UNIVERSITÉ CATHOLIQUE DE LILLE
FACULTÉ DE DROIT

MASTER 1 Droit, Gouvernance et Digital

Dissertation
"État, Administration et Numérique"

Sujet : *La surveillance étatique de masse, une pratique permise par l'essor du numérique*

Présentée par :
Antonin LACOUTURE-RAIMBAULT

Promotion : M1 DG&D
Année universitaire : 2024 – 2025

Sous la direction de :
Kamel EL HILALI

TABLE DES MATIERES

INTRODUCTION

Lors des Jeux olympiques et paralympiques de Paris en 2024, la France a expérimenté l'utilisation de la vidéosurveillance algorithmique (VSA), une technologie visant à analyser en temps réel les images captées par les caméras de surveillance pour détecter automatiquement des situations considérées comme anormales, telles que des mouvements de foule ou des objets abandonnés. Cette initiative, bien que justifiée par le gouvernement par des impératifs de sécurité, a suscité de vives critiques quant à son impact sur les libertés individuelles et le respect de la vie privée. Des organisations telles qu'Amnesty International ont exprimé leurs inquiétudes, soulignant que la VSA pourrait ouvrir la voie à une surveillance de masse intrusive et discriminatoire. La Quadrature du Net, une association de défense des libertés numériques, a également dénoncé une technologie susceptible de renforcer les biais sociaux et de cibler injustement les populations les plus vulnérables, notamment les personnes précaires passant davantage de temps dans l'espace public. Par ailleurs, des rapports ont mis en évidence l'inefficacité de ces dispositifs, avec un nombre important de faux positifs, remettant en question leur utilité réelle.

Cette situation illustre parfaitement les défis contemporains liés à l'essor du numérique dans les pratiques de surveillance étatique. À l'ère du numérique, les États ont vu leurs capacités techniques profondément transformées. La collecte, le traitement et la circulation des données à une vitesse inédite permettent désormais à l'État, en tant qu'acteur institutionnel, d'exercer un pouvoir de surveillance sans précédent. Cette évolution, bien que souvent justifiée par la nécessité de garantir la sécurité publique ou de prévenir le terrorisme, pose avec acuité la question des dérives potentielles d'un tel pouvoir, et de sa compatibilité avec les principes fondamentaux d'un État de droit. Le numérique, en tant qu'infrastructure technique et idéologique, redéfinit ainsi les frontières entre sécurité et liberté, entre transparence et opacité, entre efficacité administrative et respect des droits fondamentaux.

Historiquement, le pouvoir politique a toujours été étroitement lié à la maîtrise de l'information. L'administration moderne s'est construite autour de cette nécessité de capter, organiser et mobiliser les données afin d'orienter l'action publique. Or, les outils numériques renforcent cette dynamique en rendant l'information non seulement plus accessible mais également plus centralisée, analysable et exploitable à grande échelle. La généralisation des technologies comme la reconnaissance faciale, les algorithmes de prédiction comportementale, la vidéosurveillance intelligente ou encore le croisement massif de bases de données modifie radicalement les rapports entre citoyens et

administration. L'État ne se contente plus d'intervenir *ex post*, il anticipe, surveille et potentiellement sanctionne *ex ante*, dans une logique de prévention fondée sur des données probabilistes. Cette mutation de l'action publique est porteuse d'enjeux démocratiques majeurs. D'une part, elle interroge la légalité et la légitimité des dispositifs de surveillance de masse, au regard des principes de proportionnalité, de finalité et de nécessité qui encadrent juridiquement toute atteinte aux libertés. D'autre part, elle soulève des inquiétudes en matière de gouvernance algorithmique, de transparence des décisions publiques et de capacité de contrôle par les citoyens et les juges. Le recours aux acteurs privés pour développer ou opérer ces dispositifs ajoute une dimension de complexité supplémentaire ; entre dépendance technique, souveraineté numérique affaiblie, confusion des responsabilités.

Dans ce contexte, l'étude de la surveillance étatique de masse à l'ère du numérique s'avère juridiquement nécessaire. D'abord parce qu'elle met directement en tension des droits fondamentaux protégés par la Constitution comme le droit au respect de la vie privée, la liberté d'aller et venir ou encore la liberté d'expression, et les instruments internationaux que sont l'article 8 CEDH, et l'article 17 du Pacte international relatif aux droits civils et politiques. L'encadrement juridique de la surveillance est un enjeu de légitimité de l'action publique : sans garantie procédurale, le risque d'arbitraire devient systémique. Ensuite, l'analyse permet d'interroger la robustesse du contrôle juridictionnel en matière de technologies de surveillance, dans un contexte où les dispositifs sont souvent opaques, techniques et asymétriques.

Mais l'intérêt du sujet dépasse le cadre purement juridique. Dans un monde marqué par la multiplication des crises sécuritaires, sanitaires et climatiques, la tentation de recourir à des outils de surveillance automatisée devient de plus en plus forte. L'espace numérique est devenu le principal vecteur de circulation des idées, des contestations et des solidarités, mais aussi un terrain de contrôle. Interroger la montée en puissance de la surveillance numérique, c'est aussi comprendre comment les États façonnent le rapport des citoyens à l'espace public, au politique ou à la liberté. Il s'agit, en somme, d'une question éminemment actuelle, qui engage les fondements mêmes de la démocratie contemporaine.

La présente étude se propose ainsi, à travers une approche juridique et institutionnelle, de répondre à la question suivante : « Comment le numérique contribue-t-il au développement de la surveillance étatique de masse à travers le monde ? ». Il s'agira dans un premier temps de démontrer que le numérique agit comme un catalyseur de la surveillance globale (**I**), avant d'envisager les tensions et les réponses juridiques suscitées par cette nouvelle donne technologique dans les États de droit (**II**).

I – LE NUMERIQUE COMME CATALYSEUR D'UNE SURVEILLANCE ETATIQUE GLOBALE

Dans cette partie, nous analyserons d'abord comment les technologies numériques ont été mises au service d'une logique sécuritaire de surveillance à large échelle (*A*), avant d'étudier les mécanismes juridiques et politiques ayant contribué à leur normalisation progressive (*B*).

A – L'ESSOR DES TECHNOLOGIES NUMERIQUES AU SERVICE DE LA SURVEILLANCE

L'essor du numérique a profondément renouvelé les modalités de surveillance des populations par l'État. Si la surveillance n'est en soi ni nouvelle ni illégitime dès lors qu'elle sert l'intérêt général, la mutation technologique qu'elle traverse depuis deux décennies modifie radicalement son échelle, sa temporalité, ses objectifs et sa portée politique. À l'heure où les administrations publiques déploient massivement des outils d'analyse algorithmique, de captation continue des données et d'automatisation décisionnelle, il ne s'agit plus seulement de surveiller pour prévenir ou réprimer, mais de détecter, prédire et encadrer les comportements sociaux dans un flux constant. Le numérique devient ainsi un instrument de gouvernement des conduites.

Cette dynamique repose sur ce qu'Antonio Casilli qualifie de « *nouveau régime de surveillance de masse* » : un dispositif diffus, intégré à l'environnement numérique quotidien, dans lequel les individus participent eux-mêmes à leur traçabilité en produisant, volontairement ou non, des données d'usage, de géolocalisation, de connexion ou d'interaction sociale[1]. La surveillance cesse d'être une pratique ponctuelle pour devenir une infrastructure : elle n'intervient plus seulement dans des situations exceptionnelles, mais s'imbrique dans les rouages mêmes de l'État social et numérique. Les frontières classiques entre sphère privée et sphère publique, entre suspicion ciblée et observation de masse, entre surveillance humaine et traitement automatisé, tendent à s'effacer.

[1] 'Antonio A. Casilli. Quatre thèses sur la surveillance numérique de masse et la négociation de la vie privée. Jacky Richard et Laurent Cytermann. Étude annuelle 2014 du Conseil d'État "Le numérique et les droits fondamentaux", La Documentation Française, pp.423-434, 2014, Études et documents, Conseil d'État'.

Cette logique est incarnée de manière particulièrement frappante dans la vidéosurveillance algorithmique. Félix Tréguer, dans son ouvrage *Technopolice*, montre comment les dispositifs de détection automatisée des « *comportements anormaux* » (stationnements prolongés, rassemblements et objets abandonnés) s'intègrent aujourd'hui dans les politiques sécuritaires des grandes métropoles françaises, notamment à l'occasion d'événements d'envergure comme les Jeux Olympiques de Paris 2024 comme précédemment mentionné[2]. À la différence des caméras classiques, ces technologies ne se contentent pas d'enregistrer : elles interprètent, classent et déclenchent des alertes sans intervention humaine directe. L'espace public devient ainsi un environnement calculé, dont les usages déviants sont traités statistiquement, non juridiquement.

Cette automatisation de la détection s'accompagne d'un brouillage croissant entre régulation publique et logique technique. Les algorithmes sont souvent conçus, entraînés et maintenus par des prestataires privés, dans le cadre de contrats dont les modalités d'exécution et les critères d'efficacité restent largement opaques pour les citoyens comme pour les juges. Cela introduit une asymétrie inquiétante : ceux qui subissent la surveillance ne savent ni comment elle fonctionne, si s'ils peuvent y résister. Dans une tribune au Monde récente, Tréguer alerte sur le « *tempo des algorithmes* », qui impose aux autorités une accélération constante, au risque que les garanties démocratiques deviennent secondaires, presque accessoires[3].

L'Organisation des Nations Unies partage cette inquiétude. En 2022, le Conseil de Sécurité a reconnu que les technologies numériques, tout en offrant des opportunités inédites pour la gouvernance, pouvaient également être détournées à des fins de répression ou de contrôle social. Le numérique n'est pas neutre : il agit comme une amplification du pouvoir étatique, renforçant à la fois l'autorité et, malheureusement, les logiques de défiance[4]. L'utilisation extensive d'outils de surveillance prédictive, notamment fondés sur l'intelligence artificielle, expose les sociétés à une transformation silencieuse du rôle de l'État, qui passe d'un État garant à un État prédicteur.

---

[2] '« Une surveillance algorithmique constante de l'espace public est dangereuse politiquement »' (11 October 2024) <https://www.lemonde.fr/pixels/article/2024/10/11/une-surveillance-algorithmique-constante-de-l-espace-public-est-dangereuse-politiquement_6349397_4408996.html>.

[3] '« Technopolice » : L'accélération Du Tempo Des Algorithmes, Au Détriment Des Libertés Publiques' <https://www.lemonde.fr/idees/article/2024/10/15/technopolice-l-acceleration-du-tempo-des-algorithmes-au-detriment-des-libertes-publiques_6352342_3232.html>.

[4] 'Conseil de Sécurité: Les Technologies Numériques Présentent Autant de Défis Que d'opportunités En Matière de Paix et de Sécurité | Couverture Des Réunions & Communiqués de Presse' <https://press.un.org/fr/2022/cs14899.doc.htm>.

Cette reconfiguration a été analysée de manière approfondie par le Conseil de l'Europe. Dans une étude de 2021 consacrée aux technologies numériques avancées, l'institution souligne que la plupart des dispositifs déployés échappent aux schémas classiques de responsabilité, de transparence et de contrôle a posteriori. On voit émerger de véritables « *zones grises réglementaires* », dans lesquelles les garanties juridiques peinent à s'appliquer face à l'opacité technique[5]. Ces constats renvoient à une question centrale : qui contrôle la surveillance lorsqu'elle est assurée par des systèmes techniques ?

L'expérience des révélations d'Edward Snowden sur la NSA illustre de manière parfaite l'opacité et l'étendue des dispositifs de surveillance contemporains. Le Parlement européen, dans un rapport de 2014, a dénoncé l'ampleur des programmes de collecte massive de données opérés par les agences de renseignement, y compris en dehors de tout cadre judiciaire[6]. Ce précédent rappelle que le développement de la surveillance de masse est toujours un choix politique, et non une conséquence inévitable de la technologie. Sans encadrement strict, ces choix peuvent contourner, voire effacer les gardes fous démocratiques.

Face à ces évolutions, la Cour européenne des droits de l'homme et la Cour de justice de l'Union européenne ont certes commencé à établir des limites, notamment en condamnant la conservation généralisée des données de connexion ou les dispositifs sans contrôle indépendant préalable. Mais comme le note leur fiche thématique conjointe, ces avancées demeurent fragiles face à la rapidité du déploiement technologique[7]. En l'absence d'une gouvernance anticipatrice, les États risquent d'institutionnaliser une surveillance permanente, indistincte, dont les effets sur les libertés sont d'autant plus profonds qu'ils sont invisibles.

B – La normalisation de la surveillance par les cadres juridiques et politiques

Si les avancées technologiques ont profondément renouvelé les capacités de surveillance de l'État, c'est par l'action du droit et des institutions politiques que ces pratiques ont été intégrées dans l'architecture normative contemporaine. Loin d'être

[5] Karen Yeung, 'Étude sur les incidences des technologies numériques avancées (dont l'intelligence artificielle) sur la notion de responsabilité, sous l'angle des droits humains'.

[6] Claude MORAES, 'RAPPORT sur le programme de surveillance de la NSA, les organismes de surveillance dans divers États membres et les incidences sur les droits fondamentaux des citoyens européens et sur la coopération transatlantique en matière de justice et d'affaires intérieures | A7-0139/2014 | Parlement européen' <https://www.europarl.europa.eu/doceo/document/A-7-2014-0139_FR.html>.

[7] '*La surveillance de masse*, Fiche thématique coinjointe, Jurisprudence de la CEDH et de la CJUE'.

exceptionnelles ou provisoires, les logiques de surveillance ont été progressivement normalisées, c'est-à-dire rendues compatibles avec l'État de droit par la création de cadres juridiques permissifs. Ce processus de légalisation, en apparence protecteur, a souvent eu pour effet paradoxal de banaliser et pérenniser des dispositifs attentatoires aux libertés fondamentales. La France illustre particulièrement cette tendance avec l'adoption de la loi relative au renseignement du 24 juillet 2015, qui établit un régime de surveillance des communications encadré mais très permissif [8]. Cette loi autorise notamment l'installation de dispositifs dits de « boîtes noires » chez les fournisseurs d'accès à Internet pour analyser automatiquement les métadonnées, ainsi que la mise en œuvre de techniques de surveillance sans autorisation judiciaire préalable pour les services de renseignement. En 2017, avec la loi renforçant la sécurité intérieure et la lutte contre le terrorisme, des mesures initialement instaurées sous l'état d'urgence comme les périmètres de protection, les assignations à résidence ou les fermetures administratives de lieux de culte, ont été intégrées dans le droit commun [9]. Ce basculement progressif de l'exceptionnel vers le normal traduit un rééquilibrage des rapports entre sécurité et liberté, au détriment des libertés individuelles.

Cette juridicisation de la surveillance trouve également un relais dans les dispositifs administratifs contemporains. À l'occasion des Jeux Olympiques de 2024, le gouvernement français a autorisé, par une loi spécifique, l'usage à titre expérimental de la vidéosurveillance algorithmique pour détecter automatiquement certains comportements dans l'espace public. Si cette mesure est présentée comme temporaire, elle a suscité de nombreuses critiques, notamment de la part de la CNIL, qui dans son Cahier AIR 2024, alerte sur les risques de généralisation et d'acceptation sociale de ces dispositifs, en l'absence d'une réflexion suffisante sur leur finalité réelle[10].

La critique est partagée par Amnesty International, qui voit dans cette autorisation une atteinte disproportionnée au droit à la vie privée et un contournement de l'effort réglementaire mené par l'Union européenne pour encadrer les usages de l'intelligence artificielle[4]. Cette organisation souligne que l'absence de débat parlementaire approfondi et l'absence de contrôle indépendant renforcent la fragilité démocratique de telles initiatives. Le danger ne réside pas tant dans la technologie elle-même que dans sa légitimation silencieuse par un cadre juridique à géométrie variable.

[8] LOI n° 2015-912 du 24 juillet 2015 relative au renseignement (1) 2015 (2015-912).
[9] LOI n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme (1) 2017 (2017-1510).
[10] 'Mission éthique : publication du cahier air2024 « La surveillance dans tous ses états. Quelle éthique pour (protéger) nos libertés ? »' <https://www.cnil.fr/fr/cahier-air2024>.

Sur le plan européen, la Cour de justice de l'Union européenne a tenté de poser des limites à cette normalisation en affirmant, dans plusieurs arrêts majeurs, que la conservation généralisée et indifférenciée des données de connexion est incompatible avec la Charte des droits fondamentaux de l'UE. Dans sa jurisprudence, la CJUE rappelle que le principe de proportionnalité suppose un encadrement strict, une finalité claire et un contrôle indépendant préalable. Pourtant, ces exigences sont régulièrement contournées au nom d'impératifs sécuritaires[11].

Le processus de banalisation de la surveillance ne se limite pas à l'encadrement légal ponctuel : il s'inscrit dans une stratégie politique plus large. Un article du Monde rapporte que le gouvernement français envisage déjà la pérennisation de la vidéosurveillance algorithmique, en s'appuyant sur les expérimentations des JO 2024 comme levier de justification [12] . Cette logique d'extension par l'usage, « *expérimenter pour mieux généraliser* », est emblématique d'un État qui ajuste les cadres normatifs aux outils techniques, et non l'inverse. Le droit devient alors un instrument d'adaptation à la technologie, plutôt qu'un rempart structurant.

Ce phénomène pose une question essentielle : dans quelle mesure un cadre juridique peut-il être à la fois protecteur des libertés et permissif pour les dispositifs qui les mettent en péril ? Lorsque les lois deviennent l'outil de la généralisation des pratiques de surveillance, la frontière entre légalité et légitimité s'estompe. La normalisation juridique ne se traduit pas nécessairement par une garantie accrue, mais peut au contraire institutionnaliser une forme de vulnérabilité démocratique, en rendant la surveillance acceptable parce qu'encadrée.

II – LES TENSIONS ET DEFIS LIES A LA SURVEILLANCE DE MASSE DANS UN « ÉTAT DE DROIT NUMERIQUE »

Dans cette seconde partie, nous nous intéresserons d'abord aux atteintes que la surveillance de masse fait peser sur les principes fondamentaux de l'État de droit (*A*),

[11] Village de la Justice, '(Réflexion) La surveillance de masse à l'épreuve des libertés individuelles. Par Bouziane Behillil, Avocat, Hiba Laoufir et Romane Sylvestre, Etudiantes.' (*Village de la Justice*, 21 March 2024),<https://www.village-justice.com/articles/surveillance-masse-epreuve-des-libertes-individuelles,49214.html>.

[12] 'Le Gouvernement Étudie Une Pérennisation de La Vidéosurveillance Algorithmique' <https://www.lemonde.fr/pixels/article/2024/10/03/le-gouvernement-etudie-une-perennisation-de-la-videosurveillance-algorithmique_6342513_4408996.html>.

avant d'examiner les perspectives d'encadrement éthique et démocratique de ces dispositifs à l'échelle nationale et internationale (*B*).

A – UNE SURVEILLANCE DE MASSE EN TENSION AVEC LES PRINCIPES FONDAMENTAUX DE L'ÉTAT DE DROIT

Alors même que l'État de droit repose sur la protection des libertés fondamentales, l'expansion contemporaine de la surveillance de masse, rendue possible par les outils numériques, soulève de profondes tensions juridiques et démocratiques. Certes, garantir la sécurité des citoyens est une prérogative légitime. Mais cela peut-il justifier que l'on observe, en permanence, l'ensemble d'une population ? Cette question mérite d'être posée avec lucidité, d'autant que le droit semble parfois peiner à encadrer efficacement ces dispositifs à mesure qu'ils se banalisent.

La première tension apparaît au regard du droit à la vie privée, qui semble s'éroder à mesure que la technologie progresse. Dans un environnement numérique façonné par la captation permanente de données, l'individu devient une cible potentielle, non en raison de ses actes, mais en fonction de ce qu'il pourrait faire. Cette logique algorithmique inverse les fondements du droit pénal : la présomption d'innocence cède peu à peu la place à une présomption statistique. Le Conseil de l'Europe alerte justement sur ce basculement silencieux, où l'État, au lieu de justifier son intrusion, s'impose comme observateur légitime par défaut, reléguant l'individu à un rôle d'objet du regard public[13].

Ces dispositifs prennent aujourd'hui des formes de plus en plus sophistiquées. Les technologies de reconnaissance faciale ou de détection comportementale, comme celles mises en œuvre à l'occasion des Jeux Olympiques de Paris 2024, marquent une nouvelle étape. Il ne s'agit plus de surveiller ce que nous faisons, mais d'anticiper ce que nous pourrions faire. L'espace public devient alors un espace sous alerte constante. Dans son rapport AIR 2024, la CNIL met en garde contre cette tendance à détecter des « *comportements anormaux* » sur la base de critères opaques, dont l'impact est loin d'être neutre[14]. Car derrière la technique, ce sont des logiques sociales bien réelles qui s'activent. Les algorithmes de surveillance ne sont pas vierges de biais : ils reproduisent, souvent sans le dire, des schémas discriminatoires déjà présents dans nos sociétés.

[13] Karen Yeung, 'Étude sur les incidences des technologies numériques avancées (dont l'intelligence artificielle) sur la notion de responsabilité, sous l'angle des droits humains'.
[14] 'Mission éthique : publication du cahier air2024 « La surveillance dans tous ses états. Quelle éthique pour (protéger) nos libertés ? »' <https://www.cnil.fr/fr/cahier-air2024>.

Amnesty International le rappelle dans son analyse des dispositifs français : les populations racisées ou précaires sont plus souvent ciblées, plus souvent identifiées, plus souvent contrôlées. À la marge du droit, ces personnes deviennent centrales dans les bases de données[15]. Et si l'on prend un peu de recul, on comprend que la promesse d'un traitement égalitaire cède, dans les faits, à une réalité plus inégalitaire encore.

À cela s'ajoute une interrogation centrale sur le principe de proportionnalité. La surveillance ne se limite plus à des individus suspectés : elle devient systématique, déployée à grande échelle, sur l'ensemble de la population. Or, la jurisprudence européenne est claire : la conservation massive et indifférenciée des données est incompatible avec les droits fondamentaux. La Cour de justice de l'Union européenne rappelle que la surveillance doit être ciblée, limitée dans le temps, strictement encadrée et soumise à un contrôle indépendant[16]. Mais dans la pratique, ces garde-fous sont souvent contournés, voire purement absents.

Il y a enfin une conséquence plus diffuse, mais tout aussi préoccupante : l'effet dissuasif que produit la surveillance sur les comportements. Le simple fait de se savoir potentiellement observé suffit parfois à restreindre notre parole, à modérer nos engagements, à renoncer à certains débats. L'*Electronic Frontier Foundation* a documenté ce phénomène, connu sous le nom de *chilling effect* : on ne s'exprime plus de la même manière dans un environnement où nos faits et gestes peuvent être interprétés, conservés, analysés[17]. Ce n'est pas seulement la liberté d'expression qui s'en trouve affectée, mais aussi la liberté de réunion, d'association, de création.

En somme, les outils numériques de surveillance, présentés comme des garants de sécurité, génèrent un malaise plus profond : celui d'un droit qui ne parvient plus à protéger, d'un citoyen qui s'autocensure, et d'une société qui s'habitue à vivre sous observation. Qu'une mesure soit légale ne signifie pas qu'elle soit légitime. Et c'est peut-être là le défi fondamental posé à nos démocraties : préserver la liberté, y compris (et surtout) à l'ère des algorithmes.

---

[15] 'France. L'autorisation de la surveillance de masse lors des Jeux olympiques nuit au travail de l'UE en vue de réglementer l'intelligence artificielle' (*Amnesty International*, 23 March 2023) <https://www.amnesty.org/fr/latest/news/2023/03/france-allowing-mass-surveillance-at-olympics-undermines-eu-efforts-to-regulate-ai/>.

[16] Village de la Justice, '(Réflexion) La surveillance de masse à l'épreuve des libertés individuelles. Par Bouziane Behillil, Avocat, Hiba Laoufir et Romane Sylvestre, Etudiantes.' (*Village de la Justice*, 21 March 2024),<https://www.village-justice.com/articles/surveillance-masse-epreuve-des-libertes-individuelles,49214.html>.

[17] Karen Gullo, 'Surveillance Chills Speech—As New Studies Show—And Free Association Suffers' (*Electronic Frontier Foundation*, 19 May 2016) <https://www.eff.org/deeplinks/2016/05/when-surveillance-chills-speech-new-studies-show-our-rights-free-association>.

B – VERS UNE GOUVERNANCE ETHIQUE ET DEMOCRATIQUE DE LA SURVEILLANCE NUMERIQUE

Si la surveillance de masse soulève de vives tensions au regard des libertés fondamentales, il serait réducteur de considérer que le droit, les institutions ou la société civile restent impuissants face à cette dynamique. À rebours d'un discours parfois fataliste, des voies de résistance émergent, cherchant à réconcilier sécurité publique, innovation technologique et respect de l'État de droit. Ce chantier est encore en construction, mais il esquisse déjà les contours d'une gouvernance plus responsable des outils de surveillance numérique.

Le rôle des autorités indépendantes, en particulier, est devenu central dans cette recomposition. En France, la CNIL incarne l'un des rares contre-pouvoirs capables de formuler des avis, d'encadrer certains dispositifs et, dans certains cas, de freiner les dérives les plus flagrantes. Lors de l'expérimentation de la vidéosurveillance algorithmique pour les Jeux Olympiques de 2024, la CNIL a publié un avis particulièrement critique, alertant sur le manque de garanties effectives, notamment en matière de durée de conservation des données, de transparence sur les traitements, et d'encadrement du recours à des prestataires privés[18]. En 2024 encore, elle a prononcé plusieurs mises en demeure à l'encontre d'acteurs publics utilisant des logiciels de traitement vidéo sans encadrement suffisant [19] . Bien que ses recommandations ne soient pas toujours contraignantes, elles contribuent à instaurer un débat public et à faire exister une voix critique dans un paysage souvent dominé par la logique sécuritaire.

Au-delà de l'action institutionnelle, un véritable enjeu de transparence algorithmique s'impose. Comment accepter qu'un système puisse déclencher une alerte, catégoriser un comportement ou orienter une décision administrative, sans que les critères retenus soient accessibles ou compréhensibles ? L'article 22 du RGPD reconnaît à chacun le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé. Pourtant, dans la pratique, cette garantie demeure largement théorique. Trop souvent, le secret industriel, l'opacité des modèles ou le manque de moyens techniques rendent le contrôle effectif illusoire. Il devient urgent de rendre lisible ce qui gouverne : un

[18] 'Jeux olympiques et paralympiques 2024 : la CNIL publie son avis sur le projet de loi' <https://www.cnil.fr/fr/jeux-olympiques-et-paralympiques-2024-la-cnil-publie-son-avis-sur-le-projet-de-loi>.

[19] 'Utilisation de BriefCam et d'autres logiciels d'analyse vidéo par l'État et des communes : la CNIL prononce plusieurs mises en demeure' <https://www.cnil.fr/fr/utilisation-briefcam-logiciels-analyse-video-par-etat-communes-la-cnil-prononce-plusieurs-mises-en-demeure>.

algorithme qui classe ou qui surveille ne peut rester une boîte noire dans un État qui se veut démocratique.

À cette exigence s'ajoute un besoin croissant de régulation à l'échelle internationale. Les technologies de surveillance ignorent les frontières : les données circulent, les logiciels s'exportent, les partenariats se nouent entre services de renseignement. Or, le droit reste largement national, parfois européen, rarement mondial. C'est pourquoi le Rapporteur spécial des Nations unies sur le droit à la vie privée plaide pour un traité international visant à encadrer les pratiques de surveillance numérique, interdire les outils les plus intrusifs, et garantir un socle commun de garanties fondamentales[20]. Dans un rapport ultérieur, il souligne également le rôle que pourraient jouer les entreprises du numérique dans la mise en place de mécanismes de gouvernance éthique[21].

Le contrôle citoyen n'est pas en reste. Des organisations comme La Quadrature du Net documentent et dénoncent activement le déploiement silencieux de technologies de surveillance dans l'espace public. À l'été 2024, à l'issue des Jeux Olympiques, l'association a révélé que plusieurs expérimentations de vidéosurveillance algorithmique avaient été reconduites, voire élargies, sans réelle consultation ni évaluation indépendante[22]. Ce phénomène d'extension par l'usage, expérimenter pour mieux généraliser, illustre les dérives possibles d'un cadre juridique trop souple, où la normalisation passe davantage par l'habitude que par la loi.

Enfin, il serait incomplet de penser la régulation sans évoquer les alternatives. Face aux dispositifs de surveillance, des formes de résistance émergent du côté des citoyens, des associations, mais aussi des développeurs et des chercheurs. Le chiffrement des communications, l'anonymisation des données, ou encore les principes de *privacy by design*, qui imposent une protection des données dès la conception des outils, ne sont pas des utopies techniques : ils existent, ils fonctionnent, ils incarnent une autre façon de faire du numérique. Ce sont là des choix politiques, au sens noble du terme. Favoriser une innovation qui respecte les droits fondamentaux, soutenir des infrastructures numériques souveraines et éthiques, c'est défendre un modèle de société dans lequel la technologie ne domine pas l'humain, mais le sert.

---

[20] 'Conseil des Droits de l'Homme, Rapport du Rapporteur spécial sur le droit à la vie privée, A/HRC/37/62, 2018, <https://documents.un.org/doc/undoc/gen/g18/324/48/pdf/g1832448.pdf>.

[21] 'Conseil des Droits de l'Homme, Rapport du Rapporteur spécial sur le droit à la vie privée, A/HCR/41/35, 2019

[22] 'Comment La Vidéosurveillance Algorithmique a Été Déployée Pendant Les Jeux Olympiques' <https://www.lemonde.fr/societe/article/2024/08/14/comment-la-videosurveillance-algorithmique-a-ete-deployee-pendant-les-jeux-olympiques_6280517_3224.html>.

Il ne s’agit pas de rejeter toute surveillance, ni de nier les enjeux de sécurité auxquels nos sociétés sont confrontées. Mais vouloir encadrer, questionner, et parfois refuser certains usages n’est pas un acte de naïveté : c’est une affirmation démocratique. À une époque où l’efficience technique tend à primer sur la délibération collective, rappeler que tout n’est pas acceptable, même si c’est possible, est plus que jamais nécessaire.