Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

COMMISSION SUPERIEURE DU NUMERIQUE ET DES POSTES

AVIS N°2021-04 DU 10 JUIN 2021 PORTANT CONTRIBUTION

A LA MISSION RELATIVE AUX NOUVELLES TECHNOLOGIES DANS LE DOMAINE DE LA SECURITE

La mission confiée par le Premier Ministre à notre collègue Jean-Michel Mis, Député de la Loire, porte sur la sécurité des Jeux olympiques et paralympiques de Paris en 2024, notamment en matière de choix technologiques et de mise en place des cadres d'expérimentation nécessaires pour favoriser les innovations proposées par la filière industrielle.

Alors que des choix stratégiques doivent être pris par le gouvernement, les membres de la CSNP souhaitent apporter une contribution dans le périmètre de leurs compétences : sans exclure *à priori* aucune technologie permettant de renforcer la sécurité de ces grands évènements, les membres de la CSNP se prononcent pour un continuum entre sécurité physique et sécurité numérique (I).

Les membres de la CSNP considèrent que si la sécurité de ces grands événements constitue une obligation de résultats pour les autorités publiques, elle doit se faire en développant un cadre juridique respectueux des libertés publiques et individuelles (II). Pour répondre à cet objectif, des expérimentations sur des grands évènements pourraient être mis en œuvre en associant autorités indépendantes et société civile (III).

I. Les solutions offrant un continuum entre sécurité physique et sécurité numérique doivent pouvoir être mises en œuvre

Le champ d'application du programme de sécurité des Jeux olympiques et paralympiques de Paris en 2024 vise à réduire les menaces de nature terroriste ou criminelle et, d'une manière plus générale, le niveau de sureté pendant la phase de construction des sites, pendant les épreuves tests et pendant la période opérationnelle des Jeux. Ce programme concerne les sites de compétition et d'hébergement, les réseaux de transport, ainsi que toute autre infrastructure stratégique pour l'organisation des Jeux.

Cette responsabilité de la sécurité publique incombe à l'État français et intègre la lutte contre le terrorisme, les problématiques de délinquance liés aux phénomènes de bandes ou de constitution de black blocs ainsi que la gestion des crises sanitaires.

1. A ce stade, les membres de la CSNP considèrent que les autorités doivent pouvoir recourir à l'ensemble des technologies permettant de renforcer la sécurité des jeux contre les formes de délinquance classique ou contre le terrorisme, au nombre desquelles figurent:

   - a. Le traitement des données biométriques. Les données biométriques comprennent les données relatives à notre corps ou à notre comportement : empreinte digitale, reconnaissance du visage, ADN, géométrie de la main, empreinte palmaire, reconnaissance de l'iris et de la

rétine, rythme de frappe, démarche et posture physique ... Partout en Europe et dans le monde, des entreprises mettent au point des solutions innovantes pour mieux définir, analyser et prédire nos comportements individuels ou de masse.

Le traitement des données biométriques pourrait être utilisé à tous les stades du continuum sécuritaire : en amont (reconnaissance faciale a priori, pour prévenir l'intrusion d'individus dans des manifestations par exemple) ; en situation (pour accélérer l'enquête, du fait de la rapidité et de la précision de l'outil) et a posteriori (le traitement des bases existantes et le croisement des données permet des recoupements dynamiques).
La biométrie offre des solutions permettant la mise en œuvre de dispositifs d'authentification efficients (déploiement de mots de passe biologiques non-falsifiables pour accès aux sites physiques ou numériques les plus sensibles).

La biométrie *« aux fins d'identifier une personne physique de manière unique* » entre dans une catégorie particulière définie par deux textes adoptés par les 27 États membres de l'Union européenne en avril 2016, le règlement général sur la protection des données (RGPD) et la directive police-justice. Il s'agit d'une catégorie de données considérées comme particulièrement sensibles. Le RGPD s'applique à l'ensemble des traitements de données personnelles effectués à la fois dans le secteur public et le secteur privé. La directive police-justice concerne, pour sa part, les traitements effectués 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 par les autorités compétentes (autorités judiciaires, police, autres autorités répressives …). Elle précise que les données biométriques ne doivent être utilisées qu'en cas de nécessité absolue et sous réserve de garanties appropriées pour les droits et libertés de la personne concernée. Un tel traitement peut être effectué dans trois cas uniquement : lorsqu'il est autorisé par le droit de l'Union ou le droit d'un État membre, lorsqu'il porte sur des données manifestement rendues publiques par la personne ou pour protéger les intérêts vitaux de la personne concernée ou d'une autre personne.

- b. Le traitement algorithmique des connexions et des données permet la détection de signaux faibles. Les prochains débats relatifs au projet de loi antiterroriste – que le Sénat examinera en séance publique à compter du 29 juin - poseront néanmoins la question de la portée de ce traitement, aujourd'hui limité aux noms de domaine et potentiellement étendue aux adresses URL.

- c. Les technologies sécuritaires de mobilité, notamment les caméras aéroportées, permettent de sécuriser les sites officiels et les cibles potentielles. Elles nécessitent un encadrement juridique plus spécifique en tant que la portée et les finalités de leur utilisation sont fonctions d'une doctrine sécuritaire définie en amont de leur déploiement.

- d. Les technologies d'inclusion de l'ensemble des objets connectés dans le continuum de sécurité (smartphones, capteurs des bâtiments, ...). Notamment, les smartphones peuvent être un outil efficace de communication. Ils peuvent permettent d'une part, d'alerter localement les participants par notifications, et d'autre part faciliter une remontée d'information plus rapide et précise aux services publics de sécurité.

Du point de vue des membres de la CSNP, aucune technologie ne peut être exclue *per se* : l'usage de l'Intelligence artificielle peut permettre la gestion des mouvements de foules et la détection des mouvements et des comportements suspects. La reconnaissance faciale, la biométrie les solutions de traçage et la *blockchain* permettent de sécuriser l'accès au site les plus sensibles en contrôlant les identités.

2. Dans le prolongement des recommandations publiées dans son avis n°2021-03 sur la sécurité numérique, les membres de la CSNP attirent l'attention des autorités françaises sur les risques que font peser les actes de cybercriminalité et de cyberattaques sur les Jeux olympiques et paralympiques de Paris en 2024. En deux ans, les cyber-attaques ont été multipliées par quatre et une projection à trois ans de ces cyber-menaces suppose l'adoption dès à présent des meilleurs systèmes de cyberdéfense.

En tout état de cause, la CSNP appelle les autorités françaises et notamment le Ministère de l'intérieur à apporter une attention toute particulière au continuum entre sécurité physique et sécurité numérique.

En effet, d'une part, toutes les technologies mises en œuvre dans les systèmes de sécurité embarquent désormais de manière native les vulnérabilités génériques du numérique (cyber-attaques, accès et vol de données, biais cognitifs). D'autres part, les activités criminelles, notamment de nature terroriste ou de déstabilisation, sont de plus en plus fréquemment précédés et accompagnées par des opérations dans l'espace numérique, comme la diffusion de fausses informations, la recherche d'information et l'espionnage, la neutralisation de systèmes de surveillance, la mise en cause de l'intégrité, de la confidentialité et de la disponibilité de données sensibles de sécurité et des traitements associés.

A ce titre, la CSNP suggère que ses recommandations en matière de sécurité par conception inscrites dans son avis sur la sécurité numérique du 29 avril 2021, soient adaptées et mises en œuvre dans le cadre du développement des systèmes technologiques nécessaires à la sécurisation des grands événements sportifs et des Jeux olympiques et paralympiques de Paris en 2024.

II. Développement d'un cadre juridique respectueux des libertés individuelles et collectives

La CSNP est transpartisane et à l'image de la société française : le curseur entre sécurité et libertés publiques et individuelles peut évoluer selon la sensibilité de ses membres.

Pour autant, les membres de la CSNP sont favorables à :

- un usage proportionné des technologies à des fins sécuritaires avec le respect des libertés publiques et individuelles,
- un encadrement et un contrôle par une autorité indépendante, en l'occurrence la CNIL, de la bonne application du cadre réglementaire en matière d'enregistrement des données, de leur traitement, de leur sécurité de conservation, de leur accès par des personnes autorisées, de leur usage circonscrits à certains motifs, et de leur effacement systématique après une durée du stockage déterminée.

Les membres de la CSNP ont pleinement conscience que le cadre législatif, règlementaire et jurisprudentiel portant sur les usages de l'intelligence artificielle, de la reconnaissance faciale et de l'utilisation des données est actuellement mouvant : les négociations sur le projet de règlement sur l'intelligence artificielle (IA) proposé par la Commission européenne le 21 avril dernier, et notamment les dispositions relatives à la reconnaissance faciale, sont en cours alors que les autorités françaises ont d'ores et déjà à opter pour des solutions en vue d'être prêtes pour les Jeux olympiques et paralympiques de Paris en 2024.

Nos concitoyens ont toujours porté une extrême vigilance sur les questions de libertés individuelles et publiques portées par le développement des technologies : le dernier exemple en date, sur la mise en

œuvre de l'application TousAntiCovid a conduit les autorités françaises à opter une solution souveraine alors que nos voisins européens se sont progressivement ralliés aux solutions compatibles avec les systèmes d'exploitation dominants dans le domaine de la téléphonie mobile.

Il nous paraît important de rappeler que la perception de nos concitoyens peut évoluer dès lors qu'ils mesurent les bénéfices que peuvent apporter ces technologies lorsqu'elles sont encadrées et qu'elles ont démontré leur efficacité.

L'évolution de l'opinion publique à l'égard des systèmes de vidéo-protection dans l'espace public nous parait exemplaire : ce déploiement a donné lieu à de vives critiques avant d'être globalement accepté en vue de renforcer la sécurité dans l'espace public.

Aujourd'hui, ce sont la reconnaissance faciale et la surveillance biométrique qui font débat : une partie de la population y est farouchement opposée alors que ces technologies sont en mesure de renforcer de manière efficace la sécurité de certains sites.

Dans l'attente de l'adoption du règlement européen sur l'Intelligence artificielle[1], il nous paraît important pour l'acceptabilité de ces technologies de présenter une doctrine d'engagement qui précise de manière transparente dans quel contexte et dans quel périmètre elles seront utilisées ainsi que l'usage et l'exploitation des données ainsi recueillies dans le temps.

A cet égard, dans le cadre du rapport relatif à la proposition de loi sécurité globale[2,] publié en mars 2021, MM. les Sénateurs Marc-Philippe Daubresse et Loïc Hervé ont souligné la nécessité d'affermir les garanties données aux citoyens sur les nécessités et finalités opérationnelles précises des captations d'images, sur la formation des personnels destinataires de ces images, sur la sécurité des enregistrements et la traçabilité des accès à ces enregistrements.

De ce point de vue, l'expérimentation qui pourrait être faite à l'occasion de prochains évènements publics pour tester le déploiement de ces technologies devrait associer étroitement les autorités indépendantes telles que la CNIL et le Défenseur des droits, par exemple, mais également des associations et des représentants de la société civile pour garantir un usage raisonnable et proportionné de ces technologies. Il sera sans doute difficile d'aboutir à un consensus mais cette logique de dialogue nous semble pertinente pour encadrer le déploiement de ces technologies au plus près des craintes exprimées par nos concitoyens.

III. Un cadre permettant des expérimentations est attendu et souhaitable

Depuis le rapport publié en septembre 2018[3] par Mme Alice Thourot, députée de la Drôme, et M. Jean-Michel Fauvergue, député de Seine-et-Marne, sur la sécurité globale, plusieurs autres travaux ont tenté de faire émerger une dynamique d'innovation en matière de technologies de sécurité. Ces initiatives, essentiellement portées par la filière industrielle de la sécurité, se sont fédérées dans le cadre de la création d'un Comité stratégique de la filière des industries de sécurité, et a abouti à la signature d'un contrat de filière en janvier 2020. L'un des cinq projets structurants prévu par ce contrat concerne directement la sécurité des grands événements et des Jeux olympiques et paralympiques de Paris en 2024.

Ce projet structurant vise à assurer la sécurité Jeux olympiques et paralympiques de Paris en 2024 en s'appuyant sur l'offre technologique et industrielle française, en la valorisant et en mettant l'innovation au cœur de la réponse.

---

[1] https://ai-regulation.com/facial-recognition-in-the-draft-european-ai-regulation-final-report-on-the-high-level-workshop-held-on-april-26-2021/ La CNIL a publié une note en 2019 sur la reconnaissance faciale https://www.cnil.fr/sites/default/files/atoms/files/reconnaissance_faciale.pdf

[2] https://www.senat.fr/rap/l20-409/l20-4091.pdf

[3] https://www.gouvernement.fr/sites/default/files/document/document/2018/09/rapport_de_mme_alice_thourot_et_m._jean-michel_fauvergue_deputes_-_dun_continuum_de_securite_vers_une_securite_globale_-_11.09.2018.pdf

Les industriels de la filière expriment donc l'urgence absolue d'un cadre conventionnel exceptionnel, et éventuellement dérogatoire, permettant de mener, dès le mois de septembre 2021, les expérimentations nécessaires et de traiter les principaux points suivants :

- identification des principaux enjeux de souveraineté technologique ;
- disponibilité des données en quantité et qualité suffisante ;
- développement de l'environnement juridique et éthique adapté.

A titre d'exemple, l'industrie nationale dispose de nombreuses solutions en analyse vidéo pour l'analyse de foule, la reconnaissance faciale ou la lecture automatique des plaques d'immatriculation (LAPI), qui peuvent apporter des réponses très pertinentes sur des cas d'usages précis respectueux des libertés, mais les avancées juridiques sont extrêmement lentes.

La pandémie de COVID a *de facto* réduit considérablement le nombre de manifestations publiques et donc rendu difficiles ces types d'expérimentation mais il paraît, aux membres de la CSNP, assez urgent de les mettre en œuvre de manière pragmatique et sans délais.

Un tel cadre apparait indispensable pour engager un plan d'accélération technologique et législatif en phase avec les échéances des Jeux olympiques et paralympiques de Paris en 2024 , en concertation avec les parties prenantes - collectivités participantes, citoyens, société civile - et avec des études d'impact (coûts/bénéfices) rigoureuses et transparentes.

Ces expérimentations doivent également permettre aux autorités de préciser les cas d'usage et la doctrine de déploiement des technologies, de retirer les bonnes pratiques et de tester la bonne coordination entre les différents services et, le cas échéant, avec nos partenaires étrangers.

Un cadre clair et adapté apparaît essentiel pour débattre de façon dépassionnée et dé-corrélée de la pression de l'actualité, notamment avec les membres du Parlement et les représentants de la société civile.

La CSNP peut offrir ce cadre.

ANNEXE : CADRE REGLEMENTAIRE ET JURISPRUDENTIEL

L'usage de l'intelligence artificielle est en cours de régulation au niveau européen :

- stratégie européenne en matière d'intelligence artificielle : création du premier plan coordonné sur l'IA en 2018,
- lignes directrices pour une IA digne de confiance publiée en 2019 par le groupe d'experts de haut niveau sur l'intelligence artificielle,
- livre blanc publié en 2020 par la Commission Européenne
- consultation publique concernant le livre blanc sur l'IA
- rapport sur les conséquences de l'intelligence artificielle, de l'internet des objets et de la robotique sur la sécurité et la responsabilité
- Avis du contrôleur européen de la protection des données sur la régulation de l'intelligence artificielle ainsi que sur la surveillance biométrique.
- Annonce en 2021 du nouveau plan coordonné sur l'IA et premier cadre juridique européen sur l'intelligence artificielle

En France, l'usage de l'intelligence artificielle est peu encadré :

- La loi pour une république numérique (et la transposition du RGPD) renforce le contrôle de chacun sur l'usage de ses données privées sans pour autant définir un véritable cadre légal quant au développement et à l'utilisation de l'intelligence artificielle.
- France IA, le rapport Villani ont proposé les fondations d'une stratégie nationale ambitieuse.

Reconnaissance faciale

En France, si de nombreuses jurisprudences et délibérations de la CNIL traitent de ce sujet, les tentatives d'encadrement législatif sont rares : on citera la proposition de loi relative à la reconnaissance faciale dans les enquêtes terroristes et la prévention des attentats. De nombreuses expérimentations ont lieu dans des villes et lieux (aéroport de paris, lycées à Marseille et Nice…). Les parties prenantes, industriels comme associations de la société civile réclament un cadre légal clair.

Au niveau européen, la Commission propose d'encadrer la pratique au sein de la régulation de l'intelligence artificielle. Source : Vers un encadrement de la reconnaissance faciale en Europe

Détection des mouvements et des comportements

Plusieurs textes et décisions encadrent les dispositifs de détection des mouvements et des comportements :

- Déclaration de la CNIL n° 94-056 du 21 juin 1994 qui protège les citoyens et encadre la vidéosurveillance
- Le texte de loi de référence est la loi du 6 janvier 1978 qui encadre l'usage des données personnelles des citoyens.

- L'ordonnance n° 2018-1125 du 12 décembre 2018 protège une « personne d'une décision de justice impliquant une appréciation de son comportement fondée sur le traitement automatisé de donné à caractère personnel ».
- la loi du 21 janvier 1995 (dite « loi Pasqua ») est centrée sur la régulation de la vidéosurveillance dans les lieux publics et les lieux privés recevant du public.
- La loi du 6 août 2004 transpose les directives européennes et confère à la CNIL la responsabilité de contrôler l'usage de l'enregistrement, du traitement et de la conservation des données et des vidéosurveillances.
- La loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure vient renforcer la loi Pasqua en déployant plusieurs dispositifs supplémentaires. Cependant, face aux évolutions proposées, le texte fut contesté par la CNIL et le Conseil Constitutionnel. Le texte prévoit la mise en place d'un véritable contrôle par la CNIL des systèmes de vidéoprotection dans les lieux ouverts au public, alors que jusqu'à présent, elle ne contrôlait que ceux installés dans les lieux privés.

Au niveau européen :

- Le règlement général de protection des données fait peser sur les organismes publics et privés qui traitent les données des citoyens / citoyennes une certain nombre de responsabilités. Les images de vidéosurveillance font partie de son domaine d'application : à partir du moment où les personnes filmées sont identifiables, les enregistrements sont des données privées.
- Dans son « position paper » le Conseil et le Parlement européen ont posé les bases de ce qu'il serait interdit de traiter comme données grâce à l'IA et aux productions de vidéosurveillances. A titre d'exemple, l'utilisation de l'IA pour élaborer des scores sociaux et pour évaluer la loyauté et la fiabilité des individus serait fermement interdite.

Drones

- Drones : la CNIL sanctionne le ministère de l'Intérieur
- Suspension de l'utilisation des drones pour contrôler le déconfinement à Paris par le Conseil d'État : les contrôles de la CNIL
- Décision n° 2021-817 DC du 20 mai 2021 - Communiqué de presse20 mai 2021

Empreinte biométriques (digitale, œil)

- Loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure.
- RAPPORT D´INFORMATION fait au nom de la Commission des lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale (1) sur l'usage de la biométrie en France et en Europe

Conservation et traitement des données personnelles

- Dans son optique de lutte contre le terrorisme et les menaces sécuritaires intérieures, la France impose aux opérateurs internet et mobile de conserver les données personnelles des utilisateurs pendant un an afin de subvenir aux besoins des renseignements en cas d'enquêtes pénales grâce à la LOI n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale

- Cependant, la CJUE a fortement limité la possibilité d'imposer aux opérateurs la conservation des données de connexion par trois décisions rendues le 6 octobre 2020.
- Le Conseil d'Etat relève que la conservation généralisée aujourd'hui imposée aux opérateurs par le droit français est bien justifiée par une menace pour la sécurité nationale, comme cela est requis par la CJUE.

Blockchain

- Adaptation du code monétaire et financier grâce à l'ordonnance n° 2017-1674 du 8 décembre 2017 qui facilite la transmission de certains titres financiers non cotés au moyen de la technologie « blockchain ».
- stratégie nationale blockchain de 2019 qui propose d'établir un cadre juridique permettant l'utilisation de la blockchain dans un cadre sécurisé.
- La loi de finance 2019 et la loi PACTE du 11 avril 2019 ont mis en place un cadre juridique pour les émissions de jetons numériques. L'Autorité des Marchés Financiers consacre ainsi en avril 2019, un nouveau régime pour les cryptoactifs.
- la mission d'information commune sur les chaînes de blocs (blockchains) a abouti à la création de la Fédération française des professionnels de la Blockchain qui regroupe les acteurs français autour de même normes de standards pour peser auprès des institutions françaises et européennes.

Au niveau européen :

- Création en 2018 de l'observatoire Observatoire-forum des chaînes de blocs de l'UE
- Proposition de résolution du parlement européen,

Décision de la Cour de Justice de l'Union Européenne