CNCDH
COMMISSION NATIONALE CONSULTATIVE DES DROITS DE L'HOMME
RÉPUBLIQUE FRANÇAISE

AVIS

A - 2024 - 5

AVIS SUR LA SURVEILLANCE DE L'ESPACE PUBLIC

20 JUIN 2024

L'Avis sur la surveillance de l'espace public (A - 2024 - 5)
a été adopté lors de l'Assemblée plénière du 20 juin 2024.
(Adoption à l'unanimité)

1. Les Jeux olympiques et paralympiques de 2024 donneront lieu à une expérimentation de la vidéosurveillance « algorithmique » (VSA)[1] : les images collectées par des caméras de surveillance seront analysées par des logiciels programmés pour détecter, en temps réel, des événements susceptibles de présenter un risque pour la sécurité publique[2]. Dans un contexte marqué par une effervescence médiatique autour des progrès, réels ou fantasmés, de l'« intelligence artificielle », cette expérimentation marque une nouvelle étape dans la mise en place, inaugurée par la loi du 21 janvier 1995[3], d'un vaste dispositif technologique de surveillance de l'espace public.

2. Selon les dernières estimations, 90 000 caméras dédiées à la vidéoprotection[4] seraient présentes sur le territoire français. Le ministre de l'Intérieur a encore récemment appelé les préfets à accélérer leur déploiement[5]. D'après le rapport annexé à la loi de janvier 2023 *d'orientation et de programmation du ministère de l'Intérieur*, les crédits du fonds interministériel de prévention de la délinquance et de la radicalisation (FIPDR) consacrés à la vidéoprotection vont d'ailleurs tripler au cours des cinq années à venir et viendront cofinancer les projets portés par les collectivités territoriales, principaux acquéreurs de ces caméras. Par ailleurs, les caméras aéroportées – des drones équipées d'une caméra principalement – font l'objet d'une utilisation massive depuis leur légalisation[6].

3. Pour assurer le visionnage des flux d'images produits par toutes ces caméras, les municipalités se dotent de manière croissante de centres de supervision urbains (CSU), dans lesquels des agents scrutent des murs d'écrans qui diffusent les flux vidéos captés par les caméras. En 2019, le ministère de l'Intérieur en recensait 903[7]. Face à l'ampleur croissante des dispositifs de vidéoprotection, le constat est unanime : les capacités humaines de visionnage et d'analyse sont largement dépassées par la quantité d'images captées par toutes ces caméras[8]. En faisant appel à des traitements algorithmiques en mesure de détecter de manière automatisée et en temps réel des événements suspects prédéterminés, la VSA a justement, selon ses promoteurs, vocation à combler ces carences humaines.

4. Ces dernières années, dans le contexte de la lutte contre le

terrorisme ou de la crise sanitaire liée à la Covid-19, les pouvoirs publics ont témoigné à plusieurs reprises de leur attrait pour les nouvelles technologies de surveillance[9]. De leur côté, les députés et les sénateurs ont également manifesté leur intérêt en la matière en créant des missions d'information relatives aux images de sécurité pour les premiers et à la reconnaissance faciale pour les seconds[10]. Dans le prolongement de ce rapport d'information, les sénateurs ont d'ailleurs adopté une proposition de loi afin d'expérimenter la reconnaissance biométrique dans l'espace public. Ce texte n'a cependant toujours pas fait l'objet d'une inscription à l'ordre du jour de la commission des lois de l'Assemblée nationale. Certains médias ont pourtant révélé il y a plusieurs mois l'utilisation de la reconnaissance faciale par plusieurs polices municipales, en dehors de tout cadre légal[11].

5. La Commission nationale consultative des droits de l'homme (CNCDH) a déjà eu l'occasion d'exprimer ses préoccupations à l'égard de certaines finalités justifiant l'utilisation de drones, en particulier lors des rassemblements publics[12]. Elle s'est également prononcée pour un encadrement très strict d'une éventuelle utilisation de l'identification biométrique dans l'espace public à distance en temps réel[13]. La CNCDH se saisit de l'expérimentation de la VSA, en cours, pour formuler ses préoccupations et des recommandations à l'égard des orientations récentes, et des projets à venir, relatifs à la surveillance de l'espace public. L'expérimentation donnera lieu à une évaluation, mais la CNCDH souhaite d'ores et déjà, à près d'un mois des Jeux olympiques et paralympiques et d'un déploiement plus significatif de la VSA, formuler un certain nombre d'observations relatives à l'utilisation de cette nouvelle technologie et, plus largement, à l'égard de la vidéosurveillance.

6. La CNCDH relève d'abord que l'utilisation de la VSA s'inscrit dans la continuité du projet poursuivi par les autorités depuis la légalisation, en 1995, de l'installation de caméras dans l'espace public et les lieux ouverts au public : renforcer la surveillance de l'espace public et tendre vers un objectif d'ubiquité de la police. Or, la vidéoprotection, qui s'est largement banalisée à partir des années 2000, ne fait plus débat depuis longtemps[14]. Seules quelques organisations de défense des droits humains poursuivent leur engagement pour que le débat ne soit

pas totalement invisibilisé. Pourtant, les craintes exprimées dans les années 1990, relatives aux risques pour la liberté d'aller et venir ainsi que pour le respect de la vie privée, sont d'autant plus d'actualité que les caméras de surveillance ont proliféré. C'est pourquoi la CNCDH tient à rappeler dans cet avis que cette technologie policière ne doit être autorisée que dans de strictes limites motivées de lieux, de temps et de finalités, garanties par un contrôle effectif de leur installation et de leur mise en œuvre.

7. La CNCDH rappelle ensuite que l'essor de nouvelles technologies, telles que les caméras aéroportées ou les logiciels de traitement automatisé d'images, ont ravivé ces dernières années les craintes d'atteintes aux droits de l'Homme. Nombre de rapports institutionnels[15] et d'articles de doctrine[16] ont pointé les risques d'un dispositif de vidéosurveillance renouvelé, par son ampleur (multiplication des caméras fixes et caméras aéroportées, sans compter les caméras embarquées ou les caméras individuelles), et par son efficacité affichée, promise par les progrès des technologies numériques[17].

8. L'usage de l'intelligence artificielle dans l'analyse des images captées s'inscrit donc dans la continuité de la vidéoprotection et, dans le même temps, semble en modifier la nature[18]. Il permet en effet une systématisation et une intensification de la surveillance d'une part et, d'autre part, une implication inédite des acteurs privés – les concepteurs des logiciels – dans l'exercice d'une mission régalienne. Lorsque la VSA est en charge de détecter des comportements « anormaux », elle véhicule une conception normalisée de l'espace public, où tout écart de conduite devient suspect.

9. Cette conception est d'autant plus préoccupante que les industriels en charge de l'élaboration des logiciels contribuent en grande partie à l'élaboration de cette norme de comportement : le plus souvent les images destinées à l'apprentissage de la machine sont sélectionnées par eux en amont de son installation (une base de données) ; d'autres fois la machine est programmée pour identifier, après son installation, des régularités dans les images filmées de l'espace public[19].

10. Dans un avis de 2020, la CNCDH craignait que ce dispositif renouvelé de vidéosurveillance ne représente une nouvelle étape, après la vidéoprotection, vers une « société panoptique », et induise un nouveau type de rapport entre la police et la population, caractérisé par la défiance et la distance. Pour le moins, toutes ces nouvelles technologies ravivent la crainte d'une remise en cause de la possibilité pour quiconque d'exercer ses droits et libertés fondamentaux, y compris la liberté de manifester, dans l'espace public de manière anonyme.

11. L'avis prendra soin de distinguer les technologies utilisées, en raison de leurs effets plus ou moins attentatoires aux droits et libertés fondamentaux. Une caméra thermique ne représente pas, par exemple, la même menace pour les libertés qu'une caméra optique. De la même manière, la VSA représente une menace pour ces droits qui varie en fonction des événements « ciblés » par le logiciel, la reconnaissance faciale étant la technologie la plus intrusive.

12. Dans le cadre de cet avis, la CNCDH reprendra à son compte le terme légal de « vidéoprotection », lorsqu'il s'agira d'évoquer les caméras installées sur la voie publique ou dans les lieux et espace ouverts au public, encadrées par les articles L. 251-1 et suivants du code de la sécurité intérieure (CSI), mais emploiera la notion de vidéosurveillance pour désigner l'ensemble du dispositif constitué par ces dernières et par les caméras aéroportées, régies par les articles L. 242-1 et suivants du même code. L'avis ne traitera pas des caméras embarquées dans les véhicules ou des caméras individuelles des agents, dans la mesure où elles sont destinées à l'enregistrement de leurs interventions « lorsque se produit ou est susceptible de se produire un incident »[20].

13. La vidéosurveillance – caméras de vidéoprotection et caméras aéroportées – s'est considérablement développée à la faveur d'une législation peu contraignante. Il convient de remettre les exigences de nécessité et de proportionnalité au cœur de la légalité de ces dispositifs attentatoires à des droits et libertés fondamentaux, à plus forte raison lorsque l'on y adjoint de l'intelligence artificielle (1ère partie). Par ailleurs, les garanties prévues à l'heure actuelle pour maintenir un équilibre entre les atteintes aux droits et libertés fondamentaux et la sauvegarde de l'ordre public sont insuffisantes. La CNCDH appelle donc à renforcer les pouvoirs des organes de contrôle (2nde partie).

1ère partie
Réaffirmer les exigences de nécessité et de proportionnalité - Restreindre l'utilisation de la vidéosurveillance

14. Depuis son inscription dans la loi n° 95-73 du 21 janvier 1995 *d'orientation et de programmation relative à la sécurité*, la liste des finalités justifiant l'installation de caméras sur la voie publique a été progressivement allongée et en compte désormais onze[21]. S'y ajoutent la possibilité d'en placer également dans les « *lieux et établissements ouverts au public aux fins d'y assurer la sécurité des personnes et des biens lorsque ces lieux et établissements sont particulièrement exposés à des risques d'agression ou de vol* » ou encore, à la demande de commerçants, pour assurer « *la protection des abords immédiats de leurs bâtiments et installations* », dans les lieux particulièrement exposés aux mêmes types de risques. Hormis ces finalités d'usage « ordinaires », pour lesquelles l'installation requiert une autorisation préfectorale rendue après avis d'une commission départementale, la « tenue imminente d'une manifestation ou d'un rassemblement de grande ampleur présentant des risques particuliers d'atteinte à la sécurité des personnes et des biens » peut également constituer un motif d'autorisation préfectorale d'installation de caméras, cette fois-ci sans avis de la commission[22].

15. Ensuite, la loi n° 2022-52 du 24 janvier 2022 *relative à la responsabilité pénale et à la sécurité intérieure* qui a introduit la possibilité de recourir à des caméras aéroportées (par hélicoptères ou par drones), a prévu six finalités, dont quatre coïncident avec ce qui est prévu pour la vidéoprotection (prévention des atteintes à la sécurité des personnes dans des lieux particulièrement exposés à des risques, prévention d'actes de terrorisme, régulation des flux de transport, sécurité des personnes), mais dont deux constituent des motifs nouveaux : la sécurité des rassemblements publics et la surveillance

des frontières.

16. En légalisant les drones, le législateur a donc non seulement déployé des outils dotés de capacités de captation plus importantes et plus dynamiques que les caméras fixes, mais a aussi étendu le champ de la surveillance à des domaines sensibles qui ont trait à la liberté de manifester ou à la surveillance des personnes en migration.

17. La CNCDH a déjà eu l'occasion d'exprimer ses craintes à l'égard de l'utilisation des drones pour la surveillance des manifestations, susceptible de dissuader les personnes d'exercer leur liberté de manifester[23]. Elle relevait également que ces outils de surveillance peuvent aussi s'apparenter par eux-mêmes à des outils d'intimidation, en particulier lorsqu'ils sont équipés d'un haut-parleur ou d'une sirène. La surveillance des frontières ne figurait pas dans la proposition de loi que la CNCDH avait examinée. Or, les réserves exprimées dans l'avis de 2020 sont tout aussi valables dans ce domaine. Sans compter que ces drones engendrent des comportements à risque de la part des personnes en migration, soucieuses d'échapper à leur surveillance.

18. Initialement, la législation de 1995 distinguait entre deux types d'image : celles utilisées pour la « constitution d'un fichier nominatif » et les autres. Seules les premières étaient considérées comme des informations nominatives au sens de la loi dite « Informatique et libertés » de 1978[24]. La plupart des images collectées échappaient donc au régime légal relatif à ce que l'on appelle désormais la protection des données à caractère personnel.

19. Depuis une réforme récente[25], tous les systèmes de vidéo-protection sont assimilés à des traitements de données à caractère personnel relevant donc à la fois des dispositions du CSI et de celles relatives à ce type de données : selon les finalités envisagées, le Règlement général sur la protection des données (RGPD) ou bien les nouveaux articles de la loi de 1978 qui transposent la directive « Police - Justice » de 2016[26] (lorsqu'il s'agit des finalités en lien avec la sécurité publique). À l'origine, la demande d'autorisation d'installation des caméras de vidéoprotection devait simplement mentionner l'une des finalités légales et inclure un certain nombre de garanties (durée de

conservation, information du public, agents habilités à visionner les images etc.), sans autre exigence. Depuis la transposition de la directive de 2016, ces systèmes doivent répondre en outre à des conditions de nécessité et de proportionnalité[27]. Cependant, l'examen de ces conditions est appelé à figurer uniquement dans l'analyse d'impact relative à la protection des données (AIPD) que doit réaliser l'autorité publique responsable du traitement. Or, le plus souvent, ce document n'est pas transmis à la Commission nationale de l'informatique et des libertés (CNIL) dans la mesure où cette dernière ne doit être consultée que si l'analyse fait apparaître « *un risque élevé si le responsable de traitement ne prenait pas de mesures pour atténuer le risque* » ou si le traitement « *en raison de l'utilisation de nouveaux mécanismes, technologies ou procédures, présente des risques élevés pour les libertés et les droits des personnes concernées* »[28].

20. La CNCDH regrette que l'encadrement de la vidéoprotection soit principalement centré sur la protection des données personnelles alors qu'elle porte également atteinte à d'autres droits fondamentaux. A des fins de cohérence et de lisibilité du régime légal de la vidéoprotection, la CNCDH invite le législateur à faire figurer les exigences de nécessité et de proportionnalité dans le CSI lui-même. La Commission relève d'ailleurs que c'est ce dernier qui précise, mais s'agissant seulement des caméras aéroportées, que leur utilisation doit « *être strictement nécessaire à l'exercice des missions concernées et adaptée au regard des circonstances de chaque intervention* » [29].

21. C'est la raison pour laquelle la CNCDH insiste pour faire de la nécessité et de la proportionnalité des exigences fondamentales requises pour l'autorisation d'un système de vidéoprotection : une caméra ne devrait pas, par principe, être active à toute heure de la journée et à tout moment de l'année. La demande d'autorisation adressée au préfet devrait exposer les risques de troubles à l'ordre public justifiant l'installation de caméras, sur le modèle de ce qui est exigé de la part des autorités publiques dans l'exercice de leurs pouvoirs de police administrative. Cette évolution permettrait de rétablir l'équilibre rompu par des garanties insuffisantes[30].

22. Le cadre légal relatif aux caméras aéroportées soumet, d'ores et

déjà, à des exigences de nécessité et de proportionnalité les demandes d'autorisation adressées à la préfecture par les services de police ou de gendarmerie lorsqu'ils souhaitent y recourir. Le Conseil constitutionnel a d'ailleurs retenu une conception stricte de la proportionnalité – la subsidiarité, puisqu'il enjoint au préfet de « *s'assurer que le service ne peut employer d'autres moyens moins intrusifs au regard* [du droit au respect de la vie privée] *ou que l'utilisation de ces autres moyens serait susceptible d'entraîner des menaces graves pour l'intégrité physique des agents* »[31]. La CNCDH regrette toutefois que le respect de ces exigences ne fasse pas l'objet d'un contrôle indépendant systématique, l'intervention du juge administratif étant tributaire de la saisine en référé par une ou des associations de défense des droits. En l'état l'effectivité du système repose sur la vigilance des associations.

23. La CNCDH invite donc les pouvoirs publics à mieux faire respecter les conditions d'emploi, tant des caméras de vidéoprotection que de celles aéroportées. De plus, la manière dont les commissions départementales de vidéoprotection s'acquittent de leur mission de contrôle vis-à-vis des premières demeure obscure[32]. C'est d'autant plus regrettable qu'elles étaient conçues à l'origine comme un contre-pouvoir au pouvoir préfectoral. Par ailleurs, malgré sa détermination et la qualité de ses travaux, la CNIL est loin de disposer des ressources humaines permettant de réaliser des contrôles a posteriori auprès de toutes les municipalités

24. En conséquence, la CNCDH recommande de renforcer la mission de contrôle des commissions départementales de vidéoprotection en soumettant l'autorisation du préfet d'installer des caméras, ou de faire appel à des drones, à leur avis conforme. Un avis négatif pourra faire l'objet d'un recours par le préfet devant le juge administratif. À l'inverse, un avis positif pourra bien évidemment être contesté par toute personne concernée ou encore par une association de défense des droits humains.

25. S'agissant de la VSA et de la reconnaissance faciale, elles engendrent des problèmes particuliers et aggravent les risques d'atteintes aux droits et libertés fondamentaux déjà liés à l'utilisation des caméras fixes ou aéroportées. Pour leur conception, ces logiciels

reposent sur ce que l'on appelle l'apprentissage machine (*machine learning*) : à l'inverse d'un logiciel issu de la codification d'instructions définies par le programmeur (démarche déductive), ces logiciels sont le fruit d'un « apprentissage » réalisé à partir d'une multitude de données (démarche inductive). Or, ces données peuvent être biaisées au sens où sont surreprésentées certaines catégories de données par rapport à d'autres. Le modèle algorithmique issu de l'apprentissage reflètera ces biais.

26. Plusieurs types de biais peuvent avoir une incidence négative sur les personnes. D'abord, s'agissant de la reconnaissance faciale, des études ont montré que les logiciels étaient plus performants avec les hommes blancs, surreprésentés dans les images utilisées dans la phase d'apprentissage[33]. Autrement dit, les logiciels commettent plus d'erreurs pour l'identification de personnes d'ascendance africaine, et plus encore lorsqu'il s'agit de femmes. Ce type d'erreur peut avoir pour conséquence l'interpellation d'une personne identifiée à tort comme une personne recherchée[34]. Un autre type de discrimination est susceptible de survenir lorsque l'on utilise la VSA. Dans l'hypothèse où le logiciel a été programmé pour identifier des situations préoccupantes, les programmeurs vont soumettre à la machine un certain nombre d'images collectées antérieurement par des systèmes de vidéo et sélectionnées en raison de leur pertinence pour la finalité poursuivie. La machine pourrait donc être amenée à associer un certain niveau de risque à certaines caractéristiques récurrentes dans ces images (par exemple, le port d'une capuche).

27. Ce type de biais pourrait théoriquement être surmonté par la constitution de panels de données plus représentatifs de la diversité de la population mais la constitution de ces bases de données plus larges soulève d'autres problèmes relatifs à la protection des données. À ce sujet, la CNCDH rappelle les dérives observées chez certains acteurs industriels tentés de collecter des photographies de visage postées sur les réseaux sociaux, sans l'autorisation des personnes concernées[35].

28. S'agissant de la VSA, contrôler l'absence de biais s'apparente à l'heure actuelle à un vœu pieux. Il est quasiment impossible d'identifier les biais retenus par la machine au cours de son apprentissage. La

CNCDH relève à cet égard le caractère impraticable de la garantie prévue par l'expérimentation de la VSA relative au contrôle des biais. En revanche, il serait possible de mettre au jour les discriminations produites à travers son usage. Dès lors, tout utilisateur d'un logiciel de VSA doit s'assurer du caractère non discriminatoire de ce dernier et, dans le cas contraire, prendre toutes les mesures propres à y remédier.

29. Indépendamment de la conception et du fonctionnement de l'algorithme, la CNCDH attire l'attention sur d'autres risques de discrimination susceptibles de survenir au stade de l'utilisation du logiciel. Ainsi à travers le paramétrage des logiciels de VSA, par exemple sur le type de véhicule à détecter, un agent en charge de son utilisation au sein du centre de supervision urbain, pourrait cibler indirectement certaines catégories de la population circulant sur la voie publique[36].

30. Au-delà des contrôles sur les modalités du recours à la VSA, le principe même de son utilisation mérite d'être questionné. Si elle ne représente pas le même niveau d'immixtion dans la vie privée des individus présents dans l'espace public que la reconnaissance faciale, elle n'est toutefois pas dénuée de risques pour les libertés. Ces risques déjà présents avec la vidéoprotection sont amplifiés par la VSA et son analyse automatisée des images. La CNCDH souhaiterait formuler deux observations à cet égard.

31. D'abord, l'incidence de la VSA sur les droits et libertés fondamentaux dépend bien évidemment du type d'évènements censés être détectés par le logiciel. La CNCDH souscrit sur ce point à l'observation de la CNIL selon laquelle « *une appréciation globale de ces dispositifs n'a pas de sens : il convient de les appréhender au cas par cas, en fonction notamment des risques qu'ils comportent pour les personnes concernées* »[37]. Certains systèmes seront destinés à identifier un départ de feu quand d'autres auront une incidence plus significative sur les droits humains, notamment s'il s'agit d'une filature automatisée. À titre d'illustration, la loi JO qui prévoit l'utilisation de la VSA à titre expérimental, évoque des traitements algorithmiques chargés de détecter « *des événements prédéterminés susceptibles de présenter un risque* »[38]. Elle renvoie au décret le soin de préciser ce qu'ils recouvrent. Or, si certains événements parmi les huit retenus par

le gouvernement ne posent pas de problème particulier[39], d'autres ne manquent pas en revanche d'interpeller la CNCDH. En particulier, le « *non-respect par une personne* (…) *du sens de circulation commun* », ou encore une « *densité trop importante de personnes* » : en associant une alerte à un sens de circulation piétonnière « anormal », le premier révèle une conception de l'ordre public excessivement normalisée. Il expose ainsi le système à des signalements inopportuns qui peuvent conduire à des interpellations indues. Quant à la densité de population, elle interroge sur le seuil qui sera retenu par les utilisateurs du logiciel pour justifier une alerte.

32. Ensuite, indépendamment du type d'événement retenu pour une détection automatisée, la CNCDH s'inquiète de la perception publique de ces dispositifs de surveillance. D'après les premiers retours de terrain sur l'information du public de l'emploi de la VSA[40], celle-ci était peu lisible voire inaccessible. À ce stade, la Commission ne peut évidemment pas préjuger des améliorations éventuelles à venir en la matière. Cependant, au regard de l'information affichée sur les caméras fixes, la CNCDH craint qu'à défaut d'une recherche dans les textes officiels, les citoyens ne soient pas avertis dans le détail des objets et situations détectés par la VSA. C'est pourquoi, informés par les médias du déploiement de la « vidéosurveillance augmentée » dans l'espace public, alertés régulièrement sur les dérives de la reconnaissance faciale dans des pays totalitaires, ils risquent de développer un sentiment de surveillance accrue. Loin d'être mineures, ces évolutions et ces perceptions bouleversent en profondeur notre conception de l'espace public en lui retirant toute dimension privée. La CNCDH rappelle que l'espace public a historiquement vocation à être un lieu de circulation anonyme qui permet l'exercice des libertés et le respect de la vie privée.

33. S'agissant de l'identification biométrique dans l'espace public, en particulier la reconnaissance faciale, le risque d'atteinte aux droits et libertés fondamentaux est encore plus massif[41]. La CNCDH a déjà eu l'occasion d'exprimer ses réserves à l'égard de la règlementation de l'UE relative à l'IA qui, après avoir posé une interdiction de principe de l'identification biométrique à distance en temps réel dans des espaces accessibles au public, prévoyait de trop nombreuses exceptions[42]. Le texte finalement adopté atténue la portée de certaines d'entre elles

mais aménage encore de larges possibilités d'y recourir[43]. La CNCDH renouvelle donc sa recommandation d'interdire l'identification biométrique à distance des personnes dans l'espace public et les lieux accessibles au public, en admettant pour seule exception son utilisation pour répondre à une menace grave et imminente pour la vie, ou la sécurité des personnes et celle des ouvrages, installations et établissements d'importance vitale.

2ème partie
Renforcer les garanties qui encadrent l'utilisation des caméras

34. Le cadre légal actuel de la vidéosurveillance est censé assurer une conciliation équilibrée entre la sauvegarde de l'ordre public et le respect des droits et libertés fondamentaux. Face aux possibilités données aux autorités publiques d'utiliser ces dispositifs de surveillance, des garanties sont prévues pour assurer le respect des droits des citoyens. Ces garanties sont toutefois insuffisantes et méritent d'être renforcées, d'autant plus que les caméras sont de plus en plus performantes et parfois associées à des logiciels de traitement automatisé des images.

35. Un certain nombre de garanties, qui relèvent de la protection des données à caractère personnel, sont insuffisantes, faute d'une mise en œuvre appropriée. En principe, la présence des caméras sur la voie publique doit être accompagnée d'un panneau affichant de manière visible un certain nombre d'informations, en particulier les finalités, les coordonnées du responsable de traitement, ainsi que la possibilité d'adresser une réclamation à la CNIL[44]. Or, ces panneaux sont, en réalité, rares, de taille réduite et se fondent dans le décor. S'agissant des caméras aéroportées, le public doit être informé de leur utilisation « par tout moyen approprié », le législateur ayant ajouté deux motifs d'exception particulièrement évasifs : « *lorsque les circonstances l'interdisent ou que cette information entrerait en contradiction avec les objectifs poursuivis* »[45]. La loi JO a repris exactement les mêmes termes, y compris s'agissant des exceptions, pour l'information du public de l'utilisation d'un logiciel d'analyse automatisée des images collectées par les caméras. Jusqu'à présent, la publication d'arrêtés préfectoraux autorisant des drones tenait lieu d'information au public, tandis que les premières remontées de terrain témoignent d'un défaut d'information sur l'utilisation de la VSA.

36. La CNCDH s'interroge tant sur le sens de l'information donnée au public que sur sa portée. D'un côté, les informations portent sur

l'utilisation de dispositifs de captation fixes ou aéroportées, ou encore d'un outil d'analyse automatisée des images, d'un autre côté, elles portent sur les droits des personnes. S'agissant des premières, elles peuvent sans doute avoir une utilité pour la recherche du responsable de traitement (qu'il s'agisse d'une collectivité locale ou d'un établissement ouvert au public, par exemple). Elles seront également utiles si elles précisent l'utilisation d'un logiciel de VSA. Reste que les citoyens ont pris l'habitude de passer à côté de ces panneaux sans y prêter attention. Quant aux caméras aéroportées, les citoyens devraient être avertis en amont de leur déploiement et d'une façon qui leur permette d'accéder facilement à l'information.

37. Quand bien même les citoyens seraient correctement informés de leurs droits, ces derniers souffrent de limitations importantes. Les droits habituellement prévus par la réglementation relative à la protection des données à caractère personnel, sont principalement celui d'accéder à ces données, celui de les rectifier ou de les supprimer. D'après la loi cependant, ces droits peuvent faire l'objet de restrictions pour « *éviter de nuire à la prévention ou à la détection d›infractions pénales, aux enquêtes ou aux poursuites en la matière ou à l'exécution de sanctions pénales* » ou pour « *protéger la sécurité publique* »[46], cette possibilité étant laissée à l'appréciation du responsable de traitement. En tant que telle, la reconnaissance de ces droits n'offre donc aucune garantie aux citoyens contre des abus éventuels.

38. La plupart des textes juridiques actuellement en vigueur[47], lorsqu'ils traitent des algorithmes ayant des impacts défavorables sur les droits et libertés individuels, requièrent un examen individuel des résultats de l'IA par des moyens non automatisés. La loi d'expérimentation de la VSA prend d'ailleurs le soin de préciser que les logiciels ne procèdent qu'à des « *signalement d'attention* » et « *demeurent en permanence sous le contrôle* » d'un agent humain. La CNCDH n'est toutefois pas convaincue par cette garantie, étant donné la propension de chacun à suivre les recommandations ou alertes produites par un programme informatique (parfois appelé « biais d'automatisation »). Les agents en charge de la supervision de la VSA seront d'ailleurs d'autant plus tentés de mobiliser une équipe sur le terrain pour vérifier le risque associé à une alerte, que le logiciel conservera l'enregistrement de tous les

signalements : l'agent sera donc incité à les suivre. L'agent humain se trouvera ainsi davantage en position d'exécutant que de contrôleur vis-à-vis de la machine. L'enregistrement des alertes réalisées par le logiciel, ainsi que la mise en place d'un registre des suites qui leur sont apportées, prévus par la loi JO, présentent évidemment toute leur utilité dans le cadre d'une expérimentation. La CNCDH recommande cependant aux pouvoirs publics de mener une réflexion sur les moyens de garantir effectivement l'autonomie de l'agent face aux alertes de la machine.

39. Par ailleurs, en amont de l'installation d'un système de vidéoprotection ayant une finalité sécuritaire, une autorité publique doit réaliser une analyse d'impact relative à la protection des données personnelles. Ces analyses d'impact sont purement déclaratives, et reposent donc sur une appréciation souveraine des risques, et des moyens d'y remédier, réalisée par les autorités publiques souhaitant recourir à la vidéoprotection. En outre, leur portée est limitée à l'examen de l'incidence de cette dernière sur la protection des données et ignore par conséquent des aspects plus fondamentaux tels que l'incidence d'un dispositif de vidéoprotection sur des libertés fondamentales comme celle d'aller et venir, ou de manifester. Ces réserves valent aussi d'ailleurs pour l'analyse d'impact prévue par l'expérimentation de la VSA.

40. La CNCDH relève que la loi JO prévoit un certain nombre de garanties, en lien avec des aspects techniques, dont il sera difficile d'assurer le contrôle en pratique. Des garanties doivent notamment être apportées afin que les données d'apprentissage, de validation et de test choisies pour la conception du logiciel soient « *pertinentes, adéquates et représentatives* ». La loi ajoute que leur traitement doit être « *loyal et éthique, reposer sur des critères objectifs et permettre d'identifier et de prévenir l'occurrence de biais et d'erreurs* ». Ces données doivent aussi faire l'objet de mesures de « sécurisation appropriées ». S'y ajoute l'obligation de mettre en place un « s*ystème de gestion des risques permettant de prévenir et de corriger la survenue de biais éventuels ou de mauvaises utilisations* ». Outre qu'aucun dispositif technologique n'est en mesure d'assurer l'intégrité des images, en les mettant à l'abri de manipulations diverses, la CNIL ne dispose pas des moyens d'assurer

un contrôle effectif sur un certain nombre d'aspects technologiques, à commencer par la présence de biais éventuels dans le fonctionnement de la VSA.

41. Ces dernières années, les réformes se sont succédé pour élargir les catégories d'agents autorisées à visionner les images collectées par les caméras. La loi du 25 mai 2021 *pour une sécurité globale préservant les libertés,* notamment, a ouvert la possibilité pour des agents des collectivités locales, non membres de la police municipale, de visionner les images filmées sur la voie publique par les caméras de vidéoprotection[48]. Pour ce faire, ils doivent bénéficier d'un agrément, délivré par le préfet du département concerné, uniquement au terme d'une enquête administrative[49]. Dernière illustration de cette extension, la proposition de loi *relative au renforcement de la sûreté dans les transports* actuellement en discussion au Parlement[50], envisage d'autoriser des agents d'Ile de France Mobilité, dûment habilités, à visionner les images issues des caméras déployées dans les réseaux de transport. De manière générale, la CNCDH relève qu'aucune exigence de formation spécifique n'est prévue pour les personnes en charge du visionnage des images collectées. Elle recommande donc une formation de l'ensemble de ces agents à la fois sur les aspects techniques – y compris sur le fonctionnement de l'IA – et déontologiques.

42. La CNCDH relève que les commissions départementales de vidéoprotection avaient été conçues à l'origine comme un véritable levier de contrôle, en amont et en aval des autorisations de recourir à des caméras de surveillance de l'espace public. Il convient non seulement de renforcer leurs prérogatives de contrôle[51], mais également de revoir leur composition. À l'heure actuelle, elles sont composées de quatre membres : un magistrat du siège ou un magistrat honoraire, un maire, un représentant de la chambre de commerce et d'industrie du département, et une personnalité qualifiée choisie par le préfet en raison de sa compétence[52] « *dans le domaine de la vidéoprotection ou des libertés individuelle*s »[53]. Afin d'assurer une représentation plus équilibrée des intérêts en présence, la CNCDH recommande de réformer la commission départementale de vidéoprotection pour qu'elle soit désormais composée de la manière suivante :

- Une personne qualifiée désignée par le Défenseur des droits ;

• Un magistrat en exercice désigné par le premier président de la cour d'appel ;

• Un maire, désigné par la ou les associations départementales des maires, ou, à Paris, un conseiller de Paris ou conseiller d'arrondissement désigné par le conseil de Paris ;

• Un représentant désigné par la ou les chambres de commerce et d'industrie territorialement compétentes ;

• Un conseiller départemental désigné par un vote à une majorité qualifiée du Conseil.

43. La loi relative à l'organisation des JO a supprimé l'article du CSI[54] qui enjoignait au Gouvernement de transmettre chaque année à la CNIL un rapport faisant état de l'activité des commissions départementales de vidéoprotection et des conditions d'application du titre du CSI relatif à la vidéoprotection. Attachée à réhabiliter la mission de contrôle de ces commissions, la CNCDH regrette cette abrogation. Elle recommande l'élaboration par ces commissions d'un rapport annuel d'activité, rendu public, et destiné à faire l'objet d'un débat au Conseil départemental. À travers ces dispositifs institutionnels, la CNCDH souhaite que le déploiement de la vidéosurveillance fasse l'objet d'un débat démocratique local reposant sur l'expertise d'une instance dédiée.

44. En conclusion, la CNCDH appelle les pouvoirs publics à reconsidérer leur volonté d'accélérer le déploiement des dispositifs de vidéoprotection. Elle s'associe à la CNIL pour solliciter l'organisation d'un débat démocratique relatif à l'utilisation de la VSA. Garantir la sécurité publique est, certes, un objectif légitime ; personne ne doute que l'installation de caméras à certains endroits peut utilement y contribuer. Cela doit toutefois donner lieu à un examen circonstancié, en partant d'une exigence de minimisation de leur présence et de leur impact dans l'espace public. En outre, ce questionnement doit s'inscrire dans une réflexion plus large relative aux causes de l'insécurité, au type de rapport entre police et population à privilégier[55]. Ce qui se joue en définitive, c'est un choix de société : assurer la primauté de la liberté, des corps et des esprits, sous réserve des restrictions requises par la sauvegarde de l'ordre public, ou au contraire faire le choix de la brider par une surveillance généralisée et automatisée.

Liste des recommandations

Recommandation n° 1 : Réaliser une cartographie officielle des systèmes de vidéoprotection installés sur le territoire national, ainsi qu'une cartographie à l'échelon de la commune, accessibles au public dans les mairies et en ligne.

Recommandation n° 2 : Insérer, au sein du titre du code de la sécurité intérieure relatif à la vidéoprotection, une disposition qui conditionne l'installation d'un système de vidéoprotection à l'exigence de son caractère nécessaire et proportionné à l'exercice des finalités envisagées, et non discriminatoire.

Recommandation n° 3 : Assortir la demande d'autorisation de systèmes de vidéoprotection adressée au préfet d'une analyse d'impact sur les droits et libertés des personnes, précisant notamment les modalités d'enregistrement et de supervision.

Recommandation n° 4 : Interdire l'identification biométrique à distance en temps réel des personnes dans l'espace public et les lieux accessibles au public, en admettant pour seule exception son utilisation pour la prévention d'une menace grave et imminente pour la vie, ou la sécurité des personnes et celle des ouvrages, installations et établissements d'importance vitale.

Recommandation n° 5 : Assurer une formation appropriée sur la protection des données, incluant une composante sur le fonctionnement des logiciels issus d'un apprentissage machine, aux agents en charge du visionnage des images.

Recommandation n° 6 : Mener une réflexion sur les moyens de garantir effectivement l'autonomie d'un agent humain face aux alertes produites par un traitement algorithmique d'images.

Recommandation n° 7 : Allouer davantage de moyens humains à la CNIL pour renforcer ses capacités de contrôle des systèmes de vidéoprotection.

Recommandation n° 8 : Renforcer les pouvoirs de la commission départementale de vidéoprotection en subordonnant à son avis conforme toute installation d'un système de vidéoprotection ou d'utilisation d'une caméra aéroportée.

Recommandation n° 9 : Réformer la composition de la commission départementale de vidéoprotection en y incluant :

- Une personne qualifiée désignée par le Défenseur des droits ;
- Un magistrat en exercice désigné par le premier président de la cour d'appel ;
- Un maire, désigné par la ou les associations départementales des maires, ou, à Paris, un conseiller de Paris ou conseiller d'arrondissement désigné par le conseil de Paris ;
- Un représentant désigné par la ou les chambres de commerce et d'industrie territorialement compétentes ;
- Un conseiller départemental désigné par un vote à une majorité du Conseil.

Recommandation n° 10 : Rendre obligatoire la publication d'un rapport annuel d'activité par la commission départementale de la vidéoprotection, soumis au débat au Conseil départemental.

Liste des personnes auditionnées

Quentin BARENNE, cofondateur de Wintics.

Florent CASTAGNINO, maître de conférences en sociologie de l'Institut Mines-Télécom.

William ELDIN et François MATTENS, CEO et directeur des affaires publiques chez XXII.

Philippe LATOMBE, député, co-rapporteur d'une mission d'information sur les enjeux de l'utilisation d'images de sécurité dans le domaine public dans une finalité de lutte contre l'insécurité.

Caroline LEQUESNE, maîtresse de conférences en droit public à l'Université Côté d'Azur.

Robin MEDARD INGHILTERRA, maître de conférences en droit public à l'Université Paris 1 Panthéon-Sorbonne.

Myrtille PICAUD, chargée de recherches en sociologie au CNRS au CRESPPA-CSU.

Noémie LEVAIN, Marne STRAZIELLE, Bastien LE QUERREC, de La Quadrature du Net.

Notes de fin

1. Parfois aussi qualifiée d'« augmentée » ou d'« automatisée », ou bien encore d'« intelligente ». Prenant ses distances avec des expressions davantage destinées à la promotion qu'à la description de ces nouvelles technologies, l'avis évoquera la « VSA » pour désigner l'analyse d'images numériques par des traitements algorithmiques.
2. L'expérimentation prendra fin le 31 mars 2025 mais un rapport d'évaluation de la mise en œuvre de l'expérimentation doit être remis au Parlement au plus tard le 31 décembre 2024. Les premières utilisations ont eu lieu à titre d'essai, après la désignation en janvier 2024 des entreprises attributaires du marché public, depuis mars 2024 pour quelques concerts et événements sportifs.
3. Loi n° 95-73 du 21 janvier 1995 *d'orientation et de programmation relative à la sécurité*.
4. Consacrées à l'origine par le législateur sous le vocable de « vidéosurveillance », les caméras présentes sur la voie publique, ou dans les lieux et établissements ouverts au public sont considérées depuis la loi d'orientation et de programmation pour la performance de la sécurité intérieure, adoptée en 2011, comme des outils de « vidéoprotection ».
5. Instruction de 2023 : https://www.interieur.gouv.fr/actualites/communiques-de-presse/acceleration-des-projets-de-videoprotection-pour-securisation-des.
6. Loi *relative à la responsabilité pénale et à la sécurité intérieure* promulguée en janvier 2022. En réalité, les premiers drones ont été utilisés à partir de l'entrée en vigueur du décret d'application adopté tardivement, le 19 avril 2023. Pour la seule Préfecture de police de Paris, 144 arrêtés permettant l'usage de drones ou d'hélicoptères de surveillance ont été publiés depuis cette date : C. Le Foll, « En Île-de-France, la police s'autorise à déployer des drones plus d'un jour sur deux », *Mediapart,* 1er mars 2024.
7. Cour des comptes, *« Les polices municipales », Rapport public thématique*, octobre 2020.
8. G. Thierry, « Ces agents derrière les caméras des centres de supervision urbains », *La Gazette des communes,* 26 janvier 2022.
9. La préfecture de police a utilisé des drones pour faire respecter les règles du confinement. De son côté, le gouvernement a envisagé un temps de recourir à une application pour smartphones de « contact tracing », qui alertait les personnes ayant été en contact avec un malade testé positif à la Covid. Il a également autorisé la RATP et la SNCF à évaluer au moyen de caméras dans quelle mesure les voyageurs portaient leur masque.
10. Sénat, *Rapport d'information sur la reconnaissance faciale et ses risques au regard de la protection des libertés individuelles,* 2022 ; Assemblée nationale, *Rapport d'information sur les enjeux de l'utilisation d'images de sécurité dans le domaine public dans une finalité de lutte contre l'insécurité*, 2023.
11. Voir le média en ligne *Disclose*, « La police nationale utilise illégalement un logiciel israélien de reconnaissance faciale », 14 novembre 2023. À la suite de ces révélations, le ministre de l'intérieur a annoncé, le 20 novembre 2023, le lancement d'une « enquête administrative » dont les conclusions devaient être rendues « sous trois mois ». Aucune information n'a été communiquée depuis.
12. CNCDH, *Avis sur la proposition de loi relative à la sécurité globale* (A –2020- 16), Assemblée plénière du 26 novembre 2020, JORF n°0289 du 29 novembre 2020, texte n° 150.
13. CNCDH, *Avis relatif à l'impact de l'intelligence artificielle sur les droits fondamentaux*

(A – 2022 – 6), Assemblée plénière du 7 avril 2022, JORF n°0091 du 17 avril 2022, texte n° 99.
14. Depuis quelques années, les principales critiques ciblent l'absence d'efficacité avérée de ces systèmes, qui pèsent pourtant lourdement sur le budget des municipalités, sans compter un investissement accru de fonds publics pour équiper les communes. Autrement dit, les débats sur la proportionnalité des atteintes aux droits de l'homme par la vidéoprotection au nom du respect de l'ordre public ont été quasiment supplantés par des questionnements sur le rapport coût/avantage de cette technologie. Voir notamment le rapport de la Cour des comptes sur les polices municipales, ou le rapport de la mission d'information sur les images de sécurité.
15. Voir not. : Commission nationale de l'informatique et des libertés (CNIL), « Caméras dites « intelligentes » ou « augmentées » dans les espaces publics : Position sur les conditions de déploiement », Juillet 2022 ; Agence des droits fondamentaux de l'Union européenne , « Facial recognition technology : fundamental rights considerations in the context of law enforcement », novembre 2019.
16. Voir not. : Olivier Cahn, « Police et caméras : « Observer sans temps mort, jouir sans entrave », *AJ Pénal*, 2021, p. 128 ; Caroline Lequesne, « L'encadrement des technologies de surveillance des foules : réflexions sur la démocratie numérique dans l'espace public », in B. Frydman, N. Genicot, *L'intelligence artificielle face à l'état de droit*, Bruylant, 2024, pp.139-161 Robin Medard Inghilterra, « L'instauration d'une « technopolice » administrative en milieu urbain : cadre et enjeux juridiques », *La Revue des droits de l'homme,* 2024, n° 25.
17. On pourrait mentionner également la tentation de certaines municipalités d'adjoindre aux caméras des capteurs sonores, relayés à une application chargée de détecter de manière automatisée des bruits anormaux (coups de feu, bris de vitre, accident etc.).
18. C'est le point de vue de la CNIL : CNIL, « Caméras dites « intelligentes » ou « augmentées » dans les espaces publics : Position sur les conditions de déploiement », juillet 2022.
19. La machine peut apprendre en effet sans apprentissage supervisé : en plaçant une caméra dans un lieu donné, le logiciel qui lui est associé peut être programmé pour identifier des régularités dans les mouvements des passants, leur vitesse de déplacement, etc. Au bout d'un certain délai, le logiciel sera en mesure de détecter ce qu'il analysera comme un écart à la norme.
20. Art. L 241-1 et L 243-1 du CSI.
21. Cinq seulement étaient prévues initialement par la loi de 1995 : voir art. L 251-2 du CSI.
22. Art. L 252-6 du CSI.
23. CNCDH, *Avis sur la proposition de loi relative à la sécurité globale, Op.Cit.*
24. Loi n° 78-17 du 6 janvier 1978 *relative à l'informatique, aux fichiers et aux libertés.*
25. Loi 2023-380 du 19 mai 2023 relative aux jeux Olympiques et Paralympiques de 2024.
26. Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes 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, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil.
27. Loi 1978, art. 87.
28. Loi 1978, art. 90.
29. Art. L 242-4 du CSI.

30. Cf 2ème partie.
31. CC, Décision n° 2021-834 DC, Loi relative à la responsabilité pénale et à la sécurité intérieure, § 27.
32. Voir le rapport d'information de l'Assemblée nationale sur les enjeux de l'utilisation d'images de sécurité dans le domaine public dans une finalité de lutte contre l'insécurité.
33. CNCDH, *Avis relatif à l'impact de l'intelligence artificielle sur les droits fondamentaux, op.cit.*
34.https://www.numerama.com/politique/535715-reconnaissance-faciale-une-etude-montre-que-les-algorithmes-discriminent-plus-les-femmes-noires.html.
35. Voir not. : F. Reynaud, « Reconnaissance faciale : une enquête demandée à la CNIL sur les pratiques de Clearview AI », *Le Monde*, 27 mai 2021.
36. Pour se convaincre de l'intérêt que porte une commune à ce type de détection, voir les arrêtés municipaux anti-glanage.
37. CNIL, Caméras dites « intelligentes » ou « augmentées » dans les espaces publics : position sur les conditions de déploiement, Juillet 2022, p. 7.
38. Loi *relative aux Jeux olympiques et paralympiques*, art. 10.
39. Décret n°2023-828 du 28 août 2023 relatif aux modalités de mise en œuvre des traitements algorithmiques sur les images collectées au moyen de systèmes de vidéoprotection et de caméras installées sur des aéronefs, pris en application de l'article 10 de la loi n° 2023-380 du 19 mai 2023 *relative aux jeux olympiques et paralympiques* de 2024 et portant diverses autres dispositions, art. 3 : présence d'objets abandonnés, présence ou utilisation d'armes, non-respect par une personne ou un véhicule du sens de circulation commun, franchissement ou présence d'une personne ou d'un véhicule dans une zone interdite ou sensible, présence d'une personne au sol à la suite d'une chute, mouvement de foule, densité trop importante de personnes, départs de feux.
40. À l'heure où la CNCDH adopte cet avis, la VSA a déjà fait l'objet de quelques expérimentations lors de concerts parisiens et d'événements sportifs.
41. À ce sujet, voir not. : Défenseur des droits, « Technologies biométriques : l'impératif respect des droits fondamentaux », Rapport, Juillet 2021.
42. CNCDH, *Avis sur l'impact de l'intelligence artificielle sur les droits fondamentaux., op.cit.*
43. Le Conseil de l'UE a adopté le texte le 21 mai 2024. Il sera publié au Journal officiel de l'UE prochainement.
44. Art. R 253-6 du CSI.
45. Art. L 242-3 du CSI. Le décret d'application censé préciser les exceptions au principe d'information évoque l'urgence ou les conditions de l'opération ou encore si cette information entre en contradiction avec les objectifs poursuivis parmi quatre des finalités légales (la prévention des atteintes à la sécurité des personnes et des biens dans des lieux particulièrement exposés à des risques d'infraction, la prévention d'actes de terrorisme, la surveillance des frontières, la prévention des mouvements transfrontaliers de marchandises prohibées).
46. Loi 1978, art. 107.
47. Voir notamment : RGPD, art. 22.
48. Cette possibilité est ouverte aux agents des communes, EPCI, ou des syndicats mixtes réunissant des communes, des EPCI et éventuellement des départements, lorsque ces syndicats exercent la compétence relative aux dispositifs locaux de prévention de la délinquance. N'étant pas policiers, ils ne peuvent toutefois visionner ces images que dans la mesure où « *ce visionnage ne nécessite pas de leur part d'actes de police judiciaire* ».

49. Ministre de l'Intérieur, Circulaire du 16 avril 2024 relative à la mise en œuvre des agréments délivrés par le préfet de département pour l'application de l'article L. 132-14-1 du CSI.
50. Proposition de loi *relative au renforcement de la sûreté dans les transports*, déposée au Sénat le 28 décembre 2023.
51. Cf Première partie de l'avis.
52. Art. R 252-8 du CSI.
53. Art. L 251-4 du CSI.
54. Ancien article L. 251-7 du CSI.
55. CNCDH, *Avis sur les rapports entre police population : rétablir la confiance entre la police et la population*, Assemblée plénière du 11 février 2021, JORF n°0045 du 21 février 2021, Texte n° 43.

CNCDH
COMMISSION NATIONALE CONSULTATIVE DES DROITS DE L'HOMME
RÉPUBLIQUE FRANÇAISE

Créée en 1947 sous l'impulsion de René Cassin, **la Commission nationale consultative des droits de l'homme (CNCDH) est l'Institution nationale de promotion et de protection des droits de l'homme française, accréditée de statut A par les Nations Unies.**

L'action de la CNCDH s'inscrit dans une quadruple mission :
- Conseiller les pouvoirs publics en matière de droits de l'Homme ;
- Contrôler l'effectivité des engagements de la France en matière de droits de l'Homme et de droit international humanitaire ;
- Assurer un suivi de la mise en oeuvre par la France des recommandations formulées par les comités de suivi internationaux et régionaux ;
- Sensibiliser et éduquer aux droits de l'Homme.

L'indépendance de la CNCDH est consacrée par la loi. Son fonctionnement s'appuie sur le principe du pluralisme des idées.

Ainsi, seule institution assurant un dialogue continue entre la société civile et les experts français en matière de droits de l'homme, elle est composée de 64 personnalités qualifiées et représentants d'organisations non gouvernementales issues de la société civile.

La CNCDH est le rapporteur national indépendant sur la lutte contre toutes les formes de racisme depuis 1990, sur la lutte contre la traite et l'exploitation des êtres humains depuis 2014, sur la mise en œuvre des Principes directeurs des Nations Unies sur les entreprises et les droits de l'Homme depuis 2017, sur la lutte contre la haine et les discriminations anti-LGBTI depuis avril 2018 et sur l'effectivité des droits des personnes handicapées depuis 2020.

La CNCDH est en outre la Commission française de mise en œuvre du droit international humanitaire au sens du Comité international de la Croix-Rouge (CICR).

20 Avenue Ségur - TSA 40 720 - 75334 PARIS Cedex 07
Tel : 01.42.75.77.09
Mail : cncdh@cncdh.fr
www.cncdh.fr