect de la vie privée comme droit humain est cruciale dans une société démocratique telle que la France. La vie privée est une valeur fondamentale qui garantit la liberté individuelle et la dignité humaine. La protection de la vie privée est essentielle pour préserver la confidentialité des données personnelles et pour éviter l'ingérence de l'État dans la vie privée des citoyens.

La vie privée est considérée comme un droit fondamental Chaque individu a le droit de vivre sa vie sans ingérence indue de la part de l'État ou d'autres personnes. Ce droit inclut la confidentialité des données personnelles, la protection de la correspondance privée, le droit au secret médical et la protection de la vie familiale.

Le respect de la vie privée est également protégé par les traités internationaux, notamment la Convention européenne des droits de l'Homme, qui a été ratifiée par la France en 1974. Selon cet accord, les États membres doivent protéger la vie privée de leurs citoyens et s'abstenir d'interférer dans leur vie privée, sauf dans certaines circonstances exceptionnelles.

En France, la vie privée est considérée comme un droit fondamental qui est protégé par la Constitution. Le Conseil constitutionnel a affirmé, en 1999, que la liberté proclamée par l'article 2 de la Déclaration des droits de l'Homme et du citoyen de 1789 impliquait le respect de la vie privée. L'article 9 du Code civil stipule que « Chacun a droit au respect de sa vie privée. ». Ce droit inclut la protection des données personnelles, la protection de la correspondance privée, la protection de l'image et de la voix des individus, ainsi que le droit au secret médical.

En outre, la loi française sur la protection des données personnelles, la Loi informatique et libertés, a été adoptée en 1978 pour protéger la vie privée des citoyens. Au niveau européen, le Règlement général sur la protection des données personnelles a été adopté en 2016. Ces lois réglementent le traitement et l'utilisation des données personnelles et établit des obligations pour les organismes ou pour l'État qui traitent ces données.

Le respect de la vie privée est essentiel pour préserver la liberté individuelle et la dignité humaine. Il garantit que les citoyens peuvent exercer leurs droits sans ingérence indue de l'État ou d'autres personnes. La protection de la vie privée est également importante pour prévenir l'utilisation abusive des données personnelles et pour protéger les individus contre la discrimination, l'intimidation et la surveillance illégale.

En outre, le respect de la vie privée est essentiel pour protéger la vie familiale et les relations personnelles. Les individus ont le droit de mener leur vie privée sans avoir à craindre des interférences indésirables, qu'il s'agisse de l'État, d'entreprises ou d'autres personnes. La vie privée est également importante pour protéger la dignité des individus et leur intégrité physique, psychologique et morale.

Dans une société démocratique, le respect de la vie privée est crucial pour garantir la transparence et la responsabilité de l'État. Le gouvernement doit être tenu responsables de ses actions et être transparent dans sa gestion des données personnelles et de la vie privée des citoyens. La vie privée est également importante pour protéger la liberté d'expression et la liberté de la presse, car la confidentialité des sources et des informations confidentielles est essentielle pour le fonctionnement des médias.

En conclusion, le respect de la vie privée est un droit fondamental qui est protégé par les traités internationaux et les lois nationales dans de nombreuses démocraties, dont la France. La vie privée est essentielle pour protéger la liberté individuelle, la dignité humaine et la vie familiale. Le respect de la vie privée est également crucial pour garantir la transparence et la responsabilité de l'État et pour protéger la liberté d'expression et de la presse. Dans une société démocratique, le respect de la vie privée est essentiel pour préserver la liberté et la dignité des individus.

La surveillance généralisée

La surveillance généralisée dans une société démocratique comme la France peut être extrêmement préjudiciable pour les droits et les libertés fondamentales des individus. Elle peut entraîner une violation de la vie privée, de la liberté d'expression, de la liberté de la presse et des droits humains en général.

La surveillance généralisée peut porter atteinte à la vie privée des individus en collectant et en traitant des données personnelles sensibles. Ces données peuvent être utilisées pour profiler les personnes en fonction de leur orientation politique, de leur religion, de leur état de santé et de leur vie privée. Les individus peuvent également être surveillés de manière intrusive, comme la surveillance de leurs conversations téléphoniques et de leurs activités en ligne. Cela peut entraîner une perte de confiance dans les institutions gouvernementales et une violation des droits humains.

Une surveillance généralisée peut également restreindre la liberté d'expression et la liberté de la presse. Les journalistes et les individus peuvent être dissuadés de partager des informations importantes par crainte d'être surveillés ou poursuivis. Cela peut limiter la liberté d'expression et la capacité de la presse à informer le public sur les questions importantes, ce qui peut avoir un impact négatif sur la transparence et la responsabilité du gouvernement.

Les inégalités sociales peuvent être renforcée par la surveillance généralisée lorsqu'elle cible les groupes vulnérables tels que les minorités, les immigrés et les personnes à faible revenu. Ces groupes sont souvent les plus susceptibles d'être surveillés et peuvent être stigmatisés ou discriminés en raison de cette surveillance. Cela peut également renforcer le pouvoir des entreprises et des gouvernements en leur donnant un accès inégal aux données et aux informations.

D’une façon générale, la surveillance généralisée a un impact négatif sur la démocratie en sapant la confiance des citoyens dans le gouvernement et en restreignant la participation citoyenne. Les citoyens peuvent se sentir découragés de participer au processus démocratique si leur vie privée est menacée, leur liberté d’expression limitée et leur participation au processus politique entravée. Cela peut avoir des conséquences graves sur la qualité de la démocratie et la participation des citoyens à la vie publique.

En conclusion, la surveillance généralisée dans une société démocratique comme la France peut être extrêmement dangereuse pour les droits et les libertés fondamentales des individus. Elle peut entraîner une violation de la vie privée, de la liberté d’expression, de la liberté de la presse et des droits humains en général. Il est donc essentiel de prendre des mesures pour protéger ces droits et garantir la transparence, la responsabilité et la participation citoyenne dans le processus démocratique.

La surveillance généralisée ne doit pas être considérée comme une solution miracle pour lutter contre le terrorisme, le crime organisé ou d’autres menaces à la sécurité nationale. Des mesures alternatives doivent être envisagées, comme la coopération internationale, la prévention, la réduction des inégalités sociales et l’amélioration de la qualité de vie des citoyens.

Enfin, il est important de souligner que les dangers de la surveillance généralisée ne sont pas seulement théoriques ou hypothétiques, mais qu’ils ont déjà été observés dans de nombreux pays à travers le monde. Il est donc essentiel de rester vigilant et de s’assurer que les droits et les libertés fondamentales des individus sont protégés en tout temps, même dans des situations de crise ou d’urgence.

Vidéosurveillance

La vidéosurveillance et la *vidéoprotection* sont des technologies de surveillance de plus en plus utilisées sur la voie publique en France. Bien que ces systèmes soient présentés comme des outils efficaces pour prévenir la criminalité et améliorer la sécurité, il convient de rappeler qu’aucune étude sérieuse n’a prouvé l’efficacité de la vidéosurveillance. De plus, ils présentent surtout des dangers importants pour les droits et les libertés fondamentales des citoyens.

Le premier danger de la vidéosurveillance est la violation de la vie privée des citoyens. En effet, la surveillance des espaces publics peut permettre de collecter de nombreuses données personnelles, telles que les déplacements, les habitudes de vie ou les contacts sociaux. Ces données peuvent ensuite être utilisées à des fins de surveillance, de profilage ou de ciblage, sans le consentement des citoyens concernés. Cela constitue une atteinte grave à la vie privée et peut nuire à la confiance des citoyens dans l’État et ses institutions.

Le deuxième danger de la vidéosurveillance est le risque de discrimination et de stigmatisation. En effet, les systèmes de vidéosurveillance peuvent être utilisés de manière sélective pour cibler certains groupes de population, tels que les minorités ethniques, les sans-abris ou les personnes ayant un style vestimentaire particulier. Cela peut conduire à des pratiques discriminatoires et à des préjugés injustifiés à l’encontre de ces groupes, et porter atteinte à leur dignité et à leur intégrité.

Le troisième danger de la vidéosurveillance est le risque de dérive autoritaire. En effet, les systèmes de vidéosurveillance peuvent être utilisés pour surveiller les mouvements de l’opposition politique, des militants, des journalistes ou d’autres groupes considérés comme subversifs ou dangereux pour l’ordre public. Cela peut conduire à une restriction de la liberté d’expression, de la liberté de la presse et de la liberté d’association, qui sont des droits fondamentaux dans une société démocratique.

Le quatrième danger de la vidéosurveillance est le risque de banalisation de la surveillance. En effet, en normalisant la surveillance dans l’espace public, les systèmes de vidéosurveillance peuvent conduire à une acceptation croissante de la surveillance dans d’autres domaines de la vie, tels que la surveillance des lieux de travail, des écoles, des domiciles privés ou des espaces en ligne.

Cela peut conduire à une surveillance généralisée de la société, qui porte atteinte à la liberté individuelle et à la vie privée.

Il convient également de noter que la vidéosurveillance peut également avoir des conséquences négatives sur la sécurité publique. En effet, le déploiement de systèmes de vidéosurveillance peut donner l'illusion d'une sécurité accrue, mais peut ne pas être efficace pour prévenir la criminalité. Les criminels peuvent s'adapter en utilisant des moyens pour éviter la détection, tels que le port de masques ou la désactivation des caméras. De plus, la vidéosurveillance peut conduire à un détournement de ressources et de personnel, qui pourrait être mieux utilisé pour des mesures préventives ou des interventions sur le terrain.

En outre, la vidéosurveillance peut également être coûteuse en termes de ressources financières et humaines. Les coûts de déploiement et de maintenance des systèmes de vidéosurveillance peuvent être élevés, en particulier pour les petites villes et les municipalités. De plus, la surveillance constante des images capturées par les caméras peut nécessiter un personnel dédié, qui pourrait être utilisé pour des tâches plus essentielles. A Paris, dans un référé daté du 2 décembre 2021, la Cour de comptes préconise d'engager sans tarder une évaluation de l'efficacité du plan de *vidéoprotection* de la préfecture de police de Paris qui devait initialement couter 225,1 M€, a atteint, au 31 décembre 2020, 343 M€ et devrait couter au total entre 433 à 481 M€ soit deux fois plus que le cout initial [1].

Enfin, la vidéosurveillance peut également contribuer à une culture de la peur et de la méfiance. Les citoyens peuvent se sentir surveillés et surveiller les uns les autres, ce qui peut conduire à une atmosphère de suspicion et de paranoïa. De plus, la surveillance constante peut conduire à une perte de confiance dans les institutions et les autorités, ce qui peut nuire à la légitimité de l'État et de ses institutions.

En conclusion, la vidéosurveillance et la *vidéoprotection* sur la voie publique présentent de nombreux dangers pour les droits et les libertés fondamentales des citoyens, ainsi que pour la sécurité publique et la confiance dans les institutions. Il est donc essentiel de considérer ces risques lors de la mise en place de systèmes de surveillance, et de prendre des mesures pour garantir le respect des droits fondamentaux, ainsi que la transparence et la responsabilité dans le processus décisionnel. De plus, il est important de considérer des alternatives à la vidéosurveillance, telles que la prévention et l'intervention sur le terrain, qui peuvent être plus efficaces pour assurer la sécurité publique et préserver les droits fondamentaux.

IA et algorithmes décisionnels

L'utilisation de l'intelligence artificielle (IA) peut être utile dans certains cas. Par exemple, cette contribution extérieure a été très largement rédigée par *ChatGPT* un logiciel permettant de générer du texte selon des instructions précises permettant un gain temps considérable. L'utilisation de cet outil est d'autant plus à propos dans notre cas que probablement personne ne va lire cette contribution extérieure.

Cependant, les algorithmes dits « d'intelligence artificielle » doivent être nourrit pas une quantité astronomique de données pour leur phase d'entrainement. Ces données d'entrainement peuvent comporter des données personnelles et des données sensibles qu'il est souvent très difficile à détecter et à supprimer. Récemment, *ChatGPT* a fait scandale pour l'utilisation des données personnelles et a été interdit en Italie. Partout dans le monde les autorités chargées de la protection des données ont lancé des enquêtes. A cause de leur conception opaque, de tels algorithmes pourraient ne jamais respecter totalement les dispositions du RGPD [2].

L'utilisation croissante de ce type d'algorithme par les autorités soulève de nombreuses préoccupations quant aux risques pour les droits et les libertés fondamentales des citoyens, ainsi que pour la confiance dans les institutions publiques. En effet, l'utilisation de ces technologies peut potentiellement renforcer les stéréotypes et les biais, violer la vie privée, conduire à une surveillance de masse et à une discrimination systémique.

Tout d'abord, l'utilisation de l'IA et des algorithmes décisionnels peut renforcer les stéréotypes et les biais, qui peuvent affecter négativement les groupes de population déjà marginalisés. Les algorithmes sont souvent formés sur des données historiques, qui peuvent refléter les préjugés et les stéréotypes de la société. Par conséquent, l'IA peut reproduire ces préjugés et renforcer les stéréotypes existants, ce qui peut conduire à une discrimination systémique. Dans le cas de la police, l'utilisation de l'IA peut conduire à une discrimination accrue envers les minorités ethniques et les groupes marginalisés, en particulier dans le domaine du profilage.

De plus, l'utilisation de l'IA et des algorithmes décisionnels peut porter atteinte à la vie privée des citoyens. Les technologies d'IA peuvent être utilisées pour collecter, stocker et traiter de grandes quantités de données personnelles, telles que les données de localisation, les historiques de navigation sur Internet, les achats en ligne et les habitudes de consommation. Ces données peuvent être utilisées pour profiler les individus, pour les suivre et les surveiller, ce qui peut compromettre leur vie privée et leur liberté individuelle. Dans le cas de la police, cela peut conduire à une surveillance de masse et à une violation des droits à la vie privée des citoyens.

En outre, l'utilisation de l'IA et des algorithmes décisionnels par la police peut également conduire à une discrimination systémique. Si les algorithmes sont formés sur des données historiques qui reflètent les préjugés et les stéréotypes de la société, cela peut conduire à une discrimination accrue envers les minorités ethniques et les groupes marginalisés. Par exemple, les systèmes de reconnaissance faciale peuvent être biaisés envers les personnes de couleur, conduisant à des erreurs de reconnaissance et à des arrestations injustes.

Enfin, l'utilisation de l'IA et des algorithmes décisionnels par la police peut également affecter la confiance dans les institutions publiques. Si les citoyens estiment que les décisions importantes sont prises sans intervention humaine, cela peut nuire à la confiance dans les institutions publiques et remettre en question leur légitimité. De plus, si les décisions importantes sont prises par des algorithmes automatisés, cela peut réduire la participation citoyenne et l'engagement dans le processus décisionnel.

En conclusion, il est essentiel de prendre des mesures pour garantir la transparence et la responsabilité dans l'utilisation de ces technologies, afin de minimiser les risques pour les droits des citoyens. Le gouvernement doit être conscients des risques potentiels et doit mettre en place des garde-fous stricts pour garantir que l'utilisation de l'IA et des algorithmes décisionnels ne viole pas les droits humains.

Il est également important de garantir la participation citoyenne et la transparence dans le processus de développement et d'utilisation de l'IA et des algorithmes décisionnels notamment en garantissant l'auditabilité des algorithmes par tous grâce à l'ouverture des codes source. Le gouvernement doit impliquer les citoyens et les groupes de la société civile dans le processus décisionnel, afin de garantir que les préoccupations des citoyens sont prises en compte et que les décisions sont prises de manière responsable.

Impact environnemental de l'IA

Nous devons prendre la mesure de l'urgence climatique mondiale et refuser les technologies destructrices de notre planète. Les algorithmes d'intelligence artificielle sont connus pour avoir un impact non négligeable sur l'environnement. Or, la Charte de l'environnement de 2004 confère à chacun le droit de vivre dans un environnement équilibré et respectueux de la santé.

Le premier danger de l'IA pour l'environnement est la consommation d'énergie. Les réseaux de neurones artificiels sont connus pour être gourmands en énergie, car ils nécessitent de nombreux calculs pour traiter des quantités massives de données. Pour entrainer un algorithme d'intelligence artificielle, ce sont des centaines de processeurs graphique (GPU) qui sont utilisés. Les serveurs qui alimentent les réseaux de neurones consomment donc une quantité considérable d'électricité, ce qui augmente la demande en énergie et contribue à l'émission de gaz à effet de serre.

De plus, les centres de données qui abritent ces ordinateurs peuvent également avoir des effets négatifs sur l'environnement en raison de la production de chaleur qui nécessite une climatisation, et donc une consommation supplémentaire d'énergie ainsi qu'une consommation astronomique d'eau [3].

Un troisième danger est la destruction de l'habitat naturel par la production de déchets électroniques ou l'extraction de minerais. Les entreprises minières qui extraient les minéraux appelés « terres rares » nécessaires à la fabrication de composants électroniques, tels que le cobalt et le coltan, peuvent entraîner la destruction d'habitats naturels et de terres agricoles, ce qui peut avoir des effets négatifs sur les communautés locales et la biodiversité. De plus, les ordinateurs utilisés pour l'IA ont une durée de vie limitée et deviennent rapidement obsolètes, entraînant ainsi la production de déchets électroniques.

En conclusion, l'IA peut avoir des conséquences négatives sur l'environnement, notamment en termes de consommation d'énergie, de production de déchets électroniques, de destruction de l'habitat naturel et d'augmentation des émissions de gaz à effet de serre. Il est donc primordial d'interdire la création des technologies destructrices de l'environnement ou a minima de prévoir des mesures compensatoires fortes.

Micro-travail pour l'IA

L'intelligence artificielle nécessite des quantités massives de données pour être entraînée, et pour cela, les entreprises font souvent appel à des travailleurs et travailleuses du micro-travail pour effectuer des tâches répétitives et fastidieuses de classification de données. Cela pose de réels problèmes en termes de respect des droits humains.

Le micro-travail est souvent effectué par des travailleurs peu qualifiés dans des pays en développement, qui sont payés des salaires très bas pour effectuer des tâches fastidieuses et souvent ennuyeuses. Ces travailleurs sont souvent exposés à des conditions de travail précaires, à des pressions pour travailler de longues heures et à des violations des normes de santé et de sécurité. De plus, ils n'ont souvent pas accès aux avantages sociaux tels que les congés payés, l'assurance maladie et les pensions.

En outre, pour la vidéosurveillance algorithmique implique la reconnaissance de comportements à partir de données issues de la vidéosurveillance ce qui consistera en la classification de vidéos. Dans ce cas, les travailleurs sont susceptibles d'être exposés à des images choquantes et potentiellement traumatisantes, ainsi qu'à des contenus violents ou offensants ce qui peut compromettre leur santé mentale.

De plus, le micro-travail peut également affecter les droits à la vie privée et à la protection des données des individus. Les travailleurs du micro-travail peuvent avoir accès à des données personnelles sensibles, telles que des images biométriques. En plus, ces travailleurs sont souvent situés dans des pays étrangers et leur travail de classification implique donc une transmission de données personnelles à l'étranger dans des pays où la législation en matière de protection des données n'est pas adéquat. Cela peut entraîner des violations de la vie privée.

Enfin, le micro-travail peut également contribuer à renforcer les inégalités économiques et sociales existantes. Les travailleurs du micro-travail sont souvent payés beaucoup moins que les travailleurs dans des emplois traditionnels, ce qui peut créer une pression à la baisse sur les salaires. De plus, le travail du micro-travail est souvent effectué par des personnes dans des pays en développement, ce qui peut renforcer les déséquilibres économiques entre les pays.

En conclusion, l'utilisation de travailleurs du micro-travail pour entraîner des algorithmes d'intelligence artificielle peut avoir des conséquences négatives importantes pour les travailleurs eux-mêmes, ainsi que pour les droits humains et la vie privée des individus. Il est donc important que le gouvernement interdise le micro-travail déshumanisant et oppressant pour l'entrainement des algorithmes de la vidéosurveillance.

Traitement de données biométriques

Le traitement de données biométriques est de plus en plus répandu dans le monde, y compris en France. Les données biométriques comprennent des informations telles que les empreintes digitales, les images faciales, les empreintes rétiniennes, les empreintes palmaires et la reconnaissance vocale. Bien que ces technologies aient des utilisations potentiellement positives, comme l'identification précise des criminels, il existe également de graves dangers pour la vie privée et la sécurité des citoyens lorsque ces données sont mal utilisées ou piratées.

Le premier danger est celui de la violation de la vie privée. Les données biométriques sont des données personnelles sensibles et leur traitement doit être soumis à des règles strictes en matière de protection de la vie privée. Si ces données sont collectées et utilisées sans le consentement des citoyens, cela peut constituer une violation de leur vie privée. De plus, si ces données tombent entre de mauvaises mains, cela pourrait avoir des conséquences désastreuses pour la sécurité des individus. Les identités peuvent être volées, la vie privée peut être compromise, et les citoyens pourraient être victimes de chantage.

Un deuxième danger est lié à l'utilisation de ces données biométriques dans les technologies de surveillance de masse, telles que la reconnaissance faciale. Bien que ces technologies puissent être utilisées pour identifier les criminels, elles peuvent également être utilisées pour surveiller les citoyens innocents. Lorsque les citoyens sont soumis à une surveillance constante, cela peut créer un climat de méfiance et de peur, qui peut saper la confiance dans l'État et les institutions démocratiques.

Un autre danger est la possibilité de discrimination et de biais dans les décisions prises en utilisant ces technologies. Les algorithmes utilisés pour traiter les données biométriques peuvent avoir des biais intégrés, ce qui signifie que les décisions prises sur la base de ces données peuvent être discriminatoires et injustes. Par exemple, si un algorithme est conçu pour reconnaître les visages blancs, il peut avoir du mal à reconnaître les visages de personnes de couleur, ce qui pourrait entraîner des erreurs dans les décisions prises sur la base de ces données.

Enfin, il existe également un risque de piratage des données biométriques. Les données biométriques sont des informations très précieuses, car elles sont uniques à chaque individu et ne peuvent pas être modifiées. Si ces données sont piratées, elles peuvent être utilisées pour voler l'identité des citoyens ou pour accéder à des informations confidentielles.

En conclusion, le traitement de données biométriques dans une société démocratique comme la France présente de nombreux dangers pour la vie privée, la sécurité et la justice. Leur utilisation doit être étroitement contrôlée et réglementée. Les citoyens doivent avoir un droit de regard sur leurs données biométriques et de décider comment elles sont utilisées, afin de protéger leur vie privée et leur sécurité.

Reconnaissance faciale

La reconnaissance faciale est une technique d'identification biométrique qui utilise les caractéristiques du visage d'un individu pour l'identifier de manière unique. Elle est de plus en plus utilisée dans les systèmes de vidéo surveillance sur la voie publique en France, notamment pour lutter contre le terrorisme et la criminalité. Toutefois, l'utilisation de cette technologie soulève des préoccupations importantes en matière de respect de la vie privée et de la protection des données personnelles.

Le premier danger de la reconnaissance faciale est la possibilité d'erreurs et de biais dans les algorithmes utilisés pour l'identification. En effet, les algorithmes de reconnaissance faciale peuvent ne pas reconnaître correctement les visages en fonction de leur couleur de peau, de leur sexe ou de leur âge, ce qui peut conduire à des erreurs d'identification ou à des arrestations injustifiées. De plus, les erreurs de reconnaissance peuvent être amplifiées en cas de mauvaise

qualité des images de surveillance, de contre-jour, de flou ou de mauvaise angle de vue, ce qui peut conduire à des erreurs graves.

Le deuxième danger est lié à la surveillance de masse. La reconnaissance faciale peut être utilisée pour surveiller de manière indiscriminée et systématique les citoyens français sur la voie publique, ce qui constitue une atteinte à leur vie privée et à leur liberté de mouvement. Les systèmes de reconnaissance faciale peuvent être utilisés pour identifier et suivre les individus en temps réel, dresser des profils de leur comportement et collecter des données sur leurs déplacements et leurs habitudes. Cela peut créer une situation de surveillance constante et généralisée qui limite la liberté et l'autonomie des citoyens.

Le troisième danger est lié à la sécurité des données personnelles. Les systèmes de reconnaissance faciale nécessitent la collecte et le stockage de données biométriques sensibles, telles que les images du visage, qui peuvent être utilisées pour identifier les individus même sans leur consentement. La collecte de ces données personnelles peut être effectuée sans transparence ni contrôle de la part des individus concernés, ce qui peut conduire à des abus et des violations de la vie privée. De plus, les données biométriques stockées peuvent être piratées, volées ou utilisées à des fins malveillantes, ce qui peut causer des préjudices graves aux individus concernés.

Le quatrième danger est lié à l'utilisation abusive de la reconnaissance faciale par les autorités. Les systèmes de reconnaissance faciale peuvent être utilisés à des fins illégales ou discriminatoires, telles que la surveillance politique, la surveillance de groupes minoritaires ou la surveillance de manifestants. Ils peuvent également être utilisés pour violer les droits de la défense ou pour contourner les procédures légales, en permettant l'identification de suspects sans preuve suffisante ou sans mandat judiciaire.

En plus de ces préoccupations, la reconnaissance faciale soulève également des inquiétudes quant à la discrimination. Les systèmes de reconnaissance faciale ont tendance à être moins précis pour les personnes de couleur et les femmes, ce qui peut entraîner une surveillance et des accusations injustes. Cela est particulièrement préoccupant dans un pays comme la France, qui lutte contre les discriminations raciales et ethniques.

De plus, la reconnaissance faciale a le potentiel de restreindre la liberté d'expression et de rassemblement. Les manifestants peuvent craindre que leur présence ne soit enregistrée et qu'ils soient identifiés par la suite, ce qui peut dissuader certaines personnes de participer à des manifestations politiques légitimes. En outre, la reconnaissance faciale peut être utilisée pour restreindre l'accès à certains espaces publics ou événements en fonction de critères de sécurité arbitraires et opaques.

Enfin, la reconnaissance faciale peut contribuer à la constitution d'un état de surveillance, où les citoyens sont constamment surveillés et leurs mouvements sont suivis. Cela peut créer un climat de peur et de méfiance dans la société, ce qui peut avoir des conséquences néfastes sur la santé mentale et le bien-être des citoyens.

En conclusion, la reconnaissance faciale par les systèmes de vidéo surveillance soulève de nombreuses préoccupations en matière de vie privée, de discrimination, de liberté d'expression et de rassemblement, ainsi que de surveillance généralisée. Si elle est utilisée de manière inappropriée ou abusive, elle peut porter atteinte aux droits fondamentaux des citoyens français et remettre en question les principes démocratiques de la société. Par conséquent, il est essentiel que les autorités prennent en compte ces risques et établissent des règles claires et des mécanismes de contrôle pour encadrer l'utilisation de cette technologie

Vidéosurveillance algorithmique

L'intelligence artificielle appliquée aux images de vidéosurveillance est envisagé en France. Les algorithmes de la vidéosurveillance algorithmique doivent détecter des événements anormaux dont la liste n'est pas précisée par la loi. L'utilisation de cette technologie soulève de nombreux dangers pour les droits et les libertés fondamentales des citoyens.

Tout d'abord, l'utilisation de l'IA pour détecter des événements anormaux peut conduire à une surveillance de masse généralisée, où chaque mouvement et chaque action des citoyens sont surveillés. Cela peut avoir un effet dissuasif sur la liberté de mouvement et d'expression des citoyens, car ils peuvent craindre d'être constamment surveillés et de faire l'objet d'un examen minutieux.

De plus, l'utilisation de l'IA pour la surveillance peut entraîner des erreurs de jugement et des décisions arbitraires. Les algorithmes peuvent être biaisés en raison des données sur lesquelles ils sont formés, ce qui peut entraîner des erreurs de classification ou des discriminations. Par exemple, un algorithme peut considérer qu'un groupe de jeunes rassemblés est une foule violente, alors qu'il s'agit simplement d'une réunion de famille ou d'amis. Il est également important de rappeler que le profilage et la prise de décision automatisée sont interdites par l'article 22 du RGPD. Pourtant ce projet de loi prévoit le déclenchement automatique d'alertes qui informeront les autorités d'événement anormaux.

Ensuite, la loi précise qu'aucune donnée biométrique ne doit être traitée. Lors du débat parlementaire, des députés ont évoqué le traitement de « points » et de « vecteurs ». Cette description des données traitées élude la question des données biométriques. Dans un récent article scientifique, des chercheurs ont démontré qu'avec quelques secondes d'enregistrement des mouvements de la tête et des mains, il était possible d'identifier les personnes [4]. Cela s'apparente bien à un traitement de données biométrique tel de défini au 14 de l'article 4 du RGPD.

Enfin, les données collectées par ces algorithmes peuvent être utilisées à des fins de profilage et de discrimination. Les gouvernements ou les entreprises pourront utiliser ces données ultérieurement officiellement pour entrainer les algorithmes d'intelligence artificielle, mais ce qui est artificiel sera le contrôle de la CNIL. Sans moyens supplémentaires, cette autorité indépendante ne pourra contrôler efficacement l'utilisation qu'il sera fait de ces données. Nous avons vu récemment la CNIL indiquer n'avoir déclenché aucune enquête sur *ChatGPT* alors que son homologue italien avait interdit l'outil. Il a fallu attendre des plaintes de citoyens pour que la CNIL commence à étudier la question. Un autre exemple, concernant la vidéosurveillance, la CNIL n'a pas traité à temps une plainte sur l'exercice du droit d'accès aux images de *vidéoprotection* me concernant. Les images ont donc été détruites bafouant ainsi mon droit d'accès.

En conclusion, l'utilisation de l'intelligence artificielle pour la surveillance à travers les images de vidéosurveillance soulève de nombreux risques pour les droits et les libertés fondamentales des citoyens. L'actuel projet de loi ne garantit pas un bon équilibre des droits et ouvre la porte à la surveillance biométrique dans l'espace public.

Conclusion

L'expérimentation de la vidéosurveillance algorithmique telle que proposée à l'article 7 du projet de loi relatif aux jeux Olympiques et Paralympiques de 2024 pose de nombreux problèmes.

En premier lieu, **sur le droit à l'information**, le II bis de l'article 7 indique que « Le public est préalablement informé, par tout moyen approprié, de l'emploi de traitements algorithmiques sur les images collectées au moyen de systèmes de *vidéoprotection* […] ». Il apparaît que le législateur fait preuve d'incompétence négative en (i) ne précisant pas les modalités d'information de la mise en place de ces traitements, (ii) en omettant d'informer les personnes lors de la détection d'événements les concernant et l'enregistrement automatique des signalements tel que prévu au 2 du V du même article et (iii) en omettant d'informer les personnes lors de l'utilisation et la conservation d'échantillon d'images collectées filmant les personnes pour l'entrainement des algorithmes d'intelligent artificielle tel que prévu au VIII du même article.

En outre, **sur la durée de conservation des données**, le législateur fait également preuve d'incompétence négative en (i) ne précisant aucun durée de conservation des signalements tel que prévu au 2 du V de l'article 7 et (ii) au VIII du même article, par les mots « peut être utilisé comme données d'apprentissage pendant une durée strictement nécessaire et maximale de douze mois à

compter de l'enregistrement des images », ne prévoit qu'une durée d'utilisation et non une durée de conservation ainsi que (iii), réitéré par les mots « Ces images sont détruites, en tout état de cause, à la fin de l'expérimentation. », le législateur ne prévoit aucune durée de conservation des données d'apprentissage et seulement une durée de conservation des images utilisées pour l'apprentissage.

Ensuite, **sur la destination des données**, le législateur fait également preuve d'incompétence négative mais aussi a fait preuve d'insincérité lors des débats (i) en indiquant au V de l'article 7 que « L'État assure le développement du traitement ainsi autorisé, en confie le développement à un tiers ou l'acquiert. », le législateur confond traitement et algorithme, ne prévoit aucune mesure sur la responsabilité du traitement et de garanties dans l'éventualité où le traitement est confié par l'État à un tiers et notamment concernant les échantillons d'images collectées filmant les personnes pour l'entrainement des algorithmes d'intelligent artificielle tel que prévu au VIII du même article et (ii) en déclarant le 23 mars 2023 lors des débats à l'Assemblée Nationale que « l'État a-t-il lui-même les moyens de développer ces traitements algorithmiques ? La réponse est non » Sacha Houlié, président de la commission des lois et rapporteur, ajoute de la confusion au débat parlementaire et rend le débat insincère à cause de cette déclaration erronée et en contradiction avec le V de l'article 7 qui indique bien que « L'État assure le développement ».

Enfin, **sur l'impact environnemental et humain**, le législateur fait également preuve d'incompétence négative en ne prévoyant aucune mesure d'interdiction ou mesures compensatoires liées aux impacts environnementaux graves qu'implique l'entrainement des algorithmes d'intelligence artificielle prévu au VIII de l'article 7, ainsi qu'aucune interdiction liée au micro-travail ni aucune mesure sur les conditions de travail pour la classification des images de vidéosurveillance pour l'entrainement des algorithmes d'intelligence artificielle.

Pour tous ces motifs, j'estime que **l'article 7 du projet de loi relatif aux jeux Olympiques et Paralympiques de 2024 est contraire à la constitution**.

Amnesty International, *Access Now*, *AlgorithmWatch*, *Centre for Democracy & Technology*, *European Digital Rights*, *Human Rights Watch*, de nombreuses organisations internationales de défense des droits humains ont appelé la France à rejeter la vidéosurveillance algorithmique [5]. Entériner la surveillance algorithmique généralisée de la voie publique serait un grave recul de nos libertés publiques en France.

David Libeau

Références :

[1] Référé : Le plan de vidéoprotection de la préfecture de police de Paris, Cour des comptes, 2022 : https://www.ccomptes.fr/fr/publications/le-plan-de-videoprotection-de-la-prefecture-de-police-de-paris
[2] ChatGPT will probably never comply with GDPR, David Libeau, 2023 : https://blog.davidlibeau.fr/chatgpt-will-probably-never-comply-with-gdpr/
[3] Making AI Less "Thirsty": Uncovering and Addressing the Secret Water Footprint of AI Models, Li *et al.*, 2023 : https://arxiv.org/abs/2304.03271
[4] Unique Identification of 50,000+ Virtual Reality Users from Head & Hand Motion Data, Nair *et al.*, 2023 : https://arxiv.org/abs/2302.08927
[5] Rejeter la surveillance dans la loi sur les Jeux Olympiques 2024, 38 organisations, 2023 : https://www.hrw.org/fr/news/2023/03/07/france-rejeter-la-surveillance-dans-la-loi-sur-les-jeux-olympiques-2024