GOUVERNEMENT

Liberté
Égalité
Fraternité

Pour un usage **responsable et acceptable** par la société des **technologies de sécurité**

Rapport au Premier ministre par Jean-Michel Mis, député de la 2e circonscription de la Loire

Volume II
Contributions

Septembre 2021

SOMMAIRE

Agence nationale de la sécurité des systèmes d'information (ANSSI) 4
Alliance Police Nationale 7
Alliance pour la confiance numérique (ACN) 11
Alternative Police-CFDT Interco 25
AN2V 30
Axon 50
Commission nationale consultative des droits de l'Homme (CNCDH) 53
Commission nationale de l'informatique et des libertés (CNIL) 57
Commission supérieure du numérique et des postes (CSNP) 65
Conseil national du numérique (CNNum) 73
Contrat stratégique de filière « industries de sécurité » (CSF-IS) 75
Cybercercle 101
Datakalab 112
Fédération des Industries Électriques, Électroniques et de Communication (FIEEC) 126
Fédération Française de la Cybersécurité 132
Fédération Française des Métiers de l'Incendie (FFMI) 140
M. Adrien Basdevant, avocat 143
M. Claude Kirchner, Directeur du Comité national pilote d'éthique du numérique 152
M. Didier Baichère, député de la 1re circonscription des Yvelines 157

Contributions des conseillers du commerce extérieur de la France (CCEF) 162

M. Gilbert Réveillon, Président du groupe d'expertise TIC et Économie Numérique au Comité National des Conseils du Commerce Extérieur de la France 172

M. Hervé Debar, Professeur, Télécom SudParis, Institut Mines-Télécom 179

M. Jean-Gabriel Ganascia, informaticien et philosophe 183

M. Jean-Marie Cavada, président d'IDFrights 186

M. Sébastien Louradour, Expert Technique International, Forum Économique Mondial 189

Contribution collective de M^me^ Manon Vermenouze (Shark Robotics) et MM. Thierry Berthier (Hub France IA), Geoffroy Deltel (Photonis) et Victor Vuillard (Parrot) 199

M^me^ Françoise Soulié, Conseiller Scientifique HUB IA 281

M^me^ Laurane Raimondo, chercheure associée, Centre Lyonnais d'Études de Sécurité Internationale et de Défense 284

Palantir France 325

Renaissance numérique 329

SCSI (Syndicat des cadres de la sécurité intérieure – CFDT) 338

Serenicity 340

Syndicat National des Personnels de Police Scientifique (SNPPS) 343

Mission relatives aux technologies de sécurité menée par M. le Député Jean-Michel MIS

Eléments ANSSI

L'utilisation de nouvelles technologies permettant aux acteurs publics de mener à bien leurs missions de sécurité est un enjeu majeur de la sécurité publique des années à venir, notamment au regard des grands événements organisés par la France en 2023 et en 2024.

Cependant, l'acceptation par la population de ces nouvelles technologies fait encore défaut, ce qui pourrait à terme fragiliser le déploiement de l'action publique. Des défauts en matière de cybersécurité dans ces nouvelles technologies peuvent directement affecter la confiance de la population et constituer un motif de rejet.

Enfin, cette séquence de grands événements constitue une occasion de faire valoir l'excellence et l'innovation de l'industrie française de cybersécurité et de de contribuer à son développement et à sa montée en maturité.

A ce titre, trois axes de travail pourraient utilement être intégrés à la réflexion autour de ces nouvelles technologies et leur déploiement au profit de grands événements :

- d'abord, **en s'assurant que ces nouvelles technologies prennent bien en compte dans leur conception et leur déploiement la cybersécurité** ;
- ensuite, en **mettant en avant l'excellence de l'industrie française de cybersécurité** et notamment sur les segments identifiés comme particulièrement stratégiques au regard des enjeux de souveraineté technologique ;
- enfin, en **garantissant la cybersécurité des grands événements à venir en France en 2023 et 2024**.

1. S'assurer de la bonne prise en compte de la cybersécurité dans les nouvelles technologies utilisées par les acteurs publics

Les nouvelles technologies déployées par des acteurs publics sont souvent insuffisamment sécurisées. En effet, très fréquemment des projets technologiques sont menés au sein de l'administration sans prise en compte au bon niveau de la cybersécurité. Parce qu'il manipule des informations sensibles du point de vue de la protection des données personnelles, d'informations économiques et stratégiques pour la Nation et pour lui-même, l'Etat se doit d'être exemplaire en matière de cybersécurité, et ce notamment lorsqu'il déploie de nouvelles technologies.

Cette exemplarité passe par trois axes de travail principaux :

- **La réalisation systématique d'analyses de risques cyber en amont de l'intégration de nouvelles technologies dans l'éventail des outils de l'action public**. Ces analyses de risques pourront être partagées, en partie ou intégralement, afin de montrer en transparence la manière dont les risques cyber sont pris en compte dans la conception et le déploiement des nouvelles technologies et quelles sont les contremesures mises en œuvre pour garantir la cybersécurité de ces technologies, et donc de la population française.

- **L'intégration de clauses de cybersécurité types dans les marchés publics permettant d'acquérir et de déployer des nouvelles technologies**. De telles clauses ont été élaborées par la direction des achats de l'Etat, avec l'appui de l'ANSSI, mais elles sont encore trop peu utilisées par les acheteurs publics ou les centrales d'achat.

- **Le maintien d'un niveau du cybersécurité tout au long du cycle de vie des nouvelles technologies.** Les travaux de l'OCDE sur la responsabilité des acteurs privés, fournisseurs de technologies, qui portent en effet sur le renforcement de la sécurité des produits et des services numériques et sur la gestion responsable des vulnérabilités sont particulièrement pertinents à cet égard. Ils établissent des principes structurants permettant d'assurer le maintien en conditions de sécurité de produits ou de services tout au long de leur durée de vie, en montrant quelles sont les responsabilités du fournisseur, de l'exploitant et des utilisateurs. Ce sont des mécanismes qui doivent être pensés en amont d'un programme d'adoption d'une nouvelle technologie, notamment pour être traduit dans la relation contractuelle entre l'offreur et l'acheteur.

2. Mettre en valeur **l'excellence de l'industrie française** de cybersécurité

L'émergence d'offres de confiance au sein de l'industrie française de cybersécurité est un enjeu majeur et une priorité politique forte, comme l'illustre l'annonce par le Président de la République en février dernier d'une stratégie d'accélération industrielle dédiée à la cybersécurité.

Les grands événements sportifs de 2023 et 2024 sont une opportunité pour appuyer le **développement de l'industrie française de cybersécurité**. Il semble en effet pertinent d'offrir la possibilité aux grands industriels comme aux ETI et aux PME du secteur de contribuer à la sécurisation cyber de ces grands événements. A cet égard, l'identification de **segments stratégiques au regard des enjeux de souveraineté technologique** dans le champ des nouvelles technologies de sécurité semble nécessaire afin de concentrer nos investissements et nos efforts dans les champs de souveraineté les plus pertinents.

A ce titre, **le Campus Cyber qui sera le lieu totem français de l'écosystème de la cybersécurité et donc une vitrine de l'excellence française dans ce domaine au niveau européen et international pourrait être utilement mobilisé.** En effet, ce lieu accueille l'ensemble des parties prenantes de la cybersécurité : la recherche publique et privée, les administrations, les industriels, petits et grands… Le Campus Cyber animera de travaux communs autour de projets spécifiques comme l'intelligence artificielle, les cryptomonnaies ou la sensibilisation à grande échelle. **Ce mode de construction, très participatif, aurait ainsi pour vertu de permettre à la fois la valorisation de l'offre française mais également de favoriser l'adoption des technologies, co-construites avec des tiers de confiance.**

3. **Garantir la cybersécurité des grands événements à venir en France en 2023 et 2024**

La cybersécurité des grands événements, et en premier lieu de ceux que la France accueillera dès 2023, est cruciale. L'ANSSI accompagne le ministère de l'intérieur dans la sécurisation de ces événements, qui sera un défi d'ampleur, ces évènements étant

fréquemment la cible d'attaquants aux motivations diverses. Des **exigences fortes relatives à la cybersécurité seront appliquées aux systèmes d'information** utilisés par les organisations chargées de planifier, de conduire et de diffuser ces événements majeurs. Cette action est un facteur de confiance envers les nouvelles technologies de sécurité qui seront mises en œuvre en particulier lors de ces grands événements.

Capitaliser sur ce projet pour **développer une expertise française concernant la cybersécurité des grands événements** pourrait également être une avancée. En effet, des centres de compétence sur la cybersécurité des grands évènements sont actuellement en développement qui permettront de mieux comprendre les enjeux et les meilleures pratiques à ce sujet, ainsi que de mieux former ceux qui demain seront chargés d'en assurer la cybersécurité. Une telle réflexion pourrait associer la société civile aux pouvoirs publics, par exemple au cours d'exercices de retours d'expérience.

De même, le recours à des infrastructures informatiques maîtrisées et à des prestataires chargés de les mettre en œuvre respectant la volonté de souveraineté technologique française et européenne serait préférable. En particulier, à l'exemple des récentes annonces concernant le cloud de confiance, le recours à des technologies étrangères, qui est parfois incontournable, ne peut se faire que dans des environnements maîtrisés. L'utilisation de la certification SecNumCloud proposée par l'ANSSI permet par exemple de s'assurer de disposer d'un bon niveau de maîtrise sur ces environnements.

Mission du député Jean-Michel Mis
sur les nouvelles technologies de sécurité.
Contribution Alliance Police Nationale.

*

1/ Objectifs de la mission

La mission souhaite explorer, lors des auditions et via les contributions écrites, les axes suivants :

- Les **opportunités offertes par les nouvelles technologies de sécurité** en analysant les besoins des forces de sécurité, entre autres dans la perspective des grands événements sportifs de 2023 et 2024.

- Les principes nécessaires à **la préservation des libertés** en définissant un cadre d'emploi et en associant la société civile.

2/ Questions

a. La notion de « technologies de sécurité » est large. Quelles sont les principales selon vous ? ***[Par exemple : traitement des données (textuelles, images, sonores), biométrie, mobilité – drones -.]***

La notion de technologies de sécurité est effectivement un concept large qui ne pourra pas être totalement parcouru au travers des quelques réponses que nous allons tenter d'apporter à cette mission parlementaire. Il convient donc d'en cerner les contours. Nous allons aborder cette notion essentiellement sous l'aspect des techniques et équipements permettant d'améliorer ou renforcer la sécurité des personnels des forces de sécurité ainsi que celle des concitoyens qu'elles sont chargées de protéger. Des machines, des appareils, connectés ou non à des dispositifs ou à des êtres humains.

Dans ce cadre, les technologies de sécurité qui seront citées sont, pour leur grande majorité, déjà déployées et utilisées, mais à des stades très divers selon les cas. Ainsi nous pouvons évoquer les technologies suivantes, sans que cela soit exhaustif :

- **Les drones : drone autonome, drone captif ou drone avec télépilote.**
- **Vidéosurveillance, vidéoprotection.**
- **Portiques de sécurité, dispositifs de détection de produits dangereux.**
- **Identification biométrique : technologies d'identification par reconnaissance faciale, empreintes digitales, mais aussi par l'iris, la voix.**

b. Pour quelles finalités ? ***[Par exemple : détection de situations, analyse prédictive, suivi des personnes.]***

S'agissant des drones, nous mettons prioritairement en avant deux utilisations :

- **Dans le cadre de manifestations ou d'évènements sur la voie publique, assurer la sécurité de la zone par survol d'un drone pour avoir un visuel précis, anticiper les déplacements de foule, repérer des groupes hostiles (type black bloc par exemple). Un dispositif permettant d'accroître la sécurité de l'ensemble des participants de tels évènements, à savoir de ceux qui assurent la sécurité et de ceux qui manifestent.**
- **Comme dispositif de reconnaissance préalable à toute intervention humaine sur des missions à risques.**

Concernant la vidéosurveillance, même si celle-ci est utilisée depuis des décennies, son perfectionnement est constant pour lutter contre le terrorisme, la délinquance ou encore l'hooliganisme. Associée à un dispositif d'intelligence artificielle, elle est efficace en matière de surveillance et de traçabilité. La vidéoprotection permet quant à elle d'assurer la sûreté de sites et de lieux sensibles.

Les portiques de sécurité et autres dispositifs de détection de produits dangereux (chimiques, explosifs) sont un complément efficace à la vidéoprotection pour la détection de menaces de sécurité et de sûreté sur des sites évènementiels ou sensibles.

L'identification biométrique est désormais présente partout dans notre quotidien : passeports biométriques, documents officiels, téléphones, ordinateurs. Elle existe également sous diverses formes : empreintes, reconnaissance faciale, iris, voix. Elle sert et peut servir de manière encore plus généralisée au sein des forces de sécurité. Elle renforce la sûreté bâtimentaire, améliore la sécurité des agents, la surveillance et la traçabilité. Ses utilisations sont multiples et sont appelées à se développer encore.

c. Pensez-vous qu'elles permettraient d'anticiper les évolutions des missions de sécurité dans les 10 à 20 ans à venir ? Comment voyez-vous ces évolutions ?

La mise à disposition de technologies de sécurité performantes, par des utilisateurs bien formés et recyclés, permettrait évidemment d'anticiper les évolutions de sécurité dans les années à venir. Mais si leur emploi n'est pas complètement bridé par un cadrage juridique trop contraignant. Mais il semble impossible de tout anticiper tant les menaces et les risques évoluent. Si ce n'est à s'adapter le plus rapidement possible à ces derniers.

d. Sur chaque technologie prioritaire évoquée, quel est le cadre juridique et doctrinal en cours ou envisagé ?

La technologie repousse chaque jour un peu plus les limites du possible dans ses applications concrètes. La vraie limite au développement des technologies de sécurité, dont un grand nombre existe déjà de longue date, c'est son cadre réglementaire et législatif. Et c'est en ce domaine qu'il faut trouver le juste équilibre entre la nécessaire sécurité des forces de sécurité et de leurs concitoyens, et la garantie des libertés individuelles. Ainsi, l'intérêt d'un grand nombre de technologies de sécurité est rendu nul du fait d'une législation trop contraignante.

Nous prendrons l'exemple de l'utilisation des drones. L'intérêt de ces machines, précédemment évoqué, est rendu inopérant par l'absence de cadrage juridique ou de trop grandes contraintes juridiques. L'absence de vrai statut d'aéronef d'état pour les drones utilisés par la police nationale ou de statut « d'aéronef dérogatoire » pris en compte par la DGAC, fait que l'utilisation de ces machines en milieu urbain s'avère impossible. Sans compter qu'à partir de 2023, la législation européenne interdira le vol de ces drones sans vrai statut. Dans la réalité, ces machines sont donc clouées au sol.

Quant aux autres technologies précitées, elles sont strictement encadrées, ce qui est parfaitement logique. Mais dans un carcan juridique tellement coercitif que leur intérêt d'utilisation, en matière de sécurité, peut s'avérer finalement très limité.

e. Comment les doctrines d'emploi peuvent-elles concilier une utilisation de ces technologies et des garanties pour les libertés (gradation des règles d'engagement, instauration de contrôles, etc.) ?

Les doctrines d'emploi découlent généralement d'un cadrage législatif qui n'est pas du ressort des forces de sécurité mais bel et bien des membres du parlement qui examinent les propositions et projets de lois puis les votent en y intégrant les garanties pour les libertés. Un exercice délicat dans un pays où la tradition de la protection de la vie privée, la garantie de la liberté individuelle sont fortes. Mais dont la contre productivité peut apparaître évidente lorsqu'elle neutralise la mise en place de moyens indispensables à assurer la parfaite sécurité des individus et la protection des intérêts de la nation.

f. Les ressources financières et humaines sont-elles actuellement suffisantes pour faire face à ces évolutions ?

Les ressources financières et humaines du ministère de l'Intérieur sont actuellement insuffisantes pour répondre aux enjeux sécuritaires actuels et à venir. Depuis 2015, avec la vague d'attentats terroristes qui a touché et touche encore notre nation, une prise de conscience politique a vu le jour concernant le manque de moyens humains et matériel. Ce « rééquilibrage budgétaire » des moyens reste toutefois insuffisant tant le retard accumulé sur le dernier quart de siècle est important. Concernant les ressources humaines, il est à noter que le volet

formation, notamment aux nouvelles technologies, est et sera un élément déterminant pour réussir à mieux appréhender, utiliser et anticiper les évolutions des missions de sécurité.

g. Comment verriez-vous les partenaires du « continuum de sécurité » associés opérationnellement à l'emploi de ces technologies ?

Clairement, les forces de sécurité intérieure sont dans l'incapacité d'assurer la totalité des missions de sécurité. Cette situation n'est pas nouvelle puisque la loi d'orientation et de programmation sur la sécurité de 1995 avait officialisé la privatisation de certaines d'entre-elles en autorisant des sociétés de surveillance et de sécurité privée à assurer des missions de sécurité collective dans les espaces publics.

La création du CNAPS en 2010 (mais entré en fonction en janvier 2012), a traduit la volonté des pouvoir publics de favoriser la création de sociétés dédiées à la surveillance et à la sécurité (en amont et en aval) tout en les régulant et réglementant. Cet EPA rattaché au ministère de l'Intérieur veille au respect du livre VI du code de sécurité intérieure. L'arsenal réglementaire du CNAPS a été complété par un code de déontologie de la sécurité privée (décret n° 2014-1253). Régulation, réglementation, police administrative. Autant de missions qui nécessitent des moyens accrus pour permettre à cet EPA d'assurer parfaitement ses missions auprès et sur des sociétés de dimensions très disparates qui se sont vu conférer des missions régaliennes.

Ce contrôle doit en premier lieu être renforcé si l'on veut envisager des partenariats opérationnels avec ces entreprises du « continuum de sécurité ». En amont, ces partenariats sont déjà effectifs entre les sociétés fournissant des technologies de sécurité et les forces de sécurité intérieure qui les utilisent de plus en plus fréquemment dans leur pluralité de missions, lorsqu'il existe un cadrage juridique permettant de le faire.

En aval, ces partenariats sont plus complexes à réaliser (surveillance et intervention humaines) mais existent également (lors de grands évènements notamment). Le renforcement de ces partenariats n'est envisageable qu'à la condition de rehausser le niveau de formation et de qualification de ces salariés du secteur privé. C'est là tout l'enjeu de la réussite de la loi « sécurité globale » promulguée le 25 mai dernier, pour envisager une collaboration efficiente entre les forces de sécurité et les acteurs privés de surveillance des personnes et des biens.

*

Ce questionnaire est indicatif et ne couvre pas l'intégralité des enjeux posés par les technologies de sécurité. La mission recueillera tout élément qui lui sera apporté afin de l'intégrer dans sa réflexion.

Contribution ACN
Mission parlementaire « Pour un usage responsable et acceptable par la société des technologies de sécurité » – JM Mis
7 juin 2021

Contribution ACN :

Mission parlementaire du député Jean-Michel MIS
« Pour un usage responsable et acceptable par la société des technologies de sécurité »

7 juin 2021

Résumé de la contribution ACN :

Les entreprises membres de l'Alliance pour la Confiance Numérique (ACN) revendiquent une vision française et européenne de la confiance numérique. Cette vision s'inscrit pleinement au service des valeurs fondamentales que sont notamment les droits de l'homme, les libertés fondamentales, la démocratie, l'état de droit et la souveraineté nationale et européenne. En effet, loin de s'opposer, la sécurité et les droits et libertés fondamentaux sont consubstantiels, et leur imbrication est la clef de voûte de notre modèle de société français et européen. Les entreprises du secteur de la confiance numérique considèrent que cette conception garantit l'expression et la promotion des valeurs fondamentales européennes et constitue un atout majeur dans la compétition avec des acteurs d'autres régions du monde ne la partageant pas. L'ACN contribue activement dans le cadre du CSF Industries de sécurité à l'élaboration d'une charte éthique de la profession visant à rendre plus visibles ces valeurs.

Cette approche constitue le socle de base sur lequel s'appuie le développement de nos solutions et technologies pour contribuer à l'avantage concurrentiel des technologies françaises de sécurité ainsi qu'à l'adhésion des populations. La France dispose d'atouts très forts dans ces domaines technologiques et bénéficie notamment d'un tissu industriel complet doté de compétences de pointe reconnues, composé de leaders mondiaux mais aussi de nombreuses PME et start up très innovantes, reposant sur une recherche publique et privée performante.

Ces technologies sont diverses et comprennent notamment les techniques biométriques, l'intelligence artificielle, les solutions d'identification, la cryptographie etc. Par ailleurs, ces différentes technologies peuvent être utilisées en vue de différentes finalités (sécuritaire, sanitaire, amélioration de la gestion des flux, organisation des grands évènements, safe and smart city…), et dans des cas d'usage très variés. Chacune de ces technologies dispose de nombreuses configurations permettant tout à la fois d'atteindre la finalité souhaitée tout en s'inscrivant dans le cadre du respect des valeurs fondamentales.

Pour autant, ces technologies, du fait notamment de raccourcis conceptuels largement répandus et/ou d'exemples tirés de contextes et de régions différentes, suscitent des interrogations légitimes de la part d'une partie de l'opinion publique.

L'ACN considère qu'un encadrement légal est une réponse appropriée permettant de fixer un cadre garantissant la conformité de ces usages basés sur ces technologies au regard des valeurs fondamentales, mais aussi de garantir aux industriels de pouvoir pleinement se développer dans le cadre tout en améliorant l'acceptabilité de ces technologies par le public.

Toutefois, l'enjeu crucial pour le législateur, est de proposer des réglementations qui parviennent à éliminer les risques d'atteintes au socle de valeurs fondamentales de la France et de l'Europe, sans pour autant dénoncer ou interdire des technologies dans leur ensemble (ou per se), privant de fait notre pays d'outils indispensables à notre souveraineté numérique et à notre autonomie stratégique.

Concernant l'intelligence artificielle (IA), plus particulièrement, l'efficacité de cette technologie réside principalement dans la capacité d'entrainement de ces IA. Il est donc extrêmement important d'être en capacité de certifier les bases d'entrainement.

Les technologies d'apprentissage IA sont donc très dépendantes des bases qui leur servent d'apprentissage. A minima, comme pour tout ce qui concerne l'IA, il faut créer des standards et des processus de qualification de ces bases d'apprentissages afin d'en assurer l'éthique et s'assurer que des biais d'apprentissage discriminant (parité, couleur de peau, …) ne sont pas introduits dans ces apprentissages. Il est donc opportun de contrôler la création de bases d'apprentissage en produisant des standards et des processus de qualification de ces bases d'apprentissage, s'assurer qu'elles sont protégées. Il apparaît également nécessaire que l'Europe puisse se doter de son propre organisme de certification des algorithmes biométriques, d'un point de vue sécuritaire mais aussi éthique. Aujourd'hui, seul le NIST américain est reconnu au niveau international.

Cela passe par une clarification légale à la fois des définitions utilisées mais aussi des finalités poursuivies par la loi et des risques que l'on souhaite éviter.

Pour autant, et notamment en vue des grands évènements sportifs à venir, mais aussi considérant l'évolution des besoins sécuritaires dans les prochaines années, les aspirations des citoyens, et les évolutions technologiques futures, les technologies de sécurité et de confiance numérique permettront d'apporter des solutions opportunes et efficaces. Il apparaît nécessaire de permettre à des expérimentations d'être menées.

Questions proposées par la mission parlementaire :

1. *La notion de « technologies de sécurité » est large. Quelles sont les principales selon vous ? [Par exemple : traitement des données (textuelles, images, sonores), biométrie, mobilité.]*

    - L'analyse d'image et le traitement des données associées, par extension la biométrie de reconnaissance du visage

    - L'usage des biométries (empreintes, visage, iris, voix) au sens plus large, les technologies de capture/contrôle biométrique sans contact et la prise en compte d'un consentement de l'usager.

- L'intelligence artificielle et les technologies d'analyse massive/traitement de ces données.
- La mobilité et l'identification numérique lors d'un parcours usager dans un environnement sécurisé, nécessitant l'usage ou non de base de données centralisée.
- La cryptographie en particulier la cryptographie post quantique
- L'évaluation, la certification la qualification des produits de sécurité

2. *Pour quelles finalités ? [Par exemple : détection de situations, analyse prédictive, suivi des personnes.]*

Les technologies de sécurité évoquées précédemment apportent, en usage simple et/ou combinées, des réponses extrêmement efficaces dans divers domaines d'application. Elles permettent notamment d'assurer un niveau de sécurité impossible à atteindre sans recours aux solutions technologiques, tout en préservant une expérience fluide pour les usagers, en favorisant par exemple des parcours intégrés et transparents qui sont développés autour de la protection des données personnelles.

Les finalités poursuivies sont naturellement très dépendantes des domaines d'application considérés parmi lesquels on peut citer :

➢ **Grands évènements / foules / Smart and safe cities**

Dans le cadre de lieux ou d'évènements rassemblant un grand nombre d'usagers et/ou présentant des enjeux de sécurité particuliers, les technologies de sécurité permettent notamment :

- de mieux anticiper les risques (détection de signaux faibles, renseignement,…),
- de faciliter la gestion de l'évènement en cours,
- d'avoir une réponse plus rapide, plus appropriée en cas de survenance d'un incident (aide à la prise de décision, gestion de crise, coordination de secours, gestion post incident,…)
- de fournir des éléments/données à des fins d'enquête post incident.

Pour atteindre ces objectifs, les technologies de confiance numérique peuvent notamment apporter des réponses aux finalités plus spécifiques ci-dessous :

- Apports technologiques liés aux individus : contrôler l'accès et le parcours de personnes pour les évènements ou les lieux avec de nombreux visiteurs, les locaux sensibles :
  - Identification des personnes pour l'accès d'un usager à un environnement sécurisé, contrôle du droit à l'accès et authentification du porteur via des solutions numériques ou de contrôles de titres physiques.
  - Identification de personnes inscrites aux fichiers (liste noire) ou autorisation d'accès aux seules personnes habilitées (liste blanche).

- Gestion en mobilité de l'identité numérique de confiance du visiteur étranger à l'occasion de l'évènement sportif, de l'étape de sa demande de visa avant d'entrer sur le territoire à sa sortie de territoire.

- Apports technologiques liés aux foules : assurer la sécurité et le bon déroulement d'évènements à forte affluence et aider à la gestion des flux dans les lieux / environnements sécurisés :

  - Suivi du parcours d'un usager dans un environnement sécurisé par reconnaissance biométrique (visage) ou non biométrique.
  - Suivi, analyse et gestion des flux de personnes avec reconnaissance biométrique ou non biométrique.
  - Détection de situations à risque sur la base de statistiques issues d'analyse d'images.

➢ **Sécurité publique :**

- Vérification biométrique d'identité ; Nous entendons ici par « biométrique » : visage et empreintes qui sont les plus répandues en France, mais pourraient s'étendre aisément à l'iris qui présente de nombreux avantages (pas de trace, capture sur sujet non consentant très difficile et grande fiabilité)

  - Ces vérifications peuvent être opérées en mobilité par un piéton ou à bord d'un véhicule ; ou en poste fixe à l'entrée (contrôle d'accès)
  - L'application utilisée (en mobilité comme en poste fixe) ne remonte que l'information utile et proportionnée au contexte de l'interrogation et à l'habilitation de l'agent contrôleur

- Reconnaissance faciale en temps réel

  - Extraction de visages depuis un flux vidéo (caméra piéton, caméra de surveillance, etc.)
  - Comparaison des visages extraits contre une base de personnes d'intérêts
  - Ce procédé permet de faire un criblage de la foule aux abords d'un site sensible : dans le cadre d'événement en justifiant le déploiement (Grands événements sportifs, culturels, ou politiques particulièrement sensibles. Il s'agit, pour illustrer, de remplacer les physionomistes aujourd'hui chargés d'identifier les interdits de stades aux abords de stades les soirs de matchs à haut risque)
  - Identification rapide de la situation en carte d'alerte enlèvement ou de notification de personne disparue (enfants, personnes âgées en situation de handicap…)
  - Détection d'événements particuliers en temps réel (mouvement de foule, course, altercations, véhicules suspects…)
  - Reconnaissance de véhicules (Classification, marque, modèle, couleur, plaque minéralogique)

- **Soutien à l'investigation dans un cadre judiciaire** :
  - Analyse d'images dans le cadre d'enquête,
    - Les moyens de captation d'images sont partout : smartphones, vidéosurveillance privée (banques, commerces, particuliers, etc.) et publique. Ces images sont une mine d'information difficile à exploiter : chronophage (information linéaire) et éphémère (contraintes techniques et obligations légales conduisent à l'écrasement de ces données sous quelques jours à un mois : si elles ne sont pas saisies à temps, si l'enquête ne s'oriente pas rapidement dans la bonne rue, ces données sont perdues)
    - Le traitement automatisé de ces images (photos extraites d'un smartphone saisi, aussi bien que les vidéos récupérées sur les lieux d'une infraction) permettrait de gagner un temps considérable, de décharger les investigateurs d'un tâche harassante (visionner des heures d'images) en leur permettant de se concentrer sur leur métier (comprendre les faits et confondre des coupables). A effectif constant ces outils permettraient de traiter plus d'affaires, d'abaisser le seuil en deçà duquel une affaire ne « vaut » pas la peine d'y consacrer du temps : ces « petites affaires » sont aussi celles qui contribuent au « sentiment d'insécurité », et ce d'autant plus que les victimes ont le sentiment que l'acte ayant été commis dans le champ d'une caméra, la résolution du cas devrait être extrêmement simple, entraînant une frustration du public.
    - Ces outils d'analyse automatique ne sont pas nécessairement biométriques, dans un premier temps, mais ils font massivement usage d'algorithmes (détection et classification de mouvements, d'objets, de couleurs, de véhicules, de silhouettes, etc.) afin d'accélérer et faciliter le travail des investigateurs. Dans un deuxième temps ces outils d'analyse peuvent être d'ordre biométrique, dans ce cas ils sont potentiellement réservés à certains utilisateurs et à certaines classes de faits. Le même outil peut offrir à chaque utilisateur les seules fonctions de recherches auxquelles son statut donne accès.

- **Soutien au renseignement ayant trait à la sécurité intérieure :**
  - Reconnaissance faciale dans le but d'identifier les associés de personnes d'intérêt dans le cadre d'associations terroristes
  - Ou pour l'identification de personnes présentes sur des théâtres d'opération extérieure pour des faits de terrorisme
  - Technologies de récupération de données dans le cadre de saisies d'équipements informatiques
  - Technologie d'enrichissement et de recoupement de données (data analytics) permettant de prévenir la menace terroriste à venir en fusionnant différentes modalités (technologies biométriques, reconnaissance du langage naturel pour la communication écrite et orale dans le cadre d'interceptions ou de saisies de matériel informatique, données géographiques

3. Avec quels vecteurs ?

Les vecteurs utilisés pour mettre en œuvre ces différentes technologies sont notamment :

- Les drones
- Portail à Unicité de Passage
- Les caméras de vidéosurveillance et d'authentification (LAPI)
- Les lecteurs de contrôle d'accès biométriques
- Les Titres de Transports et Titres de Transports Numériques
- Les dispositifs d'interception de type IEM (drones par exemple)
- Programmation Neuro-Linguistique
- Intelligence Artificielle

4. *Pensez-vous qu'elles permettraient d'anticiper les évolutions des missions de sécurité dans les 10 à 20 ans à venir ? Comment voyez-vous ces évolutions ?*

Oui, assurément. La société étant en perpétuelle évolution (mobilité frontalière, idéologies, …), il semble indispensable de bénéficier de technologies innovantes permettant de prendre des décisions éclairées, d'adopter un modèle zéro-confiance et de se focaliser sur les problématiques de sûreté.

La mission de maintien de la sécurité dans l'espace public, donc soumise à ces évolutions sociétales devra notamment prendre en compte les éléments suivants :

- ✓ **Les missions**
  - Haut du spectre :
    - La convergence des menaces terroriste et criminelle, que ce soit dans la population concernée, les modus operandi observés, qui pousse les forces de l'ordre à mener des activités de renseignement permettant de prévenir le passage à l'acte ;
    - Le développement rapide de la cybercriminalité qui ne poursuit pas que des intentions criminelles, mais parfois orientées vers la disruption des capacités de réponse des forces de l'ordre ;
  - Police du quotidien :
    - Gains de productivité : par exemple dans le domaine de l'analyse d'image et de la reconnaissance du visage, depuis 4 -5 ans, il y a une formidable accélération des performances de comparaison d'image avec l'introduction des algorithmes de machine learning qui fonctionnent par apprentissage (IA). Il est illusoire de s'opposer à l'apport opérationnel et l'amélioration de la fiabilité de ces technologies, il faut donc plutôt se concentrer sur le mode

d'utilisation et le contrôle de cette utilisation. D'où le besoin de légiférer pour définir un cadre éthique et RGPD, pour ces technologies.

- Proximité avec la population et interaction avec les autres acteurs (élus, différentes forces de sécurité, etc.) : incarner le continuum de sécurité au quotidien.

✓ **L'attente du public pour une sécurité en profondeur et transparente :**

- Les premiers témoins de cette évolution sont les gardes-frontières : les flux grandissants n'ont pas réduit les menaces contre lesquelles ils luttent – au contraire – mais ils doivent satisfaire l'attente des 99,9% de voyageurs qui n'ont rien à se reprocher et sont de moins en moins tolérants à l'attente et aux contraintes ;
- Dans le domaine de l'identité numérique utilisée et contrôlée en mobilité : La crise sanitaire a favorisé l'accélération des transformations numériques dans nos sociétés. Lorsque de nouvelles contraintes émergent (besoin d'un pass sanitaire par exemple), l'approche digitale est favorisée car plus agile et flexible en fonction de l'évolution des accords de sécurité de passage aux frontières entre pays. Ce besoin d'une digitalisation des contrôles est une tendance qui va se renforcer, et les technologies mises en œuvre à l'occasion d'évènements sportifs préfigureront ce qui sera appliqué plus généralement à l'horizon 5-10-20 ans dans le domaine des mobilités entre Etats.
- Cette digitalisation des usages ne peut pas exclure la composante matérielle et physique des éléments de contrôle. Il s'agit bien de penser la complémentarité des approches et la capacité de nos technologies à être opérationnelles de manière multimodales et multisupports.
- Le retour d'expérience des spectateurs français de retour de la coupe du monde FIFA 2018 était partagé entre satisfaction quant au sentiment de sécurité, à la simplicité d'accès, la facilité de déplacement. Toutefois des questions ont été légitimement soulevées quant à l'usage qui sera fait des données de reconnaissance faciale ainsi collectées ;
- Or les industriels français du domaine assurent qu'il est techniquement possible de concilier la triple exigence de sécurité, fluidité et respect de la vie privée tel que garanti par le RGPD. A défaut de progresser dans cette direction il faudra se résoudre à limiter les flux ou à voir s'étirer les files d'attentes, elles-mêmes facteur de vulnérabilité et assurément d'insatisfaction.

5. *Sur chaque technologie prioritaire évoquée, quel est l'état de développement de l'industrie française ? Que lui manque-t-il pour se perfectionner ?*

Les industriels français et plus globalement européens bénéficient de technologies de pointe sur le marché. Les entreprises de notre secteur disposent de technologies et solutions qui sont compétitives au niveau mondial. A titre d'exemple, les entreprises françaises revendiquent un leadership mondial en matière de conception et développement de technologies cryptographiques

dans les éléments sécurisés embarqués, qui représentent le socle de confiance de l'identité internationale (le passeport) et nationale (CNIe) dans sa dimension physique puis demain dans sa dimension digitale/numérique.

Afin que le tissu industriel français puisse capitaliser sur son excellence technologique reconnue et sur les apports d'une recherche de pointe, mais aussi afin de rendre la situation équitable vis-à-vis de la concurrence internationale, il serait nécessaire de parvenir à déployer des conditions de marché propices ainsi qu'un cadre légal clair :

- ✓ Un marché domestique propice
  - Les champions nationaux ainsi que les jeunes pousses doivent pouvoir s'appuyer sur un marché national propice : le niveau d'exigence d'un système opérationnel est sans commune mesure avec le niveau d'exigence d'un démonstrateur.
    - Le développement, le maintien en conditions opérationnelles et les évolutions d'une solution en production ont un coût, d'autant plus élevé qu'ils sont réalisés avec de la main d'œuvre exclusivement française.
    - Il est difficilement audible qu'en même temps que l'acheteur public exige la propriété intellectuelle des solutions qu'il acquière, il explique que parce qu'il a exprimé un besoin et/ou octroyé une subvention il a créé une richesse que l'industriel pourra valoriser à l'export et donc exige une tarification avantageuse.
  - Que lorsque des applications sont critiques pour la sécurité de l'Etat, les fournisseurs soient soumis à une scrutation permettant de garantir la loyauté de ces applications vis-à-vis de ses utilisateurs et de sa fonction. Dans ce contexte, des acteurs ayant fait le choix de localiser leur R&D en France, dans des conditions sujettes à des normes de sécurité élevées, devraient pouvoir faire valoir cet avantage. Nous appelons de nos vœux une réglementation française et européenne et l'avantage donné aux entreprises qui en respectent les principes et les valeurs.

- ✓ Un cadre réglementaire clair

Le cadre légal et réglementaire national et européen doit pouvoir soutenir cette base industrielle et technologique en définissant des cas d'usages éthiques. C'est une condition essentielle pour garantir une souveraineté numérique au niveau national et européen. Il est important de noter que ces besoins sont de mieux en mieux accompagnés par la commission Européenne avec ses réglementations eIDAS, NIS2, E privacy, Cyber act ? ….

Pour ce faire, il apparaît pertinent de :

- ➢ Légiférer sur l'Intelligence Artificielle (IA) et plus particulièrement sur les modes d'apprentissages IA au service de l'analyse d'image et de la biométrie :

  Aujourd'hui, un tissu extrêmement riche et innovant d'entreprises de toutes tailles (start up, PME, ETI, grands groupes) développe en France des technologies d'intelligence artificielle. Néanmoins, ce tissu industriel innovant et foisonnant se heurte à une problématique commune : l'absence d'un cadre réglementaire clair et précis. Sans cadre légal clair, l'aléa

juridique inhérent à ces sujets empêche ces entreprises de développer, d'expérimenter et d'améliorer leurs technologies d'IA et ne leur permet pas d'être compétitives au regard de leurs concurrentes étrangères soumises à des réglementations différentes. Au demeurant, un cadre légal précis permettrait également l'adoption rapide de ces technologies par les clients potentiels.

En amont, l'intelligence artificielle ne peut être développée que grâce à des données d'entraînement par rapport à la tâche qui lui est confiée. Plus particulièrement, les solutions d'analyse d'images pour la sécurité nécessitent une grande quantité d'images issues de caméras de vidéosurveillance sur les voies publiques.

Il est aujourd'hui interdit de collecter ces images pour entraîner les logiciels d'intelligence artificielle. La conséquence directe est que les technologies d'intelligence artificielle développées en France sont moins performantes que dans les pays où le cadre légal favorise la R&D.

En aval, le flou juridique sur les notions de base légale de traitement, notamment l'intérêt légitime et de données biométriques, freine l'adoption de ces technologies par les clients potentiels qui craignent un risque réputationnel fort. Ainsi le développement commercial des entreprises françaises d'intelligence artificielle est extrêmement lent et ne répond pas aux attentes des investisseurs, ce qui empêche le développement de l'écosystème IA.

Les technologies d'apprentissage IA sont donc très dépendantes des bases qui leur servent d'apprentissage. A minima, comme pour tout ce qui concerne l'IA, il faut créer des standards et des processus de qualification de ces bases d'apprentissages afin d'en assurer l'éthique et s'assurer que des biais d'apprentissage discriminant (parité, couleur de peau, …) ne sont pas introduits dans ces apprentissages.

Il faut donc :

- ✓ **Contrôler la création de bases d'apprentissage,**
- ✓ **S'assurer qu'elles sont protégées,**
- ✓ **Plus globalement réglementer les conditions de stockage et d'usage de ces images.**

De même il apparait nécessaire que l'Europe puisse se doter de son propre organisme de certification des algorithmes biométriques. Aujourd'hui, seul le NIST américain est reconnu au niveau international.

- ➢ **Favoriser l'émergence de niveaux de certification européens des technologies biométriques indépendamment des critères de performances made in USA :**
  - La certification des équipements européens ne doit plus dépendre des critères FBI/NIST mais doit répondre à des critères plus spécifiques à l'Europe : respects du RGPD, performances anti-spoofing.
  - La création d'un référentiel européen et d'un organisme de certification permettrait de dessiner une « voie européenne » intégrant les critères éthiques à la seule certification technologique et sécuritaire.

- La participation large et active aux organismes de normalisation Européen (ETSI, CEN CENELEC) et internationaux doit être soutenue par les pouvoirs publics car se joue là les enjeux technologiques de demain.

➢ **Accélérer le déploiement de l'identité Numérique et mobile en France**

Avec la perspective d'une meilleur appropriation et acceptation de ces notions d'identification numérique, le déploiement rapide d'une identité numérique en France et un développement des services numériques de vérification s'appuyant sur cette identité numérique ou sur les titres d'identité régaliens devrait contribuer à une préparation de l'écosystème Français en vue des prochains grands évènements sportifs.

➢ **Faciliter les activités de recherche exploitant des données personnelles**

Les activités de recherche portant sur le traitement des données personnelles devraient être rendues plus simples grâce à un régime dérogatoire (à des seules fins de recherche), comme rendues possibles par le RGPD (opportunité saisie par d'autres pays européen, mais pas par la France).

6. *Comment les configurations techniques peuvent-elles concilier une utilisation de ces technologies et des garanties pour les libertés (protection des données, contrôles automatisés, etc.) ?*

Les configurations techniques répondent dans de très nombreux cas d'usage aux risques inhérents à l'usage de ces technologies. En effet, les acteurs du domaine de la confiance numérique se placent sans ambiguïté dans le cadre conceptuel des valeurs fondamentales françaises et européennes. Les produits et solutions qu'ils développent sont conçus pour intégrer des notions telles que la protection de la vie privée ou des libertés fondamentales.

Il est pour autant naturel et légitime que le législateur souhaite poser un cadre pour s'assurer que toutes les solutions proposées s'inscrivent dans ce cadre. Cet encadrement législatif est parfaitement bienvenu pour les industriels dans la mesure où il leur permet de pouvoir se développer dans un champ aux contours clairs mais aussi dans la mesure où un tel cadre permet également de renforcer la confiance que les utilisateurs peuvent accorder aux technologies mises en œuvre.

Toutefois, l'enjeu crucial pour le législateur, est de proposer des réglementations qui parviennent à éliminer les risques d'atteintes au socle de valeurs fondamentales de la France et de l'Europe, sans pour autant dénoncer ou interdire des technologies dans leur ensemble (ou *per se*), privant de fait notre pays d'outils indispensables à notre souveraineté numérique et à notre autonomie stratégique. Dans ces domaines très stratégiques, le législateur devrait suivre le conseil avisé de Montesquieu et « n'y toucher que d'une main tremblante », sous

peine d'obérer durablement nos capacités à maîtriser notre avenir numérique, en privant de fait les acteurs nationaux de pouvoir participer aux avancées mondiales dans ces domaines.

Cela passe par une clarification légale à la fois des définitions utilisées mais aussi des finalités poursuivies par la loi et des risques que l'on souhaite éviter.

Ci-dessous quelques exemples permettant d'illustrer des configurations techniques permettant de concilier une finalité poursuivie et le respect des exigences liées aux valeurs fondamentales :

- Exemple de la reconnaissance du visage (le consentement)

Par essence, la biométrie du visage est passive : son usage n'est pas conditionné à l'action de l'usager traduisant son accord à l'utilisation de son image pour son identification/authentification, comme peuvent l'être la biométrie empreinte ou la biométrie vocale.

Afin de rendre l'usage de cette technologie compatible avec notamment le RGPD une approche basée sur les principes suivants peut-être proposée :

- Rendre « active » l'authentification biométrique par le visage, en limitant la capacité de matching des équipements à du matching 1 :1, dont l'image de référence biométrique est cryptée, non réversible et reste toujours sous le contrôle de l'usager traduisant ainsi son consentement ou non à cette authentification,
- Ces équipements doivent pouvoir être certifiés et ne doivent pas pouvoir stocker le résultat de leur identification,
- Ces équipements doivent assurer une traçabilité de leur matching, - Ces équipements doivent pouvoir être certifiés anti-spoofing, c'est-à-dire résister aux fraudes afin d'éviter l'usurpation d'identité.

Cette solution d'identification du visage 1 contre 1 a fait l'objet d'un retour positif de la CNIL en ce qu'elle respecte la protection des données des passagers qui utilisent cette solution pour faciliter leur parcours d'embarquement dans un aéroport.

- Exemple de l'identité numérique « à la main » de son porteur :

A l'image de la CNIe qui intègre un compartiment numérique avec une identité numérique protégée par un code PIN, l'accès et le contrôle de l'identité numérique d'un porteur doit rester conditionnée au consentement du porteur et se traduit par le déverrouillage de l'accès au compartiment via le code PIN.

La généralisation de ce principe à l'échelle nationale à travers le déploiement rapide d'une identité numérique en France devrait favoriser l'appropriation et l'acceptation de ces modalités d'échange numérique entre le porteur et le contrôleur avant les évènements sportifs prévus à l'horizon de 2 ans.

➢ Exemple de l'analyse d'image à vocation d'analyse statistique :

De nombreuses solutions d'industriels émergent dans le domaine de l'analyse des images issues de caméras. Ces analyses résultant de l'utilisation de l'intelligence artificielle peuvent notamment se fonder sur des éléments non biométriques pour produire un contenu extrêmement riche et utile, avec des finalités extrêmement diversifiées (meilleure compréhension des flux de personnes, finalité sanitaire dans l'exemple de la détection du port du masque, etc.) particulièrement utile en prévision des futurs grands évènements (notamment sportifs) en France, tout en respectant un usage proportionné et éthique des données traitées.

Le retour d'expérience à travers la mise en application des technologies d'analyse d'image dans le domaine des transports (RATP, SNCF, …) pour la détection du port du masque, met en lumière les conditions de succès pour une technologie de traitement d'image respectueuse des libertés :

- Des technologies capables de fonctionner sans stockage des données,
- Le besoin d'une règlementation pour avancer, à l'exemple du décret publié en accord avec la CNIL pour le domaine des transports.

Le législateur doit se saisir des sujets d'analyse d'image et envisager une réforme du régime juridique de la vidéoprotection pour y intégrer un usage raisonné et éthique des technologies de vision par ordinateur :

1. **Moderniser le régime de la vidéoprotection afin d'y intégrer l'analyse d'images par ordinateur ;**
2. **Prendre en compte la protection des données à caractère personnel dans le régime de la vidéoprotection ;**
3. **Etendre le périmètre des finalités de la vidéoprotection afin d'y intégrer la sécurité sanitaire par exemple.**

➢ Exemple de la notion d'identité temporaire pour les événements sportifs (Fan ID)

L'usage d'une identité temporaire pour les événements sportifs pourrait constituer un cas d'utilisation pertinent de nouvelles solutions d'identification temporaires.

Solution sans base de données, elle préserve l'identité des porteurs tout en assurant un niveau élevé de sécurité. Elle permet la gestion de l'identité, la délégation d'identité, le contrôle dans tout type d'environnement (sans accès au réseau, avec un smartphone ou une caméra de type vidéo surveillance).

7. *Les cadres d'expérimentation sont souvent mis en avant pour le perfectionnement de ces technologies. Quelles sont selon vous les priorités ? Quels seraient les contours de ces cadres ? A quelles fins ?*

A propos des expérimentations :

- La priorité d'une expérimentation doit être de **faire la démonstration de la valeur sociétale du système**, telle qu'espérée dans le cadre de sa conception. Par conséquent le public participant doit être correctement sondé, avant, pendant et après l'expérimentation, tant par des méthodes de sondage quantitatives que qualitatives. A défaut ce sont les commentateurs pas nécessairement correctement informés et surtout pas directement impliqués qui risquent de faire « l'opinion ».
- La **vérification du bon fonctionnement du système** en termes de performances, sorti du laboratoire, dans des conditions opérationnelles ou les plus proches possible des conditions opérationnelles.
- Le **bon fonctionnement des processus décisionnels** associés aux résultats produits par le système, notamment dans le cadre de l'identification biométrique, concernant le contrôle et la confirmation manuelle des informations produites par le système.
- Sur des expérimentations sur un moyen terme, de vérifier que l'évolution des usages de ces systèmes reste **compatible avec l'intention initiale** ayant mené à leur déploiement.
- Enfin les expérimentations sont un exercice particulièrement onéreux (il engage des ressources qui coûtent et ne sont plus disponibles pour des tâches productives), ceci impose de considérer au moins trois aspects :
  - Les expérimentations doivent s'inscrire dans une perspective d'acquisition et/ou l'existence de débouchés ;
  - Les industriels doivent être impliqués en amont (planification), l'objectif étant que ces expérimentations leur profitent ;
  - La finalité de l'expérimentation doit être partagée et intangible (effets à obtenir clairs et compris) : les industriels ne doivent pas être instrumentalisés ou piégés (engager l'industriel dans un exercice, pro bono, pour en changer les règles en cours… toujours pro bono).

Quelques exemples d'expérimentations qui pourraient utilement être menées, en particulier en prévision et/ou dans le cadre des Jeux Olympiques 2024 :

- S'appuyer sur le décret Transport pour **l'expérimentation des technologies d'analyse d'images à vocation statistique** dans le domaine de l'organisation d'évènements majeurs en répétition des JO 2024.

- **Favoriser l'utilisation de l'identité numérique ou d'une identité numérique dont elle est dérivée sur smartphone** dans la gestion des contrôles d'accès à certains évènements.

- **Tester la notion de fan ID** (identité temporaire du supporter) à l'occasion de la Coupe du Monde de Rugby 2023 en répétition des JO 2024.

Plus généralement, il serait intéressant de permettre aux entreprises technologiques de la confiance numérique d'innover dans l'esprit de la proposition de loi N°4127, « d'expérimentation créant un cadre d'analyse scientifique et une consultation citoyenne sur les dispositifs de reconnaissance faciale par l'intelligence artificielle », et notamment de :

- Permettre aux technologies d'exprimer leur potentiel dans le cadre d'expérimentations rendues possibles par une loi spécifique,

- Faire de la pédagogie sur les garde-fous technologiques et réglementaires pour rassurer les usagers et la population dans son ensemble en rendant les résultats de ces expérimentations disponibles aux instances compétentes, voire (mieux) en les associant directement au processus d'expérimentation.

A propos de l'ACN (www.confiance-numerique.fr) :

L'Alliance pour la Confiance Numérique (ACN) représente les entreprises (leaders mondiaux, PME et ETI) du secteur de la confiance numérique notamment celles de la cybersécurité et de l'identité numérique. La France dispose dans ce domaine d'un tissu industriel très performant et d'une excellence internationalement reconnue grâce aux différentes acteurs dynamiques du secteur. D'après l'Observatoire ACN de la confiance numérique 2021 (disponible en téléchargement sur www.confiance-numerique.fr), on dénombre, dans le secteur, plus de 2000 entreprises réalisant en France près de 13,4 Milliards d'euros de chiffre d'affaire dans ce secteur en forte croissance (8,1% de croissance moyenne annuelle en France sur la période 2015-2020). L'ACN est membre de la FIEEC (Fédération des Industries Electriques, Electroniques et de Communication) et participe aux travaux du Comité Stratégique de Filière – CSF – des industries de sécurité. Par ailleurs, l'ACN est également membre fondateur de l'ECSO (European CyberSecurity Organisation).

ALTERNATIVE Police
47 avenue Simon Bolivar 75019 PARIS
0180496687 – secretariat@alternativepn.fr

Denis JACOB
Secrétaire Général

Réf.: APN/BN/DJ/2021-036

PARIS, le 31 mai 2021

Monsieur Jean-Michel MIS
Député
Assemblée nationale
126, rue de l'Université
75007 PARIS

Monsieur le député,

Par courriel en date du 21 mai, vous m'avez sollicité afin de vous transmettre une contribution de mon organisation syndicale sur la question des technologies, à la sécurité et aux libertés, dans le cadre d'une mission que vous a confié monsieur le Premier Ministre

Aussi, c'est avec plaisir que je vous prie de trouver à la suite de ce courrier, les différentes réflexions conduites par Alternative Police CFDT qui allient à la fois la nécessité des nouvelles technologies pour l'efficacité du travail policier au quotidien pour une meilleure sécurité et de l'incontournable impératif respect des libertés.

Je vous en souhaite bonne réception en vous précisant que mes représentants restent à votre disposition pour tout renseignement complémentaire que vous jugeriez utile de solliciter.

Je vous prie de croire, Monsieur le Député, à l'expression de mes sentiments les plus respectueux.

Le Secrétaire Général

Bien cordialement

Denis JACOB

L’emploi des nouvelles technologies par les forces de sécurité

SUJET :

Intelligence artificielle, analyse automatisée des données, des images, vidéos, drones

QUESTIONS :

Leurs utilisations engendrent des limitations des libertés individuelles et publiques.
Qu’elles sont les opportunités, détaillez objectifs concrets et opérationnels et les gains attendus ?
Réflexion sur cadre d’emploi pour limiter rapport intrusif et réfléchir à cadre d’emploi cohérent de ces technologies.

PROPOS LIMINAIRE :

L'intérêt sécuritaire de faire appel à ces nouvelles technologies repose sur deux aspects principaux :

- L’un préventif et administratif : Dissuasion
- L’autre répressif et judiciaire : Matérialisation de l’infraction. La matérialisation est un des éléments qui concourt à la manifestation de la vérité.

C’est sur ce second aspect, judiciaire, que nous présentons notre argumentaire.

La procédure et la réponse pénale reposent sur deux éléments :

- L’élément de preuve matériel et l’élément moral (reconnaissance de l’acte, aveux, les explications, le niveau de compréhension de l’acte exécuté et éventuellement l’irresponsabilité pénale, l’erreur de droit, les obligations telle la légitime défense).
- L’élément matériel et moral déterminent la qualification de l’infraction et de la peine encourue.

L’aveux, la reconnaissance de culpabilité ne suffit pas à faire condamner l'auteur d'un fait. Il faut obligatoirement matérialiser l’infraction, d’où la nécessité d’outils et de technologies nouvelles. La Police Judiciaire est sans cesse contrainte à de nouvelles infractions liées à la modernité, aux nouvelles technologies et doit s’adapter afin d’y répondre.

DEVELOPPEMENT :

Nous constatons que de récentes infractions naissent de technologies nouvelles, notamment par le biais du numérique de l’informatique (escroqueries, terrorisme, stupéfiants, armes, prostitutions, jeux d’argent, pédopornographie etc.).
C’est pourquoi, nous devons constamment nous adapter et faire appel à de nouvelles technologies à même de répondre à la matérialisation des infractions commises.

La Police Judiciaire utilise déjà de nombreux procédés techniques pouvant porter atteintes aux Libertés Individuelles tels que :

- La téléphonie (écoutes téléphoniques, exploitation des facturations détaillées, bornage des cellules d’appels, Imsi catcher.).
- Le patrimoine (Recherches comptes bancaires, biens immobiliers et mobiliers, véhicules, locations, coffre-fort, Fichiers Impôts, recherches de sociétés, etc.)
- La fixation d 'image et son, photographie, vidéo et sonorisation de domiciles, de véhicules.

Ces éléments participent à matérialiser, à identifier, figer une scène ou des paroles échangées. Ils sont versés à la procédure. La Police Technique et Scientifique participe à la matérialisation de l'infraction en exploitant les traces A.D.N et les la dactyloscopie (empreintes)

Outre ces techniques utilisées, la Police Judiciaire utilise également des logiciels d 'aides à l'enquête, lesquels ont été présentés et autorisés par la CNIL avant exploitation.

En dehors de notre documentation spécialisée, nous disposons également :

- D'un Logiciel d'analyse criminelle (ANACRIM). Des Policiers et gendarmes sont formés es qualité d'analyste criminel. Ils renseignent ce logiciel à l'aide des éléments contenus dans une procédure et ce dernier apporte des contradictions ou des oublis dans l'enquête. Ce logiciel et ces analystes sont indispensables pour des procédures lourdes comportant des milliers de feuillets réalisés sur plusieurs années par des policiers multiples et variés.
- Le service de Police Judiciaire SALVAC dispose également de son propre logiciel (Licence Canadienne payée chaque année au pays). Les fonctionnaires de ce groupe alimentent une base de données à l'aide de procédure criminelle et dont le but étant d'identifier après analyse réalisée par le logiciel, des tueurs en série.
- Le Logiciel d'analyse téléphonique MERCURE est utilisé comme un outil d 'aide à l'enquête judiciaire qui permet de matérialiser des contacts téléphoniques ainsi que des bornages d'appels.

AUTORITE DE CONTROLE :

L'ensemble des technologies utilisés et susmentionnées en matière de police Judiciaire, le sont après autorisation d'un Magistrat et demeurent sous son contrôle constant et permanent.
De même, ces technologies sont utilisées en fonction d'un certain degré de l'infraction. Elles ne sont pas ou rarement utilisées en matière contraventionnelle.

Ainsi, le Magistrat (Parquet, Juge d'instruction ou J.L.D) se portent garants de la conservation des libertés individuelles et publiques.

De même, l'utilisation de ces nouvelles technologies ne sont pas infaillibles. La personne humaine reste incontournable car elle doit contrôler les éléments apportés par ces derniers et les considérer comme une aide à l'enquête et non pas comme un élément probant.

Pour exemple, un logiciel de reconnaissance vocale qui serait à même de remplacer un enquêteur afin de retranscrire des échanges téléphoniques se limite à la retranscription sans comprendre la teneur des propos échangés.

De même, après reconnaissance numérique d 'empreinte digitale réalisée par la base de données, un contrôle humain reste nécessaire pour confirmer la comparaison.

Le contrôle est également exercé par les droits de la défense (avocats) ou victimes, lorsque des éléments émanant de nouvelles technologies sont versés à une procédure.

GAINS OBTENUS :

L'utilisation de ces technologies nous permet de limiter en grand nombre le personnel ressource. En effet, une exploitation d'un bornage téléphonique ou d 'une balise de véhicule permettra à un seul enquêteur de réaliser le suivi numérique H 24 d'un individu alors qu'il en faudrait 18 pour un suivi physique (3 groupes de 6 fonctionnaires pour 3 vacations de 8 heures)

Les logiciels d'analyse permettent d'apporter des éléments manquants à des procédures qui ne peuvent pas être exploitées par l'humain (ceci eu égard au nombre conséquent d'années d'instructions, de feuillets rédigés, de Policiers qui se sont succédés).
Il en est de même pour ce qui concerne l'exploitation de la téléphonie à l'aide du logiciel MERCURE. Le gain de temps obtenu par une analyse informatique est considérable.
La captation d 'image, l ' emploi de photos ou vidéos permettent de fixer une scène dans le temps. Ainsi de nombreux détails qui pourraient échapper à l'œil humain sont numérisés et pixelisés.

En matière de scène de crime, l'utilisation de technologie permettant la fixation d'image est indispensable. En effet, une instruction judiciaire pouvant être conduite durant plusieurs années avant un jugement ou l'interpellation d'un mis en cause, le « gel » d'une scène de crime est une aide matérielle à la manifestation de la vérité.
De même une surveillance humaine de 360° sollicite l'emploi de 4 fonctionnaires alors qu'une unique caméra le réalise sans limitation de durée et sans nécessité de remplacement des ressources humaines.

En matière de Police judiciaire, l'emploi de caméra permet de matérialiser de nombreuses scènes d'infractions et de préserver les ressources en effectifs mais aussi de ne pas se faire repérer ou identifier.

Le système de vidéosurveillance miniaturisé est également utilisé dans des espaces où le Policier ne peut être présent (hall d 'immeuble avec trafic de stupéfiants, entrepôts etc.)
L'utilisation de drones permet de surveiller à distance, notamment en zone rurale sans avoir à approcher des objectifs ou des scènes à observer.

L'utilisation d 'images communiquées à l'aide d'un drone pourrait être complémentaire à un bornage téléphonique ou un balisage. Outre la localisation réalisée par ces derniers, l'image obtenue du drone serait un support additionnel permettant de voir une scène alors que la localisation se limite à … localiser.

Une surveillance dite « physique » réalisée par des effectifs de Police sur du long terme (comme pour un trafic de stupéfiants) est très difficile car les véhicules de Police d'un groupe d'enquête ne sont pas nombreux et que passé plusieurs surveillances et filatures, ils sont identifiés. La forte pénurie de véhicules dans les groupes d'enquêtes engendre une surveillance à distance (bornage, balise) indispensable.

L'utilisation de drone semble fort utile à certaines occasions. Tout comme l'emploi de ces derniers afin de repérer les accès et sorties d'une habitation avant pénétration pour interpellation.

En matière de Police de maintien de l'ordre, l'utilisation de drones peut être utile afin de constater ce qui se produit au sein d'une manifestation sans avoir à l'infiltrer et d'identifier ou repérer d'éventuels perturbateurs.

La généralisation de la caméra « piéton » des effectifs de Police de voie publique permettra également de constater des scènes d'infraction.

Un logiciel de reconnaissance faciale pourrait également être à l'étude. Notamment pour les recherches judiciaires, les contrôles frontières aux aéroports. En effet, lorsqu'un individu contrôlé sur la voie publique est dépourvu de pièce d 'identité et qu'il communique une identité verbale, il peut être présenté à l'officier de police judiciaire, lequel dispose d'un délai de 4 heures pour s'assurer de l'identification de cette personne. Une comparaison de sa photographie avec notre base de données des infractions criminelle ou des personnes recherchées semble judicieux.

L'analyse réalisée par le logiciel reste également un outil utile à l'enquête qui doit être soumis à contrôle et approbation du Policier.

LA REPONSABILITE EN CAS DE DEFAILLANCE :

Si les éléments matériels apportés par ces nouvelles technologies sont défaillants et entraînent une erreur de jugement, la responsabilité s'apparente à l'erreur de fait commise par une juridiction dans son appréciation de la culpabilité d'une personne poursuivie. Cette dernière peut, si elle a été condamnée définitivement (après appel), être réparée sous certaines conditions en se pourvoyant en révision. De même, la Justice indemnise les victimes d'erreurs ou d'errances judiciaires.

L'Etat offre réparation aux victimes du préjudice qu'elles peuvent avoir subi d'un dysfonctionnement ou d'un manque de moyen de l'institution judiciaire.

Il existe déjà une requête à adresser au Juge du contentieux de la protection siégeant près les différents T.G.I, aux fins de rectification d 'erreur matérielle.

CONCLUSION :

Les nouvelles technologies sont d'une nécessité absolue pour renforcer la rapidité et l'efficacité de l'action policier.

Elles doivent évidemment faire l'objet d'un cadre juridique afin de préserver la garantie des Libertés individuelles et publiques. Un contrôle peut être exercé par l'autorité judiciaire d'une part pour ce qui concerne l 'aspect répressif (Procureur, Juge d'Instruction, JLD) et par le Préfet de Police, le Juge administratif, la CNIL, conseil national du numérique, etc. pour ce qui concerne l'aspect préventif.

Le gain obtenu repose essentiellement sur l'aspect humain. Le nombre d'effectif, l'économie des ressources humaines, mais également sur les moyens matériels comme le parc automobile.

Les logiciels d'analyse sont des outils d'aide à l'enquête pour un gain de temps considérable et de limiter le nombre d'exploitants.

ASSOCIATION NATIONALE DE LA VIDÉOPROTECTION

Mission relative aux nouvelles technologies dans le domaine de la sécurité

Apports attendus de ces technologies et garanties à mettre en place

Rapport de l'AN2V à l'attention de M. Jean-Michel MIS, Député de la Loire,

Contacts AN2V :

- Dominique Legrand – Président AN2V – dl@an2v.org – 06 07 86 07 68
- Rémi Fargette – Directeur Général AN2V – rf@an2v.org – 06 28 45 04 27

ASSOCIATION NATIONALE DE LA VIDÉOPROTECTION

Table des matières

I. Introduction 3

II. Donner un cadre juridique unique à la vidéosurveillance - vidéoprotection, prenant en compte le droit européen sur la protection des données personnelles. 4

III. Donner un cadre juridique à l'audio, utilisé dans des dispositifs de sûreté 7

IV. Donner un cadre juridique aux métadonnées. 9

V. Encadrer l'utilisation de la lecture automatisée de plaques d'immatriculation. 10

VI. Favoriser l'expérimentation dans le domaine de l'intelligence artificielle appliquée à la sûreté. 11

VII. Donner un statut aux agents publics exploitant les dispositifs de vidéoprotection. .12

VIII. Permettre le stockage distant des données 14

IX. Contributions directes de nos entreprises membres..... 15

I. Introduction

Le Premier ministre a confié à **M. Jean-Michel MIS, Député de la Loire,** une mission relative aux nouvelles technologies dans le domaine de la sécurité afin de déterminer les apports attendus de ces technologies tout en veillant aux garanties à mettre en place pour encadrer strictement leur usage. Celui-ci a souhaité recueillir les attentes de l'association nationale de la vidéoprotection.

Il convient de rappeler que notre association avait déjà été entendue le mardi 27 octobre par M^{me} Alice Thourot et M. Jean-Michel Fauvergue, rapporteurs de la proposition de loi relative à la sécurité globale. Suite à cette audition, et à leur demande, nous avions rédigé une note de synthèse relative aux mesures qui nous paraissaient alors prioritaires au regard de notre expérience de 16 ans dans le domaine des technologies de sûreté.

La « loi pour une sécurité globale préservant les libertés » a été publiée ce mercredi 26 mai au Journal Officiel. Elle a permis de répondre à certaines attentes de nos membres. Toutefois, ce texte est très en retrait par rapport aux besoins de la profession.

Nos attentes prioritaires sont les suivantes :

1. **Donner un cadre juridique unique à la vidéosurveillance - vidéoprotection, prenant en compte le droit européen sur la protection des données personnelles.**
2. **Cette loi doit impérativement intégrer la composante « audio » des dispositifs, en donnant un cadre juridique à l'analyse des signatures sonores.**
3. **Donner un cadre juridique aux métadonnées.**
4. **Développer l'utilisation de la lecture automatisée de plaques d'immatriculation, en lui donnant un cadre juridique spécifique.**
5. **Favoriser l'expérimentation dans le domaine de l'intelligence artificielle appliquée à la sûreté.**
6. **Donner un statut aux agents publics exploitant les dispositifs de vidéoprotection.**
7. **Permettre le stockage distant des données (Cloud)**

Cette note repose sur les contributions de nos **140 membres industriels fournissant des produits ou des services dans le domaine de la sûreté**. A ce sujet, il faut noter que ce sont les industriels travaillant sur les technologies les plus avancées (analyse de son, intelligence artificielle) qui se sont le plus fortement mobilisés, preuve que ces sujets nécessitent un encadrement juridique qui permettra à des PME françaises, dynamiques et innovantes, de se développer et de donner vie au plan de relance et de relocalisation.

L'AN2V se tient à la disposition du législateur pour contribuer à l'évolution de ce cadre juridique.

II. Donner un cadre juridique unique à la vidéosurveillance - vidéoprotection, prenant en compte le droit européen sur la protection des données personnelles.

Constat :

Les professionnels concernés (utilisateurs, fournisseurs et mêmes les institutionnels) méconnaissent le régime juridique de la vidéosurveillance, de la vidéoprotection et de la protection des données personnelles. Cela est étroitement lié à une réglementation est complexe et inadaptée. Voici un exposé de la situation actuelle.

Il existe actuellement **deux régimes juridiques** concernant l'installation de caméras de sûreté :

- **Code de sécurité intérieure** : pour les caméras installées sur la voie publique et dans les lieux ouverts au public (vidéoprotection).
- **La loi de 1978** mise en conformité avec le pack européen sur la protection des données : elle réglemente les caméras installées dans des lieux privés (vidéosurveillance).

Le fondement de cette répartition est l'article ***L251-1 du CSI :***

« Les enregistrements visuels de vidéoprotection répondant aux conditions fixées aux articles L. 251-2 et L. 251-3 sont soumis aux dispositions du présent titre, à l'exclusion de ceux qui sont utilisés dans des traitements automatisés ou contenus dans des fichiers structurés selon des critères permettant ***d'identifier, directement ou indirectement, des personnes physiques****, qui sont soumis à la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. »*

La réglementation de la vidéoprotection, issue la LOPSI de 1995 puis intégrée au Code de la sécurité intérieure, repose donc sur le principe que l'image n'est pas à elle seule une donnée personnelle. Il faut un traitement spécifique pour le système relève de la loi de 1978.

Mais cette analyse n'est pas celle proposée par la CNIL, qui se base sur les textes européens.

La CNIL, s'appuyant notamment sur le paquet européen, considère en effet que l'image d'une personne est une donnée personnelle puisqu'elle peut permettre « *d'identifier, directement ou indirectement, des personnes physiques ».* De ce fait, si l'on suit cette analyse, l'ensemble des systèmes de vidéoprotection / vidéosurveillance sont des traitements de données à caractère personnel.

Loi de 1978 - Article 2 – al 2 :
« Constitue un fichier de données à caractère personnel tout ensemble structuré de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique. »

Cette analyse n'est visiblement pas partagée par le ministère de l'Intérieur. Il suffit de consulter les sites de la CNIL et du ministère pour comprendre la différence d'analyse. A noter que la CNIL a fait un énorme effort d'information par le biais notamment de fiches pratiques.

De fait, la CNIL revendique aujourd'hui des compétences sur les systèmes de vidéoprotection qui vont au-delà de ce qui est prévu par le CSI, en exigeant une mise en conformité des systèmes au droit européen. La plupart des exploitants prennent d'ailleurs en compte ces textes dans leur organisation.

A ce problème de fond s'ajoutent d'autres difficultés :

- Les commissions départementales de vidéoprotection ont chacune leur propre interprétation des textes. Nos professionnels constatent des règles différentes d'un département à l'autre. Il semble ne pas y avoir de doctrine nationale, de coordination.

- La commission nationale de la vidéoprotection, créée par le Code de la sécurité intérieure (CSI), a disparu sans explication…

- La plupart des exploitants ont à la fois des caméras de vidéoprotection et de vidéosurveillance en fonction des espaces traités. Un commerce utilise de la vidéoprotection dans l'espace ouvert au client, et de la vidéosurveillance dans les zones réservées au personnel.

- Des textes autres que ceux déjà cités encadrent directement ou indirectement la vidéosurveillance-vidéoprotection : code du travail, textes spécifiques à certaines activités (stades, casinos…).

Dans ce contexte, utilisateurs et fournisseurs sont désorientés. Même les juristes professionnels ont des analyses contradictoires sur les textes !

Les professionnels de la sûreté méconnaissent trop souvent la réglementation, en particulier les textes sur les données personnelles. Ils ont une responsabilité et doivent progresser dans ce domaine, en proposant aussi plus de garanties dans leurs solutions, en renforçant les protections, en mettant en œuvre des études d'impact. Il faut limiter les risques pour les clients.

Nous considérons :

- Que la loi de 1978 n'est pas le bon support juridique pour les technologies de sûreté. Ce texte ne peut pas remplacer les dispositions du CSI. Il n'est pas dédié à nos dispositifs, il est difficilement compréhensible pour les professionnels et beaucoup trop générique.
- Que les textes du CSI relatifs à la vidéoprotection ne sont plus adaptés et doivent être mis en conformité avec le droit européen.

Proposition AN2V :

AN2V demande donc un texte unique et clair, dédié à tous les systèmes vidéo (et audio) de sûreté :

- Caméras installées sur la voie publique (vidéoprotection),
- Caméras installées dans des établissements publics ou privés ouverts au public (vidéoprotection),
- Caméras embarquées sur des robots,
- Caméras embarquées sur des aéronefs,
- Caméras embarquées par les agents des forces de sécurité au sens large, ou sur leurs véhicules,

Et plus largement, nous souhaitons un cadre juridique pour tous les dispositifs de sûreté : systèmes de détection de signatures sonores, contrôles d'accès (biométrie), intelligence artificielle, reconnaissance faciale…

Il faut rappeler ici que la CNIL, souvent critiquée par la profession pour ses prises de position, est la première à demander au législateur de poser un cadre juridique clair.

Important : une nécessaire prise en compte des réticences de nos concitoyens.

Lors de nos discussions avec les entreprises membres, nous avons longuement évoqué le contexte actuel et la perception par nos concitoyens des technologies de sûreté. Voici une synthèse de ces discussions…

On constate actuellement une crispation de l'opinion publique sur les technologies de sûreté. Cela a été constaté dans les débats autour de la loi sécurité globale. Les médias mélangent tout, il n'y a pas de nuance. Le risque est qu'une loi mal présentée soit rejetée en bloc.

Pour répondre à cela nous estimons qu'il faut :

- Définir des finalités d'utilisation précises et limitées,
- Prévoir des conditions d'exploitation strictes,
- Informer de manière claire et transparente,
- Proposer des alternatives lorsque cela est possible.

Bref, donner un cadre conforme aux grands principes du RGPD. La France est un pays de libertés, et aussi un pays contestataire. Il faut avancer avec précaution, en partant de cas concrets, de dispositifs Éthiques compréhensibles par la population.

Par ailleurs, la responsabilité de l'institution judiciaire dans les problèmes de délinquance est souvent évoquée. Ce sont souvent les mêmes individus « *défavorablement connus des services de police* » qui sont arrêtés plusieurs fois « grâce » aux technologies de sûreté.

Une remise en question des politiques pénales et carcérales nous paraît indispensable et complémentaire à un élargissement de l'utilisation de la technologie.

III. Donner un cadre juridique à l'audio, utilisé dans des dispositifs de sûreté

Constat :

L'analyse de situations nécessite de recueillir différentes données permettant à l'opérateur d'un système de comprendre ce qui est en train de se produire. Aujourd'hui, il peut voir grâce aux caméras mais il ne peut pas entendre. Or, il existe des solutions technologiques qui permettent de détecter des signatures sonores significatives. Ces capteurs sonores permettent de réaliser des détections précoces, de mieux localiser les événements.

Pourtant, le capteur ne renvoie qu'une alerte et pas de son. Il ne s'agit pas de capter tous les sons sans discernement, d'enregistrer des conversations. Comme pour le LAPI, une utilisation de l'audio est faite officieusement, par exemple dans les transports publics. Et cela constitue un apport très important pour les services de police.

Cette technologie de dispose d'aucun fondement juridique et son utilisation est bloquée par la CNIL.

Contribution d'une PME française interrogée :

- ⇨ **SENSIVIC**

« Les "innovations" technologiques abordées concernent les caméras sur les drones, et les bodycams. On reste uniquement sur l'image et ce qui porte l'image. Rien sur les technologies connexes telles que celle que nous développons (détection automatique d'anormalité sonore).

C'est justement notre point d'achoppement avec la CNIL, qui stipule dans le courrier qui nous a été adressé : "une base législative spécifique apparait nécessaire pour la mise en œuvre de tels dispositifs sur la voie publique et dans les lieux ouverts au public".

Bref, je pense qu'un texte de loi relatif à la Sécurité Globale devrait porter non seulement sur la vidéoprotection mais également sur les technologies émergentes, telles que la détection des anormalités sonores (mais il y en a certainement d'autres) afin de les rendre possibles, en les encadrant.

Ce que voulait mettre en place Serenicity à St-Étienne pouvait effectivement être sujet à caution - le son semblait être transporté jusqu'à un serveur et était donc potentiellement "piratable". Les américains de Shottspotter vont certainement aborder l'Europe prochainement avec une technologie de détection de coups de feu très invasive. Nos autres concurrents étrangers utilisent des techniques souvent contraires au respect des vies privées.

La détection des anormalités sonores est en train d'entrer dans la sécurité, c'est inéluctable. La loi doit l'encadrer. »

Proposition AN2V :

- Création d'un cadre juridique spécifique pour cette technologie dans le CSI.
- Idéalement, ces dispositions seraient intégrées à une nouvelle loi globale « **audiovidéoprotection** »

Il ne s'agit absolument pas de capter des conversations. Aucune conservation de son n'est faite pas le système. Sur ce sujet, il y a donc un réel travail de pédagogie à entreprendre, car de fortes oppositions peuvent se faire entendre, fondées sur de mauvaises informations.

Outre la position de Sensivic, très respectueuse des libertés individuelles, et "assez simple à proposer", une deuxième marche plus ambitieuse pourrait être étudiée avec l'idée d'enregistrer l'audio avec l'image, comme une métadonnée de l'image (comme sur une bande VHS), moyennant un cryptage solide à la source, où les données ne pourraient être décryptées/lues que par les forces judicaires par exemple. L'audio peut dans certains cas critiques apporter une information précieuse pour l'élucidation.
Nous attirons l'attention du législateur sur le fait que toutes les caméras récentes peuvent disposer d'une capture audio, et que l'image telle que pratiquée à ce jour ne préserve pas l'anonymat des discussions puisque certains savent lire sur les lèvres !

IV. Donner un cadre juridique aux métadonnées.

Constat :

La réglementation actuelle ne prend pas en compte une évolution technique des caméras (et d'autres technologies) qui est passée presque inaperçue : **les métadonnées**.

Les métadonnées sont des informations rattachées à l'image, qui permettent de la décrire et de réaliser des recherches par critères.

Problèmes :

Ces métadonnées sont des données, or le code de sécurité intérieure ne parle que d'images. Le silence actuel sur ce sujet arrange plutôt les professionnels (personne n'en parle) mais il nous semble important de ne pas laisser perdurer ce flou.

Il faut distinguer les métadonnées à caractère personnel ou non.

Il faut définir des finalités permettant l'usage des métadonnées.

Cela renforce encore la nécessité de mettre en conformité le CSI avec les textes régissant les données personnelles.

Proposition AN2V :

- Intégrer les métadonnées dans la réglementation intérieure. Attention : ce ne sont pas des données personnelles et cette avancée technologique est bénéfique.
- Il ne s'agit donc pas « d'interdire » mais simplement d'encadrer une technologie présente sur quasiment toutes les caméras du marché.
- La réglementation pourrait ainsi prévoir une durée de conservation pour ces données.

V. Encadrer l'utilisation de la lecture automatisée de plaques d'immatriculation.

Constat :

La lecture automatisée de plaques d'immatriculation est un outil fiable, performant, assez peu coûteux, et qui pourrait être d'une redoutable efficacité dans le travail quotidien des services de sécurité intérieure.

Des évènements tragiques ont démontré la difficulté à retrouver un véhicule recherché, alors même que sa plaque est connue et que ce véhicule circule dans des zones couvertes par la vidéoprotection. On préfère encore aujourd'hui faire décoller des hélicoptères et déployer des barrages routiers plutôt que d'exploiter des solutions de type LAPI…

L'usage du LAPI est réglementé par la loi de 1978, sur la base de l'article L251-1 du CSI

CSI - Article L251-1 : Les enregistrements visuels de vidéoprotection répondant aux conditions fixées aux articles L. 251-2 et L. 251-3 sont soumis aux dispositions du présent titre, à l'exclusion de ceux qui sont utilisés dans des traitements automatisés ou contenus dans des fichiers structurés selon des critères permettant d'identifier, directement ou indirectement, des personnes physiques, qui sont soumis à la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Problèmes :

La CNIL a une vision très restrictive de l'usage du LAPI. Le Maire peut installer du LAPI à ses frais, mais ne peut pas l'utiliser : réservé aux policiers et gendarmes. Le LAPI ne peut être utilisé que pour du stationnement réglementé (ex - stationnement **payant**). La CNIL a récemment dénoncé l'utilisation du LAPI sur 4 communes à des fins de verbalisation de stationnements **gênants**…

Des initiatives sont menées par la DGGN pour créer un réseau national des capteurs LAPI mais ce projet avance lentement. Il n'aura jamais la couverture de toutes les caméras déployées sur les communes !

Les utilisateurs sont perdus : certains utilisent du LAPI illégalement, d'autres renoncent à cette technologie. La réglementation actuelle (loi de 1978) ne traite pas directement cet outil. Les professionnels ne s'accordent même pas sur la définition de la LAPI : simple visualisation ou constitution de base de données de plaques ? Uniquement la plaque, ou d'autres éléments d'identification ? (type de véhicule, marque, couleur, combien de passagers à l'intérieur du véhicule…)

Proposition AN2V :

- Création d'un réseau LAPI national, intégrant l'ensemble des capteurs publics et privés, couplé au fichier des véhicules recherchés. Mis en place par certaines communes à l'échelon local, sous contrôle de la police nationale, cette technologie serait particulièrement efficace.
- Création d'un cadre juridique spécifique pour cette technologie dans le CSI.
- Ce cadre doit prendre en compte tous les usages possibles, et notamment tous les textes liés à l'environnement (co-voiturage, sites propres, zones à faible émission).

VI. Favoriser l'expérimentation dans le domaine de l'intelligence artificielle appliquée à la sûreté.

Constat :

La vie réelle est différente de l'expérimentation en laboratoire. Il faut pouvoir utiliser des données réelles et sensibles (un coup de feu sur l'espace public par exemple). Pour reconnaître un événement, il faut que le système ait été confronté à cet événement. Les propriétaires de données doivent pouvoir les partager avec des entreprises françaises et des chercheurs.

Il s'agit aussi d'une question de souveraineté. Les entreprises françaises innovantes ne peuvent pas expérimenter en conditions réelles, à la différence de leurs concurrents étrangers. Nos entreprises prennent du retard, qui ne sera bientôt plus rattrapable.

Mutualiser des données permet aussi de « benchmarker », de comparer les performances de différentes solutions sur des données comparables.

Contributions de nos PME françaises interrogées avant notre audition :

⇨ **FOXSTREAM**

- *Depuis 20 ans l'intelligence artificielle a évolué vers ce que l'on appelle aujourd'hui le deep learning (l'apprentissage profond). Le deep learning est de loin beaucoup plus puissant que tout ce qui a été fait depuis 40 ans au niveau de l'intelligence artificielle.*
- *Le deep learning est une technique basée sur l'apprentissage. Le logiciel « apprend », au vu des exemples qui lui sont donnés. Plus le nombre d'exemples donnés au logiciel est important, plus la précision de son « expertise » sera grande.*
- *L'accès aux données pour donner des exemples au logiciel, afin d'affiner les algorithmes est devenu juste **primordial/essentiel/indispensable**.*

La question est donc : Comment des minuscules PMEs comme Foxstream, ou des sociétés plus grandes, peuvent accéder à ces données (data) ?

Ce que nous aimerions, c'est que dans la loi soit inscrit une phrase du type : « Toutes sociétés, à conditions qu'elles soient françaises/européennes et dûment habilitées, peuvent, dans un but de recherche ou de développement de nouveaux produits, et sous condition de l'accord de l'entité, public ou privé, source de ces vidéos, accéder aux vidéos nécessaires à l'élaboration de leurs algorithmes, vidéos qui en dehors de ce contexte ne sont pas public. »

⇨ **VIDETICS**

« Il est important pour nous d'avoir une réglementation sur l'usage de l'analyse vidéo par IA. Il est très compliqué pour nous de déployer nos solutions en France, de par l'absence de réglementation sur l'usage des métadonnées que l'on peut extraire de nos analyses. Je pense sincèrement que nous pouvons apporter des solutions extrêmement précieuses pour les villes sans passer forcément par la reconnaissance faciale. »

Proposition AN2V :

- Création d'un cadre juridique spécifique dans le CSI permettant l'expérimentation de cette technologie à grande échelle, dans un contexte expérimental.
- Dans la perspective de l'organisation de prochains grands événements (JO, CDM Rugby) il faut pouvoir réaliser des déploiements de reconnaissance faciale, et plus largement de solutions utilisant l'IA, distinguer les recherches sur liste blanche et sur liste noire.
- Recourir dans les grands appels d'offres à des solutions proposées par des entreprises françaises serait évidemment un plus.

VII. Donner un statut aux agents publics exploitant les dispositifs de vidéoprotection.

Nous avons jusqu'à présent abordé les technologies. Il faut aussi prendre en compte **les personnels qui exploitent les dispositifs de sûreté**.

Constat :

Les choses sont organisées sur le plan de la sécurité privée : carte professionnelle, formations…

Il en va différemment pour les agents municipaux chargés d'assurer l'exploitation de dispositifs de vidéoprotection et qui n'ont aucun statut. La loi est muette sur ce point. Les élus se réfèrent donc à des statuts non adaptés, et leurs agents manquent de reconnaissance. Ils exercent pourtant un travail nécessitant d'importantes compétences, dans des conditions souvent pénibles (travail en 3x8, vacations longues, WE au travail, compétences requises sur de nouveaux outils comme l'intelligence artificielle…).

Le maire ne pouvant déléguer la surveillance de la voie publique à une entreprise privée (décision du Conseil Constitutionnel de 2011 réaffirmant un principe fondateur de notre Droit). La seule obligation est donc que l'agent soit un agent municipal, et qu'il soit habilité par l'autorisation préfectorale.

De fait, certains maires confient leurs systèmes à des policiers municipaux, d'autres à des ASVP et d'autres encore à des agents administratifs.

Par ailleurs, les opérateurs vidéo réalisent souvent un travail d'investigation pour le compte des services de police et de gendarmerie, sous leur contrôle (relatif). Or, ils effectuent des actes d'investigation qui nécessitent, dans les textes, des compétences judiciaires qu'ils n'ont pas.

L'organisation au quotidien d'un centre superviseur urbain n'est pas encadré par la loi. C'est l'autorisation préfectorale qui fixe les grandes lignes, chaque maire s'organise librement ensuite.

La situation des ASVP et opérateurs vidéo est donc un peu la même que celle des polices municipales avant que des textes ne les encadrent plus étroitement. Le rapport initial de M^{me} Alice Thourot et M. Jean-Michel Fauvergue proposait de donner un statut aux ASVP. Ce point n'a pas été repris dans la proposition de loi et c'est dommage, compte-tenu de l'évolution rapide des effectifs d'ASVP.

Proposition AN2V :

- Création d'un cadre d'emploi spécifique pour les agents municipaux exploitant des technologies de sûreté. Cela pourrait être un statut donné aux ASVP, intégrant la fonction d'opérateur de vidéoprotection.
- Apporter une clarification concernant le statut des opérateurs dans le cadre de systèmes intercommunaux (EPCI ou syndicat mixte). Les EPCI connaissent actuellement des difficultés à faire valider leurs projets intercommunaux par les commissions départementales, lorsque l'EPCI recrute et encadre les opérateurs. C'est pourtant prévu par la loi.

VIII. Permettre le stockage distant des données

Aujourd'hui, le stockage distant des données n'est pas accepté par les commissions départementales dans le cadre de dispositifs de vidéoprotection. Cette interdiction porte aussi bien vers le stockage de données par des opérateurs privés que par des opérateurs publics (Syndicat mixte).

Pourtant, rien de s'y oppose formellement dans notre réglementation : c'est une doctrine. De plus, cette technologie peut permettre des avancées en matière de sécurisation des données, de cyber sécurité.

Contribution d'une entreprise membre AN2V :

⇨ **Eagle eye networks**

Les meilleures pratiques en matière de cybersécurité sont essentielles pour protéger les entreprises, les employés et leurs données. Heureusement, les véritables systèmes sur le cloud intègrent la cybersécurité. La sécurité des ordinateurs et des réseaux vise à protéger la confidentialité, l'intégrité et la disponibilité des systèmes en réseau et des données qu'ils contiennent. Ces trois facteurs sont primordiaux pour les systèmes vidéo, étant donné que la vidéo enregistrée par une caméra peut devenir une preuve juridique essentielle. Cependant, pour la plupart des systèmes vidéo, la connectivité Internet met en danger la confidentialité, l'intégrité et la disponibilité, car la plupart des systèmes ne disposent pas de protections intégrées contre les cyberattaques. Ainsi, de nombreux systèmes vidéo sont sans défense, et les attaques de cybersécurité sont en augmentation.

Lorsqu'un système de vidéosurveillance est connecté à Internet, la cybersécurité doit être entièrement prise en compte par le fournisseur de services sur le cloud, qui doit fournir à l'utilisateur final des fonctions de connexion sécurisée, des autorisations d'accès et des pistes d'audit si nécessaire. La cybersécurité du système doit inclure :

• Cryptage sécurisé des vidéos mises en mémoire tampon et enregistrées localement,
• Surveillance constante contre les menaces,
• Pas de ports ouverts ni de pare-feu sur site,
• Pas de logiciel sur site à patcher (les mises à jour sont automatiques),
• Stockage triple redondance pour les événements,
• Authentification à deux facteurs.

Les données stockées dans le Cloud ne sont accessibles que par l'utilisateur final et ne peuvent être utilisées par l'hébergeur (ni Cloud Act), tant qu'elles sont enregistrées dans un Cloud privé dédié à la vidéosurveillance.

Proposition AN2V :

- A minima, il conviendrait de donner la possibilité pour les communes de faire appel à des entreprises souveraines labellisées pour le stockage de leurs données sensibles.
- Plus largement, il faudrait ouvrir ce marché à des entreprises privées étrangères, moyennant un stockage sur le territoire national, selon des critères de sécurité à définir.

IX. Contributions directes de nos entreprises membres

Certaines de nos entreprises ont souhaité vous transmettre leurs remarques. Nous les ajoutons à ce rapport, sans aucun filtre.

⇨ **SENSIVIC**

La société SENSIVIC a souhaité répondre à votre questionnaire :

La notion de « technologies de sécurité » est large. Quelles sont les principales selon vous ? [Par exemple : traitement des données (textuelles, images, sonores), biométrie, mobilité.]
Le point de départ de la sécurité est d'abord la compréhension de la scène à laquelle on est confronté pour évaluer les meilleures contre-mesures à appliquer. Une scène peut comprendre :

- des objets (armes par destination ou par usage, cibles de malveillance…)
- des véhicules
- des personnes physiques (victimes ou agresseurs)
- des animaux (victimes ou agresseurs)
- …

L'analyse de la scène suppose d'abord un recueil, par tous moyens, le plus complet possible, des données caractérisant tous les éléments de la scène.
Si la caméra est un capteur bien connu et largement utilisé, il existe d'autres capteurs qui peuvent être indispensables (radars etc), le principal est le capteur de sons.
Le piège consisterait à vouloir recueillir les données sonores, les transmettre en l'état pour traitement au centre d'analyse. Ce cas de figure conduirait à un surdimensionnement du réseau, au surdimensionnement des serveurs, à l'écoute et à la transmission indifférenciées, ouvrant le risque d'intrusion dans la vie privée.
Or pour exploiter les informations extraites du son, seules les données les plus pertinentes méritent d'être transmises. Les capteurs ou détecteurs effectuent alors à la source les traitements nécessaires. Par exemple un détecteur n'a pas besoin de transmettre les données qui ont permis d'élaborer la décision qui, elle, est transmise au centre de supervision.

Pour quelles finalités ? [Par exemple : détection de situations, analyse prédictive, suivi des personnes.]

- Détecter et réagir en temps réel : dans un grand évènement, en cas de crise, la détection/réaction doit être en temps réel pour éviter d'être débordé par une situation : coup de feu, cris de panique, bris de vitre, vandalisme sur le mobilier ou les distributeurs, collision, tentatives d'intrusion sur les zones moins surveillées, détection des comportements agressifs (agressions verbales)…
- Fiabiliser l'analyse : meilleure évaluation du risque par la combinaison de différentes technologies de captation, pouvant aller jusqu'à la généralisation automatique de la levée de doute

Pensez-vous qu'elles permettraient d'anticiper les évolutions des missions de sécurité dans les 10 à 20 ans à venir ? Comment voyez-vous ces évolutions ? Sur chaque technologie prioritaire évoquée, quel est l'état de développement de l'industrie française ? Que lui manque-t-il pour se perfectionner ?

Dans le domaine du son pour la sécurité, les technologies sont rares. La France a une offre très compétitive.

L'expérimentation, le développement et l'amélioration de telles technologies nécessitent l'accès (sous contrôle) à des sites réels, donc à l'espace public. La règlementation française rend ces expérimentations très difficiles à mettre en place. Ces difficultés nous pénalisent par rapport à nos concurrents étrangers (américains par exemple)

Comment les configurations techniques peuvent-elles concilier une utilisation de ces technologies et des garanties pour les libertés (protection des données, contrôles automatisés, etc.) ?

Dans le cas des données sonores, l'exigence est l'anonymisation des données : le traitement du son doit être effectué dès la capture, sur site, dans le détecteur lui-même. Le système doit garantir qu'aucune donnée fournie par le détecteur/capteur ne peut permettre de remonter à sa source.

Les cadres d'expérimentation sont souvent mis en avant pour le perfectionnement de ces technologies. Quelles sont selon vous les priorités ? Quels seraient les contours de ces cadres ? A quelles fins ?

Sous un contrôle à définir, une expérimentation sur site doit pouvoir permettre au moins temporairement de traiter des données non encore anonymisées. Ne serait-ce que pour mettre au point la technique d'anonymisation finalement mise en œuvre.

Au-delà de cette précaution préliminaire la mise au point et le perfectionnement d'un dispositif nécessite des collectes de données en volume suffisant. Les expérimentations doivent donc pouvoir être conduites pendant des durées à apprécier en concertation entre l'industriel et la collectivité locale qui autorise et supervise l'expérimentation.

⇨ **BOSCH**

La société BOSCH nous a envoyé une contribution libre

Pour légiférer sur l'outil il faut avant tout se poser la question des finalités et de qui utilise (de manière large ou très précise quand c'est possible), mais catégoriser est important sans pour autant laisser trop de flou… Flou = prise de position CNIL

En face de cela, on doit identifier les moyens proportionnés :

Mettre d'abord au premier plan l'information "classique"
- Les différents rôles de la caméra et du capteur sonore, leur complémentarité ou pas. En cas de prise sonore, il ne faut peut-être pas pouvoir identifier avec la vidéo…
- Les classer, et partir de là pour définir le côté légal de la sécurité

Au-delà de la donnée classique il y a les données parallèles :
- Métadonnées : géolocalisation, dimension, vitesse, genre, etc…,
- La convergence des données : téléphone, position, etc… (le son seul versus le son + la vidéo par exemple)

Il faut définir quelles données entrent dans le cadre du RGPD ou non, pour clarifier ce que je peux faire simplement et ce qui nécessite des efforts (ou pas d'effort si je classifie aussi des finalités par rapport à des typologies de sites).

De là on peut identifier les limites à fixer (qui collecte les données, qui peut les exploiter, les cas de multi-utilisations : [x] a besoin du numéro de plaque, [y] a besoin de voir s'il y a un piéton sur la route ou un contre sens) :
- Une caméra peut avoir divers usages, divers utilisateurs, du privé vers le public ou l'inverse ou inter-public
- En respectant la législation Européenne (d'où l'intérêt de définir clairement quelles métadonnées ou autres données sont dans un cadre restrictif, et lesquelles ne le sont pas pour libérer l'utilisation (et éventuellement la notion d'évaluation, etc…)
- On peut aussi à partir de là mettre face à face le bénéfice (j'atteints mon objectif) et le prix en terme de données, de risque et ensuite trouver des compromis quand c'est possible (capteur sonore ok si pas identification avec un système vidéo sauf si site classé x, y ou z, etc….)

Par ailleurs la loi doit adresser la problématique de la mise en place notamment via la nécessité de niveaux de certifications des sociétés mettant en place des systèmes qui sont ou pourraient permettre une génération de données sensibles (liés au RGPD) y compris pour un système dont la finalité n'exploiterait pas ces données sensibles

Enfin sur le consentement, pour rebondir sur les outils pour les bus => J'achète mon ticket je coche "je consens", cela veut dire que la loi ne doit pas traiter que l'outil mais peut aussi adresser des problématiques de l'usager/utilisateur

Note: La loi devrait de manière globale être articulée ainsi :
- Je légifère sur la sécurité (outils, finalités, utilisateurs dans le cadre strict de la sécurité)
- Un volet technologique (c'est le sens de l'innovation actuel chez nous les industriels), sur des produits et systèmes capables de traiter d'autres finalités que la sécurité ou de l'étendre
- Ainsi je traite aussi le cas de figure où le produit de sécurité est utiliser en dehors (totalement) ou en complément du cadre de la sécurité (ex. Comptage dans le Bus donné par un participant)
La loi doit comprendre et laisser libre cours à l'innovation (peut être en élargissant au-delà de la zone France, en proposant un modèle intéressant pour des états avec les mêmes problématiques au sein de l'EU)

⇨ **WABTEC / FAIVELEY**

La société WABTEC - FAIVELEY nous a envoyé une contribution libre

La problématique de l'utilisation de l'image de personnes captée par une caméra dans un espace fréquenté par le public est un point fondamental et bloquant pour permettre de progresser significativement dans le contexte d'innovation. Je peux témoigner d'une quantité importante que nous discutons avec les opérateurs publics (RATP, SNCF, KEOLIS, TRANSDEV, …), mais que nous gardons dans les cartons faute de pouvoir les déployer.

Le point de blocage (tel que nous l'avons compris) réside dans le point essentiel du RGPD de ne permettre la capture d'une image qu'à la condition préalablement du consentement explicite de l'usager quel que soit le traitement ou les protections pouvant être mises en œuvre pour garantir la préservation des données personnelles. Aujourd'hui seules quelques finalités couvertes par le CSI, comme la vidéoprotection échappe à cette règle en autorisant la capture de ces images (moyennant ensuite de respecter les autres règles d'exploitation).

En l'espèce, le cas survenu sur l'expérimentation du comptage des masques en mai 2020 est un cas d'école et le retour de la CNIL éclaire bien cette problématique (voir PJ).

Le gouvernement a répondu dans l'urgence à travers le décret du 11 mars 2021 en limitant le cadre et la durée d'application pour je pense calmer le jeu.

Une avancée notable serait de pouvoir par décret se libérer de cette contrainte en offrant tout un jeu de garantie visant à débarrasser l'image (de manière irréversible) de toute donnée à caractère personnel, offrant ainsi l'ouverture à toute finalité autre que celles du CSI, dans l'application des lois intégrant le RGPD.

Ce problème vient de la confusion (que j'ai pu identifier en séance) entre le système lui-même et la finalité. Nous voyons de plus arriver des systèmes capables de supporter plusieurs finalités (partage des ressources).

Ce blocage sur l'image est d'autant plus remarquable que par ailleurs la CNIL se positionne (dans le cadre du comptage) vis-à-vis d'autre technologie (téléphone portable) – La capture des @MAC ou @BT est un traitement sur des données à caractère personnel quasiment aussi sensible que l'image d'une personne. À ce titre, il est intéressant de comparer 2 positions de la CNIL : la première sur les caméras intelligentes, l'autre sur les solutions de comptage. Il semble que dans le second cas (bien qu'applicable lui aussi dans le contexte RGPD), la nécessité d'autorisation préalable ne soit pas aussi évidente. Les mesures prises dans le second cas pourraient être appliquées à celui de l'image procurant le même niveau de protection.

La mesure d'audience à l'aide des téléphones

https://www.cnil.fr/fr/dispositifs-de-mesure-daudience-et-de-frequentation-dans-des-espaces-accessibles-au-public-la-cnil

Les caméras intelligentes

https://www.cnil.fr/fr/la-cnil-appelle-la-vigilance-sur-lutilisation-des-cameras-dites-intelligentes-et-des-cameras

Il en ressort que plus qu'une finalité, il devrait être possible moyennant de débarrasser dans des conditions convenues l'information (métadonnée) de toute donnée à caractère personnel son traitement pourrait être réalisé en dehors de tout contexte RGPD. Et ceci pourrait être applicable quelle que soit la nature de l'information image, téléphone, son …

⇨ **AUTRES ENTREPRISES**

D'autres remarques intéressantes ont été formulées que nous ajoutons ici pour information :

Impossibilité de modifier la finalité d'un dispositif
Lorsqu'une caméra est installée en s'appuyant sur une finalité, on ne peut l'utiliser pour répondre à une autre finalité. On ne peut par exemple pas faire du comptage pour une caméra autorisée à des fins de prévention des atteintes aux biens et aux personnes. De ce fait, on se prive de nombreux usages basiques très utiles (Smart city).
Exemple des bus : très bien équipés avec des systèmes très performants mais sous utilisés.
On confond système et usage.

Le problème du consentement
Dans beaucoup de cas d'usage, le recueil du consentement des personnes est impossible à mettre en œuvre. Et proposer une alternative n'est souvent pas possible.

Le rapport bénéfice -risque
Cette notion pourrait être un critère intéressant en matière de sûreté.
En incendie tout est normalisé et réglementé. En sûreté ce n'est pas le cas, alors que les risques sont tout aussi élevés.

La CNIL
Souvent à l'origine de nombreux blocages de nouvelles technologies.
Elle se plaint d'une absence de texte pour réglementer les nouvelles technologies et sollicite le législateur. En l'absence de textes spécifiques elle s'appuie sur les textes relatifs à la protection des données à caractère personnel.
La CNIL semble beaucoup moins ouverte au dialogue et à l'expérimentation qu'il y a quelques années.

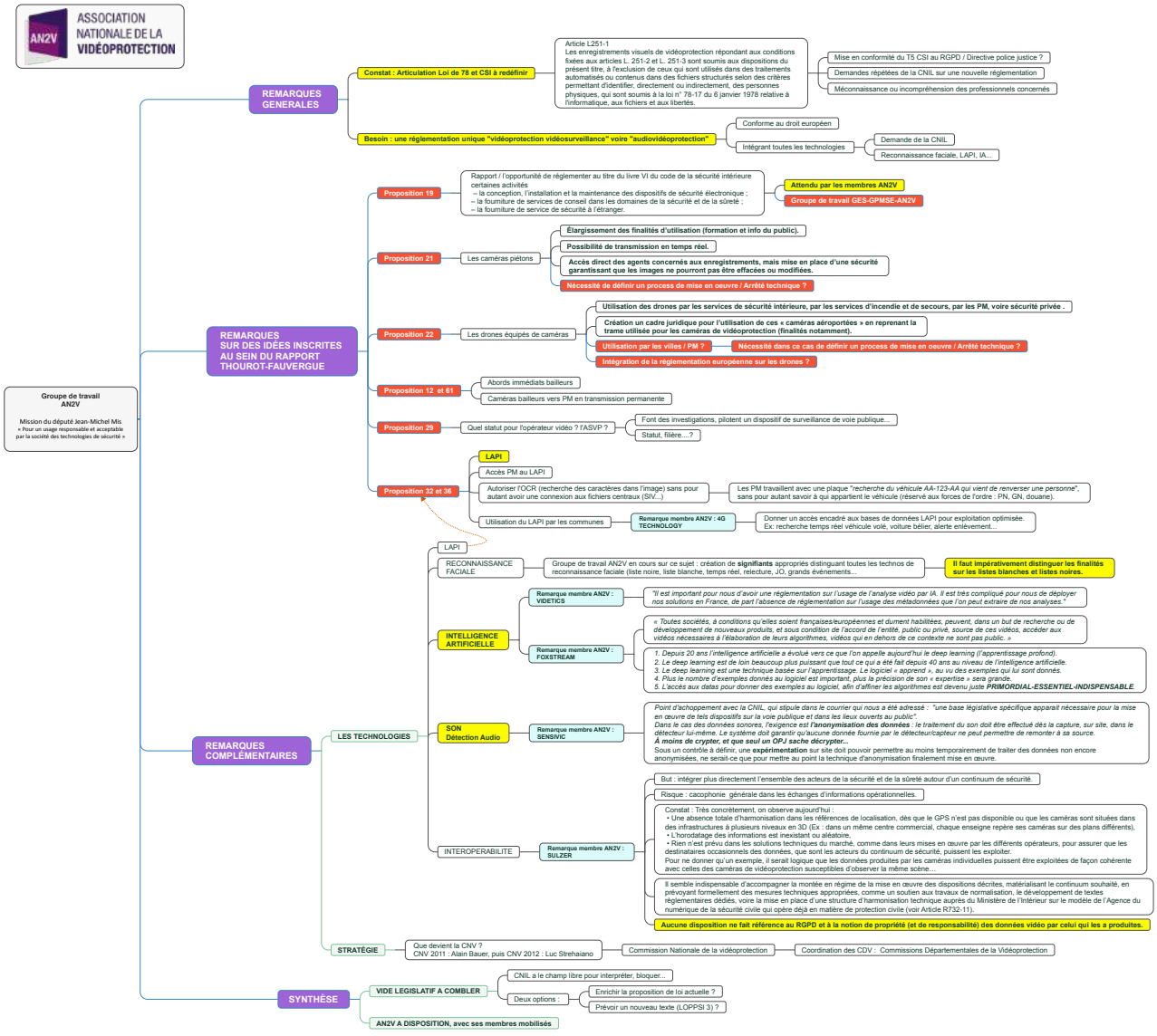
Sur l'ambition d'une loi sur les technologies de sûreté :
Deux approches s'opposent :

- Forcer les lignes en étant très ambitieux, quitte à crisper les opposants aux technologies et le institutionnels concernés (CNIL, Conseil constitutionnel…).
- Avoir une approche minimaliste pour être sûr que le texte ne soit pas censuré.

Quoi qu'il en soit tous les participants s'accordent sur le fait qu'il faut une loi pour de l'interdiction en l'absence de textes qui prévaut actuellement : « la reconnaissance faciale est interdite, la captation audio est interdite… » …

Les enjeux sont importants avec de prochains grands rendez-vous en France : coupe du monde rugby, JO…

Géolocalisation 3D
Il n'existe pas aujourd'hui de solution pour dire où l'on se trouve en 3 dimensions. Possible en 2D via le GPS. Il faut donc définir une méthode commune pour décrire des lieux. Les plans de la RATP ne sont pas ceux de la SNCF par exemple. Il faut une géolocalisation intérieure / extérieure en 3D pour obtenir un moyen unique et partagé permettant de définir où l'on se trouve.


ASSOCIATION NATIONALE DE LA VIDÉOPROTECTION
AN2V
Groupe de travail AN2V
Mission du député Jean-Michel Mis « Pour un usage responsable et acceptable par la société des technologies de sécurité »
REMARQUES GENERALES
Constat : Articulation Loi de 78 et CSI à redéfinir
Article L251-1
Les enregistrements visuels de vidéoprotection répondant aux conditions fixées aux articles L. 251-2 et L. 251-3 sont soumis aux dispositions du présent titre, à l'exclusion de ceux qui sont utilisés dans des traitements automatisés ou contenus dans des fichiers structurés selon des critères permettant d'identifier, directement ou indirectement, des personnes physiques, qui sont soumis à la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
Mise en conformité du T5 CSI au RGPD / Directive police justice ?
Demandes répétées de la CNIL sur une nouvelle réglementation
Méconnaissance ou incompréhension des professionnels concernés
Besoin : une réglementation unique "vidéoprotection vidéosurveillance" voire "audiovidéoprotection"
Conforme au droit européen
Intégrant toutes les technologies
Demande de la CNIL
Reconnaissance faciale, LAPI, IA...
REMARQUES SUR DES IDÉES INSCRITES AU SEIN DU RAPPORT THOUROT-FAUVERGUE
Proposition 19
Rapport / l'opportunité de réglementer au titre du livre VI du code de la sécurité intérieure certaines activités
– la conception, l'installation et la maintenance des dispositifs de sécurité électronique ;
– la fourniture de services de conseil dans les domaines de la sécurité et de la sûreté ;
– la fourniture de service de sécurité à l'étranger.
Attendu par les membres AN2V
Groupe de travail GES-GPMSE-AN2V
Proposition 21
Les caméras piétons
Élargissement des finalités d'utilisation (formation et info du public).
Possibilité de transmission en temps réel.
Accès direct des agents concernés aux enregistrements, mais mise en place d'une sécurité garantissant que les images ne pourront pas être effacées ou modifiées.
Nécessité de définir un process de mise en oeuvre / Arrêté technique ?
Proposition 22
Les drones équipés de caméras
Utilisation des drones par les services de sécurité intérieure, par les services d'incendie et de secours, par les PM, voire sécurité privée .
Création un cadre juridique pour l'utilisation de ces « caméras aéroportées » en reprenant la trame utilisée pour les caméras de vidéoprotection (finalités notamment).
Utilisation par les villes / PM ?
Nécessité dans ce cas de définir un process de mise en oeuvre / Arrêté technique ?
Intégration de la réglementation européenne sur les drones ?
Proposition 12 et 61
Abords immédiats bailleurs
Caméras bailleurs vers PM en transmission permanente
Proposition 29
Quel statut pour l'opérateur vidéo ? l'ASVP ?
Font des investigations, pilotent un dispositif de surveillance de voie publique...
Statut, filière...?
Proposition 32 et 36
LAPI
Accès PM au LAPI
Autoriser l'OCR (recherche des caractères dans l'image) sans pour autant avoir une connexion aux fichiers centraux (SIV...)
Les PM travaillent avec une plaque "recherche du véhicule AA-123-AA qui vient de renverser une personne", sans pour autant savoir à qui appartient le véhicule (réservé aux forces de l'ordre : PN, GN, douane).
Utilisation du LAPI par les communes
Remarque membre AN2V : 4G TECHNOLOGY
Donner un accès encadré aux bases de données LAPI pour exploitation optimisée.
Ex: recherche temps réel véhicule volé, voiture bélier, alerte enlèvement...
REMARQUES COMPLÉMENTAIRES
LES TECHNOLOGIES
LAPI
RECONNAISSANCE FACIALE
Groupe de travail AN2V en cours sur ce sujet : création de signifiants appropriés distinguant toutes les technos de reconnaissance faciale (liste noire, liste blanche, temps réel, relecture, JO, grands évènements...
Il faut impérativement distinguer les finalités sur les listes blanches et listes noires.
INTELLIGENCE ARTIFICIELLE
Remarque membre AN2V : VIDETICS
"Il est important pour nous d'avoir une réglementation sur l'usage de l'analyse vidéo par IA. Il est très compliqué pour nous de déployer nos solutions en France, de part l'absence de réglementation sur l'usage des métadonnées que l'on peut extraire de nos analyses."
Remarque membre AN2V : FOXSTREAM
« Toutes sociétés, à conditions qu'elles soient françaises/européennes et dument habilitées, peuvent, dans un but de recherche ou de développement de nouveaux produits, et sous condition de l'accord de l'entité, public ou privé, source de ces vidéos, accéder aux vidéos nécessaires à l'élaboration de leurs algorithmes, vidéos qui en dehors de ce contexte ne sont pas public. »
1. Depuis 20 ans l'intelligence artificielle a évolué vers ce que l'on appelle aujourd'hui le deep learning (l'apprentissage profond).
2. Le deep learning est de loin beaucoup plus puissant que tout ce qui a été fait depuis 40 ans au niveau de l'intelligence artificielle.
3. Le deep learning est une technique basée sur l'apprentissage. Le logiciel « apprend », au vu des exemples qui lui sont donnés.
4. Plus le nombre d'exemples donnés au logiciel est important, plus la précision de son « expertise » sera grande.
5. L'accès aux datas pour donner des exemples au logiciel, afin d'affiner les algorithmes est devenu juste PRIMORDIAL-ESSENTIEL-INDISPENSABLE
SON Détection Audio
Remarque membre AN2V : SENSIVIC
Point d'achoppement avec la CNIL, qui stipule dans le courrier qui nous a été adressé : "une base législative spécifique apparaît nécessaire pour la mise en œuvre de tels dispositifs sur la voie publique et dans les lieux ouverts au public".
Dans le cas des données sonores, l'exigence est l'anonymisation des données : le traitement du son doit être effectué dès la capture, sur site, dans le détecteur lui-même. Le système doit garantir qu'aucune donnée fournie par le détecteur/capteur ne peut permettre de remonter à sa source.
À moins de crypter, et que seul un OPJ sache décrypter...
Sous un contrôle à définir, une expérimentation sur site doit pouvoir permettre au moins temporairement de traiter des données non encore anonymisées, ne serait-ce que pour mettre au point la technique d'anonymisation finalement mise en œuvre.
INTEROPERABILITE
Remarque membre AN2V : SULZER
But : intégrer plus directement l'ensemble des acteurs de la sécurité et de la sûreté autour d'un continuum de sécurité.
Risque : cacophonie générale dans les échanges d'informations opérationnelles.
Constat : Très concrètement, on observe aujourd'hui :
• Une absence totale d'harmonisation dans les références de localisation, dès que le GPS n'est pas disponible ou que les caméras sont situées dans des infrastructures à plusieurs niveaux en 3D (Ex : dans un même centre commercial, chaque enseigne repère ses caméras sur des plans différents),
• L'horodatage des informations est inexistant ou aléatoire,
• Rien n'est prévu dans les solutions techniques du marché, comme dans leurs mises en oeuvre par les différents opérateurs, pour assurer que les destinataires occasionnels des données, que sont les acteurs du continuum de sécurité, puissent les exploiter.
Pour ne donner qu'un exemple, il serait logique que les données produites par les caméras individuelles puissent être exploitées de façon cohérente avec celles des caméras de vidéoprotection susceptibles d'observer la même scène...
Il semble indispensable d'accompagner la montée en régime de la mise en œuvre des dispositions décrites, matérialisant le continuum souhaité, en prévoyant formellement des mesures techniques appropriées, comme un soutien aux travaux de normalisation, le développement de textes réglementaires dédiés, voire la mise en place d'une structure d'harmonisation technique auprès du Ministère de l'Intérieur sur le modèle de l'Agence du numérique de la sécurité civile qui opère déjà en matière de protection civile (voir Article R732-11).
Aucune disposition ne fait référence au RGPD et à la notion de propriété (et de responsabilité) des données vidéo par celui qui les a produites.
STRATÉGIE
Que devient la CNV ?
CNV 2011 : Alain Bauer, puis CNV 2012 : Luc Strehaiano
Commission Nationale de la vidéoprotection
Coordination des CDV : Commissions Départementales de la Vidéoprotection
SYNTHÈSE
VIDE LEGISLATIF A COMBLER
CNIL a le champ libre pour interpréter, bloquer...
Deux options :
Enrichir la proposition de loi actuelle ?
Prévoir un nouveau texte (LOPPSI 3) ?
AN2V A DISPOSITION, avec ses membres mobilisés

Mission du député Jean-Michel Mis

« Pour un usage responsable et acceptable par la société des technologies de sécurité »

*

1/ Objectifs de la mission

La mission souhaite explorer, lors des auditions et via les contributions écrites, les axes suivants :

- Les **opportunités offertes par les nouvelles technologies au service d'une meilleure offre de sécurité** en analysant les besoins des forces de sécurité, entre autres dans la perspective des grands événements sportifs de 2023 et 2024.

- Les principes nécessaires à **la préservation des libertés** en définissant un cadre d'emploi global et cohérent des technologies de sécurité et en associant la société civile à cette définition pour renforcer la compréhension et l'acceptabilité des nouvelles technologies dans la société.

2/ Questions

La notion de « technologies de sécurité » est large. Quelles sont les principales selon vous ? ***[Par exemple : traitement des données (textuelles, images, sonores), biométrie, mobilité.]***

Axon a opté pour une approche transversale et intégrée de l'innovation en matière de sécurité. En effet, les technologies commercialisées par Axon reposent sur un écosystème cohérent de dispositifs, dans une logique de désescalade de la violence, de protection et de responsabilisation des agents des forces de l'ordre et des citoyens.

En effet, Axon commercialise des pistolets à impulsions électriques (PIE) TASER, armes intermédiaires non-létales mais au fort pouvoir dissuasif et qui permettent de répondre aujourd'hui aux exigences de protection des populations civiles dans le cadre des interventions. Ces PIE peuvent être associés aux caméras-piétons Axon Body 3, légères, faciles d'utilisation et dotées d'une grande autonomie. Elles fonctionnent également avec la technologie Axon *Signal* qui déclenche automatiquement la caméra en mode vidéo lorsqu'un PIE est mis en route ou une autre arme de poing est sortie de son étui, assurant une totale transparence des interventions.

Axon commercialise également des caméras embarquées dans les véhicules des forces de l'ordre, ainsi que des solutions de drones, et des solutions vidéo pour les sales d'audition, qui fonctionnement dans l'écosystème intégré Axon.

La technologie Axon permet enfin une retransmission en direct des images captées par les caméras-piétons, les caméras embarquées et les drones, et qui peuvent dès lors être consultées par les équipes habilitées, *via* la technologie Axon *Evidence* (logiciel en mode SAAS, avec les données hébergées en *cloud*).

Enfin les technologies d'IA d'Axon permettent le floutage des visages, l'horodatage ainsi que la retranscription en mode des textes des interventions.

Pour quelles finalités ? ***[Par exemple : détection de situations, analyse prédictive, suivi des personnes.]***

Les dispositifs commercialisés par Axon permettent, dans un environnement technologique intégré, d'offrir aux forces de l'ordre des outils les protégeant, tout en assurant aux citoyens l'exemplarité des

agents. Il s'agit là d'une forte demande de la population dans un contexte de tensions grandissantes lors des interventions des agents ces dernières années.

Ainsi, le PIE TASER a fait ses preuves comme arme de dissuasion qui évite une escalade de la violence et présente un potentiel létal quasiment nul. Dans un contexte où les forces de l'ordre sont amenées à devoir répondre parfois dans la précipitation à des menaces, le PIE TASER représente une alternative précieuse aux autres techniques d'interventions tout en évitant le contact direct.

Les caméras-piétons et caméras-embarquées sont quant à elles des dispositifs essentiels dans la documentation et la collecte de preuves à l'occasion des interventions. Elles protègent à la fois les agents et les citoyens, et permettent de rétablir la vérité dans un contexte souvent chaotique. La technologie *Signal* assure à ce titre que l'utilisation des caméras ne soit pas uniquement à la discrétion des agents, en déclenchant automatiquement leur fonctionnement, renforçant ainsi la légitimité de l'action des forces de l'ordre.

L'application Axon *Evidence* offre ~~enfin~~ une interface simple, qui permet une gestion efficace des différents dispositifs Axon, avec la possibilité de stocker les vidéos captées sur un cloud, et de les partager via un lien numérique avec toutes les parties prenantes (justice, etc.). C'est ce que fait d'ores et déjà, par exemple, la police municipale de Bordeaux, ou encore la SUGe avec les OPJ ou, à plus grande échelle, la police métropolitaine de Londres avec la justice en partageant environ 5 500 fichiers par mois.

Pensez-vous qu'elles permettraient d'anticiper les évolutions des missions de sécurité dans les 10 à 20 ans à venir ? Comment voyez-vous ces évolutions ?

Les technologies Axon permettent dans une large mesure de répondre aux nouvelles exigences de l'action des forces de l'ordre.

En effet, elle offre aux agents, *via* l'utilisation des caméras-piétons, la possibilité de ne pas se laisser dépasser par l'intensification de la guerre des images. Elles permettent aussi une action plus efficace et plus immédiate grâce à la transmission en direct des images captées, répondant ainsi aux exigences de réactivité.

Les PIE TASER permettent quant à eux de ne pas recourir systématiquement aux armes létales et aux techniques d'intervention contestées, comme la clé d'étranglement par exemple. Il permet une solution intermédiaire d'action qui souvent manque à nos agents.

Sur chaque technologie prioritaire évoquée, quel est l'état de développement de l'industrie française ? Que lui manque-t-il pour se perfectionner ?

Le système informatique de la police et de la gendarmerie nationale doit être amélioré en utilisant la fibre et en permettant le transfert sécurisé de fichiers vidéo volumineux (depuis les caméras-piétons par exemple).

Une couverture Wifi sécurisée autour des commissariats/gendarmeries permettrait également à l'avenir le déchargement automatique des vidéos des caméras embarquées des véhicules de police/gendarmerie directement vers les logiciels de traitement des preuves vidéo.

Le stockage en *cloud* sécurisé doit lui aussi être largement adopté afin de faciliter l'usage de logiciels performants et bénéficier des nouvelles technologies offertes par l'IA. Le but étant de réduire les tâches administratives afin de :

- Faire que les agents passent plus de temps sur le terrain ;

- Partager plus facilement les données en interne comme en externe pour traiter des affaires plus efficacement ;
- Utiliser la retransmission des images en direct pour permettre une meilleure coordination des équipes ;
- Pouvoir faire des statistiques nationales sur l'utilisation des outils afin d'analyser le retour sur investissement.

Comment les configurations techniques peuvent-elles concilier une utilisation de ces technologies et des garanties pour les libertés (protection des données, contrôles automatisés, etc.) ?

Axon a mis en place un *board* éthique afin d'échanger sur les sujets de nouvelles technologies et protection des libertés.

L'intelligence artificielle développée par Axon permet de flouter les visages des personnes filmées lors des interventions. Cependant, l'identification des visages développée par Axon ne va pas jusqu'à la reconnaissance faciale en vue de matcher les visages avec un autre fichier de recherche d'individus, préservant ainsi l'identité des citoyens.

Les cadres d'expérimentation sont souvent mis en avant pour le perfectionnement de ces technologies. Quelles sont selon vous les priorités ? Quels seraient les contours de ces cadres ? A quelles fins ?

Il est en effet essentiel d'expérimenter les différentes solutions avant un déploiement massif, pour éviter les nombreux écueils de matériels s'avérant inopérants une fois déployés et pouvoir comparer différentes solutions de différents fabricants.

*

Ce questionnaire est indicatif et ne prétend pas de couvrir l'intégralité des enjeux posés par les technologies de sécurité. La mission recueillera tout élément qui lui sera apporté afin de l'intégrer au mieux dans sa réflexion.

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

Nouvelles technologies et sécurité – Observations de la CNCDH

En raison de la brièveté du délai imparti à la CNCDH pour répondre à la sollicitation de M. le Député Jean-Michel Mis, les présentes observations n'ont pas vocation à traiter de manière exhaustive des « *enjeux de libertés individuelles et publiques* » soulevés par l'usage des nouvelles technologies dans le domaine de la sécurité. A défaut d'une validation en temps utile par les membres de la CNCDH en assemblée plénière, elles ont été alimentées par des avis antérieurs de la Commission.

La CNCDH a en effet eu l'occasion ces dernières années de se prononcer à plusieurs reprises sur l'utilisation des nouvelles technologies à des fins de sécurité (applications de *contact tracing*[1], caméras aéroportées[2], algorithmes de détection d'une menace terroriste[3]). Un groupe de travail au sein de la CNCDH mène actuellement un travail d'analyse et de réflexion relatif à l'impact de l'intelligence artificielle sur les droits de l'Homme, qui aboutira à un avis, vraisemblablement en novembre 2021.

A titre liminaire, la CNCDH tient à rappeler que les droits de l'homme ne peuvent être seulement assimilés à des « *garanties mises en place pour encadrer strictement l'usage* » de dispositifs techniques de sécurité, comme le laisse entendre la lettre de mission du Premier ministre. Davantage qu'une modalité juridique de mise en conformité d'un cadre d'emploi à la Constitution, les droits de l'homme définissent des exigences de principe au fondement de notre régime politique. Ils sont également consubstantiels à la sécurité, leur respect étant un gage de cohésion sociale et de préservation de l'ordre public.

Il ressort de l'ensemble des avis antérieurs de la CNCDH deux préoccupations essentielles à l'égard de ces nouvelles technologies sécuritaires : d'abord, la nécessité de les utiliser, leur caractère adapté à l'objectif qui leur est assigné, ne fait pas l'objet d'une évaluation suffisante ; ensuite, l'ampleur des atteintes qu'elles sont susceptibles d'engendrer à l'égard des droits et libertés fondamentaux met sérieusement en cause leur caractère proportionné.

La nécessité de recourir aux nouvelles technologies : un manque d'évaluation

Au regard des exigences conventionnelles et constitutionnelles, les restrictions apportées aux libertés doivent répondre à un triple test de nécessité, d'adaptation et de proportionnalité.

[1] Avis du 28 avril 2020 sur le suivi numérique des personnes, JORF n°0108 du 3 mai 2020.
[2] Avis du 26 novembre 2020 sur la proposition de loi relative à la sécurité globale, JORF n°0290 du 1 décembre 2020.
[3] Avis du 16 avril 2015 sur le projet de loi relatif au renseignement dans sa version enregistrée le 1er avril 2015 à la présidence de l'Assemblée nationale, JORF n°0171 du 26 juillet 2015.

Le Conseil constitutionnel demeure toutefois le plus souvent en retrait par rapport au législateur dans l'appréciation de la nécessité et du caractère adapté d'une mesure restrictive des libertés, rappelant qu'il ne dispose pas d'un « *pouvoir général d'appréciation et de décision identique à celui du Parlement* ». C'est particulièrement le cas lorsqu'il s'agit pour la loi d'introduire de nouveaux systèmes de surveillance, puisque le Conseil constitutionnel se limite alors à examiner s'ils sont assortis « *de garanties particulières de nature à sauvegarder l'exercice du droit au respect de la vie privée* »[4].

Il est pourtant essentiel, tant pour la représentation nationale que pour les citoyens, de disposer d'éléments d'information leur permettant de procéder à un examen critique de l'utilité de ces nouvelles technologies et de leur impact sur les droits et libertés fondamentaux, d'autant plus qu'elles pèsent lourdement sur les finances publiques.

La CNCDH relève à cet égard que la vidéosurveillance introduite en 1995 par la loi d'orientation et de programmation relative à la sécurité, n'a jamais jusqu'à maintenant fait l'objet d'une évaluation globale, répondant à des critères de scientificité, à commencer par l'indépendance et l'impartialité des chercheurs. Or, depuis sa mise en place, les équipements n'ont cessé de se perfectionner (avec des objectifs rotatifs à 360°, une amélioration constante de la résolution des images, etc.) et de très nombreuses municipalités ont installé des caméras sur la voie publique, sans avoir de recul sur les promesses d'un surcroît de sécurité garanties par les industriels du secteur.

Quoi qu'il en soit, dans son rapport récent sur les polices municipales, la Cour des comptes relève que « *au vu des constats locaux résultant de l'analyse de l'échantillon de la présente enquête, aucune corrélation globale n'a été relevée entre l'existence de dispositifs de vidéoprotection et le niveau de la délinquance commise sur la voie publique, ou encore les taux d'élucidation* »[5].

Pouvoir apprécier la nécessité d'utiliser de nouvelles technologies particulièrement intrusives et attentatoires aux droits et libertés fondamentaux est d'autant plus essentiel qu'elles réhabilitent le spectre d'une « société panoptique » menaçant les droits et libertés fondamentaux des citoyens.

Sur les droits et libertés fondamentaux mis en cause par les technologies de sécurité : un problème de proportionnalité

L'usage des nouvelles technologies à des fins sécuritaires, dans le sens d'une surveillance accrue des citoyens, tant sur la voie publique que sur internet, menace directement la protection des données personnelles. De ce point de vue, il risque de porter atteinte au respect de la vie privée.

L'examen des modalités de la conciliation entre les impératifs d'ordre public et le respect de la vie privée prend la forme dans la jurisprudence du Conseil constitutionnel[6] d'un contrôle, comme il a été

[4] Voir récemment à propos des caméras aéroportées : Décision n° 2021-817 DC du 20 mai 2021, *Loi pour une sécurité globale préservant les libertés*, § 135. Dans le même sens, il y a vingt-cinq ans, à propos des caméras de vidéosurveillance installées sur la voie publique : Décision n° 94-352 DC du 18 janvier 1995, *Loi d'orientation et de programmation relative à la sécurité*, §4.
[5] Cour des comptes, « Les polices municipales », Rapport public thématique, Octobre 2020, p. 70.
[6] C'est également valable pour la Cour européenne des droits de l'homme.

rappelé plus haut, des garanties susceptibles d'encadrer l'utilisation de nouvelles technologies, notamment :
Une formulation claire et précise des motifs d'utilisation de la technologie;
L'information du public ;
La limitation de l'accès aux données éventuellement recueillies ;
Une durée limitée de conservation des données, le cas échéant, d'autant plus brève qu'il s'agit de données sensibles ;
Des procédures de contrôle du respect des garanties.

Cette approche n'est toutefois pas suffisante, d'abord en raison de l'exigence de nécessité qui n'est pas prise en compte (cf supra), mais aussi parce qu'elle n'envisage pas les effets indirects de ces dispositifs sur d'autres droits et libertés.

En effet, au-delà de la protection des données et du respect de la vie privée, l'utilisation des nouvelles technologies peut induire des attitudes de contournement légitime à leur égard, susceptibles de menacer l'exercice d'autres droits et libertés fondamentaux. Dans son avis sur le suivi numérique des personnes, principalement consacré à l'application de *contact tracing* STOPCOVID, la CNCDH exprimait ses craintes à l'égard de « *l'incidence sur les libertés d'un dispositif de surveillance renforcé par l'utilisation d'outils numériques : le sentiment d'être surveillé en permanence risque d'entraver l'exercice effectif des libertés individuelles et collectives* ».

Dans le même sens, la CNCDH alertait dans son avis relatif à la proposition de loi relative à la sécurité globale : « *La mobilisation de caméras aéroportées, notamment pour l'encadrement des manifestations, est susceptible de dissuader les personnes de manifester, ne sachant ce qu'il adviendra des images collectées par ces caméras volantes* », soulignant de surcroît que « *ces outils de surveillance, peuvent également s'apparenter par eux-mêmes à des outils d'intimidation, en particulier lorsqu'ils sont équipés d'un haut-parleur* ».

La CNCDH concluait ce dernier avis en exprimant son inquiétude face à *« l'accroissement sans précédent de ces dispositifs techniques de captation et de traitement d'images à des fins de poursuites d'infraction et de gestion des foules d'autant que leurs conditions de déploiement ne paraissent pas suffisamment répondre aux exigences imposées par le principe de proportionnalité propre à garantir le respect des droits et libertés fondamentaux des individus ou groupes d'individus dont l'image serait ainsi captée et traitée. De telles préoccupations sont en outre amplifiées dès lors que se multiplient les appels à l'usage dans l'espace public de technologies de reconnaissance faciale fondées sur le traitement de données biométriques*[7]*. A cet égard, la CNCDH rejoint la CNIL*[8] *et l'Union européenne*[9] *sur l'importance de mener un débat démocratique et éthique en la matière, compte tenu des risques que comporte le recours à ces technologies s'agissant des atteintes aux libertés et droits fondamentaux « à grande échelle », ou encore des effets que pourrait induire le renforcement de la surveillance permis par cette technologie sur la vie privée et sur l'anonymat dont disposent les citoyens dans l'espace public ».*

[7] Le Livre blanc de la sécurité intérieure, publié le 16 novembre 2020, préconise l'expérimentation de la reconnaissance faciale dans l'espace public.
[8] CNIL, « Reconnaissance faciale. Pour un débat à la hauteur des enjeux », 2019.
[9] Commission européenne, Livre blanc sur l'Intelligence artificielle, 2020, p. 25.

Ce faisant la CNCDH souligne également l'effet cumulatif des dispositifs de surveillance de l'espace public, jusqu'à la surveillance d'internet. Il est essentiel de ne pas s'en tenir simplement à une approche segmentée des technologies de sécurité, qui consisterait à envisager leur impact sur les droits fondamentaux de manière isolée. La mobilisation croissante, présente et à venir, de ces outils aura vraisemblablement une incidence sur la société et la conception que l'on se fait de la liberté. Une surveillance accrue, générale et indifférenciée, inaugurée par la vidéosurveillance et amplifiée par le couplage des caméras à des logiciels de détection des comportements suspects, à quoi s'ajoutera peut-être demain les drones, pourrait non seulement dissuader les gens de se réunir et de manifester, mais aussi inciter les individus à se conformer à certaines normes sociales.

C'est d'autant plus vrai que les algorithmes utilisés pour détecter des menaces parviennent à des résultats qui souffrent d'un défaut d'explicabilité (c'est pourquoi elles sont parfois assimilées à des « boîtes noires »). Autrement dit, à rebours du principe de légalité et de sécurité juridique, principes qui garantissent contre les risques d'arbitraire – les citoyens doivent connaître les conséquences juridiques de leur actes –, l'utilisation de ces algorithmes est susceptible d'engendrer une incertitude dans l'esprit des gens sur ce qu'il est permis ou non de faire.

Mission du député Jean-Michel Mis

« Pour un usage responsable et acceptable par la société des technologies de sécurité »

*

1/ Objectifs de la mission

La mission souhaite explorer, lors des auditions et via les contributions écrites, les axes suivants :

- Les **opportunités offertes par les nouvelles technologies au service d'une meilleure offre de sécurité** en analysant les besoins des forces de sécurité, entre autres dans la perspective des grands événements sportifs de 2023 et 2024.

- Les principes nécessaires à **la préservation des libertés** en définissant un cadre d'emploi global et cohérent des technologies de sécurité et en associant la société civile à cette définition pour renforcer la compréhension et l'acceptabilité des nouvelles technologies dans la société.

2/ Questions

Quels sont selon vous les principaux enjeux de liberté dont il est question face aux technologies de sécurité ?

Les technologies de sécurité sont susceptibles de soulever de nombreux enjeux du point de vue des droits fondamentaux, sans qu'il s'agisse d'une nouveauté historique : de tout temps, les objectifs légitimes de recherche des auteurs d'infractions, de préservation de l'ordre public et de lutte contre le terrorisme doivent être conciliés avec la liberté d'expression et d'information, la liberté de conscience, la liberté de circulation, la liberté d'entreprise, l'inviolabilité du domicile, etc.

En ce qui concerne les domaines de compétence de la CNIL, les technologies de sécurité sont susceptibles d'impacter directement les droits au respect de la vie privée et à la protection des données à caractère personnel. Les progrès technologiques impliquent en effet des possibilités de collecte et de traitement de données à caractère personnel dans des volumes inédits et en croissance exponentielle. En théorie, les technologies de sécurité permettent notamment de capter les nombreuses traces laissées par les individus dans l'espace numérique (données délibérément partagées sur un profil, mise en ligne de contenus par un tiers, données captées dans l'espace public, mais également traces laissées inconsciemment par la navigation sur le web ou dans l'utilisation d'objets connectés, etc.) et reposent sur une capacité technologique démultipliée d'exploitation de ces informations, avec le « big data », le développement des « mégabases » ou « mégadonnées », ainsi qu'avec l'essor des techniques d'intelligence artificielle (IA) – la massification des données permettant un travail de combinaison et d'enrichissement des données par diverses techniques, grâce à des traitements algorithmiques recourant à des formes plus ou moins sophistiquées d'IA. Par nature, elles impliquent donc un potentiel de surveillance individualisé ou collectif sans précédent, c'est-à-dire un risque d'atteinte substantielle aux droits à la vie privée et à la protection des données ainsi qu'aux autres libertés fondamentales dans l'exercice desquelles ces technologies interviennent (lorsqu'il s'agit de surveiller une manifestation, par exemple, la navigation sur internet, les déplacements, etc.).

Il faut néanmoins rappeler que, comme toutes les libertés fondamentales, les droits à la vie privée et à la protection des données ne sont pas des droits absolus et doivent être mis en balance avec d'autres objectifs ou intérêts, dans le respect du principe de proportionnalité. Le cadre constitutionnel et conventionnel n'interdit donc pas des atteintes à ces droits fondamentaux mais leur juste conciliation avec d'autres intérêts publics tels que ceux poursuivis par les technologies de sécurité.

C'est dans cette perspective que la CNIL examine toutes les solutions de sécurité qui lui sont soumises dans le cadre de ses avis. La CNIL est particulièrement attentive au fait que la multiplication de ce type de dispositifs pourrait modifier la manière dont chacun vit et exerce sa liberté individuelle dans l'espace public, voire dans l'espace privé. Le sentiment que l'on est, ou que l'on peut être, surveillé de façon permanente dans l'espace public, pour un grand nombre de finalités, modifierait fondamentalement l'exercice de nos libertés.

Quelles technologies et usages vous inspirent le plus de prudence quant au respect de ces libertés ?

Les textes relatifs à la protection des données sont dits « technologiquement neutres » : ils s'appliquent à toutes les technologies existantes et n'ont ni pour objet ni pour effet de s'opposer à telle ou telle technologie dès lors que les conditions dans lesquelles il y est recouru sont conformes aux principes de protection des données.

Néanmoins, le RGPD et la loi « Informatique et Libertés » ne sont pas indifférents aux risques soulevés par le traitement de certaines catégories de données. Les données dites « sensibles » (données relatives à l'origine raciale ou ethnique, aux opinions politiques, aux convictions religieuses ou philosophiques ou à l'appartenance syndicale, données génétiques, données biométriques, données concernant la santé et la vie ou l'orientation sexuelles d'une personne) font ainsi l'objet d'une protection particulière, de même que les données relatives aux condamnations pénales ou aux infractions. Toute technologie ou tout traitement portant sur de telles données, ce qui est naturellement et légitimement très fréquent en matière de sécurité, doit nécessairement impliquer la prudence et la mise en œuvre de conditions particulières.

En pratique, certaines technologies sont donc par nature plus sensibles que d'autres du point de vue du droit à la protection des données : ainsi des méthodes de reconnaissance biométrique ou génétique, par exemple. Les usages de technologies de sécurité devant faire l'objet d'une vigilance particulière de ce point de vue sont également nombreux. On peut penser en particulier à toutes les technologies de surveillance des comportements dans l'espace public, physique ou numérique, dans la mesure où elles interviennent dans le champ de nombreuses libertés fondamentales : caméras « augmentées », reconnaissance faciale, mais également surveillance des communications électroniques par exemple. On peut également penser à toutes les technologies qui permettent la collecte et le traitement de données à l'insu des personnes (drones par exemple) ou sans que celles-ci soient mises à même de comprendre le traitement dont elles font l'objet (algorithmes auto-apprenants d'intelligence artificielle par exemple). Enfin, à toutes les technologies qui, par nature, impliquent, non plus seulement la surveillance des seules populations « à risque » ou « suspectes », mais la surveillance de tous aux fins d'identifier les personnes dangereuses : cette inflexion du paradigme de la surveillance est à l'œuvre en de nombreux domaines (PNR, techniques de l'algorithme pour les communications électroniques, etc.). Certains usages, par exemple de la reconnaissance faciale (dans l'espace public, sans information des personnes et reposant sur le scan de tous les visages captés par les caméras), sont susceptibles de répondre à ces trois caractéristiques simultanément et doivent de ce fait faire l'objet d'une vigilance toute particulière.

Néanmoins, conformément au principe de neutralité technologique et au-delà de ces risques potentiels intrinsèques, c'est bien cas d'usage par cas d'usage que le respect des libertés mises en cause par une technologie de sécurité doit être examiné.

Comment assurer l'équilibre, dans une société toujours plus imprégnée de technologies, entre les impératifs de liberté et de sécurité ?

Du point de vue du droit à la protection des données, deux principes doivent guider la prise de décision en matière d'usage de technologies de sécurité : la nécessité et la proportionnalité. C'est à l'aune de ces deux exigences impérieuses que le recours à des technologies potentiellement attentatoires doit être examiné.

La nécessité impose d'apprécier rigoureusement l'utilité d'une technologie, ou plus exactement de ses cas d'usage envisagés. Le besoin doit être tout à la fois réel, effectif et actuel : il ne suffit pas qu'une technologie soit potentiellement utile, sans que ses bénéfices concrets et précisément délimités aient été évalués. Il faut se prémunir de la tentation du solutionnisme technologique, qui consiste notamment à vouloir faire usage d'une technologie dès lors qu'elle est disponible sans même définir les besoins qu'elle est censée satisfaire. En outre, la condition de nécessité implique que l'objectif poursuivi ne puisse pas être raisonnablement atteint, ou de manière substantiellement équivalente, par des moyens moins intrusifs.

L'application du critère de proportionnalité a deux effets possibles. Le premier est d'interdire le recours à certaines technologies particulièrement intrusives pour des objectifs qui ne justifient pas cette atteinte : la technologie est efficace, mais disproportionnée au regard de l'avantage qu'on peut en attendre. Ainsi, l'utilisation d'une technologie de reconnaissance faciale automatique sur une caméra de vidéoprotection afin de repérer la commission d'une simple contravention semble disproportionnée. Le second effet possible de l'application du principe de proportionnalité est de conduire la CNIL à n'accepter le recours à une technologie qu'à la condition que certaines garanties soient mises en place. Ce sont en effet les garanties dans les conditions effectives de mise en œuvre d'une technologie qui seules permettent d'atteindre l'équilibre entre ces deux impératifs tout aussi légitimes dans une société démocratique. Ces garanties sont précisément celles prévues par les textes en matière de protection des données : la délimitation précise des objectifs assignés à l'outil dans le respect du principe de proportionnalité (il est par exemple disproportionné, quand bien même cela serait utile, de permettre la surveillance par drones de tout l'espace public aux fins de lutter contre les contraventions), la minimisation des données traitées au regard des objectifs assignés, le principe de subsidiarité qui doit présider au choix de tel ou tel cas d'usage en fonction de son caractère intrusif, le renforcement des droits des personnes à chaque fois que cela est possible, etc.

Au titre de ces garanties, les modalités de contrôle des dispositifs sont essentielles : plus ces modalités sont nombreuses, diverses et fréquentes (en amont et en aval), dans la limite naturellement de l'efficacité de l'action des forces de sécurité, plus la probabilité d'atteindre le juste équilibre entre liberté et sécurité est importante.

En tout état de cause, ces doubles verrous (nécessité et proportionnalité) imposent des analyses au cas par cas, éventuellement regroupées par grandes catégories de technologies (la reconnaissance faciale, l'intelligence artificielle, etc.) mais appliquées in concreto à des cas d'usages bien déterminés. C'est ainsi que la CNIL a par exemple raisonné en matière de reconnaissance faciale (https://www.cnil.fr/fr/reconnaissance-faciale-pour-un-debat-la-hauteur-des-enjeux)

Quelle perception avez-vous d'une association citoyenne à la définition des conditions d'appropriation de ces nouvelles technologies, à des fins de sécurité mais aussi plus généralement ? Quelle forme cette association pourrait-elle prendre ? Quelles technologies particulières devrait-elle nécessairement couvrir ?

Cette dimension relève davantage de la bonne conduite des politiques publiques que des missions de la CNIL. Néanmoins, deux observations peuvent être apportées.

Tout d'abord, la question de l'appropriation des nouvelles technologies ne doit pas constituer la préoccupation première, chronologiquement parlant, pour les technologies particulièrement attentatoires aux libertés. Pour celles qui mettent en cause les droits fondamentaux et qui nécessitent la recherche d'un nouvel équilibre entre les intérêts en présence, il semble nécessaire de déterminer en premier lieu les usages acceptables d'une telle technologie, et les conditions dans lesquelles il peut y être recouru, et de ne traiter l'enjeu de l'acceptabilité qu'à la fin du raisonnement, comme ultime étape et non comme postulat, pour les seuls dispositifs reconnus comme parfaitement légitimes et licites. L'association citoyenne doit dès lors, pour ces usages à risque, concerner davantage la délimitation de ces cas d'usage que les conditions de leur acceptabilité.

Ensuite, une fois ces usages déterminés, la question de leur appropriation est en effet centrale. La CNIL dispose, en vertu de la loi « Informatique et Libertés », de missions de sensibilisation des personnes sur leurs droits à l'égard du traitement de leurs données, au titre de laquelle elle fournit de nombreux conseils pratiques sur son site internet (https://www.cnil.fr/fr/prenez-1-heure-pour-adopter-de-meilleurs-reflexes-pour-votre-vie-privee-numerique par exemple), et d'éducation au numérique pour les enfants (cf. par exemple : https://www.cnil.fr/fr/les-droits-numeriques-des-mineurs). Elle est donc prête à prendre toute sa part à cette perspective d'appropriation des nouvelles technologies, qui doit comporter un volet relatif à la nécessaire protection de ses données dans ce cadre.

Quelle forme peut prendre une doctrine d'application du RGPD qui concilie le respect des libertés et l'exploitation des dérogations à des fins de sécurité ?

Il faut tout d'abord rappeler que le cadre juridique relatif à la protection des données (RGPD, Directive police-justice, loi « Informatique et Libertés ») comporte en effet toutes les dérogations nécessaires au bon exercice des missions de sécurité. Ces dérogations font l'objet d'un encadrement strict, conformément à la volonté des législateurs européen et national, mais sont suffisantes pour garantir la préservation de ces intérêts publics : possibilité de traiter des données sensibles si nécessaire, possibilité d'écarter les droits des personnes si leur exercice remet en cause les finalités du traitement concerné, de ne pas recueillir le consentement des individus naturellement, d'exclure certains pouvoirs de sanction de la CNIL, etc. Des débats, par exemple entre la CNIL, les juridictions compétentes et les autorités publiques, peuvent émerger sur la légalité ou l'opportunité de la mobilisation de telle ou telle dérogation mais le cadre juridique est en tout état de cause suffisamment adapté aux spécificités de ces missions.

En outre, ce cadre juridique se fonde sur une approche par le risque : c'est en fonction des risques présentés par tel ou tel traitement de données, que ses modalités précises de mise en œuvre doivent être déterminées (mesures de sécurité, analyse d'impact préalable ou non, etc.).

Dans ces conditions, et compte tenu des observations précédentes sur la nécessité d'une analyse au cas par cas, il apparait difficile d'établir une doctrine d'application générale sur l'application de ces dérogations qui ne se résumerait pas à une présentation des textes. Un tel document, s'il est jugé utile, pourrait en revanche être rapidement élaboré par la CNIL. La CNIL est par ailleurs à la disposition des autorités publiques compétentes pour élaborer une telle doctrine d'emploi appliquée à une technologie particulière et déclinée en quelques cas d'usages topiques.

Les nouvelles technologies de sécurité suscitent d'importants besoins en compétences mixtes, notamment juridiques et techniques. Comment faites-vous face à ces évolutions pour assurer votre mission ?

La régulation des données personnelles dans le monde numérique suppose effectivement une capacité d'expertise non seulement juridique mais aussi technologique, pour répondre aux attentes à la fois des professionnels qui sont demandeurs de sécurité juridique pour accomplir leur travail mais également des citoyens qui ont besoin, pour adhérer d'avoir confiance dans les outils proposés.

La CNIL a besoin de recruter des profils de juristes et d'ingénieurs. Il est rare de recruter des profils parfaitement mixtes, mais il existe des profils de juristes qui sont sensibilisés aux sujets informatiques, et des ingénieurs qui ont suivi des formations en droit des données personnelles. Ces profils sont rares et très recherchés.

La CNIL expérimente en particulier des difficultés pour recruter ses profils d'ingénieur. La rémunération offerte est, pour tous les profils, souvent en dessous de ce que peut offrir le marché de l'emploi privé. Lorsqu'un emploi n'est pas pourvu par fonctionnaire en détachement ou en mise à disposition, il est crucial de pouvoir offrir un recrutement en CDI.

La CNIL constate que le fait d'avoir une expérience chez le régulateur demeure attractif et bien valorisé dans la suite du parcours professionnel. Elle s'est engagée dans une démarche de constitution d'une « marque employeur ».

Par ailleurs, la CNIL promeut et essaye de participer à la mise en réseau des expertises et outils avec les autres composantes de l'Etat numérique.

La régulation ne saurait, enfin, s'appuyer sur une expertise exclusivement juridique et technologique : la CNIL poursuivra son investissement dans d'autres approches, sur le plan éthique en particulier.

En tout état de cause, les effectifs de la CNIL sont actuellement limités et ne permettent pas encore, malgré les efforts budgétaires consentis, une régulation optimale du traitement de données, par rapport notamment aux homologues européens de la CNIL.

Le monde de la donnée suscite un volume d'activité accru pour les régulateurs et les parties prenantes. Comment y faire face pour adapter le cadre protecteur à la société de demain ?

En ce qui concerne la protection des données, plusieurs observations peuvent être faites, concernant tout d'abord les parties prenantes. Le RGPD a opéré de ce point de vue une révolution copernicienne, déjà observée dans d'autres domaines du droit comme par exemple celui de la lutte contre le blanchiment de capitaux, en remplaçant les anciennes déclarations auprès de la CNIL par une plus grande responsabilisation (Démarche générale dénommée "compliance").

Les organismes traitant des données participent dorénavant de la régulation et ont été dotés des moyens juridiques nécessaires à cet effet, par la mise à disposition de nombreux outils de la conformité : délégués à la protection des données, analyses d'impact, registres de traitement, codes de conduite, certifications, etc. Cela implique une charge nouvelle pour ces organismes mais également une plus grande responsabilité et liberté dans leurs activités numériques. L'attention à la protection des données constitue enfin un avantage compétitif certain, comme l'ont montré par exemple, récemment, les interrogations du public sur la modification des conditions d'utilisation de la messagerie Whatsapp.

Le régulateur fait aussi, naturellement, l'objet de fortes attentes dans ce nouveau cadre, en termes de prévisibilité juridique et de moyens d'action répressifs. A cet égard, outre les développements qui précèdent sur les limites des effectifs de la CNIL et les changements apportés ces dernières années à sa politique de recrutement, la CNIL mise sur deux leviers d'action pour garantir la protection des personnes dans le monde numérique : la sécurisation des acteurs et leur responsabilisation.

En effet, les conséquences concrètes du RGPD restent trop souvent incertaines et il faut donc poursuivre le travail de clarification des règles et proposer des cadres sécurisants par des recommandations et des lignes directrices. C'est dans l'intérêt des responsables de traitement et c'est également la condition pour que les droits des personnes soient en pratique respectés. L'accompagnement restera ainsi une priorité pour la CNIL, sous toutes ses formes (générale sur les grandes notions, sectorielle ou individuelle avec les nouveaux outils de la conformité) et c'est pourquoi l'institution s'est récemment dotée d'une « charte d'accompagnement des professionnels »[1]. La CNIL doit également s'inscrire dans le mouvement de développement des certifications ou autres formes de label qui permettent de transformer la contrainte réglementaire en avantage comparatif, en atout économique. Garante du respect des règles de sécurité informatique lorsque des données personnelles sont traitées, elle doit également continuer à agir pour une meilleure connaissance et un meilleur respect des recommandations de cybersécurité, qu'elle contribue à façonner à travers sa doctrine, l'instruction des violations de données personnelles qui lui sont signalées et ses actions répressives[2].

Du côté de l'effectivité des droits des personnes, la CNIL a proposé une réforme de sa procédure de sanction lui permettant, pour les affaires peu graves et ne soulevant pas de difficultés particulières, de prononcer des sanctions d'un montant limité dans des conditions simplifiées par rapport aux contraintes actuelles des différentes procédures prévues par la loi « Informatique et Libertés ». Cette réforme, actuellement en cours d'examen au Sénat dans le cadre du projet de loi relatif à la différenciation, la décentralisation, la déconcentration et portant diverses mesures de simplification de l'action publique locale, lui permettra d'adopter plus rapidement de plus nombreuses mesures correctrices en cas de manquement au cadre juridique.

Ces deux actions se complètent et sont nécessaires l'une à l'autre : le travail de pédagogie manquera de crédibilité si les règles n'apparaissent pas effectives ; l'action correctrice et répressive de la CNIL n'est acceptable que si les obligations des responsables de traitement sont tout à fait claires.

L'un des moyens de garantir un bon usage de ces technologies et de procéder avant tout à des expérimentations. Quelles seraient selon vous les conditions que ce cadre expérimental devrait réunir ?

La CNIL partage cette orientation et propose fréquemment, lorsqu'elle est saisie de dispositifs particulièrement innovants et potentiellement attentatoires au droit à la vie privée, de procéder par voie d'expérimentation ou de prévoir des clauses de revoyure, comme elle l'a fait par exemple sur certains dispositifs de recueil de renseignements à des fins de lutte anti-terroriste.

La démarche doit néanmoins être sincèrement expérimentale. Cela implique notamment une limitation dans le temps et dans l'espace des dispositifs en cause, une identification exacte des objectifs poursuivis par ces expérimentations et de leurs critères de réussite. La définition précise de leurs modalités d'évaluation, qui doit être rigoureuse, contradictoire, pluridisciplinaire et menée dans des délais

[1] La CNIL publie sa charte d'accompagnement des professionnels | CNIL
[2] Cybersécurité (cnil.fr)

raisonnables, ainsi que la détermination des autorités chargées de celle-ci, constituent des dimensions essentielles. La comparaison avec d'autres dispositifs techniques pouvant répondre aux mêmes besoins permettra en outre une meilleure évaluation des systèmes de reconnaissance faciale. Le cadre juridique doit ainsi garantir la sincérité des expérimentations conduites, dont l'issue ne saurait être préjugée. Il doit pour cela consacrer une méthode expérimentale rigoureuse, inspirée du cadre juridique plus général en la matière et du « guide méthodologique » récemment élaboré par le Conseil d'État, afin de tirer tout le parti possible d'une telle démarche tout en faisant montre de la prudence nécessaire face aux risques posés par la reconnaissance faciale.

Cette prudence n'a pas pour objet de brider l'innovation technologique. Au contraire, une véritable démarche expérimentale permettra de tester et de parfaire des solutions techniques respectueuses du cadre juridique, lorsqu'elles se présenteront, et intégrant directement les contraintes liées à ces règles.

Une telle démarche peut en outre bénéficier d'un cadre juridique allégé, dès lors que le RGPD prévoit des dérogations importantes pour les traitements de recherche scientifique (en matière de données sensibles, de droits des personnes, etc.). La CNIL admet l'utilisation de ces dispositions spéciales sur la recherche dès lors que les expérimentations ont pour seul objet cette recherche scientifique, à l'exclusion de tout effet opérationnel direct sur les personnes concernées. De telles expérimentations peuvent ainsi avoir lieu en conditions réelles, comme par exemple dans le cas du recours expérimental à la reconnaissance faciale dans le cadre du carnaval de Nice, sous réserve de ne pas avoir de conséquence directe sur les personnes concernées.

*

Ce questionnaire est indicatif et ne prétend pas de couvrir l'intégralité des enjeux posés par les technologies de sécurité. La mission recueillera tout élément qui lui sera apporté afin de l'intégrer au mieux dans sa réflexion.

Par la suite, il été demandé des précisions sur les points suivants :

- ***L'audit des algorithmes***

La question de l'audit des algorithmes est très large et est susceptible d'impliquer de nombreux acteurs, la notion d'audit pouvant être interprétée largement. La CNIL est ainsi compétente pour opérer des contrôles sur les traitements de données à caractère personnel y compris les éventuels algorithmes qu'ils pourraient contenir. D'autres AAI pourraient également contrôler des algorithmes qui seraient utilisés pour prendre des décisions dans leur domaine de compétence (on peut penser à l'Autorité de la Concurrence (ADLC) par exemple, qui serait compétente si des algorithmes étaient utilisés de façon anticoncurrentielle. Mais des organismes privés pourraient également intervenir dans ce domaine, afin d'auditer ou certifier des algorithmes dans une optique de gestion de la qualité. Ainsi le Laboratoire national de métrologie et d'essais (*LNE) travaille sur un référentiel de certification (https://www.lne.fr/fr/actualites/ia-appel-public-commentaires-referentiel-certification), et l'AFNOR travaille à la réalisation de normes dans ce domaine qui pourraient ensuite servir de base à des certifications attribuées après une phase d'audit (https://register.gotowebinar.com/register/8491065821675055115).*

Il faut également indiquer que le projet de règlement sur l'IA de la Commission européenne prévoit de confier la mission de réguler les systèmes d'IA à des entités publiques, qui disposeraient très

probablement de pouvoirs de contrôles, et prévoit que dans certains cas les systèmes d'IA devront faire l'objet d'une évaluation des risques réalisées par un tiers indépendant, qui devra donc auditer leur fonctionnement.

- ***Les garanties techniques : l'anonymisation***

L'anonymisation des données, qui ne doit pas être confondue avec la pseudonymisation, consiste à casser tout lien entre des données et les personnes concernées par ces données à l'origine. Le mètre étalon en la matière est l'avis du G29 05/2014 sur les Techniques d'anonymisation qui définit ce qu'est l'anonymisation au regard du droit européen, et qui propose différentes techniques pratiques d'anonymisation. L'anonymisation est un problème complexe, qui nécessite en général une analyse au cas par cas afin de déterminer précisément les techniques d'anonymisation qui permettent d'anonymiser les données sans pour autant les rendre inutiles. Certains types de données (photos de personnes, vidéos, sons, données déplacement) sont très difficile à anonymiser correctement. De plus certaines finalités (recherche en santé, biométrie, …) ne sont pas conciliables avec l'anonymisation et doivent donc être opérés sur des données à caractère personnel, ce qui fait tomber les traitements associés dans le champ d'application du cadre juridique relatif à la protection des données personnelles. A contrario*, lorsque des données sont correctement anonymisées et qu'il n'est plus du tout possible de réidentifier les personnes concernées, ces données sortent alors de ce champ et peuvent être utilisées sans contrainte.*

- ***Les garanties juridiques : l'information des personnes***

La bonne information des personnes peut constituer une des garanties, citées dans les développements qui précèdent, de nature à atteindre le juste équilibre entre les intérêts en cause. Si l'obligation d'information sur les conditions de mise en œuvre du traitement de données dont les personnes font l'objet peut légitimement être écartée lorsque cette information fait obstacle ou nuit à la finalité même du traitement en cause (par exemple, de surveillance à l'insu des personnes), il n'en demeure pas moins qu'elle doit rester le principe à chaque fois que cela est permis par les circonstances de l'espèce. L'information est en outre la principale voie d'accès aux autres droits dont disposent les personnes à 'l'égard du traitement dont elles font l'objet : droits d'accès aux données, de rectification des données inexactes, d'opposition et d'effacement illicitement traitées, etc.

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

COMMISSION SUPERIEURE DU NUMERIQUE ET DES POSTES

MISSION RELATIVE AUX NOUVELLES TECHNOLOGIES DANS LE DOMAINE DE LA SECURITE

CONTRIBUTION DE LA CSNP

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, etM. 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.

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

Créer une instance de réflexion globale sur les technologies de sécurité

Note du Conseil national du numérique

le 3 juin 2021

M. Jean-Michel Mis, député, a été saisi par le Premier ministre d'une **mission sur les questions de technologies de sécurité à l'aune des évènements sportifs internationaux** qui seront organisés sur le territoire français en 2023 (coupe du monde de rugby) et 2024 (jeux Olympiques et Paralympique). Cette note vise à partager des éléments de réflexion répondant à divers points de la lettre de mission, à commencer par la nécessité de disposer d'une réflexion et d'échange sur le long terme impliquant l'ensemble des parties prenantes intéressées.

Un accroissement du recours aux technologies de sécurité et un débat parcellisé

Le recours à des technologies numériques fait partie intégrante de l'arsenal juridique et opérationnel de l'État en matière de sécurité. **L'intégration entre technologies de sécurité et technologies numériques s'est faite de manière progressive et avec une intensité particulière au cours de ces dix dernières années** : évolution des technologies de renseignement - du traitement algorithmique des données à l'IMSI catcher (balise d'interception des communications de téléphonie mobile), traitement des données de connexion, mise en place de fichiers, création d'outils d'identification ou d'authentification et les capteurs associés (i.e. reconnaissance faciale), essor de la ville intelligente, développement des aéronefs sans équipage ou encore réflexion sur les systèmes d'armes autonomes ou semi-autonomes.

Cette intégration s'est faite à l'issue de développements opérationnels, ponctués ou non par des décisions juridictionnelles à l'échelle nationale ou locale, des débats législatifs mais aussi au regard des décisions de principe en matière de droits fondamentaux, tant au niveau européen que constitutionnel. Au quotidien, il en va de la mission de nombreuses autorités d'examiner l'usage des technologies de sécurité sous l'angle de la sécurité des réseaux, de la protection de la vie privée et des données personnelles, du contrôle démocratique, des droits fondamentaux, des enjeux géopolitiques, économiques etc. **Nous assistons alors de fait à une parcellisation du débat** tenant à la fois au nombre d'enceintes qui abordent ces questions, qu'à la diversité des technologies étudiées.

La nécessité d'un cadre de dialogue ouvert et pluriel

L'usage des technologies pour des missions de sécurité ainsi que les modalités de contrôle qui leur sont appliquées revêtent des enjeux d'une importance particulière pour la sauvegarde de nos démocraties. En sus des contrôles imposés en droit et du rôle du Parlement, il est nécessaire que l'ensemble des personnes intéressées (administrations, académiques, citoyens, associations, entreprises, journalistes, élus locaux et nationaux) puissent **disposer d'un cadre d'échange global, continu, qui ne soit pas uniquement rythmé par les projets législatifs, couvrant l'ensemble des dimensions du sujet et l'ensemble des technologies concernées.**

Pour assurer une telle mission, il convient d'être en mesure de nourrir un dialogue avec et entre le plus grand nombre d'interlocuteurs, de disposer des ressorts humains permettant de mobiliser l'ensemble des personnes concernées ainsi que d'une expertise de fond générale sur la totalité des problématiques abordées (questions stratégiques, droits fondamentaux, connaissances technologiques, etc.). Il est d'autant plus **important d'avoir ces échanges au niveau local** puisqu'il revient généralement aux collectivités locales ou aux autorités déconcentrées de l'État de décider des modalités concrètes de déploiement des technologies.

Qu'une structure réunissant l'ensemble de ces prérequis soit chargée d'offrir un cadre de débat sur le recours aux technologies de sécurité répondrait à de nombreux enjeux : adopter des positions cohérentes et conformes au corpus commun des grands principes régissant la matière, rassembler des connaissances éparses, garantir la rencontre et l'écoute de l'ensemble des composantes de la société, assurer une continuité de long terme dans le suivi des différents débats etc.

Le rôle potentiel du Conseil national du numérique

Au cours de ses dix années d'existence et conformément à sa vocation, le Conseil national du numérique s'est illustré à de nombreuses reprises comme une **enceinte de concertation et d'échange** à même d'accueillir une parole plurielle sur des sujets techniques d'importance économique, politique, juridique et sociale. Dans le cadre de la mandature actuelle, **le Conseil s'est vu confier la mission de conduire une réflexion au long cours sur notre relation au numérique**, pris en tant que fait social majeur.

Pour réaliser cette mission, le Conseil se propose de **porter au débat les points de vue et positions de l'ensemble des personnes prenant ou souhaitant prendre une part active au sujet**. Il le fait d'ores et déjà à travers ses travaux de fond et la publication de prises de paroles extérieures sur son site. Pour les deux années à venir, il s'est fixé une feuille de route ambitieuse visant à réunir des publics variés au cours d'évènements récurrents offrant ainsi un cadre pérenne au débat.

Dans le cadre de la crise sanitaire, ces échanges ont pour l'instant lieu à distance au cours de rencontres en ligne. Néanmoins, dès que la situation sanitaire le permettra, **le Conseil reprendra et intensifiera ses déplacements sur l'ensemble du territoire pour assurer l'existence d'un dialogue engageant l'ensemble des composantes de la société** sur les différentes questions auxquelles renvoie notre relation au numérique. Celles relatives aux technologies de sécurité occuperont une place de premier plan.

Dans le cadre de l'organisation de ces échanges, le Conseil s'engage à **agir de manière collective au sein de l'État** afin d'impliquer le plus d'entités expertes et intéressées comme il a su le faire pour de précédents débats. Seule une logique partenariale et multilatérale permettra d'assurer la prise en compte de toutes les perspectives en présence. C'est pourquoi le Conseil se propose d'agir en interface et en coordination de tous les acteurs en vue de l'organisation de l'ensemble des rencontres. Enfin, **la restitution des échanges devra se faire de manière transparente, concertée et publique** afin de bâtir sur l'expérience acquise et les connaissances partagées.

CSF Industries de sécurité

Paris le 10 juin 2021

Nouvelles technologies et missions de sécurité

Ref : mission de monsieur le député Jean-Michel Mis confiée le 23 avril 2021 par le Premier Ministre.

PJ :
- Observatoire de la filière Industrie de sécurité 2020
- Industries de sécurité : Anticiper les technologies de rupture (2018)

Cette note constitue la synthèse des éléments présentés par le CSF à l'audition du 4 juin et elle ne reprend pas les réponses écrites des participants (projet JO, ACN, AN2V), plus détaillées. Elle ajoute des considérations sur la souveraineté.

La filière des industries de sécurité est une filière importante (30 Mds€), d'excellence et qui s'appuie sur des leaders mondiaux et un tissu dense d'ETI, PME, start-up innovantes et une recherche de niveau mondial. Après une première étude économique en 2015, elle est suivie depuis 2017 par un observatoire économique. La filière est présente sur tous les segments du marché qui présente trois grands volets : produits physiques (y compris plateformes) ; produits et services électroniques et numériques, produits et services de cybersécurité. La croissance est tirée par le numérique et la cybersécurité qui prennent une part de plus en plus importante.

La filière a été rassemblée dès 2013 autour d'une coopération public-privé (CoFIS puis CSF Industries de sécurité à partir de 2018) avec les objectifs clés de répondre aux besoins, de développer la filière et d'assurer la souveraineté sur les technologies clés. Le contrat de filière mis en place en 2020 entre l'État et l'industrie comporte cinq projets structurants proposés par l'industrie pour leur fort impact visé :

- Sécurité des JO Paris 2024 et des grands évènements
- Cybersécurité et sécurité de l'IoT
- Identité numérique
- Territoires de confiance
- Numérique de confiance

Tous ces projets sont motivés en tout ou partie par la souveraineté. Maintenir ou développer la souveraineté est particulièrement ardu du fait de l'apparition continuelles de nouvelles technologies.

L'anticipation est le maitre mot, et c'est dans cet esprit que la filière a identifié en 2018 une liste de ruptures technologiques et les a analysées sous les angles des futurs usages, économique et de souveraineté (document « Anticiper les ruptures technologiques »). Ces technologies génériques sont les suivantes, celles intéressant très directement la sécurité intérieure sont mise en gras :

- **intelligence artificielle** (domaine transverse),
- composants de confiance (domaine transverse),
- **internet des objets et objets connectés**,
- **big data & analytique**,
- **conjuguer mondes réels et virtuels**,
- **identifcation, authentification**,
- **plateformes intégrées véhicules / services**,
- **détecter les produits dangereux, illicites ou contrefaits**,
- **intervenant augmenté**,
- **observation, locale**,
- blockchain,
- ubérisation et post ubérisation de la sécurité,
- plateformes ouvertes pour la sécurité.

La filière travaille pour toutes les applications de sécurité, mais la sécurité intérieure est un client particulièrement important auquel la filière a consacré des efforts singuliers, pour n'en citer que quelques-uns :

- Identification des technologies critiques (2017)
- Démonstrateurs de communication (2016)
- Démonstrateur de video-protection (2015)
- Travaux AN2V sur les aspects juridiques de la vidéo-protection (en continu)
- Charte de solidarité en situation d'exception entre le ministère de l'intérieur et le CICS (2017)
- Travaux industriels dès 2017 pour préparer la sécurité des JO 2024 (mapping 2017, proposition globale en 2019, etc.)
- Accompagnement sur le Livre blanc de 2020

La filière essaye d'attirer l'attention du ministère de l'intérieur sur des sujets avec une grande anticipation, mais ces sujets ne débouchent pas rapidement. Plusieurs raisons peuvent y contribuer, telles que : manque de vision, manque de moyens, manque d'appétence, division interne. La filière fait le

constat que le ministère de l'intérieur a un besoin criant d'accélération technologique, qui est nécessaire pour qu'il puisse se projeter dans l'avenir.

Au grès des exercices (Livre blanc, rapport Thourot Fauvergue, …), l'industrie fait part des mêmes perspectives et des conditions nécessaires pour que les technologies puissent trouver le chemin d'applications étendues au sein de l'État.

L'apport des technologies pour la sécurité est clair dans de nombreux domaines (facilitation du travail des forces, vision transverse et sans couture, coordination, traiter des masses de données, anticiper les risques, retrouver automatiquement les données sur les personnes dans les videos, etc. – détaillé dans les réponses mentionnées plus haut).

L'estimation du rapport coût/bénéfices est à faire dans chaque cas, mais plusieurs points sont communs :

- De nombreuses technologies présentent des enjeux fort de souveraineté (Big data, IA, Cyber, Cloud, Identité numérique, …)
- Nécessité de disposer de données massives, disponibles dans la durée, pour concevoir et améliorer les solutions
- Prépondérance des questions juridiques et éthiques, qu'il s'agit de traiter avec une grande précision afin de ne pas interdire en bloc et de façon dogmatique toutes les applications, alors que certaines solutions peuvent intelligemment répondre à tous les critères.
- Nécessité de permettre des expérimentations, réelles et significatives, par dérogation s'il le faut, pour avancer les solutions intelligentes ; et a contrario, ne pas faire des expérimentations, compliquées et allongées inutilement, un tunnel dont ne sortent jamais les applications.

Il ressort aussi régulièrement que les relations entre le ministère de l'intérieur et l'industrie bienferaient significativement de processus et instances permanentes public-privé permettant de travailler de concert sur la compréhension des problèmes et l'identification d'approches conceptuelles, organisationnelles et technologiques pour y répondre[1]. Cela pourrait être pour les JO un observatoire public-privé de la sécurité des grands événement, mais cela ne doit pas s'arrêter à cela.

Deux points nécessitent un développement : l'éthique et la souveraineté.

ETHIQUE

La filière dès 2013 a mis l'éthique au cœur de son action. Les enjeux affichés par le CICS incluaient dès 2015 « Industrie de sécurité et débat de société ». La filière s'est proposée à l'occasion du contrat de filière de rédiger une charte éthique et d'organiser une réflexion récurrente autour d'elle. Cette charte

[1] Il est intéressant de noter que, sauf erreur, le ministère de l'intérieur, contrairement à de nombreux cas à l'étranger (Espagne, UK, …) ne fait pas appel à des cabinets de conseils pour analyser ses processus, son organisation, ses pistes d'évolution.

indiquera que les valeurs de l'UE constituent le cadre pour les entreprises et que liberté et sécurité ne s'opposent pas. Elle se veut constituer un différentiant économique pour la filière face aux entreprises non UE. Développer des technologies respectueuses de ce cadre, c'est défendre les valeurs de l'UE, il convient de la faire savoir.

Le CSF propose ainsi de mettre en place une instance entre les parlementaires et l'industrie pour faire le point annuellement de l'application de la charte comme des nouveaux sujets qui émergent et des dispositions à prendre à leur propos. Cette réflexion aurait le mérite d'être décorrélée des points chauds de l'actualité.

SOUVERAINETE

La maitrise souveraine des technologies est indispensable dans deux cas :

- Lorsqu'il s'agit de technologies pour lesquels les risques de contrôle extérieur, de déni de service, de non-disponibilité, d'écoute, de manipulation[2], etc. sont inacceptables : cybersécurité, communications, dispositifs d'alerte, Cloud, Big data, IA, analyse video, matériel d'écoute, systèmes manipulant des données sensibles, etc. Lorsque le risque de perte de souveraineté est avéré (fournisseur unique, non compétitivité, perte de compétences, rachat, …), ces technologies sont dites critiques.
- Lorsqu'il s'agit de technologies nécessaires pour le maintien économique à terme des entreprises françaises, notamment sur des technologies de rupture qui vont prendre un poids économique considérable, y compris pour les usages en France : IA, Big data, Identité numérique, Blockchain, etc. Ces technologies peuvent aussi renter dans la catégorie ci-dessus.

Pour illustration la filière a établi en 2017 avec l'État une liste[3] de technologies critiques. Cette liste est déjà ancienne est devrait être revue. Elle ne concerne que des technologies existantes et non les technologies nouvelles sur lesquelles un effort important doit être fait : volonté de l'État, investissement,

[2] Par exemple instruction secrète qui ne mentionnera pas certains types d'événements (par exemple associé à un numéro présent sur l'image, à une caractéristique d'une intrusion cyber, etc.).

[3] Cette liste comporte notamment :

- Systèmes de contrôles d'accès électroniques
- Détection spécialisée pour risques NRBCE
- Observation et Surveillance (local) *(notamment video-protection, traitements, analyse d'images, etc.)*
- Technologies cryptographiques
- Sondes d'analyse et sondes souveraines de détection
- Matériels de chiffrement réseaux
- Les technologies de sécurisation du cloud
- Logiciel de reconnaissance du locuteur
- Logiciel d'exploration internet profond « deep web »
- Logiciel de reconnaissance faciale
- Intercepteur d'identifiants téléphonie mobile
- Détection et interception de signaux à étalement de spectre

réglementation, … Les technologies de ruptures sont, elles, décrites dans le document CoFIS « Anticiper les ruptures technologiques » de 2018 qu'il conviendrait également de revisiter.

La France n'est pas toujours au rendez-vous de la souveraineté. Les exemples sont très nombreux, en voici trois :

- Le recours à l'entreprise Palantir en 2016 pour du Big data au ministère de l'intérieur alors que l'industrie française proposait une démarche de développement de telles capacités. Ce n'est que plus tard que l'État a mis les moyens nécessaires (ministère des armées avec Atos et Thales).
- Le recours du Health Data Hub (données de santé, donc sensibles) à des solutions Cloud de Microsoft, décision qui a été finalement renversée après un tollé de l'éco-système.
- Le recours à un produit "caméra piéton" hors UE (Motorola).

Pour tous les marchés avec un volume financier fort, il faudrait systématiquement étudier sérieusement la capacité à produire en France et réaliser le sourcing (au besoin en identifiant les compétences existantes en France, à combiner pour arriver à la solution recherchée) avant de lancer la consultation. Dans le dernier cas ci-dessus, l'AN2V souligne que la commande aurait pu être honorée de façon satisfaisante par le fournisseur français Pryntec ou par un leader européen.

Le recours à des solutions non souveraines dans des domaines où il faut veiller au développement et au maintien de notre industrie, s'il est majoritaire et persistant, conduira inexorablement à l'étouffement de nos entreprises et à la dépendance totale à terme.

Il présente ainsi le double risque 1) d'être immédiatement exposé opérationnellement (risques mentionnés plus haut) et 2) de perdre pied et de n'avoir aucune solution maitrisée à terme.

Ce risque est particulièrement fort pour toutes les solutions reposant sur de l'IA où les règles sur l'utilisation des données pour le développement et les expérimentations sont très contraignantes. Ces règles peuvent conduire à se reposer sur des solutions étrangères déjà développées (mais non de confiance).

Pour mémoire, le CSF est très axé sur la souveraineté :

- Dans le projet JO pour assurer le contrôle aussi complet que possible des solutions de sécurité (notamment vis-à-vis d'éventuels acteurs étatiques extérieur) maitrisée par la filière
- Dans le projet Cyber, où le risque pris avec des solutions non souveraines est très fort et démultiplié, l'objectif est de développer une base industrielle souveraine. Le plan d'accélération cyber de l'État vise bien la souveraineté.
- Dans le projet identité numérique où l'objectif est d'avoir des identités numériques maitrisées et non imposées par les GAFA
- Dans le projet territoires de confiance où une partie de problème est de maitriser en France les données des collectivités locales

- Dans le projet numérique de confiance, qui vise à mettre en place les conditions du développement d'offres Cloud de confiance. Le plan d'accélération Cloud annoncé par l'État va dans ce sens.

Les grands événements de 2023 et 2024 : une vitrine pour la France, une opportunité de modernisation pour le Ministère de l'Intérieur, une ambition de politique industrielle pour les entreprises Françaises

Des technologies souveraines pour une sécurité éthique, transparente, compatible avec les libertés publiques et acceptée par les citoyens.

Les technologies représentent aujourd'hui, dans le domaine de la sécurité, à la fois une piste d'efficacité opérationnelle et une possibilité de diminuer le besoin en effectifs, notamment dans le cadre des grands rassemblements de personnes et des grands événements.

Les technologies sont donc une formidable opportunité pour l'État et singulièrement le ministère de l'intérieur, mais force est de reconnaître qu'elles suscitent méfiance et appréhension de la part des tenants des libertés publiques.

Il convient donc de développer des outils qui répondent à la fois aux besoins opérationnels, au souci de transparence des usages et aux impératifs de libertés publiques. Ces outils serviront en premier lieu à une modernisation des forces du ministère de l'intérieur pour leurs missions permanentes, mais ces technologies devront naturellement être au rendez-vous des prochains grands événements que sont la coupe du monde de Rugby et les JOP 2024.

Les Jeux Olympiques et Paralympiques de Paris 2024 représentent pour la France un défi capacitaire hors norme. Celui d'accueillir dans un esprit sportif et festif, pendant plusieurs semaines et en toute sécurité, l'ensemble des athlètes, des délégations et des millions de spectateurs. Ces Jeux seront également suivis par plusieurs milliards de téléspectateurs et la sécurité de cet événement sera un enjeu majeur pour l'image de la France.

Afin d'être au rendez-vous de cet événement majeur, en liaison avec les différents acteurs concernés, une démarche collaborative a été mise en place depuis 2018 entre l'Etat, organisateurs et industriels.

Dans le cadre du Comité Stratégique de Filière (CSF) et suite à la signature du contrat de filière en janvier 2020, l'industrie française de sécurité, réunissant des grands groupes, PME-ETI, et start-ups a ainsi mobilisé une équipe de France de la sécurité capable d'offrir des solutions technologiques performantes et compétitives tout en respectant le souci d'éthique et de transparence, qui sera l'ADN de la technologie de sécurité française.

En effet, loin des technologies intrusives des pays comme la Chine, les États-Unis ou la Russie pour ne citer qu'eux, il est possible et même souhaitable de développer, en France, des technologies de sécurité éthiques, transparentes, cohérentes avec le cadre des libertés publiques et acceptées par la population. Ce modèle peut être expérimenté, testé et développé à la faveur des grands rendez-vous sportifs à venir, mais pourra servir ensuite de modèle européen et symbolisera les valeurs portées par la France.

Ces technologies de sécurité alliant intelligence artificielle et cybersécurité en particulier sont au cœur des enjeux de souveraineté nationale. Il est essentiel pour la France, non seulement de maitriser ces technologies mais aussi de consolider sur son sol les savoirs faires nécessaires au développement, à fabrication et l'utilisation maîtrisée de ces technologies.

Pour développer, proposer et ajuster ce type de solutions technologiques, il est crucial de procéder à des expérimentations ciblées qui permettront de confronter les possibilités techniques aux impératifs éthiques et aux nécessités opérationnelles. Ces expérimentations sont incontournables si l'on souhaite donner au gouvernement en 2022 les éléments de choix pertinents et documentés, tant du point de vue juridique, budgétaire, technologique qu'opérationnel.

L'équipe de France des industriels s'engage, aux côtés de l'État, dans la préparation et la conduite de ces expérimentations dès à présent pour une sécurité éthique, transparente et efficace.

Ses recommandations sont les suivantes

1. Conformément à la lettre du Ministre de l'Intérieur adressée au Président de la République, un abondement budgétaire de 20 M€ à engager sur l'exercice 2021 hors plafond ;
2. Finaliser avec la filière industrielle, la liste et le cadre des expérimentations indispensables ;
3. La publication d'un décret gouvernemental autorisant la réalisation d'expérimentations sur le territoire national en phase 1 de ce programme ;
4. Contractualiser les expérimentations avec les industriels représentant la filière avant fin septembre 2021.

1 Un programme de sécurité pour le Ministère de l'Intérieur, qui s'appuie sur des Grands événements

1.1 Le contexte

La France organise en 2023 la coupe du monde de rugby et les JOP en 2024. Ces deux événements mondiaux peuvent utilement mis à profit dans une quadruple perspective : sécurité, anticipation, souveraineté et héritage.

Quatre objectifs peuvent ainsi être définis :

- Garantir la sécurité et l'esprit festif des événements ;
- Accélérer la modernisation des équipements des forces de secours et de sécurité ;
- Fédérer l'industrie française de la sécurité et en faire un champion international ;
- Contribuer à l'héritage, notamment du programme olympique, et développer un modèle exportable.

Dans cette perspective, le travail collaboratif entre l'État et les industriels a permis de dégager, grâce à une approche structurée et programmatique, des pistes d'expérimentations, ainsi qu'un programme de Recherche et Développement ambitieux qui identifie les technologies nécessaires au futur des forces.

Depuis l'élaboration conjointe d'un *« plan global de sécurité »* en 2019 les échanges se sont poursuivis en vue de définir un plan d'expérimentations visant à vérifier l'apport opérationnel de certaines technologies disponibles, en parallèle des études sur les technologies et dispositifs de sécurité innovants. En effet, la tenue d'expérimentations est essentielle dans la conduite du programme et la mise à disposition de nouvelles technologies au profit des forces de sécurité.

Organisées en coordination avec les futurs besoins des forces de sécurité et choisies d'un commun accord entre les industriels et l'Etat, elles sont une étape incontournable dans le programme de modernisation des forces de sécurité intérieure. Ces expérimentations seront menées dans le respect du droit et des libertés fondamentales et dans ce cadre représentent une opportunité d'accélérer la maturation de technologies Françaises efficaces et respectueuses des libertés et de l'éthique. Il s'agit ici de devenir leader international dans ce domaine pour la filière sécurité du CSF et pour la France de montrer une voie alternative, celle d'une sécurité éthique et transparente.

1.2 Les protagonistes

La proposition d'offre globale de sécurité se veut être cohérente au regard des enjeux mais surtout être un optimum à travers différents critères d'évaluation. Le caractère unique de cette proposition d'offre s'illustre par son ambition : couvrir les points d'intérêts vitaux pour la Nation.

Il est primordial que l'État reste souverain dans la sécurisation d'un tel évènement compte-tenu de la criticité de certaines missions de sécurité : éléments de renseignement et cybersécurité.

Afin de répondre à un tel enjeu, le projet a vocation à rassembler l'ensemble des acteurs français nécessaires au succès de la démarche :

- Les Industriels de la filière (grands groupes, ETI, PME, startups).
- L'État (ministère de l'Intérieur, ministère de l'Économie et des Finances, etc.).
- Les utilisateurs (État, Paris 2024, SOLIDEO, collectivités, opérateurs d'importance vitale et opérateurs de services essentiels, opérateurs de sites, acteurs de la sécurité privée, fédérations, les acteurs du tourisme, etc.).

Figure 1 Groupe Mixte

L'association de ces différents acteurs a permis la création du **Groupe Mixte** État– Industrie – Paris 2024, qui entend favoriser le dialogue entre les parties prenantes du projet afin d'aiguiller et valider les propositions de l'Industrie.

1.3 Les objectifs de la démarche commune Etat-Entreprises

Cette démarche a visé, dans le cadre d'une approche structurée et programmatique, à bâtir la proposition de sécurité des grands évènements à venir, de manière cohérente et globale. L'objectif est d'assurer la sécurité des JOP 2024 ainsi que de la Coupe du Monde de rugby de 2023, pour ensuite porter la proposition à l'export. Les JO doivent être un accélérateur de la modernisation des forces de sécurité intérieure.

Ce processus s'est effectué via la mise en commun de ressources par les différentes entreprises formant la branche sécurité du Comité Stratégique de Filière et dans le cadre du projet structurant « Sécurisation des grands évènements et des JO 2024 ». La proposition couvre différents axes afin d'apporter une réponse pertinente et mesurée aux attentes de l'État et des utilisateurs en matière de sécurité :

- Une architecture modulaire afin de répondre au triple enjeu des besoins sécuritaires, de l'évolution des briques technologiques et dans une logique de réutilisation.

- Une identification des différentes solutions et pistes d'innovation pertinentes afin de répondre aux critères de performance associés en s'appuyant, notamment, sur les travaux des AMI et de l'ANR (voire sur les programmes de financement de l'innovation européens ou français : PIAVE, PSPC Régions, PIA, etc.).

- Une organisation de la filière de sécurité française afin d'apporter une solution globale de sécurité pérenne en France et exportable à l'international, en promouvant le modèle de gouvernance et de collaboration, établi avec la CNSJ (coordination nationale pour la sécurité des jeux) et la DPSIS (Délégation ministérielle aux Partenariats, aux Stratégies et aux Innovations de Sécurité).

La solution cohérente et globale de sécurité présentée permet, dans un premier temps, de faire face à l'ensemble des aspects de sécurité, sûreté, cybersécurité et de défense dans un continuum de sécurité qui permettra également une grande efficience des ressources mises en œuvre au profit de :

- La coordination entre les différentes parties prenantes (régaliennes, locales et privées),
- La gestion des flux et des accès,
- La surveillance,
- La protection,
- Des centres de commandement,
- Des communications,
- De la cybersécurité,
- De la planification et mise en œuvre.

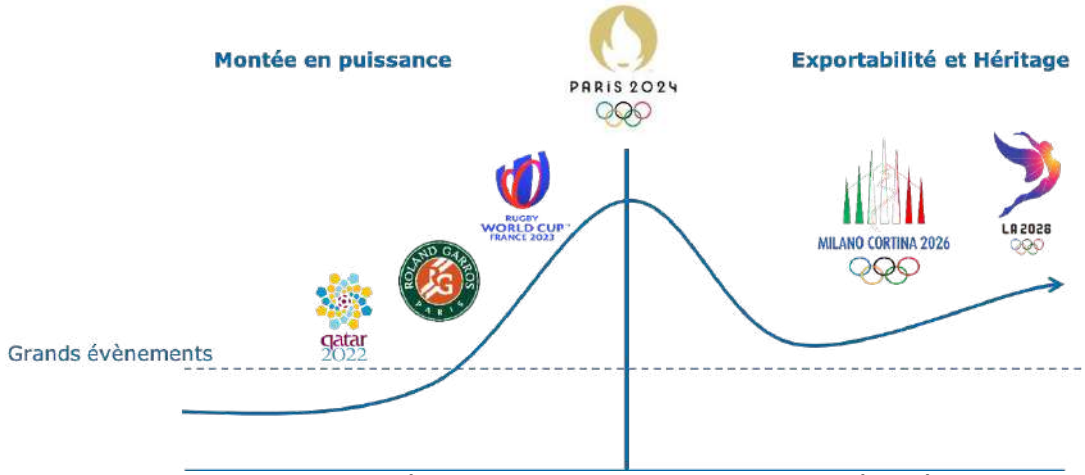


Figure 2 : Structuration de la démarche pour une solution globale de sécurité pour les Jeux Olympiques et l'Héritage

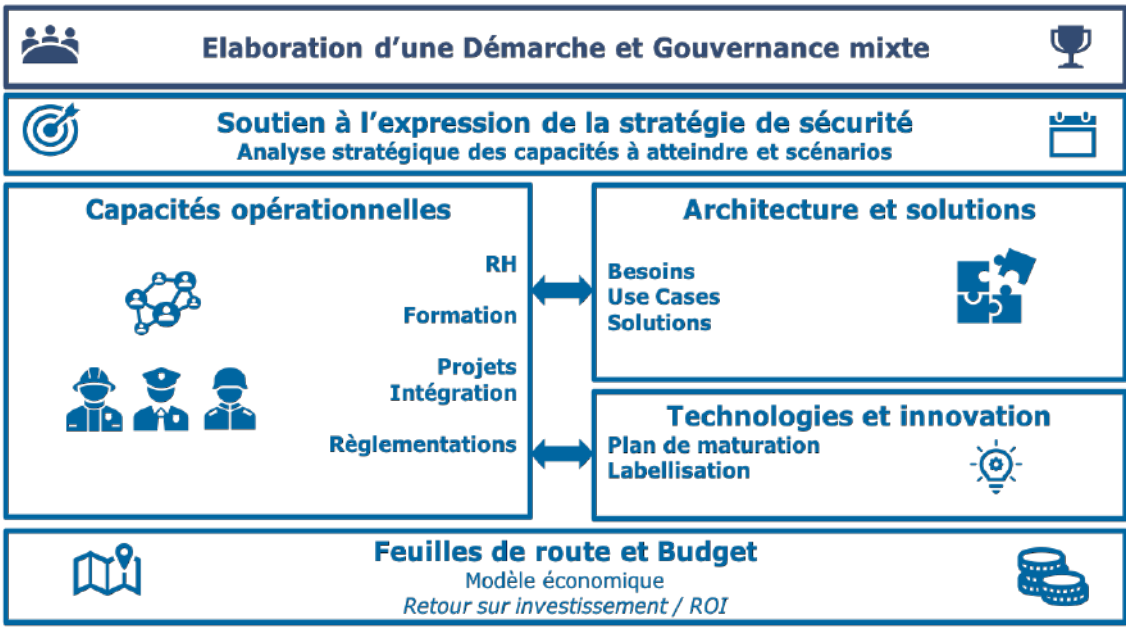


Figure 3 : Plan global de sécurité

1.4 Le contrat de filière

Pour soutenir cette démarche, le contrat de filière a été signé fin janvier 2020 entre l'Etat, Agnès Panier-Runacher, Christophe Castaner et le président du CSF, Marc Darmon. « La sécurité des grands événements et des JO Paris 2024 » est un des cinq projets ambitieux inscrits dans ce nouveau contrat de filière.

Le projet vise à développer une offre industrielle globale pour sécuriser les grands événements avec comme champ d'application exceptionnel les Jeux Olympiques et Paralympiques de 2024.

Ce projet d'offre française de sécurité des grands événements représente une opportunité unique, non seulement d'offrir le meilleur niveau de sécurité à nos concitoyens et à l'ensemble des participants internationaux aux Jeux de 2024, de moderniser par l'utilisation de nouvelles technologies les forces de sécurité intérieures, mais aussi de créer une filière industrielle cohérente et solidaire, à même de répondre dans la durée aux besoins de ses forces de sécurité et de se valoriser à l'international.

1.5 Pour une sécurité éthique, transparente et compatible avec les libertés publiques

Le déploiement de technologies de rupture implique nécessairement la conformité au cadre législatif en cohérence avec les recommandations de la CNIL.

Le programme prévoit ainsi un volet d'analyse du cadre législatif et des contraintes d'acceptabilité sociale. L'objet de cette analyse est de garantir la conformité juridique des dispositifs et technologies envisagés et de favoriser leur acceptabilité. Elle suit la démarche suivante :

- Lister les technologies qui présentent un risque juridique élevé notamment pour des raisons de sécurité des personnes, de traitement de données personnelles ou de nouveaux usages
- Identifier les contraintes légales applicables à chacune des technologies tel que le Règlement Général sur la Protection des Données (RGPD)
- Analyser les impacts des technologies sur le cadre législatif.
- En cas de traitement de données à caractère personnel, l'équipe d'étude réalisera une analyse d'impacts sur la vie privée des personnes. Celle-ci comprend à la fois une analyse de risques cybersécurité du traitement ainsi qu'une analyse juridique
- Déterminer les mesures de mitigation de ces risques
- Valider les mesures auprès des autorités compétentes, telles que la Commission Nationale de l'Informatique et des Libertés (CNIL)
- Rédiger un plan de communication et de contact pour permettre la mise en œuvre et le bon accueil des technologies.

Cette analyse juridique et législative est essentielle pour autoriser le déploiement des technologies concernées dans la stratégie de sécurité, ainsi que pour garantir l'acceptabilité de ces technologies.

2 Les technologies de sécurité

2.1 Introduction

Le programme développé par le Groupe Mixte s'articule autour d'une démarche organisée en 6 modules afin de répondre de manière globale et pertinente aux différents enjeux que posent les JOP 2024 en matière de sécurité. Dans notre proposition, sont donc abordés les sujets de : gouvernance, stratégie de sécurité, capacités opérationnelles, architecture de solutions, technologies et innovation, et enfin l'aspect économique et programmatique de l'approche.

Pour ce faire, le CSF a donc procédé à un certain nombre d'analyses :

- Une étude synthétique des enjeux et besoins sécuritaires sur la base des travaux du CoFIS ainsi que des différents rapports et plans rédigés jusqu'alors.
- Une analyse comparative des grands évènements à la fois sur les aspects budgétaires, organisationnels et capacitaires.
- L'identification des grandes missions de sécurité et des briques technologiques associées.

Ainsi que des recommandations :

- La définition de scénarios et paradigmes en fonction du soutien à l'expression de la stratégie de sécurité élaborée.
- Une feuille de route et un modèle de gouvernance entre les différents acteurs pour structurer l'approche jusqu'en 2024.

En l'espace de quelques mois, le CSF a organisé de nombreuses rencontres et ateliers afin de définir conjointement l'approche et le contenu de la proposition. De ce fait, ont eu lieu :

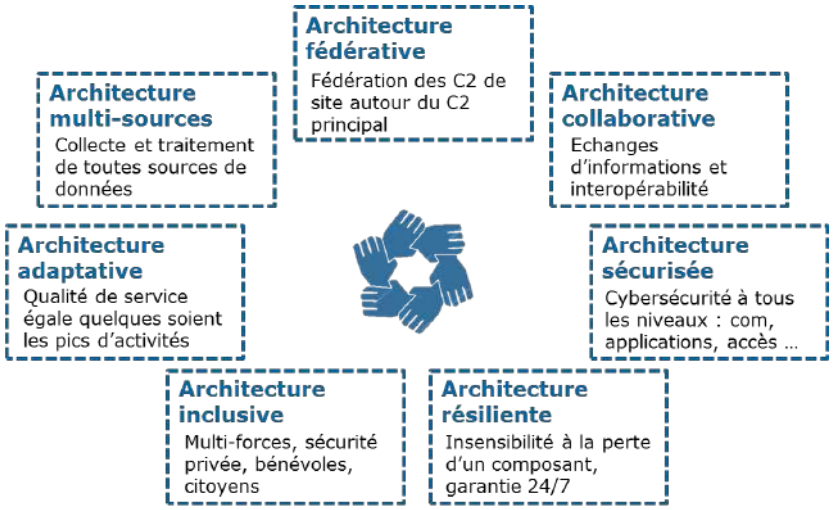
- Des comités de pilotage mixte rassemblant des représentants des deux entités précitées, afin de rendre compte de l'état d'avancement des travaux ainsi que de la définition de la marche à suivre.

2.2 Architecture fonctionnelle du système de sécurité

La solution globale de sécurité s'inscrit dans un environnement complexe, représenté par de nombreux acteurs, publics et privés, et des solutions préexistantes qu'il faut intégrer dans le dispositif

global, mais aussi de nouvelles technologies qui ont pour objectif d'assister les forces de sécurité dans leur métier.

Pour répondre aux enjeux de sécurité des JOP 2024 en tenant compte du contexte existant, l'architecture de cette solution sera fondée sur les grands principes suivants :



Les éléments technologiques permettant de répondre à ces principes d'architecture ont été étudiés par le groupe de travail « Technologies et Programme R&D » du groupe mixte en vue d'effectuer un recensement des technologies prioritaires croisé avec le résultat des AMIs (Appels à Manifestation d'Intérêt pour la sécurité des JOP 2024 lancés en 2019). Les domaines couverts par ces technologies sélectionnées sont :

- Les détecteurs ;
- La Détection, Reconnaissance, Identification (DRI) & l'Intelligence Artificielle (IA) ;
- Les robots et les vecteurs aéroportés ;
- L'IT et la Sécurité des Systèmes d'Information (SSI) ;
- L'internet des objets (IoT) ;
- La mobilité et l'interface Homme-Machine (IHM).

2.3 Les technologies prioritaires

Ces technologies présentent un potentiel de gain opérationnel pour les forces de sécurité dans leur ensemble. Leur développement et montée en maturité permettra également de valoriser le tissu industriel et de recherche français.

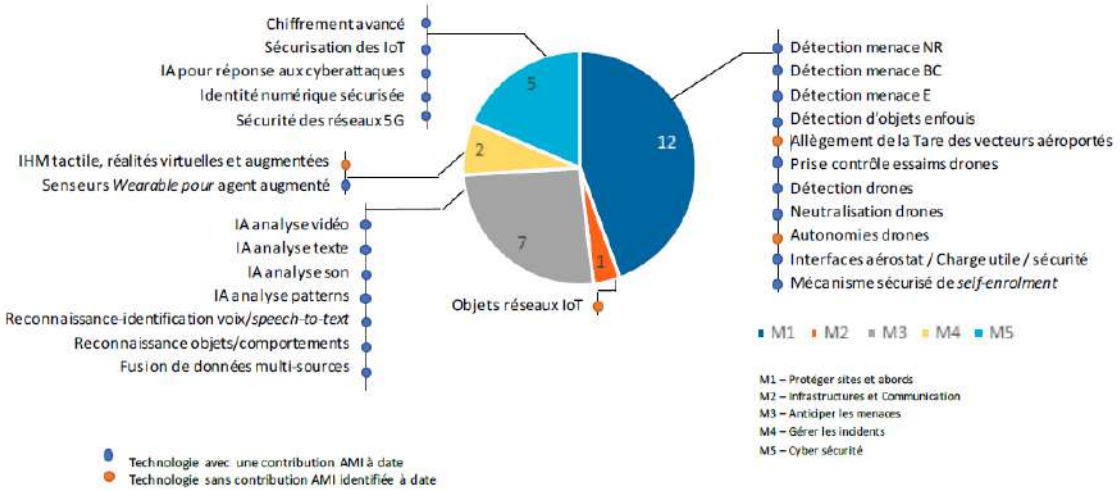


Figure 4 : Liste des technologies prioritaires identifiées

3 Les expérimentations

L'Addendum Concept d'Architecture ainsi que le document Technologies et Programme R&D de notre proposition mettent en lumière 152 technologies dont **27 technologies prioritaires**. Ces technologies disponibles ou en développement, ont été sélectionnées pour répondre aux missions des forces de sécurité intérieure dans le cadre des Jeux et de la Coupe du Monde de Rugby 2023.

Effectué en parallèle des études sur les dispositifs de sécurité existants et sur les technologies, le **plan d'expérimentations** a pour objectif de vérifier l'apport opérationnel de certaines technologies disponibles. Ces technologies sont proposées en réponse aux six cas d'usage priorisés lors d'ateliers réalisés entre les industriels et l'Etat en décembre 2019. Ceux-ci ont pu réunir des représentants de la Préfecture de Police de Paris, de la CNSJ, du SGDSN, de la DPSIS, de l'ANSSI, de la DGPN, de Safe Cluster ainsi que Rugby World Cup France 2023.

Le plan d'expérimentations décrit ci-dessous se concentre ainsi sur les cas d'usage suivants :

- Gestion des accès
- Contrôle des drones
- Protection des voies d'accès
- Plateforme de Commandement
- Gestion des informations et des communications
- Cybersécurité

Chaque cas d'usage fait l'objet d'une proposition d'une à trois expérimentations ajustées sur un thème particulier tel que la détection d'armes dissimulées et d'explosifs lors du contrôle d'accès. Afin d'anticiper la planification de ces expérimentations, des évènements prévus avant fin 2022 et représentatifs des enjeux des Jeux ont été identifiés.

La **tenue d'expérimentations est essentielle** dans la conduite du programme et la mise à disposition de nouvelles technologies au profit des forces de sécurité. Elles vont permettre de vérifier :

- Leur pertinence face au besoin des forces et l'objectif opérationnel ;
- Les ajustements nécessaires des cadres et doctrines d'emploi ;
- Les plans de formations et d'entraînement nécessaires à la meilleure maîtrise de ces technologies par les forces de sécurité ;
- Les impacts juridiques et sociétaux liés à l'utilisation de ces technologies.

Compte-tenu du fait que certains programmes ont d'ores et déjà été lancés par le ministère de l'Intérieur, comme le Réseau Radio du Futur, nous proposons de prioriser nos efforts communs sur les cas d'usage suivants :

- Plateforme collaborative d'Aide à la Décision (IA) et de Commandement
- Décèlement et identification de situations à risque dans les foules
- Cybersécurité

4 Annexes

4.1 Liste des technologies identifiées

Le document Technologies et Programme R&D (document en pièce jointe de la note *Pour Une Sécurité Ethique)* vient mettre en lumière les technologies de sécurité nécessaires à la réalisation des cinq grandes missions de sécurité pour les Grands Événements sportifs :

- M1 – Protection des sites, leurs abords et les cas particuliers
- M2 – Mettre en place des infrastructures et des moyens de communication
- M3 – Anticiper les menaces avant et pendant les JOP 2024
- M4 – Gérer les incidents opérationnels et de sécurité
- M5 – Protéger les systèmes d'information et de communication contre des attaques Cyber

Il a pour objectif de proposer une sélection de 27 technologies qui nécessitent un effort de R&D pour arriver à niveau de maturité suffisant à l'horizon 2023. A l'heure actuelle, un premier croisement a été réalisé entre les quatre thèmes proposés par les AMI pour la sécurité des JOP 2024 lancés en 2019 et les cinq missions de sécurité. Ce recoupement révèle que les solutions labellisées au travers des AMI peuvent contribuer à 23 des 27 technologies sélectionnées.

M1 - Protéger les sites, leurs abords et les cas particuliers						
Technologies matures et TRL (TR7 et plus)			Technologies en émergence ou développement et TRL (TRL 6 ou moins)			Séelc
19	Lidars 2D	8	19	LAPI freeflow avec capacités de DRI et couleur	4	
20	Détecteurs d'ouverture de porte, de fenêtre	9	20	Analyse video pour détection comportementale	4	
21	Contrôle d'accès	9	21	Analyse vidéo pour détection d'objet abandonné	4	
22	Détecteurs de fumée	7	22	Tracking video en foule	5	
23	Tracking video en intrusion	7	23	Tracking video multi cameras	4	
24	Panneaux d'affichage dynamique	8	24	Technologie de détection & neutralisation de drone autonome à mois de 10s	4	Y
25	Suivi de téléphone portable	8	25	Détection et neutralisation d'une menace saturante	5	Y
26	SCADA avec capteurs de pression	9	26	Allègement de la tare des vecteurs aéroterrestres	5	Y
27	Badges longue portée	8	27	-		
28	Liens HF	8	28	-		
29	Caméras sous-marines	8	29	-		
30	Hydrophones	8	30	-		
31	Caméra visible sans analyse vidéo embarquée	9	31	-		
32	Detection faciale collaborative sur serveur	9	32	-		
33	Reconnaissance faciale collaborative sur serveur	9	33	-		
34	LAPI simple contrôlé ou freeflow (noir & blanc sans DRI)	7	34	-		
35	Analyse video pour mesures de flux (comptage & densité)	7	35	-		
36	Technologie de brouillage intelligent dédiée au déminage	9	36	-		

Tableau 1 – Liste des technologies de la Mission M1

M2 - Mettre en place des infrastructures et des moyens de communications						
Technologies matures et TRL (TR7 et plus)			Technologies en émergence ou développement et TRL (TRL 6 ou moins)			Séelc t.
1	Réseau 4G transportable (Format Shelter, Véhicule)	8	1	Réseaux PMR (numérique/LTE)	6	
2	Réseau de desserte fibre optique, cuivre, FH, WiFi	8	2	Réseaux IoT (NB-IOT/ LTE-M)	6	
3	Réseau de desserte Satellite	8	3	Réseau 5G transportable (Format Shelter, Véhicule)	5	
4	Edge Computing	7	4	Réseaux PMR (5G)	5	
5	Cloud hybride public / privé	8	5	Réseau de desserte fibre optique, cuivre, FH dernière génération 2024 (THD)	6	
6	Sondes applicatives et optimisation	9	6	Objects connectés pour réseaux IoT (NB-IOT / LTE-M)	4	Y
7	Bulle 4G transportable (Format Véhicule, Manpack)	9	7	Cloud souverain	4	
8	Bulle Satellite de type FSS (Fixe) - GEO	8	8	Bulle 5G transportable (Format Shelter, Véhicule)	5	
9	Bulle Satellite de type MSS (Mobile) - GEO	8	9	Bulle Satellite de type FSS (Fixe) - LEO/MEO (orbite basse)	5	
10	Réseaux IoT (LoRa / Sigfox)	7	10	Bulle Satellite de type MSS (Mobile) - LEO/MEO (orbite basse)	5	
11	-		11	Vecteurs aéroportés pour complément de couverture	6	

Tableau 2 – Liste des technologies de la Mission M2

M3 - Anticiper les menaces avant et pendant JO						
Technologies matures et TRL (TR7 et plus)			Technologies en émergence ou développement et TRL (TRL 6 ou moins)			Séelc t.
1	Big data storage	8	1	Outils de géolocalisation	6	
2	Big data analytics	7	2	Analyse video à base d'IA	5	Y
3	PMR	9	3	Analyse de texte à base d'IA	6	Y
4	Serious games	7	4	Analyse de sons à base d'IA	5	Y
5	Enregistrement audio et vidéo	8	5	Analyse de pattern à base d'IA	6	Y
6	Mécanismes d'appairage intelligent et sécurisé entre billet et JO'Pass	7	6	Reconnaissance & identification vocale & speech-to-text	6	Y
7	LAPI simple contrôlé ou freeflow (noir & blanc sans DRI)	7	7	Reconnaissance d'objets / situations / comportements anormaux	5	Y
8	-	0	8	Fusion de données multi-sources	5	Y
9	-	0	9	LAPI contrôlé ou freeflow couleur sans DRI	6	
10	-	0	10	LAPI freeflow avec capacités de DRI et couleur	6	

Tableau 3 – Liste des technologies de la Mission M3

M4 - Gérer les incidents opérationnels et de sécurité						
Technologies matures et TRL (TR7 et plus)			Technologies en émergence ou développement et TRL (TRL 6 ou moins)			Séelc
1	Hyperviseur	7	1	Passerelles d'interconnexion multimédia entre centres de commandement	6	
2	Outils numériques & cartographiques avec BIM et geolocalisation temps réel	8	2	Outils IA pour gestion intelligente multimédia & multifux en centres d'appel	5	
3	Gestion de l'affichage vidéo multi-vidéo	8	3	Analyse contextuelle intelligente	4	
4	Système d'alerte à la population multimédia et multiflux	7	4	Analyse et reconnaissance de patterns intelligentes	6	
5	-		5	outils IA décisionnels et situationnels augmentés pour gestion de crise	6	
6	-		6	IHM Tactile, Réalité virtuelle, Réalité augmentée, 3D	5	Y
7	-		7	Plateforme communication / collaboration multimédia	5	
8	-		8	Dispatcher et Recording multimédia	4	
9	-		9	Speech to text (orienté métiers et missions)	6	
10	-		10	Technologies intelligentes de réalité augmentée multisoures et temps réel	4	
11	-		11	Senseurs "wearables" pour "agent augmenté"	5	Y

Tableau 4 – Liste des technologies de la Mission M4

M5 - Protéger les systemes d'information et de communication contre des attaques cyber							
Technologies matures et TRL (TR7 et plus)			Technologies en émergence ou développement et TRL (TRL 6 ou moins)			Selec t	
1	Pare-feu	9	1	DLP	6		
2	Pare-feu applicatif (Waf)	9	2	Identité numérique sécurisée	6	Y	
3	Proxy / reverse proxy	9	3	Chiffrement / Déchiffrement avancé (homomorphique, quantum-safe...)	4	Y	
4	Bastion d'administration et/ou d'accès	9	4	Sécurisation des IoT utilisés dans la solution de sécurité (security by design)	5	Y	
5	EDR (Postes de travail / serveurs)	9	5	SOAR	5		
6	CASB (Cloud)	8	6	UEBA	5		
7	MFA (authentication multifacteur)	9	7	Outil IA de réponses aux cybermenaces et cyberattaques	6	Y	
8	Anti-DDOS	8	8	Sécurité des réseaux 5G	5	Y	
9	Sondes (détection/prévention d'intrusion)	9	9	-			
10	Scanner de vulnérabilité	9	10	-			
11	NAC	9	11	-			
12	Passerellles d'interconnexion / Diodes	9	12	-			
13	Stations blanches	9	13	-			
14	Solution de scellement de configuration	7	14	-			
15	Solutions de chiffrement (réseau, fichiers, filesystems, BDD)	9	15	-			
16	Solutions d'anonymisation	9	16	-			
17	Anti-SPAM	8	17	-			
18	IAM	8	18	-			
19	Solutions des conteneurs sécurisés	8	19	-			
20	UEM	8	20	-			
21	Authentification contextuelle	8	21	-			
22	API de communications (chiffrement, authentification...)	8	22	-			
23	SIEM	7	23	-			
24	Honeypots	8	24	-			
25	CTI (Cyber Threat Intelligence)	7	25	-			
26	Sondes de détection (réseau et spécialisées)	8	26	-			

Tableau 5 – Liste des technologies de la Mission 5

4.2 Liste des expérimentations identifiées

4.2.1 Plateforme d'Aide à la Décision et de Commandement

Priorité	Sujet	Objectif
1	Traitement de la prise de décision et du suivi d'intervention pour le centre national	Tester le traitement de prise de décision et de suivi d'intervention pour la gestion des incidents à partir d'alertes, d'incidents externes ou d'événements planifiés en s'appuyant sur une cartographie et une tenue de situation.
2	Plate-forme d'échanges multi-source	Échanges d'informations entre centres de commandement existants de nature différente (police, sapeurs-pompiers, samu, Cojo 2024, …). Possibilité de faire un ou deux échanges dans l'expérimentation 1. Cette expérimentation nécessite des évolutions sur des SI tiers opérationnels.
3	Veille à partir d'une collecte d'informations source ouverte	Assurer une veille en rendant robuste la collecte de données multimédia sources ouvertes provenant du web dans un contexte international
3	Croisement de données de sources diverses	Croisement de données multi-sources (collecte d'informations en source ouverte (Exp 2) et agences de renseignement) afin de corréler des événements hétérogènes et de fournir des éléments pertinents (information, alerte, compréhension, …) ciblés pour différents acteurs.
4	Contrôle du niveau de risques externes par le suivi d'informations	Elaborer un suivi et une anticipation des risques externes adapté à un grand événement ou une crise et générer une alerte vers la gestion d'incidents si nécessaire
5	Analyse de fréquentation à partir de données mobiles	Utiliser les informations de fréquentation à partir des données mobiles pour avoir une connaissance de la situation en quasi-Temps Réel orientée sécurité publique.
6	Analyse de capteurs locaux	Capacité et contraintes de prise en charge par le C2 mobile des capteurs locaux à sa zone de responsabilité, qu'ils soient déployés pour l'occasion ou bien préexistants

4.2.2 Décèlement et identification de situations à risque dans les foules

Priorité	Sujet	Description
1	Détection de situation de crise dans une foule à partir de capteurs locaux	L'objectif est d'utiliser l'image et le son pour détecter des anomalies. Afin de diminuer le coût humain et d'augmenter la qualification des données, l'IA préanalyse ces données pour transmettre les potentiels alarmes adaptées aux cas d'usages des opérateurs en écartant les fausses alarmes. L'analyse d'un incident depuis le centre de commandement consiste ainsi à qualifier sa réalité, puis à le catégoriser sur sa gravité et sa zone d'impact.
2	Surveillance périmétrique extérieure (Fan zone, voies d'accès, …)	L'objectif est d'implémenter dans la maquette et de tester opérationnellement une solution de surveillance du périmètre extérieur. Cette solution s'appuie sur un réseau de capteurs déposés pour détecter les intrusions dans des sites éphémères et des zones extérieures non équipées. Les expérimentations sur ces technologies permettront de quantifier les économies de personnels dans le cadre des JOP2024.
3	Surveillance aéroportée des sites et abords	L'objectif est d'implémenter une solution de surveillance aéroportée afin de vérifier la fluidité et la sécurité des voies de circulation. Cette solution doit permettre une surveillance continue avec une mise en œuvre simplifiée ne nécessitant pas de personnels dédiés et hautement qualifiés.
4	Contrôle des drones : contrôle et protection	Ce cas d'usage vise donc à intégrer au sein de la maquette des solutions de contrôle des drones. Ce contrôle inclus la surveillance, l'identification, la classification et le positionnement des drones civils dans l'espace aérien mais également la neutralisation si besoin.
5	Acquisition de renseignements de sécurité sur sources ouvertes lié à la foule	L'objectif est de démontrer que les technologies de renseignement sur sources ouvertes peuvent apporter des éléments opératifs de maîtrise à la sécurité des grands évènements, tant en anticipation (avant l'évènement) qu'en réaction (post évènement).
6	Détection électronique d'explosifs	L'objectif est de mettre en œuvre une solution innovante de détection électronique d'explosifs adapté aux situations des GES, en présence de foule et avec un caractère opérationnel qualifié. Cette solution permettrait également de réduire les besoins en brigades cynophiles aux entrées des sites.
7	Surveillance NRBC et suivi environnemental	L'objectif est d'intégrer dans la maquette une solution de surveillance nucléaire des accès, des personnes et d'assurer un suivi environnemental afin de garantir la sécurité optimale des Jeux

4.2.3 Cybersécurité

Priorité	Sujet	Objectif
1	Profiter des technologies les plus abouties de Managed Detection and Response associée à l'Intelligence Artificielle au cœur du SOC	Profiter des technologies les plus abouties de Managed Detection and Response associée à l'Intelligence Artificielle au cœur du SOC, ainsi que la prise en compte des Micro SOC locaux déployés dans le contexte OT/IOT ci-dessous ou la relation avec les SOCs existants
2	Sécurité d'objets de type OT/IoT	La plateforme vise à s'assurer que les objets communicants de type OT ou IoT ne constituent pas des sources de vulnérabilités particulières. Sujet d'autant plus crucial que le nombre d'IoT présents sur les sites et hors sites sera sans doute beaucoup plus important qu'aujourd'hui. Un volet d'analyse Edge/Micro SOC local pour accélérer la réaction sera nécessairement pris en considération. Avantage : développer des règles de réaction très spécifiques et adaptées au périmètre couvert.
3	Gestion de crise cyber	Profiter des technologies de la maquette afin de simuler d'une crise et tester la bonne synchronisation des différents intervenants et des équipes de surveillance (CERT / CSIRT) privées ou publiques avec les autres organes de gestion de crise, en simulant une crise cyber qui pourrait avoir des impacts dans le monde réel, mais aussi en simulant des actions opportunistes ou coordonnées suite à une crise cyber. Cet exercice de gestion de crise pour simuler une crise cyber et une crise de type sécurité civile
4	Cyber stress test : Exercice de « Red Team »	L'objectif est de tester la résistance des sites évalués aux attaques cyber qui pourraient avoir lieu lors des JO2024 ou des grands événements sportifs. Cet exercice sert à tester des solutions innovantes qui permettent d'apporter une protection ad hoc de ces types d'attaques. L'objectif étant de pouvoir généraliser les dispositions retenues sur l'ensemble des sites.

Paris le 15 juillet 2021

Nouvelles technologies et missions de sécurité

Ref : mission de monsieur le député Jean-Michel Mis confiée le 23 avril 2021 par le Premier Ministre.

En complément de la note du 10 juin, et suite aux échanges entre JM Mis et l'équipe CSF JO, cette fiche donne un aperçu des faiblesses de la filière française de sécurité et cybersécurité. Ces éléments sont importants pour décider des politiques de déploiement en donnant toute leur place aux questions de souveraineté, d'innovation, et de soutien à la filière, notamment par la commande publique.

La filière a réalisé plusieurs exercices permettant d'identifier ses forces et faiblesses sur les divers segments. Il s'agit tout particulièrement :

- De la première étude économique de la filière (étude Pipame de 2015) qui a renseigné la majorité des segments de l'offre. Cette étude est maintenant assez ancienne, mais nombre de constats restent valables.
- Du recensement des technologies critiques en 2017
- De l'étude sur les technologies de rupture en 2018
- De l'AMI pour identifier les solutions innovantes pour répondre au besoin de sécurité des JO en 2019 et des travaux consécutifs du projet CSF JO. Sont ainsi identifiés les domaines à TRL encore bas, mais cependant sans indication claire du niveau de l'offre française.
- D'autres exercices (observatoire de la filière 2018 et 2020, ou observatoire annuel de la confiance numérique), présentent les forces et faiblesses de façon générique et macroscopique (structures, recherche, investissements, politiques publiques, etc.), sans identifier précisément les faiblesses précises sur les segments (par exemple absence d'offre).

Ces exercices ne permettent pas d'avoir une vision exhaustive et robuste des faiblesses de l'offre française, ni de les mettre en perspective (priorités et criticité vis à vis des besoins). Il est notable que l'exercice sur les technologies critiques ne recensent pas les technologies sur lesquelles l'offre française est d'emblée inexistante.

Sur la base de ces éléments (synthétisés en annexe), des technologies sur lesquelles une faiblesse de l'offre française, voire européenne, est patente sont – par exemple et sans exhaustivité :

- **Le domaine des capteurs, et de l'instrumentation de façon générale**, et notamment :
  - Les caméras – et de plus en plus à mesure que les traitements sont intégrés,
  - Les scanners de tous types
  - Les détecteurs chimiques (mais offre européenne / allemande performante)
- **Le domaine de la cybersécurité** où plusieurs lacunes sont reconnues, telles que firewall, Data Leak Protection, la sécurité de l'IoT, la sécurité des réseaux 5G,
- **Le domaine des traitements de données** dès lors que ceux-ci nécessitent des investissements important et constants, ainsi que des masses critiques de données disponibles et utilisables, notamment sur le plan légal et réglementaire. Cela concerne bien sûr le **Big data** (à noter effort en cours de Thales et Atos pour constituer une offre), l'**IA** pour lequel on observe schématiquement que les experts mondiaux sont français mais les offres dominantes étrangères, l'analyse vidéo, etc.

L'exercice CoFIS sur les technologies de rupture montre de plus que pour la quasi-totalité des domaines émergents le maintien ou le développement de capacités vont constituer de réels défis. Il faut signaler tout particulièrement l'identité numérique, le Cloud, les services en ligne, la Blockchain, mais aussi les drones (filière très éclatée, face à un leader mondial très avancé), la réalité augmentée / virtuelle.

Une politique de déploiement des nouvelles technologies de sécurité bien constituée devra prendre en compte les domaines sur lesquels l'offre française est insuffisante et clairement indiquer si la souveraineté est incontournable, et si elle doit être assurée au niveau national ou européen.

Annexe

Domaines dans lesquels les faiblesses sont reconnues ou potentielles

Les domaines explorés sont rappelés ci-dessous, ceux sur lesquels des faiblesses reconnues ou potentielles de l'offre française sont surlignés en jaune :

Pipame 2015	Technologies critiques 2017	Technos de rupture 2018	AMI et travaux JO (TRL ≤ 6)
Analyse selon un trentaine de segments, trop ancienne pour être reprise intégralement.	- Systèmes de contrôles d'accès électroniques - Détection spécialisée pour risques NRBCE - Observation et Surveillance (local) *(notamment video-protection, traitements, analyse d'images, etc.)* - Technologies cryptographiques - Sondes d'analyse et sondes souveraines de détection - Matériels de chiffrement réseaux - Les technologies de sécurisation du cloud - Logiciel de reconnaissance du locuteur - Logiciel d'exploration internet profond « deep web » - Logiciel de reconnaissance faciale - Intercepteur d'identifiants téléphonie mobile - Détection et interception de signaux à étalement de spectre	- Intelligence artificielle (domaine transverse) - Composants de confiance (domaine transverse) - Internet des objets et objets connectés - Big data & analytique - Conjuguer mondes réels et virtuels - Identification, authentification - Plateformes intégrées véhicules / services - Détecter les produits dangereux, illicites ou contrefaits - Intervenant augmenté - Observation locale - Blockchain - Ubérisation et post ubérisation de la sécurité - Plateformes ouvertes pour la sécurité	**Cyber** - Data Leak Protection - Identité numérique sécurisée - Chiffrement / déchiffrement avancé - Sécurisation des IoT - SOAR (security orchestration automation and response) - UEBA (user and entity behavior analytics) - Outils IA de réponses aux attaques cyber - Sécurité des réseaux 5G **Autres domaines** : se reporter à la contribution du projet JO du CSF

DISPOSITIF FISCAL INCITATIF EN FAVEUR DES ENTREPRISES EXPORTATRICES

Le contrat de filière des industries de sécurité signé en janvier 2020 par la filière et le gouvernement introduit l'importance du développement des exportations de cette industrie de souveraineté en ces termes :

> « La filière s'est forgé une image d'industrie d'excellence qui est aujourd'hui reconnue non seulement sur le territoire national mais également en Europe et dans le monde. Le volume d'exportation, de l'ordre de 50 % du chiffre d'affaires global de la filière, soit 13 Md€, atteste cette reconnaissance au-delà des frontières nationales.
>
> **Le développement des exportations est à la fois une nécessité et une opportunité** pour les industriels de la filière.
>
> **Nécessité** car il ne saurait exister de développement pérenne d'une industrie dans un marché globalisé sans croissance à l'exportation. En particulier, les efforts d'investissements sont tels qu'ils ne peuvent s'appuyer économiquement que sur des volumes d'affaires importants que la seule réponse aux besoins nationaux ne peut satisfaire et ce, de surcroît, dans un contexte budgétaire national toujours plus tendu. La filière regroupant de nombreuses technologies de souveraineté, il est vital de consolider les acteurs du secteur en développant les exportations.
>
> **Opportunité** car les besoins pour plus de sécurité connaissent une croissance soutenue, à fort niveau de résilience au plan mondial, et les ruptures technologiques annoncées (IA, 5G/IOT, etc …) apparaissent comme autant de leviers pour se positionner sur les projets y faisant appel. »

Afin d'améliorer la compétitivité de l'industrie française, le contrat engage l'Etat et la filière à réfléchir à un dispositif fiscal qui soutienne cet objectif. Cette initiative a par ailleurs été reprise par Business France dans ses travaux sur le plan de relance export et figure dans les actions inscrites dans le plan.

On ne peut que partager ces constats et adhérer à la nécessité d'un développement renforcé des exportations de la filière. L'objectif du contrat de filière de créer un dispositif fiscal performant de soutien aux exportations de la filière doit être réaffirmé et les actions concrètes y afférentes engagées dans les meilleurs délais.

La crise sanitaire actuelle, qui se double d'une crise économique marquée, donne un relief particulier à cet objectif puisqu'une des priorités est désormais le renforcement de notre souveraineté, en particulier industrielle. **Cela passe par des mesures favorisant le développement à l'international des entreprises françaises et dont l'ambition doit être supérieure aux mesures existantes.**[1]

[1] https://www.economie.gouv.fr/covid19-soutien-entreprises/les-mesures/plan-de-soutien-aux-entreprises-francaises-exportatrices

Les principes directeurs à retenir pour les travaux à venir quant à la mise au point d'un dispositif fiscal de soutien aux exportations sont :

- **de renforcer la compétitivité de notre filière sur le marché international et, en particulier, d'en faciliter l'accès à nos PME et ETI innovantes.** La complémentarité grands groupes, souvent leaders dans les marchés export, avec ces structures plus petites est ici déterminante et doit être non seulement encouragée mais soutenue.
- **d'élaborer à cette fin un dispositif incitatif[2] favorisant, dans le cadre des marchés d'export, le « chasser en meute », c'est-à-dire le recours pour les entreprises chef de file à des PME et ETI françaises**. Il pourrait par exemple prendre la forme d'un crédit d'impôt qui ne serait accordé qu'en cas de gain d'un marché export, limitant ainsi les dépenses fiscales de l'Etat mais permettant d'afficher *a priori* des offres plus compétitives car intégrant ce potentiel crédit d'impôt.
- **de réserver le dispositif à des entreprises exportant en dehors de l'UE afin** notamment de respecter l'article 87 du Traité CE qui prohibe les aides affectant les échanges entre États membres.

Le coût d'une telle mesure serait à relativiser pour l'État puisque les moindres recettes perçues d'un côté seraient au moins en partie compensées par les recettes supplémentaires générées par le surcroît d'activité du chef de file et des PME/ETI, dans une logique économiquement vertueuse.

Ce dispositif pallierait en outre les limites de l'ex-CICE pointées dans un rapport sénatorial de 2016[3] – il a profité essentiellement à des entreprises non tournées vers l'international et le seuil de 2,5 SMIC ne correspondait pas aux réalités des industries compétitives – **et viserait un objet différent de l'ex-crédit impôt export** (éteint fin 2017) qui permettait le financement des dépenses de prospection commerciale des PME dans la limite de 40 k€.

Pour avancer, un groupe de travail doit être constitué au plus vite avec pour mandat de travailler à la mise au point d'un tel dispositif, associant par exemple l'administration, la représentation nationale et le CSF-IS.

La restitution des conclusions et propositions du groupe de travail devra enfin se tenir dans un calendrier compatible avec l'inscription de cette éventuelle mesure fiscale dans le PLF 2023.

[2] Un tel diapositif pourrait d'ailleurs être retenu pour d'autres industries que celles de la sécurité.
[3] https://www.senat.fr/rap/r15-789/r15-789.html

Réponses

Mission du député Jean-Michel Mis

« Pour un usage responsable et acceptable par la société des technologies de sécurité »

*

1/ Objectifs de la mission

La mission souhaite explorer, lors des auditions et via les contributions écrites, les axes suivants :

- Les **opportunités offertes par les nouvelles technologies au service d'une meilleure offre de sécurité** en analysant les besoins des forces de sécurité, entre autres dans la perspective des grands événements sportifs de 2023 et 2024.

- Les principes nécessaires à **la préservation des libertés** en définissant un cadre d'emploi global et cohérent des technologies de sécurité et en associant la société civile à cette définition pour renforcer la compréhension et l'acceptabilité des nouvelles technologies dans la société.

2/ Questions

La notion de « technologies de sécurité » est large. Quelles sont les principales selon vous ? *[Par exemple : traitement des données (textuelles, images, sonores), biométrie, mobilité.]* Pour quelles finalités ? *[Par exemple : détection de situations, analyse prédictive, suivi des personnes.]*

Les finalités sont diverses mais ont un objectif global de protection des personnes et des biens. Très souvent perçues en France comme permettant une surveillance de masse et par voie de conséquence attentatoires aux libertés et droits fondamentaux, les finalités doivent faire l'objet de la communication nécessaire dans le débat public et auprès du Parlement.

Parallèlement ces mêmes technologies sont désormais utilisées dans des domaines éloignés de la stricte sécurité, en matière de santé publique, de protection des salariés, de contrôle de l'environnement, etc…

- **La reconnaissance faciale : un domaine où les applications sont nombreuses**

La vidéoprotection couplée à des systèmes de reconnaissance faciale constitue un véritable enjeu.

L'utilisation de l'image d'un visage dans la reconnaissance, la comparaison voire l'identification d'individus intéresse fortement le domaine de la sécurité. En phase d'investigation il est ainsi possible de comparer l'image captée avec une base de données pour repérer une personne qui fait l'objet d'un intérêt particulier parce que mis en cause, victime ou témoin. En phase préventive et en temps réel, l'image peut permettre de révéler un indicateur (signal faible) prenant la forme de comportements anormaux afin de préparer la survenue d'un trouble ou d'un désordre qui nécessite une réaction.

L'identification de Mohamed ABRINI « l'homme au chapeau » des attentats de Bruxelles, a d'ailleurs été rendue possible grâce à un logiciel de reconnaissance faciale. S'appuyant sur ce constat, une récente proposition de loi a été déposée par un sénateur en novembre 2018 pour permettre le couplage des informations détenues dans le fichier TAJ (traitement des antécédents judiciaires) avec celles du fichier des personnes recherchées, et de le relier à un système de vidéoprotection. (***Où en est-on ?***). De nombreuses villes parmi lesquelles Nice ont déjà franchi le cap et des adaptations des lois déjà existantes interviendront forcément.

Pour autant, la CNIL n'est pas favorable à la généralisation de la reconnaissance faciale dans tous les lieux publics. *« Si cette technologie n'en est qu'à ses balbutiements, il importe de comprendre que son caractère intrusif est croissant puisque la liberté d'aller et venir anonymement pourrait être remise en cause »*, prévient-elle sur son site. Elle admet toutefois que la vidéosurveillance peut, en tout cas, accélérer le travail des enquêteurs après qu'un attentat a été commis. Après le massacre de Nice, l'itinéraire du criminel avant le drame a ainsi été retracé grâce aux caméras.

En matière de reconnaissance faciale, les limitations ne seront pas forcément techniques mais bien politiques, légales, financières voire philosophiques, et elles se font sentir de façon plus ou moins importante en fonction de la catégorie de personnes à laquelle on s'intéresse.

- **Un besoin de vidéoprotection intelligente**

La reconnaissance faciale peut être utilisée dans le cadre des contrôles d'identité opérés en surveillance des mobilités, pour lutter contre le terrorisme, contre la délinquance itinérante, la pression migratoire et l'insécurité routière. Cette sécurité des mobilités doit se concevoir à l'aune des recours aux nouvelles technologies qui permettent de démultiplier les contrôles et en particulier des outils NEO et des caméras piétons. **Il ne faut pas exclure non plus le couplage de la reconnaissance faciale aux systèmes de lecture automatisée des plaques d'immatriculation permettant de lier un véhicule et les visages du conducteur et de son éventuel passager.**

Son application est aussi envisageable lors de la gestion de troubles forts à l'ordre public pour identifier des casseurs ou des leaders.

Les zones sensibles, musées, ports, aéroports, stades, zones faisant l'objet d'un périmètre de protection prévu par la loi SILT pourraient être équipées de dispositifs fixes ou mobiles permettant d'identifier les personnes (reconnaissance faciale, scanner de la main, ...) et de biper si des interdits de stades, assignés à résidence, personnes recherchées, extrémistes, ..., préalablement rentrés dans une base de données étaient détectés sur ces capteurs (caméras fixes, mobiles, LAPI, téléphones, …). *Le législateur ne l'autorise pas en France, mais au regard du contexte et des récents événements, des adaptations législatives sont envisageables. Pour de nombreux pays, cette application est parfaitement concevable dès aujourd'hui.*

En police judiciaire, les applications sont nombreuses. Les enquêteurs ont besoin, pour leurs affaires de disposer d'outils permettant d'identifier rapidement des personnes, des véhicules et de transmettre des alertes instantanées lors de hits avec des personnes ou de véhicules recherchés ou signalés. Il peut s'agir, par exemple, de caméras placées en des endroits stratégiques (entrées d'immeubles, de locaux particuliers, lieux de culte...) permettant de filmer les visages et de les comparer aux bases.

Le challenge consiste aussi dans la capacité à traiter rapidement les informations de ces enregistrements à l'aide d'outils spécifiques.

La contribution de la vidéoprotection à la résolution des affaires de délinquance de masse atteste de son efficacité. Son couplage à de la reconnaissance faciale pourrait être redoutable. Il faut donc se tourner vers de la vidéoprotection intelligente.

- **Un renseignement criminel qui se heurte aujourd'hui à de nombreux obstacles**

Le renseignement criminel est un élément essentiel pour l'action des forces de sécurité. Il possède des finalités stratégiques et tactiques qui sont à la fois distinctes et complémentaires.

Le premier a pour objectif la création de connaissance concernant les particularités d'un problème de sécurité. Il a en outre la possibilité d'analyser différentes informations quant à l'évolution des phénomènes socio-démographiques, socio-économiques, technologiques et politiques afin de mieux comprendre comment et jusqu'à quel point la criminalité est susceptible d'être affectée par ces changements. Il oriente donc le processus décisionnel et guide les gestionnaires dans le choix de contrôle de la criminalité et des phénomènes criminels prioritaires.

Le second est essentiellement nominatif et permet de mieux connaître une cible criminelle et ce dans une fenêtre de temps plus réduit. Plus particulièrement il s'intéresse aux délinquants, à leurs activités, à leurs réseaux de contacts, aux capitaux qu'ils détiennent et aux autres informations d'ordre personnel. Il est complété par les informations recueillies par les filatures, les écoutes téléphoniques et les informateurs.

Le renseignement criminel se heurte aujourd'hui à l'ampleur des problèmes et au volume d'informations à gérer. Alors que les forces de sécurité s'intéressent à l'action d'une police guidée par le renseignement (ILP – Intelligence-led policing), elles sont confrontées à de nombreux obstacles. Ces derniers proviennent à la fois de la nature même du renseignement, de la rationalité des acteurs qui évoluent dans ce domaine, de la structure organisationnelle des services de police et de la culture des organisations policières.

- **Une masse de données qui nécessite des outils adaptés s'appuyant sur l'intelligence artificielle**

Les services centraux des forces de sécurité constatent que la quantité de données croît exponentiellement et que ce phénomène est continu et durable. De plus les méthodes traditionnelles arrivent à leurs limites et il est indispensable de trouver de nouvelles façons de travailler. Ils se tournent donc vers l'intelligence artificielle pour les appuyer dans cette démarche.

Il s'agit de guider les analystes dans la découverte d'informations pertinentes. Le système doit pouvoir proposer des solutions et des hypothèses possibles, avec des probabilités de réussite en amont.

Pour que le cycle du renseignement soit efficace, l'intelligence artificielle doit permettre de résoudre un certain nombre de points :

- sur l'expression des besoins : pour définir les plans de recherche en réalisant la synthèse des faits passés et en suggérant des besoins en fonction de cas similaires

- sur la collecte : pour dissocier le bruit de l'information (Quoi collecter et dans quel contexte ? Quelle est la fiabilité des informations collectées ?)

- sur le traitement : pour, de manière automatique, nettoyer, fusionner, transformer et restituer les informations.

Il est donc indispensable de pouvoir disposer d'outils d'analyse capables de visualiser une masse de données importantes et de détecter les relations plus pertinentes.

Enfin, il est impératif de diffuser la bonne information à la bonne personne et au bon moment. Cette phase passe par des alertes adaptatives et la suggestion des canaux de diffusion.

Pensez-vous qu'elles permettraient d'anticiper les évolutions des missions de sécurité dans les 10 à 20 ans à venir ? Comment voyez-vous ces évolutions ?

- **Rester attentif à l'évolution des technologies et des usages**

Si les drones n'ont pas été cités dans la question précédente c'est parce qu'ils ne sont pas, en eux-mêmes, une technologie de sécurité. La question n'est en effet pas seulement de développer des technologies de sécurité mais d'intégrer toute technologies utiles au service des missions de sécurité.

Ainsi, il serait probablement présomptueux de penser que les technologies utilisées aujourd'hui ou en cours de développement suffiront à relever les défis de sécurité auxquels notre société sera confrontée dans 20 ans, à l'heure des territoires intelligents, de la 6G, des véhicules volants et autonomes, de la télémédecine, voire des implants électroniques augmentant les capacités humaines.

Comme évoqué dans le document d'accompagnement de ce questionnaire, le Cybercercle recommande la création d'un observatoire des technologies et des usages ayant potentiellement un impact sur les missions de sécurité, afin d'anticiper les évolutions technologiques nécessaires ou d'identifier les nouvelles pratiques de criminalité.

Sur chaque technologie prioritaire évoquée, quel est l'état de développement de l'industrie française ? Que lui manque-t-il pour se perfectionner ?

D'une manière générale, pour favoriser la performance de l'industrie nationale dans ce domaine :

- Les administrations utilisatrices de technologies de sécurité doivent connaître l'offre industrielle et l'état de la recherche (d'où l'observatoire préconisé);
- Un cadre souple d'expérimentation doit exister afin de tester des technologies dans des conditions opérationnelles crédibles (cf proposition du Cybercercle);
- La commande publique doit être plus agile.

Comment les configurations techniques peuvent-elles concilier une utilisation de ces technologies et des garanties pour les libertés (protection des données, contrôles automatisés, etc.) ?

Les cadres d'expérimentation sont souvent mis en avant pour le perfectionnement de ces technologies. Quelles sont selon vous les priorités ? Quels seraient les contours de ces cadres ? A quelles fins ?

Les cadres d'expérimentation sont pertinents mais parfois remis en cause et annulés juridiquement (exemples des drones mis en place par la préfecture de police : annulation par le conseil d'État). Il faut anticiper les risques juridiques et les encadrer de façon précise au regard du RGPD par exemple

en fixant les critères (durée de l'expérimentation, durée de la conservation des données, sanction du non-respect ou exploitation intempestive).

Pour ces raisons, le Cybercercle propose la mise en place d'un cadre d'expérimentation durant laquelle les entités expérimentant la technologie seraient accompagnées par des administrations et autorités indépendantes (cf document d'accompagnement).

*

Ce questionnaire est indicatif et ne prétend pas de couvrir l'intégralité des enjeux posés par les technologies de sécurité. La mission recueillera tout élément qui lui sera apporté afin de l'intégrer au mieux dans sa réflexion.

Contribution-propositions à la mission de M. le député Jean-Michel MIS
« Pour un usage responsable et acceptable par la société des technologies de sécurité »

1. Contexte

Aujourd'hui, le monde se divise en deux catégories, les pays qui innovent et exportent et qui sont le berceau des géants d'internet (GAFAM, BATX)[1] ou des perturbateurs de segments économiques (NATU)[2], et ceux qui tentent de compenser leur domination par la réglementation. L'Europe, à défaut d'avoir su faire émerger des acteurs qui tiennent tête à ces géants, notamment en raison d'un dévoiement idéologique de la politique de concurrence, fait sans aucun doute partie de cette seconde catégorie[3].

Le défi porté par ces groupes mondiaux s'accroît puisqu'ils entendent désormais proposer des alternatives à ce qui était auparavant l'apanage des États - monnaie, identité par exemple. Ils interviennent également en matière morale et culturelle, sans respect a priori pour les législations nationales.

Concrètement, l'Europe, et en premier lieu la France, n'a pas négocié les virages technologiques de ces dernières décennies : l'Internet, le Cloud, la 5G, l'identité numérique et l'Intelligence Artificielle. Par idéologie, des gouvernements français n'ont pas soutenu ou ont laissé partir des entreprises qui seraient aujourd'hui des champions mondiaux (l'équipementier Alcatel par exemple). Par idéologie également – souveraineté mal comprise par exemple – nous nous apprêtons à être dominés en matière de quantique ou de 6G.

Dans le *Livre blanc de la sécurité intérieure* publié fin 2020 par le ministère de l'Intérieur après un travail effectué avec l'ensemble des services, identifie plusieurs technologies pour « porter le ministère de l'Intérieur à la frontière technologique » : identité numérique, biométrie, intelligence artificielle, odorologie, reconnaissance faciale, etc.

Parmi les quelques 200 propositions portées par ce rapport, celles relatives aux technologies visent essentiellement des projets en cours ou d'ores et déjà prévus comme, par exemple :

Proposition :
La première brique du démonstrateur de gilet tactique intelligent visera à permettre la connexion d'une caméra-piéton au terminal afin de permettre la retransmission d'images à un coût raisonnable dès que cela sera juridiquement possible.

Proposition :
Développer dans les cinq prochaines années un projet de PC opérationnel mobile avec des technologies mutualisées « Sécurité intérieure ».

S'il est compréhensible que l'urgence soit à la réponse aux besoins opérationnels en utilisant les technologies existantes, il semble important d'anticiper les technologies à venir et d'être en mesure de faire face aux défis de sécurité que pourront poser les nouveaux usages de ces technologies. Il aura fallu 15 ans pour que l'État arrête sa stratégie en matière de cloud computing[4]. Deux propositions du *Livre blanc* vont d'ailleurs dans ce sens sans toutefois aller au bout de la démarche :

[1] GAFAMI : Google, Amazon, Facebook, Apple, Microsoft, Intel – BHATX : Baidu, Huawei, Alibaba, Tencent, Xiaomi
[2] NATU : Netflix, Airbnb, Tesla, Uber
[3] Avec une difficulté supplémentaire dans une telle situation, c'est que légiférer sur l'existant est un combat quasiment voué à l'échec tant le temps des arcanes législatifs nationales et européennes n'est pas celui de l'innovation.
4 Amazon a lancé ses services cloud en 2006. Le projet Andromède (Numergy, Cloudwatt) lancé en 2011 aura coûté 250 millions d'€ au contribuable sans succès

Proposition :

Formaliser un dispositif d'animation et de pilotage de la recherche et innovation en sécurité intérieure, qui pourrait prendre la forme d'un comité de recherche et d'innovation, aux missions identifiées.

Doter le ministère d'un centre technique pluridisciplinaire, accueillant des cadres et des agents des métiers, des ingénieurs et des techniciens susceptibles de dialoguer avec les acteurs de la recherche et de l'innovation universitaires et industriels, de tester et valider des solutions.

Faire du SAELMI un acteur à part entière de la mise en œuvre de processus de recherche et d'innovation en lui permettant de monter en compétence sur la mise en œuvre de l'innovation via l'encadrement de l'expérimentation avec des industriels et l'achat public d'innovation.

Déployer des outils favorables aux acteurs de la recherche et innovation : une plate-forme ministérielle en ligne consacrée à la recherche et à l'innovation, fédérant de manière souple l'ensemble des acteurs et des ressources, dotée d'un forum, d'un Wiki des projets en cours et des solutions proposées ainsi que d'un annuaire des acteurs et des compétences.

Propositions :

– Autoriser le recours à des technologies émergentes (drones, ballons, caméras-piétons) pour renforcer l'efficacité des professionnels de la sécurité privée et améliorer leur protection.

– Favoriser les expérimentations de dispositifs de sécurité utilisant les nouvelles technologies (lutte anti-drones, technologies d'intelligence artificielle) sur des sites sensibles.

Dans ce contexte global, le CyberCercle avance quelques propositions prenant en compte les travaux du Livre blanc et les expériences passées en matière de technologies ou de cadre juridique.

2. Propositions

Préambule

Il apparaît primordial d'arrêter de courir après les évènements pour lesquels le combat est désormais perdu. Il faut se concentrer sur les grands principes qui peuvent être, par exemple, l'encadrement des usages, enjeu majeur pour anticiper ce qui est à venir et par essence ce qui n'existe pas encore. Se positionner non pas par rapport aux technologies existantes, mais sur les grands principes qui assurent la pérennité et permettent de résister au temps – surtout dans un champ où les évolutions peuvent être très rapides. Qui plus est, sans chauvinisme déplacé, la France est particulièrement experte sur le sujet. Il n'y a qu'à prendre l'exemple de la Directive européenne NIS[5] qui est une résultante des chantiers menés par la France autour de la cybersécurité après l'épisode estonien et dont l'aboutissement national est le volet cybersécurité de la LPM (Loi de programmation Militaire) de 2013. Comment ne pas non plus parler de la Loi Informatique et Liberté de 1978 toujours aussi pertinente aujourd'hui puisque cela a donné naissance en 2016 au RGPD[6]. Quel esprit visionnaire fût celui de la France et de constater qu'un texte vieux de 40 ans est aujourd'hui toujours d'actualité. Lorsque l'on voit l'accélération du nombre de pays à travers le monde qui légifèrent sur le sujet depuis 2020 ne pourrait-on pas imaginer être capable de peser à nouveau à l'international sur d'autres sujets ?

Enfin, encadrer les usages avec en filigrane la protection de nos concitoyens et la préservation de leur vie privée, c'est aussi apporter de la confiance dans les esprits et donc favoriser l'acceptation des technologies. Mais pour cela, il faut avoir une politique globale et ne pas prendre dans le même temps des décisions diamétralement opposées en faisant des choix qui mettent à mal cette confiance. Il doit y avoir une ligne directrice claire sur le sujet et maintenir le cap sur la durée.

Redonner de la confiance, cela passe aussi assurer de la transparence et redonner le contrôle de leurs données aux Français à l'instar de ce que l'Estonie[7] a pu mettre en place : savoir à tout moment qui a eu accès à nos données.

Pour autant, si l'encadrement des usages et la question des fondements éthiques sont primordiaux, il ne faut pas perdre de vue la technologie. Il faut changer notre rapport à l'innovation. Il faut une doctrine pour soutenir l'émergence de projets novateurs, être en capacité de retenir sur notre territoire ces acteurs au lieu

[5] NIS : Network and Information Security (Directive (UE) 2016/1148)

[6] RGPD : Règlement Général pour la Protection des Données

[7] Le prétexte habituel des administrations est d'indiquer que l'Estonie est un petit pays dans lequel il est plus facile de mettre en place le numérique. C'est une preuve complémentaire de l'incompréhension des décideurs sur un des aspects fondamentaux du numérique : la capacité à traiter simultanément un grand nombre de processus et de données.

de les voir aspirer par des intérêts étrangers. C'est un enjeu de souveraineté d'autant plus fondamental sur les questions de sécurité.

Quelques pistes d'actions concrètes

- **Etablir une cartographie de l'existant**

Pour soutenir l'innovation et favoriser leur utilisation par les forces de sécurité, encore faut-il savoir ce qui se passe autour de soi. Comment peut-on aider et soutenir des projets innovants si nous n'avons pas une vision précise de ce qui se fait sur l'ensemble du territoire national ? Il apparaît ainsi indispensable de faire un inventaire exhaustif de l'existant et de faire vivre cet inventaire dans le temps. La souveraineté commence aussi par cet état des lieux. Pour faire un parallèle avec la cybersécurité, c'est comme si l'on demandait à une entreprise de déployer une stratégie de cybersécurité sans qu'elle ait effectué l'inventaire de ses actifs informationnels au préalable. Comment protéger ce qui est inconnu ?
Pour reprendre l'initiative, il faut être à même d'identifier sur notre territoire nos atouts technologiques, ce qui fera la valeur économique de demain et soutenir les acteurs qui la portent.

Autre cartographie à conduire : les besoins de sécurisation de l'existant. Il serait souhaitable d'identifier ce qui est déjà au service des forces de sécurité (technologies, entreprises clés) et ce qui se doit d'être protégé.

- **Mettre en place un observatoire des technologies et des usages utiles à l'action des forces de l'ordre et plus largement aux missions de sécurité**

L'objectif de cet observatoire serait d'identifier d'une part les technologies et les cadres juridiques utilisés à l'étranger susceptibles d'être utiles aux missions de sécurité du ministère, et d'autre part d'identifier les usages susceptibles de poser des défis de sécurité.

Il existe des services aux objectifs comparables[8] au sein du ministère de l'intérieur, mais globalement la mission n'est pas remplie et ne peut l'être en l'état. Afin de ne s'interdire aucun domaine de réflexion, cet observatoire devrait être créé au sein d'une entité interministérielle, par exemple au SGDSN (sous réserve d'une redynamisation de cet organisme), qui présente l'avantage de traiter (théoriquement) du continuum sécurité-défense.

L'observatoire aurait également pour mission d'effectuer un parangonnage des cadres d'emplois des technologies et des cadres juridiques des États-membres de l'Union européenne, afin de mettre en évidence d'éventuels décalages défavorables aux acteurs français de la sécurité, et en particulier aux forces de l'ordre.

L'observatoire pourrait enfin inventorier les technologies et solutions existantes afin de vérifier leurs conditions de sécurité numérique très fortement améliorables pour ce qui concernent certaines d'entre elles (vidéo, contrôles d'accès, drones, etc.) et de mettre en avant les solutions ayant fait leurs preuves.

Un rapport annuel serait transmis au Parlement afin de sensibiliser les parlementaires sur ces questions et d'alimenter d'éventuels débats éthiques ou relatifs au cadre législatif. Ce rapport serait également rendu public.

[8] Plusieurs institutions disposent déjà d'outils proche de ceux d'un observatoire mais elles agissent de manière individuelle et n'échangent pratiquement jamais ou très rarement.
A titre d'exemple, la DPCIS semble effectuer un travail de veille en matière de cybermenace ainsi qu'une veille des chantiers juridiques européens https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000042326064
Elle pilote à cet effet le rapport annuel ministériel sur l'état de la menace.
https://www.interieur.gouv.fr/Actualites/Communiques/L-etat-de-la-menace-liee-au-numerique-en-2019

- **Autoriser a priori l'expérimentation de toutes technologies à des fins de sécurité pour une période de six mois à un an**

L'objectif serait de tester l'utilité éventuelle d'une technologie pour les missions de sécurité avant même d'envisager son déploiement à grande échelle. Un cadre juridique dont l'efficacité serait comparable à celui de la loi informatique et libertés de 1978 serait élaboré afin de ne pas viser une famille de technologies en particulier[9].

En contrepartie de cette autorisation a priori :

- ✓ L'obligation de déclarer l'expérimentation lorsqu'elle touche le public, par exemple auprès du Conseil national du numérique.
- ✓ Cette déclaration ouvrirait l'autorisation d'expérimentation et déclencherait le suivi et l'instruction d'une éventuelle décision d'exploitation sous l'égide du ministère de l'Intérieur (direction des affaires publiques et des affaires juridiques, services du ministères susceptibles d'employer les technologies concernées). La CNIL (données [10]) et l'ANSSI (sécurité numérique) seraient associées à cette instruction. Le CNN pourrait également émettre un avis consultatif.
- ✓ Seraient identifiés les éventuels obstacles à la mise en œuvre des technologies suivies (cadre législatif ou réglementaire, questions éthiques, coûts d'acquisition et de mise en œuvre, etc.).
- ✓ A l'issue de l'expérimentation, si les obstacles sont levés, une autorisation d'exploitation est donnée qui fixe les conditions d'emploi et d'éventuelles limites.

Le ministère remettrait au Parlement un rapport annuel de synthèse des technologies expérimentées (éventuellement protégé par le secret de la défense nationale).

- **Contrôler la mise en œuvre des technologies de sécurité utilisées par le ministère**

Afin de limiter les critiques récurrentes sur leur mise en œuvre, un contrôle des technologies de sécurité utilisées par le ministère de l'Intérieur pourrait être effectué par la CNTCR dont la mission serait élargie aux missions des services de sécurité (un rapprochement des outils utilisés par le renseignement et par les forces de sécurité va d'ailleurs en ce sens – IA, reconnaissance faciale, traitement massif de données, etc..).

Cette instance a fait ses preuves dans le suivi des technologies mises en œuvre par les services de renseignement. Elle a développé une expertise métiers/éthique/débat public exceptionnelle. Elle est crédible y compris auprès des ”libertaires” - bien sûr grâce à la personnalité de son président.

Dans l'hypothèse de l'élargissement de ses missions, ses effectifs devraient évidemment être renforcés.

La CNCTR remettrait un rapport annuel de synthèse (éventuellement protégé par le secret de la défense nationale).

- **Respecter deux lignes rouges**

Malgré la tentation et les demandes récurrentes, les technologies utilisées ou expérimentées dans le cadre des missions de sécurité du ministère ne devraient pas avoir recours :

- ✓ Au piégeage indifférencié de logiciels ou d'équipements.
- ✓ A l'affaiblissement du chiffrement, par la limitation de la taille des clés ou l'introduction de backdoor.

9 Il y aura toujours de nouvelles technologies susceptibles d'améliorer les capacités des forces de sécurité (voir par exemple https://www.technologyreview.com/2019/06/27/238884/the-pentagon-has-a-laser-that-can-identify-people-from-a-distanceby-their-heartbeat/) Elles poseront d'éventuelles questions éthiques ou relativement aux libertés individuelles ou publiques. Le cadre prévu doit toutefois permettre l'expérimentation.

[10] Serait examiné par exemple l'éventuel traitement massif de données par un géant de la tech étranger.

- **Soutenir la filière pme-pmi françaises avec des process adaptés, agiles et favorisant une politique de la demande**

Soutenir l'innovation, c'est aussi arrêter, de construire les politiques publiques de soutien à l'innovation avec comme référent les grands acteurs français dont la taille est un handicap : elles n'ont plus l'agilité nécessaire à l'innovation tous azimuts et sont aujourd'hui entrées dans une certaine philosophie de rente de situation quant aux subsides publics.

Il faut une nouvelle dynamique et donc des process étatiques de soutien à la R&D, allégés et adaptés aux caractéristiques de ces entreprises innovantes de dimension plus restreinte.
Ce besoin d'agilité sur l'innovation au service des forces de sécurité est d'autant plus fondamental que les criminels sont très réactifs quant à l'usage des technologies.

Soutenir l'innovation, ce n'est pas nécessairement et systématiquement injecter de l'argent public. C'est aussi mettre en place les structures qui permettront l'incubation de ces acteurs et les aideront à appréhender les différentes fonctions supports au cours de leur croissance afin qu'ils puissent mettre toute leur énergie dans leur cœur de métier, dans la logique du "startup studio" retenu dans le cadre de la stratégie nationale d'accélération de la cybersécurité[11]

Dans le champ qui nous occupe, c'est aussi favoriser le dialogue public-privé / forces de sécurité – entreprises innovantes afin de favoriser l'innovation au service des acteurs de la sécurité, et avec agilité : faire une politique de la demande et non plus une politique de l'offre. Une telle démarche vertueuse a été mise en œuvre avec succès au ministère de la Santé.

Enfin, identifier les créateurs d'innovation et les soutenir, n'est pas suffisant. Il faut aussi transformer l'essai, passer à l'industrialisation, mais aussi faire en sorte que les pépites perdurent et restent françaises ou européennes, lorsque c'est nécessaire, afin de renforcer le lien sécurité - souveraineté. Les exemples ne manquent pas pour lesquels on peut s'interroger sur le fait de savoir si une réflexion stratégique a été menée par l'État : Morpho, Sentryo, Alsid, Squeer… Il faut se donner les moyens de les retenir, sous réserve de ne pas entraver leur développement.

Sans faire abstraction des enjeux de sécurité nationale, la réponse à cette situation doit inévitablement passer par un partenariat européen. Rien qu'un exemple avec l'Intelligence Artificielle (IA) : En 2018, Amazon est l'entreprise qui a investi le plus dans la recherche (*Garcia-Montero, 2018*)[12], principalement dans l'IA, à hauteur de 22.6Mds$. A titre de comparaison le budget du CNRS (Centre National de la Recherche Scientifique) en 2018 était de 3.7Mds€ (*INISAN-EHRET, 2018*)[13] et la Présidente de la Région Ile de France, Valérie Pécresse, déclarait en octobre 2018 vouloir faire de l'Ile-de-France la capitale européenne de l'IA avec 20M€ d'investissement par an (*Mundubeltz-Gendron, 2018*[14]). Nous sommes sur un facteur 1000 et nous avons clairement un problème d'échelle.

- **Une dimension RH à repenser**

Du fait des règles de fonctionnement RH dans la de nombreuses institutions, on observe aujourd'hui une perte récurrente de l'« Homme Projet », appelé au bout de trois ans à changer de poste – ou, en fonction de

[11] https://www.gouvernement.fr/investissement-d-avenir-annonce-du-laureat-de-l-appel-a-manifestation-d-interet-start-up-studio

[12] Garcia-Montero, C. (2018). *Amazon reste l'entreprise qui investit le plus en R&D dans le monde.* Récupéré sur https://www.journaldunet.com/solutions/reseau-social-d-entreprise/1419678-amazon-reste-l-entreprise-qui-investit-le-plus-en-r-d-selon-statista/

[13] INISAN-EHRET, M.-L. (2018). *LES COMPTES 2018DU CNRS : budget au bilan et des comptes sociaux aux comptes consolidés.* Récupéré sur http://www.dgdr.cnrs.fr/dcif/Chiffres-cles/comptes-2018/Rapport-CNRS-CF-2018.pdf

[14] Mundubeltz-Gendron, S. (2018). [CES 2018] Valérie Pécresse veut faire de l'Ile-de-France une "start-up région". (L. Digitale, Éd.) Récupéré sur https://www.usine-digitale.fr/article/ces-2018-valerie-pecresse-veut-faire-de-l-ile-de-france-une-start-up-region.N636498

ses capacités, à partir dans le privé. Afin que sur les projets innovants un suivi soit assuré au sein de l'Etat, du lancement du sujet à sa mise en œuvre, voire à son MCO et MCS, par des interlocuteurs référents identifiés par l'ensemble des organisations impliquées dans le projet, publiques et privées, il serait fondamental de s'assurer de la pérennité de personnels qualifiés. Aussi pourrait-il être pertinent de promouvoir au sein des institutions, une filière métiers technologiques qui ne répondraient pas aux mêmes règles de gestion de carrière que la filière traditionnelle.

Autre point d'attention au niveau RH : les chefs de projets fonctionnels, qui sont souvent éphémères dans leur poste, n'ont souvent suivi que des formations superficielles sur l'innovation numérique et voient le sujet à travers les offres des salons professionnels où la vente de solutions nouvelles est la priorité. Ils ont gagné rapidement une connaissance de l'état de l'art du numérique sans avoir l'expérience et le recul nécessaire pour prendre les précautions élémentaires pour la sécurité et la pérennité du projet.

Par ailleurs, la diversité des recrutements pourrait complexifier la bonne marche du système, car certains recrutement peuvent se trouver en situation précaire de par leur statut et leur contrat.

Il pourrait ainsi être pertinent de promouvoir-renforcer au sein des institutions une filière métiers technologiques qui ne répondraient pas aux mêmes règles de gestion de carrière que la filière traditionnelle, et plus largement, de repenser une véritable démarche RH quant aux porteurs de projets, techniques ou fonctionnels.

Au-delà de cette proposition de filière RH interne, il serait indispensable de former l'ensemble des utilisateurs de ces technologies innovantes. Le problème est parfois, non pas dans la technologie elle-même, mais bien de son usage. On peut ainsi observer un problème global de sensibilisation, voire de formation, aux nouvelles technologies, qui de fait peut entraîner des problèmes d'usages.

- **Favoriser la diffusion de la connaissance du cadre juridique**

Dans ce contexte, tant les acteurs de l'innovation que les forces de sécurité, doivent évoluer dans un cadre juridique stable et connu. La tentation de créer des textes juridiques à chaque problématique est omniprésente. Or il apparaît que l'arsenal est aujourd'hui suffisant (engorgement complet du J3). Le problème essentiel réside dans sa connaissance, son identification et son interprétation, ainsi que dans la formation au niveau juridique de 'ensemble des acteurs concernés.

Travail collectif des seniors advisors du CyberCercle avec Bénédicte PILLIET, Présidente, en particulier :

Christian DAVIOT

Éric EGEA

Kevin GOMART

Général Jacques HEBRARD

Philippe LOUDENOT

Myriam QUEMENER

MISSION DU DEPUTE JEAN-MICHEL MIS :

« POUR UN USAGE RESPONSABLE ET ACCEPTABLE PAR LA SOCIETE DES TECHNOLOGIES DE SECURITE »

CONTRIBUTION DE DATAKALAB

La présente contribution s'inscrit dans le cadre de la mission *« Pour un usage responsable et acceptable par la société des technologies de sécurité »* confiée à Monsieur le Député Jean-Michel Mis.

Datakalab est une *startup* française spécialisée dans l'analyse d'images à finalité statistique, qui développe des technologies de vision par ordinateur éthiques et *privacy by design*[1]. Datakalab a souhaité répondre au questionnaire soumis et contribuer à cette mission en proposant une évolution du cadre législatif français en matière d'intelligence artificielle, en particulier à finalité sécuritaire.

Alors que la souveraineté numérique est au cœur des débats et que les enjeux sécuritaires sont majeurs, en particulier à l'aube des grands événements sportifs de 2023 et 2024, le cadre légal et règlementaire français actuel ne permet ni aux acteurs privés ni aux acteurs publics et à l'Etat de tirer pleinement partie des opportunités offertes par les nouvelles technologies.

La législation française doit évoluer afin de promouvoir et encadrer le développement de nouvelles technologies d'intelligence artificielle, au rang desquels la vision par ordinateur, et d'encourager l'émergence de champions nationaux respectueux des droits et libertés fondamentaux, particulièrement en matière de vie privée et de protection des données personnelles. C'est la recherche d'un équilibre entre nécessité d'évoluer et d'utiliser les technologies innovantes d'une part, et proportionnalité et respect des libertés fondamentales d'autre part qui doit être au cœur du débat.

Table des matières

PARTIE 1 : Questions posées 2
PARTIE 2 : Pour un encadrement legislatif de la vision par ordinateur 4
ANNEXE : Propositions d'amendements au code de la sécurité intérieure 12

[1] Pour en savoir plus, https://www.datakalab.com/

114 Boulevard Malesherbes 75017 Paris
SASU au capital de 1 000€ - RCS Nanterre : 818 830 275

PARTIE 1 : QUESTIONS POSEES

1. **La notion de *« technologies de sécurité »* est large. Quelles sont les principales selon vous ? [Par exemple : traitement des données (textuelles, images, sonores), biométrie, mobilité.]**

Cette contribution se focalise sur la technologie de **vision par ordinateur**. La vision par ordinateur est une branche de l'intelligence artificielle dont le principal but est de permettre à une machine d'analyser, traiter et comprendre une image prise par un système d'acquisition tel qu'une caméra. La programmation de ces opérations permet à l'utilisateur d'effectuer de manière quasi-instantanée l'analyse d'un grand nombre d'images et d'en retirer un certain nombre d'informations prédéterminées.

En particulier, dans le cadre d'un dispositif de ***edge computing***, le flux vidéo est analysé en temps réel et localement, de sorte que les images ne sont pas stockées, et ne peuvent pas être visionnées sur un moniteur.

2. **Pour quelles finalités ? [Par exemple : détection de situations, analyse prédictive, suivi des personnes.]**

Au rang des applications possibles de la vision par ordinateur se trouvent les usages à finalité statistique pouvant servir en matière sécuritaire : produire des statistiques fondées sur l'analyse automatisée des flux vidéos afin d'optimiser le positionnement des agents sur la voie publique et/ou dans les transports publics ou encore de comptabiliser des densités de personnes.

Cette même technologie peut aussi permettre de détecter des situations, des comportements, compter des objets ou personnes présents sur les images.

Il est important de distinguer la vision par ordinateur de la reconnaissance faciale : si la reconnaissance faciale utilise les technologies d'analyse de vision par ordinateur, elle n'en est qu'un sous-domaine ayant une finalité très précise, à savoir authentifier ou identifier une personne. La reconnaissance faciale n'est pas mise en œuvre par Datakalab est n'est dès lors pas l'objet de la présente contribution.

Par exemple, dans le cadre de la crise sanitaire, Datakalab a développé un dispositif d'analyse en temps réel d'un flux vidéo de caméras installées dans des lieux publics afin de mesurer le taux de fréquentation du lieu et le pourcentage de personnes portant un masque de protection sanitaire ; cette technologie anonymise les images en temps réel, sans aucune visualisation possible des images ni stockage de données à caractère personnel. Cette technologie peut également être utilisée pour compter des personnes ou des densités de population dans une zone donnée.

3. **Pensez-vous qu'elles permettraient d'anticiper les évolutions des missions de sécurité dans les 10 à 20 ans à venir ? Comment voyez-vous ces évolutions ?**

L'usage des technologies de vision par ordinateur à finalité sécuritaire est déjà dans le débat public sans pour autant être aujourd'hui encadré. Ces technologies seront très certainement la norme dans ce domaine d'ici 10 à 20 ans.

4. **Sur chaque technologie prioritaire évoquée, quel est l'état de développement de l'industrie française ? Que lui manque-t-il pour se perfectionner ?**

Datakalab a souhaité faire part de son expérience et en tirer les conséquences dans le cadre de la présente contribution, en proposant des pistes d'évolution du cadre législatif français en matière de vision par ordinateur. Il est renvoyé à la **PARTIE 2** ci-dessous.

5. **Comment les configurations techniques peuvent-elles concilier une utilisation de ces technologies et des garanties pour les libertés (protection des données, contrôles automatisés, etc.) ?**

Datakalab est convaincue que l'utilisation des technologies innovantes de sécurité peut intégrer des garanties fortes pour les droits et libertés des personnes. Datakalab propose de :

- **Préconiser des solutions d'IA embarquées pour garantir confidentialité et performance dans les analyses.** La majorité des solutions d'IA s'appuie sur des solutions dans un serveur centralisé ou dans le cloud, tant pour l'apprentissage (créer un modèle d'IA à partir de bases de données) que pour l'inférence (analyser des données nouvelles).

  Par construction, il y a donc une séparation entre l'endroit où les données sont capturées (une caméra par exemple) et celui où ces données sont analysées. Si on veut remettre en question ce découpage, il faut sortir l'IA du cloud et la rapprocher de ses utilisateurs.

  Deux besoins majeurs viennent conforter ce changement de paradigme :
  - La confidentialité : L'IA embarquée, c'est-à-dire la capacité pour un système d'exécuter localement des algorithmes évolués d'IA, permet de conserver les données en local. Cela est critique pour toutes les applications qui manipulent des données personnelles confidentielles, en particulier pour le domaine de la sécurité et qui doivent garantir le droit à la vie privée,
  - Le temps de décision : Le temps d'échange de données entre un capteur et un serveur situé dans le cloud n'est pas négligeable si on veut garantir une analyse non biaisée, il faut donc optimiser ce temps de décision en la rendant locale

- **Certifier les modes d'apprentissages IA au service de l'analyse d'image.** A l'exemple de centres d'excellence tels que le CEA, des programmes de qualification des modes d'apprentissage IA ont été initiés autour de :
  - la confiance vue des utilisateurs par la mise en place de modèles et mécanismes de compréhension globale du fonctionnement d'une IA et d'explication des résultats qu'elle produit dans son contexte d'usage et celui des utilisateurs;
  - la confiance par des méthodes outillées d'assurance de la conformité des IA à des processus et référentiels de développement et de certification;
  - la confiance par l'exemple via la conception et l'évaluation de cas applicatifs de référence.
    Ce type d'organismes doit, selon nous, servir d'appui pour définir ces standards et préciser les processus de qualification de ces bases d'apprentissages

6. **Les cadres d'expérimentation sont souvent mis en avant pour le perfectionnement de ces technologies. Quelles sont selon vous les priorités ? Quels seraient les contours de ces cadres ? A quelles fins ?**

Il est renvoyé aux développements de la **PARTIE 2** ci-dessous.

PARTIE 2 : POUR UN ENCADREMENT LEGISLATIF DE LA VISION PAR ORDINATEUR

1. UN CADRE LEGISLATIF ET REGLEMENTAIRE FRANÇAIS INADAPTE A LA TECHNOLOGIE DE VISION PAR ORDINATEUR

Le cadre légal et règlementaire français ne permet pas le développement pérenne et l'encadrement efficace des technologies de vision par ordinateur. Cette situation est la source d'une insécurité juridique importante : d'abord pour la population qui se retrouve exposée à des technologies non régulées, et ensuite pour les acteurs du secteur, sociétés productrices de ces technologies bloquées dans leur développement, et entités publiques et privées utilisatrices réticentes à expérimenter ces technologies. L'expérience de Datakalab illustre ces difficultés.

1.1. Vision par ordinateur et traitement de données à caractère personnel

Dès lors que la vision par ordinateur implique la captation et l'utilisation de l'image des personnes se trouvant dans le champ des caméras, son usage implique un traitement de données à caractère personnel et est donc soumis à la réglementation applicable en la matière (le RGPD[2] et la loi dite Informatique et Libertés[3]), y compris lorsque les images sont anonymisées à très bref délai[4].

La directive « Police-Justice »[5] (transposée au sein du chapitre XIII de la loi Informatique et Libertés) s'applique lorsque le traitement est réalisé (i) par une autorité publique ou ayant des prérogatives de puissance publique, et (ii) 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, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces.

Ce cadre général de la protection des données à caractère personnel s'applique indifféremment, quelle que soit la technologie utilisée afin d'effectuer le traitement.

1.2. Illustration : les blocages rencontrés dans le déploiement d'un dispositif statistique de détection algorithmique du port de masque sanitaire dans les lieux publics

Dans le cadre de la crise sanitaire actuelle, Datakalab a développé dès le mois d'avril 2020 des algorithmes capables de **quantifier statistiquement le port du masque de protection sanitaire, en utilisant des techniques de vision par ordinateur**. Le dispositif est basé sur des caméras auxquelles sont adossées un mini-ordinateur local capable de traiter les flux d'images en temps réel, en les anonymisant immédiatement afin de ne conserver que des lignes de données agrégées indiquant le nombre de personnes passant devant une caméra, et parmi elles, le nombre de personnes portant un masque.

[2] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE
[3] Loi no 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, plus connue sous le nom de loi informatique et libertés
[4] La notion de bref délai s'entend ici comme le temps nécessaire aux machines pour réaliser les opérations d'anonymisation afin de limiter le risque qu'un humain puisse, avec des moyens raisonnables, accéder aux données identifiantes. La CNIL préconise à ce titre une durée maximale de cinq minutes au-delà de laquelle aucune donnée identifiante ne doit être conservée. (voir : Dispositifs de mesure d'audience et de fréquentation dans des espaces accessibles au public : la CNIL rappelle les règles | CNIL)
[5] 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

Ce dispositif a intéressé plusieurs acteurs afin d'avoir de la visibilité sur le port du masque dans des lieux publics, et en particulier dans les transports publics, permettant ainsi de disposer d'outils de pilotage chiffrés et d'organiser un déploiement adapté des ressources afin de faire de la sensibilisation à l'importance du port du masque par exemple.

Datakalab a contacté la Commission Nationale de l'Informatique et Libertés (« CNIL ») dès avril 2020 pour obtenir son avis et ses recommandations sur ce dispositif. **La CNIL a salué les garanties fortes en matière de protection des données personnelles** intégrées dans le dispositif (***privacy-by-design***), et en particulier l'anonymisation à très bref délai et son renforcement par un système d'agrégation des données, l'absence de stockage des images des caméras, l'absence de suivi des personnes, l'absence de traitement de données biométriques etc.

Toutefois, **la CNIL a émis des réserves relatives à l'exercice du droit d'opposition** des personnes concernées[6] :

- Selon la CNIL, l'exception au droit d'opposition prévue pour les finalités statistiques nécessaires à l'exécution d'une mission d'intérêt public[7] est inapplicable dès lors que la détermination des taux de fréquentation et de port de masques en un lieu déterminé ne serait pas une finalité statistique au sens de la règlementation applicable ;

- Selon la CNIL, les modalités du droit d'opposition proposé par Datakalab (faire « non de la tête » devant la caméra entrainant la suppression de la ligne de données correspondantes) et intégré au dispositif ne sont pas satisfaisantes puisque : (i) il « *contraint les individus à afficher publiquement leur opposition au traitement* » et serait « *difficilement généralisable, particulièrement à grande échelle* », (ii) il ne permet pas aux personnes passant dans le champ de la caméra d'exercer leur opposition préalablement au traitement, mais uniquement en cours de traitement ; en l'état actuel de sa doctrine[8], la CNIL ne propose pas de modalité d'exercice alternative du droit d'opposition ;

- En conséquence, la CNIL a considéré que : « *le dispositif envisagé ne pourra être valablement mis en œuvre que dans les conditions prévues par l'article 23 du RGPD, à savoir que toute limitation des droits des personnes, en l'espèce leur droit d'opposition,* ***doit être prévue par un texte spécifique du droit de l'Union ou d'un Etat membre qui doit comporter des dispositions spécifiques*** ».

C'est donc la difficulté de mise en œuvre pratique du droit d'opposition qui a bloqué le déploiement du dispositif proposé par Datakalab, et ce malgré l'intérêt général de la solution.

1.3. L'interprétation stricte du cadre légal et règlementaire ne permet pas l'expérimentation et le développement de la vision par ordinateur française

S'agissant de la notion de droit d'opposition, deux points d'interprétation du cadre législatif et règlementaire méritent d'être évoqués.

[6] Article 21 du RGPD
[7] L'article 21.6 du RGPD indique : *« Lorsque des données à caractère personnel sont traitées à des fins de recherche scientifique ou historique ou à des fins statistiques en application de l'article 89, paragraphe 1, la personne concernée a le droit de s'opposer, pour des raisons tenant à sa situation particulière, au traitement de données à caractère personnel la concernant, à moins que le traitement ne soit nécessaire à l'exécution d'une mission d'intérêt public. »*
[8] Voir Fiche de la CNIL sur les caméras thermiques « FAIRE « NON » DE LA TÊTE : UNE MODALITÉ D'OPPOSITION INSUFFISANTE ET PEU PRATIQUE », ici : https://www.cnil.fr/fr/cameras-dites-intelligentes-et-cameras-thermiques-les-points-de-vigilance-de-la-cnil-et-les-regles

Premièrement, l'article 21.6 du RGPD prévoit une exception au droit d'opposition lorsque les données à caractère personnel sont traitées à des fins statistiques nécessaires à l'exécution d'une mission d'intérêt public :

Le Considérant 162 du RGPD définit les finalités statistiques comme : *« **toute opération de collecte et de traitement de données à caractère personnel nécessaires pour des enquêtes statistiques** ou la production de résultats statistiques. Ces résultats statistiques peuvent en outre être utilisés à différentes fins, notamment des fins de recherche scientifique. **Les fins statistiques impliquent que le résultat du traitement à des fins statistiques ne constitue pas des données à caractère personnel mais des données agrégées**, et que ce résultat ou ces données à caractère personnel ne sont pas utilisés à l'appui de mesures ou de décisions concernant une personne physique en particulier. »*[9]

Si cette disposition indique clairement que les résultats statistiques peuvent être utilisés à différentes fins, notamment de recherche, et que les résultats doivent être des données agrégées, rien n'oblige à ce que les résultats statistiques soient utilisés à des fins de recherche scientifique[10]. La loi Informatique et Libertés ne restreint pas d'avantage le périmètre de la notion de traitement à des finalités statistiques[11].

En conséquence, les textes applicables pourraient être interprétés afin de permettre aux dispositifs basés sur des technologies de vision par ordinateur déployées pour des finalités statistiques nécessaires à l'exécution d'une mission d'intérêt public, de bénéficier de la dérogation au droit d'opposition.

Deuxièmement, l'article 21 du RGPD qui définit les contours du droit d'opposition n'impose pas que celui-ci doive s'exercer nécessairement en amont du traitement, ni qu'il ait un caractère privé.

L'exercice du droit d'opposition peut survenir *« à tout moment »* et aucune disposition ne prévoit de droit d'opposition préalable au traitement. Cela ressort clairement de la rédaction du RGPD[12], des lignes directrices du groupe de travail Article 29[13] et de la doctrine de plusieurs autorités de protection des données européennes[14].

---

[9] Voir Considérant 162 du RGPD, voir aussi en ce sens l'Avis 03/2013 du Groupe de travail Article 29 sur la limitation des finalités (00569/13/EN WP 203) : *« Les "fins statistiques", en particulier, couvrent un large éventail d'activités de traitement, allant des fins commerciales (par exemple les outils analytiques des sites web ou les grandes applications de données destinées aux études de marché) aux intérêts publics (par exemple les informations statistiques produites à partir des données collectées par les hôpitaux pour déterminer le nombre de personnes blessées à la suite d'accidents de la route). »*

[10] La présence des termes *« en outre » et « notamment »* montre bien qu'il ne s'agit que d'une possibilité parmi d'autres et non d'une limitation stricte

[11] L'article 78 de la loi informatique et libertés renvoie en la matière vers le Décret 2019-536 lequel indique de manière large en son article 116 : *« Les dérogations (…) relatif aux traitements (…) à des fins statistiques s'appliquent uniquement dans les cas où les droits prévus aux articles 15, 16, 18 et 21 du règlement (UE) 2016/679 du 27 avril 2016 susvisé risqueraient de rendre impossible ou d'entraver sérieusement la réalisation des finalités spécifiques et où de telles dérogations sont nécessaires pour atteindre ces finalités. »*

[12] Voir Article 21.3 du RGPD *« Lorsque la personne concernée s'oppose au traitement à des fins de prospection, les données à caractère personnel **ne sont plus traitées à ces fins**. »* voir également la rédaction initiale de la Commission : *« Lorsqu'il est fait droit à une opposition conformément aux paragraphes 1 et 2, le responsable du traitement **n'utilise ni ne traite plus les données à caractère personnel concernées.** »*
voir : https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:52012PC0011&from=EN

[13] les lignes directrices du groupe de travail « Article 29 » concernant la prise de décision individuelle automatisée et le profilage soulignent que : « Une fois que la personne concernée exerce ce droit, le responsable du traitement doit interrompre (ou éviter de démarrer) le traitement à moins qu'il ne puisse démontrer des motifs légitimes et impérieux qui l'emportent sur les intérêts, les droits et libertés de la personne concernée. Le responsable du traitement peut également être amené à effacer les données personnelles données. » voir : https://www.cpdp.bg/userfiles/file/WP29/wp251rev01_fr.pdf

[14] Selon l'autorité de protection irlandaise : «[…] **le responsable du traitement des données doit arrêter le traitement dès qu'il reçoit votre objection**. » voir : https://www.dataprotection.ie/en/individuals/know-your-rights/right-object-processing-personal-data-article-21-gdpr, voir également en ce sens l'interprétation de l'autorité de protection britannique : https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-object/

Quant au caractère public ou privé de l'opposition, cette notion est étrangère au cadre législatif et réglementaire applicable qui n'impose aucune modalité d'exercice et encourage *« l'utilisation de procédés automatisés utilisant des spécifications techniques »*[15].

Le déploiement des technologies de vision par ordinateur implique nécessairement l'adaptation de la réglementation en matière de droit d'opposition, soit par des exceptions à son application, soit par la mise en œuvre de modalités nouvelles d'exercice du droit d'opposition.

1.4. Le décret du 10 mars 2021 : un cadre d'expérimentation inédit pour la technologie de vision par ordinateur

Tirant les conséquences de l'analyse de la CNIL, Datakalab et ses clients ont cherché à recourir au mécanisme de l'article 23 du RGPD, rarement mis en œuvre[16], qui permet de déroger à l'application du droit d'opposition par voie de mesure législative ou règlementaire (loi, décret, règlement ou arrêté).

Le 10 mars 2021, le décret relatif au recours à la vidéo intelligente pour mesurer le taux de port de masque dans les transports a été adopté[17]. Ce décret permet le déploiement encadré de technologies de visions par ordinateur par les gestionnaires des transports publics et espaces affectés au transport, pour une durée d'un an, afin de mesurer le taux de port de masque dans les transports.

Ce décret est une grande avancée pour le développement des technologies de vision par ordinateur. Ce décret donne un premier cadre d'expérimentation pour un usage encadré et éthique de ces technologies. L'expiration de la période d'un an autorisée par le décret sera l'occasion de faire un point sur les usages qui auront été déployés, leur utilité et leur impact sur les libertés et droits fondamentaux.

Si l'adoption de mesures règlementaires pour autoriser et encadrer l'usage des technologies de vision par ordinateur est une voie est envisageable, elle présente néanmoins des inconvénients. En particulier, le risque de multiplication des textes règlementaires (source de potentielles incohérences), les délais longs d'adoption et les périmètres restreints sont autant de freins pour les producteurs et utilisateurs de ces solutions. A cela s'ajoute les délais allongés des processus de commande publique.

Enfin, la nécessité d'un débat sociétal sur la question de la vision par ordinateur et, plus généralement, de l'intelligence artificielle dicte de passer par un processus législatif.

2. UN ENCADREMENT LEGISLATIF NECESSAIRE DE LA TECHNOLOGIE DE VISION PAR ORDINATEUR

2.1. L'opportunité de légiférer au niveau national

[15] Article 21.5 du RGPD
[16] Ceci a été souligné par la CNIL dans son avis sur le Décret autorisant la détection de masques dans les transports : https://www.cnil.fr/fr/avis-sur-le-decret-video-intelligente-port-du-masque
[17] Voir Décret n° 2021-269 du 10 mars 2021 relatif au recours à la vidéo intelligente pour mesurer le taux de port de masque dans les transports Décret n° 2021-269 du 10 mars 2021 relatif au recours à la vidéo intelligente pour mesurer le taux de port de masque dans les transports - Légifrance (legifrance.gouv.fr)

La France a été pionnière en Europe quant à la protection des données liées à la société de l'information : sa première loi sur la protection des données personnelles date de 1978 (loi Informatique et Libertés), soit quarante ans avant l'adoption européenne du RGPD.

Depuis plusieurs années, de nombreux acteurs, groupes de réflexion et institutions se sont emparés des enjeux de l'intelligence artificielle. Comme cela est souligné par le rapport du gouvernement *« France IA »*, ces initiatives ont permis de mettre en évidence l'excellence de la recherche française dans le domaine de l'IA et son potentiel de transfert pour des applications industrielles, *« cependant, elles pointent aussi le risque pour la France de se faire distancer rapidement sur un terrain où la suprématie est assurée à l'heure actuelle par les grandes entreprises américaines et asiatiques »*[18]

Au niveau européen, **une proposition de règlement établissant des règles harmonisées sur l'intelligence artificielle**[19] a été publiée en avril 2021. Le texte propose de mettre en place de nouvelles obligations graduées selon le niveau de risques des technologies et propose un système de supervision et de sanctions par des autorités nationales, avec pour objectif de stimuler la compétitivité de l'Union Européenne dans le domaine de l'IA[20].
Cette proposition n'étant qu'au début de la procédure législative ordinaire, son adoption peut prendre plusieurs années[21]. **A l'aube de la présidence française du Conseil de l'Union Européenne, il est crucial que la France s'empare du sujet[22].**

2.2. Propositions d'encadrement législatif des technologies de vision par ordinateur

2.2.1. Une loi spéciale pour les technologies d'intelligence artificielle

La première proposition consiste à positionner la France, à la veille de sa présidence du Conseil de l'UE, en laboratoire de la règlementation en matière d'IA (y compris de vision par ordinateur).

Cette loi, en accord avec les principes d'ores et déjà mis en avant par le projet de règlement européen, pourrait être basée sur une approche par les risques : les règles applicables aux fournisseurs de solutions utilisant l'intelligence artificielle doivent être **proportionnées à l'intensité des risques pour les droits et libertés des personnes**[23]. Contrairement à un encadrement

[18] Voir Rapport de Synthèse France intelligence artificielle, ici :
https://www.vie-publique.fr/sites/default/files/rapport/pdf/174000247.pdf
[19] Proposition de règlement du 21 avril 2021 établissant des règles harmonisées sur l'intelligence artificielle, disponible ici en anglais : https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence Ce projet de règlement fait suite au Livre blanc **« Intelligence artificielle »** de la Commission européenne publié le 19 février 2020.
[20] Communication from the Commission to the European Parliament, the Council, the European economic and social committee and the Committee of the regions – COM (2021) 205 final – 21/04/2021, disponible ici :
https://digital-strategy.ec.europa.eu/en/library/communication-fostering-european-approach-artificial-intelligence
"*By earning people's trust, the envisaged risk-based legislation should foster the uptake of AI across Europe and boost Europe's competitiveness. The Commission's proposal therefore pursues the twin objectives of addressing the risks associated with specific AI applications in a proportionate manner and of promoting the uptake of AI.*"
[21] Cette procédure peut, en pratique, prendre plusieurs années avant qu'un texte ne soit définitivement adopté. La procédure d'adoption ordinaire se décompose en trois parties. La Commission, qui dispose du monopole de l'initiative législative, propose dans un premier temps un texte, qui est transmis simultanément au Parlement européen et au Conseil de l'Union européenne. Dans un second temps, le Parlement se prononce à la majorité simple, en amendant, rejetant ou en approuvant la proposition de la Commission. Le Conseil peut ensuite accepter la proposition du Parlement, ou adopter une position différente, qui fera l'objet d'une seconde lecture au Parlement. Dans un troisième temps, si le Conseil n'accepte pas les amendements proposés par le Parlement, alors le Comité de conciliation est convoqué. En cas d'accord sur le texte dans le cadre du Comité de conciliation, celui-ci doit encore être confirmé par le Conseil et le Parlement en troisième lecture.
[22] D'après le Considérant (1) de la proposition de règlement précitée, les Etats membres ne seront plus autorisés à imposer des restrictions à la commercialisation des solutions basées sur l'intelligence artificielle, si ces restrictions ne sont pas expressément prévues par le projet de règlement
[23] Voir considérant 14 de la proposition de règlement : *In order to introduce a proportionate and effective set of binding rules for AI systems, a clearly defined risk-based approach should be followed. That approach should tailor the type and content of such rules to the intensity and scope of the risks that AI systems can generate. It is therefore necessary to prohibit certain artificial intelligence practices, to lay down requirements for high-risk AI systems and obligations for the relevant operators, and to lay down transparency obligations for certain AI systems.*

indifférencié[24], cette approche permet de focaliser la supervision et le contrôle des autorités sur les technologies présentant le plus de risques[25].

Plusieurs **principes directeurs** contenus dans la proposition de règlement pourraient être développés dans le cadre d'une initiative législative nationale :

- Préalablement à la mise sur le marché des IA, une évaluation de conformité pourrait être mise en place pour les systèmes présentant de forts risques pour les personnes[26]. Cette évaluation pourrait être effectuée soit par un organisme tiers, soit selon des procédures internes prédéfinies, en fonction du niveau de risques;
- Tout au long du développement et de l'utilisation des IA, les producteurs pourraient être soumis à des obligations de documentation[27], et de transparence[28] sous réserve de la confidentialité de certaines informations[29] ;
- La non-conformité pourrait être sanctionnée en fonction de la gravité de la violation[30]. La supervision de la mise en œuvre du cadre légal ainsi que le prononcé des sanctions devraient être confiés à une autorité nationale indépendante et spécialisée[31].

Ainsi par exemple, parmi les systèmes basés sur des technologies de vision par ordinateur, les obligations applicables aux systèmes de reconnaissance faciale en temps réel ne devraient pas être les mêmes que celles applicables aux technologies ayant pour finalité exclusive la production statistique, comme celles développées par Datakalab.

---

[24] Proposition de règlement établissant des règles harmonisées sur l'intelligence artificielle – Explanatory memorandum - §3.1 "*Using a risk-based framework was considered a better option than blanket regulation of all AI systems. The types of risks and threats should be based on* ***a sector-by-sector and case-by-case approach****. Risks also should be calculated taking into* ***account the impact on rights and safety****"*

[25] Proposition de règlement établissant des règles harmonisées sur l'intelligence artificielle – Explanatory memorandum - §3.3 "*By requiring a restricted yet effective set of actions from AI developers and users, the preferred option limits the risks of violation of fundamental rights and safety of people and* ***foster effective supervision and enforcement, by targeting the requirements only to systems where there is a high risk that such violations could occur****."*

[26] Proposition de règlement établissant des règles harmonisées sur l'intelligence artificielle – Explanatory memorandum - §1.1 "*Those AI systems* (high-risks) *will have to comply with a set of horizontal mandatory requirements for trustworthy AI and follow conformity assessment procedures* ***before those systems can be placed on the Union market****."*

[27] Le chapitre 2 relatif aux systèmes d'intelligence artificielle à haut risque de la proposition de règlement prévoit, notamment, des obligations de **documentation des initiatives mises en œuvre pour atténuer les risques identifiés par le producteur** (article 9), des **caractéristiques techniques du système** (article 11), ou que les fournisseurs de systèmes à haut risque **conservent les journaux générés automatiquement par leurs systèmes** (« *logs* »), dans la mesure où ces journaux sont sous leur contrôle. Cette obligation de documentation a déjà été consacré par le RGPD.

[28] L'article 13 de la proposition de règlement notamment, prévoit que les systèmes à haut risque sont conçus et développés de manière à ce que leur fonctionnement soit suffisamment **transparent** pour permettre aux utilisateurs d'interpréter les résultats du système et de les utiliser de manière appropriée. Avant toute utilisation, les utilisateurs devraient se voir délivrer un certain nombre d'informations relatives, entre autres, aux **caractéristiques du système, à ses performances, ou encore à son niveau de précision et de sécurité**. La teneur des informations devant être délivrées au public dépend du niveau de risque du système (voir l'article 52 de la proposition de règlement pour les obligations de transparence applicables aux systèmes présentant peu de risques).

[29] L'article 70 de la proposition de règlement prévoit que les autorités nationales doivent respecter la confidentialité de certaines informations des fournisseurs de systèmes d'intelligence artificielle. Ainsi, les informations protégées au titre de la **propriété intellectuelle**, du **secret d'affaire ou des savoir-faire** sont couvertes par cette obligation de protection de la confidentialité incombant aux autorités nationales, sous réserve des limites prévues par la directive 2016/943 sur la protection des savoir-faire et des informations commerciales non divulgués (secrets d'affaires) contre l'obtention, l'utilisation et la divulgation illicites. Le règlement prévoit explicitement que le code source doit bénéficier de la confidentialité des informations.

[30] En ce sens, l'article 71 de la proposition de règlement prévoit une amende administrative en cas de violation du règlement. Le montant maximal de l'amende dépend **d'une part du niveau de risque des systèmes dont il est question**, et d'autre part **de la nature des obligations violées**. L'amende maximale autorisée par la proposition de règlement s'élève à 30 millions d'euros, ou 6% du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu.

[31] L'article 59 de la proposition de règlement prévoit que les Etats membres devront désigner une ou plusieurs autorités compétentes chargées d'assurer l'application et la mise en œuvre du règlement. Les autorités nationales compétentes sont organisées de manière à **garantir l'objectivité et l'impartialité de leurs activités et de leurs tâches**. Elles peuvent fournir des recommandations et conseils sur la mise en œuvre du règlement. Au niveau européen, l'article 56 prévoit la création d'un Conseil européen de l'intelligence artificielle (« *European Artificial Intelligence Board* ») chargé, entre autres, d'assurer l'uniformisation des pratiques administratives des Etats membres, ainsi que d'émettre des avis, recommandations et contributions relatives aux obligations applicables aux systèmes d'intelligence artificielle à haut risque.

2.2.2. L'adaptation du cadre légal existant afin de permettre l'usage des technologies de vision par ordinateur à des finalités sécuritaires

Le cadre légal et règlementaire actuel ne permet pas le déploiement de technologies de vision par ordinateur à des finalités sécuritaire en France. Non seulement la France se prive de l'opportunité d'utiliser de nouveaux outils utiles en matière de sécurité, mais en plus, cela bloque l'émergence de champions nationaux dans le domaine de la vision par ordinateur.

Les dispositions du Code de la sécurité intérieure (« CSI ») qui encadrent le régime juridique de la **vidéoprotection**, permettent la mise en place de systèmes de vidéoprotection assurant la transmission et l'enregistrement d'images prises sur la voie publique, sur autorisation préfectorale. Toutefois, à l'analyse de ce régime, un constat s'impose : **seul le traitement des images par visionnage par des êtres humains est prévu au sein de ce régime** (L.252-2 CSI). La vision des images par ordinateur est donc automatiquement exclue, même dans le cas du simple ajout d'une couche logicielle à des systèmes de vidéoprotection existant, qui ont pourtant été expressément autorisés par la préfecture.

Le ministère de l'Intérieur expose dans son Livre Blanc de la Sécurité Intérieure[32] de novembre 2020 la nécessité pour les services publics de construire une politique des données et de mobiliser les technologies d'intelligence artificielle qui sont, rappelle-t-il, avant tout des outils d'aide à la décision[33]. L'étude souligne également que le déploiement de dispositifs d'intelligence artificielle permettrait de faciliter le travail des agents en leur apportant de la donnée agrégée, et en fournissant des outils qui permettent de synthétiser l'information pour les aider à travailler de façon efficace[34].

Le législateur doit se saisir de ce sujet et réformer le régime juridique de la vidéoprotection pour y intégrer un usage raisonné et éthique des technologies de vision par ordinateur, en particulier via leur déploiement au sein des systèmes de vidéoprotection, dans la mesure où elles sont strictement encadrées.

Il est proposé, en **ANNEXE** à la présente contribution, des amendements au Code de la Sécurité Intérieure afin de :

- Moderniser le régime de la vidéoprotection afin d'y intégrer l'analyse d'images par ordinateur ;
- Prendre en compte la protection des données à caractère personnel dans le régime de la vidéoprotection ;
- Etendre le périmètre des finalités de la vidéoprotection afin d'y intégrer la sécurité sanitaire.

[32] Livre Blanc de la Sécurité Intérieur – Ministère de l'Intérieure, publication du 16 novembre 2020, accessible ici : https://www.interieur.gouv.fr/Actualites/L-actu-du-Ministere/Livre-blanc-de-la-securite-interieure
[33] Voir Livre Blanc « 3.2. Construire une politique des données et mobiliser les technologies d'intelligence artificielle »
[3434] Voir Livre Blanc page 248 « L'apprentissage machine »

2.2.3. Un cadre national expérimental à l'horizon 2024

Les propositions susvisées d'encadrement général des technologies d'intelligence artificielle et d'encadrement de leur usage sécuritaire peuvent passer par une phase intermédiaire expérimentale, et ce conformément à l'article 37-1 de la Constitution[35].

La phase expérimentale doit permettre le développement d'une IA française éthique et performante, qui pourra notamment être déployée à des finalités sécuritaire à l'occasion des Jeux Olympiques 2024.

L'expérimentation a déjà porté ses fruits pour pousser l'innovation dans des secteurs dans lesquels la protection des personnes est primordiale[36] et peut offrir une solution temporaire à la France pour se positionner en tant que puissance technologique et pionnière de la protection des droits des personnes.

[35] *La loi et le règlement peuvent comporter, pour un objet et une durée limités, des dispositions à caractère expérimental.*
[36] Par exemple, dans le secteur de la santé, la loi de financement de la sécurité sociale pour 2018 a introduit, en son article 51, un dispositif permettant d'expérimenter de nouvelles organisations en santé reposant sur des modes de financement inédits qui a permis le développement de nombreuses startup française innovantes en santé, voir : https://solidarites-sante.gouv.fr/systeme-de-sante-et-medico-social/parcours-des-patients-et-des-usagers/article-51-lfss-2018-innovations-organisationnelles-pour-la-transformation-du/article-51

ANNEXE : PROPOSITIONS D'AMENDEMENTS AU CODE DE LA SECURITE INTERIEURE

MODERNISER LE REGIME DE LA VIDEOPROTECTION POUR Y INTEGRER LA VISON PAR ORDINATEUR

- **PROPOSITION n°1 :**

Il est proposé d'ajouter à l'article L.252-2[37] du CSI un troisième alinéa rédigé ainsi :

> « *Dans les cas prévus à l'article L. 251-2, le visionnage des images peut également être assuré au moyen de technologies de vision par ordinateur sans intervention humaine, dès lors que ces technologies assurent une anonymisation en temps réel des images sans stockage de celles-ci, et que les données conservées ne permettent pas d'identifier une personne, directement ou indirectement.* »

- **PROPOSITION n°2 :**

Il est également proposé d'établir, par voie d'arrêté du Ministre de l'Intérieur, les normes techniques applicables aux technologies de vision par ordinateur utilisées pour la vidéoprotection, à l'instar de l'arrêté du 3 aout 2007 portant définition des normes techniques des systèmes de vidéosurveillance et prévu par l'article 252-4 du CSI.

Il est proposé d'ajouter à l'article L.252-4[38] du CSI un quatrième alinéa rédigé ainsi :

> « *Les systèmes de vidéoprotection intégrant des technologies de vision par ordinateur doivent répondre à des normes techniques définies par arrêté du ministère de l'intérieur après avis de la Commission nationale de la vidéoprotection[39].* »

PRENDRE EN COMPTE LA PROTECTION DES DONNEES A CARACTERE PERSONNEL DANS LE REGIME DE LA VIDEOPROTECTION

L'objet des présents amendements est d'harmoniser le régime de la vidéoprotection avec la règlementation sur la protection des données personnelles, afin de permettre aux autorités compétentes de mettre en œuvre des systèmes de vidéoprotection en limitant le droit d'opposition des personnes, là où cela est nécessaire et proportionné.

---

[37] Article L.252-2 du CSI – version en vigueur :
L'autorisation préfectorale prescrit toutes les précautions utiles, en particulier quant à la qualité des personnes chargées de l'exploitation du système de vidéoprotection ou visionnant les images et aux mesures à prendre pour assurer le respect des dispositions de la loi.
Dans le cas prévu au dernier alinéa de l'article L. 251-2, le visionnage des images ne peut être assuré que par des agents de l'autorité publique individuellement désignés et habilités des services de police et de gendarmerie nationale.

[38] Article L252-4 du CSI – version en vigueur :
Les systèmes de vidéoprotection sont autorisés pour une durée de cinq ans renouvelable.
Les systèmes de vidéoprotection installés doivent être conformes à des normes techniques définies par arrêté du ministre de l'intérieur après avis de la Commission nationale de la vidéoprotection, à compter de l'expiration d'un délai de deux ans après la publication de l'acte définissant ces normes.
Les autorisations mentionnées au présent titre et délivrées avant le 1er janvier 2000 expirent le 24 janvier 2012. Celles délivrées entre le 1er janvier 2000 et le 31 décembre 2002 expirent le 24 janvier 2013. Celles délivrées entre le 1er janvier 2003 et le 24 janvier 2006 expirent le 24 janvier 2014.

[39] L'avis de la commission nationale de la vidéoprotection est à confirmer car cette commission a vocation a disparaître d'ici 2022

- **PROPOSITION n°3 :**

Il est proposé de modifier l'article L. 251-2 du CSI par l'ajout d'un dernier alinéa ainsi rédigé :

> *« Lorsque la transmission et l'enregistrement d'images prises sur la voie publique par le moyen de la vidéoprotection impliquent un traitement de données à caractère personnel au sens de la loi n° 78-17 du 6 janvier 1978, les autorités publiques compétentes peuvent, par voie règlementaire, limiter la portée des droits des personnes concernées par le traitement de leurs données à caractère personnel, lorsqu'une telle limitation respecte l'essence des libertés et droits fondamentaux et qu'elle constitue une mesure nécessaire et proportionnée dans une société démocratique aux fins d'assurer les finalités énoncées à l'alinéa 1er du présent article.* »

Sur la base de cette autorisation générale, deux options sont envisagées afin de faire application de l'article 23 du RGPD :

- soit la prise de décrets par chaque ministère concerné (notamment, transports, intérieure, santé publique) ;
- soit l'insertion dans le formulaire CERFA 13806*03 relatif à la demande d'autorisation d'un système de vidéoprotection[40] déposé à la préfecture, d'une partie relative aux données à caractère personnel qui pourrait être insérée après la partie 7 « traitement des images ».

Dans les deux cas, conformément à l'article 23 du RGPD, les dispositions spécifiques suivantes devront être précisées :

- finalités du traitement ou des catégories de traitement;
- catégories de données à caractère personnel;
- l'étendue des limitations introduites;
- garanties destinées à prévenir les abus ou l'accès ou le transfert illicites;
- détermination du responsable du traitement ou des catégories de responsables du traitement;
- durées de conservation et aux garanties applicables, en tenant compte de la nature, de la portée et des finalités du traitement ou des catégories de traitement;
- risques pour les droits et libertés des personnes concernées; et
- droit des personnes concernées d'être informées de la limitation, à moins que cela risque de nuire à la finalité de la limitation.

- **PROPOSITION n°4 – amendement de cohérence :**

Il est proposé de modifier l'article L. 251-1 du CSI ainsi :

> *« Les enregistrements visuels de vidéoprotection répondant aux conditions fixées aux articles L. 251-2 et L. 251-3 sont soumis aux dispositions du présent titre, ~~à l'exclusion de ceux qui sont utilisés dans des traitements automatisés ou contenus dans des fichiers structurés selon des critères permettant d'identifier, directement ou indirectement, des personnes physiques, qui sont soumis~~ et au Règlement (UE) 2016/679 sur la protection des données à caractère personnel, et à la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés "*

Cet amendement a simplement pour objet de mettre en conformité le CSI avec le cadre légal applicable en matière de données à caractère personnel.

[40] cerfa_13806.do (service-public.fr)

ETENDRE LE PERIMETRE DES FINALITES DE LA VIDEOPROTECTION POUR Y INTEGRER LA SECURITE SANITAIRE

Plus que jamais, la sécurité sanitaire est un enjeu d'intérêt général qui requiert la mobilisation d'importants moyens humains et financiers. Les nouvelles technologies offrent des moyens efficaces et fiables à la réalisation de cet objectif collectif. En particulier, les technologies de vision par ordinateur permettent d'analyser en temps réel un flux d'images afin d'y détecter automatiquement des comportements, tels que le non-respect du port de masque, le non-respect des mesures de distanciation sociale.

Les données obtenues par les outils de vision par ordinateur qui seraient intégrés aux systèmes de vidéoprotection permettraient d'aider les agents en charge de la mise en œuvre de la vidéoprotection, en disposant de statistiques plus précises et d'indicateurs chiffrés pouvant les aider dans leur travail.

- **PROPOSITION n°5 :**

Il est proposé de modifier l'article L. 251-2 du CSI par l'ajout d'un 12° ainsi rédigé :

« La transmission et l'enregistrement d'images prises sur la voie publique par le moyen de la vidéoprotection peuvent être mis en œuvre par les autorités publiques compétentes aux fins d'assurer :
1° La protection des bâtiments et installations publics et de leurs abords ;
2° La sauvegarde des installations utiles à la défense nationale ;
3° La régulation des flux de transport ;
4° La constatation des infractions aux règles de la circulation ;
5° La prévention des atteintes à la sécurité des personnes et des biens dans des lieux particulièrement exposés à des risques d'agression, de vol ou de trafic de stupéfiants ainsi que la prévention, dans des zones particulièrement exposées à ces infractions, des fraudes douanières prévues par le dernier alinéa de l'article 414 du code des douanes et des délits prévus à l'article 415 du même code portant sur des fonds provenant de ces mêmes infractions ;
6° La prévention d'actes de terrorisme, dans les conditions prévues au chapitre III du titre II du présent livre ;
7° La prévention des risques naturels ou technologiques ;
8° Le secours aux personnes et la défense contre l'incendie ;
9° La sécurité des installations accueillant du public dans les parcs d'attraction ;
10° Le respect de l'obligation d'être couvert, pour faire circuler un véhicule terrestre à moteur, par une assurance garantissant la responsabilité civile ;
11° La prévention et la constatation des infractions relatives à l'abandon d'ordures, de déchets, de matériaux ou d'autres objets ;
12°La prévention des risques sanitaires dans un objectif de santé publique.

Il peut être également procédé à ces opérations dans des 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.

Après information du maire de la commune concernée et autorisation des autorités publiques compétentes, des commerçants peuvent mettre en œuvre sur la voie publique un système de vidéoprotection aux fins d'assurer la protection des abords immédiats de leurs bâtiments et installations, dans les lieux particulièrement exposés à des risques d'agression ou de vol. Les conditions de mise en œuvre et le type de bâtiments et installations concernés sont définis par décret en Conseil d'Etat. »

Mai 2021

CONTRIBUTION DE LA FIEEC

A L'ATTENTION DE M. LE DEPUTE JEAN-MICHEL MIS

MISSION « « POUR UN USAGE RESPONSABLE ET ACCEPTABLE PAR LA SOCIETE DES TECHNOLOGIES DE SECURITE »

INTRODUCTION

- La FIEEC est une grande Fédération de l'industrie qui rassemble **26 syndicats professionnels** dans les secteurs du numérique, de l'énergie, des automatismes, de l'électricité, de l'électronique, du numérique et des biens de consommation durables. Les secteurs qu'elle représente regroupent plus de **2 000 entreprises**, emploient près de **420 000 salariés** et réalisent **107 milliards d'euros** de chiffre d'affaires, dont 29 % à l'export.

- Les industries numériques sont des pourvoyeuses de solutions technologiques permettant de **répondre aux nouveaux besoins sociétaux** et d'adresser les nouveaux usages que ce soit dans le domaine de la mobilité, des territoires intelligents, de la e-santé, du bien vieillir, du développement durable et de la sécurité.

- La FIEEC est convaincu que les **technologies jouent un rôle majeur dans le domaine de la sécurité** dans ses différentes composantes et promeut de longue date **la sécurité et la confiance numérique**, comme en témoigne la parution dès 2017 de son guide « *Confiance et sécurité dans un monde connecté. Une filière d'excellence en France* » : https://www.fieec.fr/wp-content/uploads/2017/12/fieec - confiance et securite numerique dans un monde connecte - juillet.pdf. Notre profession est également engagée notamment au sein du CICS et de la filière « Industries de sécurité ».

- Pour ces raisons, la FIEEC note avec intérêt la **Mission sur les technologies de sécurité** confiée par le Gouvernement à M. le Député Jean-Michel MIS et se tient à sa disposition pour lui présenter plus avant sa contribution et ses propositions.

Fédération des Industries Electriques, Electroniques et de Communication
11-17 rue de l'Amiral Hamelin 75116 PARIS
Tél. : 01 45 05 72 04 – contact@fieec.fr – www.fieec.fr

REPONSE AU QUESTIONNAIRE

1. La notion de « technologies de sécurité » est large. Quelles sont les principales selon vous ? *[Par exemple : traitement des données (textuelles, images, sonores), biométrie, mobilité.]*
2. Pour quelles finalités ? *[Par exemple : détection de situations, analyse prédictive, suivi des personnes.]*

Face aux évolutions des menaces et des actes malveillants, les technologies de sécurité sont **diverses** et répondent à des enjeux et des **objectifs multiples** dans le monde physique et virtuel : protection des personnes et des biens, sécurisation des installations, lutte contre le terrorisme, sécurité des territoires et des libertés individuelles…

Grâce aux innovations apportées par les technologies numériques, il est désormais possible d'anticiper, de repenser les scénarios de prévention et d'alerte, de redéployer avec réactivité les mesures de sécurité qui s'imposent.

Pour faire à ces défis majeurs, plusieurs technologies essentielles peuvent être soulignées qui peuvent répondre à des finalités spécifiques ou plurielles selon le cas considéré :

- La **vidéosurveillance / vidéoprotection** : Une installation de vidéosurveillance est un ensemble d'équipements et de systèmes permettant d'analyser des séquences d'images et de mettre à disposition des informations qui permettent de déclencher les actions appropriées liées principalement à la sécurité des biens et des personnes. La vidéoprotection est un ensemble de moyens mis en œuvre (équipements, personnel de surveillance, interventions, forces de l'ordre, justice...) pour exploiter au mieux les données générées par un système de vidéosurveillance et renforcer la perception de sécurité du public.

  Les caméras peuvent être installées dans les rues, dans les lieux publics comme les centres commerciaux et les immeubles recevant du public ou des travailleurs, dans les gares etc … Elles peuvent être fixes sur un mur ou un mât, mobiles et déplaçables en fonctions des besoins constatés. Elles peuvent être embarquées c'est-à-dire dans un véhicule, un train, demain sur les agents assermentés et concourir à renforcer le sentiment de sécurité de nos concitoyens et empêcher ou limiter la commission d'un acte malveillant.

  La série de normes européennes EN 62676 définit les exigences pertinentes d'un système de vidéosurveillance notamment en termes d'interopérabilité.

- **La détection d'intrusion :** Le principe d'une installation de détection d'intrusion est de détecter l'approche, la pénétration et la présence d'un intrus dans des sites, bâtiments ou locaux. Une fois détecté, un signal est transmis à la centrale d'alarme qui commandera un signal local pour alerter/dissuader et/ou transmettra un signal à l'extérieur du bâtiment vers une endroit tiers (station de télésurveillance par exemple). L'accès à distance de ces systèmes (via un smartphone par exemple) procure une souplesse d'utilisation pour les occupants des lieux.

  La série de normes européennes EN 50131 définit les exigences pertinentes d'un système de détection d'intrusion et la certification tierce partie NFA2P est une garantie d'un fonctionnement fiable et efficace en conformité avec cette série de normes.

Des caméras vidéo associées permettant une levée de doute et des équipements de contrôle d'accès peuvent venir en complément de la détection intrusion.

- **Le contrôle d'accès :** Le principe d'une installation de contrôle d'accès est de filtrer (autoriser ou refuser) l'entrée dans des sites, bâtiments ou locaux.

  Les systèmes à usage résidentiel, interphonie, système de lecture par badge ou clavier codé assurent les fonctions suivantes :
  - Permettre la communication audio et vidéo entre un visiteur et un résident
  - Autoriser l'accès d'un visiteur aux parties communes de l'immeuble
  - Limiter l'accès des résidents aux espaces et locaux autorisés
  - Limiter l'accès des prestataires aux espaces et locaux autorisés (ex. certification tierce partie Vigik®)

  Les systèmes à usage professionnel (tertiaire et industriel) assurent le contrôle d'accès du personnel, des prestataires de service et des visiteurs aux espaces et locaux autorisés.

  Les systèmes de contrôle d'accès peuvent intégrer une solution biométrique.

- Les **solutions biométriques** (reconnaissance faciale, de l'iris, de l'empreinte digitale ou de la voix par exemple) qui peuvent avoir plusieurs finalités :

  - Détection de situation à risque sur la base de statistiques issues d'analyse d'image
  - L'identification par reconnaissance du visage pour l'accès puis le parcours d'un usager dans un environnement sécurisé
  - Le contrôle du droit à l'accès et l'authentification du porteur via des solutions numériques ou de contrôles de titres physiques,
  - La gestion en mobilité de l'identité numérique de confiance du visiteur étranger à l'occasion de l'évènement sportif, de l'étape de sa demande de visa avant d'entrer sur le territoire à sa sortie de territoire

- Les **solutions de cybersécurité** : elles permettent d'assurer la sécurisation d'un bien ou d'une solution numérique afin d'éviter toute attaque informatique qui compromettrait son bon fonctionnement et pourrait engendrer des risques pour une infrastructure ou des personnes (endommagement, fuite de données…). Elles sont un maillon essentiel pour garantir la sécurité de bâtiments, des infrastructures qu'il s'agisse d'entreprises, d'administration ou de particulier.

  Le niveau de cybersécurité doit être adapté à la criticité du produit, du système, de l'infrastructure, de la chaîne de production ou d'approvisionnement considéré en fonction d'une analyse de risque.

- Les **composants et systèmes électroniques**, où la France dispose là-aussi d'une filière d'excellence, jouent un rôle croissant dans l'amélioration des technologies de cybersécurité mais aussi plus largement des technologies à usage civil ou à double usage.

3. **Pensez-vous qu'elles permettraient d'anticiper les évolutions des missions de sécurité dans les 10 à 20 ans à venir ? Comment voyez-vous ces évolutions ?**

La crise sanitaire a souligné le **caractère stratégique des infrastructures et équipements numériques** pour notre économie et notre société avec le développement du télétravail, de la télémédecine ou encore de l'éducation à distance. Par ailleurs, le contexte est marqué par l'**évolution des formes de délinquance (ex. cybercriminalité**, nouvelles formes d'atteintes aux biens ou aux personnes…).

Pour faire face à cette double évolution, le **rôle des technologies de sécurité est amené à s'accroître sensiblement** au bénéfice des missions de sécurité privées ou publiques.

A titre d'exemple, dans le domaine de l'**analyse d'image et de la reconnaissance du visage** souligne une accélération des performances de comparaison d'image avec l'introduction des algorithmes de « maching learning » qui fonctionnent par apprentissage (IA) est à souligner.

En matière d'**identité numérique** utilisée et contrôlée en mobilité, la crise sanitaire a favorisé l'accélération de la digitalisation des contrôles. Les technologies mises en œuvre à l'occasion d'évènements sportifs pourraient préfigurer ce qui sera appliqué plus généralement à l'horizon 5-10-20 ans dans le domaine des mobilités entre Etats.

La multiplication des attaques informatiques impliquera enfin une intégration plus profonde des **solutions de cybersécurité** dans les politiques des collectivités publiques et des acteurs privés.

4. **Sur chaque technologie prioritaire évoquée, quel est l'état de développement de l'industrie française ? Que lui manque-t-il pour se perfectionner ?**

La France dispose d'une **filière d'excellence** dans le secteur des technologies de sécurité et de leur installation, que ce soit notamment dans les domaines de la sécurité électronique (contrôle d'accès, détection d'intrusion, vidéoprotection), de la biométrie, de l'identité numérique ou encore de la cybersécurité. Cet **écosystème innovant et fort d'une expertise reconnue** regroupe aussi bien des grands groupes leaders mondiaux que des PME et ETI.

Pour permettre la croissance de ce secteur industriel majeur, il convient d'**assurer un cadre notamment au niveau réglementaire propice à la capacité d'innovation** des entreprises. C'est un aspect capital dans le domaine des technologies numériques où la concurrence internationale est forte.

Dans le domaine de l'intelligence artificielle par exemple, il convient d'adopter une **approche pragmatique et équilibrée dans la définition d'un nouveau cadre pour l'IA** notamment dans le contexte de la réglementation européenne proposée par la Commission. Il s'agit de permettre la **conciliation entre la bonne gestion et la protection des données et innovation**. S'il doit par exemple proscrire les biais d'apprentissage et protéger les bases d'apprentissage, le cadre réglementaire devra assurer la sécurité juridique et ne pas faire peser sur les entreprises des contraintes disproportionnées par rapport à leurs compétiteurs internationaux, dans la bataille mondiale de l'IA et des données.

En matière de **cybersécurité**, le développement de standards européens et internationaux sur lesquels s'appuieront les schémas de cybersécurité permettra d'accompagner pleinement son déploiement, avec des exigences adaptées au besoin du marché en fonction des risques.

Pour la **sécurité électronique** (détection d'intrusion, contrôle d'accès, vidéoprotection), tous ces systèmes fonctionnent de plus en plus sur réseau IP et sont de plus en plus accessibles via des dispositifs externes (smartphone, cloud). Le nombre de « portes d'entrée » dans ces systèmes est donc grandissant : leur intégrité et leur sécurité de fonctionnement doivent donc être assurés. Des solutions existent et sont mises en œuvre pour déjouer au maximum les tentatives d'accès frauduleuses dans ces systèmes. La CSPN de l'ANSSI et la certification @ du CNPP sont des garanties que ces solutions sont bien présentes.

Ces systèmes de sécurité électronique offrent de plus en plus de fonctionnalités tout en :

- Etant performants ;
- Répondant aux critères environnementaux (éco conception, performance énergétique, …) ;
- Garantissant le respect de la vie privée (RGPD) ;
- Assurant la sécurité numérique des systèmes installés ;
- Facilitant l'émergence de services.

Avec la perspective d'une meilleure appropriation et acceptation de l'**identification numérique**, le déploiement rapide d'une identité numérique en France et un développement des services numériques de vérification s'appuyant sur cette identité numérique ou sur les titres d'identité régaliens devrait quant à lui contribuer à une préparation de l'écosystème Français en vue des prochains grands évènements sportifs.

De manière générale, le renforcement de la **lutte contre les produits non conformes ou contrefaisants** par les autorités de surveillance du marché est une condition sine qua non du bon déploiement de technologies numériques. La surveillance du marché permet d'assurer que les produits mis sur le marché sur notre territoire sont sûrs et conformes aux réglementations en vigueur, ce qui assure la sécurité de l'utilisateur et garantit une concurrence loyale entre tous les acteurs.

5. Comment les configurations techniques peuvent-elles concilier une utilisation de ces technologies et des garanties pour les libertés (protection des données, contrôles automatisés, etc.) ?

Notre profession considère la sécurité numérique et la protection des données comme un **enjeu fondamental**. Aussi, le ***privacy by design*** **et le** ***security by design*** constituent des instruments fondamentaux dans la chaîne de valeur de la *privacy* pour ces équipements qui doivent être bien protégés. Cette politique doit être la plus efficace possible à la fois pour garantir la confiance de l'utilisateur et s'inscrit dans une démarche d'investissement responsable.

La protection des données personnelles et le progrès et l'innovation économique ne sont pas contradictoires mais bien **conciliables et complémentaires**. La FIEEC a été **précurseur** pour travailler étroitement avec la CNIL pour élaborer un **cadre équilibré** permettant à la fois la protection des données personnelles et la capacité d'innovation des entreprises.

C'est dans cet esprit que la FIEEC s'investit pleinement dans l'accompagnement des entreprises à la **bonne mise en œuvre de leurs obligations** (ex. colloques avec la CNIL, guides pratiques sur le RGPD, packs de conformité sur les smart grids, la silver économie, le véhicule connecté...).

En matière d'**identité numérique** par exemple, l'accès et le contrôle de l'identité numérique d'un porteur doit rester conditionnée au consentement du porteur et se traduit par le déverrouillage de l'accès au compartiment via le code PIN. La généralisation de ce principe à l'échelle nationale au travers le déploiement rapide d'une l'identité numérique en France devrait favoriser l'appropriation et l'acceptation de ces modalités d'échange numérique entre le porteur et le contrôleur avant les évènements sportifs prévus à l'horizon de 2 ans.

6. **Les cadres d'expérimentation sont souvent mis en avant pour le perfectionnement de ces technologies. Quelles sont selon vous les priorités ? Quels seraient les contours de ces cadres ? A quelles fins ?**

Les expérimentations sont importantes car elles permettent de :

- Tester la robustesse d'une solution, sa facilité d'implémentation et de maintien en condition opérationnelle ;
- Confronter la solution et les usages au cadre réglementaire et légal ;
- Identifier la meilleure expérience utilisateur permettant de susciter l'adhésion de l'usager.

Les technologies modernes ont pour vocation d'être inclusives et universelles, c'est-à-dire adaptées à toutes les populations quelques soient les âges, les genres, les nationalités, les handicaps éventuels, les statuts citoyens ou professionnels. **L'expérimentation lors d'un évènement sportif international tel que les JOP 2024 est une occasion unique** permettant de s'assurer de l'acceptabilité par un public très varié de technologies innovantes apportant de la sécurité dans un temps très restreint et ainsi pouvoir finaliser des technologies pour qu'elles soient les mieux adaptées possibles avant un déploiement plus large.

Les exemples d'expérimentations suivantes pourraient être envisagés :

- s'appuyer sur le décret Transport pour l'expérimentation des technologies d'analyse d'images à vocation statistique dans le domaine de l'organisation d'évènements majeurs en répétition des JO ;
- favoriser l'utilisation de l'identité numérique ou à ses dérivations sur smartphone dans la gestion des contrôles d'accès à certains évènements
- tester la notion de fan ID (identité temporaire du supporter) à l'occasion de la Coupe du Monde de Rugby 2023 en répétition des JOP Paris 2024.

*****

Fédération Française de la Cybersécurité - 75 rue de Lourmel 75015 Paris

A l'attention de Monsieur le député Jean-Michel MIS

Paris le 8 juin 2021,

Mission parlementaire député Jean-Michel MIS

Réponse de la Fédération Française de la Cybersécurité à Jean-Michel MIS chargé par le Premier ministre d'une mission sur « l'utilisation des nouvelles technologies dans le domaine de la sécurité ».

La Fédération :

La Fédération Française de la Cybersécurité a pour objet de rassembler toutes les organisations d'entreprises, les associations professionnelles, les entreprises, les personnes et plus largement tous les acteurs directs ou indirects de la Cybersécurité Française dans le respect de leur diversité, pour leur apporter un soutien et des services utiles à leur fonctionnement.

Elle souhaite promouvoir l'image des activités de la Cybersécurité française ; favoriser les échanges d'idées ainsi qu'une collaboration aussi étroite que possible entre les organisations de la Cybersécurité et faire connaître le point de vue des entrepreneurs, des utilisateurs et des parties prenantes sur les sujets concernant directement ou indirectement leurs activités.

La consolidation de la filière avec les personnes y travaillant ou souhaitant y faire leur carrière fait partie intégrante de nos souhaits et doit permettre également de créer des vocations futures auprès de la jeunesse, des étudiants et des personnes souhaitant réaliser une reconversion professionnelle.

Notre objectif est également d'accompagner les entreprises, afin qu'elles bénéficient d'un environnement législatif et réglementaire favorable au développement de leur activité et concourent plus efficacement à la cybersécurité générale de la nation.

La Fédération souhaite contribuer activement à enrichir la réflexion sur les évolutions de la Cybersécurité et les problématiques liées son écosystème en France.

La constitution de la Fédération Française de la Cybersécurité obéit au principe de liberté et de pleine autonomie des organisations et des membres qui la composent.

Les moyens d'action de la Fédération consistent en toute action permettant de poursuivre son objet, notamment l'organisation d'actions de communication, de rencontres régulières, de tables rondes et de congrès, d'études, d'actions médiatiques, d'actions d'influence auprès des pouvoirs publics, ou encore la publication de bulletins et de travaux.

Ainsi conformément à sa raison d'être la Fédération Française de la Cybersécurité souhaite apporter au travers de ce courrier son expertise afin de contribuer à la mission parlementaire qui vous est confiée.

Contexte :

L'intitulé exprimé de la mission pourrait laisser à penser en première lecture qu'elle s'inscrit dans le domaine de la sureté davantage que celui de la cybersécurité. Néanmoins la cybersécurité couvre un large champ dont les infrastructures font l'objet de nombreuses attaques, physiques et virtuelles. La question se pose alors de définir comment assurer une protection des biens essentiels, tels que des infrastructures, l'outil de production, les systèmes d'informations ou encore les systèmes industriels [1].

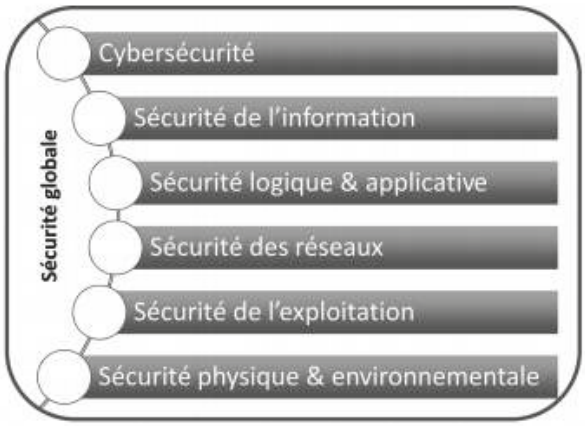


Figure 1 **Domaine d'application de la sécurité**, *source Cybersécurité Analyser les risques Mettre en œuvre les solutions, Solange Ghernaouti*

Toutes les sphères d'activité de l'informatique et des réseaux de télécommunication sont concernées par la sécurité informatique. En fonction de son domaine d'application, celle-ci peut se décliner en (figure 1) :

- Sécurité matérielle, physique et environnementale ;
- Sécurité logique, sécurité applicative et sécurité de l'information ;
- Sécurité de l'exploitation ;
- Sécurité des réseaux de télécommunication ;
- Cybersécurité.

En complément de ces notions de sécurité vient s'ajouter la sécurité CPS dite cyberphysique. Le concept Cyber-Physical System ou systèmes cyberphysique en français, a été défini en 2006 lors de travaux réalisés par le National Science Foundation américaine, et notamment par le Pr. Edward LEE de l'université de Berkley, Californie.

Les CPS sont des « systèmes embarqués intelligents » qui rendent les produits encore plus interconnectés, interdépendants, collaboratifs et autonomes [2]. Ils permettent d'améliorer ou de proposer de nouvelles fonctionnalités ou de nouveaux services. Ainsi la définition proposée par MONOSTRI en 2014 synthétise la complexité des CPS :

« Les CPS sont des systèmes formés d'entités collaboratives, dotées de capacités de calcul, qui sont en connexion intensive avec le monde physique environnant et les phénomènes s'y déroulant, fournissant et utilisant à la fois les services de mise à disposition et de traitement des données disponibles sur le réseau ».

Ainsi l'on peut convenir que des réponses soient apportées sur les questions de sécurité physique des infrastructures y compris la cyberphysique des systèmes (e.g. IoT) et cybersécurité d'une manière plus générale, en considérant une évolution des menaces de cyberattaques qui a quadruplé en 2020, et qui vraisemblablement devrait s'intensifier à l'horizon des grands évènements en france.

Vision FFCyber : assurer un cade favorable au développement et à l'usage des nouvelles technologies de sécurité

Sécurité physique des infrastructures : des vulnérabilités peuvent exister sur les infrastructures qui hébergent des réseaux informatiques qu'ils soient de composante IT ou OT. Cela étant, il semble difficile de surveiller selon les secteurs d'activité des emprises parfois diffuses et en nombre importantes. Les SOC (Security Operation Center) peuvent jouer un rôle en admettant d'y inclure une automatisation de monitoring des alarmes des tentatives d'intrusion, de subordination d'identité, etc…

Un projet européen Horizon 2020 dénommé safecare [3] pour le milieu de la santé, a proposé de développer des systèmes de détection d'intrusion. Le premier livrable décrit les spécifications dudit système considérant :

- Détection automatique des intrusions physique
    - Recours à la biométrie
- Système de gestion des habilitations d'accès
    - Recours au système de gestion des vidéosurveillance (VMS)
- Capacités d'identification des personnes impliquées dans les incidents
- Détection automatique des incendies
- Système de détection incendie jumelé à un système de vision (VMS) pour améliorer le contrôle et lever de doutes des alarmes incendies

Pour le système d'intrusion physique, trois solutions pour détecter l'intrusion sont spécifiées : détection d'utilisation frauduleuse de la clé de contrôle d'accès, de tailgating (i.e. atteinte à **la sécurité physique** par laquelle une personne non autorisée suit un individu autorisé pour entrer dans un lieu sécurisé afin de voler des informations confidentielles) et de violation du contrôle d'accès par la force.

Pour le système de détection incendie, une solution de détection à l'aide des caméras de surveillance est proposée de deux manières différentes ; lorsqu'un incendie est détecté, confirmer qu'il y a un incendie ; et essayer de détecter les incendies tout le temps.

Envoyer les incidents validés, les alertes d'intrusion, les alertes d'incendie et les journaux d'accès aux bases de données centrale. Ici le trait d'union avec notre proposition d**'intégrer** ces futurs systèmes dans les **SOC du futur**. En effet, le SOC est une division qui assure la sécurité de l'organisation et surtout le volet sécurité de l'information. Plus spécifiquement un SOC est lié aux personnes, aux processus et aux technologies utilisées pour s'assurer de la connaissance de la situation grâce à la détection, au confinement et à l'assainissement des menaces informatiques. Un SOC gère les incidents pour l'entreprise en s'assurant qu'ils sont correctement identifiés, analysés, communiqués, actionnés / défendus, enquêtés et signalés. Le SOC surveille également les applications pour identifier une éventuelle cyberattaque ou intrusion (événement) et détermine s'il s'agit d'une menace (incident) réelle et malveillante, si cela pourrait avoir un impact sur l'entreprise.

L'intérêt de ces travaux de recherche sont aussi dans la considération de solutions à bas coûts, durables et prenant en compte des besoins de rapidité et de précision de la détection :

- Les solutions doivent être conçues pour tenter de détecter l'incident même avant qu'il ne se soit réellement produit ;
- Les solutions doivent répondre en temps quasi réel ;
- Les solutions doivent être capables de détecter l'incident juste après qu'il ait eu lieu;
- Les solutions doivent avoir une grande précision, éviter les faux positifs et exactitude du rapport

Les **données** demeurent prépondérantes dans tous ces systèmes et notamment ceux qui font appel au traitement automatisé par de l'intelligence artificielle. D'un point de vue normatif, il est nécessaire de rappeler qu'aucune norme actuelle ne traite des sujets de la qualité de la donnée pour le machine learning. Cela nous pousse naturellement à fortement recommander au plus vite de lancer des groupes de travail sur cette thématique au niveau national voire européen. Le projet safecare traite aussi ce sujet de la donnée [4] en lien avec les spécifications des systèmes de sécurité physique en fixant des exigences au niveau des données.

Par exemple, la solution ne doit, en aucun cas, activement compromettre la communication entre le système de collecte de données et les capteurs du banc d'essai, ou les fonctionnalités des dispositifs médicaux et autres infrastructures existantes. Les données transférées entre les systèmes médicaux contiennent probablement des informations sensibles sur les patients. Lorsque la solution effectue l'analyse de ces données à des fins de détection d'intrusion, il s'agit d'une forme de traitement des données personnelles. Par conséquent, la vie privée de la patiente doit être respectée par le logiciel.

Cybersécurité :

Du point de vue de la Cybersécurité, nous retenons deux axes.

- La discipline : qui intègre le management, le juridique, la formation, etc…
- La technologie : liée à la sécurité de l'information, mais de plus en plus élargie à d'autres technologies (e.g. Blockchain, Machine learning, etc…)

La discipline nous inspire le besoin de ne pas négliger l'évolution du système de **management** en considération de l'introduction des NTIC (Nouvelles Technologie d'Information et de Communication). Si des Directives (e.g. Directive sur la sécurité des réseaux et des systèmes d'information (Directive NIS) ((UE) 2016/1148) et des normes existent (e.g. ISO27001, IEC62443, …) force est de constater que la temporalité d'édition, de renouvellement des standards n'est pas à l'échelle de l'évolution des technologies.

Le **juridique** (CNIL, RGPD,…) est à la fois gage de souveraineté, mais peut aussi parfois représenter un verrou à la modernité.

La souveraineté doit considérer un encadrement des données pour assurer la privacy. Nous sommes d'accord pour convenir que les données, et tout particulièrement les données personnelles, sont la matière première de la société de l'information [5]. À ce titre, elles représentent un enjeu économique stratégique. Mais sachant que la valorisation de ces données résulte essentiellement de leur traitement et de leur mise en relation, nous pouvons nous interroger sur la capacité à traiter ces dernières avec une régulation des plus contraignantes. Sans projet de recherche (i.e. pour tout ce qui touche le traitement vidéo, les protocoles légaux à respecter rendent parfois difficile d'un point de vue économique, temporel l'acceptabilité d'un projet de R&D) il demeure difficile d'entrevoir un potentiel de valeur de la donnée. En d'autres termes, si nous nous limitons dans les projets de recherche pour des raisons d'accès aux données, de privacy, d'éthique, alors nous ne développerons que très peu de solutions, ni concurrentielles et par définition ni souveraines. Laissant place actuellement aux solutions asiatiques, americaines. Dès lors le cadre n'est pas à remettre en cause, mais devrait pouvoir bénéficier de flexibilité pour des fins de recherche appliquée.

La **formation**, nous semble un sujet à ne pas édulcorer. L'apport massif de nouvelles technologies de sécurité ne pourra à elle seule répondre aux enjeux. Il faudra appuyer ces nouveaux systèmes de formations, et voire au-delà en augmentant la filière des métiers de la cybersécurité. Par construction, doter des SOC de nouvelles fonctionnalités de supervision au titre de la sécurité engendre des ressources supplémentaires, complémentaires.

La fédération forte d'une expertise dans le collège formation, peut apporter son soutien au développement rapide et qualitatif de formations adaptées. C'est déjà d'ailleurs le cas, avec la formation développée tout récemment par la fédération à destination de jeunes de Seine Saint-Denis (93).

Les formations actuelles sont majoritairement ciblées sur des populations de niveau bac +5, ingénieur. Or, un constat partagé fait écho de tendre vers des formations de techniciens (Bac+2), de bachelier voire de donner l'accès à la filière à des non diplômés (i.e. avec une formation adaptée).

Dans ce scenario, les SOC et les entreprises d'autres secteurs peuvent d'ores et déjà être sensibilisées au recrutement d'alternants de formations de ces niveaux déjà existantes afin d'augmenter très efficacement leur résilience informatique à des coûts maîtrisés.

Cela permettrait :

- De soulager, de renforcer les équipes dans les SOC.
- D'alimenter la filière (difficulté à recruter)
- D'assurer une charge non négligeable dévolu à la sensibilisation des utilisateurs.

Il nous faut accélérer le développement de la filière, et nous avons tous les atouts pour répondre.

La **technologie** offre un champ des possibles : La France regroupant beaucoup d'expertises sur le machine learning, la blockchain, l'IoT, les drones, les robots,..

Pour aller plus en profondeur d'un point de vue technique, nous pouvons évoquer l'exemple des composantes hardware et la multiplication des attaques hardware qui impactent toute les couches par la suite.

Aujourd'hui, nous n'avons que peu de ressources humaines compétentes pour de l'audit de hardware et recherche de vulnérabilités hardware. Les ingénieurs électroniciens n'ont presque jamais la fibre cybersécurité et les ingénieurs en cybersécurité ne connaissent rien au hardware.

De plus en plus de solutions de traitement de données, d'apprentissage automatique utilisent les couches basses du calcul (e.g. calcul en enclave INTEL pour implémenter du chiffrement homomorphe ou de la differential privacy). Cela deviendra un problème à considérer si l'on souhaite s'inscrire dans un schéma de technologie pour la sécurité. La technologie apporte toujours son lot de compromis entre renforcement de la sécurité et apparition de nouveaux risques, de vulnérabilités nouvelles.

Nous pouvons citer dans ce même ordre d'idée, l'IA au service de la sécurité versus la sécurité de l'IA. L'intelligence artificielle nourrit l'espoir d'automatisation, de gain de performance et de renforcement in fine de la sécurité. C'est juste et concevable mais sans compter que l'IA elle-même reste très vulnérable. Il est facile par des techniques bien connues (e.g ; poisonning, inference, evasion, etc…) de tromper, de détourner les prédictions d'une IA. Les systèmes peuvent subir une prise de contrôle sans même s'en rendre compte, voire pire influer sur des prises de décision contraires à la sécurité. Ce sujet doit être traité à sa hauteur dans toute volonté de développer ces technologies pour la sécurité. Ici également, la France a de nombreux atouts avec des organismes du programme de recherche 3IA tels que :

- à Grenoble - "MIAI@Grenoble-Alpes" avec pour applications privilégiées la santé, l'environnement et l'énergie.
- à Nice - "3IA Côte d'Azur" avec pour applications privilégiées la santé et le développement des territoires.
- à Paris - "PRAIRIE" avec pour applications sur la santé, les transports et l'environnement.
- à Toulouse - "ANITI" avec pour applications privilégiées le transport, l'environnement et la santé.

mais aussi des organisations comme le HUBFranceIA, France is AI.

Le volet financier doit être évoqué, si nous souhaitons soutenir la recherche. Le gouvernement français, le ministère de l'économie par la voie de la DGE et de BPI réalisent des mesures de soutien aux entreprises sans précédent avec des plans de relance (e.g. PIA4, GrandDéfiCyber,..). Si ces plans peuvent s'accompagner de campagnes de communications, de nombreuses PME méconnaissent leur contenu, leur cadre. Quand ce n'est pas le cas, la gestion du dossier d'appel à projet, peut représenter pour une startup, une PME un effort à ne pas négliger et qui parfois limite l'accès par renoncement. Lorsque l'on se compare à des pays comme Israel, les USA, la Chine, on y voit une simplification des démarches qui permettent de se concentrer sur la finalité : élaborer des solutions fiables et avec efficience pour ne pas risquer d'être déjà dépassé « technologiquement parlant » lors d'un lancement du projet.

Pour conclure, la fédération française de la Cybersécurité souligne cette décision de mission parlementaire qui vous est confiée. Cela traduit la volonté et le soutien du gouvernement sur les enjeux de sécurité et plus largement de cybersécurité. Nous restons à votre disposition, pour tout renseignement supplémentaire et/ou vous aider à mener à bien cette rédaction de rapport.

Nous vous prions d'agréer, Monsieur le Député, l'assurance de notre profond respect.

Le collège R&D de la fédération française de la Cybersécurité

Cyril Cappi VP R&D FFCyber

Bibliographie

[1] Cybersécurité Analyser les risques Mettre en œuvre les solutions, Edition DUNOD, Solange Ghernaouti, 2019.

[2] RAPPORT CARTOGRAPHIE DES SYSTÈMES CYBERPHYSIQUES, Ministère de l'économie des finances et de la relance, janvier 2020

[3] Specification of the intrusion detection system Deliverable 4.3, https://www.safecare-project.eu/wp-content/uploads/2020/02/Specification-of-the-Intrusion-Detection-System.pdf

[4] Specification of data collection system Deliverable 4.5, https://www.safecare-project.eu/wp-content/uploads/2020/02/Specification-of-Data-Collection-System.pdf

[5] Le devoir de souveraineté numérique, Senat http://www.senat.fr/rap/r19-007-1/r19-007-13.html

Contribution écrite pour le rapport du député Jean-Michel MIS consacré à « l'utilisation des nouvelles technologies dans le domaine de la sécurité »

La Fédération Française des Métiers de l'Incendie (FFMI), par l'intermédiaire de l'un de ses membres affiliés, en l'occurrence le Groupement Français des Industries Electroniques de Sécurité Incendie (GESI), travaille depuis quelques années sur deux thématiques qui pourraient utilement s'inscrire dans le sujet de ce rapport parlementaire.

A) Travaux sur l'Alarme Menace (ex Alarme Attentat) :

La FFMI a commencé à travailler sur l'alarme Menace dès 2017, via un guide PPMS (Plan Particulier de Mise en Sûreté). Un groupe de travail s'est ensuite constitué au sein de l'AFNOR en 2018.

Le premier objectif était de fournir des solutions de dispositifs alarme menace (attentat) présentant un minimum de sureté de fonctionnement, par des fonctionnalités telles que surveillance des liaisons sécurisées - surveillées, alimentation sécurisée (fonctionnement pendant plusieurs heures hors secteur), et étant issues de solutions technologiques éprouvées des systèmes de sécurité incendie (notamment par le biais d'évaluations réalisées par des laboratoire indépendants). Travaux menés sous les auspices des préfets et DELVILLE (ex DMISC).

Des pistes de réflexion ont été élaborées, qui ont été transmises aux autorités compétentes (DGSCGC et SGDSN), sous les auspices des Préfets Patrick Butor BUTOR (ex Délégué ministériel aux normes) et Thierry DELVILLE (ex Délégué ministériel aux industries de sécurité et à la lutte contre les cybermenaces, DMISC).

Un vrai besoin avait été identifié : celui d'un système de diffusion d'information pour celui qui détecte la menace, vers quelqu'un qui va déclencher des scénarios et qui va ensuite devoir diffuser cette information.

Un point de vigilance avait été soulevé : les fonctions qui seraient ajoutées aux SSI ne doivent pas venir contrecarrer ce qui est déjà prévu dans les normes incendie en vigueur.

Le SGDSN a publié des recommandations début 2019 :

- Les fonctionnalités du SSI sur la sécurité incendie sont prioritaires

- Définir une norme d'application volontaire de compatibilité technique sans interférence négative avec les SSI

- Ne pas faire de doctrine au sein des normes techniques

- Dénomination de l'alarme attentat jugée non adaptée : adoption du terme « Menace », plus adapté à certains cas concrets, comme des intrusions malveillantes dans des établissements scolaires ou de soins par exemple.

- Plan de sécurisation d'établissement (PSE) à généraliser à tous les établissements prenant en compte 3 étapes : Transmission de l'alerte / Gestion de l'alerte / Diffusion de l'alarme

À moyen terme, il s'agit à la fois de développer l'élaboration du contenu des PSE à tous les établissements, et de proposer des solutions techniques répondant aux besoins (norme de la commission AFNOR S61I par exemple).

Le GT Alarme Menace de la Commission AFNOR S61I a plusieurs objectifs :

- Offrir des solutions pouvant répondre aux besoins exprimés par les chefs d'établissements
- Définir les exigences pour permettre la diffusion de l'alarme menace à partir des SSI
- Proposer des produits/systèmes pouvant répondre aux besoins exprimés dans les PSE
- Permettre de donner l'alerte vers un point central et de diffuser une alarme (sélective ou non)
- Permettre des scenarios de mise en sureté sans diminuer le niveau de sécurité incendie de l'établissement et sans impacter l'intégrité des SSI
- Respecter les observations du SGDSN

B) Travaux sur la cybersécurité :

Un premier GT cyber du GESI a été créé en juin 2017 afin de répondre à une demande de plus en plus fréquente des clients. Un an plus tard, le CNPP et l'ANSSI ont rejoint ce GT. En termes de livrables, l'objectif est de finaliser des profils de sécurité GESI/CNPP/ANSSI d'ici la fin de l'année 2021. A moyen terme, d'ici mi-2023, il s'agit de travailler à une Certification "cyber incendie" en option de la marque NF SSI.

La définition des profils cyber des produits électroniques de sécurité incendie visent à rassurer les utilisateurs quant à l'impossibilité de pénétrer leurs installations via le système de sécurité incendie. Le profil évalue les vulnérabilités pour un produit et les équipements qui lui sont raccordés.

Un profil de sécurité basé sur le modèle de l'ANSSI contient différents éléments :

- La définition des menaces potentielles (altération ou dysfonctionnement du système, déni de service)

- La description des objectifs de sécurité
- La détermination des éléments sensibles à évaluer (matériels, protocoles, logiciels)
- La classification du système, c'est-à-dire le niveau de risque acceptable
- Le niveau de robustesse (au regard de la classification)

On distingue généralement trois classes travaillées dans les profils des systèmes incendie:

- Classe 1 : il s'agit de systèmes installés pour lesquels le risque d'une attaque existe, et dont l'impact peut être considéré comme faible au regard de l'exploitation

- Classe 2 : il s'agit de systèmes installés considérés comme sensibles pour lesquels le risque d'une attaque existe, et dont l'impact peut être considéré comme significatif au regard de l'exploitation

- Classe 3 : il s'agit de systèmes installés considérés comme très sensibles pour lesquels le risque d'une attaque existe, et dont l'impact peut être considéré comme critique au regard de l'exploitation

  De façon générale, les sites d'Opérateurs d'Importance Vitale (OIV) présentant des Systèmes d'Information d'Importance Vitale (SIIV) peuvent entrer dans cette dernière catégorie.

Au niveau fédéral de la FFMI, plusieurs échanges ont déjà eu lieu avec le Ministère de l'Intérieur, et notamment à l'époque avec le Préfet DELVILLE, puis plus récemment avec le Préfet Olivier de MAZIERES, en charge de ce sujet en sa qualité de Délégué ministériel aux partenariats, aux stratégies et aux industries de sécurité (DPSIS).

Une réunion d'échanges fut également organisée en novembre 2020 avec David TORTEL, Conseiller en charge des technologies et du numérique au cabinet du Ministre de l'Intérieur, et Bruno ULLIAC, conseiller technique Sécurité Civile.

A propos :

La Fédération Française des Métiers de l'Incendie (FFMI) est l'organisation professionnelle représentative de l'ensemble des métiers de la protection incendie dite « active ». Elle rassemble 12 syndicats professionnels, comptant 300 entreprises adhérentes qui emploient 25 000 salariés en France, et réalisent un chiffre d'affaires cumulé d'environ 3 milliards d'euros.

Crée en 1961, elle a pour principe fondateur la promotion de la qualité des produits et des services associés (installation et maintenance). Cette qualité est la garantie de la fiabilité et de l'efficacité des solutions de prévention et de protection mises en œuvre, et partant, du niveau de sécurité des personnes et des biens.

www.ffmi.asso.fr

Contribution du 3 juin 2021 – Mission du député Jean-Michel Mis

« Pour un usage responsable et acceptable pour la société des technologies de sécurité »

Par Adrien Basdevant, avocat spécialisé en droit des nouvelles technologies, membre du Conseil National du Numérique

1. Reconnaissance faciale et prédiction de la criminalité

Source : Extrait de MÉCANISMES D'UNE JUSTICE ALGORITHMISÉE, rapport pour la fondation Jean Jaurès, juin 2021, avec Aurélie Jean et Victor Storchan

Un groupe de recherche de l'université de Harrisburg a développé en mai 2020 une IA de reconnaissance prétendument capable de prédire si quelqu'un va être un criminel, sans biais racial, seulement en se basant sur l'image du visage de la personne. Une pétition « Abolish the Tech to prison pipeline » a été mise en ligne pour s'opposer à la parution de l'article dans la revue *Springer*. Plusieurs scientifiques et experts du domaine tels que Pawel Drozdowski, Timnit Gebru, Margaret Mitchell ou Deborah Raji dénoncent ainsi les travaux hasardeux de l'IA appliquée à la procédure judiciaire ou la criminalité et ceux qui utilisent des jeux de données biométriques ou issus de la biologie. La plupart des algorithmes d'IA ne font que trouver des corrélations entre les données d'entrées dont ils se servent pour s'entraîner et les résultats de la tâche de sortie à effectuer. Or, il est bien établi que l'on peut trouver facilement un grand nombre de corrélations absurdes.

Les nouvelles technologies de prédiction devront respecter les principes du droit pénal. Or, elles sont conçues sur des critères de dangerosité des individus – c'est-à-dire leurs actions possibles dans le futur – et non sur l'évidence de culpabilité – exigeant la preuve de faits commis.

Le risque est de voir sanctionné demain l'écart à une prétendue norme sociale ou économique définie par un code informatique, sans rapport avec la norme juridique. On ne punirait plus un sujet pour ses actions, mais pour son profil dans une situation donnée. Quelle sera alors la référence ?

La professeure de droit Mireille Delmas-Marty nous prévient : « *À terme, c'est la disparition entre armée et police, ennemi et criminel, et, finalement, la confusion entre guerre et paix, qui sont ainsi programmées.* » La question de la place du droit pénal, des garanties procédurales et, partant, de l'État de droit devront être posées avec insistance.

Cette question devient aujourd'hui fondamentale tant elle tient à l'avenir de la démocratie. Que se passera-t-il lorsque les données désigneront des criminels avant même qu'ils n'aient commis leurs crimes ? Que restera-t-il de la présomption d'innocence pour celui qui présente les caractéristiques d'un multirécidiviste ?

Il s'agirait alors de glisser insensiblement du commencement d'exécution à l'acte préparatoire, puis de l'acte préparatoire à la potentialité de commettre un crime. Indéniablement, cette piste ne peut être envisagée qu'avec intérêt par les organismes publics ou privés en charge de la sécurité, que ce soit pour des raisons de sécurité publique ou d'intérêt commercial.

La plus neuve des technologies, par un extraordinaire raccourci, rejoindrait alors la plus vieille des criminologies. Les systèmes numériques prédictifs permettraient d'identifier le criminel en puissance. Tout comme les caractéristiques morphologiques devaient permettre d'identifier le criminel-né, selon le père de la criminologie italienne, Cesare Lombroso.

La présomption d'innocence est un principe fondamental de notre État de droit et l'une des premières caractéristiques de nos démocraties libérales. Elle permet de savoir les faits qui nous sont reprochés, de participer aux audiences et d'être entendus. Ces principes devront être respectés par les concepteurs et les utilisateurs de ces nouveaux outils.

2. Reconnaissance faciale et lutte contre le terrorisme

Source : Entretien Adrien Basdevant par Laurence Neuer dans Le Point, novembre 2020
https://www.lepoint.fr/editos-du-point/laurence-neuer/lutte-contre-le-terrorisme-la-reconnaissance-faciale-s-imposera-t-elle-05-11-2020-2399590_56.php

Lutte contre le terrorisme : la reconnaissance faciale s'imposera-t-elle ?

Pour l'heure, la loi s'oppose au déploiement de cette technologie d'identification des personnes, défendue par Valérie Pécresse. Mais jusqu'à quand ? Interview.

« *Souriez, vous êtes reconnu !* » L'idée fait son chemin à la faveur du contexte de menace terroriste : une fois les masques baissés, la reconnaissance faciale pourrait s'inviter à l'entrée des gares, voire sur les quais des RER et des métros pour identifier des personnes recherchées et les interpeller avant qu'elles ne montent dans les trains. C'est en tous cas l'ambition de Valérie Pécresse pour lutter contre la « hausse alarmante de l'insécurité » à Paris et en Île-de-France. « Nous sommes en risque terroriste très élevé, or on n'a aucun moyen d'utiliser l'intelligence artificielle pour les repérer alors qu'on a désormais des caméras partout. N'attendons pas un drame pour agir ! » a justifié, dans les colonnes du Parisien, la présidente de la région Île-de-France, qui souhaite aussi armer la police municipale et renforcer les prérogatives des agents de sécurité privée.

En France, « le recours à des caméras « intelligentes » n'est prévu par aucun texte particulier » rappelle la CNIL sur son site. Et, faute pour les personnes filmées de pouvoir consentir (ou non) au système , c'est le principe de l'interdiction qui s'applique. Ainsi, le dispositif vidéo mis en place au moment du déconfinement à la station Chatelet Les Halles pour comptabiliser les visages masqués a

été interrompu, alors même que les images des personnes étaient supprimées presque instantanément.

Reste que la reconnaissance faciale est déjà utilisée en France, notamment à l'aéroport de Lyon Saint-Exupéry pour réduire les files d'attente. « Dans l'aéroport de Nice, une personne fichée comme personne recherchée peut grâce à ce système être interpellée. Pourquoi ne pas faire dans une gare ce qu'on peut déjà faire dans un aéroport ? », a plaidé Valérie Pécresse au micro de France info.

Le cadre légal pourrait-il céder sous la pression des attentats et du sentiment d'insécurité des citoyens ? Les réponses d'Adrien Basdevant, avocat spécialisé en droit du numérique, co-auteur de l'Empire des données (https://www.lepoint.fr/editos-du-point/laurence-neuer/ceux-qui-detiennent-les-donnees-possedent-le-pouvoir-23-03-2018-2204904_56.php

L'usage des caméras dites de « vidéoprotection » est **très encadré juridiquement. Que prévoit la loi ?**

Adrien Basdevant : La vidéoprotection, contrairement à la « vidéosurveillance » (qui se pratique dans un cadre privé) concerne les lieux publics, et peut répondre à différentes finalités : protéger certains bâtiments, repérer les infractions à la circulation, réguler les flux de transport, surveiller les lieux particulièrement exposés aux infractions, ou encore, prévenir les actes de terrorisme.

Le système est encadré par l'article L.251-2 du Code de la sécurité intérieure et la loi informatique et libertés qui prévoient notamment de réaliser, avant le déploiement d'un tel système, une analyse d'impact sur la protection des données, d'informer les personnes susceptibles d'être filmées (par voie d'affiches ou de panneaux), de limiter la durée de conservation des images à un mois maximum. Pour assurer la sécurité des données traitées, le visionnage des images ne peut être opéré que par les personnes spécifiquement habilitées.

Que dit la loi concernant l'utilisation de ces caméras à des fins de reconnaissance faciale ?

La loi est claire : l'exploitation de données biométriques pour le compte de l'État nécessite un décret en Conseil d'État après avis de Cnil. En effet, la reconnaissance faciale ajoute une couche algorithmique au système d'enregistrement des images. Cette fonctionnalité logicielle permet de les analyser de manière automatique. Sa spécificité est qu'elle traite des données biométriques qui permettent d'identifier une personne sur la base de ses caractéristiques physiques. Elles sont considérées comme très sensibles et sont à ce titre strictement encadrées.

Le problème de ce type de système, c'est l'interconnexion des fichiers, par exemple, le fait de coupler les visages des personnes à des fichiers de police judiciaire. Actuellement, le fichier TAJ, dédié aux antécédents judiciaires, peut être utilisé pour faire de la reconnaissance faciale, mais seulement pour une comparaison en temps différé avec des images obtenues lors d'une enquête, et non en temps réel.

Et pourtant, la reconnaissance faciale semble s'installer dans l'espace public au travers d'« expérimentations » : en février 2019, au carnaval de Nice, pour repérer les mineurs en fugue ou les personnes interdites de grands rassemblements, ou encore à l'aéroport de Lyon Saint-Exupéry, pour réduire les files d'attente.

En fait, tout dépend de l'objectif assigné au système de reconnaissance faciale. S'agit-il d'authentifier une personne, autrement dit de s'assurer que la personne qui par exemple se présente au guichet d'un aéroport est bien celle qu'elle prétend être ? Dans ce cas, la technologie vise à certifier l'identité de cette personne en comparant un gabarit (la signature numérique correspondant aux

caractéristiques du visage d'une personne déterminée) à un autre gabarit pré-enregistré, stocké sur un support. C'est le cas, par exemple, du système de contrôle d'identité aux frontières « Parafe », qui compare le visage du voyageur entrant dans le sas avec la photo stockée dans le microprocesseur de son passeport biométrique.

L'autre système de reconnaissance faciale, auquel semble faire référence Valérie Pécresse, aurait pour but d'identifier une personne parmi d'autres, par exemple dans une foule, ce qui implique de comparer ses données biométriques à celles d'autres personnes qui devront donc être à cette fin être identifiées. Ainsi, plus personne ne pourrait circuler anonymement….

Quelle est la position de la Cnil sur ces deux types de reconnaissance faciale ?

La Cnil a donné des avis favorables concernant les systèmes d'authentification, sous réserve qu'ils soient nécessaires et proportionnés. La commission a ainsi donné un avis favorable à Parafe ou encore à Alicem, cette application pour smartphone qui permet de prouver son identité sur Internet de manière sécurisée, à l'aide de son smartphone et de son passeport.
https://www.lepoint.fr/editos-du-point/laurence-neuer/alicem-l-identite-numerique-par-reconnaissance-faciale-en-question-15-10-2019-2341264_56.php

En revanche, à Nice, le recours à la reconnaissance faciale à l'entrée des lycées dans le seul but de fluidifier leur accès a été refusé, car jugé inadéquat et disproportionné.

Que vous inspire l'idée de constituer un comité d'éthique « Etat-région » visant à trouver « le juste équilibre entre l'impératif de sécurisation des réseaux de transports et la préservation des libertés* », comme proposé par *Valérie Pécresse ?

En soi, créer un comité d'éthique est bien mais ce n'est pas suffisant. L'éthique pose les questions fondamentales sur ces choix de société, elle peut être complémentaire au droit, mais ne peut le remplacer. D'autant qu'il faut clairement poser les problèmes. Or, on nous dit, pour nous rassurer, avec la reconnaissance faciale « *on cherche des comportements, non des personnes* ». Cette déclaration relève d'une incompréhension des réalités du profilage et du traitement algorithmique. D'abord, on n'a pas besoin de connaître l'identité d'une personne pour pouvoir l'identifier. Ensuite, l'enjeu est de savoir si on considère les individus comme des sujets de droits, ou si on les résume à l'agrégation de leurs données et au calcul de scores de dangerosité.

C'est la raison pour laquelle, au niveau européen, les usages d'intelligence artificielle à hauts risques dont fait partie la reconnaissance faciale seront soumis à des études d'impact détaillées. Et les textes à venir viendront certainement les limiter…

Et pourtant, cette technologie a tendance à se banaliser, il suffit de penser aux nouvelles versions des smartphones qui utilisent des empreintes biométriques (visage, empreintes digitales) …

On s'acclimate peu à peu aux technologies qui nous surveillent. Or l'usage de ces technologies n'est pas neutre. Il ne s'agit pas d'une simple commodité. Réfléchissons à deux fois avant d'accepter d'allumer notre téléphone portable via notre empreinte digitale ou la reconnaissance faciale pour gagner « simplement » 2 secondes, plutôt que d'avoir recours à un code !

Cela illustre bien le risque qui se présente à notre société : être dirigée par des choix technologiques qui ne sont soumis à aucun débat démocratique. La norme étant intégrée en temps réel dans le code

informatique des plateformes que nous utilisons au quotidien, nos comportements s'en trouvent déterminés sans n'avoir été précédés d'aucun dialogue social et politique.

Les systèmes publics de reconnaissance faciale se banalisent aussi. Qu'est-ce qui légitime cette surveillance, cet enregistrement continu des faits et gestes sinon l'anxiété de nos sociétés et l'impératif de sécurité ? On est dans une société qui n'accepte pas l'incertitude. On se dit que la caméra ne change rien pour ceux qui n'ont rien à se reprocher et qui donnent déjà beaucoup d'informations sur eux sur les réseaux sociaux. On considère qu'on peut être à la fois libre et surveillé. Autant de raisons qui justifient que nous sommes aujourd'hui dans un triple état d'urgence : sanitaire, terroriste et économique !

Les usages abusifs et liberticides de cette technologie sont déjà nombreux ! S'y ajoutent les failles techniques relevée ici et là : à Londres, par exemple, le système mis en place pour identifier les personnes recherchées accuserait un taux d'erreur d'environ 80% !
https://www.essex.ac.uk/news/2019/07/03/met-police-live-facial-recognition-trial-concerns

On commence par surveiller les transports, puis on arrive aux écoles, aux lieux de culte, aux festivals, aux stades, aux jardins, aux lieux d'habitation et de travail. Le risque suprême c'est la surveillance totale de la population, en temps réel.

Ce déploiement massif pourrait ainsi se normaliser, sans que cela ne nous choque plus, comme l'illustre le scandale Clearview, cette entreprise américaine qui se voit reprocher d'avoir collecté plus 3 milliards de photographies sur internet, principalement sur les réseaux sociaux. Des centaines de services de police aux États-Unis ont ainsi utilisé ce système en l'interconnectant avec des fichiers de personnes condamnées. On voit ainsi comment l'association de différentes technologies nous fait entrer dans une infrastructure de surveillance !

Tout dépend donc des datas utilisées en relation avec ces systèmes, car ce n'est pas la même chose d'appliquer la reconnaissance faciale au fichier des personnes recherchées (qui concerne plus que 600 000 personnes) qu'au traitement des antécédents judiciaires (qui concerne près de 20 millions de personnes) ! Par ailleurs, le périmètre de ces fichiers est potentiellement très large : il comprend aussi bien les personnes concernées par certaines mesures administratives (débiteurs du Trésor, interdits de stades…) que celles recherchées dans le cadre d'une enquête judiciaire que celles constituant une menace pour l'ordre public ou la sûreté de l'État.

En plus, comme vous le soulignez, le risque de détournement d'usage et de piratage est important. Une fois que la base de données biométrique des millions de visages sera constituée et prête à l'emploi, comment ne pas s'empêcher d'y avoir recours dans d'autres contextes ou pour d'autres finalités, comme par exemple la détection des émotions ?

Heureusement, il y a des résistances : des villes comme San Francisco ont voté une interdiction de l'utilisation de la reconnaissance faciale par la police. Les associations de défense des libertés publiques et les chercheurs continuent à lancer des appels à moratoire. Beaucoup luttent contre la banalisation de l'usage des technologies et de leur glissement subreptice à l'ensemble des secteurs de la société.

Comment poser le débat de manière raisonnable dans le contexte des prochains jeux olympiques ?

La première question à se poser est celle de la pertinence de l'outil technologique : la reconnaissance faciale est-elle l'outil adéquat pour la situation envisagée ? Est-il proportionné à la finalité

envisagée ? Qui peut y avoir accès ? Dans quel contexte ? Selon quels gardes de fous permettre la surveillance sans un consentement préalable des individus ? …

Concernant les JO de 2024 de Paris, il ne peut y avoir de déploiement large de ces technologies sur le territoire sans un préalable travail de sensibilisation et d'information des usagers. Il convient également de définir des règles plus précises pour encadrer les expérimentations, en fonction du niveau de risques présenté.

Mais malgré cela, l'encadrement strict de cette technologie risque hélas d'être dépassé par les systèmes développés dans plusieurs endroits du monde.

3. Pour un Parquet National du Numérique

> *Source : Dans un article de doctrine de 2017 (« Pour un parquet national du numérique et une 33ème chambre de la cybercriminalité », Adrien Basdevant, édition Lamy numérique), nous suggérions la création d'un parquet national du numérique pour les infractions de cybercriminalité complexes, puis à nouveau dans l'ouvrage « L'Empire des données – Un essai sur la société, les algorithmes et la loi » (Don Quichotte, 2018). Cet article de revue juridique présentait ainsi l'opportunité que constituerait une spécialisation de l'ensemble de la chaîne pénale de l'enquête, à l'instruction, jusqu'à la phase de jugement; ainsi qu'à une meilleure formation des magistrats.*
>
> *Dans son avis du 29 avril 2021 sur la sécurité numérique, la Commission supérieure du Numérique et des Postes (CSNP) vient de recommander au Gouvernement, d'« étudier la création d'un parquet national cyber, disposant des ressources et des expertises suffisantes pour instruire les dossiers liés aux affaires de cyber-délinquance les plus complexes.»*
>
> *A l'heure où le Parquet Européen Financier va débuter ses premières procédures, la nécessité de réfléchir à un Parquet Européen du Numérique semble plus que jamais d'actualité.*
>
> *Dans ce contexte, l'usage des technologies par les acteurs publics devraient également participer à cette mission d'identifier les auteurs d'actes criminels en relation avec des infractions éminemment complexes. Réfléchir à une meilleure offre de sécurité, comme vous l'y invite votre mission, nécessite de réfléchir à une meilleure juridictionnalisation des éventuelles infractions complexes commises en relation avec les nouvelles technologies, afin d'assurer une prévisibilité et une effectivité de la sécurité juridique en lien avec ces outils.*

La cybercriminalité sera au cœur du contentieux de demain. Combien d'attaques informatiques révélées, de réseaux en lignes démantelés suffiront à nous en faire prendre pleinement conscience ? À l'heure où l'ensemble de notre société et de notre économie est mis en données, le risque réside dans l'explosion de cette délinquance, alors qu'un sentiment d'impunité persiste.

Qu'est-ce que la cybercriminalité ? Ses facettes sont multiples. À défaut de l'existence d'une définition légale consacrée, la cybercriminalité recouvre l'ensemble des infractions pénales

tentées ou commises à l'encontre ou au moyen d'un système d'information et de communication. Elle s'étend de l'escroquerie, aux vols de données, en passant par l'usurpation d'identité, mais renvoie également à la pédopornographie, la diffusion de contenus illicites ou malveillants, l'espionnage de sociétés ou encore la saturation de sites internet. Cette activité peut s'avérer très lucrative. En trois ans, *Silk Road*, le plus grand site de vente de drogues au monde, aurait généré un trafic évalué à 1,2 milliard de dollars avec des commissions de l'ordre de 80 millions de dollars.

La cybercriminalité se « démocratise ». Loin de cibler uniquement les grands groupes, elle atteint aujourd'hui indifféremment petites et moyennes entreprises, individus, et collectivités. Tous les secteurs sont concernés, de l'agriculture à l'éducation en passant par l'industrie lourde, car désormais la quasi-totalité de nos activités et interactions sont reliées à un système d'information, et par conséquent vulnérables aux intrusions et piratages. En effet, chaque organisation devient une entreprise de technologie de l'information dont les données constituent une richesse convoitée.

Un manque de sensibilisation. Ce constat inquiétant révèle un déficit de connaissance minorant sa gravité. Les contremesures proposées sont aujourd'hui insuffisantes. Dans ce contexte, il devient urgent de réfléchir aux modalités d'organisation collective pour lutter contre ces menaces, encore peu maîtrisées, mais qui deviendront à n'en pas douter notre quotidien de demain. Cette nouvelle forme de délinquance fait fi des frontières et ne peut être appréhendée qu'à travers son aspect transnational de sorte que la première nécessité réside dans la mise en place d'une coopération internationale efficace. Elle présente en outre un degré de complexité rendant nécessaire une spécialisation pointue des acteurs et des outils afin de mieux saisir les mécanismes employés, comme dans le cas d'emploi de processus d'anonymisation par le navigateur TOR (*The Onion Router*) ou de demandes de rançon en *bitcoin*.

***Silk Road*, un exemple topique.** Fermé par le FBI en novembre 2014, le site « route de la Soie » proposait, entre autres, d'après l'accusation, la vente et l'achat, uniquement en *bitcoin*, de drogues, armes, faux papiers, et des services de tueurs à gages. Durant le procès, les avocats de Ross Ulbricht - poursuivi pour avoir dirigé ce marché noir et finalement condamné par les juridictions américaines en mai 2017 à la réclusion criminelle à perpétuité - ont remis en cause plusieurs aspects de l'enquête, en particulier le comportement de deux agents fédéraux qui ont tenté d'extorquer et faire chanter l'accusé. Shaun Bridges, membre des services secrets américains, a ainsi été condamné après avoir plaidé coupable du détournement de 800.000 dollars en devise électronique *bitcoin.* Quand Carl Mark Force, agent de la DEA (service de la Justice américaine en charge de la lutte contre les stupéfiants - *Drug Enforcement Administration* en anglais) a écopé de 78 mois de prison pour extorsion de fonds et blanchiment d'argent. Cette affaire complexe souligne les spécificités inhérentes aux technologies, et la nécessité de former les prochaines générations d'enquêteurs, de juges et d'avocats pour en appréhender toutes les subtilités. Une spécialisation de l'ensemble de la chaîne pénale paraît nécessaire : de l'enquête, à l'instruction, jusqu'à la phase de jugement.

L'analogie avec le Parquet National Financier. Les limites actuelles pour lutter contre la cybercriminalité ressemblent à celles qui existaient en matière économique et financière avant la création, en 2014, du Parquet National Financier : aggravation et complexification de la délinquance économique, absence d'interlocuteur précisément déterminé au niveau national et international, spécialisation insuffisante des magistrats, insuffisance des moyens humains et techniques, coût du manque à gagner résultant de la fraude. Le Parquet National Financier pourrait ainsi servir d'exemple. La création d'un Parquet spécialisé dans le numérique permettrait de répondre aux problématiques posées par les infractions propres aux réseaux électroniques, notamment les attaques visant les systèmes d'information, le déni de service et le piratage ainsi que celles commises à l'aide des réseaux de communication électroniques et de systèmes d'information lorsque celles-ci atteignent un certain degré de complexité ou constituent des atteintes particulièrement graves. Son niveau élevé de spécialisation et les outils de pointe qui lui seraient confiés permettraient par exemple d'identifier les auteurs ayant recours à des processus de chiffrement et de récolter des preuves rendues plus difficiles à obtenir par des technologies avancées. Certaines initiatives ont déjà été déployées dans l'État de Rio au Brésil, ou en Espagne où existe un Procureur Général en charge de la cybercriminalité qui bénéficie de l'aide de 70 parquetiers réunis au sein d'un parquet spécifique dédié à ce type de criminalité.

La formation des magistrats. La création d'une filière judiciaire numérique suppose de débattre en amont du type de spécialisation des magistrats, de leur nombre, de la centralisation ou la décentralisation d'un tel parquet, voire de la possibilité de mettre en œuvre un parquet au niveau européen. Un enjeu majeur sera alors de coordonner l'action du Parquet du Numérique avec les différents services spécialisés existants, le numérique étant souvent un moyen permettant à la grande délinquance organisée de blanchir l'argent ou de financer des réseaux terroristes, pour lesquels d'autres organes sont déjà compétents. A terme, la création d'une 33ème Chambre correctionnelle spécialisée et exclusivement dédiée au jugement des infractions instruites par le Parquet National du Numérique - à l'image de la 32ème Chambre correctionnelle, dédiée aux affaires émanant du Parquet National Financier (Affaire Cahuzac, Wildenstein, etc.) - pourrait s'avérer pertinente. Besoin de formation donc au numérique, pour ces nouvelles compétence mixtes, notamment juridiques et techniques.

La pertinence d'une coordination paneuropéenne. L'ensemble des constats qui précèdent amène à envisager une coopération à un niveau supranational, notamment en considération du caractère substantiellement transnational de la cybercriminalité. Au soutien de la mise en œuvre d'un tel mécanisme de coopération, retenons le raisonnement développé par les institutions de l'Union européenne pour la mise en place d'un parquet européen pour les infractions pénales portant atteinte aux intérêts financiers de l'UE. Les questions de sécurité, justice et droits fondamentaux relevant des compétences partagées entre l'UE et les Etats membres, le principe de subsidiarité trouve ici une application particulièrement pertinente en ce qu'une action au niveau européen serait beaucoup plus efficace pour combattre les infractions relevant de la cybercriminalité. À ce titre, la création d'un Parquet Européen du Numérique concrétiserait également plusieurs des priorités de l'UE en matière de Justice, par exemple concernant la protection des consommateurs dont l'objectif affiché est

notamment d'adapter le droit de la consommation à l'ère du numérique mais également d'apporter *« une réponse plus forte, coordonnée et globale face à […] la cybercriminalité »*.

L'urgence nous commande dès à présent de réfléchir à l'évolution du contentieux lié au numérique au niveau européen. Cette évolution paraîtra prospective pour certains. L'anticiper est pourtant primordial. La conduite du changement est un long processus. Mais inéluctablement cela sera l'unique façon de disposer demain de parquetiers et de services d'enquêtes disposant des connaissances et des moyens nécessaires pour aborder les affaires de cybercriminalité.

4. Questions à adresser

Source : En complément des réponses aux questions posées lors de notre audition du 3 juin 2021, voici certains points d'attention.

- La question est davantage celle des usages que des technologies. Par exemple, l'interconnexion en temps réelle à des fins de contrôle plutôt que les technologies sous-jacentes le permettant. En effet, les technologies évoluent rapidement, il est donc plus constructif de proposer des politiques publiques sur les usages qui en sont faits.
- Eviter de mettre toutes les technologies et usages dans le même sac. La vision par ordinateur ne signifie pas nécessairement traitement de données biométriques, ni reconnaissance faciale.
- Certains nouveaux outils mis à disposition des forces de l'ordre devrait faire l'objet d'un débat démocratique (exemple : 500 commissariats seront bientôt équipés d'un outil pour aspirer les données d'un smartphone en 10 minutes)
- Anticiper les possibles contrôles communs, par exemple CNIL avec Défenseur des droits.
- Comment / Par quels outils réaliser ces contrôles ? L'étude d'impact (DPIA) du RGPD devrait être complété pour intégrer d'autres dimensions (notamment biais, discrimination, etc.). C'est d'ailleurs le sens de la prochaine régulation européenne sur l'IA (cf. projet Commission européenne d'avril 2021). Cela renvoie d'ailleurs à la précédente question sur qui sera en charge de contrôler ce nouveau texte européen, la CNIL ?
- Faut-il créer de nouveaux acteurs ou instances ? Qui des observatoires algorithmiques, tiers indépendants (par exemple pour contrôler l'usage faits des données et technologies par les agents publics, possibilité d'étude des codes et mécanismes des solutions algorithmiques utilisés par le public à des fins de sécurité).

Contribution écrite à la demande de Monsieur Jean-Michel Mis, député, dans le cadre de sa mission « Pour un usage responsable et acceptable par la société des technologies de sécurité »

Claude Kirchner
Directeur du Comité national pilote d'éthique du numérique
31 mai 2021

Monsieur le Député,

Je vous remercie de votre sollicitation et de votre confiance.

La réponse que je vous fais résulte de réflexions issues du Comité national pilote d'éthique du numérique (CNPEN) et de mes implications tant scientifiques que dans les instances nationales et internationales portant sur le numérique et ses nombreuses implications sociétales, en particulier en cybersécurité.

Le sujet de votre mission est capital pour notre société et son avenir. Dans la profonde conversion numérique que nous vivons, la dualité entre confiance et sécurité prend une dimension bien supérieure à celle qu'elle pouvait avoir auparavant. Interroger les enjeux d'éthique qui apparaissent dans ce contexte pourrait certainement faire le sujet d'une saisine du CNPEN dans le proche avenir et permettre de traiter le sujet et d'approfondir des éléments que je vous soumets ici. Cela inclut le sujet spécifique des avancées scientifiques et techniques en reconnaissance faciale dont le CNPEN s'est récemment auto-saisi. Je vous joins la description de cette saisine sur la « Reconnaissance faciale, posturale et comportementale : entre questionnements et enjeux d'éthique », qui devrait déboucher sur un avis publié fin 2021.

Je me tiens bien entendu à votre disposition dans le cadre de la suite de vos travaux.

Considérations générales

Avant de donner des éléments de réponses aux questions que vous me posez, il me semble utile de préciser quelques éléments.

En français, les termes sécurité et sûreté sont souvent considérés comme synonymes ou utilisés suivant les communautés ou les disciplines scientifiques ou techniques l'un pour l'autre. C'est une source de confusion potentielle qu'il ne faut pas ignorer. Dans la suite de cette note, j'utiliserai le terme *sûreté* pour désigner la qualité d'un dispositif physique ou informationnel à réaliser correctement la fonction pour laquelle il est conçu, dans un contexte complètement maitrisé, le terme anglo-saxon correspondant étant *safety*. Je parlerai de *sécurité* pour désigner la qualité d'un dispositif à rester conforme à sa fonction même en cas d'interaction avec son contexte de fonctionnement pouvant (souvent intentionnellement) le perturber, en anglais *security*.

Sur les enjeux que vous abordez, la notion de proportionnalité est fondamentale. En termes de risque épidémique, faire face à une épidémie de Covid ou à une épidémie de fièvre Ébola ne mettra pas en œuvre le même type de mesure en fonction de l'importance du risque mortel. Dans la mise en œuvre des technologies de sécurité, l'explicitation des risques encourus et de leurs conséquences potentielles est fondamentale. L'émergence de nouveaux risques liés à de nouvelles capacités humaines ou technologiques (ou leur combinaison) favorise l'émergence de craintes, voire de peurs. Je pense important de veiller à ce qu'elles n'érodent la valeur fondamentale de

liberté, démocratiquement assumée. Nos instances démocratiques doivent dans ce contexte veiller à éviter ou minimiser les effets de dépassement de seuil souvent appelés effets cliquets.

Éléments de réponses aux questions posées

Quels sont selon vous les principaux enjeux de liberté dont il est question face aux technologies de sécurité ?

Affichée au fronton de nos mairies et de nombreux établissements publics, la valeur Liberté est la première de notre république. Cette valeur est multiforme et centrale dans le dilemme entre liberté de l'individu et liberté collective. La Covid-19 en a été un exemple remarquable entre liberté de déplacement individuel et capacité collective à protéger chacun d'entre nous.
Sans sécurité des biens, des personnes et des informations (information est ici compris au sens conceptuel plus approprié en français que le terme « donnée ») il ne peut y avoir de liberté ni des individus, ni collective. La sécurité est en effet nécessaire à l'établissement de la confiance sans laquelle il n'est pas possible de se retrouver dans un espace de liberté.

Le triangle entre liberté, confiance et sécurité est complexe car une tension existe également entre sécurité et confiance. En effet, et tout particulièrement dans le monde numérique, les moyens d'assurer la sécurité repose sur la confiance : confiance dans l'accès proportionné aux données personnelles, confiance dans l'audit des moyens techniques mis en œuvre mais aussi confiance dans les moyens de se protéger, typiquement confiance dans les programmes permettant de chiffrer l'information. L'exemple des portes dérobées (*backdoors)* permettant d'ouvrir l'accès à des informations supposées chiffrées en est un exemple important : de tels moyens d'accès rompent la confiance dans les outils proposés et dans ceux qui les promeuvent.

Le terme liberté est polysémique et concerne aussi bien la capacité d'expression, la capacité d'atteindre l'attention d'une personne (parler à une personne particulière), la capacité de déplacement, de penser, d'agir, ou encore la capacité à se réunir.

Préserver les différents aspects de la sécurité dans un contexte social, national et international complexe peut amener à prendre des mesures basées sur la limitation des libertés individuelles ou collectives. Se baser sur les retours d'expérience des organisations de grands évènements internationaux ne parait pas nécessairement approprié : on peut penser par exemple aux dispositifs de sécurité qui ont été ou seront mis en place par la Chine et la Russie et qui reposent sur des valeurs et des acceptabilités de leurs populations qui sont différentes des nôtres.

Dans le contexte européen et en particulier français, il faudra prendre en compte également la proposition de réglementation européenne de l'IA (*Artificial Intelligence Act* du 21 avril 2021) qui d'ici les prochains évènements sportifs organisés par la France en 2023 et 2024 sera sans doute applicable et qui dans l'état actuel de la proposition pose de nombreuses questions sur la mise en œuvre de la reconnaissance faciale.

Quelles technologies et usages vous inspirent le plus de prudence quant au respect de ces libertés ?

J'ai cité précédemment la mise en place de portes dérobées (aussi appelées clef maitre). La reconnaissance faciale ou comportementale, la géolocalisation, l'exploitation des données d'usages, … et génériquement toutes les technologies permettant d'acquérir des informations sur les personnes doivent être considérées avec la plus grande prudence et doivent faire l'objet d'une vigilance démocratique active et non naïve.

Comment assurer l'équilibre, dans une société toujours plus imprégnée de technologies, entre les impératifs de liberté et de sécurité ?

Cette balance est historiquement connue pour être difficile. L'émergence de nouvelles technologies rend l'équilibre encore plus difficile à atteindre puisque les attaquants comme les défenseurs disposent de moyens plus performants dans une escalade difficilement maitrisable d'autant que les moyens mis pour compromettre la sécurité peuvent être absolument considérables tant du point de vue humain que technologique. La proportionnalité des mesures de sécurité doit alors être au cœur des mesures de sécurité prises, comme évoqué plus haut
L'un des éléments nouveau central à prendre en compte est la manipulation à grande échelle des opinions individuelles ou publiques mettant en jeu l'une des libertés les plus essentielle à l'être humain, la liberté de penser. Des affaires telles que celle de Cambridge Analytica ont montré combien la sécurité ne dépend plus seulement de moyens physiques ou informationnels mais aussi de la capacité à détecter les manipulations de personnes ou de foules (physiques ou numériques).
Il est remarquable que dans ce contexte, le Chili vienne d'inscrire dans sa constitution la notion de neuro-protection : « *On October 7th, 2020, the Chilean congress presented an amendment to the Constitution that defines mental identity, for the first time in history, as a right that cannot be manipulated. Additionally, the amendment states that any mental intervention, including medical therapies, must be legally regulated.*
On April 12th, 2021 the Chilean congress approved the final text amending article 19 of the Constitution endorsing the rights to physical and mental integrity and protecting cerebral activity and its data. » (voir https://nri.ntc.columbia.edu/projects).

Quelle perception avez-vous d'une association citoyenne à la définition des conditions d'appropriation de ces nouvelles technologies, à des fins de sécurité mais aussi plus généralement ? Quelle forme cette association pourrait-elle prendre ? Quelles technologies particulières devrait-elle nécessairement couvrir ?

Cette association citoyenne est importante et fondamentalement délicate car elle repose sur des hiérarchies de valeurs qui ne sont pas partagées par tous et qui peuvent être très contextuelles. Par exemple, des technologies intrusives comme la reconnaissance faciale peuvent être tolérées ou acceptées par certains à l'entrée d'un stade alors que dans une rue ou une gare elles pourront être ressenties comme trop intrusives. Les objectifs de telles associations citoyennes doivent donc être clairement spécifiés et maintenus dans leurs déroulés. S'agit-il de définir des mesures d'acceptabilité d'usages du numérique qui seront de toutes les manières employées ? De préparer la réflexion globale sur ces thèmes pour éviter une trop forte polarisation du débat lorsqu'il émergera dans la sphère publique ? D'éviter les recours de dernière minute d'associations et autres représentants de la société civile ? Autrement dit, comment prendre en compte en amont les possibilités de crispations qui risquent de surgir, certaines tardivement ? Il s'agit certainement de favoriser l'émergence de contributions de la manière la plus constructive possible : consultations citoyennes, appels à contributions, états généraux, tables rondes, grands débats, comité de suivi citoyen ; tout en sachant qu'aujourd'hui les citoyens ne sont (malheureusement) pas suffisamment familiers et encore moins formés, en France, à ce type de contribution.

Il faut aussi prendre en compte les expériences, notamment récentes, sur des comités de suivi comme celui de SIDEP et Contact Covid et comprendre s'ils ont été satisfaisants et représentatifs en particulier des opinions citoyennes. Le manque de représentativité ayant pour conséquence la perte de confiance et l'absence d'appropriation des travaux. De tels comités ont aussi pour objectif de favoriser les discussions pour co-construire ou co-adapter des propositions de régulation entre citoyens, administration et régulateur, dont bien sûr la CNIL.

Ce type de comités est intéressant et utile pour créer de la compétence et de la confiance, mais ils sont aussi difficiles à mettre en place pour des technologies de surveillance qui, par définition, sont

très intrusives – questions de l'accès à des informations sensibles – et nécessitent par conséquent de veiller à créer davantage de confiance dans les systèmes d'audit de ces outils.

Bien sur les expériences des associations citoyennes dans d'autres pays européens seront utiles à prendre en compte et de telles initiatives devraient aussi s'appuyer sur des comités existants ayant cette expérience et cette compétence comme le CESE, le CNPEN, le CNNum ou la CNIL.
L'expérience de l'appel à contributions, lancé en juillet 2020 par le CNPEN sur les enjeux d'éthique liés aux agents conversationnels (*Chatbots*), est utile à mentionner. Cet appel reposait sur la réponse à une série de questions dont les contextes étaient explicités. Les retours ont été particulièrement intéressants d'une part pour les contributions qui ont été faites aussi bien par des citoyens, des associations, des entreprises ou des administrations mais aussi, et presque davantage, pour l'utilisation de l'appel à d'autres fins que de contribuer à la réflexion du comité. En effet, nous avons eu des retours significatifs d'utilisation du questionnaire d'une part à des fins de sensibilisation ou de formation et, de manière non anticipée, en interne d'entreprises pour permettre l'appropriation de ces problématiques, la discussion et les échanges autour des enjeux d'éthique mis en question.

Quelle forme peut prendre une doctrine d'application du RGPD qui concilie le respect des libertés et l'exploitation des dérogations à des fins de sécurité ?

Je ne sais pas répondre à cette question aujourd'hui, mais pour y contribuer, il me semblerait intéressant de s'appuyer sur une réflexion conjointe de la CNIL, du CNPEN et du CNNum pour combiner les compétences du régulateur et des réflexions éthique et sociétale en numérique.

Les nouvelles technologies de sécurité suscitent d'importants besoins en compétences mixtes, notamment juridiques et techniques. Comment faites-vous face à ces évolutions pour assurer votre mission ?

Dans le cadre du CNPEN, une triple compétence est nécessaire, combinant les aspects techniques du numérique, les aspects éthiques et philosophiques et enfin les aspects légaux. Les cultures sont différentes, les vocabulaires utilisés peuvent être assez spécifiques, etc. De plus il est aussi important compte tenu de l'universalité du numérique d'associer des techniques autres en fonction du sujet abordé ; en médecine, en environnement, en sociologie par exemple. Les échanges issus de ces croisement conceptuels et d'usage sont très riches et nécessitent des méthodologies d'approche, de confrontation éventuelle et d'échange qui se bâtissent dans le temps. Elles sont vraiment fructueuses, mais demandent à la fois du temps disponible pour avancer ensemble et permettre d'aboutir à des combinaisons faisant sens. C'est tout l'intérêt de bâtir de telles instances de réflexion pour permettre de répondre de manière efficace aux sujets, nouveaux, qui ne manquent pas d'arriver. Il ne s'agit pas d'anticiper les sujets, mais d'anticiper la mise en place de méthodologie, de compétences et de savoir-faire pour aider à traiter les nouveaux sujets lorsqu'ils émergent.

Le monde de la donnée suscite un volume d'activité accru pour les régulateurs et les parties prenantes. Comment y faire face pour adapter le cadre protecteur à la société de demain ?

Le rôle des comités d'éthique m'apparait déterminant dans ce contexte. En effet régulation et droit ne peuvent se construire qu'en partant de réflexions éthiques permettant d'éclairer citoyens, décideurs et la société en général sur les choix possibles.
Les décisions de régulation et législatives liées à l'émergence de nouvelles technologies de sécurité, devront pouvoir s'appuyer sur les travaux d'un comité national d'éthique du numérique

de manière similaire à ce qui est réalisé depuis 1983 par le CCNE pour les sciences de la vie et de la santé dans le cadre de la biologie et de la médecine.

L'un des moyens de garantir un bon usage de ces technologies est de procéder avant tout à des expérimentations. Quelles seraient selon vous les conditions que ce cadre expérimental devrait réunir ?

Ces expérimentations sont importantes en effet.

Notons d'abord qu'il ne s'agira pas seulement de tester les technologies, de vérifier qu'elles fonctionnent comme escompté, mais de permettre aussi l'acculturation de participants actifs et passifs à ce type de techniques ainsi que de se rendre compte de toutes les dynamiques humaines que leur mise en place pourra susciter – y compris évitements, crispations, contestations, adhésion, etc. Pour ce faire un comité de suivi citoyen s'impose et doit pouvoir accéder en toute transparence aux informations nécessaires.

Mais il ne faut pas ignorer les limites de ces expérimentations : pour qu'elles aient un sens et une portée, il faut un important travail d'information, des retours sur expérience… or pour ce type de technologies, on ne peut avoir le consentement de tous. D'autre part, même si l'on parvient à informer toute la population potentiellement concernée de l'expérience à venir, les opposants à ces technologies ne seront pas volontaires pour y participer, voire s'y opposeront. Globalement, pour que de telles expérimentations soient fructueuses, il sera important :

- d'associer la population concernée *ab initio ;*
- de mettre en place un comité de suivi associant toute les parties concernées, publiant régulièrement et en toute indépendance ses conclusions ;
- de déterminer clairement et strictement les dates de début et de fin de l'expérimentation ;
- de veiller aux conditions de l'expérimentation, en particulier relatives au choix des cohortes choisies et des biais potentiels ;
- de garder la maitrise démocratique de tous les éléments de l'expérimentation. En particulier le recours à des sociétés privées devra se faire sous le contrôle strict du comité de suivi ;
- Des tiers de confiance clairement identifiés et crédibles devront être mis en place pour auditer les parties de l'expérimentation qui du fait de leur sensibilité nécessiteraient de garder confidentielles certaines informations.

---ooo---

Didier Baichère 07/06/2021

Contribution écrite – Didier Baichère
Député des Yvelines et Vice-président de l'OPECST

En complément du travail de Monsieur le rapporteur Jean-Michel Mis et de l'audition que nous avons eu ensemble, je tiens à m'exprimer pour présenter ma réflexion sur les enjeux posés par les dispositifs de reconnaissance faciale par l'intelligence artificielle (IA), nourrie par deux années de travail. Les dispositifs de reconnaissance faciale par l'IA reposent sur l'identification ou l'authentification visuelle d'individu par comparaison entre plusieurs photographies et/ou vidéos. Ils utilisent pour cela un type de données spécifiques : les données biométriques. La reconnaissance faciale par l'IA s'est imposée comme une des plus puissantes technologies biométriques d'identification et de contrôle de l'identité des personnes à partir d'une image numérique ou d'un support vidéo. L'identification ne repose alors plus sur des documents d'identité ou une position géographique, mais uniquement sur le visage de la personne elle-même.

En raison de sa nature, ces technologies sont directement visées par la mission parlementaire. Comme il est indiqué dans la lettre de mission, les nouvelles technologies dont la reconnaissance faciale par l'IA offrent de nombreuses perspectives notamment dans le champ des missions de sécurité. Dans un sondage Odoxa récent, conduit pour Saegus sur la reconnaissance faciale (mai 2021), les personnes interrogées associent spontanément la reconnaissance faciale à la surveillance (51%) et à la sécurité (41%) ; mais également à l'identité (40%), la technologie (39%) et à l'intelligence artificielle (39%). Ainsi, pour que la réflexion soit aboutie et complète, nous ne devons pas envisager la reconnaissance faciale seule mais la globalité des différents cas d'usages qu'elle induit. Se laisser enfermer dans un débat d'application purement sécuritaire ferme la porte au développement de nombreux usages pour la santé ou une meilleure inclusion (handicap, vieillissement et perte d'autonomie dont les collectivités locales pourraient se saisir...).
Un travail minutieux et en concertation avec toutes les parties prenantes a permis d'identifier les cas d'usage qu'englobait le terme souvent trop générique de reconnaissance faciale. Lors de la rédaction de la note scientifique sur la reconnaissance faciale en octobre 2019, j'avais observé que nous sommes bien souvent rattrapés par les usages des nouvelles technologies qui envahissent notre vie quotidienne. Peu de nos concitoyens se pose la question des fondamentaux scientifiques qui y sont associés et des conséquences sur la société que nous lèguerons à nos enfants. En effet, la reconnaissance faciale par l'IA représente une somme d'opportunités et de limites qui sont directement liées à la réflexion sur la société dans laquelle nous souhaitons vivre demain :

- La reconnaissance faciale par l'IA s'est imposée comme une des plus puissantes technologies biométriques d'identification et de contrôle de l'identité des personnes à partir d'une image numérique ou d'un support vidéo.
- Au cours des dix dernières années elle s'est immiscée dans notre vie quotidienne à travers différents usages comme le déverrouillage du téléphone.
- Les points de vue et prises de position sur cette technologie sont nombreux autant que divers : le sujet fait souvent polémique en raison des dérives sécuritaires qu'il inspire.
- Les collectivités locales en première ligne sur le sujet ne sont pas armées pour répondre à de telles problématique. Plusieurs collectivités et entreprises lancent ou ont lancé ces derniers mois en France les premières expérimentations d'usage de la technologie de reconnaissance faciale.

Après deux ans de travaux pendant lesquels j'ai auditionné de nombreux acteurs institutionnels, industriels et associatifs, je suis arrivé à deux conclusions :

1. Nous devons créer un **cadre d'expérimentation transparent et éthique** pour les technologies de reconnaissance faciale qui mobilisent l'IA aux fins d'en garantir un usage responsable. Il conviendra dans ce cadre de s'appuyer sur les progrès des méthodologies d'audit des algorithmes de l'IA et sur les réflexions en matière de droits à l'oubli dès lors que des données personnelles aussi sensibles que les données biométriques sont en jeu.

2. Nous devons organiser une consultation citoyenne effective, de type états généraux, afin de donner la parole aux citoyens français et de créer les conditions d'un débat éclairé et apaisé sur le sujet.

I Initier une expérimentation scientifique de trois ans avec une évaluation détaillée afin de pouvoir délimiter des lignes rouges et enrichir la réflexion et la connaissance nécessaire pour légiférer et réglementer ces technologies dans le futur.

L'intelligence artificielle, et plus particulièrement les technologies qui en découlent, est un sujet d'actualité permanent. La Commission européenne a proposé un projet de règlement pour permettre à l'Europe de rattraper son retard dans la course à l'IA et protéger ses citoyens de ses dérives. Cependant, nous connaissons le temps long de l'Union européenne. Il me semble donc important de ne pas l'attendre et de privilégier « une voie Française », celle qui permet d'aborder de manière méthodique, scientifique et éthique les différents cas d'usage de la reconnaissance faciale par l'IA. Il nous faut dans les mois à venir créer un cadre responsable qui protège le citoyen et les collectivités territoriales des dérives. Poser ce cadre expérimental, c'est aussi être force de proposition dans les débats européens pour avancer en cohérence et construire un modèle technologique éthique et humain.
Rien n'empêche les pays européens de converger sur le principe d'une approche méthodologique commune basé sur l'expérimentation et la consultation.

Parmi les multiples enjeux que pose la reconnaissance faciale par l'IA, notre souveraineté numérique en est une. Nous devons aussi construire un cadre qui assurera notre souveraineté industrielle dans le respect des libertés publiques. **Pouvoir expérimenter ces dispositifs de manière scientifique et raisonnée doit permettre de conclure à la nécessité ou non d'une évolution de la réglementation en la matière et de définir les potentielles lignes rouges : « cette évaluation des risques est nécessaire pour déterminer ceux qui ne sont pas acceptables dans une société démocratique et ceux qui peuvent être assumés moyennant des garanties appropriées ».** En effet, une réglementation imprécise dans sa rédaction pourrait être fatale et venir entraver l'innovation ; l'effet serait similaire à celui d'un moratoire et desservir les citoyens Français.
L'enjeu de la souveraineté technologique de la France est souvent mis en avant. Cependant, plus encore que cela, il s'agit d'encadrer les expérimentations pour qu'elles se déroulent à l'image de nos valeurs éthiques et démocratiques. Instaurer une expérimentation permettra de cadrer le pilotage par un comité de supervision, le périmètre, les acteurs et les territoires et ainsi empêcher les expérimentations « sauvages ».
Cette expérimentation scientifique de la reconnaissance faciale par l'IA, cadrée par une proposition de loi, proposerait une méthodologie scientifique précise et détaillée pour différents cas d'usage pour être au plus près des enjeux et garantir l'éthique et la transparence de la démarche.

- **Pour faire face à la réalité de l'utilisation de ces technologies, un raisonnement par cas d'usage s'impose.**

Appréhender les enjeux que posent ces nouvelles technologies dans leur ensemble biaise le débat car ils dépassent les simples aspects sécuritaires. La sureté et la sécurité des espaces sont un cas d'usage parmi d'autres. J'aime à en citer trois autres à titre d'exemple : la gestion de flux, les services de santé et sociaux et les services marketing. Aborder la question à travers différents cas d'usage permettra de mieux comprendre les arbitrages à effectuer, car chacun d'eux nécessite un protocole particulier d'expérimentation afin d'être le plus précis possible. Ainsi, cette distinction des usages permettra notamment de fixer des lignes rouges plus adaptées à la réalité. La sensibilité des algorithmes peut être différentes selon les cas d'usage.

- **Pour un usage éthique et transparent de ces technologies, deux paramètres doivent être pris en compte pour une expérimentation réussie : la création un comité de supervision qualifié à même de définir des protocoles stricts et la mise en place d'une méthodologie d'audit des algorithmes utilisés.**

Le rôle du comité de supervision de l'expérimentation est de répondre aux doutes exprimés face à ces technologies et ses usages, et d'assurer une impartialité dans les débats et les orientations. Ce comité composé à la fois de scientifiques et de personnes qualifiées de la société civile pourra se concentrer sur la définition de la méthodologie à développer, au bon déroulement de l'expérimentation pour chacun des différents cas d'usage.

L'une de ces missions primordiales pour assurer l'éthique de l'expérimentation sera également d'évaluer en détail l'expérimentation, de veiller au développement de l'audit de la méthodologie et du comportement du système d'apprentissage. Développer l'audit de la méthodologie scientifique des algorithmes de reconnaissance faciale utilisée dans les expérimentations serait un premier pas pour garantir leur conformité scientifique et éthique comme le souligne le rapport Donner un sens à l'intelligence artificielle : pour une stratégie nationale et européenne : « *il faut accroître la transparence et l'audibilité des systèmes autonomes d'une part, en développant les capacités nécessaires pour observer, comprendre et auditer leur fonctionnement et, d'autre part, en investissant massivement dans la recherche sur l'explicabilité.* ».[1] Cette question de l'audit n'a pas été exploitée par la suite. Pourtant, l'audit est une évidence dans les processus industriels, elle doit pouvoir le devenir dans la reconnaissance faciale. Le sondage Odoxa conduit pour Saegus sur la reconnaissance faciale, publié en mai 2021, montre d'ailleurs que les Français interrogés soutiennent tous les moyens permettant de se prémunir des risques de la reconnaissance faciale : Commission réunissant experts et citoyens (77%), audit des algorithmes (64%) et souveraineté (82%).

2 Organiser une consultation citoyenne effective afin de définir collectivement la société de demain

La reconnaissance faciale par l'IA s'est installée dans le débat public. Comme c'est souvent le cas pour ces nouveaux usages qui s'installent rapidement dans nos vies quotidiennes, ils sont accompagnés de mythes et de fantasmes qui rendent caduques toute réflexion éthique. L'usage en matière de reconnaissance faciale se développant, la qualité scientifique nécessaire à garantir la vie privée et à fournir une aide à la décision passe finalement dans l'inconscient collectif au second plan. De plus comme le souligne le sondage cité plus haut, les Français se sentent de plus en plus mal informés sur l'utilisation de leurs données par des technologies de reconnaissance faciale (75% aujourd'hui contre 72% en 2020) alors même que le sujet est de plus en plus évoqué dans le débat public et dans l'actualité.

[1] *Donner un sens à l'intelligence artificielle : pour une stratégie nationale et européenne,* Cédric Villani - Marc Schoenauer - Yann Bonnet - Charly Berthet - AnneCharlotte Cornut - François Levin - Bertrand Rondepierre, 28 mars 2018, P. 138

En conséquence, je suis favorable **à l'organisation simultanée d'une consultation citoyenne effective de type états généraux,** sur le modèle de ce qui est fait pour les lois de bioéthique, **afin de faire naître les conditions d'un débat citoyen et pédagogique, afin d'éclairer et mesurer les perceptions des Français et enfin de détecter les lignes rouges à ne pas franchir.** Instituer des états généraux permettra d'élever le débat et de tirer des recommandations plus détaillées avec la remise d'un rapport qui sera étudier à l'Office parlementaire d'évaluation des choix scientifiques et technologiques. A ce titre, il est important, qu'au préalable à tout projet de réforme de la régulation en matière de reconnaissance faciale voire d'évolution dans l'utilisation des données biométriques, de donner la parole aux citoyens français.

Conclusion

Je défends donc la nécessité d'une loi d'expérimentation qui permettra de cadrer à la fois le pilotage par un comité de supervision, le périmètre, les acteurs et les territoires concernés par une expérimentation et enfin les modalités d'une consultation citoyenne effective pour faire la pédagogie nécessaire sur les opportunités et les limites que représentent la reconnaissance faciale par l'IA. Cette loi d'expérimentation et de méthodologie traduira les engagements en matière de transparence et d'éthique que je souhaite voir appliqués aux acteurs et aux technologies de développement de la reconnaissance faciale dans l'espace public. C'est d'ailleurs pour cette raison que j'ai choisi de déposer une proposition de loi d'expérimentation créant un cadre d'analyse scientifique et une consultation citoyenne sur les dispositifs de reconnaissance faciale par l'intelligence artificielle**, n° 4127** qui a inspiré cette contribution écrite. L'intelligence artificielle, et plus particulièrement les technologies qui en découlent, est un sujet d'actualité permanent. En témoigne la récente prise de position de la Commission européenne qui a publié un projet de règlement pour permettre à l'Europe de rattraper son retard dans la course à l'IA et protéger ses citoyens de ses dérives. D'ailleurs, sans détailler, les articles 53 et 54 de ce projet de règlement européen propose un protocole pour des expérimentations, des « bacs à sable d'IA » afin de tester les algorithmes dans des environnements et durées contrôlés. Cependant, nous ne pouvons attendre : nous connaissons le temps long de l'Union européenne.

Enfin, je souhaite privilégier « une voie Française » celle qui permet d'aborder de manière méthodique, scientifique et éthique les différents cas d'usage de la reconnaissance faciale par l'IA. Il nous faut dans les mois à venir créer un cadre responsable qui protège le citoyen et les collectivités territoriales des dérives. Poser ce cadre expérimental, c'est aussi être force de proposition dans les débats européens pour avancer en cohérence et construire un modèle technologique éthique et humain. D'ailleurs, les Français interrogés dans le cadre du sondage cité vont dans ce sens que la souveraineté n'est pas négociable : 82% d'entre eux affirment qu'il est important que la France se dote des moyens de développer et d'exploiter ses propres technologies d'IA plutôt que d'utiliser des technologies étrangères.

C'est d'autant plus important qu'en plus de cette question de souveraineté numérique, la pandémie nous a permis de prendre conscience des potentielles nouvelles applications que les nouvelles technologies offrent. A titre d'exemple, je peux vous citer l'algorithme qui détecte dans les transports si les usagers portent correctement le masque avec un technologie d'anonymisation des données contrôlée et suivie de près par la CNIL. Il me semble important que la méthode scientifique, celle que je propose dans cette contribution écrite et plus en détail dans ma proposition de loi, soit le raisonnement systématique à adopter. Le caractère scientifique et éthique de cette méthode permettra de construire un cadre adapté non seulement pour les dispositifs de reconnaissance faciale par l'IA mais à tous ces nouveaux usages qui émergent. Comme il est rappelé dans la lettre de mission, la France va accueillir dans les prochaines années des événements sportifs de grandes envergures tels que la coupe du monde de rugby en 2023 ou les jeux olympiques en 2024. Ces échéances sont certes

importantes pour notre rayonnement international, elles le sont également pour mettre en place une expérimentation sérieuse comme je le propose afin de définir un cadre et lancer une consultation citoyenne.

Mission du député Jean-Michel Mis

« Pour un usage responsable et acceptable par la société des technologies de sécurité »

*

1/ Objectifs de la mission

La mission souhaite explorer, lors des auditions et via les contributions écrites, les axes suivants :

- Les **opportunités offertes par les nouvelles technologies au service d'une meilleure offre de sécurité** en analysant les besoins des forces de sécurité, entre autres dans la perspective des grands événements sportifs de 2023 et 2024.

- Les principes nécessaires à **la préservation des libertés** en définissant un cadre d'emploi global et cohérent des technologies de sécurité et en associant la société civile à cette définition pour renforcer la compréhension et l'acceptabilité des nouvelles technologies dans la société.

Table des matières – Réponses de CCE

QUESTIONNAIRE REMPLI PAR CHARLES BURGEAT, CCE COMITE SUEDE 2
QUESTIONNAIRE REMPLI PAR XAVIER DUPONT, CCE COMITE HONG KONG 4
QUESTIONNAIRE REMPLI PAR MORANE REY-HUET, CCE COMITE AUVERGNE RHONES-ALPES 6
QUESTIONNAIRE REMPLI PAR VERONIQUE DENIS-PELLIET, CCE COMITE SINGAPOUR 8
QUESTIONNAIRE REMPLI PAR LAURENT DELON, CCE COMITE USA 9

QUESTIONNAIRE REMPLI PAR CHARLES BURGEAT, CCE COMITE SUEDE

Questions

La notion de « technologies de sécurité » est large. Quelles sont les principales selon vous ? *[Par exemple : traitement des données (textuelles, images, sonores), biométrie, mobilité.]*

- *La collecte de données via des capteurs (e.g. cameras) fixes ou mobiles (intégrés à des drones par exemple)*
- *La communication de ces données via des réseaux de communication fixes ou mobiles (Wifi, radio-communication 3/4/5 G).*
- *Le traitement et l'analyse des données (big data, IA)*
- *La protection de ces données, via la sécurisation à la fois des communications et des serveurs (cyber-sécurité)*
- *La biométrie, permettant soit d'identifier une personne parmi une foule, soit de confirmer l'identité d'une personne: reconnaissance faciale, de l'iris, des empreintes digitales, de la voix, du comportement... ces technologies reposent à la fois sur des capteurs "hardware" (camera, capteur d'empreintes, micro...) et sur des algorithmes (software).*
- *Les technologies d'identité électronique (eID)*

Pour quelles finalités ? *[Par exemple : détection de situations, analyse prédictive, suivi des personnes.]*

Par exemple:

- *Avec anonymat:*
  - *Mesure et prévisions de l'affluence*
  - *Détection de situations (accidents, aggression, rassemblement...)*
- *Sans anonymat:*
  - *Vérification d'identité en présentiel, ou à distance, permettant l'accés physique (à un lieu, une zone, un stade) ou numérique (connection à un service)*
  - *Certification et vérification de certains critères (par exemple d'âge, de santé....) nécessaires à une authorisation d'accés*
  - *Géolocalisation et suivi des personnes*

Pensez-vous qu'elles permettraient d'anticiper les évolutions des missions de sécurité dans les 10 à 20 ans à venir ? Comment voyez-vous ces évolutions ?

Il me semble que les différents usages de l'identité électronique sont voués à se développer, à la manière de ce qui existe en Suède aujourd'hui. L'utilisation d'une telle identité pour ce qui concerne les accés numériques (connections à distance) est évidente, mais l'identité électronique (couplée ou non à des technologie de biomètrie) peut également être considérée pour des accés physiques à des zones particulières en fonction de certains critères qui lui seront associés (e.g. âge, état de santé,...). L'autorisation d'accés est ainsi rendue plus fiable et plus rapide que celle nécessitant la vérification d'un certificat "matériel" classique (document d'identité, billet d'entrée nominatif, carte d'embarquement...) .

Sur chaque technologie prioritaire évoquée, quel est l'état de développement de l'industrie française ? Que lui manque-t-il pour se perfectionner ?

Concernant les technologies d'identité électronique, l'industrie francaise possède les briques technologiques nécessaires (biométrie, securisation des données etc) via des champions nationaux (e.g. Thales, Idemia...) En revanche, il manque encore une offre finale à l'utilisateur qui soit réellement globale et utlisable pour une multitude de services d'identifications (telle que proposée par le conglomérat BankID ou la sociéte FrejaeID en Suède par exemple). L'utilisation de "France connect" qui pourrait se rapprocher d'une telle offre, reste encore assez marginale.

Comment les configurations techniques peuvent-elles concilier une utilisation de ces technologies et des garanties pour les libertés (protection des données, contrôles automatisés, etc.) ?

Il me semble important d'insister sur les aspects ci-dessous:

- *Information et consentement éclairé des utilisateurs sur l'utilisation de leurs données personnelles*
- *Possibilité d'effacement de ces données*
- *Sécurisation de ces données lorsqu'elles sont collectées, transmises, stockées, puis enfin traitées. C'est le rôle de la cyber-sécurité, généralement parlant*

Par ailleurs, l'aspect "inclusif" n'est pas à négliger, au-delà des problématiques de sécurité. Un accés plus facile, plus rapide et plus sûr (à un service ou à une zone géographique) a une valeur pour l'utilisateur.

Les cadres d'expérimentation sont souvent mis en avant pour le perfectionnement de ces technologies. Quelles sont selon vous les priorités ? Quels seraient les contours de ces cadres ? A quelles fins ?

*

QUESTIONNAIRE REMPLI PAR XAVIER DUPONT, CCE COMITE HONG KONG

Questions

La notion de « technologies de sécurité » est large. Quelles sont les principales selon vous ? *[Par exemple : traitement des données (textuelles, images, sonores), biométrie, mobilité.]*

Xavier DUPONT. Les technologies liées à la sécurité les plus mentionnées sont l'intelligence artificielle, la blockchain, la réalité virtuelle etc…. Mais rarement les objets connectés. Il est important d'insister sur une collecte de données de qualité et sécurisée grâce aux objets connectés. Ces données labellisées sont nécessaires pour que les modèles prédictifs aient des résultats satisfaisants. La cybersécurité des objets connectés est un autre élément clef pour éviter les cas de plus en plus nombreux de hacking/vulnérabilité ; le dernier en date étant celui du réseau électrique en Inde https://www.businessinsider.in/tech/news/chinese-cybercriminals-are-targeting-the-indian-power-sector-according-to-a-report/articleshow/81274093.cms

Pour quelles finalités ? *[Par exemple : détection de situations, analyse prédictive, suivi des personnes.]*

Xavier DUPONT : Les objets connectés sont utiles dans tous les secteurs d'activité et ont trois objectifs :

- *Réduire les couts de fonctionnement/d'opération,*
- *Améliorer la satisfaction client,*
- *Générer des nouveaux modèles économiques tournés autour des services (SaaS).*

Dans la sécurité nous pouvons mentionner quelques cas d'usage comme :

- *La création de profil de conducteurs de tout type de véhicules lié au domaine de l'assurance (Usage Base Insurance & Pay As You Drive)*
- *L'analyse en temps réel du trafic sur des routes mais aussi dans des lieux fermés tel que des centres commerciaux. Reference de la société espagnole de data mining TC Group https://www.tcgroupsolutions.com/en/ qui fournit des données marketing aux centres commerciaux*
- *La remontée d'alertes permettant de faire de la maintenance préventive.*

Pensez-vous qu'elles permettraient d'anticiper les évolutions des missions de sécurité dans les 10 à 20 ans à venir ? Comment voyez-vous ces évolutions ?

Xavier DUPONT : Les objets connectés sécurisés sont une nécessité pour une collecte de plus de données critiques au déploiement d'autres technologies à venir tel que l'IA. Ils sont rarement sécurisés et aucun standard de cyber sécurité existe couvrant les objets connectés. Les éléments de sécurité (Chip dédié a la sécurité) sont de plus en plus répandus.

Sur chaque technologie prioritaire évoquée, quel est l'état de développement de l'industrie française ? Que lui manque-t-il pour se perfectionner ?

Xavier DUPONT : Certains opérateurs dédiés du type Sigfox ou équipementiers comme Kerlink sont parmi les rares sociétés françaises dans le domaine qui ont une envergure internationale. Orange Business Service joue un rôle d'intégrateur spécialisé et cherche des projets à travers son réseau

international. Il existe aussi de nombreuses petites sociétés « deep tech » sur des applications de niche mais pas de « licornes » françaises.

Comment les configurations techniques peuvent-elles concilier une utilisation de ces technologies et des garanties pour les libertés (protection des données, contrôles automatisés, etc.) ?

Xavier DUPONT : Il est nécessaire de créer un guide des bonnes pratiques dans le domaine de la cybersécurité adapté aux objets connectés comme il a été fait aux états unis par la National Institute of Standards and Technology (NIST) et la publication du NISTIR 8259 « Foundational Activities and Core Device Cybersecurity Capability Baseline »

Les cadres d'expérimentation sont souvent mis en avant pour le perfectionnement de ces technologies. Quelles sont selon vous les priorités ? Quels seraient les contours de ces cadres ? A quelles fins ?

Xavier DUPONT : Les priorités dans le cadre d'expérimentations lié aux objets connectés serait la définition de guides d'implémentation qui couvrirait :

- *Protocoles de communication standardisés par applications*
- *Guide de bonne pratique dans le domaine de la cybersécurité*

*

QUESTIONNAIRE REMPLI PAR MORANE REY-HUET, CCE COMITE AUVERGNE RHONES-ALPES

La notion de « technologies de sécurité » est large. Quelles sont les principales selon vous ? *[Par exemple : traitement des données (textuelles, images, sonores), biométrie, mobilité.]*

Morane REY-HUET @Meersens : Il faut bien différencier accès sécurisé vs donnée sécurisée vs anonymisation ou pseudo anonymisation des données. Il faut sécuriser de bout en bout. Dans la santé les données et les systèmes de sécurité sont toujours liés à des protocoles qui définissent clairement les niveaux de sécurité et surtout le permettre d'utilisation de ces données. De ce fait pour assurer que la data est traité dans des bac à sable sécurisé on utilise des serveur HDS ou HIPAA avec des clefs encryptées et un traitement de la donnée du type boite noir. La biométrie devient de plus en plus courante, beaucoup via https, mais le problème est de bien comprendre le flux de la data et les hébergements associés qui vont devoir se plier aux règlementations des pays. C'est enjeux de sécurité vont être par ailleurs des barrières pour l'internationalisation de nos entreprises et services.

Pour quelles finalités ? *[Par exemple : détection de situations, analyse prédictive, suivi des personnes.]*

Morane REY-HUET @Meersens : Aujourd'hui on est encore beaucoup dans une approche de monitoring mais plus on avance, plus les vitesses de calcule et les réseaux de communication grandissent, plus l'IA, le machine learning vont faire de l'aide à la décision, voir agir directement sur une machine, une recommandation, un changement de comportement et de plus en plus pour faire du prédictif, de l'optimisation/efficience de process, apporter de nouvelles valeurs ajoutées, limiter des risques…

Pensez-vous qu'elles permettraient d'anticiper les évolutions des missions de sécurité dans les 10 à 20 ans à venir ? Comment voyez-vous ces évolutions ?

Morane REY-HUET @Meersens : la question de s'assurer que la data n'a pas été altéré de son point de collecte à son utilisation est critique. Le déploiement de solution pour assurer la sécurité des données va être exponentielle, mais il reste l'enjeux des croisements des données comme Google qui ont la capacité de reconsolider un ensemble de sources de données à priori éparses et de congruences variées pour des fins différentes et parfois non souhaitées. A mon avis, c'est les problèmes que nous rencontrerons qui définiront les politiques et les solutions à mettre en place. Les assurances vont jouer un rôle important pour couvrir une partie de ces risques.

Sur chaque technologie prioritaire évoquée, quel est l'état de développement de l'industrie française ? Que lui manque-t-il pour se perfectionner ?

Morane REY-HUET @Meersens : Regarder ce problème au niveau de la France et pas à minimum au niveau Européen me semble peu pertinent. Il nous manque des leaders en cloud (OVH n'est pas à la hauteur), en IoT (essentiellement Chine), en IA. Le programme DeepTech de BPI est excellent mais doit être boosté.

Comment les configurations techniques peuvent-elles concilier une utilisation de ces technologies et des garanties pour les libertés (protection des données, contrôles automatisés, etc.) ?

Morane REY-HUET @Meersens : une CNIL plus facile d'accès, des cas d'usages d'application de la GDPR car il y a trop de zones d'interprétations. Même si on veut bien faire et on est toujours dans l'inquiétude de se faire « retocker » par l'état sur ces sujets de data. Il faut peut-être renforcer l'ISO 27001 / HDS.

Les cadres d'expérimentation sont souvent mis en avant pour le perfectionnement de ces technologies. Quelles sont selon vous les priorités ? Quels seraient les contours de ces cadres ? A quelles fins ?

Morane REY-HUET @Meersens : Nous travaillons avec le Health Data Hub et le Green Data Hub pour amener des liens de causalités entre environnement et santé en lien avec le PNSE4, mais cela est d'une complexité et d'un coût sans commune mesure alors que l'objectif est urgent et nécessaire. Il faut fluidifier le crunching de data sur l'open data pour apporter de nouveaux servies et devenir leader. Sans apprentissage avec des jeux de data pertinent nous allons prendre un retard considérable face aux USA et Chine qui n'ont pas les contraintes que nous avons.

*

QUESTIONNAIRE REMPLI PAR VERONIQUE DENIS-PELLIET, CCE COMITE SINGAPOUR

Questions

La notion de « technologies de sécurité » est large. Quelles sont les principales selon vous ? *[Par exemple : traitement des données (textuelles, images, sonores), biométrie, mobilité.]*

Réponse : biométrie, mobilité (incluant IOTs) et Cybersécurité

Pour quelles finalités ? *[Par exemple : détection de situations, analyse prédictive, suivi des personnes.]*

Détection des anomalies et des personnes, suivi des incidents, besoins accrus de protection des données

Pensez-vous qu'elles permettraient d'anticiper les évolutions des missions de sécurité dans les 10 à 20 ans à venir ? Comment voyez-vous ces évolutions ?

Oui, elles vont permettre cette anticipation, il faudra conjuguer avec une grande accélération des développements (applications, usages…) liés en grande partie à la 5G et ensuite à l'arrivée de la 6G et le nombre d'acteurs qui se multiplient dans cet écosystème.

Sur chaque technologie prioritaire évoquée, quel est l'état de développement de l'industrie française ? Que lui manque-t-il pour se perfectionner ? I

l y a énormément d'acteurs français mais très souvent de petite taille ou assez moyennes sur chacune de ces technologies, la France n'est plus vraiment représentée au niveau des grands acteurs (les Américains et les Asiatiques sont beaucoup plus agressifs).

Comment les configurations techniques peuvent-elles concilier une utilisation de ces technologies et des garanties pour les libertés (protection des données, contrôles automatisés, etc.) ?

C'est aux Etats et institutions (ou instances européennes) de fixer les limites et les contours de ces utilisations.

Les cadres d'expérimentation sont souvent mis en avant pour le perfectionnement de ces technologies. Quelles sont selon vous les priorités ? Quels seraient les contours de ces cadres ? A quelles fins ?

La Cybersécurité est une priorité ainsi que tout ce qui touche aux services 'à distance' tout particulièrement dans le contexte actuel. Là encore, les gouvernements ont un rôle à jouer en instaurant un suivi par exemple des personnes mais sans exploitation ultérieure des données. Tout est dans la définition du 'Data Management' (avec un usage des données exclusivement et idéalement cantonné à l'application ou l'usage en question).

*

QUESTIONNAIRE REMPLI PAR LAURENT DELON, CCE COMITE USA

Questions

La notion de « technologies de sécurité » est large. Quelles sont les principales selon vous ? *[Par exemple : traitement des données (textuelles, images, sonores), biométrie, mobilité.]*

Laurent Delon : Aux Etats Unis, les bases de données des réseaux sociaux et enregistrements permettent de faire du « tracking » de personnes. La reconnaissance d'images avec algorithmes très puissants fait peur. En même temps, les progrès dans les véhicules autonomes permet du tracking très précis. Beaucoup de puces semiconducteur IA sont développées pour faire du « Computing at the Edge » Les US sont en avance dans ce domaine. Les réseaux 5G sont importants et en particulier les « 5G Private Networks » qui permettent a une entreprise de gérer et sécuriser son propre réseau (sans un operateur Telecom / Mobile). D'autres parts, des technologies de virtualisation de la « stack 5G » nécessite d'autres technologies en sécurité. A Hong Kong, les étudiants qui ont manifestes en 2019 et 2020 ont été suivit par les cameras qui ont permis les reconnaissances de visages.

Pour quelles finalités ? *[Par exemple : détection de situations, analyse prédictive, suivi des personnes.]*

Laurent Delon : Le suivi des personnes est bien entendu une des finalités. Chaque Smartphone remonte environ 10 MB de données par jour – a but purement mercantile pour Facebook, Google etc…. Au moment de l'insurrection du 6 Janvier à Washington DC, ces débordements auraient pu être anticipe grâce aux analyses prédictives

Pensez-vous qu'elles permettraient d'anticiper les évolutions des missions de sécurité dans les 10 à 20 ans à venir ? Comment voyez-vous ces évolutions ?

Laurent Delon : Absolument, tout est enregistré et les Etats Unis ont des polices « Opt Out » donc chacun est suivi de façon digitale. Avec le Quantum Computing (capacité de puissance de calcules), les déploiements de réseaux 5G (qui permettent haut-débit d'info mais aussi latence très faible – voir véhicules autonomes par exemple) et la croissance exponentielle des données, ces missions de sécurité en temps réels seront possibles.

Sur chaque technologie prioritaire évoquée, quel est l'état de développement de l'industrie française ? Que lui manque-t-il pour se perfectionner ?

Laurent Delon : Je peux donner mon avis sur le Semiconducteur qui devient une technologie critique dans la 5G (qui permet d'échanger beaucoup d'info et en temps réel), l'administration Biden a annoncé une aide de 50 Milliard de Dollars pour le développement et fabrication aux US de ces puces. La France doit donc s'allier avec les pays Européens étant donnes la somme d'argent nécessaire. Le partage des données entre pays sera importante.

Comment les configurations techniques peuvent-elles concilier une utilisation de ces technologies et des garanties pour les libertés (protection des données, contrôles automatisés, etc.) ?

Laurent Delon : Je pense que l'utilisation de « tokens » et des méthodes de « provisioning » par zone / lieu ou temps ou personnel versus professionnel avec le control de l'individu sur (la vente ou accès de tiers a) ses données.

Les cadres d'expérimentation sont souvent mis en avant pour le perfectionnement de ces technologies. Quelles sont selon vous les priorités ? Quels seraient les contours de ces cadres ? A quelles fins ?

Laurent Delon : Je pense qu'en faisant intervenir les Ecoles et Universités - étudiants et jeunes (plus aptes a comprendre les nouvelles technologies) ces technologies pourront être mieux compris. Il est important aussi que ces cadres d'expérimentation se fassent au-delà d'un contexte franco-français.

Ce questionnaire est indicatif et ne prétend pas de couvrir l'intégralité des enjeux posés par les technologies de sécurité. La mission recueillera tout élément qui lui sera apporté afin de l'intégrer au mieux dans sa réflexion.

Mission du député Jean-Michel Mis

« Pour un usage responsable et acceptable par la société des technologies de sécurité »

*

1/ Objectifs de la mission

La mission souhaite explorer, lors des auditions et via les contributions écrites, les axes suivants :

- Les **opportunités offertes par les nouvelles technologies au service d'une meilleure offre de sécurité** en analysant les besoins des forces de sécurité, entre autres dans la perspective des grands événements sportifs de 2023 et 2024.

- Les principes nécessaires à **la préservation des libertés** en définissant un cadre d'emploi global et cohérent des technologies de sécurité et en associant la société civile à cette définition pour renforcer la compréhension et l'acceptabilité des nouvelles technologies dans la société.

2/ Questions

La notion de « technologies de sécurité » est large. Quelles sont les principales selon vous ? *[Par exemple : traitement des données (textuelles, images, sonores), biométrie, mobilité.]*

*Les technologies de sécurité servent à concevoir, identifier, capter, diffuser, traiter, interpréter, stocker, partager et désactiver l'usage des données sensibles qui requiert un étalonnage de criticité et de confidentialité jusqu'au statu de **secret d'état** qui impose un embargo publique supposé durer de longues années en étanchéité totale : que ce soit des données humaines individuelles et/ou collectives, environnementales (naturelles ou de synthèses numériques) et/ou des données machines via des smart sensors (capteurs intelligents) ou encore des standards (ISO ou autres organismes domestiques et/ou internationales.*

Les usages de ces données passent par des technologies de sécurité « hardware » et/ou « software » et/ou de normalisation via des standards style (ISO inexistant vs BSN celui de la Blockchain Security Network en Chine largement en avance de phase et de généralisation en Chine diffusé auprès de tous les fournisseurs ou clients sur ce marché gigantesque de plus d'1 milliard d'utilisateurs digitaux quotidien par smartphone… cf https://medium.com/@vipinsun/bsn-the-internet-of-blockchains-aa4360b8f7c9) ou encore des architectures comme les systèmes d'information style « plateforme de marché » centralisées ou décentralisées donc données et processus transactionnels avec des moyens de paiement physiques ou dématérialisés (monnaies électroniques, crypto-actifs etc.) et un mix des deux (unités de comptes de programmes de fidélité et/ou jeton-token).

La massification de certaines typologies des usages numériques de données sur un territoire facilite les rapports de force dans l'adoption des standards reconnus par des tiers de confiance et/ou régulateurs institutionnalisés… cf les standards 5G et maintenant 6G via la Chine alors que les débats « philosophiques » en France retardent pour le moins son adoption et son déploiement et conséquemment la formation et l'expertise des RH associés selon un état de l'art à rayon variable (local, régional, national, international et/ou global)…

Un autre bel exemple des décalages et prismes culturels repose sur la réalité du périmètre mal connu de la finance internationale avec pourtant les normes, codes financiers & bancaires et réglementations dont de KYC (Know You Customer), AML (Anti-Monetary Loundering) ou Ratios prudentiels avec une amplitude opérationnelle globale de plus de 10 fois le PNB mondial annuel (90 Trn$/an) qui est transigé PAR JOUR en dehors de places financières régulées (OTC vs bourses etc.) donc en opacité totale voire relative par rapport à la transparence que pourrait apporter la blockchain via ses unités de comptes sur ses réseaux numériques (crypto-actifs avec une classe d'actifs agrégés valorisée au total à un peu moins de 2Trn$).

Les lobbyistes institutionnels savent aussi faire pression sur les influenceurs, les politiques et les décideurs régulateurs contre certaines technologies comme la Blockchain et les crypto-actifs pour éviter trop de transparence trop vite sous les excuses d'exposition du darkweb et deep weeb où tout se trouve et tout se vend

… dont les données de sécurité de centrales nucléaires avec les plans de caméra et les procédures manuelles de badges de sécurité comme j'ai pu le démontrer au patron de l'unité de cybersécurité du FBI en temps réel à l'Ambassade de France de Washington, DC USA.

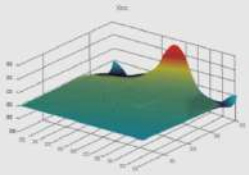
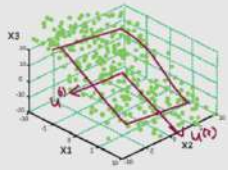
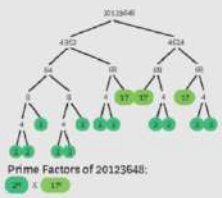
La compromission de ces données (vs data integrity) ont pu se révéler à tous les niveaux de la chaine de valeurs :

- Hardware cf menace SPECTRE (2019) ou encore Neo SPECTRE vs les backdoors de la NSA grâce aux puces INTEL dans des milliards d'ordinateurs…
- Software cf les ransomwares qui se démultiplient chaque année à une vitesse exponentielle, illustrant que la course n'est pas que sur la nature de la donnée mais aussi sur la vitesse à laquelle on y a accès sur toute la chaine de valeurs identifiée au début de ce témoignage.

De nouvelles ouvertures de brèches et de couvertures se sont donc imposées avec l'avènement du Quantum Computing, certes non universel pour l'instant mais déjà suffisamment avancé sur certains périmètres très précis d'optimisation de performances d'exécution de programme en quelques millisecondes (cf les enjeux de la suprématie quantique annoncée et revisitée ou pas par les ténors des GAFAMI : faire en quelques minutes ce qui ne peut être calculé qu'en plusieurs dizaines ou centaines voire milliers d'années avec un super calculateur sur la vectorisation et/ou la factorisation des données etc. cf graphiques ci-dessous).

Attention en plus de ces GAFAMI il y a les BATHX (Google, Amazon, Facebook, Apple, Microsoft, IBM vs Baidu Alibaba Tencent Huawei, Xiaomi) pour ne citer qu'eux… mais plusieurs s'éxécutent dans le cloud avec une offre commercialisée de QC, de blockchain et même pour certain d'une combinaison des deux (minages de crypto-actifs via le Quantum Computing) comme le font déjà depuis des années plus de 2000 développeurs japonais et tout autant de russes…

EXHIBIT 1 | Quantum-Advantaged Computational Problems

Type of problem	Useful for…	Industry applications include…
 Combinatorial optimization	Minimizing or maximizing an objective function, such as finding the most efficient allocation of resources or the shortest total distance among a set of points (e.g., the traveling salesman problem)	• Network optimization (e.g., for airlines, taxis) • Supply chain and logistics optimization • Portfolio optimization in financial services
 Differential equations	Modeling the behavior of complex systems involving fundamental laws of physics (e.g., Navier Stokes for fluid dynamics and chemistry)	• Fluid dynamics simulations for automotive and aeronautical design and medical devices (e.g., blood flow analysis) • Molecular simulation for specialty materials design and drug discovery
 Linear algebra	Machine learning tasks involving matrix diagonalization, such as clustering, pattern matching, and principal components analysis, as well as support vector machines, which are ubiquitous in applications across industries	• Risk management in quantitative finance • DNA sequence classification • Marketing and customer segmentation
 Factorization	Cryptography and computer security, where the most common protocols today (e.g., RSA) rely on the infeasibility (for classical computers) of factoring the product of two large prime numbers	• Decryption and code breaking (e.g., for governments)

Source: BCG analysis.

Ce qui se passe dans le monde occidental n'est pas directement comparable avec les pratiques culturelles significativement différentes en Asie ou USA

- En Asie car de portées plus collectivistes (comme la Chine où la priorité est dans le paradigme du contrôle absolu par l'état des données numériques pour la protection de la communauté dans son ensemble - d'où les scores de risque sociaux - vs à l'opposé du paradigme historique et culturel de la protection tabou des données personnelles en France) et/ou de pirateries institutionnelles dans des pays comme la Chine (cf le cas de l'Acier et le jugement de l'état de Pennsylvanie sur des généraux de l'armée chinoise qui ont pillé pendant près de 20 ans les brevets américains sur l'acier et produits dérivés) ou de la Russie et tant d'autres. Aux USA les vertus de la donnée n'ont de raison d'être que la monétarisation de ces données ; et l'ambition politique est de protéger l'entreprise et le capital qui sont 2 variables d'ajustements pour la création d'emplois alignant des valeurs de capitalisme à des programmes politiques bien compris. L'Europe se positionnerait au milieu des 2 opposés USA vs Chine.

Il y a enfin avec le QC l'identification des menaces enfin « avouable » de pouvoir casser les codes RSA (cf expériences de Google) et Diffier-Hellman mais aussi des clés symétriques algorithmiques.

Pour quelles finalités ? *[Par exemple : détection de situations, analyse prédictive, suivi des personnes.]*

- L'enjeu réside pour partie de réduire les délais requis d'identification de ces préemptions déviantes de données par un humain ou un bot… avec des cibles distinguées de manière non aléatoire… que ce soit donc par un individu en isolation, une organisation structurelle étatique qui commandite des attaques sur d'autres états ou des cibles d'entreprises pour espionnage ou ruptures de charges opérationnelles et/ou fonctionnelles ; ou encore commandites par des états qui proposent jusqu'à un « safe harbor » à ces mêmes hackers, ou pour des visées plus mercantanlistes comme le «hacking as a service » dans le darkweeb permettant d'acheter une prestation de services de hacking sur des cibles à préciser… et enfin il existe le cas des mercenaires hors la loi par idéologies de natures diverses et variées utilisant là aussi des humains ou des BOTS.

- D'après des études comme celles de Vérizon ; les cadrages politico-juridiques et médiatiques des pays occidentaux amènent des différences nationales très significatives allant d'une moyenne autour des 210 jours en Europe et 140 jours aux USA. Bien que ces données géopolitiques sont de moins en moins accessibles aux individus à cause des lobbyistes institutionnels à l'œuvre… les USA ont significativement réduit le nombre de jours requis pour l'identification de captation de données stratégiques et la reconnaissance de ces attaques en édifiant des dispositifs très contraignants et alliant des sanctions juridiques dont des actions au pénal pour la direction générale.

- La réglementation a aussi un role à jouer dans la propagation d'opportunité et de menaces de sécurisation des données, notamment les données personnelles dans le cas de la RGPD où de nouvelles catégories et de pratiques d'attaques (cyberattacks) ont émergé grâce à la centralisation et la portabilité des données… là encore une certaine « omerta » politico-médiatiques culturelles n'a pas permis la diffusion de ces états de faits mais la RGPD bien que culturellement influencée par la CNIL a permis l'émergence de nouvelles attaques dont on n'a pas encore mesuré toute l'amplitude… notamment en France alors qu'il suffit de sortir de nos frontières pour que l'information de cette nature circule.

Pensez-vous qu'elles permettraient d'anticiper les évolutions des missions de sécurité dans les 10 à 20 ans à venir ? Comment voyez-vous ces évolutions ?

L'agence américaine NIST travaille depuis son d'appel d'offre international de 2016 sur les standards des algorithmes cryptographiques post-quantique ; la liste finale issus des 7 semi-finalistes (dont quelques équipes de chercheurs français) ne sera connue que fin 2021 pour un usage généralisé en 2024…

La Suisse se caractérise par l'hébergement de la société ID-Q qui génère des clés quantiques de sécurisation QKD depuis de nombreuses années, largement financée et notamment d'investisseurs étrangers…

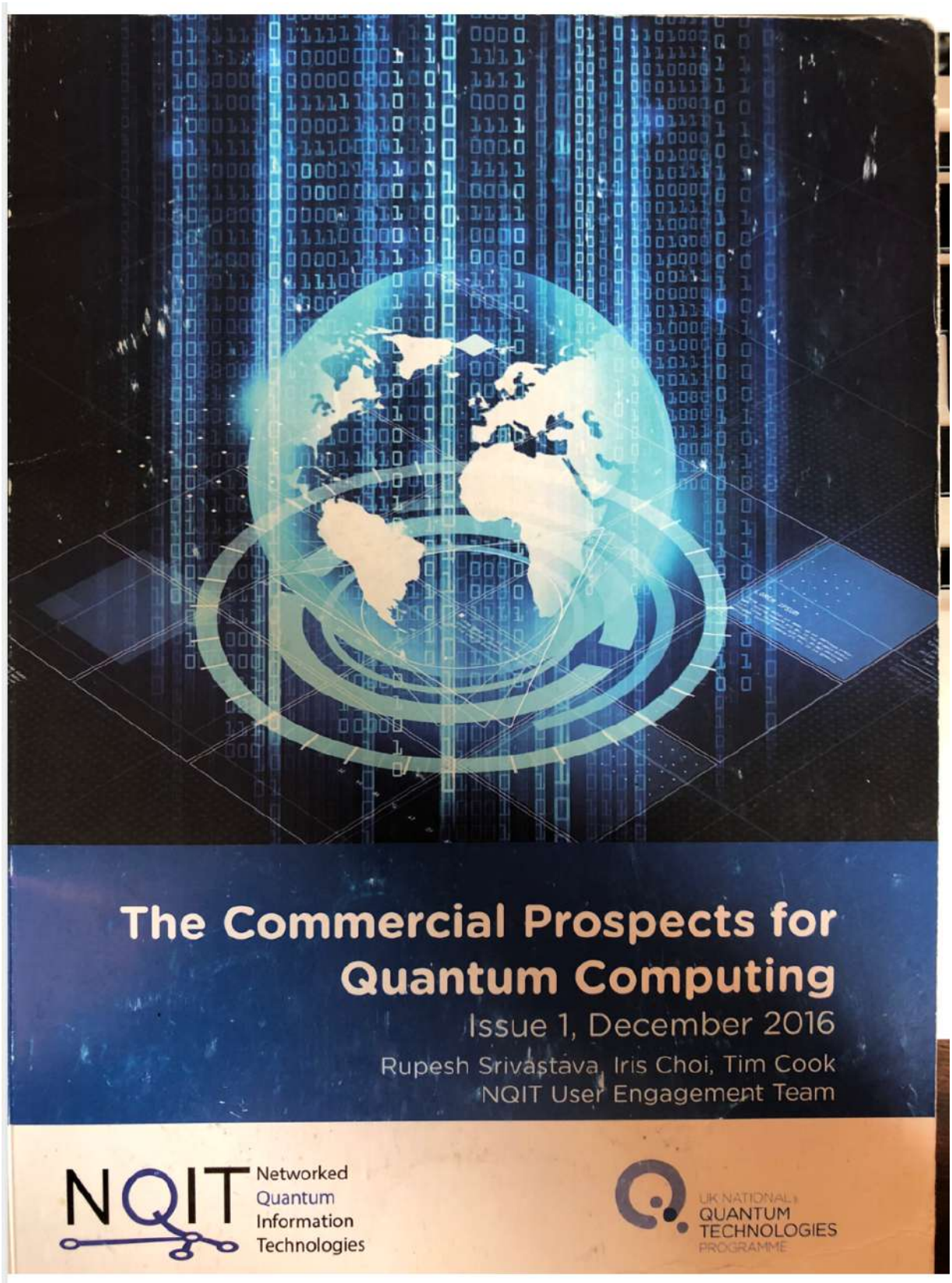
Le Canada et le UK se caractérisent par des niveaux d'investissements singulièrement plus conséquents qu'en France dans des écosystèmes de startups dans le QC et ses 4 grands partis pris scientifiques qui convergent tous vers l'avènement très concurrentiel d'un ordinateur quantique universel, avec en prime au UK une approche commerciale des solutions quantiques depuis 2016… là encore caché en France jusqu'à encore 2021 alors les risques que cela fait courir de retard au niveau des organisations telles que les entreprises et la formation des ressources expertes locales… notamment de part le croisement de l'IA avec le QC et la BC… des verticales scientifiques et professionnelles qui sont aussi en fertilisations croisées… expériences que ne s'interdisent absolument pas les chercheurs chinois, russes et américains. Les prismes et tabous culturels sont très efficaces (protection des données personnelles vs les données de la collectivité vs les données de l'entreprise capitalistique).

Les Pays-Bas ne sont pas en reste non plus avec un écosystème de startups en QC beaucoup plus avancé qu'en France (financement et débouché commerciaux déjà engagés là aussi alors qu'en France une certaine omerta scientifique et bienséance politico-médiatique on veut nous faire croire qu'il n'y a aucune déclinaison exploitable d'ici 2025 voire 2035 avec le CEA Leti …

Les grands acteurs français du QC ont pu ainsi profiter à leur tour de leur « safe harbor » pour prendre le temps de monter en puissance et en gamme dans les parties pris scientifiques et notamment l'alternative presque « cache misère » de simulation quantique… au péril des entreprises, entrepreneurs et écosystèmes français mal préparés face à ces enjeux d'intégration de gains de performance sensiblement améliorée, de périmètres couverts et cette inertie a certainement été très utile pour améliorer leurs postures concurrentielles, voire de protectionnisme contre les prédateurs étrangers… il faudrait peut-être déjà avoir à l'esprit l'importance qu'a pu joué la licence d'exploitation de Westinghouse dans la création de la filière complémentaire de l'énergie atomique française au sein du CEA dès les années : un transfert de technologie à faire au plus vite en parallèle des « petits » efforts actuels de création d'une hypothétique autonomie de souveraineté numérique à l'horizon 2035 en QC (avec 1,5Bn€ sur la filière la France n'y est certainement pas dans la 1ère league)…

Le Japon également n'est pas en reste dans le développement commercial du QC certes là encore non universel mais ultra efficace d'un acteur canadien comme DWAVE avec plus de 500 études de cas clairement identifiées comme valorisation le QC adiabatique… affichant des gains de performances jusqu'à des millions de fois supérieurs aux ordinateurs classiques.

Quant à la Chine elle est en avance de phase depuis les démonstrations MICIUS de 2018 de communication quantique satellitaire… qui depuis trouvent des couches intermédiaires de relais via les drones militaires.



Sur chaque technologie prioritaire évoquée, quel est l'état de développement de l'industrie française ? Que lui manque-t-il pour se perfectionner ?

On le voit bien il y a des enjeux de gouvernance de la sécurité avec des partis pris de nature diverse et variée pour trouver un équilibre en fonction d'objet plus complexes qu'il n'y parait dans ce simple

« position paper »… et ce n'est plus un secret les lobbyistes français sont très largement sous représentés à la commission européenne …

Comment les configurations techniques peuvent-elles concilier une utilisation de ces technologies et des garanties pour les libertés (protection des données, contrôles automatisés, etc.) ?

Les paradigmes culturels facilitent ou inhibent consciemment et inconsciemment les influenceurs et les décideurs… les partis pris politiques sont les résultantes de cycles longs dans nos régimes républicains à l'inverse de ce qui a pu se passer aux USA avec les déséquilibres géopolitiques impulsés par l'administration américaine sous la Présidence de Mr TRUMP, notamment dans le découplage Chine-USA sur les semi-conducteurs et autres secteurs industrielles…

Un seul acteur technologique européen vient perturber cet échiquier bi-polaires USA-Chine avec l'émergence de la société privée hollandaise ASML valorisé 2 fois la valorisation boursière de Total et 3 fois Airbus…

ASML construit des machines à semi-conducteurs à plus de 200 millions de dollars l'unité, permettant de mettre en production des micro-processeurs de moins de 7 nanos (technologie EUV allant jusqu'à 2 nano comme communiqué par IBM la semaine dernière… et composants technologiques de 7 nano est moins interdits d'export en Chine par le biais renouvelé de l'application sanctionnée de l'extraterritorialité américaine). C'est une technologie sous-jacente à pratiquement tous les écosystèmes numériques car les serveurs et les ordinateurs (dont quantique) utilisent ces micro-processeurs dont une « unité cellulaire numérique de base » et pour lesquelles (de 5 nano à 300mm) il y a rupture de stocks mondiale sur toute la chaine de valeurs pour les 2 prochaines années impactant aujourd'hui toutes les verticales industrielles (dont automobiles, smartphones etc…).

Ce sont tous les écosystèmes numériques (IC, chips, transistors, capteurs, micro-processeurs) qui dépendent de ces technologies de lithographie… que s'arrachent les grands fondeurs mondiaux Intel, Samsung, PSMC etc… qui ont d'ailleurs financés en fonds propre et pour partie la création de cette nouvelle génération de technologie EUV détenue par ASML… un Partenariat capitalistique intéressant à relever pour la France bien larguée sur plusieurs verticales technologiques à effet de productivité à court terme et pas de promesses scientifiques d'avoir des millions de Qbits en 2035 voire 2050… cette recherche fondamentale à l'horizon 2035 est structurante et indispensable à la France mais en parallèle elle ne doit pas exclure le transfert de technologie comme ce fut le cas pour l'énergie atomique avec la licence d'exploitation Westinghouse…

Une licence d'exploitation avec le Canadien DWAVE devient plus qu'urgent sur le QC même si cela ne fait pas les affaires d'ATOS, le CEA et autres consorts scientifiques… l'Allemagne a su prendre l'avantage sur la France en investissant les 12 millions d'euro d'une machine DWave qui permet de mesurer concrètement les effets de l'intrication et de superposition sur plus de 500 études de cas mondiaux… la méthode des études de cas comme le fait l'université d'Harvard est reconnue de valeurs scientifiques comme toute autre méthode de recherche scientifique…

Les cadres d'expérimentation sont souvent mis en avant pour le perfectionnement de ces technologies. Quelles sont selon vous les priorités ? Quels seraient les contours de ces cadres ? A quelles fins ?

La priorité réside dans une approche à mener en parallèle et non pas en substitution l'une de l'autre… l'erreur et les fantasmes de l'un comme de l'autre des détenteurs d'enjeux résident bien dans l'éventualité d'une substitution… alors qu'il s'agit d'un effort supplémentaire d'intégrer les 2 niveaux

de complexité à faire les 2 approches en même temps, qui permettent d'ailleurs les mécanismes de fertilisations croisées et de décloisonnement avec les meilleures synergies à impacts mesurables…

Donc comme l'illustre les nombreuses études de cas menées par le réseau mondial des CCE que je préside sur les TIC et les Économies Numériques il faut mener en parallèle tant la recherche fondamentale que la recherche appliquée (innovation à moins de 2 ans) et réussir à sortir des cloisonnements plus moins stériles à long terme :

- Blockchain et leurs unités de compte que sont les crypto-actifs dans leur réseau respectifs (BTC, ETH etc…)
- Intelligence Artificielle dont Machine Learning, approches neuronales
- Quantum computing sur ces 4 partis pris scientifiques avec un contrat de licence pour utiliser le leader mondial qu'est la machine de DWave à 5K Qbits en déplaise à IBM, Atos, le CEA etc
- Microprocesseurs et machines à fonderies style ASML
- Communication quantique satellitaire, internet quantique et de drones relais comme cela est déjà fait en Chine
- Décloisonnement des « data lakes » avec ZERO KNOWLEDGE utilisé en reconnaissance faciale à Hong Kong ce qui induirait une modification constitutionnelle en France pour l'usage de ces outils à forte valeur ajoutée (scientifique et technologique) produisant des données structurantes pour les enjeux de sécurisation des organisations structurelles… donc là on est dans les processus et modèles opératifs (« operating systems » et « modèles d'affaires »)
- « Sustainable by design » les puces de 2 nano prototypées par IBM illustre des gains de performances phénomales et la continuité encore possible de la loi de Moore (puisqu'1 semaine seulement après IBM c'est autour du Taiwannais TSMC d'annoncer une nouvelle technologie pour faire moins qu'1 nano) le tout autour de « l'empreinte et la conscience carbone ».

Donc Hardware, Software et processus de responsabilisations sur des indicateurs de performances mesurables et pour lesquels les parties prenantes doivent être auditées et redevables («to be acountable » comme le prédispose la culture anglosaxonne).

Par contre il faut aussi bien comprendre l'importance des processus chinois de prise de part de marché indépendamment des ROI (retour sur investissement) court terme avec les cycles de reporting mensuels et trimestriels des bourses financières comme le NASDAQ et autres… le parti communiste dans son 15^{e} plan quinquennal place ces technologies comme prioritaire mais ne fixe pas d'objectifs de rentabilité financière mais de leadership ET surtout de synergies ouvertes entre le militaire et le civil… la politique de la nouvelle route de la soie sur 130 pays avec le dumping de l'acier sur les infrastructures et les technologies sont éloquantes des ambitions poursuivies et bien sur le point d'orgues du RMB digital (5 ans avant les américains et le dollar digital et 7 ans avant l'euro numérique de la BCE)… là encore les obstacles culturels expliquent les besoins et enjeux de traçabilité et de contrôle sur le plus grand périmètre possible des données dont les « data lakes » d'une envergure

*

Ce questionnaire est indicatif et ne prétend pas de couvrir l'intégralité des enjeux posés par les technologies de sécurité. La mission recueillera tout élément qui lui sera apporté afin de l'intégrer au mieux dans sa réflexion.

Mission du député Jean-Michel Mis

« Pour un usage responsable et acceptable par la société des technologies de sécurité »

*

1/ Objectifs de la mission

La mission souhaite explorer, lors des auditions et via les contributions écrites, les axes suivants :

- Les **opportunités offertes par les nouvelles technologies au service d'une meilleure offre de sécurité** en analysant les besoins des forces de sécurité, entre autres dans la perspective des grands événements sportifs de 2023 et 2024.

- Les principes nécessaires à **la préservation des libertés** en définissant un cadre d'emploi global et cohérent des technologies de sécurité et en associant la société civile à cette définition pour renforcer la compréhension et l'acceptabilité des nouvelles technologies dans la société.

2/ Questions

Quelles sont les principales nouvelles technologies de sécurité selon vous ? *[Par exemple : applications d'IA et d'automatisation, traitement des données (textuelles, images, sonores), biométrie, équipements de l'agent en mobilité]*

Comme quasiment tous les cas d'usage aujourd'hui, les technologies de sécurité sont impactées par l'introduction du numérique à des fins de commande et de contrôle. Les objets de sécurité incluent donc des capteurs de plus en plus diversifiés, collectant un ensemble de données acheminées vers des plates-formes d'analyse et de prise de décision, décisions qui sont ensuite renvoyées vers des mécanismes de contrôle (gestion de la circulation, des systèmes de santé, …). Cela ouvre donc de nombreuses applications reposant sur la captation et l'analyse de données (sujet bien compris à ce stade), mais aussi la capacité à poser un diagnostic et à dérouler des actions suite à celui-ci.

Les principales nouvelles technologies sont donc :

- Toutes sortes de nouveaux capteurs, avec les risques afférant à des déploiements non ou peu maitrisés, notamment en raison du nombre et de la diversité technologique des capteurs. Nous pourrions par exemple imaginer des déploiements de capteurs à grande échelle pour mieux détecter (plus tôt) les feux de forêt, les montées des eaux, les glissements de terrain (événements physiques), mais aussi les déplacements de personne. Sont inclus dans ces nouveaux capteurs la surveillance des infrastructures critiques (santé, eau, énergie, mobilité, etc.), qui sont déjà instrumentées mais dont les données ne sont pas disponibles à l'extérieur.
- Des capacités de communication standardisées et disponibles pour tous, permettant d'améliorer en continu la communication entre les primo-intervenants de toute nature et les centres de contrôle auxquels ils sont liés. Dans ce contexte, ces technologies doivent également significativement améliorer l'interaction entre les différents services, fournissant des capacités de communication à tous. Ces capacités de communication pourront également être plus adaptatives au contexte, permettant de dédier des ressources en cas de besoin.
- De nouveaux mécanismes et outils (principalement logiciels) pour le traitement de ces données massives, permettant d'améliorer des services existants aujourd'hui (services d'urgence – médicaux, pompiers, services de protection de bâtiments sensibles, investigation criminelle, etc.), ou de concevoir de nouveaux services, comme une détection plus rapide des

incidents et une meilleure information mise à disposition des intervenants, permettant de mieux focaliser leur action et de limiter les risques qu'ils prennent.

- Des plates-formes d'acquisition, d'agrégation et de fusion de données issues de sources très hétérogènes (capteurs physiques, événements informatiques, logs de contrôle d'accès, réseaux sociaux, téléphonie, …), augmentant sensiblement la couverture de la surveillance par rapport à ce qui est possible aujourd'hui.
- La généralisation du contrôle à distance de nombreux équipements (carrefours, voies de circulation, portes, cameras, …), permettant à des centres distants de soutenir l'action des intervenants sur le terrain (dégagement de voies d'accès, blocage de flux de personnes pour éviter les perturbations, …).
- L'interaction avec d'autres équipements (par exemple bâtiments) pour lesquels des interfaces et accès spécifiques pourraient être donnés aux services de sécurité, pour faciliter des interventions en cas de besoin (exemple de badge « universel » qui ne serait actif que lorsqu'une situation d'intervention est mise en place).

Ces technologies peuvent trouver de nombreuses applications dans les domaines de la sécurité et de la défense, pour la protection de sites sensibles, pour le soutien et l'appui aux opérations de secours (ambulances, pompiers, hôpitaux, …) pour le soutien et l'appui aux opérations de maintien de l'ordre, pour la prévision d'événements catastrophiques ou non désirés,

Pour quelles finalités ? *[Par exemple : détection de situations, analyse prédictive, suivi des personnes.]*

Les finalités sont également nombreuses, et dépendent pour beaucoup de la capacité à capter une information (donc du développement de capteurs) et à en tirer du sens (donc de l'évolution des algorithmes dit d'intelligence artificielle tout d'abord, mais aussi de nouveaux environnements d'exploitation de ces algorithmes, capables de fournir la puissance de calcul nécessaire et également la capacité à visualiser et à présenter les résultats.

Les finalités pertinentes semblent permises par les évolutions technologiques anticipées :

- Détection et analyse de situations critiques, la partie analyse étant critique pour permettre la réponse nécessaire. Cette partie analyse devra permettre une évaluation de la criticité du problème rencontré, évaluer les moyens nécessaires pour y répondre, et faciliter l'intervention des primo-intervenants de toute nature.
- Analyse post-mortem du déroulement des opérations, à partir des données d'intervention collectées sur les équipements des primo-intervenants et des capteurs d'environnement, pour analyser le bon fonctionnement des opérations de sécurité, faire évoluer les doctrines d'intervention et de sécurité (voir la législation) et servir également à l'entrainement des équipes.
- Détection d'anomalies (fumées suspectes, déplacements de personnes et de véhicules, bruits, …), notamment sur la base de signaux faibles, et de déviations par rapport à une activité « normale » (dont la définition, sur le plan scientifique, est un problème difficile).
- Une interconnexion des systèmes (y compris systèmes d'information), permettant une anticipation de certains risques. Les exemples concernent l'interconnexion encore améliorée des systèmes de prévision météorologiques pour prévenir des catastrophes naturelles (vents, inondations, …).
- Une meilleure gestion du risque sur les infrastructures critiques, notamment une meilleure prévision des incidents possibles et la mise en place de ressources pour les prévenir.
- L'identification et le suivi du déplacement de personnes, que ce soit par de la captation d'images, par de la captation de signaux de déplacement, ou plus généralement par de la

captation d'activité. La transformation de nos objets connectés (téléphones, montres, …) en « mini-ordinateurs constamment connectés » génère un ensemble de traces qui est de nature à accroitre la capacité à suivre les individus, de manière de plus en plus personnalisée d'une part, et également à postériori, suite à la conservation non maitrisée des données informatiques.

Pensez-vous qu'elles permettraient d'anticiper les évolutions des missions de sécurité dans les 10 à 20 ans à venir ? Comment voyez-vous ces évolutions ?

L'évolution repose sur une intégration croissante des technologies numériques dans les missions de sécurité, pour des besoins multiples : captation d'information, gestion des missions, formation et entrainement, anticipation et gestion de la menace.

Quels sont selon vous les principaux enjeux de liberté dont il est question face aux nouvelles technologies de sécurité ?

Le premier enjeu est la sécurité des données collectées, associée à l'assurance que l'usage qui est fait de ces données respecte les principes du Règlement Général sur la Protection des Données (RGPD), notamment le fait que les données collectées soient pour un

Quelles technologies et usages vous inspirent le plus d'interrogations quant au respect de ces libertés ?

La numérisation généralisée du secteur de la sécurité entraine de nouveaux risques, dont certains significatifs et nouveaux, liés aux attaques informatiques, ou plus généralement .

- Risque technologique, lié à la numérisation du secteur. Cela expose naturellement à des risques d'attaques cyber, sur les capteurs, sur les communications et sur les données, qui peut perturber le fonctionnement des systèmes de sécurité. Cette numérisation induit également un risque d'exposition majeur de données personnelles, au travers des vulnérabilités des systèmes d'information et des objets connectés. L'accès à ces données personnelles est naturellement problématique pour le respect des libertés.
    - Un exemple est l'émergence des deepfakes. L'impact de cette manipulation de données devrait être évaluée dans un contexte de sécurité, ou la fiabilité des informations collectées est capitale.
- Risque cognitif, surévaluation de la capacité du système à remplir sa mission par les opérateurs, sur-confiance en la technologie qui ferait négliger d'autres signaux, ou perte de confiance dans la technologie. Cela peut induire des erreurs d'évaluation par
- Risque lié à la mutualisation technologique. L'interconnexion croissante et attendue des ressources peut créer des maillons faibles dans la chaine technologique. On peut par exemple

La génération de données et le possible détournement de ces données est bien évidemment un risque pour les libertés individuelles.

Comment assurer l'équilibre, dans une société toujours plus imprégnée de technologies, entre les impératifs de liberté et de sécurité ?

Il faut être capable d'expliquer ce que fait une technologie, ses avantages pour la société, et d'offrir des garanties que cette technologie fait tout ce qu'elle doit faire, et seulement ce qu'elle doit faire.

Pour atteindre ce résultat, deux conditions semblent nécessaires :

- D’un point de vue technologique, la certification des composants et systèmes utilisés semble indispensable. Elle a l’avantage de fixer des normes de développement et de maintenance des équipements et systèmes.
- D’un point de vue humain, la formation et la certification des professionnels est indispensable pour assurer leur capacité à utiliser au mieux les technologies. Cette formation doit inclure une partie réglementation.

Une mission de régulation et d’analyse des problèmes devrait être confiée à une instance existante.

L’un des moyens de garantir un bon usage de ces technologies et de procéder avant tout à des expérimentations. Quelles seraient selon vous les conditions que ce cadre expérimental devrait réunir ?

Le cadre expérimental doit à la fois permettre une validation des résultats et une acceptabilité de la technologie. Les conditions suivantes semblent nécessaires :

- Des objectifs clairs et limités dans le temps.
- Une publication des résultats.
- Un périmètre (physique et logique).
- Une supervision par une autorité externe et neutre, chargée d’évaluer les résultats.

*

Ce questionnaire est indicatif et ne prétend pas de couvrir l’intégralité des enjeux posés par les technologies de sécurité. La mission recueillera tout élément qui lui sera apporté afin de l’intégrer au mieux dans sa réflexion.

Mission du député Jean-Michel Mis

« Pour un usage responsable et acceptable par la société des technologies de sécurité »

*

1/ Objectifs de la mission

La mission souhaite explorer, lors des auditions et via les contributions écrites, les axes suivants :

- Les **opportunités offertes par les nouvelles technologies au service d'une meilleure offre de sécurité** en analysant les besoins des forces de sécurité, entre autres dans la perspective des grands événements sportifs de 2023 et 2024.

- Les principes nécessaires à **la préservation des libertés** en définissant un cadre d'emploi global et cohérent des technologies de sécurité et en associant la société civile à cette définition pour renforcer la compréhension et l'acceptabilité des nouvelles technologies dans la société.

2/ Questions

Avant de répondre à vos questions, je crois important de rappeler un point essentiel sur les libertés : il existe — et, d'une certaine façon, il a toujours existé — une tension autour de ce terme, tension entre liberté et égalité d'un côté, tension entre liberté et fraternité de l'autre, mais aussi tensions entre liberté et solidarité et entre liberté et sécurité. Nous ne nous appesantirons pas sur sa définition philosophique, qui demanderait pourtant de longs développement. Mais, il est important de rappeler en préalable la définition de l'article 4 de la déclaration des droits de l'homme et du citoyen : *La liberté consiste à pouvoir faire tout* ***ce qui ne nuit pas à autrui*** *: ainsi, l'exercice des droits naturels de chaque homme n'a de bornes que celles qui assurent aux autres Membres de la Société la jouissance de ces mêmes droits. Ces bornes ne peuvent être déterminées que par la Loi.*

« ce qui ne nuit pas à autrui » : ceci signifie que nous nous demanderons comment laisser tout faire tout en évitant de nuire. Ce sont ces limites à l'action qui doivent être discutées. En effet, les technologies de surveillance peuvent être bénéfiques pour les libertés si elles **ne conduisent pas empêcher de faire ce qui ne nuit pas à autrui**. Elles sont donc légitimes à empêcher de faire ce qui nuit à autrui ! C'est ce qu'il convient ici d'évaluer ce que signifie nuire et à distinguer les nuisances effectives, par exemple la contrainte, l'enfermement, l'opprobre, des nuisances potentielles, par exemple de la prédiction de nuisance d'un individu potentiellement délinquant.

La **surveillance n'est pas nécessairement privative de liberté** si elle est bienveillance, autrement dit, si elle ne nuit pas, mais qu'elle vise au bien, par exemple la surveillance sanitaire.

Le **consentement relève-t-il de la liberté** ? C'est une question…

Quelles sont les principales nouvelles technologies de sécurité selon vous ? *[Par exemple : applications d'IA et d'automatisation, traitement des données (textuelles, images, sonores), biométrie, équipements de l'agent en mobilité]*

- Traitement masse de données — sécurité civile, sécurité sanitaire
- Sécurité sanitaire : données de santé, exemple médiator, épidémie, médecine préventive, etc.
- Sécurité civile
    - Déplacements (Syrie)
    - Écoutes téléphoniques (reconnaissance parole, émotions, accents, …)
    - Caméra et enregistrement vidéo

        - Reconnaissance faciale, posturale, etc.
    - Cybersécurité

Pour quelles finalités ? *[Par exemple : détection de situations, analyse prédictive, suivi des personnes.]*

Bien distinguer les finalités, par exemple, pour la reconnaissance faciale et posturale :

- Authentification (sécurité, s'assurer, par exemple, que la personne qui ouvre son compte sur internet est bien celle qui est censée le faire
- Identification : repérer dans la foule, les individus, suivre à la trace de l'activité de chacun, etc.
- Catégorisation :
    - émotion, ethnie, orientation sexuelle… (privatif de liberté !) — utilisation de données « involontaires » (même s'il y a consentement), par exemples l'expression du visage qui trahit éventuellement le malaise, le « mensonge », etc.
    - Prédiction de comportement

Pensez-vous qu'elles permettraient d'anticiper les évolutions des missions de sécurité dans les 10 à 20 ans à venir ? Comment voyez-vous ces évolutions ?

- Cybersécurité — enjeux majeur pour le futur, d'autant plus qu'il fait intervenir des acteurs agissant depuis des territoires étrangers hostiles, comme la Russie
- Censure et surveillance des communications sur les réseaux sociaux
    - Nécessité de surveiller certains échanges (préparation d'attentat, etc.), pour assurer la sécurité
    - Incitation à la haine, diffamation, etc. — ce qui est contraire à la loi dit être empêché. L'État ne doit pas se défausser de ses responsabilités sur les réseaux sociaux ici.
- Imposition de régulation et de normes extrêmement lourdes et pénalisantes, qui s'opposent aux législations nationales, et, par là à la souveraineté populaire dont les parlementaires sont les représentants

Quels sont selon vous les principaux enjeux de liberté dont il est question face aux nouvelles technologies de sécurité ?

- Catégorisation → C'est certainement le plus grand danger pour l'autonomie de sujet, pour le choix individuel et donc pour la liberté
    - Crédit social, scores, etc.
    - Prédiction
    - Orientation sexuelle ou politique, etc.
- Identification → risques de suivi de toutes les activités. Il y a là un enjeux important pour le législateur. Il faut d'un côté utiliser les technologies pour assurer la sécurité (pensons aux parking, pour donner l'alerte en cas d'agression, ou au cyberespace) tout en préservant la liberté d'aller et venir. Ceci signifie, par exemple, que l'on doit autoriser les autorités judiciaires à commander l'utilisation de techniques d'identification des enregistrement des caméras de surveillance de rue, mais ne pas l'autoriser de façon systématique.

Quelles technologies et usages vous inspirent le plus d'interrogations quant au respect de ces libertés ?

Comment assurer l'équilibre, dans une société toujours plus imprégnée de technologies, entre les impératifs de liberté et de sécurité ?

Je crois qu'un enjeu majeur consistera à convaincre la population de la nécessité de technologies de surveillance et, en même temps, à expliquer le besoin de garde-fous contre les usages abusifs, en particulier de sociétés privés.

L'un des moyens de garantir un bon usage de ces technologies et de procéder avant tout à des expérimentations. Quelles seraient selon vous les conditions que ce cadre expérimental devrait réunir ?

Oui, à l'évidence, il faut pouvoir conserver le droit à l'expérimentation, par exemple sur la reconnaissance faciale et comportementale.

Je tiens aussi à ajouter que la régulation et l'imposition de normes a priori m'apparaît extrêmement dommageable. En revanche, il faut éduquer la population et recourir à des organismes de certification extérieur qui garantiront certaines propriétés des dispositifs technologiques, par exemple du fait que les données personnelles sont uniquement traitées localement ou qu'elles sont cryptées et stockées sur des sites protégés, etc.

*

Ce questionnaire est indicatif et ne prétend pas de couvrir l'intégralité des enjeux posés par les technologies de sécurité. La mission recueillera tout élément qui lui sera apporté afin de l'intégrer au mieux dans sa réflexion.

« Pour un usage responsable et acceptable par la société des technologies de sécurité »

*

1/ Objectifs de la mission

La mission souhaite explorer, lors des auditions et via les contributions écrites, les axes suivants :

- Les **opportunités offertes par les nouvelles technologies au service d'une meilleure offre de sécurité** en analysant les besoins des forces de sécurité, entre autres dans la perspective des grands événements sportifs de 2023 et 2024.

- Les principes nécessaires à **la préservation des libertés** en définissant un cadre d'emploi global et cohérent des technologies de sécurité et en associant la société civile à cette définition pour renforcer la compréhension et l'acceptabilité des nouvelles technologies dans la société.

2/ Questions

Quels sont selon vous les principaux enjeux de liberté dont il est question face aux technologies de sécurité ?

S'il y a une liberté qu'il faut absolument sauvegarder parce qu'elle déterminera et conditionnera tout notre environnement numérique sécuritaire : c'est la protection de notre vie privée via la protection de nos données personnelles. La sécurité individuelle et collective ne pourra être assurée qu'à la lumière d'une bonne analyse de la façon dont nous déciderons de légiférer sur la mise à disposition de nos données dans l'espace privé et public. Cela régira tout le reste : la liberté d'expression, la liberté de la presse, la liberté d'opinions qu'elle soit politique ou religieuse.

Quelles technologies et usages vous inspirent le plus de prudence quant au respect de ces libertés ?

Nous sommes de plus en plus exposés dans nos vies en ligne. Jusqu'à aujourd'hui les législations française et européenne se sont plutôt concentrées sur la protection de la confidentialité des données alors qu'on se rend compte de plus en plus qu'il faut surtout s'intéresser à l'utilisation, à la territorialité des données à leur collecte et leur revente. La sécurisation de nos libertés est là.

La santé est un secteur très exposé. L'exploitation des données médicales sensibles sont un grand danger. Il faut que le l'historique des données soit pseudonymisé afin d'éviter à tout prix la rupture du secret médical. Le secteur de l'éducation est également préoccupant car une très grande quantité de données sur la scolarité des élèves (comportement, résultats, notations, situation des familles) circulent et permettent de les suivre toute la durée de leurs études. Il faut intensifier la lutte contre le terrorisme et les propos infamants, ll' homophobie, le raciste, le complotisme etc..qui passe par un usage des réseaux sociaux qu'il faut règlementer . L'économie est aussi un secteur où la sécurité a un rôle à jouer, car la confidentialité des données des entreprises, la vulnérabilité des chaînes d'approvisionnement dans certains domaines sont aussi une menace. Enfin si l'on prend le scandale Cambridge Analytica, il est bien la preuve que sans une bonne gestion des données même les démocraties sont en danger.

Comment assurer l'équilibre, dans une société toujours plus imprégnée de technologies, entre les impératifs de liberté et de sécurité ?

Nos données sont aujourd'hui stockées dans des Etats tiers et entre les mains d'éditeurs de données dont nous ne maîtrisons pas le niveau de protection. Il faut aussi résoudre les questions liées au traçage, à la surveillance de masse, aux fakes news. Il faut exiger plus de transparence sur les transferts de données hors de l'UE, de même que sur les technologies empruntées à des pays tiers par des entreprises européennes et qui peuvent tomber sous des lois de contrôle extra-territoriales. La législation en matière de droit numérique doit s'étoffer. Il faut envisager une charte des droits fondamentaux du numérique de manière à poser des règles précises en matière de responsabilité aux plateformes. Les technologies évoluent très vite mais les grands principes de liberté et de sécurité resteront les mêmes. L'équilibre ne sera trouvé que si nous assurons notre « souveraineté numérique nationale ou européenne » et il est évident que la priorité absolue est de créer « un cloud européen » qui puisse protéger les données personnelles, administratives ou industrielles des européens en conformité avec le RGPD. Il faut se donner pour objectif de stocker l'intégralité de nos données dans des centres de datas situés et contrôlés en Europe.

Quelle perception avec la création d'une association citoyenne à la définition des conditions d'appropriation de ces nouvelles technologies, à des fins de sécurité mais aussi plus généralement ? Quelle forme cette association pourrait-elle prendre ? Quelles technologies particulières devrait-elle nécessairement couvrir ?

Le monde associatif doit pouvoir intervenir dans le débat sur les usages citoyens mais l'enjeu va bien au-delà. Il a un rôle pédagogique très important. Il faut en effet accompagner la création d'associations de terrain dont les personnels proches des citoyens seront à même de former ceux qui sont en difficulté à l'utilisation, à la maîtrise et à la gestion d'internet au quotidien. Un fonds pour le développement du numérique dans la vie associative avait vu le jour en 2014. Il devait donner au monde associatif des éléments de réflexions et mettre à sa disposition une palette d'utilisations du numérique et optimiser leur potentiel de développement. Il faudrait peut-être le relancer. Mais par-dessus tout, le moment est venu d'apprendre à l'école à se méfier du numérique comme on a appris aux enfants de se méfier en traversant la rue. Développer l'attractivité du numérique ne peut aller sans un apprentissage de l'usage.

Quelle forme peut prendre une doctrine d'application du RGPD qui concilie le respect des libertés et l'exploitation des dérogations à des fins de sécurité ?

TRIBUNE DE L'INSTITUT CONCERNANT LE RGPD ET L'EXTRATERRITORIALITE est jointe au questionnaire et répond à cette question.

Les nouvelles technologies de sécurité suscitent d'importants besoins en compétences mixtes, notamment juridiques et techniques. Comment faites-vous face à ces évolutions pour assurer votre mission ?

Dans la mesure où la mission doit privilégier les pistes assurant le renforcement du niveau de sécurité, Il faudrait sans doute envisager la création d'un groupe de travail de haut niveau privé-public réunissant toutes les compétences pour renforcer les moyens financiers et judiciaires de lutte contre les contenus illégaux, illicites et les contrefaçons. Les problèmes de cybersécurité sont primordiaux et il faut œuvrer à contribuer le plus efficacement possible à inverser le rapport de force qui s'installe de plus en plus avec les grandes plateformes qui bénéficient encore d'une absence réelle de responsabilité.

Il faut donc que la France soit leader pour exiger que l'Europe continue à se doter de règlements très contraignants. Le droit européen ne s'est attaqué jusqu'à maintenant essentiellement qu'au droit de la concurrence. Le DSA est donc de ce point de vue une vraie avancée puisqu'il propose un cadre plus contraignant à l'égard des plateformes structurantes. Le virage est important mais insuffisant. Nous espérons que le Parlement européen saura renforcer le cadre de la proposition de la Commission.

Le monde de la donnée suscite un volume d'activité accru pour les régulateurs et les parties prenantes. Comment y faire face pour adapter le cadre protecteur à la société de demain ?

Il faut mener des actions législatives en France et les étendre au niveau européen pour qu'elles aient un sens. Il est donc indispensable de travailler sur la moralisation de la modération des contenus. Tout ce qui est interdit dans la vie réelle, doit l'être à terme dans la vie virtuelle :

- *Remise au cœur du système de l'humain*
- *Transparence et neutralité des procédures aboutissant aux algorithmes*
- *Développer des politiques de communication vers les citoyens sur le partage des données (respect du consentement et encadrement de la circulation des données)*
- *Envisager un tiers de confiance collectif, neutre et éthique*
- *Enfin soutenir tous les projets qui encouragent la souveraineté numérique des données européennes et donc favoriser tous les projets d'entreprises françaises et européennes de stockage des données.*

L'un des moyens de garantir un bon usage de ces technologies et de procéder avant tout à des expérimentations. Quelles seraient selon vous les conditions que ce cadre expérimental devrait réunir ?

En reprenant les éléments développés ci-dessus et en les concrétisant par la mise en place de « projets pilotes » je pense que nous aurions déjà une base presque complète des conditions qu'un cadre expérimental devrait réunir.

Ce questionnaire est indicatif et ne prétend pas de couvrir l'intégralité des enjeux posés par les technologies de sécurité. La mission recueillera tout élément qui lui sera apporté afin de l'intégrer au mieux dans sa réflexion.

Contribution à la mission confiée par le Premier Ministre au député Jean-Michel Mis : « pour un usage responsable et acceptable par la société des technologies de sécurité »

Rédacteur : Sébastien Louradour – Expertise France - Expert Technique International en poste à San Francisco – en détachement au Centre pour la Quatrième Révolution Industrielle du Forum Économique Mondial

San Francisco, le 31 mai 2021

Cher Monsieur le député,

Je vous remercie de m'avoir sollicité pour apporter ma contribution à la mission qui vous a été confiée par le Premier Ministre « pour un usage responsable et acceptable par la société des technologies de sécurité ».

Au cours de ces deux dernières années, j'ai eu l'opportunité de participer à la construction de règles d'usage responsable de la reconnaissance faciale en lien avec une communauté internationale d'experts sur le sujet. Mes travaux ont notamment permis de construire un dialogue rassemblant chercheurs, société civile, entreprises technologiques et agences gouvernementales pour tester des modèles de gouvernance, afin de s'assurer de leur robustesse, de leur pertinence et leur mise en œuvre opérationnelle. Ce travail qui s'inscrit dans le cadre de la mission des Experts Techniques Internationaux à vocation à promouvoir l'influence de la France à l'international, notamment de ses acteurs économiques, et contribuer au développement des innovations et des nouvelles technologies.

La première partie de cette note présente comment le contexte politique aux Etats-Unis d'Amérique y influence la régulation de la reconnaissance faciale. Elle revient sur les acteurs d'influence et brosse le tableau du cadre législatif, notamment la loi votée par l'Etat de Washington, première loi votée par un Etat américain pour encadrer l'usage de la reconnaissance faciale.

La note présente ensuite la proposition de la Commission européenne pour encadrer l'usage de l'intelligence artificielle, qui articule la façon dont la reconnaissance faciale pourrait être régulée.

Cette note apporte enfin un éclairage sur les modèles de gouvernance testés au cours des travaux que j'ai réalisé. En particulier, elle revient sur le cas d'usage de la gestion des flux, qui s'applique au contrôle d'accès tels que dans les aéroports ou dans les stades. Elle revient enfin sur le cas d'usage des enquêtes de police, sujet hautement sensible compte tenu des risques qui y sont associés.

Pour conclure ce propos introductif, je me permets de vous livrer trois convictions que j'ai bâti au cours de ma mission :

Observer le cheminement de technologies aujourd'hui matures permet d'anticiper le potentiel développement de futures technologies de rupture. La reconnaissance faciale appartient à la catégorie des technologies facilitatrices, au même titre que le GPS, par exemple. Pour poursuivre l'analogie, il y a 20 ans, le GPS était développé pour le secteur de la défense et quelques applications de niche. Depuis, le croisement de cette technologie avec de nouvelles (internet, smartphone, objets connectés) a décuplé sa capacité initiale donnant naissance aux services basés sur la géolocalisation et permettant notamment le succès d'Amazon ou Uber. La reconnaissance faciale va très certainement engager un parcours comparable et faire émerger de nouveaux champions dans des domaines encore inconnus aujourd'hui. En ce sens, il s'agit d'une technologie qui a le potentiel de transformer durablement nos usages. En cela, favoriser son développement sur le territoire français et sa souveraineté est indispensable pour protéger durablement l'identité numérique des citoyens.

Privilégier la mise en place de processus d'atténuation des risques plutôt que de se concentrer sur des solutions technologiques. Afin de mettre en place une gouvernance pérenne, il est préférable de privilégier une approche « qualité des systèmes de management » plutôt qu'une approche par configuration technologique. Par exemple, plutôt que d'établir un seuil de performance de l'algorithme, susceptible de constamment évoluer, il est préférable de mettre en place des processus d'atténuation des risques pouvant être provoqués par un manque de performance ou une défaillance de l'algorithme. Il s'agit de l'approche de contrôle et d'audit que nous avons co-construite en partenariat avec AFNOR Certification et qui a été largement reprise par la proposition de loi de la Commission européenne sur l'IA.

Bâtir une expertise « Tech Policy » en France afin d'avoir la capacité de pleinement tirer parti de la quatrième révolution industrielle. Bien que la France doive indiscutablement favoriser l'émergence de champions numériques dans le domaine des technologies de sécurité, celle-ci doit également bâtir en parallèle une expertise dans le domaine de la gouvernance de ces nouvelles technologies. La croissance des startups va en effet de pair avec un cadre de gouvernance pérenne et stable qui favorise leur développement. Cela nécessite une réponse réglementaire qui établit des lignes rouges qui protègent les libertés individuelles et collectives et des règles qui favorisent l'adoption de ces technologies pour simplifier, moderniser et accélérer le travail des forces de sécurité. Une modalité à envisager pour bâtir une telle réglementation est la méthode de co-construction multipartite de cadres pilotes, notamment appliquée dans le cadre des travaux auxquels j'ai pu participer ces deux dernières années.

Je vous souhaite une excellente lecture et me tiens à votre disposition pour tout besoin d'échange complémentaire.

Veuillez, Monsieur le député, recevoir mes salutations les plus sincères.

Sébastien Louradour

I. Etats-Unis d'Amérique : la reconnaissance faciale au cœur des critiques dans un contexte de dénonciation des violences policières et de combat pour l'égalité raciale

La mort de George Floyd au cours d'une interpellation de police à Minneapolis le 25 mai 2020 a déclenché une vague d'indignations et de protestations à l'échelle du pays dont le séisme s'est étendu aux acteurs technologiques et qui, un an plus tard, **continue de provoquer d'importants changements politiques et sociaux**. A l'instar de la plupart des entreprises américaines, les géants du numérique se sont également investies dans le mouvement « black Lives Matter », d'une part pour témoigner leur soutien au mouvement mais également pour éviter les critiques qui pourraient se concentrer sur eux.

La dénonciation des violences policières étant au centre des préoccupations, **les « technologies de surveillance » utilisées par les forces de police, telles que la reconnaissance faciale (RF) ou les cameras au corps, ont immédiatement été pointées du doigt par les acteurs de la société civile**, travail souvent engagé depuis plus de deux ans (comme cela est présenté plus loin dans la note).

En réponse à ces accusations, la société **IBM[1] a pris la décision de se retirer de façon définitive du marché de la reconnaissance faciale** en affirmant que la RF ne devrait jamais être employée pour la surveillance de masse, ou encore le profilage racial. Le PDG d'IBM a également appelé à un dialogue national pour déterminer si les forces de police devraient utiliser la RF, et le cas échéant dans quelles conditions. **Les sociétés Amazon[2] et Microsoft[3] ont également suivi la décision historique d'IBM et mis en pause *sine die* l'usage de la reconnaissance faciale pour les forces de police**.

Un atlas de la surveillance aux Etats-Unis[4], mis en ligne par The Electronic Frontier Foundation (EFF) recense **375 départements de police utilisant actuellement la RF**. L'atlas recense également 1 738 partenariats entre la police et l'application Neighbors[5] qui permet d'accéder aux données enregistrées par **les caméras de surveillance Ring** (fixées sur le palier des portes d'entrées de particuliers) commercialisées par Amazon. Bien que ces données puissent techniquement être analysées via des outils de reconnaissance faciale, et malgré les craintes formulées[6], aucun rapport n'indique à ce stade que les forces de police en font cet usage.

La société civile américaine, fer de lance de la protestation contre les technologies de reconnaissance faciale

De nombreuses organisations de défense des libertés publiques américaines dénoncent depuis plusieurs années l'usage de la reconnaissance faciale par les forces de police. Parmi les plus vocaux, ACLU (American Civil Liberty Association), qui mène **une campagne[7] intitulée « Press Pause »** pour appeler à un moratoire sur l'usage de la reconnaissance faciale par les agences gouvernementales. D'autres organisations, telle qu'Amnesty International, appellent à une **interdiction totale de l'usage de la reconnaissance faciale**. Un troisième groupe enfin, mené par Joy Buolawini (Algorithmic Justice league), appelle à une régulation stricte de la reconnaissance faciale

[1] https://www.npr.org/2020/06/09/873298837/ibm-abandons-facial-recognition-products-condemns-racially-biased-surveillance
[2] https://www.nytimes.com/2020/06/10/technology/amazon-facial-recognition-backlash.html
[3] https://www.washingtonpost.com/technology/2020/06/11/microsoft-facial-recognition/
[4] https://atlasofsurveillance.org/
[5] https://ring.com/neighbors
[6] https://www.govtech.com/public-safety/California-Police-Amazon-Ring-Partnerships-Raise-Concerns.html
[7] https://www.aclum.org/en/campaigns/press-pause-face-surveillance

via un **modèle d'évaluation *ex ante* par une agence gouvernementale inspirée de la FDA** (Federal Drug agency) équivalent de l'ANSM (Agence Nationale de Sécurité du Médicament) en France.

Dans une interview intitulée « A Case For Banning Facial Recognition[8] » publiée le 9 juin 2020 par le New York Times, Timnit Gebru, alors chercheuse chez Google et ayant récemment collaboré sur un papier de recherche avec Joy Buolawini dénonce : « même un système de reconnaissance faciale parfait peut être mal utilisé. Je suis une femme noire vivant aux Etats-Unis qui a dû faire face à de sérieuses conséquences liées au racisme. **La reconnaissance faciale est utilisée contre la communauté noire.** Au cours des manifestations contre la mort de Freddy Gray, la police de Baltimore a utilisé la reconnaissance faciale pour identifier des manifestants en rapprochant les images avec leurs profils sur les réseaux sociaux ».

Cette affirmation démontre que le débat actuel sur la reconnaissance faciale aux Etats-Unis **ne se résume plus simplement à un problème de performance variant selon la couleur de peau, mais à la dénonciation d'un racisme systémique de la part des forces de police et de l'usage de technologies qui renforcent un système d'oppression vis-vis des communautés afro-américaines.** Cet angle d'analyse figure également dans le débat scientifique sur l'intelligence artificielle et se cristallise autour de la définition d'une « seconde vague de la responsabilité des algorithmes »[9][10]. En substance, **il s'agit d'interroger la « neutralité » supposée des algorithmes en mettant en évidence les systèmes de pouvoir qui sont à l'œuvre et dont l'objectif est leur maintien**. Cette « seconde vague » considère en effet qu'il ne s'agit pas de corriger les algorithmes afin qu'ils ne comportent plus de biais (ce qui correspond à l'approche de la « première vague ») mais à **transformer les systèmes de valeurs et de pouvoirs qui génèrent notamment des situations de « discriminations systémiques[11] ».**

[8] https://www.nytimes.com/2020/06/09/technology/facial-recognition-software.html
[9] https://lpeblog.org/2019/11/25/the-second-wave-of-algorithmic-accountability/
[10] https://onezero.medium.com/the-seductive-diversion-of-solving-bias-in-artificial-intelligence-890df5e5ef53
[11] https://www.nature.com/articles/d41586-020-02003-2

II. Une légalisation américaine disparate, influencée tant par la société civile que par Microsoft

Autre défenseur d'une régulation de la reconnaissance faciale, le Président de Microsoft - Brad Smith - s'exprime depuis 3 ans pour appeler à un **usage responsable de cette technologie**. Dans un post daté du 31 mars 2020[12], il annonçait qu'une loi venait d'être adoptée par l'Etat de Washington pour réguler l'usage de la reconnaissance faciale (**bill 62 80[13]**). Cette loi, présentée plus loin dans cette note, portant sur l'usage de la RF par les agences gouvernementales a été rédigée par le sénateur Joe Nguyen, employé de Microsoft, dont le siège de situe tout près de Seattle dans l'Etat de Washington. Cette loi est présentée par Brad Smith comme le modèle à suivre pour encadrer l'usage de la technologie[14]. **C'est à ce stade la seconde[15] loi aux Etats-Unis qui encadre, sans l'interdire, l'usage de la reconnaissance faciale à l'échelle d'un Etat.**

Des interdictions d'usage par les agences gouvernementales locales, notamment les forces de police, ont en effet été prononcées depuis 2 ans notamment par les municipalités suivantes : San Francisco et Oakland en Californie, Brookline, Cambridge, Northampton, et Somerville au Massachusetts. **L'interdiction de l'usage de caméras au corps utilisant la reconnaissance faciale a également été prononcée** dans les États de Californie, de l'Oregon et du New Hampshire.

Il est à noter **qu'une proposition de bannir complètement l'usage de la RF par les agences fédérales** a par ailleurs été présentée par des membres démocrates du congrès. « The Facial Recognition and Biometric Technology Moratorium Act[16] » est défendu par deux sénateurs (Ed Markey du Massachusetts et Jeff Merkley de l'Oregon) et deux représentants de la chambre (Pramila Jayapal de l'Etat de Washington et Ayanna Pressley du Massachusetts).

Comme le souligne un récent article de MIT Tech Review, **le climat politique entourant le sujet de la reconnaissance faciale s'est durci au cours de cette dernière année**, ce qui provoque la réticence des fournisseurs de technologies et les agences gouvernementales à en faire désormais usage. Il prédit ainsi que même sans loi, **des agences gouvernementales pourraient décider unilatéralement d'interdire leur usage[17]**.

[12] https://blogs.microsoft.com/on-the-issues/2020/03/31/washington-facial-recognition-legislation/
[13] https://app.leg.wa.gov/billsummary?BillNumber=6280&Year=2019&Initiative=false
[14] https://www.biometricupdate.com/202004/washington-state-restricts-facial-recognition-use-with-passage-of-microsoft-backed-law
[15] La seconde, votée en mai 2021 dans l'Etats du Massachusetts encadre de façon beaucoup plus légère que la loi de Washington l'usage de la reconnaissance faciale
[16] https://www.markey.senate.gov/news/press-releases/senators-markey-and-merkley-and-reps-jayapal-pressley-to-introduce-legislation-to-ban-government-use-of-facial-recognition-other-biometric-technology
[17] https://www.technologyreview.com/2021/05/21/1025155/amazon-face-recognition-federal-ban-police-reform/

III. Présentation et analyse de la loi de l'Etat de Washington – bill 62 80 : Créer de la transparence avec des mécanismes d'évaluation consultatifs et donner à l'autorité judiciaire le pouvoir d'activer la surveillance de lieux publics

Il s'agissait, au moment de son adoption, du premier texte de loi qui légifère spécifiquement sur l'usage de la reconnaissance faciale. Influencé par Microsoft, le texte pose les bases d'un usage légitime de la RF par les agences gouvernementales, mais laisse ouverte la question de son évaluation et de son contrôle. Cette loi s'articule autour de plusieurs grands axes :

- **Un débat public consultatif pour chaque cas d'usage envisagé mais pas d'évaluation ex ante**

Un rapport de transparence doit être rédigé pour chaque cas d'usage proposé par une agence gouvernementale. Il permet notamment de définir le cas d'usage prévu et d'éviter qu'il y ait un détournement de la technologie à d'autres fins. Ce rapport détaillé permet de documenter l'usage réalisé. Il est ensuite soumis à un débat public et sa version finale doit être rendue publique. Il n'existe en revanche pas de dispositif d'évaluation *ex ante* permettant d'interdire le cas d'usage présenté dans le rapport de transparence. En outre, les systèmes de reconnaissance faciale sont soumis à une expérimentation préalable lorsque leur usage peut avoir des conséquences pénales pour les individus.

- **Seule l'autorité judiciaire peut autoriser son usage à des fins de surveillance.**

L'usage de la reconnaissance faciale par les forces de police est autorisé dès lors qu'un mandat est fourni par l'autorité judiciaire ou que des circonstances exceptionnelles l'exigent. Cela concerne notamment la surveillance des espaces publics, et le suivi ou la recherche active de personnes. Pour le reste, il est rappelé que l'usage de la reconnaissance faciale ne peut être accordé s'il enfreint le premier amendement ou l'exercice des libertés fondamentales.

- **Enquêtes et procès : la reconnaissance faciale seule ne peut faire l'objet d'une preuve**

Dans le cas d'un procès s'appuyant sur des données de reconnaissance faciale, la défense doit en être tenue informée. Pour autant, pour être recevable, une preuve s'appuyant sur la reconnaissance faciale doit systématiquement s'accompagner d'autres preuves légalement obtenues au cours de l'investigation. Tout usage de la reconnaissance faciale ayant une potentielle conséquence légale sur des individus doit systématiquement être revu par un agent.

- **Evaluation des usages : mise en place d'un comité de suivi consultatif et obligation de mettre à disposition une API pour tester la performance de l'algorithme sans pour autant établir de seuils ou de standards à respecter**

Un comité de suivi consultatif est nommé. Il est notamment composé de parlementaires, de représentants de la société civile, d'agences gouvernementales, de chercheurs et d'industriels. Son rôle consiste en particulier à réaliser des évaluations sur le déploiement de la technologie par les agences de l'Etat.

Une API doit être fournie par le fournisseur de technologie pour réaliser des tests indépendants de performance de l'algorithme, identifier des biais, et le cas échéant demander au fournisseur de rectifier son algorithme sous 90 jours. Il n'est en revanche pas précisé ce qui correspond à un résultat satisfaisant ou insatisfaisant en matière d'écart de performance, laissant ouverte la possibilité d'un recours en justice, et à la jurisprudence, pour abriter ce qui relève d'un seuil de performance approprié.

IV. Présentation et analyse de la proposition de la Commission européenne pour encadrer l'usage de la reconnaissance faciale à des fins d'identification.

Après plus de deux années de concertations et de travaux sur la question de l'usage responsable de l'intelligence artificielle, la Commission européenne a présenté le 21 avril 2021 sa **proposition de loi européenne sur l'intelligence artificielle**[18]. **La biométrie à distance occupe une place d'importance dans le texte** et augure d'une stricte règlementation de sa mise en œuvre dans **les cas d'usage associés aux activités d'identification** des individus. Il est dès à présent à noter que **la proposition ne concerne pas les activités d'authentification**, c'est-à-dire la comparaison d'un titre d'identité avec le visage correspondant, laissant le RGPD comme principal texte encadrant cet usage.

Les systèmes de biométrie à distance utilisés en temps réel et *a posteriori* à des fins d'identifications de personnes sont **considérés à haut risque** et devraient ainsi nécessiter une **évaluation *ex-ante* du fournisseur de technologie** pour attester de son respect du cadre législatif et pour bénéficier de l'accès au marché européen. Une évaluation *ex-post* du fournisseur est également exigée.

A cela s'ajoute le cas d'usage spécifique de l'usage en temps réel des technologies de biométrie à distance à des fins **d'identification et réalisée par les forces de l'ordre**. **Ce cas d'usage est prohibé, à moins qu'il ne respecte les conditions spécifiques suivantes** :

- 1. « la recherche ciblée de victimes potentielles spécifiques, y compris les enfants disparus » ;
- 2. « la prévention d'une menace spécifique, substantielle et imminente pour la vie ou la sécurité physique des personnes physiques ou d'une attaque terroriste » ;
- 3. « la détection, la localisation, l'identification ou la poursuite d'un auteur ou d'un suspect d'une infraction pénale visée à l'article 2, paragraphe 2, de la décision-cadre 2002/584 / JAI du Conseil et passible dans l'État membre concerné d'une peine privative de liberté ou d'un mandat de rétention pour une durée maximale d'au moins trois ans, telle que déterminée par le droit de cet État membre. »

Des conditions complémentaires sont également nécessaires telles que l'autorisation en amont par une autorité judiciaire ou une autorité administrative indépendante, **à moins d'une situation d'extrême urgence** qui dans ce cas précis exonère d'une telle approbation. Enfin, **chaque pays membre est tenu de voter une loi** qui autorise en totalité, en partie, ou interdit l'usage de la biométrie à distance pour ce cas d'usage spécifique.

Evaluation *ex-ante* et *ex-post* des fournisseurs de technologie

L'évaluation *ex-ante* (évaluation de la conformité des fournisseurs de technologie) inclue :

- Une revue du respect des attendus et règles définis dans le chapitre 2 du projet de loi
- Une évaluation de la qualité des systèmes de managements, qui incluent les procédures de gestion des risques et un contrôle du système après son entrée sur le marché européen.
- L'évaluation de la documentation technique du système d'IA concerné.

Certifier la qualité des processus plutôt que la performance des algorithmes

Alors que les fournisseurs de technologies ont pour nécessité d'atteindre le plus haut niveau de performance des systèmes qu'ils déploient, cet objectif, bien que nécessaire, ne représente pas l'étape la plus significative pour prévenir le risque de dommages.

[18] https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence

Ainsi, **la Commission européenne ne détaille aucun seuil de performance à respecter**, mais requière en revanche l'obligation de fournir une documentation portant sur les processus mis en œuvre pour limiter les risques associés au cas d'usage pour lequel la reconnaissance faciale est utilisée.

Le déploiement d'un système de management de la qualité est une étape majeure dans la mesure ou les fournisseurs de technologie vont **devoir concevoir les processus internes adéquats pour activement limiter les risques potentiels**.

Un focus sur les processus et le management des risques

Alors qu'il sera de la responsabilité des fournisseurs de technologie de déterminer la façon dont ils souhaitent bâtir leurs processus de qualité, **des organismes tiers accrédités** auront la charge de vérifier la conformité des processus avec les attendus de la législation européenne. **Pour se mettre en conformité, les fournisseurs de technologie vont être dans l'obligation de bâtir une approche sur mesure pour définir, implémenter et mettre en œuvre les processus adéquats.**

V. Projet pilote du Forum Economique Forum pour encadrer l'usage de la reconnaissance faciale pour simplifier et sécuriser la gestion des flux

Démarré en avril 2019, et piloté par le Forum Économique Mondial, **ces travaux consistent à établir des règles pour assurer un usage responsable de la reconnaissance faciale pour la gestion des flux.**

Ce projet multipartite associe des acteurs privés (Microsoft, Amazon, Idemia, IN Groupe, NEC, Aéroport de Paris, SNCF, Aéroport de Tokyo-Narita, AFNOR Certification), publics (CNNum, CNIL, Commission européenne, Gouvernement du Japon), société civile et chercheurs.

Les travaux ont conduit à bâtir un cadre d'usage, présenté dans un livre blanc publié en mars 2020 et disponible en français[19]. Ces travaux ont permis d'établir un cadre de gouvernance pour les usages associés à la gestion des flux (i.e. aéroports, gares, stades, etc.).

Ce cadre de gouvernance comprend une **série de principes à respecter** (couvrant notamment la protection des données, la gestion des risques, et la transparence vis-à-vis des utilisateurs), **une liste de bonnes pratiques pour accompagner les acteurs à mettre en place les principes, et un questionnaire d'auto-évaluation pour permettre aux organisations utilisant la technologie de confirmer qu'ils respectent les principes énoncés.**

Un référentiel pilote testé par des acteurs industriels

Afin de vérifier la conformité au cadre de gouvernance l'adoption du cadre d'usage, **un référentiel d'audit a été construit avec AFNOR Certification** pour permettre à cet organisme de délivrer un label aux utilisateurs de la technologie qui se soumettent à un audit externe. L'objectif consiste à proposer une **évaluation *ex post*** qui encourage les projets d'innovation tout en se conformant à des principes de responsabilité collégialement conçus. Ce référentiel d'audit est présenté dans le second livre blanc, publié en décembre 2020, et disponible en français[20].

Ce référentiel d'audit a vocation à être adopté de façon volontaire par les acteurs du transport à l'échelle internationale ainsi qu'à informer le législateur pour créer des mécanismes d'évaluation inscrits dans une loi sur la reconnaissance faciale.

[19] http://www3.weforum.org/docs/WEF_Cadre_d'action_Reconnaissance_Faciale_2020.pdf
[20] https://fr.weforum.org/whitepapers/responsible-limits-on-facial-recognition-use-case-flow-management

VI. Groupe de travail INTERPOL/UNICRI/Police des Pays-Bas/Forum Economique Mondial pour établir une position commune sur la gouvernance de la reconnaissance faciale pour le cas d'usage des enquêtes de police

Le Forum Economique Mondial a lancé en janvier 2021 une initiative pour définir **un modèle de gouvernance pour l'usage de la reconnaissance dans le cadre des enquêtes de police**. Il s'agit de travaux menés par la coalition d'acteurs gouvernementaux suivante : INTERPOL, UNICRI et la Police des Pays-Bas.

L'objectif de ces travaux est de **produire une position commune établissant des propositions de règles d'usages**, accompagnés d'un **questionnaire d'auto-évaluation** permettant à tout département de Police de se saisir de ce document comme outil pour concrètement mettre en place des règles de gouvernance et d'encadrement des technologies de RF.

La méthode de rédaction retenue intègre une concertation avec une communauté de projet étendue, composée **d'experts issus de la société civile, de la recherche, d'entreprises technologiques et d'agences gouvernementales**. Cette communauté de projet a notamment été invitée en février 2021 à un workshop en ligne pour contribuer à une première réflexion sur des pistes de gouvernance. Cette communauté de projet est également invitée à commenter la proposition de principes d'usages formulée par le groupe de travail.

A l'issue de ces travaux, **un livre blanc présentant une version définitive des principes d'usage et du questionnaire d'auto-évaluation sera publié**. Cette publication devrait intervenir au cours du quatrième trimestre 2021.

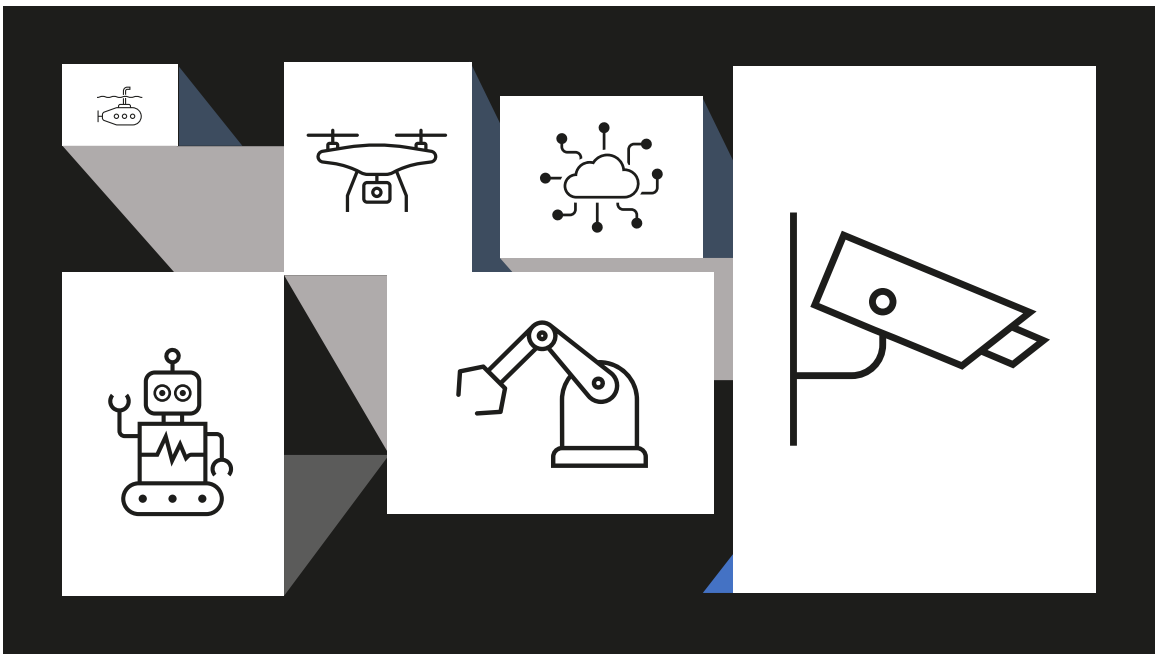
Contribution collective de Mme Manon Vermenouze (Shark Robotics)
et MM. Thierry Berthier (Hub France IA), Geoffroy Deltel (Photonis)
et Victor Vuillard (Parrot)

Note contributive

Robotique de sécurité

Mission parlementaire dirigée par le Député Jean-Michel MIS

« Sur l'utilisation des nouvelles technologies dans le domaine de la sécurité »



« La robotique au service des forces de sécurité, police, gendarmerie, douanes et sécurité civile »

07 juin 2021

CONTRIBUTEURS :

Thierry BERTHIER (coordinateur de la note), Pilote du groupe Sécurité, Intelligence Artificielle, Robotique du Hub France IA. Conseiller scientifique de la Fédération professionnelle européenne Drones4Sec.

Victor VUILLARD, Président de la Fédération professionnelle européenne des drones de sécurité Drones4Sec. Responsable sécurité du groupe PARROT.

Manon VERMENOUZE, Directrice de la communication et des affaires publiques de SHARK Robotics.

Geoffroy DELTEL, CTO, Digital Vision General Manager de Photonis

DESTINATAIRE :

Monsieur le Député Jean-Michel MIS

SOMMAIRE

PREAMBULE – Généralités sur la robotique 4

PARTIE I – Les cas d'usage des drones, de la robotique et leurs apports au domaine de la sécurité 11

PARTIE II – Les champions français de la robotique et du drone de sécurité : PARROT, SHARK ROBOTICS, PHOTONIS, HOVERSEEN, OBVIOUS TECHNOLOGIES, ECA GROUP 16

PARTIE III – Les drones de confiance, cybersécurité et protection des données à caractère personnel 51

PARTIE IV – Les préconisations pour renforcer la filière industrielle de sécurité et faciliter la diffusion des technologies auprès des services de sécurité 57

PARTIE V - Le marché mondial de la robotique de sécurité sur la période 2021-2026 - croissance, tendances et prévisions. Les chiffres de la robotique en France. 63

PREAMBULE

Généralités sur la robotique

En deux décennies, les progrès conjugués de la robotique, de l'intelligence artificielle, de l'optoélectronique, des matériaux, des capteurs et des batteries électriques permettent de construire des systèmes robotisés utiles, robustes et efficaces. Qu'ils soient terrestres, aériens ou maritimes, ces robots, drones, rover répondent à des besoins « métiers » des forces de sécurité (Police, Gendarmerie, Douanes, Sécurité Civile, Sapeurs-Pompiers). Ils permettent d'éloigner l'homme du danger, d'accroitre son rayon d'action, de gagner un temps précieux dans un contexte de crise ou d'urgence. Les robots d'inspections ou de levée de doute augmentent considérablement les capacités de réaction des équipes chargées de la surveillance d'une zone terrestre aérienne ou navale.

Un robot est le produit d'un grand nombre de technologies

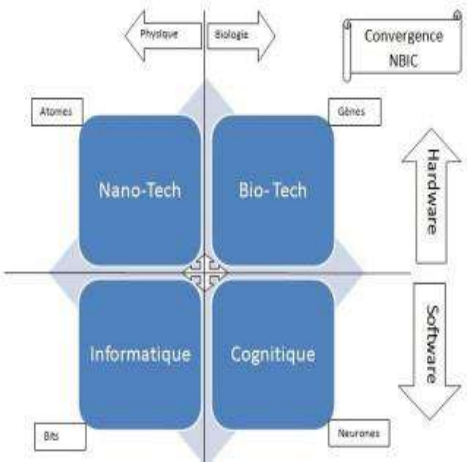
La robotique, c'est un vaste ensemble de segments technologiques qui s'additionnent pour pouvoir construire un robot : mécanique, électronique, mécatronique, matériaux, optique, capteurs multispectraux, software, mathématiques, contrôle optimal, systèmes multi-agents, apprentissage par renforcement, computer vision, Machine Learning, cybersécurité, IoT, communications, antennes, électromagnétisme, impression additive, des neurosciences, des sciences cognitives, de la R&D, des laboratoires de recherche, …

Les domaines adressés par la robotique sont tout aussi variés : industrie, production, logistique, transports, défense, sécurité civile, pompiers, surveillance des territoires, écologie, dépollution automatisée (terre, air, mer), santé médecine (implants, prothèses intelligentes, robots chirurgicaux), agriculture (la robotique autonome est le moteur de la révolution agricole), énergie, BTP construction, biotechnologies, pharmacologie, industrie minière, aéronautique civile et militaire, aérospatiale, secteur ferroviaire et métros, automobile et mobilités intelligentes,…

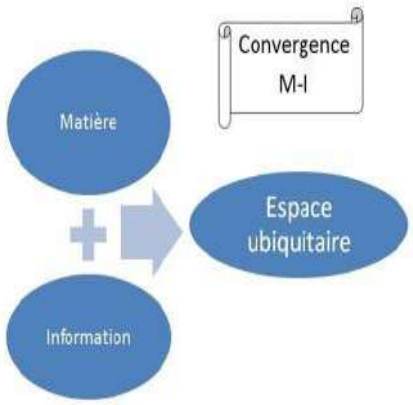
La robotique se situe au cœur de quatre dynamiques de convergences technologiques

La robotique s'inscrit au cœur des quatre grandes convergences technologiques du 21ième siècle : NBIC, MI, DIADEH, CKTS :

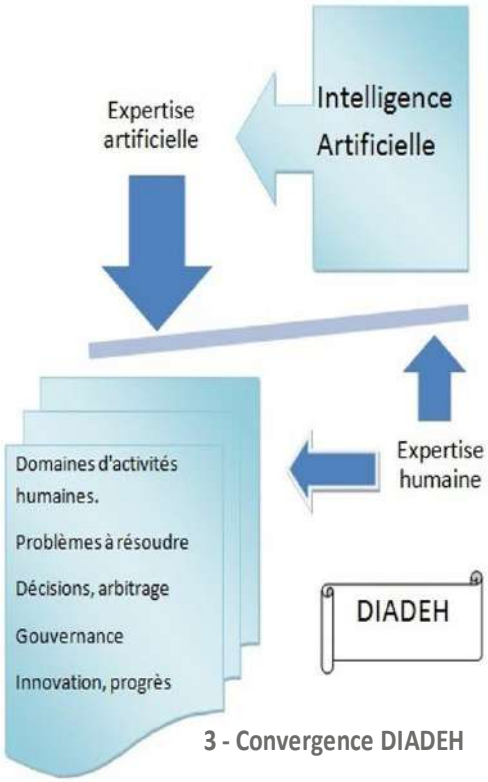
- La convergence NBIC est la convergence des Nanotechnologies, des Biotechnologies, de l'Informatique et des sciences Cognitives.
- La convergence MI est la convergence de la Matière et de l'Information pour produire un espace ubiquitaire.
- La convergence DIADEH (Diffusion de l'IA sur les Domaines d'Expertise Humaine) est la convergence de l'expertise humaine et de l'intelligence artificielle pour produire une expertise hybride.
- La convergence CKTS (Convergence of Knowledge and Technology for the benefit of Society).



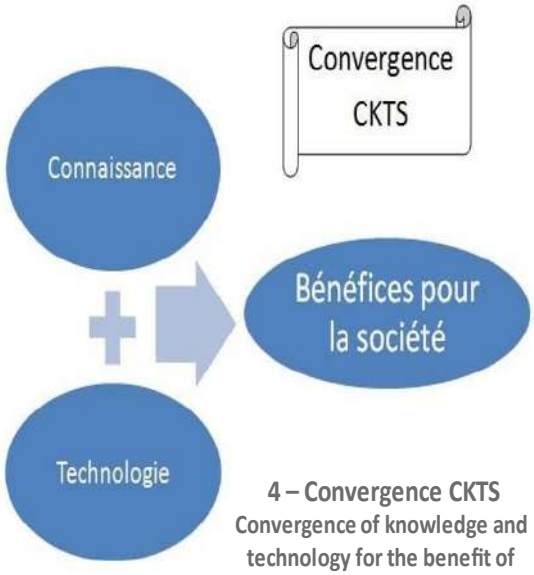
1 - Convergence NBIC



2 - Convergence Matière– Information



3 - Convergence DIADEH



4 – Convergence CKTS
Convergence of knowledge and technology for the benefit of society

Le 21 -ème siècle est celui de la robotique autonome et de la « société 5.0 » :

Société 1.0 des chasseurs-cueilleurs,

Société 2.0 de l'agriculture,

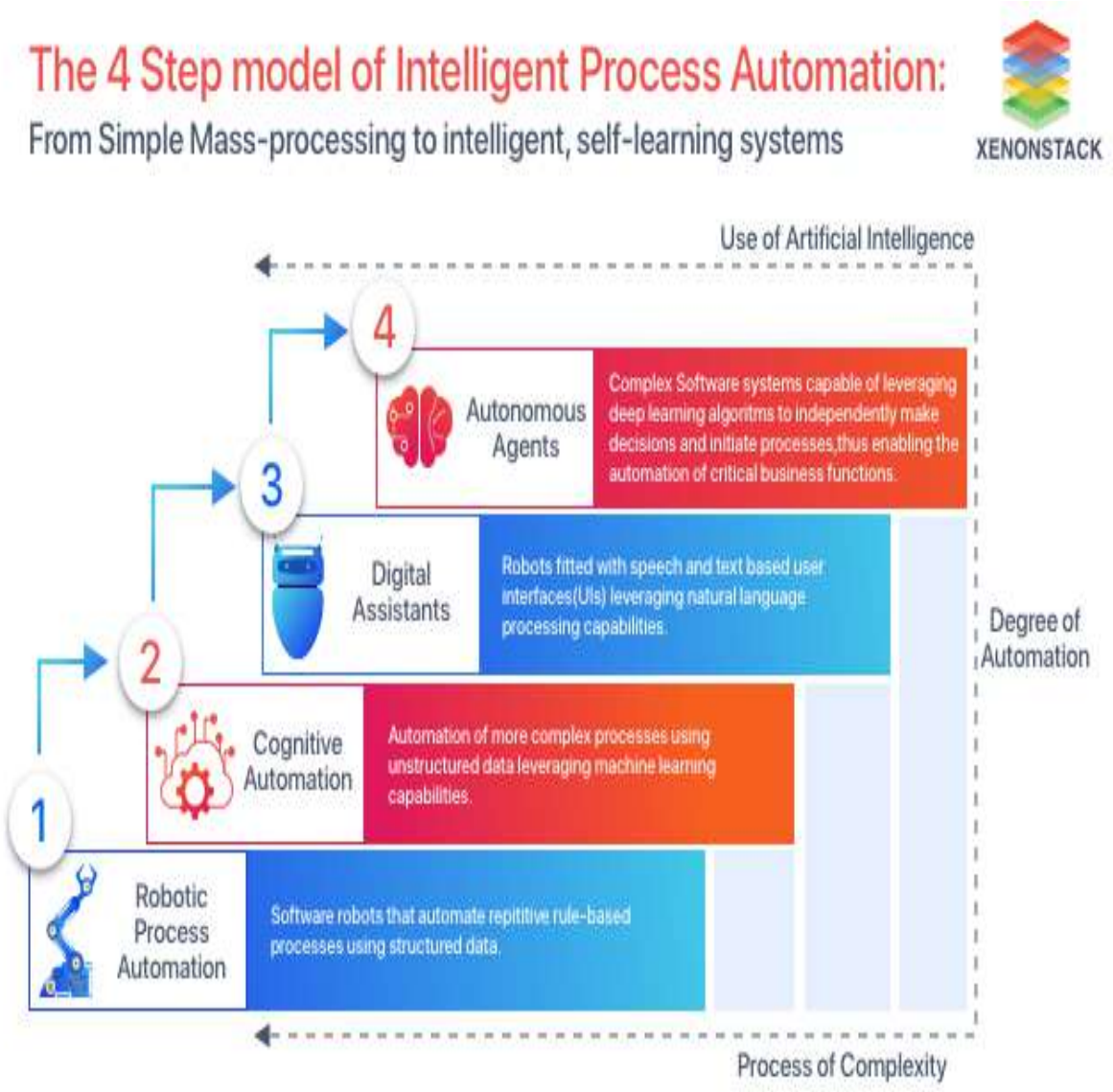
Société 3.0 de l'industrie,

Société 4.0 de l'information,

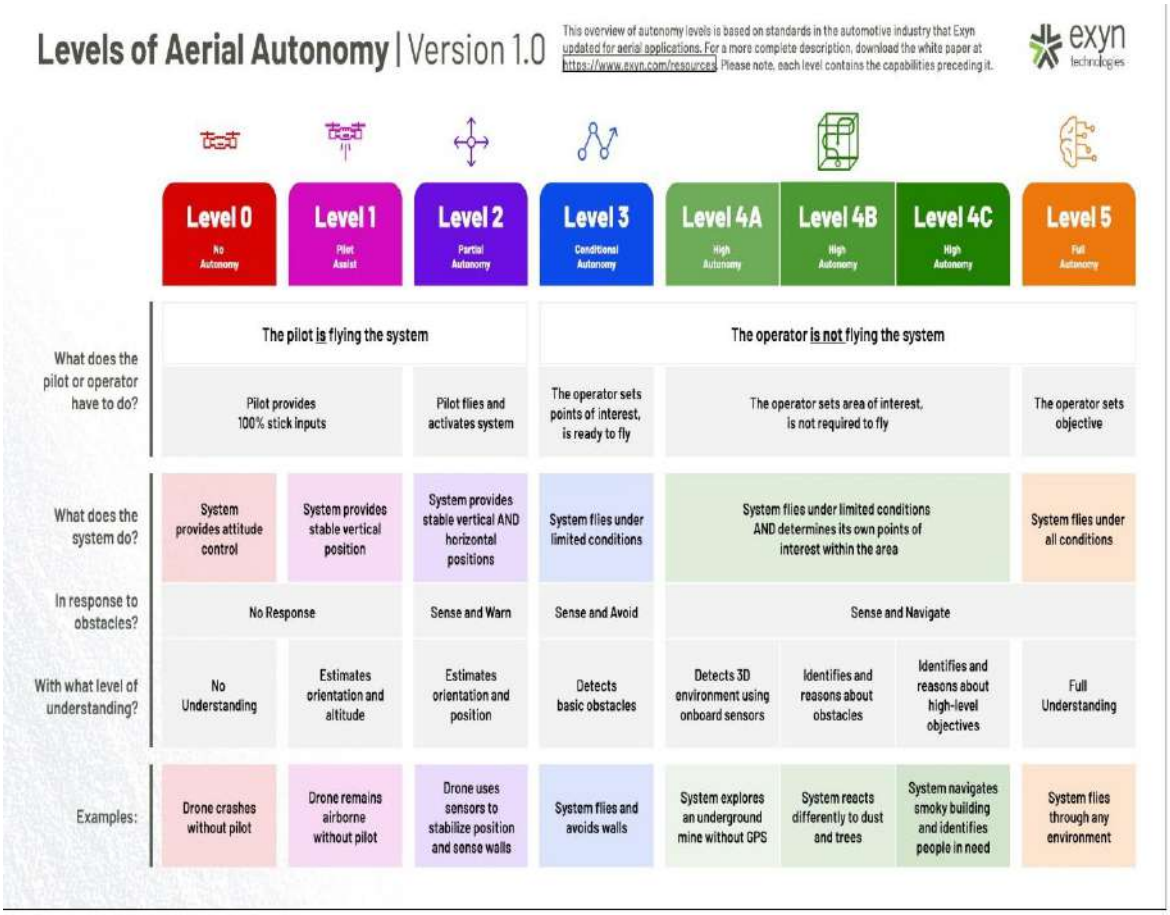
Société 5.0 : smart society, robotique ubiquitaire, smart city, industrie 4.0

Niveau d'autonomie d'un robot

Le niveau d'automatisation d'un processus physique ou numérique dépend du degré d'intervention de l'opérateur ou du superviseur humain dans l'exécution du processus.



Pour les drones aériens et robots terrestres, il existe une classification en six niveaux d'automatismes qui permet de définir précisément le niveau d'autonomie du système.



Les robots investissent tous les secteurs d'activités humaines.

Une forte valeur ajoutée de la robotique dans les innovations de services

Source – DGE 2017

Sécurité et surveillance : un large champ d'application pour la robotique

Source – DGE 2017

Le développement de la robotique est associé à des défis scientifiques et techniques stratégiques pour la France

Source – DGE 2017

PARTIE I

Les cas d'usage des drones, de la robotique et leurs apports au domaine de la sécurité

Depuis quelques années, les drones et les robots sont venus compléter les outils dont disposent les policier, gendarmes, pompiers et la sécurité civile de manière générale. Nous décrivons ci-dessous quelques cas d'usage qui montrent la variété de contextes et les bénéfices que les drones et robots y apportent. Cette liste n'est bien sûr pas exhaustive, cas le domaine reste naissant. La technologie évolue très vite. L'appropriation des drones et des robots par les utilisateurs progresse également et les cas nouveaux cas d'usages se multiplient de mois en mois.

1. Robot pompier, de surveillance ou de déminage

Le robot pompier COLOSSUS développé par SHARK Robotics intervient sur tous les types de feux, en particulier dans les parkings souterrains ou les zones d'accès difficiles pour les secours. Il est intervenu durant onze heures dans le brasier de la cathédrale Notre Dame de Paris à des températures atteignant les 900 degrés. Les robots de déminages interviennent en zone de guerre ou sur une scène d'attaque terroriste pour dépiéger un lieu. Robot déminage ou dépiégeage

2. Surveillance - visions jour et thermique

Les drones volants sont avant tout utilisés pour leur capacité de vision, que ce soit sur la voie jour ou la vision nocturne ou thermale. Ils constituent un outil de choix pour l'observation, la surveillance, la recherche ou le renseignement. Ils sont utilisés dans de multiples contextes, y compris dans les plus sensibles comme les opérations de police judiciaire, le grand banditisme ou l'anti-terrorisme.

La capacité des drones d'observer de haut, de manière discrète, permet de recueillir plus d'information, tout en limitant l'exposition des policiers ou gendarmes. Ils peuvent rester en vol ou être posé sur un espace en hauteur comme un toit d'immeuble. Le fait qu'ils soient pilotés évite qu'un policier ou gendarme s'expose lors d'une planque ou pour installer un dispositif de captation vidéo dans une zone soit dangereuse, soit qui risquerait par cette activité de porter atteinte à la discrétion de l'opération.

Les visions nocturnes ou thermal permettent d'identifier des activités également de nuit. La vision thermal permet d'acquérir des informations complémentaires y compris de jour, par exemple de détecter la chaleur du moteur d'une voiture ou du canon d'une arme qui vient

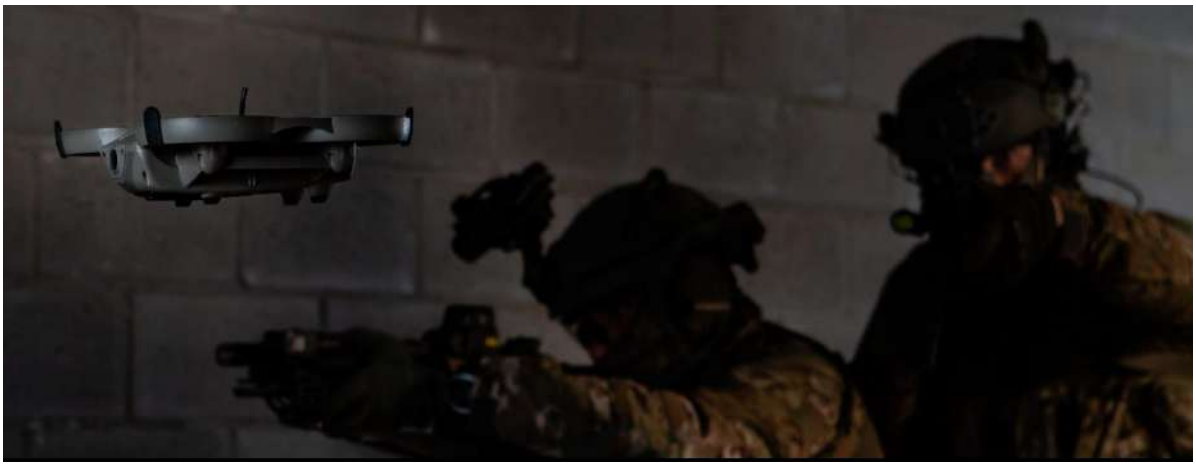
juste de faire feu. Cette capacité est également utile lorsque qu'une cible est camouflée ou difficilement visible, comme pourrait l'être un fugitif habillé de camouflage dans une forêt.

La vision thermal est aussi utilisée de plus en plus par les pompiers et la sécurité civile. Ils s'en servent d'une part pour détecter des départs de feu, en particulier dans le sud de la France durant la période estivale, d'autre part lorsqu'un incendie est déclaré, pour obtenir une vision haute de l'incendie et identifier les zones d'un bâtiment où le foyer est plus vif.

En matière de capacité, les drones peuvent offrir une vision entre plusieurs centaines de mètres et plusieurs kilomètres. En considérant les drones produits de manière industrielle de moins d'un kg, Parrot est le seul acteur européen à fournir de telles solutions. Son modèle Anafi USA pèse moins de 500 g et il dispose de 3 optiques, une optique grand angle pour le pilotage, une autre disposant d'une capacité de zoom x32 et une troisième optique avec capteur thermal FLIR Boson. Cette configuration permet d'identifier de jour une personne et voir si elle est armée à 2 km, ainsi que d'identifier une personne de nuit à 300 mètres de distance. La composante de poids est importante pour la discrétion. Le drone est inaudible à 150m en environnement calme. A cette distance, il n'est pas non plus identifiable à l'œil nu (la version Security Edition propose également l'extinction de toute lumière y compris leds de la batterie, afin d'assurer une discrétion de nuit).

3. Colonnes d'assaut

Les robots roulants ou drones volants peuvent être intégrés dans une colonne d'assaut afin d'obtenir la vision d'une zone quelques secondes avant d'y engager des hommes. Par exemple, les forces spécialisées telles que le RAID ou le GIGN utilisent des drones Loki de la société belge Sky Hero.



Le drone est conçu pour être robuste. Il peut se glisser sous une voiture ou dans une gaine d'aération, se cogner su n'importe quel côté tout en restant stable. Il peut être équipé d'accessoires, par exemple d'un brise-glace pour passer une vitre. La chaine vidéo est conçue pour offrir le moins de latence possible, ce qui permet une certaine instantanéité dans la prise de décision de l'évolution de la colonne d'assaut.

4. Surveillance physique de sites sensibles ou de grands événements

Les drones volants servent également de plus en plus pour la surveillance, soit de l'enceinte physique de bâtiments ou installations sensibles, soit de grands événements tels que les JO 2024, la coupe du monde de rugby ou le défilé du 14 juillet.

Pour la surveillance physique d'un site sensible, les drones peuvent être installés à demeure dans une station d'accueil, qui permet de recharger le drone et lancer ses missions. Dans des solutions tels que celles d'Hoverseen, le drone et sa station se greffent à des VMS (Video Management System) utilisés pour de la vidéosurveillance ou vidéoprotection. Ils peuvent ainsi être utilisés pour réaliser des rondes sur certaines zones, y compris lorsqu'elles sont difficilement accessibles (au-dessus d'installations industrielles, d'un toit, d'un terrain accidenté) ou pour aller lever un doute. En effet, lorsqu'une alerte de sécurité physique est émise par un équipement autre que la vidéosurveillance (ex : capteur volumétrique, vibration d'un grillage, faisceau IR), la solution est usuellement d'envoyer un rondier. Cela nécessite d'avoir suffisamment de personnel de sécurité sur site. Certains sites peuvent être relativement étendus, par exemple sur plusieurs km ; dans ce cas, le rondier aura parfois besoin de plusieurs dizaines de minutes, là où un drone prêt à décoller sera sur zone dans l'ordre de la minute. Le vol du drone est complètement automatisé, l'image retransmise sur un mur d'écran et il est possible à l'agent de surveillance d'orienter la vision du drone comme une caméra PTZ. L'automatisation du vol sur des scénarios prédéterminés permet de s'abstraire de la présence continue d'un télépilote tout en respectant la réglementation aérienne – un agent de sécurité suffit. Les scénarios définis dans l'automatisation offrent aussi la possibilité de définir des zones d'exclusion, par exemple en limite de site ou lorsque des fenêtres d'habitations risqueraient de se trouver dans le champs visuel du drone, afin de garantir la protection des libertés individuelles et des données à caractère personnelles.

5. Recherche de personne disparue

La recherche de personnes disparues, par exemple en forêt ou en montagne peut nécessiter des dispositifs importants, sur d'importantes zones à couvrir. Sans remplacer l'humain, l'utilisation de drone volant permet d'une part de couvrir des zones importantes rapidement, d'autre part d'assister l'humain dans la levée de doute. Par exemple, pour le secours d'alpinistes accidentés en montagne, le terrain escarpé peut rendre les recherches très lentes,

en particulier lorsque la localisation des victimes est peu précise. Dans ce cas, le drone peut faire une cartographie rapide. Les capacités thermal peuvent aider à identifier les personnes, dont la chaleur va ressortir. Même lorsque les équipes de secours sont proches, ils peuvent utiliser un drone pour rechercher la victime dans une zone non visible, comme derrière des rochers ou dans une crevasse. Un drone type Parrot Anafi ou Anafi USA, de par sa compacité (respectivement 320 g et 495 g) peuvent facilement être portés dans le sac à dos d'un gendarme du PGHM ou d'un CRS de haute montagne.

6. Cartographie

Le vol d'un drone (quadcoptère ou aile fixe) peut être automatisé pour créer une grille de vol où le drone va prendre des photos à intervalle régulier. Les photographies seront ensuite injectées dans un logiciel de photogrammétrie, qui va recoller ces images les unes avec les autres afin de recréer une carte en 2D ou un modèle en 3D. L'entreprise suisse Pix4D, filiale du français Parrot, est le leader mondial des logiciels de photogrammétrie. Elle peut être utilisée autant pour modéliser un seul bâtiment, une ville entière, ou une étendue plate ou avec un relief changeant de plusieurs km².

Les cas d'usages sont multiples. Les cartes peuvent être particulièrement utiles pour obtenir une vision immédiate d'une zone dévastée lors d'une catastrophe naturelle, afin d'orienter les secours vers les personnes à secourir ou pour établir une évaluation des dégâts. Pix4D propose une version Pix4D React, dont l'objet est de permettre cette cartographie le plus rapidement possible est totalement hors ligne, ce qui permet une utilisation d'une part dans des zones reculées sans connexion Internet, d'autre part la capacité de traiter les modèles de terrains sur des poste isolés lorsqu'il s'agit de sujets sensibles.

Ce type de cartographie peut être utile également pour la sécurité de grands événements, afin de disposer d'une reconstitution de l'environnement à jour, y compris lorsque des installations temporaires y figurent. La cartographie en temps réel permet de suivre une évolution, voire identifier des anomalies entre différents moments d'un événement. Par exemple, cela permettrait d'identifier un véhicule qui n'a jamais bougé, ou à l'inverse un véhicule qui est nouveau dans une zone.

Ces modèles numériques en 3D peuvent d'avérer précieux pour un centre de commandement, en cas d'événement particulier comme une prise d'otage ou une attaque numérique. Les reconstitutions 3D peuvent être créées en quelques minutes lorsque l'événement se produit, ou être créées en avance sur des sites où un événement est redouté. Ces modèles permettent en particulier d'avoir une vision précise de l'ensemble des entrées ou des chemins d'entrées ou de sorties possibles, y compris sur les toits.

Des modèles de situations passées peuvent servir à des reconstitutions, des exercices ou des formations. Les reconstitutions en 3D peuvent modéliser un accident.

7. Evolution du domaine des drones et de la robotique

Les drones et les robots sont aujourd'hui majoritairement pilotés, dans un modèle un pilote = un drone, même si certaines phases peuvent être automatisées et permettent au pilote de mener d'autres actions en parallèle. La technologie évolue pour offrir plus d'autonomie et de connectivité :

- L'augmentation des capacités de calcul et l'intelligence artificielle permettent d'augmenter le niveau d'autonomie des robots et des drones,
- La connectivité évolue de modèles où des solutions radio point à point sont utilisés vers l'intégration de connexions directes vers Internet, en particulier en utilisant des modules 4G ou 5G. Ce progrès permet d'une part d'envoyer plus facilement des données vers des logiciels de traitement et d'autre part d'intégrer les drones et robots dans des solutions de commandement. Ces dernières vont faire progresser le modèle 1 pilote = 1 drone vers un modèle où un humain supervise l'action de plusieurs robots ou drones et intervient dans la prise de décision, les difficultés que les robots ne peuvent pas résoudre seuls, les actions qui demandent une validation humaine.

Ces évolutions arrivent très vite. A titre d'exemple, le français Parrot a annoncé la sortie le 30 juin 2021 d'un tel drone robot, disposant d'autonomie, d'une connectivité accrue et d'un niveau élevé de cybersécurité.

8. Résumé des bénéfices des drones et des robots

Les drones ou les robots viennent rarement remplacer les hommes, mais ils permettent de :

- Gagner en efficacité, en apportant plus d'informations, plus rapidement. Les actions déléguées au drone ou robot permettent à l'humain de se concentrer sur les actions à plus forte valeur ajoutée. La vue globale, en hauteur, est précieuses pour la prise de décision ou le commandement des opérations ;
- Eloigner l'homme du danger, en apportant une vision ou une action précise, sans que l'humain soit directement exposé.

En complément de ces avantages directs pour les métiers des domaines de la sécurité, les drones et les robots apportent un gain de coût. En particulier, le dernier livre blanc de la sécurité intérieur met en exergue une sous-capacité des moyens aériens. L'acquisition d'hélicoptères et la formation de leurs pilotes représentent un coût très important, là où un drone peut remplir des missions d'observation à moindre coût. A titre comparatif, le coût d'acquisition d'un drone représente 1 à 2 heures du coût d'opération d'un hélicoptère (sans même prendre en compte l'amortissement de son acquisition).

Nombreux drones ou robots offrent aussi un avantage écologique en fonctionnant avec un moteur électrique. Les émissions de CO_2 d'un hélicoptère de 5 tonnes seront évidemment sans commune mesure avec celles d'un drone de 500 g. Le fait qu'ils puissent s'approcher du danger leur permet également une plus grande précision : l'utilisation du robot pompier Colossus de Shark Robotics sur un incendie permet, par sa précision, d'économiser un important volume d'eau en comparaison d'une intervention classique non robotisée, à efficacité équivalente ou supérieure.

PARTIE II

Les champions français de la robotique et du drone de sécurité

Parmi les champions et pionniers français de la robotique, nous trouvons :

- **PARROT**, numéro deux mondial du drone léger (derrière le n°1 chinois DJI), leader européen du drone aérien

- **SHARK ROBOTICS**, numéro un français de la robotique terrestre, TOP2 européen, TOP10 mondial et numéro un mondial des robots pompiers et batteries résistantes aux très hautes températures (11 heures à 800° - 900° dans le brasier de Notre Dame de Paris).

- **PHOTONIS**, leader européen des systèmes de vision nocturnes et des systèmes de vision multispectrale.

- **HOVERSEEN**, startup leader français du vol autonome de drones aériens légers.

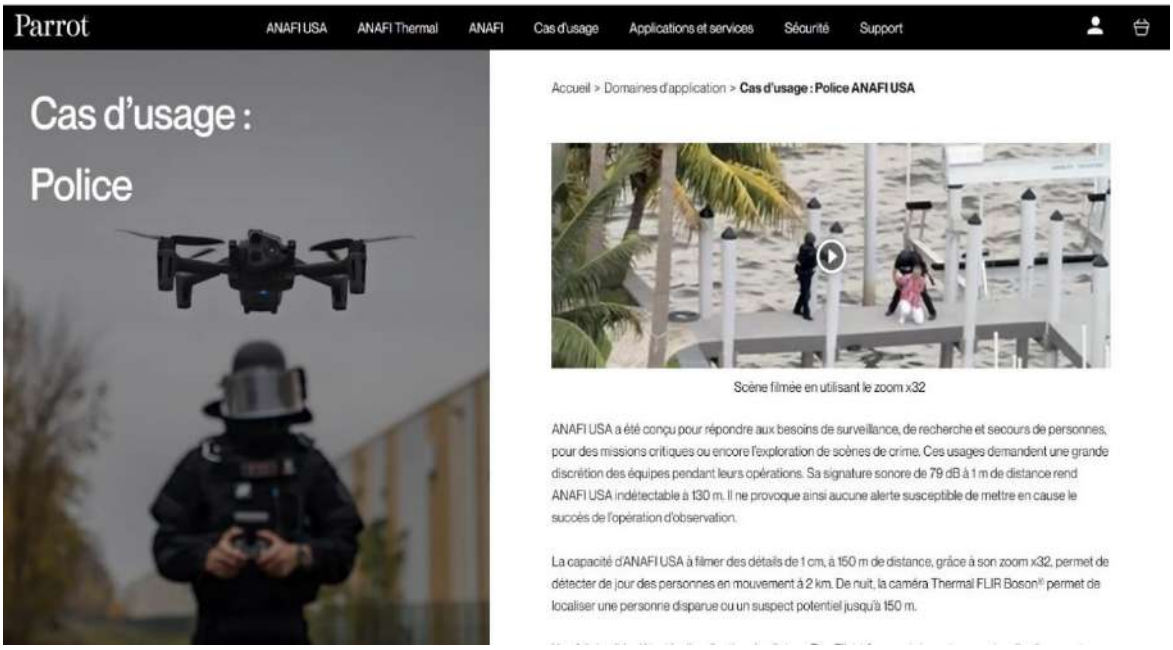
- **OBVIOUS TECHNOLOGIES**, éditeur français de solutions de commandement et de contrôle innovantes pour la sûreté, la sécurité et les opérations critiques.

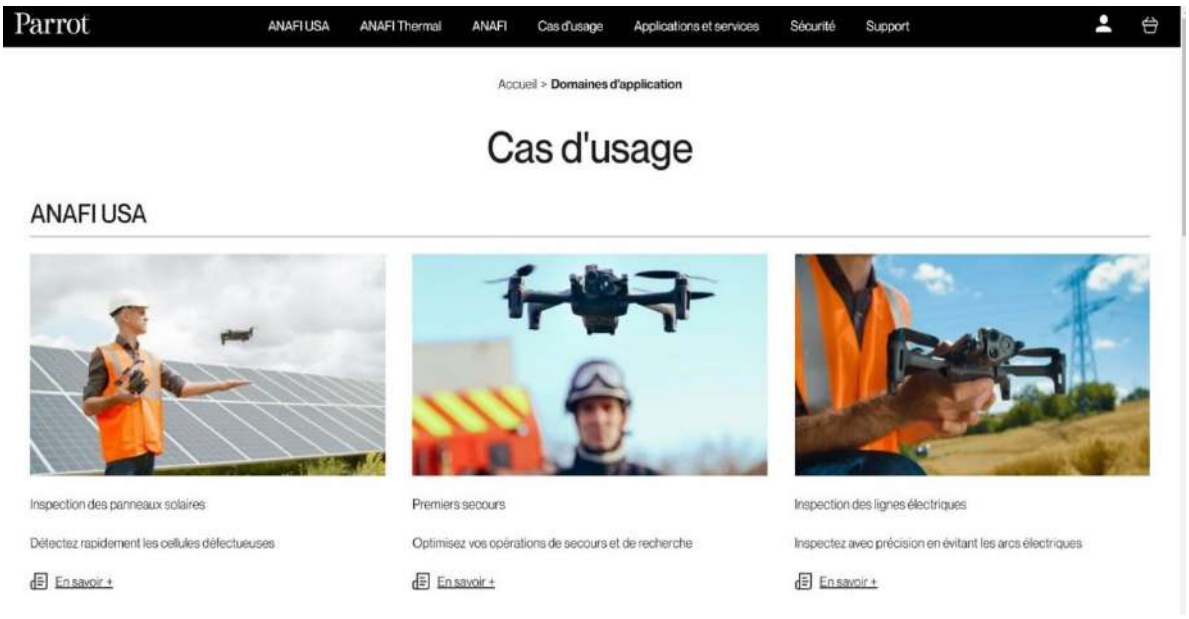
- **ECA Group**, leader français et européen de la robotique marine et sous-marine.

PARROT

Le groupe PARROT est numéro deux mondial du drone léger, leader français et européen du drone aérien. Parrot a été pionnier en inventant les drones récréatifs pour le grand public en 2010. Depuis 3 ans, Parrot a annoncé sa réorientation vers les drones professionnels, dont ceux utilisés pour la défense et la sécurité. Depuis que l'entreprise créée des drones, elle a produit plus de 4,5 millions de drones, capitalisant année après année sur le panels de technologies, le process d'industrialisation et de qualité et l'interfaçage avec les logiciels de traitement des données captées avec des drones.

https://www.parrot.com/fr





Source – PARROT

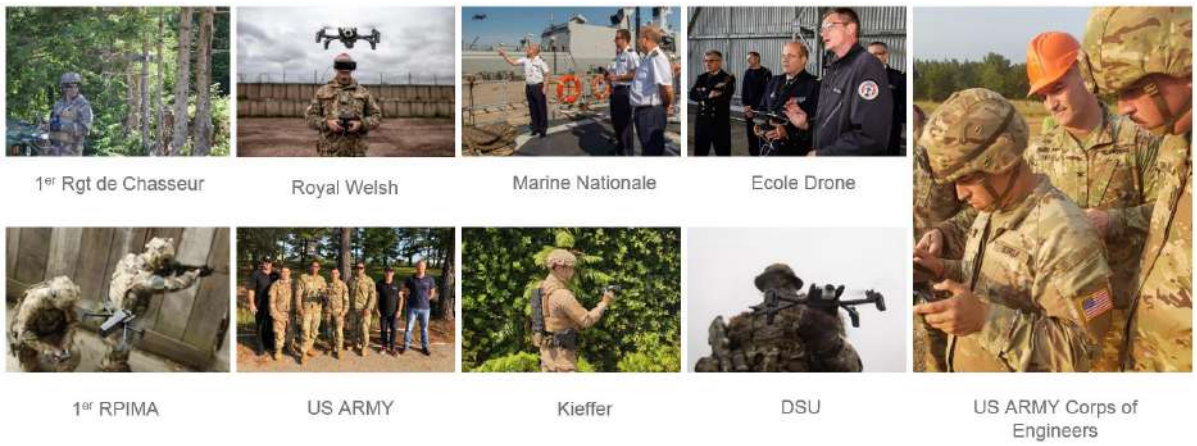
PARROT - ANAFI USA

ANAFI USA est la dernière évolution de Parrot dans le développement et la mise sur le marché de solutions innovantes de drones professionnels. Fort de son expérience de plus de dix ans, Parrot est devenu un nom de confiance dans le domaine des drones, offrant à ses clients des écosystèmes matériels et logiciels inégalés. De plus, sa liste croissante de partenaires industriels innovants et expérimentés continue de renforcer et d'enrichir les offres de sa plateforme.

Source – PARROT

Lorsqu'ils arrivent sur une zone d'intervention, les pompiers ont besoin de voir les zones particulièrement critiques et de se faire une idée précise de la situation globale. Les équipements optiques, gimbal et objectifs de pointe, du drone ANAFI USA ont été conçus dans ce but. Le zoom 32x s'articule autour de deux caméras 21 mégapixels permettant aux opérateurs de voir la scène de manière très détaillée à une distance en vol manuel de 5 km. ANAFI USA peut repérer des détails aussi petits que 1 cm à une distance de 50 m, avec précision.

Source – PARROT



Source – PARROT

ANAFI USA a été conçu pour répondre aux besoins de surveillance, de recherche et secours de personnes, pour des missions critiques ou encore l'exploration de scènes de crime. Ces usages demandent une grande discrétion des équipes pendant leurs opérations. Sa signature sonore

de 79 dB à 1 m de distance rend ANAFI USA indétectable à 130 m. Il ne provoque ainsi aucune alerte susceptible de mettre en cause le succès de l'opération d'observation.
La capacité d'ANAFI USA à filmer des détails de 1 cm, à 150 m de distance, grâce à son zoom x32, permet de détecter de jour des personnes en mouvement à 2 km. De nuit, la caméra Thermal FLIR Boson permet de localiser une personne disparue ou un suspect potentiel à plus de 150 m.

Une fois la cible détectée, l'application de pilotage FreeFlight 6 permet de partager sa localisation exacte avec les équipes d'interventions.

Source – PARROT

ANAFI USA est compatible avec de nombreux outils tiers d'assistance à la décision. Lors d'une mission de recherche de personne disparue ou d'un incendie impliquant la gestion de plusieurs drones, la plateforme de management DroneSense permet d'élaborer, de dimensionner et de gérer une flotte d'ANAFI USA.

Les logiciels Pix4Dcapture et Pix4Dmapper permettent de cartographier rapidement en 3D une scène d'accident pour rouvrir une route en toute sécurité. Pix4Dreact permet de cartographier sans connexion internet une zone de recherche pour détecter, en mode collaboratif, des points d'intérêts où envoyer le drone en reconnaissance.

ANAFI USA pèse 500 g. Sa mise en œuvre prend 55 secondes. Ces atouts le rendent facile à déployer quelle que soit la situation envisagée. Il permet ainsi aux forces de l'ordre de gagner du temps et de l'argent.

Sa liaison Wi-Fi sécurisée et le chiffrement robuste de la carte SD avec l'algorithme AES-XTS associé à une clé de chiffrement 512 bits rendent ANAFI USA utilisable pour les missions les plus confidentielles. Fabriqué aux Etats-Unis, ANAFI USA respecte pleinement les réglementations TAA (Trade Agreement Act) et NDAA (National Defense Authorization Act) et peut être acheté par le biais du Calendrier GSA 2020. Anafi USA a été retenu dans le programme américain de drones de confiance Blue sUAS. Anafi USA est le drone retenu dans le marché cadre du Ministère des Armées pour les 5 prochaines années.

Les points clés de ANAFI USA

- Indétectable à 130 m
- Détecte les personnes en mouvement jusqu'à 2 km de jour et à plus de 150 m de nuit
- IP53 : vol sous la pluie et résistant à la poussière
- Analyse des données post-vol et modélisation de scènes
- Compact et déployable rapidement, en moins de 55 secondes
- Données sécurisées pour les missions confidentielles

ANAFI USA c'est aussi tout un écosystème logiciel

Compatible avec le logiciel de cartographie Pix4Dreact, leader du secteur, le drone ANAFI USA permet aux équipes de secours de convertir rapidement les images obtenues en cartes 2D précises sur leur ordinateur portable.

Avec son kit de développement logiciel SDK open-source et à son utilisation de protocoles standards, ANAFI USA prend en charge un écosystème en plein essor d'applications et de services professionnels, tels que :

Pix4D

Génération de cartes et de modèles 3D précis pour prendre de meilleures décisions.

Survae

Génération de cartes interactives et évolutives grâce à une plateforme d'unification de vidéos, photos et coordonnées satellite.

DroneLogbook

Gestion de flotte et conformité.

Kittyhawk

Conformité et sécurité des flottes de drones, gestion d'espaces aériens

DroneSense

Gestion de projets et de programmes « drones ».

Planck AeroSystems

Atterrissage sur véhicules en mouvement.

Skyward, A Verizon company

Plate-forme de gestion de l'aviation, comprenant l'espace aérien, l'accès LAANC - Low Altitude Authorization & Notification Capability - ainsi que la formation, le matériel et la connectivité pour les déploiements de flottes de drones d'entreprise.

Fusion 4K + Thermal

Pour équilibrer la résolution de l'image thermique et de l'image visible, et ainsi bénéficier d'informations non visibles en thermique, l'image affichée est une fusion des informations des deux caméras. Stabilisé sur trois axes, le bloc optique combine à l'électro-optique un capteur infrarouge, permettant d'identifier les températures entre -10°et +400°.

Comparaison entre la vision RBG et thermale lors de l'inspection d'un volcan

Source – PARROT

Pilotage assisté

A partir de l'application FreeFlight, il est possible de configurer différents modes de pilotage. Il existe ainsi le mode FlightPlan, permettant de définir un plan de vol à partir d'une carte, des points d'intérêt spécifiques et l'orientation de la caméra. L'application calcule automatiquement le temps qui sera nécessaire à la conduite de la mission. Grâce à la capacité de la caméra de s'orienter à 90° vers le haut, il est possible d'inspecter le dessous de structures, et de réaliser des photos panorama 360° de la scène

PARROT et la cybersécurité

La cybersécurité est une priorité absolue pour les drones. Lorsque les drones sont utilisés pour des missions sensibles, les utilisateurs doivent faire confiance à leur drone et s'assurer que leurs données sont entièrement protégées. Les drones sont de plus en plus utilisés par les professionnels de la sécurité publique et de l'inspection, les forces de défense et les entreprises.

Parrot investit fortement pour mettre en œuvre la meilleure cybersécurité et la meilleure protection des données personnelles. La cybersécurité et la protection des données personnelles sont mises en œuvre dès la conception des drones Parrot : des fonctions de sécurité sont définies pour que les données soient protégées et pour que les utilisateurs gardent le contrôle complet de leurs données.

Parrot définit le futur de la sécurité des drones en intégrant les composants de sécurité les plus avancés et notamment des *secure elements* de WISeKey, pionnier de la cybersécurité IoT. Le haut niveau de sécurité est vérifié grâce à des audits internes et externes ainsi qu'un programme de bug bounty en partenariat avec YesWeHack, la première plateforme européenne de bug bounty. Un audit a été mené par Bishop Fox, parmi les meilleurs en sécurité offensive, et le résultat est rendu public par Parrot dans sa page sécurité.

La transparence de Parrot et le haut niveau de sécurité de son drone Anafi USA a permis à ce dernier d'être retenu dans le programme de drones de confiances Blue sUAS du gouvernement américain.

Ce prix CSO50 (50 meilleures stratégies sécurité au niveau mondial) témoigne à nouveau du niveau de confiance des drones que Parrot fournit aux professionnels les plus exigeants du monde. Les lauréats seront présentés lors de la conférence annuelle CSO50 + Awards qui aura lieu du 16 au 18 novembre 2021.

Sources - PARROT

SHARK ROBOTICS

SHARK ROBOTICS est le champion français de la robotique terrestre, Top2 européen, Top10 mondial de robotique terrestre et le leader mondial des robots pompiers.

https://www.shark-robotics.com/

Source – SHARK ROBOTICS

Robot pompier multi-missions

La France, pays précurseur dans l'utilisation des robots pompiers grâce à l'initiative de Shark Robotics de développer un robot pompier grâce à la Brigade des sapeurs-pompiers de Paris

La France est le pays détenant aujourd'hui le plus grand nombre de robots pompiers en Europe, et le deuxième au Monde derrière la Chine. Shark Robotics a le monopole en France sur ce marché, et a notamment équipé les Pompiers de Paris, de Marseille, les Marins Pompiers ou encore les Pompiers de Bordeaux ; l'entreprise a également équipé la Belgique, l'Italie et Israël (!). Cette avance est liée au travail engagé en 2016 par la start-up devenue aujourd'hui PME, avec le développement du premier robot pompier Colossus grâce au retour d'expérience de la Brigade des Sapeurs-Pompiers de Paris, une collaboration « public – privé » en somme. Colossus est un robot 100% made in France, tout comme l'intégralité des robots Shark Robotics : sa conception et sa fabrication sont intégralement réalisées à La Rochelle (France).

Objectif premier : éloigner l'Homme du risque

Visionnaire, leur objectif fixé et atteint était d'éloigner l'Homme du risque en engageant un robot dans les situations les plus périlleuses capable d'accomplir plusieurs missions comme l'inspection, la reconnaissance, l'extinction de feux, mais également de venir en soutien des pompiers avec d'autres modules missions comme le porte brancard ou la panière de transport. Rappelons qu'entre 2009 et 2019, 102 pompiers sont morts en service rien qu'en France**.** Cette collaboration Shark Robotics / BSPP s'est révélée vertueuse, puisqu'elle a permis de développer un robot tenant à la fois compte des besoins opérationnels des pompier, grâce à l'ingénierie en boucle courte, mais également des contraintes de terrain. Pour convaincre les autres unités de pompiers d'acquérir un tel outil de robotique, les employés de Shark Robotics ont dû accomplir un véritable travail d'évangélisation des pompiers pour les convaincre des bénéfices de la robotique.

Aujourd'hui, Shark Robotics a fait le choix de segmenter le marché des robots pompier sn proposant 3 types de robots : le Colossus (robot de 500 kg), le Rhyno Protect (200 kg) et l'Alligator (65kg) afin de correspondre aux différents besoins et budgets des sapeurs-pompiers. Notons que Shark Robotics a développé très rapidement début 2020 un kit de décontamination contre le Covid-19 servant à désinfecter les surfaces ; ce kit constitue aujourd'hui une option utilisée par les différentes unités.

Le robot Colossus (robot de 500 kg)

Source – SHARK ROBOTICS

Le robot Rhyno Protect (200 kg) et l'Alligator (65kg) afin de correspondre aux différents besoins et budgets des sapeurs-pompiers.

Source – SHARK ROBOTICS

Utilisation régulière des robots pompiers par les unités équipées

En matière d'intervention, les robots pompiers sont très régulièrement employés par les unités pour différentes missions : ventilation, extinction de feu, décontamination, inspection, reconnaissance. La Brigade des marins pompiers de Marseille, a indiqué avoir utilisé le robot Colossus plus de 83 fois, et ce, en moins d'un an. La modularité des robots et la facilité d'utilisation sont particulièrement appréciées par les utilisateurs ; de même que le SAV soit situé en France comme l'outil de production de Shark Robotics, permettant une grande réactivité en cas de besoin. L'outil robotique est devenu un indispensable pour les unités pompiers de telle sorte qu'elles avouent en manquer lorsque les robots sont immobilisés pour de la maintenance.

Les robots sont utilisés aussi bien pour des feux de grande ampleur, des feux logistiques, des feux agricoles, que des feux de parking comme celui de Choisy Le Roi en janvier 2018 qui a mobilisés 180 sapeurs-pompiers dans un parking de 2000m2. Autre exemple, sans aucun doute, le plus connu de tous : l'incendie de Notre-Dame de Paris : le robot Colossus a été déployé à un moment où la situation devenait extrêmement dangereuse pour l'Homme : du plomb fondait, la température dépassait les 800 degrés, le toit de la nef menaçait de s'effondrer, ; il ne faisait alors nul doute que l'usage du robot devenait nécessaire. Cet événement a d'ailleurs fait connaitre les robots pompiers Shark Robotics à travers le monde, de sorte que l'entreprise a remporté en 2020 le prix de la technologie d'innovation par la

société américaine des ingénieurs en mécanique (ASME). Depuis cet événement les Pompiers de paris ont acquis 4 nouveaux robots Shark Robotics.

Source – SHARK ROBOTICS

Le retour d'expérience des sapeurs-pompiers : des bénéfices multiples au-delà d'éloigner l'Homme du risque

Après 5 ans d'utilisation, les retours d'expérience des sapeur- pompiers ont montré que la robotique présentait d'autres atout au-delà d'éloigner l'Homme du risque. La robotique permet aux sapeurs-pompiers d'effectuer leurs missions de manière plus efficaces :

Gagner en efficacité et solutionner la problématique de disponibilités des personnels et des matériels

L'extinction d'un incendie usuel (de hangar, garage, entrepôt) peut se diviser en deux phases : l'attaque, et le retour à la normale, plus long, durant lequel sont notamment éteints les feux résiduels. L'engagement d'un robot pompier s'inscrit dans la continuité de la règle d'Engagement Minimum qui limite le nombre de victimes en cas d'accidents. Dès l'attaque du feu, l'engagement d'un robot pompier permet un gain d'efficacité dans l'extinction d'incendie en zone d'exclusion, dans lesquelles l'engagement présente un risque. En effet, il permet de détecter les sources de l'incendie et de les attaquer directement, avec précision, aux endroits appropriés inaccessibles aux personnels humains. Sans cela, l'attaque ne peut pas se faire au plus près des flammes et nécessitera donc plus de temps, de personnels et d'équipements. Le robot permet de soulager un binôme de reconnaissance ou de l'établissement d'une lance. Durant la phase de retour à la normale, pour les zones d'exclusion, le robot permet de détecter les feux résiduels grâce à ses caméras thermiques, et de s'y engager sans exposer le personnel aux risques. Des moyens matériels, capacitaires et humains peuvent alors être désengagés de l'intervention plus tôt que si le robot n'avait pas

été engagé. Par exemple, un moyen élévateur aérien pourra se désengager en phase de retour à la normale quand l'incendie aura été maîtrisé.

Protéger l'environnement en diminuant la consommation d'eau et en limitant drastiquement la pollution des sols

Parallèlement à cette règle d'engagement minimum, la protection de l'environnement est actuellement intégrée comme une mission à part entière des sapeurs-pompiers en France, et protéger la nature des produits toxiques lors des interventions fait partie de leur quotidien.

Sur un incendie, lors de la phase de retour à la normale, la localisation des feux résiduels peut s'avérer difficile à appréhender pour les pompiers, en particulier lorsque pénétrer à l'intérieur d'un bâti est impossible à cause de risques d'effondrements. D'importantes quantités d'eau sont alors employées dans le but de maîtriser le feu à distance, et ces eaux se chargent rapidement en éléments issus de la décomposition et de la dégradation des produits et composés industriels ou agricoles (contenus dans le hangar ou l'entrepôt). Un risque majeur est alors qu'elles se déversent dans les cours d'eau voisins et entraînent des dégâts environnementaux irréversibles (à l'image de l'incendie de l'entrepôt de de la SANE, à Nancy en 1996, responsable de la mort d'une tonne et demie de poisson sur 1,5km). Outre une pollution des rivières, ces eaux d'extinction polluées sont susceptibles de s'infiltrer et de contaminer les sols, et éventuellement des aquifères d'eau potable situés à proximité. De telles atteintes à l'environnement ne peuvent être éliminées qu'à grands frais.

Un robot permet des interventions précises et concentrées sur les feux résiduels. Cela entraîne des impacts positifs remarquables pour l'environnement, en effet, la diminution de la quantité d'eau utilisée est considérable : des milliers de litres peuvent être économisés grâce à cette solution. Par conséquent, la quantité d'eau polluée par les produits est également notablement réduite, limitant ainsi les risques d'intoxication des espèces et l'atteinte des eaux souterraines. L'avantage est donc incontestable sur l'aspect environnemental mais également sur l'aspect financier car l'intervention ciblée du robot permet de réduire considérablement les coûts des dommages causés par un incendie, les dégâts étant à la charge de celui qui les a occasionnés.

Réduire les litiges juridiques impliquant les sapeurs-pompiers

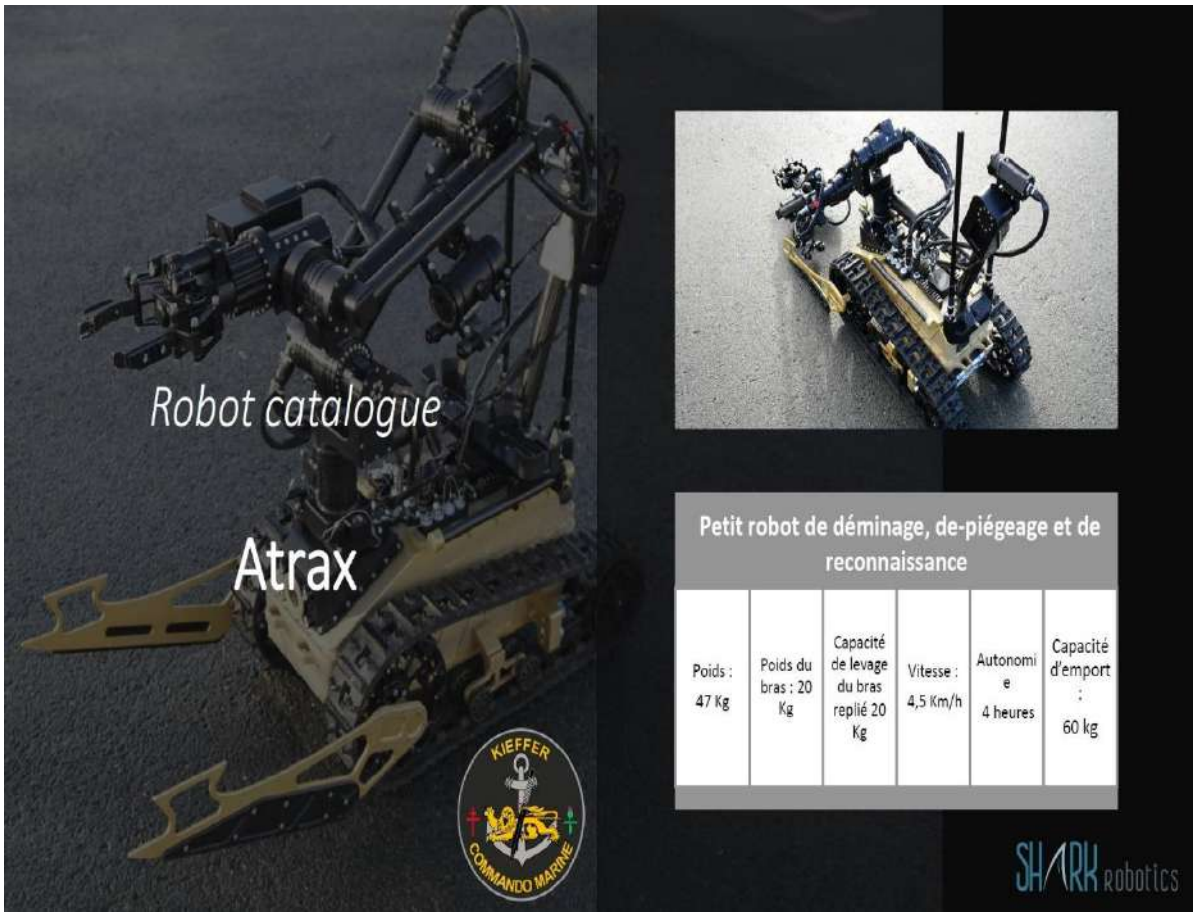
Les recours des sociétés d'assurances, de plus en plus fréquents, font peser des contraintes supplémentaires sur les épaules des pompiers sur le terrain et les activités des sapeurs-pompiers se judiciarisent. Les SDIS peuvent notamment être accusés d'infractions non intentionnelles de dommages à l'environnement. Un ensemble de textes et de jurisprudences rendent l'engagement de la responsabilité administrative des SDIS plus aisé, et les assurés n'hésitent pas à chercher réparation. Dans ce contexte, un robot permet de sécuriser la portée juridique d'un engagement et de limiter par cette occasion tout litige.

D'une part, l'économie d'eau, en plus de représenter une économie financière pour les collectivités et les contribuables (le mètre cube coûtant environ 4 euros, à comparer avec le débit d'une bouche d'incendie de 60 mètres cubes par heure), permet de limiter l'ampleur

des dégâts des eaux inhérents à l'extinction, ainsi que les dégâts environnementaux issus liés aux eaux d'extinction. D'autre part, la capacité d'enregistrement vidéo du robot permet de rendre compte de la réalité de l'intervention et des origines des dégâts. Des preuves supplémentaires du déroulement des opérations peuvent appuyer la véracité des informations reportées, et par exemple limiter les contentieux juridiques entre pompiers et assurances.

Robot démineur ATRAX

Suivant la même logique de cette collaboration public / privé initié avec le robot Colossus, Shark Robotics a développé un robot de déminage, de dépiégeage et de reconnaissance, l'ATRAX pour et grâce au retour d'expérience du Commando Kieffer (Marine nationale). Des flippers anti-guirlandes IED ont ainsi pu être spécifiquement développés grâce à cet échange direct avec le Commando. Créé sur-mesure en adéquation avec les besoins opérationnels des démineurs, l'ATRAX a été déployé de nombreuses fois en opérations extérieures pour épauler les commandos dans leurs missions.



Source – SHARK ROBOTICS

Herse robotisée BULKHEAD

De même, Shark Robotics a mis au point une herse robotisée, BULKHEAD, grâce au retour d'expérience de la DNRED, qui permet de protéger les personnels utilisateurs. Chaque année, le service des douanes enregistre des morts de douaniers liés à l'exercice de leur fonction (Go fast…). Et les dispositifs de herses manuelle classiques mettent en danger la vie des agents car ces derniers sont obligés d'aller au contact du véhicule pour déployer le système de herse. Le fuyard est alors tenté d'éviter la herse en fonçant sur le douanier. Pour pallier ce problème, Shark Robotics a codéveloppé en 2017 avec la Direction des Opérations Douanières la herse BULKHEAD. Avec son système et ses pointes brevetés, cette herse est capable de crever les pneus d'un véhicule en 2 secondes, et ce, à distance. Elle constitue l'outil idéal pour créer un dispositif sécuritaire rapide et efficace préservant la vie des agents qui l'utilisent.

Source – SHARK ROBOTICS

Cette herse robotisée est un exemple emblématique de ce que peut apporter la technologie aux forces de sécurité. Il permet de traiter les GoFast sur les routes françaises sans mettre en danger le policier qui l'utilise.

Robot Porte Cible motorisé pour les séances de tir

Source – SHARK ROBOTICS

Robot mule BARAKUDA pour le soutien et l'évacuation des blessés

Source – SHARK ROBOTICS

XTREM, des batteries électriques ultra résistantes aux chocs thermiques, mécaniques, électriques et emballements chimiques.

Source – SHARK ROBOTICS

PHOTONIS

PHOTONIS est le leader européen des équipements de vision nocturne. ETI de haute technologie, reconnue mondialement comme un innovateur majeur en optronique, avec plus de 80 ans d'expérience dans l'innovation, le développement, la fabrication et la vente de technologies dans le domaine de la photo détection et de l'imagerie.
Forte d'un chiffre d'affaire d'environ 150M€, de 1000 employés et d'une présence mondiale, PHOTONIS participe à l'export français, représentant ainsi 15% de l'export français total en optronique.

Ses unités de production sont installées à Brive.

https://www.photonis.com/solutions/law-enforcement

Figure 1 : Illustrations des technologies PHOTONIS
(de g. à d. : vision nocturne, caméras nocturnes, caméras thermiques)

Les composants développés par PHOTONIS se retrouvent dans des applications critiques dans les domaines tels que la défense, la surveillance, la sécurité, le médical, la détection et l'imagerie scientifique, la sûreté nucléaire, l'exploration spatiale, le contrôle industriel, etc.
Les composants de PHOTONIS sont par exemple présents dans le laser mégajoule (caméra ultra-rapide de l'expérience), sur Hubble (optique à rayons X), au CERN et au CEA…

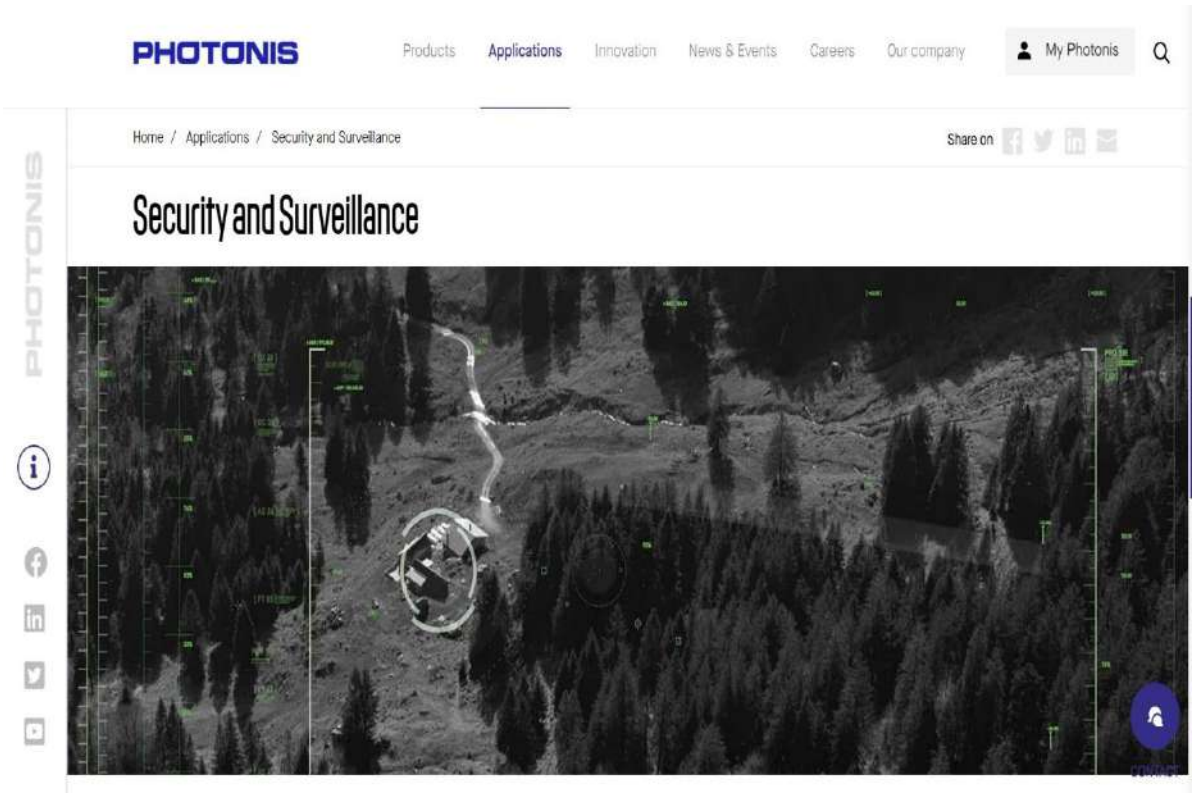
Figure 2 : Caméras PHOTONIS
(de g. à d. : caméra de vision nocturne, caméras infrarouge / thermique)

Leader mondial dans le domaine des tubes à intensification de lumière, PHOTONIS participe à équiper nos forces et celles de nos alliés afin de répondre aux mieux à leurs besoins en vision nocturne. PHOTONIS propose également des modules caméras bas niveau de lumière et infrarouge qui sont par exemple intégrés dans de récents programmes de défense comme celui des lunettes de tir FPSA (Fusil de précision pour semi-automatique) utilisant à la fois la technologie bas niveau de lumière et la technologie infrarouge de PHOTONIS, le programme de véhicule SCORPION où la caméra PHOTONIS est « l'œil » du véhicule Jaguar, mais aussi dernièrement une jumelle numérique à fusion d'images, la TacFusion.

La TacFusion est une jumelle d'observation multi-spectrale de moins de 1Kg, équipée des technologies PHOTONIS en bas niveau de lumière et infrarouge. Elle a été conçue afin de

permettre aux opérateurs d'assurer au mieux leurs missions de recherche, de sauvetage ou de surveillance. Sa connectivité permet le déport sans fil de son flux vidéo ainsi que l'enregistrement et l'horodatage de films et photos. Elle est actuellement en test dans les forces de police et gendarmerie françaises.

Figure 3 : Caméras multi-spectrales PHOTONIS
(de g. à d. : Module caméra multi-spectrale, jumelle TacFusion incorporant les technologies PHOTONIS, image multi-spectrale TacFusion)

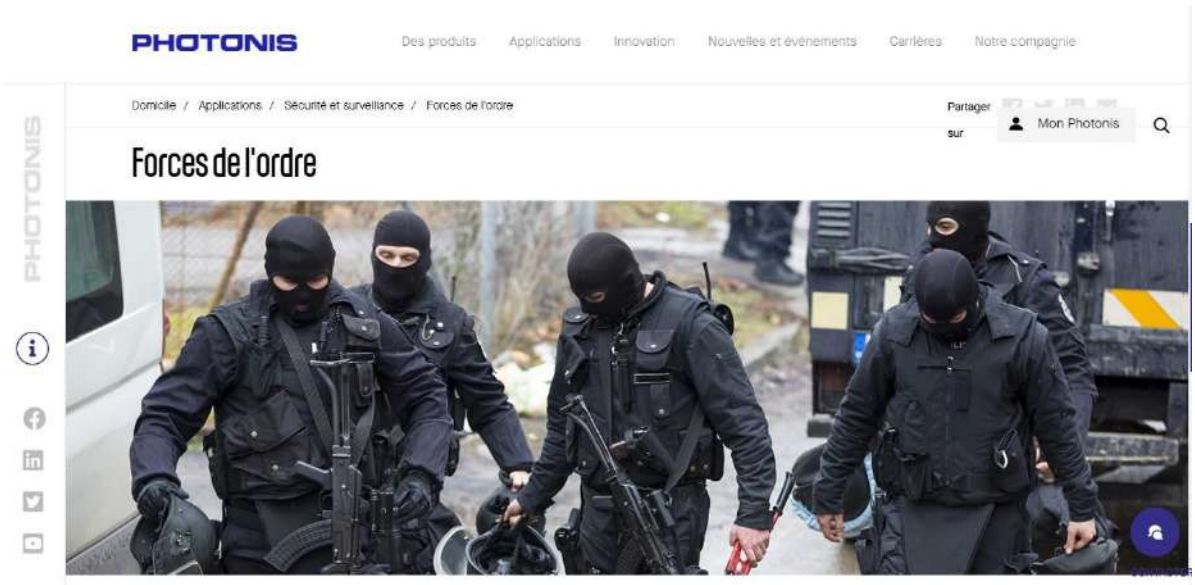


Source - PHOTONIS

En tant que leader des technologies de capteurs de vision nocturne, Photonis est bien placé pour étendre la détection dans le domaine de la sécurité intérieure. Les capteurs peuvent détecter la présence de produits chimiques, de radiations ou de menaces de gaz spécifiques, effectuer une cartographie d'images et même aider aux enquêtes médico-légales.

Alors que les tensions mondiales augmentent, la nécessité d'une surveillance 24h/24 et 7j/7 pour protéger les actifs mobiles et fixes doit être fiable dans un large éventail de conditions environnementales et opérationnelles. Les caméras choisies dans le cadre d'un réseau de surveillance étendu doivent avoir la capacité de fournir une imagerie de haute qualité dans une large gamme de conditions d'éclairage. Les caméras CMOS à faible luminosité de Photonis

peuvent fournir une imagerie de jour comme de nuit pour les applications statiques et mobiles.



Source - PHOTONIS

Afin de répondre aux problèmes techniques qui affectent l'observation à longue distance dans des conditions de faible luminosité, Photonis a développé une famille de caméras à ultra faible luminosité, utilisant les technologies EBCMOS (Electron Bombarded CMOS) ou ICMOS (Intensified CMOS). Ces caméras offrent une fréquence d'images rapide, une résolution supérieure et une sensibilité accrue, ce qui les rend bien adaptées aux observations à longue distance dans des conditions sombres (même d'objets en mouvement rapide) sans avoir besoin d'un éclairage ou d'un refroidissement supplémentaire. L'architecture numérique empêche également les dommages causés par des événements lumineux soudains et des halos, ce qui lui permet de fonctionner aussi bien en plein jour que dans des situations de faible luminosité.

Les tubes intensificateurs d'image Photonis sont utilisés pour un certain nombre de systèmes de détection de faible luminosité et de surveillance, y compris la vision nocturne. La grande variété d'écrans au phosphore et d'options de photocathode permet une personnalisation en fonction de différentes applications telles que le dépistage chimique portable, le LIDAR/LADAR, le contrôle du périmètre ou même la détection de décharge corona UV.

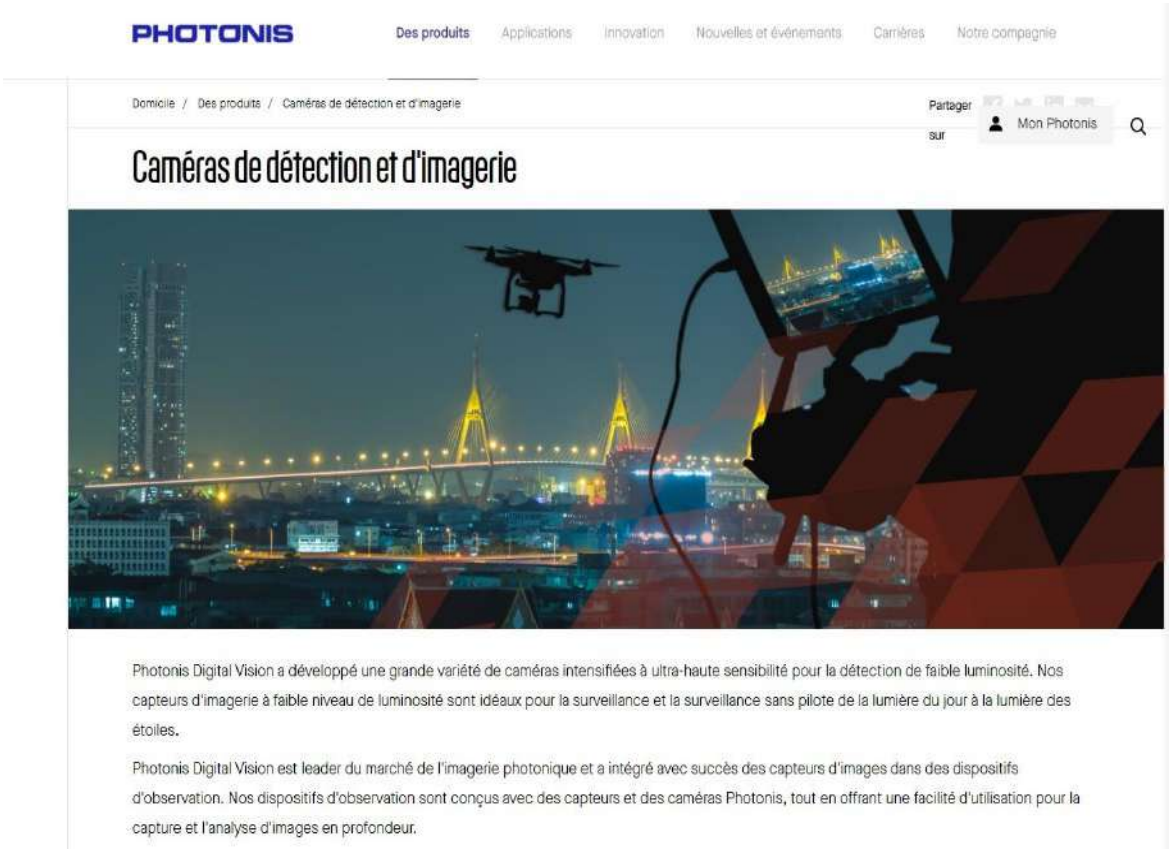
- Lunette de poche Jour & Nuit
- Caméra de tableau de bord
- Capteurs sans surveillance
- Caméra d'enregistrement d'épreuves jour et nuit
- Identification de la personne cible jour et nuit

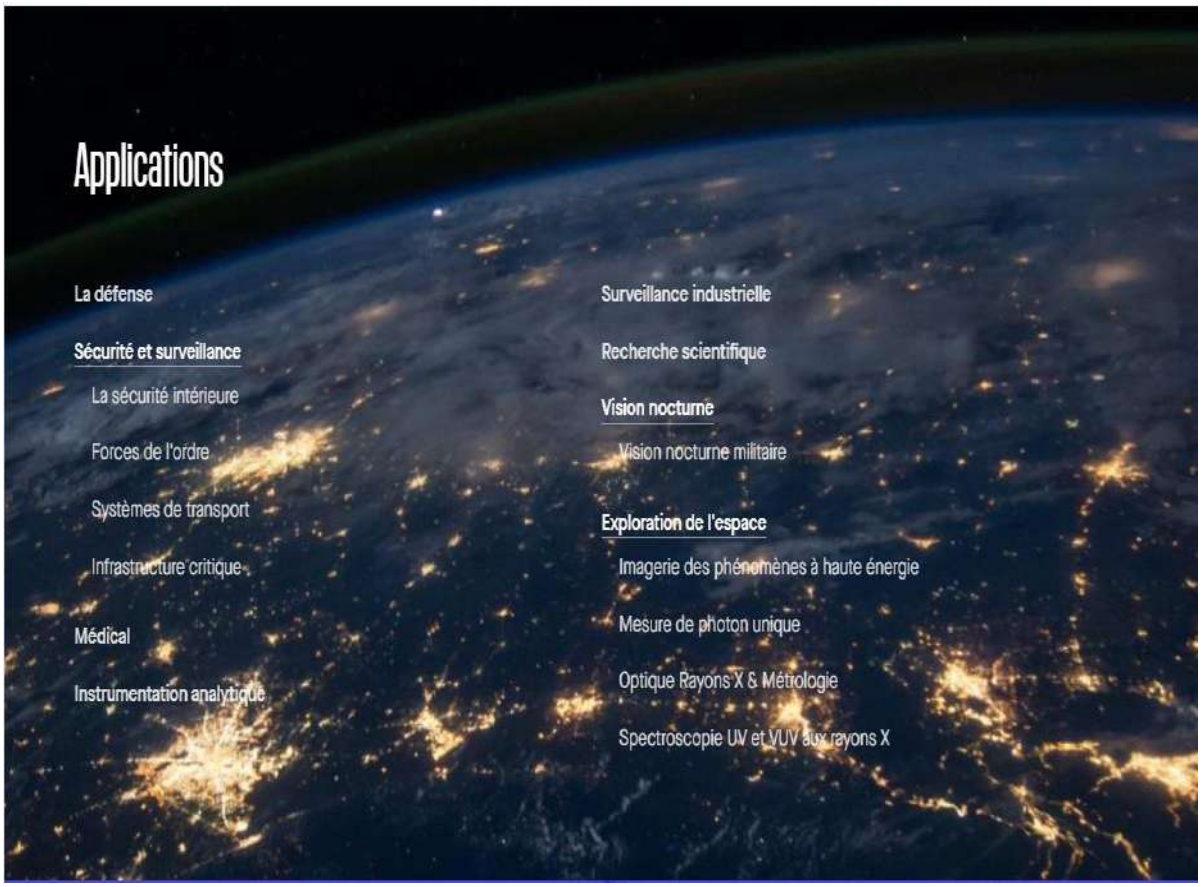
Photonis Digital Vision a développé une grande variété de caméras intensifiées à ultra-haute sensibilité pour la détection de faible luminosité. Nos capteurs d'imagerie à faible niveau de luminosité sont idéaux pour la surveillance et la surveillance sans pilote de la lumière du jour à la lumière des étoiles.

Photonis Digital Vision est leader du marché de l'imagerie photonique et a intégré avec succès des capteurs d'images dans des dispositifs d'observation. Nos dispositifs d'observation sont conçus avec des capteurs et des caméras Photonis, tout en offrant une facilité d'utilisation pour la capture et l'analyse d'images en profondeur.

Source – PHOTONIS

PHOTONIS souhaite poursuivre l'intégration de ses caméras dans les plateformes dédiées à la défense et à la sécurité, et ainsi fournir aux opérateurs français l'avantage de ses dernières technologies de capteurs. L'un des secteurs les plus porteurs et exigeants est sans aucun doute celui des charges utiles optroniques pour drones. Dans ce domaine, grâce au partenariat avec des sociétés françaises leader du domaine comme PARROT, PHOTONIS peut fournir des alternatives plus performantes, plus sûres et sans contraintes d'export aux technologies américaines (FLIR) ou chinoises (DJI) déjà présentes sur le marché. Bien que les solutions PHOTONIS soient déjà relativement compactes, l'emport sur drones nécessite néanmoins un effort de R&D supplémentaire dans le sens d'une réduction des volumes et poids des solutions actuelles. En particulier, PHOTONIS pourra ainsi fournir des caméras thermiques et nocturnes ultra-compactes, mais aussi des caméras multi-spectrales (fusion d'images associant un capteur jour/nuit à une caméra thermique).





Source – PHOTONIS

HOVERSEEN

HOVERSEEN s'est spécialisée dans les drones aériens légers en vol automatique de surveillance et d'inspection (sans pilote opérateur).

https://www.hoverseen.com/fr/

Source - HOVERSEEN

Des drones-caméras automatiques

Ils réalisent des missions automatiques sans télépilote en suivant des plans de vol intégrés. Ils diffusent des flux vidéo HD en temps réel sur les écrans de contrôle. Le téléchargement en 4K est disponible a posteriori. En fin de mission les drones retournent dans leur base où ils se rechargent sans intervention humaine.

Les composants du système

- Un drone léger de 395g avec un capteur 4K et un capteur thermique.

- Une base de contrôle et de rechargement du drone. Elle pèse 50kg, elle ne comporte qu'une seule pièce mécanique et peut être installée sur un toit.

- Un ensemble logiciel qui permet l'intégration en standard aux solutions de vidéosurveillance (ONVIF, RTSP, H.264, PTZ), comme à d'autres solutions métiers utilisant la vidéo.

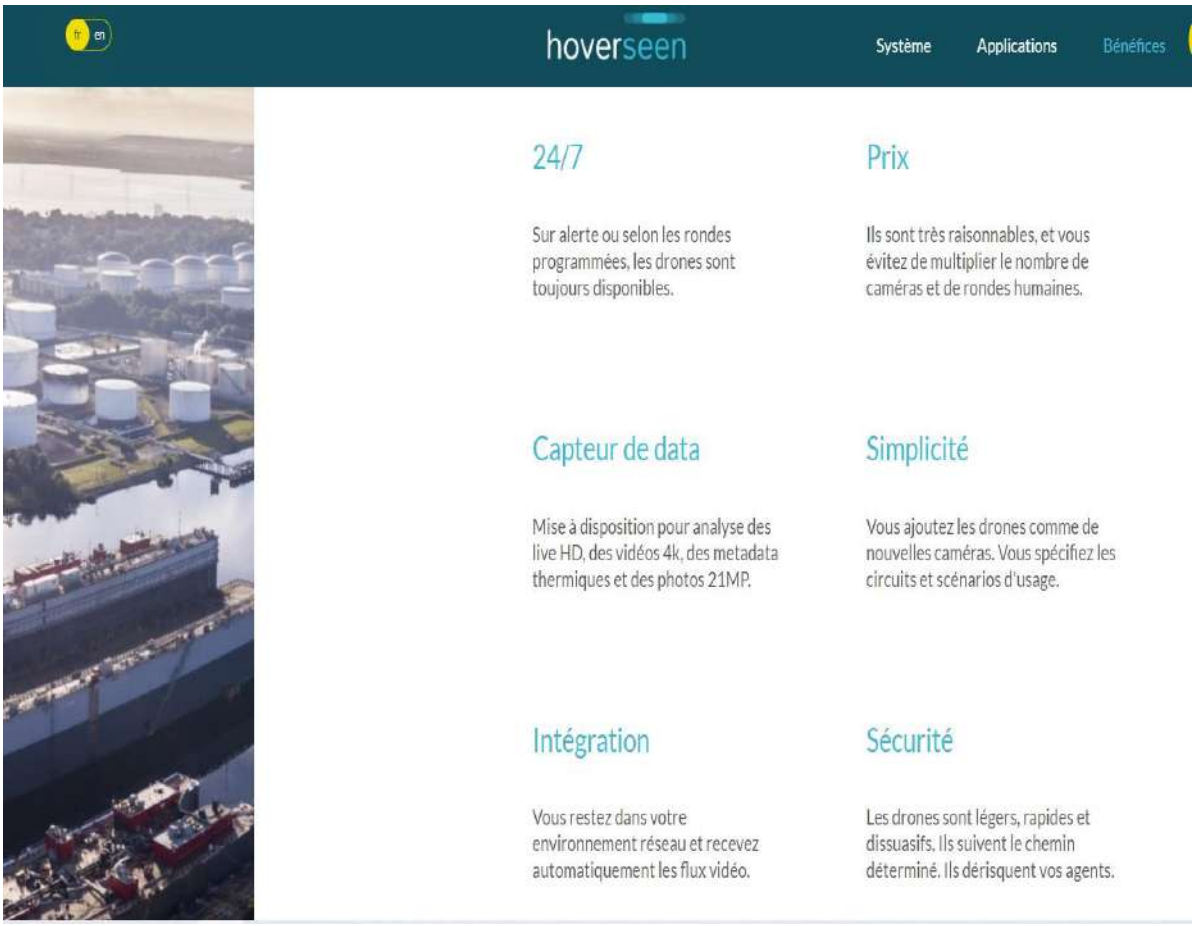
Simplicité et sécurité

Le drone-camera permet de couvrir les angles morts et les zones inaccessibles. Il est rapide, il diminue les risques pour les agents, il limite leurs déplacements.

La légèreté du drone réduit les risques air-sol et air-air, et permet des vols en milieu périurbain.

Les plans de vol sont validés par des télépilotes professionnels et sécurisés dans le système. Les opérateurs de vidéosurveillance sont formés au système.

Source - HOVERSEEN



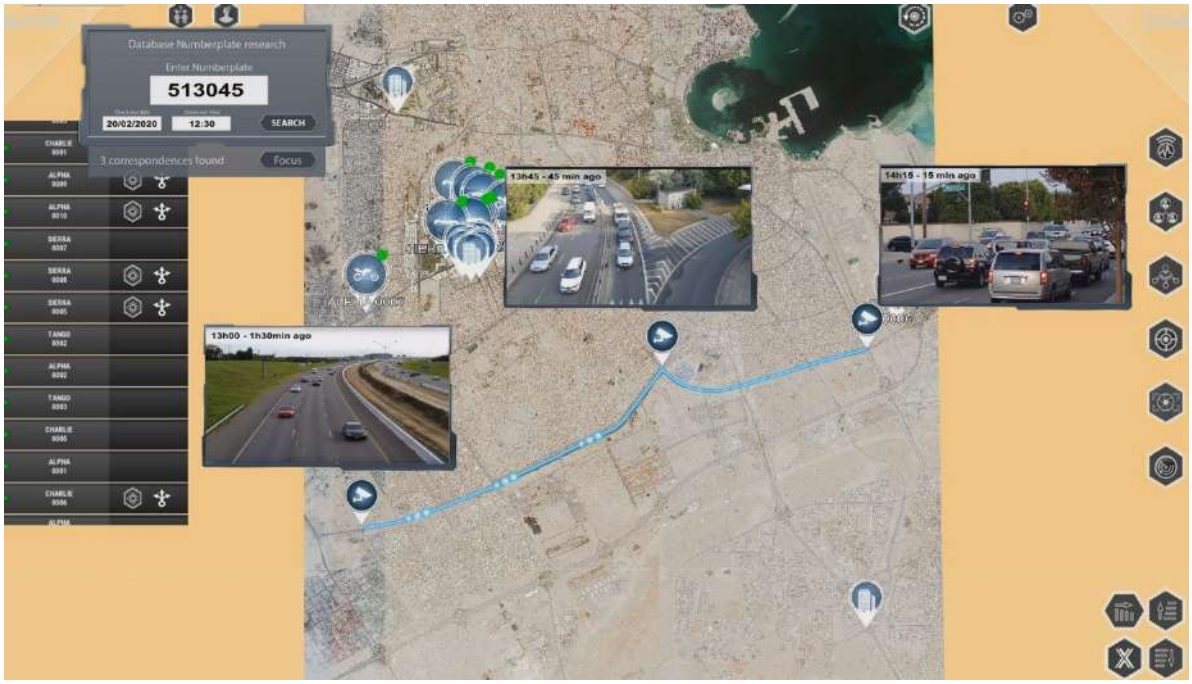
Source - HOVERSEEN

OBVIOUS TECHNOLOGIES

OBVIOUS TECHNOLOGIES est un éditeur français de solutions de commandement et de contrôle innovantes pour la sûreté, la sécurité et les opérations critiques.

https://obvious.tech/

LA SUITE LOGICIELLE OODA



Source – OBVIOUS TECHNOLOGIES

OODA est une suite logicielle complète offrant une plate-forme de commandement et de contrôle où les intervenants de chaque mission peuvent accéder aux informations dont ils ont besoin, de la manière la plus appropriée compte tenu de leur rôle, de leur localisation et de leur situation opérationnelle.

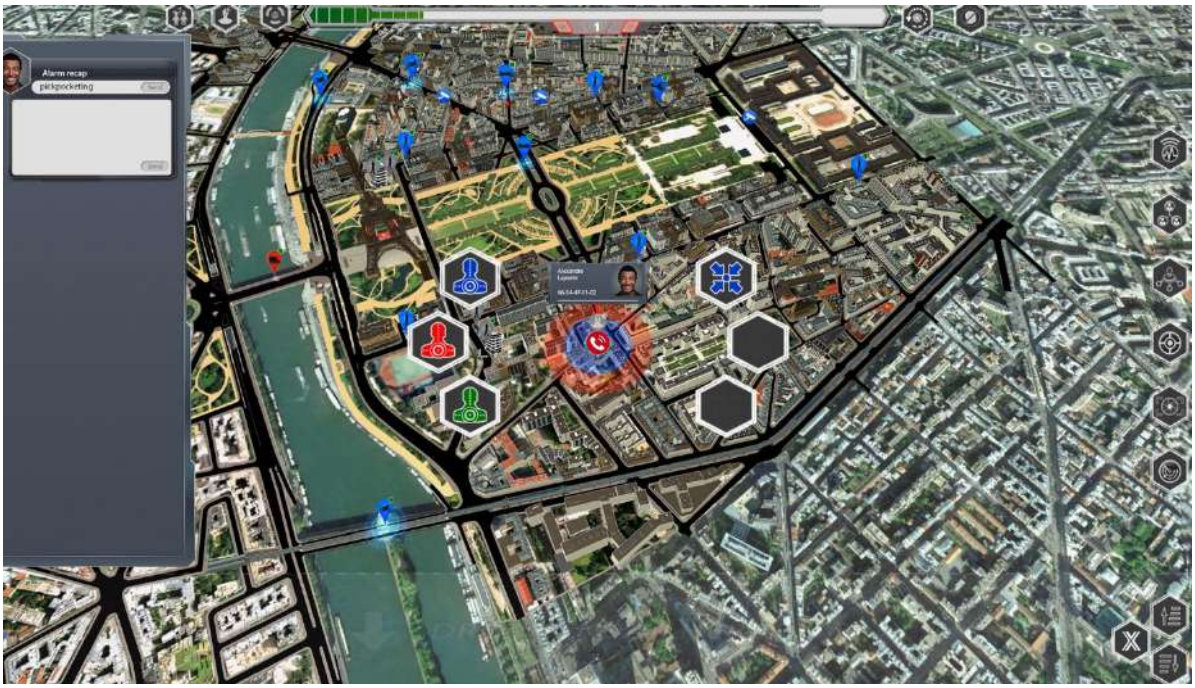
OODA PSIM et OODA C2, pour tous les postes des opérateurs de la salle de contrôle, configurés selon les privilèges attribués aux utilisateurs (y compris la gestion des alarmes, la surveillance vidéo, la connaissance de la situation 3D et une gestion des rapports)

OODA Tactical Command, pour les centres de commandement délocalisés et mobiles qui ont besoin de commander, à proximité du terrain, un événement spécial ou une zone d'intérêt, avec un groupe d'agents

OODA Mobile, pour les agents de terrain qui ont besoin de recevoir des informations claires sur les incidents en cours, tout en communiquant en permanence en temps réel avec la salle de contrôle

OODA Crisis, utilisé par les décideurs ayant des besoins particuliers ou lors de situations stratégiques, et pouvant être utilisé depuis une table à écran tactile

OODA Wall, permettant aux superviseurs de murs vidéo de contrôler et de réorganiser rapidement, les informations affichées sur le mur vidéo, directement depuis l'interface OODA.

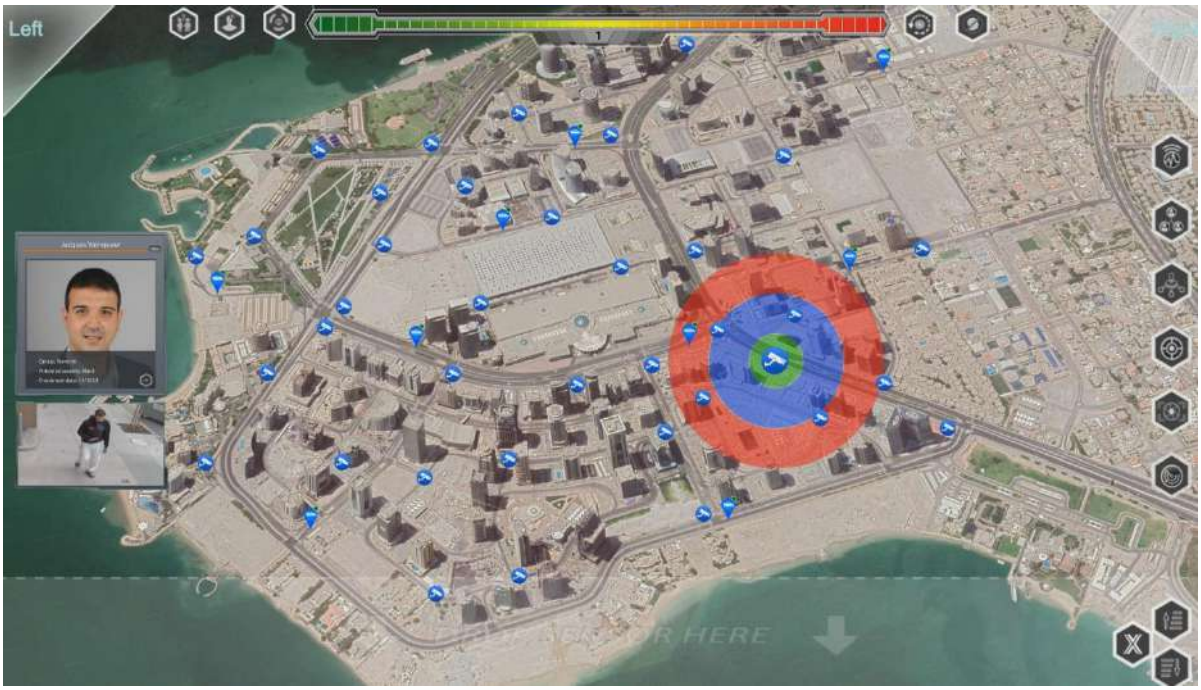


Source – OBVIOUS TECHNOLOGIES

Source – OBVIOUS TECHNOLOGIES

Source – OBVIOUS TECHNOLOGIES

Source – OBVIOUS TECHNOLOGIES



Source – OBVIOUS TECHNOLOGIES

ECA GROUP

ECA Group est le leader des solutions de navire de surface sans équipage (USV) et drones d'inspection sous-marine.

https://www.ecagroup.com/en/find-your-eca-solutions#defence-security

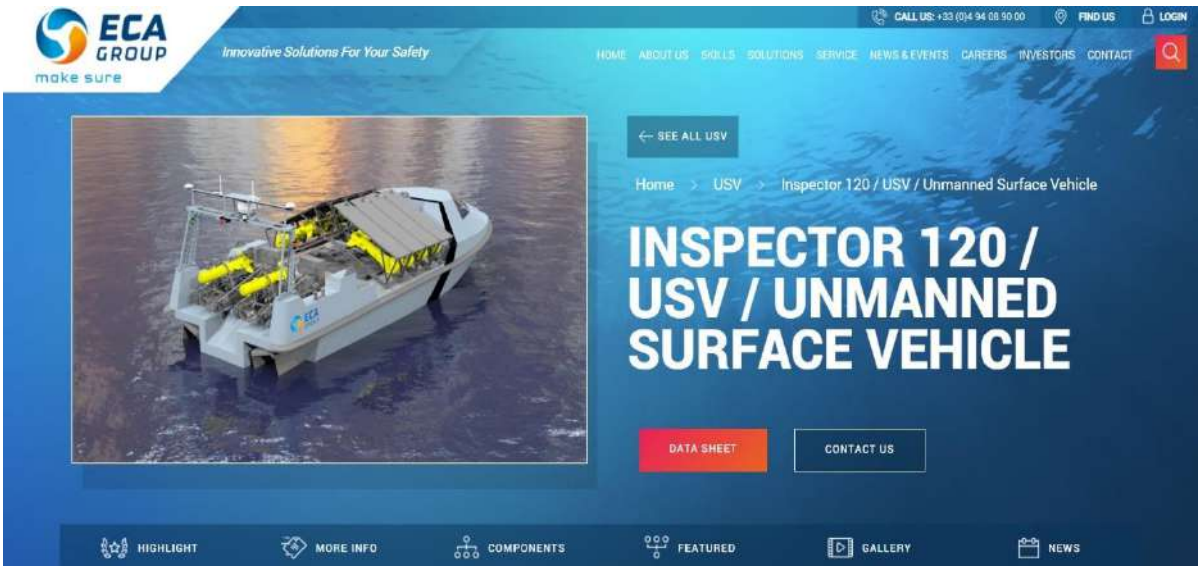
Depuis plus de 80 ans, ECA Group a développé ses compétences dans plusieurs domaines robotique, systèmes automatisés, simulation et procédés industriels. Ses innovations technologiques et ses solutions développées sont valorisées par des clients du monde entier et pour différentes applications dans les secteurs de la défense, du maritime, de l'aérospatial, de la simulation, des équipements industriels et de l'énergie. ECA Group reprend ses compétences dans 3 grandes catégories : la robotique et les systèmes intégrés, l'aérospatiale et la formation par simulation.

Source – ECA GROUP

Robotique et systèmes intégrés

Acteur majeur de la détection et de la destruction des mines dans le secteur de la Défense, ECA Group équipe avec ses solutions robotiques neuf des 10 plus grandes armées du monde.

Le Groupe ECA combine son expertise dans la conception de drones opérant sur l'eau - USV, sous l'eau - AUV, ROV , sur terre - UGV et dans l'air, et dans le développement de systèmes intégrés, afin de développer une gamme complète de solutions adaptées aux besoins du secteur de la défense, du maritime, du nucléaire, des plates-formes pétrolières et de l'industrie. Par ailleurs, le Groupe ECA développe un programme de recherche sur les « systèmes robotiques » du futur.



Source – ECA GROUP

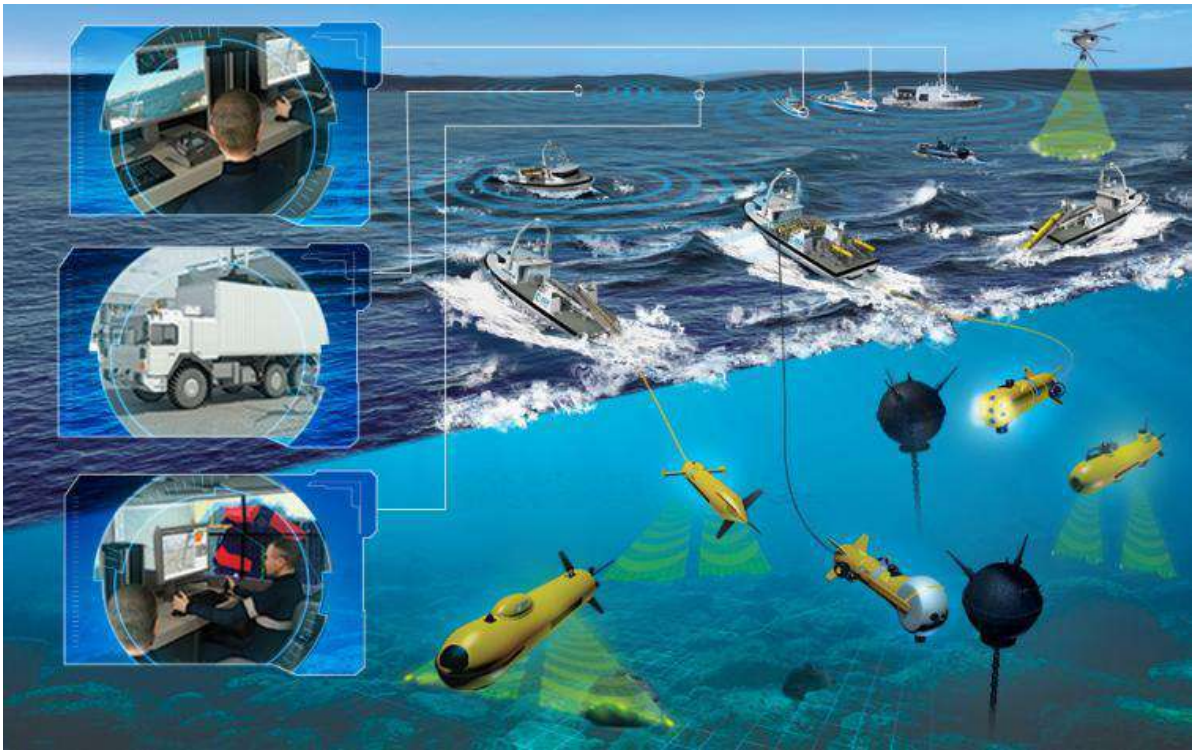
Robotique maritime

Le Groupe ECA conçoit des solutions d'automatismes qui assurent une très large gamme de missions pour les activités maritimes telles que les plates-formes pétrolières offshore, les opérations sous-marines ou l'hydrographie & océanographie.

Ces solutions robotiques sont utilisées dans le monde entier et remplissent leurs missions pour l'exploration sous-marine, l'inspection de pipelines, les opérations sur chantiers immergés, la recherche minière, les systèmes de contrôle et de commande, la vidéosurveillance, etc. Solutions robotiques basées sur des véhicules sous-marins autonomes (AUV) et à distance. des véhicules sous-marins opérés (ROV) équipés de caméras et de bras articulés réalisent des missions d'intervention ou d'inspection adaptées à la grande variété des besoins de nos différents clients.

Ils permettent à nos clients de bénéficier de l'expertise du Groupe dans l'acquisition et le traitement des données sonar.

ECA Group propose également une gamme de solutions basées sur simulateur pour la formation du personnel à la conduite de divers véhicules et pour d'autres activités qui se déroulent à bord des navires.



Source – ECA GROUP

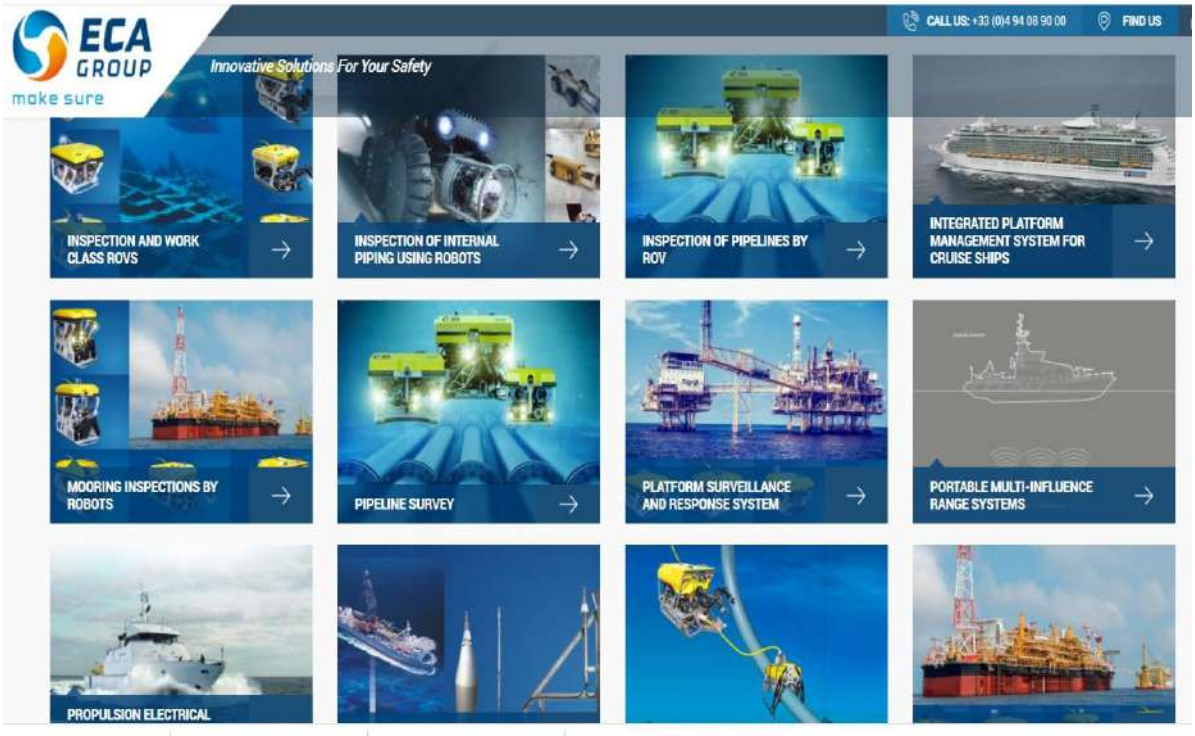
L'offre de navires de surface robotisés permet de mettre en place un contrôle des côtes et frontières maritimes H24-365 à cout réduit, avec un large spectre de clients et clients potentiels : Marine Nationale, SNSM secours en mer, Douanes, sécurité civile, ….

Energie et équipements industriels

ECA Group propose des solutions clé en main innovantes et performantes basées sur la robotique à ses clients du secteur Industrie & Energie. Ses robots robustes et fiables dédiés aux missions d'inspection, d'intervention et de maintenance sont particulièrement adaptés aux environnements difficiles et exigeants tels que le nucléaire, l'énergie, les infrastructures, l'aéronautique, l'automobile, etc. Ces solutions globales sont utilisées dans les industries pour approcher au plus près des sources de danger : drones terrestres équipés de caméras ou de bras articulés, systèmes de contrôle vidéo très résistants aux radiations, etc.

S'appuyant sur sa gamme de robots aériens, terrestres et sous-marins équipés des capteurs les plus sophistiqués et adaptés à chaque besoin spécifique, ECA Group a développé des solutions fiables et de haute qualité pour la surveillance et l'inspection des infrastructures et des sites industriels : barrages, ponts, raffineries, centrales nucléaires, parcs éoliens, etc. Par sa connaissance des procédés industriels et des automatismes, ECA Group est en mesure de

proposer à ses clients des solutions clés en main innovantes et performantes : démantèlement de centrales nucléaires, conception de lignes d'assemblage flexibles pour les clients industriels, etc. Dans le secteur de l'énergie, le Groupe ECA produit des moteurs électriques et des convertisseurs particulièrement adaptés aux industries ferroviaires et navales.



ROV ECA d'inspection des barrages

Source – ECA GROUP

Source – ECA GROUP

PARTIE III

Drones de confiance, cybersécurité et protection des données à caractère personnel

1. Enjeux de la confiance et de la cybersécurité

Les cas d'usages exposés en première partie montrent l'importance de n'utiliser que des drones de confiance dans le domaine de la sécurité :

- Certains contextes d'opérations ont un niveau de sensibilité important (ex : grand banditisme, anti-terrorisme) ;
- Au-delà d'opérations prises isolément, il est nécessaire de considérer l'impact potentiel qu'une puissance étrangère, liée à un fournisseur de drones, puisse capturer des informations sur une partie significative des opérations par drone menées en France par la police et la gendarmerie ;
- Dans l'ensemble des cas d'usage exposés, les drones et les données qu'ils capturent se doivent d'être fiable. Leur logiciel embarqué doit être protégé. Le chiffrement et l'authentification entre le drone et sa télécommande doivent assurer un niveau de sécurité suffisant. Les données capturées par le drone, ainsi que ses propres données de vol, doivent être protégées. Les mesures de sécurité doivent permettre de s'assurer que le drone ne peut pas être piégé, intercepté ou ses données volées.

Le niveau de sécurité devra par ailleurs s'élever progressivement, afin de prendre en compte :

- L'accroissement de la connectivité des drones, en particulier sur des liaisons 4G ou 5G, qui démultiplient les cas d'usages et leurs avantages, mais augmentent en même temps l'exposition des drones et le niveau de risques ;
- L'augmentation du fonctionnement autonome des drones, ce qui nécessite d'autant plus de confiance dans l'intégrité du logiciel qui permet ce fonctionnement autonome.

Enfin, le débat public montre que les citoyens français se focalisent parfois sur les cas d'usages qui ne sont pas forcément majoritaires, mais pour lesquels ils identifient un potentiel impact sur les libertés des personnes ou sur les données à caractère personnel. Les derniers avis du Conseil d'Etat, de la CNIL et du Conseil Constitutionnel viennent rappeler le besoin de cybersécurité et de protection des données à caractère personnel. Un défaut de prise en compte de ces aspects peut avoir un impact négatif dans la mesure où à défaut d'autorisation, les drones sont cloués au sol et ils ne peuvent pas répondre à l'ensemble des usages vertueux, en particulier ceux qui sont susceptibles d'assurer une meilleure sécurité des citoyens français et de leur porter secours de manière efficace. Il est indispensable que les drones disposent d'un niveau de cybersécurité élevé et soient choisis avec des critères de confiance.

2. Les risques identifiés

Des recherches en cybersécurité récentes, menées par les entreprises française Synacktiv[1] et américaine GRIMM[2], et largement reprises dans la presse internationale[3], montrent comment DJI, fabricant chinois de drones largement utilisés en France par la police et la gendarmerie :

- a des fonctions cachées dans ses applications,
- capture des données depuis les équipements de ses utilisateurs,
- intègre des portes d'entrées logicielles qui permettraient à DJI de prendre le contrôle du smartphone d'un utilisateur.

Ces recherches des entreprises en cybersécurité Synacktiv et GRIMM sont détaillées, GRIMM a même publié les outils[4] permettant de reproduire leurs observations. Elles recoupent les observations qu'a pu faire une autre entreprise en cybersécurité, River Loop Security, qui a identifié également des fonctions de vol de données dans d'autres produits de la marque DJI[5]. Suite à ces révélations, DJI a communiqué sur les évolutions que la marque va apporter pour corriger ces fonctions. Il faut toutefois noter que des fonctions similaires[6] avaient été identifiées en 2017[7] et 2018[8] ; DJI avait alors supprimé les fonctions dangereuses incriminées, mais en avait ensuite réintroduit d'autres, comme l'ont montré les recherches de Synacktiv et GRIMM.

Les fonctions dangereuses sont parfois pernicieuses, Synacktiv a montré que certaines données continuent à être collectées même quand l'application parait fermée et l'application a les droits de modifier les paramètre réseau, ce qui laisse un risque résiduel même lorsque le téléphone de l'utilisateur est en mode avion. Certains utilisateurs régaliens peuvent arguer qu'ils n'utilisent les solutions de DJI que dans un environnement coupé d'Internet. Il faut toutefois noter qu'une interconnexion intermittente reste nécessaire pour mettre à jour les appareils ou pour demander à DJI d'autoriser le vol dans certaines zones (No Fly Zones). C'est le cas par exemple pour un utilisateur qui doit intervenir à proximité d'un aéroport, une centrale nucléaire de production d'électricité ou une enceinte militaire.

---

[1] https://www.synacktiv.com/en/publications/dji-android-go-4-application-security-analysis.html

[2] https://blog.grimm-co.com/2020/07/dji-privacy-analysis-validation.html

[3] https://www.nytimes.com/2020/07/23/us/politics/dji-drones-security-vulnerability.html

[4] https://github.com/grimm-co/dji-go-4

[5] https://www.riverloopsecurity.com/blog/2020/05/dji_mimo/

[6] https://www.theregister.com/2017/08/15/dji_go_app_jspatch_tinker_silent_update_no_review/

[7] https://www.theverge.com/circuitbreaker/2017/8/28/16216428/dji-drone-app-update-data-collection

[8] https://gizmodo.com/dji-releases-security-findings-it-hopes-will-quash-chin-1825469976

Lorsque Synacktiv et Grimm ont publié le résultat de leurs recherches et que DJI a démenti ou minimisé ces constats, Kevin Finisterre a communiqué sur les réseaux sociaux[9] le 5 août 2020, puis lors d'une conférence[10] le 9 novembre 2020, pour interpeler DJI, le principal lobbyist de la marque et ses utilisateurs, en indiquant que lorsqu'il avait eu accès aux données des serveurs de DJI, il avait trouvé des documents qui détaillaient les projets de DJI de récupération de données en masse depuis les équipements de ses utilisateurs. Kevin Finisterre avait eu accès à ces données lorsqu'il avait participé au Bug Bounty de DJI et découvert en novembre 2017 qu'il était possible d'accéder aux ressources Cloud[11] de la marque avec une clé d'accès qui était publique. Les ressources accessibles contenaient à la fois des documents internes de DJI et les données des clients. Plutôt que de respecter les termes de son Bug Bounty et de rémunérer le chercheur en sécurité pour ses trouvailles, DJI l'avait menacé. Ce dernier a alors choisi de rendre ses découvertes publiques et de rendre public le mauvais comportement de DJI.

L'ensemble des preuves apportées par les chercheurs en sécurité met en évidence le niveau de risque élevé pour les utilisateurs de drones DJI en matière de cybersécurité et de manque de contrôle par l'utilisateur des données de vol, des photos ou vidéos capturées par les drones ou des données stockées ou accessibles depuis le smartphone ou la tablette qui sert à piloter un drone DJI. Certaines des fonctionnalités cachées mises en œuvre par DJI sont en outre susceptibles d'enfreindre les principes juridiques applicables en matière de traitement de données à caractère personnel (RGPD).

N'importe quel constructeur de drone est susceptible d'avoir une faille de sécurité dans ses logiciels, mais ce que montrent les chercheurs en cybersécurité est la présence de fonctions cachées, placées intentionnellement par DJI. Ce constat amène vers les problématiques suivantes :

1) Le fait que le constructeur chinois DJI ait placé intentionnellement des fonctions visant à voler des données pose la question de la confiance et des critères techniques et organisationnels qui permettent de l'établir
2) Lors de sa dernière étude, Synacktiv a investi plusieurs mois de travail, avec des intervenants d'une expertise importante, pour analyser uniquement certaines versions du logiciel de pilotage fourni par le constructeur DJI. Si DJI a placé des fonctions cachées dans ce logiciel-là, il est raisonnable de se questionner sur le risque que des fonctions dangereuses équivalentes soient introduites par le constructeur chinois non seulement dans le logiciel de pilotage, mais aussi dans le micrologiciel du drone, le micrologiciel de la télécommande, les logiciels de maintenance, etc. Se pose alors la capacité à pouvoir vérifier le niveau de cybersécurité des drones utilisés dans le domaine de la sécurité. Etant donné le manque d'experts en cybersécurité, ainsi que

[9] https://twitter.com/d0tslash/status/1291046555680747522

[10] https://prezi.com/view/Wiv59uVilOhZLxzWAXbS/

[11] http://www.digitalmunition.com/WhyIWalkedFrom3k.pdf

leur coût, il est important de pouvoir optimiser leur vérification et faire en sorte qu'elle se base sur une transparence accrue de la part du constructeur.

3. Exemple du programme US de drones de confiance Blue sUAS

Face aux preuves techniques identifiées par les experts en cybersécurité, les Etats-Unis ont pris conscience relativement tôt de l'espionnage mené par la Chine via les drones de son constructeur. Entre 2017 et 2020, différents ministères ont interdit l'usages de ces drones, en commençant par le DoD (Department of Defense), rejoint progressivement par le DoI, DoJ et DHS (respectivement Intérieur, Justice et sécurité intérieure).

Les Etats-Unis ont cherché à se doter d'une offre de drones de confiance pour remplacer les drones chinois. Sous l'impulsion de l'US Army, un projet à été confié au DIU (Defense Innovation Unit, l'équivalent de l'agence de l'innovation de la défense aux Etats-Unis) pour définir une offre alliant d'une part des critères de performance et d'autre part des critères de confiance et de cybersécurité. Parmi les critères de cybersécurité figuraient :

- L'intégration de fonctions de sécurité, comme le chiffrement des données captées par le drone et l'utilisation de protocoles radio sécurisés entre la télécommande et le drone,
- La maîtrise des données par l'utilisateur,
- L'utilisation de protocoles standards dont la cybersécurité est vérifiable,
- Une transparence sur l'ensemble des logiciels du drones, qu'ils soient développés par le fournisseur de drone ou intégré (bibliothèques, dépendances),
- La conception et la fabrication dans un pays de confiance,
- La transparence sur l'ensemble des composants matériels et le choix de composants ne venant que de pays de confiance,
- Des audits de cybersécurité de la solution finale.

Le projet du DIU a sélectionné 5 fournisseurs et modèles de drones, dont 4 américains (Skydio, Flir/Altavian, Vantage Robotics et Teal) et un français (Parrot). Bien que non américain, Parrot a été retenu, car il s'agissait de la solution la plus aboutie. Parrot était alors le seul fournisseur non Chinois à être capable de proposer une solution industrielle pour les drones de cette catégorie. Le soutien du DIU à des plus petits acteurs américain a permis de recréer une offre souveraine américaine, alors que l'écosystème des entreprises de drones avait précédemment été laminé par la Chine. L'enveloppe du DIU pour ce projet était de 11 millions de dollars. Ce projet ne portait que sur le développement d'un modèle répondant aux critères du DIU (l'acquisition finale des drones se faisant sur des contrats séparés). Pour soutenir la filière drones aux Etats-Unis, le DIU a mené des projets complémentaires, en particulier un pour une charge utile d'optique et un autre pour différents logiciels (autopilote, logiciel de pilotage, logiciels d'analyse des données captées par drone).

Il est intéressant de noter l'agilité avec laquelle ce projet a été mis en œuvre par le DIU. Parrot a fait une première présentation au DIU de son modèle historique en janvier 2019. Sur la base des demandes d'évolutions du DIU, un contrat a été signé en avril 2019, pour une livraison des premiers prototypes fin 2019. Sur la base des prototypes développés pour le DIU, Parrot

a décidé de proposer sur son catalogue un modèle sur étagère, Anafi USA. Le drone Anafi USA est en particulier le modèle retenu dans le cadre du marché de micro-drone du ministère des Armées en France.

Ce programme de drones de confiance, initié pour les propres besoins du DoD aux Etats-Unis, a ensuite été généralisé à l'ensemble des administrations fédérales américaines. Le catalogue d'achats GSA (équivalent de l'UGAP en France) a annoncé fin janvier 2021 supprimer toutes ses références de drones, hormis les 5 drones qualifiés dans le programme Blue sUAS du DIU.

L'exemple du programme Blue sUAS de drones de confiance aux Etats-Unis nous apporte les leçons suivantes :

- Importance d'un volontarisme et d'une vision affirmée,
- Définition de critères de confiance et de cybersécurité,
- Rapidité et agilité dans la mise en œuvre,
- Moyens financiers débloqués pour soutenir une offre souveraine,
- Mise à disposition du résultat à l'ensemble des ministères.

4. Intégrer le besoin de confiance et de cybersécurité dans les drones utilisés en France dans le domaine de la sécurité

A la vue des enjeux mis en avant dans la section 1, des risques identifiés dans la section 2 et de l'exemple de solution américaine illustrée dans la section 3, il apparait indispensable de :

1) A court terme, intégrer dans les appels d'offre public d'acquisition de micro-drones des critères systématiques de confiance, de cybersécurité et de protection des données à caractère personnel, qui écartent de facto les modèles qui ne présenteraient pas un niveau satisfaisant de cybersécurité ou pour lesquels on pourrait craindre un risque d'espionnage. A cet effet, l'ANSSI pourrait être chargée d'assister les ministères pour exprimer et vérifier les critères de sécurité que les appels d'offres publics devraient contenir (ou mandater un CESTI - Centre d'Évaluation de la Sécurité des Technologies de l'Information - agréé par l'ANSSI). Les éléments suivants devraient être considérés :
    a. Définir les mécanismes de sécurité attendus, en particulier concernant l'intégrité des logiciels, le chiffrement et l'authentification de la connexion entre le drone et sa télécommande, assurer un chiffrement des données captées par le drone et la protection des données de vol.
    b. S'assurer que l'implémentation des fonctions de sécurité est vérifiable. Par exemple, si un fournisseur propose un protocole de communication propriétaire, les fonctions de sécurité de ce protocole doivent être décrites de manière suffisamment transparente pour être vérifiées.
    c. Imposer à chaque candidat de fournir un rapport détaillé de traçabilité des composants matériels et des logiciels embarqués dans ses produits
    d. Au titre de la sécurité des approvisionnements, exiger de chaque candidat la preuve qu'il dispose, au sein de l'Union européenne ou de l'espace économique

européen, la capacité technique à concevoir et à modifier les logiciels embarqués dans le drone ou sa manette ;

e. Imposer à chaque candidat de décrire précisément la manière dont sont produites, stockées ou communiquées les données utilisateur et pour chaque étape, les mécanismes permettant de les protéger ;
f. Considérer l'ensemble du cycle de vie des produits, y compris les opérations de mises à jour logicielle ou de maintenance ;

2) Définir un programme de drones de confiance, qui permettra à moyen terme de mettre en commun et faciliter le travail de sélection et d'analyse cybersécurité que mènent chaque ministère.

PARTIE IV

Préconisations pour renforcer la filière industrielle de sécurité et faciliter la diffusion des technologies auprès des services de sécurité

PRECONISATIONS

P1 – Il faut rééquilibrer les arbitrages entre PME-ETI françaises et grands groupes industriels dans l'attribution des contrats publics. L'Etat doit davantage faire confiance aux PME-ETI dans les commandes publiques. Ce nécessaire rééquilibrage pérennisera la présence de pépites technologiques sur le territoire national et accélèrera la réindustrialisation du pays.

A l'image de ce qu'indiquait le nouveau président-directeur général du CNES Philippe Baptiste lors de son audition parlementaire du 10 mai 2021, la France doit pouvoir favoriser les PME/ETI françaises dans l'attribution de contrats pour pérenniser la présence de ces pépites technologiques sur le territoire national. En effet, ces entreprises ne recherchent pas toujours des subventions ou des aides pour développer leurs technologies, mais elle privilégient la signature de contrats pour réaliser des produits innovants. Ces contrats leur permettent ensuite de se valoriser auprès d'éventuels investisseurs et de clients internationaux.

Le gain peut être élevé pour la structure publique en raison de l'agilité et de la réactivité des PME/ETI capables de produire des produits disruptifs, innovants, dans des délais réduits tout en réduisant la facture de l'Etat. Faute de pouvoir se financer pour grandir, le risque est de voir certaines des meilleures pépites technologiques françaises être rachetées par des capitaux étrangers.

P2 – Les marchés publics et appels d'offres en drones et robotique concernant Police Gendarmerie, Pompiers, Sécurité Civile doivent introduire des exigences impératives de confiance, de cybersécurité et de protection des données à caractère personnel. La cybersécurité doit être vérifiable et assurer une traçabilité des données produites et utilisées par les robots durant leur utilisation.

Cette préconisation vient combler la situation actuelle où des Ministères régaliens et administrations françaises, voire des Opérateurs d'Importance Vitale, achètent ou utilisent des drones aériens du constructeur chinois DJI qui a à plusieurs reprises introduit des fonctions cachées dans ses logiciels visant à récupérer des données depuis l'équipement de l'utilisateur, voire à en prendre le contrôle avec des mécanisme de mise à jour parallèle. Les analyses de sécurité des drones DJI ont rapporté les trois failles de sécurité suivantes **(cf. PARTIE III et rapport d'analyse de sécurité des drones DJI fourni en annexe de cette note) :**

F1 : Le constructeur a (volontairement) placé des fonctions cachées dans ses applications.

F2 : Les applications embarquées capturent des données depuis les équipements des utilisateurs du drone.

F3 : Le constructeur a intégré des portes d'entrée logicielles (backdoor) qui permettraient de prendre le contrôle du smartphone de l'utilisateur de drone DJI.

Depuis 2016, plusieurs études de sécurité ont été menées par différents laboratoires. Chacune d'entre elles a confirmé les failles de sécurité F1, F2, F3 en particulier l'intégration de fonctions d'exfiltration de données dans plusieurs produits DJI.

A la suite de ces publications, la compagnie chinoise DJI a annoncé des évolutions, des adaptations et des corrections dans ses produits, en 2017, en 2018 et en 2019 mais à chaque fois, les études suivantes ont retrouvé les trois failles de sécurité sous des formes différentes, davantage dissimulées, obfusquées. Certaines des fonctionnalités cachées intégrées aux drones DJI par le constructeur chinois ne respectent pas la réglementation (RGPD) en matière de traitement des données à caractère personnel.

Une clause éliminatoire devrait exiger une description vérifiable des fonctions de sécurité et une traçabilité des données produites et utilisées par les robots. Cette clause devrait avoir un poids suffisant pour ne plus fonder le choix du fournisseur de robot sur le seul argument du prix de vente et de remettre la sécurité et la confiance au cœur du processus d'attribution du marché. L'ANSSI pourrait être chargée d'assister les ministères pour exprimer et vérifier les critères de sécurité que les appels d'offres publics devraient contenir (ou mandater un CESTI - Centre d'Évaluation de la Sécurité des Technologies de l'Information - agréé par l'ANSSI). Les éléments suivants devraient être considérés :

a. Définir les mécanismes de sécurité attendus, en particulier concernant l'intégrité des logiciels, le chiffrement et l'authentification de la connexion entre le drone et sa télécommande, assurer un chiffrement des données captées par le drone et la protection des données de vol.

b. S’assurer que l’implémentation des fonctions de sécurité est vérifiable. Par exemple, si un fournisseur propose un protocole de communication propriétaire, les fonctions de sécurité de ce protocole doivent être décrites de manière suffisamment transparente pour être vérifiées.
c. Imposer à chaque candidat de fournir un rapport détaillé de traçabilité des composants matériels et des logiciels embarqués dans ses produits
d. Au titre de la sécurité des approvisionnements, exiger de chaque candidat la preuve qu'il dispose, au sein de l'Union européenne ou de l'espace économique européen, la capacité technique à concevoir et à modifier les logiciels embarqués dans le drone ou sa manette ;
e. Imposer à chaque candidat de décrire précisément la manière dont sont produites, stockées ou communiquées les données utilisateur et pour chaque étape, les mécanismes permettant de les protéger ;
f. Considérer l’ensemble du cycle de vie des produits, y compris les opérations de mises à jour logicielle ou de maintenance ;

2) Définir un programme de drones de confiance, qui permettra à moyen terme de mettre en commun et faciliter le travail de sélection et d’analyse cybersécurité que mènent chaque ministère (cf. PARTIE III décrivant un exemple de programme de drones de confiances aux Etats-Unis).

Enfin, les clauses de sécurité dans les marchés et un programme de drones de confiance favoriseraient de fait les constructeurs de drones et robots européens soumis aux réglementations (RGPD) en matière de sécurité des données et pourrait agir comme un outil efficace de souveraineté technologique européenne.

P3 – Réorienter les fonds d’investissement français vers le secteur de la robotique qu’ils ignorent et délaissent depuis plusieurs décennies.

En France, les fonds d’investissement refusent de financer les startups et entreprises du secteur de la robotique et du hardware sous prétexte de la trop forte concurrence de marchés étrangers. De plus, pour les entreprises de robotique qui travaillent avec les forces armées (BITD) il est encore plus difficile de lever des fonds auprès des fonds d’investissement français adhérant au dispositif ISR (Investissement Socialement Responsable). La réponse la plus souvent formulée est « Vous avez pour client le Ministère des Armées ou la Police Gendarmerie, ce qui entre en contradiction avec notre déontologie de financement ISR. Nous vous conseillons de vous adresser à des fonds spécialisés Innovation défense AID». Ces verrous d’investissement pénalisent fortement les startups de robotique du secteur sécurité et défense. Certaines d’entre elles sont contraintes de masquer ou de sous-estimer leur activité de défense pour augmenter leurs chances de lever.

Il convient de revoir les clauses ISR afin qu’elles ne soient plus interprétées par les fonds français comme incompatibles avec un soutien à des entreprises de robotique de sécurité ou de hardware de sécurité.

Enfin, il faut réorienter les fonds français vers le financement du secteur du hardware car leur doctrine actuelle de « hardware blacklist » contribue fortement à aggraver notre dépendance au hardware asiatique ou américain. Là aussi, cette préconisation est une mesure de souveraineté industrielle.

P4 – Créer la nouvelle liste de champions WR10 au sein de la French Tech, aux côtés des actuelles listes FT120 et NEXT40

Les listes 2021 FT120 et NEXT40 publiées par la French Tech il y a deux mois ne contiennent toujours aucune entreprise du secteur de la robotique. Ce constat préoccupant est également valable pour les listes des années précédentes. Les classements FT120 et le NEXT40 semblent résolument incompatibles avec la filière de robotique française. Pourtant, nous disposons sur le territoire national de champions industriels de niveau mondial :

PARROT : numéro deux mondial du secteur des drones aériens légers.

PHOTONIS : TOP3 mondial des systèmes de vision nocturne et multispectral.

SHARK ROBOTICS : leader français de la robotique terrestre, TOP2 européen, TOP10 mondial, leader mondial des robots pompiers et des batteries haute résistance aux fortes températures.

ECA GROUP : TOP10 mondial de la robotique navale, marine et sous-marine.

Aucun de ces quatre champions industriels de niveau mondial ne figurent dans les classements de la French Tech qui s'appuie sur des critères d'entrée liés aux levées de fonds de plus de 20 millions d'euros.

Nous proposons de créer au sein de la French Tech un troisième classement indépendant du FT120 et du NEXT40. Ce classement nommé WR10 (World Ranking 10) concerne les startups et entreprises françaises ayant atteint le TOP10 mondial d'un secteur technologique stratégique (software, hardware, IoT, cybersécurité, robotique, Intelligence Artificielle, data sciences, électronique, nanotechnologie, biotechnologies, …).

Les avantages d'une liste French Tech WR10

Avantage n°1 : Le WR10 permet de réduire les « trous dans la raquette » dans le FT120. Avec le WR10, il devient impossible de passer à côté de sociétés comme PARROT ou SHARK ROBOTICS dans le secteur de la robotique. Il est impossible de rater la pépite française VUPEN (2004-2015) devenue ZERODIUM aux Etats-Unis en 2015 championne mondiale en détection de vulnérabilités, cybersécurité. Il est impossible de passer à côté de VALNEVA VIVALIS en Biotech et ses 100 millions de doses de vaccin anti-COVID.

Avantage n°2 : Le WR10 est un outil d'intelligence économique offensive et un message envoyé à la communauté internationale : La France soutient ses startups championnes de

niveau mondial avec un accompagnement « sur mesure » du type GCAS (dispositif de soutien aux entreprises d'intérêt stratégique vital).

Avantage n°3 : Le WR10 nécessite une veille permanente dans les domaines industriels stratégiques et la construction de métriques similaires à celles utilisées par les Etats-Unis.

Les critères et métriques d'accès à la liste French Tech WR10

L'accès au WR10 s'effectue sur la base des différents classements internationaux du domaine industriel de l'entreprise ou de la startup. Les concours d'innovations de rang mondial remportés constituent des critères additionnels (Awards américains de la robotique, Challenges DARPA, Challenges Google AI, concours Space-X, Challenge Blue Origin, …).

Le calcul de l'indice d'innovation d'une entreprise constitue un indicateur chiffré intéressant lorsque celle-ci a développé une stratégie de dépôt de brevets.

L'Indice d'innovation « II » d'une entreprise est calculé sur une période d'activité T (comptée en années). Il est défini par l'égalité :

$$II = \frac{Nombre\ de\ brevets\ déposés}{Effectif * Durée\ d'activité}$$

Exemples de calculs d'indices d'innovation II entre 1995 et 2015 :

II(Samsung) = 138 934 / (20 x 400 000) = 0,01736

II(Microsoft) = 56809 / (20 x 166175) = 0,01709

II(Google) = 23577 / (20 x 85050) = 0,01386

II(Shark Robotics) = II = $\frac{60}{35*5}$ = 0,343 calculé le 24 avril 2021 sur la base de ses cinq premières années d'activités. Cet indice est l'un des plus élevés au niveau mondial.

P5 – Créer et soutenir ROBOTICS VALLEY, la filière de robotique nationale en coopération avec la filière aéronautique AEROSPACE VALLEY en Occitanie et Nouvelle Aquitaine.

Le projet ROBOTICS VALLEY en Nouvelle Aquitaine et Occitanie s'appuie sur la création d'une grande filière française de la robotique en s'appuyant sur les champions présents (PHOTONIS, SHARK ROBOTICS, ECA, DASSAULT, THALES, AIRBUS, DELAIR, PARROT…) et en attirant d'autres champions dans le cluster national. Cette filière s'applique à la formation (du CAP jusqu'au Doctorat) dans les domaines liés à la robotique avec la création en France du premier lycée de la robotique. L'ancrage de la Robotics Valley est à la fois régional (Nouvelle Aquitaine et Occitanie) et européen avec sa présence à Bruxelles via une Fédération Professionnelle créée en 2021 : Drones4Sec (Fédération européenne professionnelle des drones de sécurité) présidée par PARROT.

P6 – Créer l'Agence d'Innovation du Ministère de l'Intérieur (AIMI) à l'image de l'AID pour faciliter les interactions entre les industriels de la sécurité et le Ministère.

La création de l'Agence d'Innovation du Ministère de l'Intérieur (AIMI) ou d'une Agence d'Innovation de la Sécurité Civile (AISC) pourrait inclure l'actuelle DMIA et étendre son périmètre à la robotique de sécurité, au hardware et capteurs, à l'optoélectronique, aux matériaux du futur, à l'IoT, à la cybersécurité, aux antennes, aux sciences des données et à l'intelligence artificielle. L'agence AIMI (ou AISC) pourrait travailler de concert avec la base industrielle de sécurité notamment en fluidifiant et en accélérant les itérations d'innovation quand un besoin métier apparait pour les forces de sécurité (Police, Gendarmerie, Douanes, Sapeurs-Pompiers, sécurité Civile). Cette agence renforcerait le lien Public-Privé et pourrait accélérer la relocalisation de la production de certains dispositifs et systèmes de sécurité. Enfin, elle permettrait d'abaisser les délais de marchés des matériels de sécurité à l'image du mode de fonctionnement du DIU américain (Defense Innovation Unit) lancé en 2015 pour accélérer les temporalités de la commande publique américaine.

PARTIE V

Marché mondial de la robotique de sécurité et prévisions pour la période 2021-2026

Source – DronesSec

Le marché mondial de la robotique de sécurité 2021-2026

Croissance, tendances et prévisions

Les robots de sécurité sont conçus pour remplacer les gardes de sécurité en patrouille et pour assurer une surveillance mobile par vidéosurveillance. Un robot de sécurité se déplace automatiquement dans une zone restreinte, sans supervision directe de l'opérateur. Les images de ses caméras intégrées sont transmises au poste de sécurité. La portée du rapport comprend les types de robots de sécurité - véhicule aérien sans pilote, véhicule terrestre sans pilote et véhicule sous-marin autonome. L'étude s'étend aux industries des utilisateurs finaux de ces robots dans les espaces de défense et militaires, résidentiels et commerciaux.

Le marché des robots de sécurité est segmenté par type de robot (véhicule aérien sans pilote, véhicule terrestre sans pilote et véhicule sous-marin autonome), par type d'industrie de l'utilisateur final (défense, service, industrie et commercial), par type d'applications (surveillance, renseignement, détection d'explosifs, patrouille et opérations de sauvetage) et par localisation des constructeurs.

Aperçu du marché de la robotique de sécurité

Le marché était évalué à 8,87 milliards USD en 2020 et devrait atteindre 19,77 milliards USD d'ici 2026, pour croître à un TCAC d'environ 14%, au cours de la période de prévision (2021-2026). La pandémie de COVID-19 a accru les perspectives d'introduction de technologies sans pilote dans le secteur des entreprises de sécurité privée et de protection des actifs.

Les cas d'usages de robots terrestres (UGV) sur des fonctions de surveillance se multiplient. Par exemple, les autorités tunisiennes ont utilisé le P-Guard d'Enova Robotic, une machine robuste conçue pour des applications multi-terrains, selon un communiqué du partenaire de l'entreprise pour les caméras, VIVOTEK. Le robot est équipé de deux objectifs grand angle de 4 mégapixels, de vues panoramiques à 180 degrés et d'illuminateurs infrarouges efficaces jusqu'à 20 mètres. De telles tendances devraient stimuler l'adoption de robots de sécurité, en particulier pendant la pandémie.

- Le développement de nouvelles technologies a également considérablement amélioré les capacités de ces robots. Actuellement, ils peuvent être déployés sur des terrains et des environnements difficiles pour effectuer une surveillance et d'autres actions basées sur l'analyse. L'inclusion de différents capteurs dans les robots de sécurité a amélioré les capacités des robots à analyser leur environnement et à fournir des données plus fiables. Cela a grandement profité à leur incorporation dans les dispositifs militaires.

- Des développements, comme K5 par KnightscopeInc., indiquent une future portée potentielle pour les robots de sécurité. Auparavant, ces robots avaient des capacités insuffisantes. Avec les progrès de la technologie des capteurs et des capacités d'automatisation, ces robots ont été développés pour être utiles dans les applications de travail. Le développement et les améliorations de la technologie des réseaux neuronaux et de vision artificielle ont également donné à ces robots la capacité d'apprendre au fil du temps et d'améliorer leurs fonctionnalités.

- Pour 325 millions de citoyens américains, on compte seulement 700 000 policiers locaux, étatiques et fédéraux, chargés de protéger et d'assurer la sécurité. Il n'y a pas assez de force pour effectuer la tâche efficacement. L'adoption massive des robots de sécurité va compenser cette pénurie.

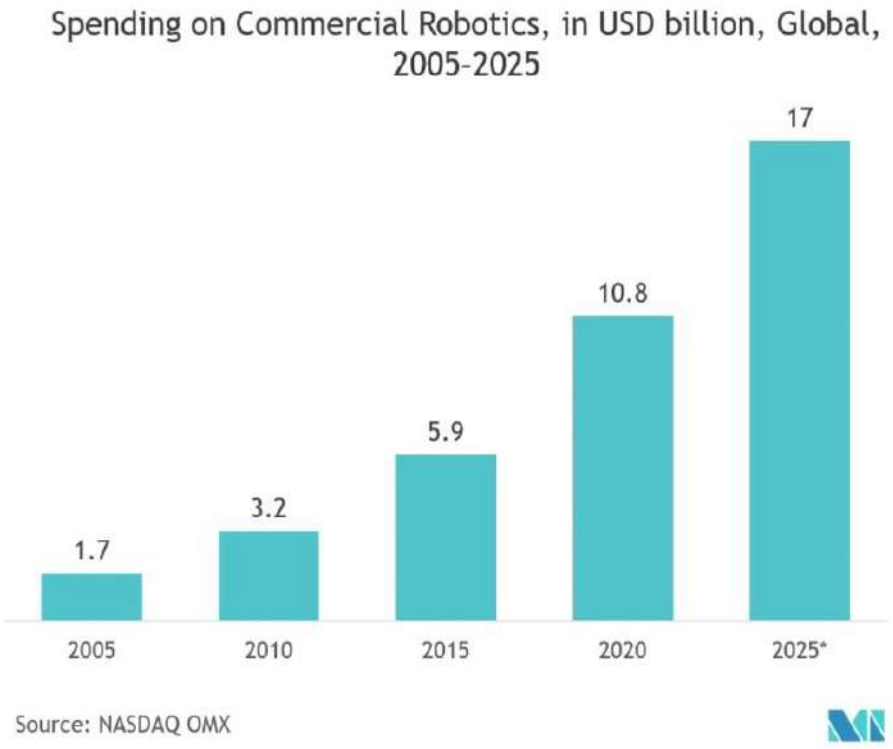
Tendances clés du marché de la robotique de sécurité

- Les entreprises commerciales et les entreprises connexes représentent une part massive de l'économie, l'industrie disposant d'importants budgets à consacrer à l'amélioration de la sécurité. Ainsi, les robots de sécurité de ce secteur offrent une proposition de valeur attrayante et quantifiable.

- Alors que des milliards de dollars sont dépensés en R&D dans les véhicules autonomes, les robots d'intérieur pour les espaces commerciaux récoltent les avantages technologiques et économiques des capteurs, de l'informatique, de l'apprentissage automatique et des logiciels open source. Avec l'augmentation du budget des dépenses de sécurité commerciale et la disponibilité d'un marché largement inexploité, le secteur des robots de sécurité devrait croître à un rythme important de 2021 à 2026.

- La tendance des robots d'intérieur gagne en popularité sur le marché, avec leur large gamme d'applications dans différents secteurs, tels que les bureaux et les hôpitaux, entre autres.

- Les robots ont le potentiel d'offrir une gamme d'avantages commerciaux et de sécurité, et les entreprises du marché développent de nouveaux systèmes robotiques pour des applications spécifiques.



Les États-Unis devraient représenter la plus grande part du marché mondial

- En raison de leurs avantages (comme la qualité et la fiabilité), les forces de sécurité et de surveillance américaines utilisent de plus en plus des solutions s'appuyant sur des systèmes robotisés (sans pilote).

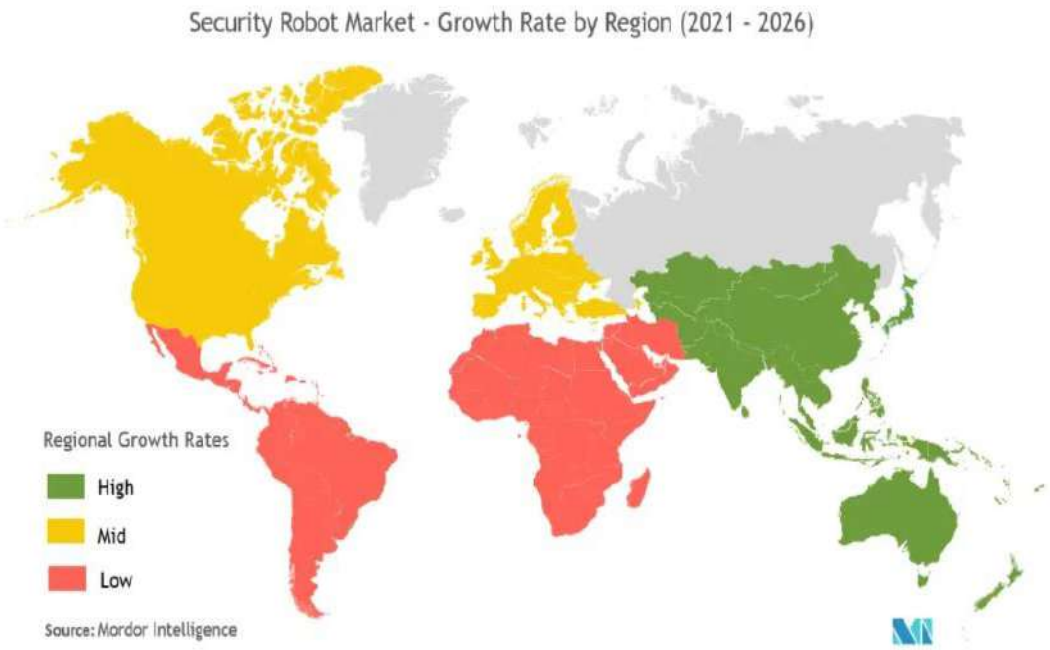
- En février 2020, le robot de sécurité Cobalt réalise des patrouilles autonomes. Il se déplace à environ trois kilomètres à l'heure. Si quelqu'un passe devant lui, ses capteurs lui permettent de s'arrêter. Il peut patrouiller en autonomie dans les

entreprises. Certaines sociétés du Kansas et du Missouri commencent à l'utiliser. Kenton Brothers Inc. utilise un robot de sécurité Cobalt Robotics pour patrouiller en autonomie dans son entreprise de Kansas City.

- Au cours de la dernière décennie, le nombre de conflits actifs a augmenté dans tout le pays, parallèlement à une augmentation des attaques terroristes dans les lieux publics et les écoles. Ces instabilités géopolitiques et les conflits territoriaux associés ont entraîné un besoin croissant de robots de sécurité dans le pays au cours de la période de prévision. En raison de l'augmentation des activités terroristes, l'augmentation des problèmes de sécurité à travers le pays devrait également booster la demande de systèmes robotisés pour les services de sécurité américains.

- L'une des principales contraintes pour le marché des robots de sécurité aux États-Unis réside dans les règles et réglementations strictes concernant l'utilisation de robots de sécurité et la dépendance vis-à-vis des carnets de commandes du gouvernement pour fournir des robots de sécurité.

- Les préoccupations négatives croissantes concernant l'utilisation de robots de sécurité entravent la croissance du marché. Un robot de sécurité de San Fransisco a été « licencié » pour intrusion sur les trottoirs publics sans l'approbation de la ville et pour s'être fait des ennemis humains. Le robot, qui était utilisé par la SPCA de San Francisco pour patrouiller dans son parking et ses terrains, a suscité une vague massive de réactions du public pour avoir irrité les piétons et empêché les sans-abri de s'asseoir à l'extérieur de la propriété. Selon Mashable, il a également valu une réprimande de la ville, qui a averti la SPCA que le robot empiétait sur les trottoirs publics sans permis approprié.



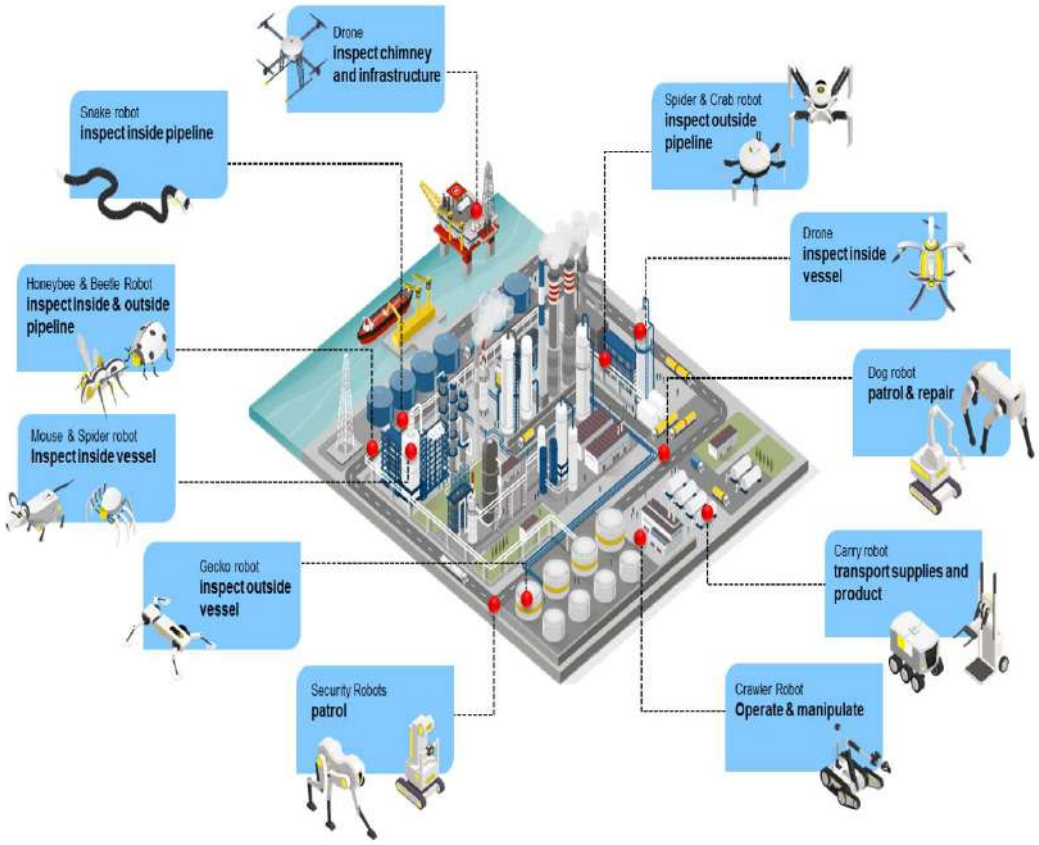
Panorama concurrentiel

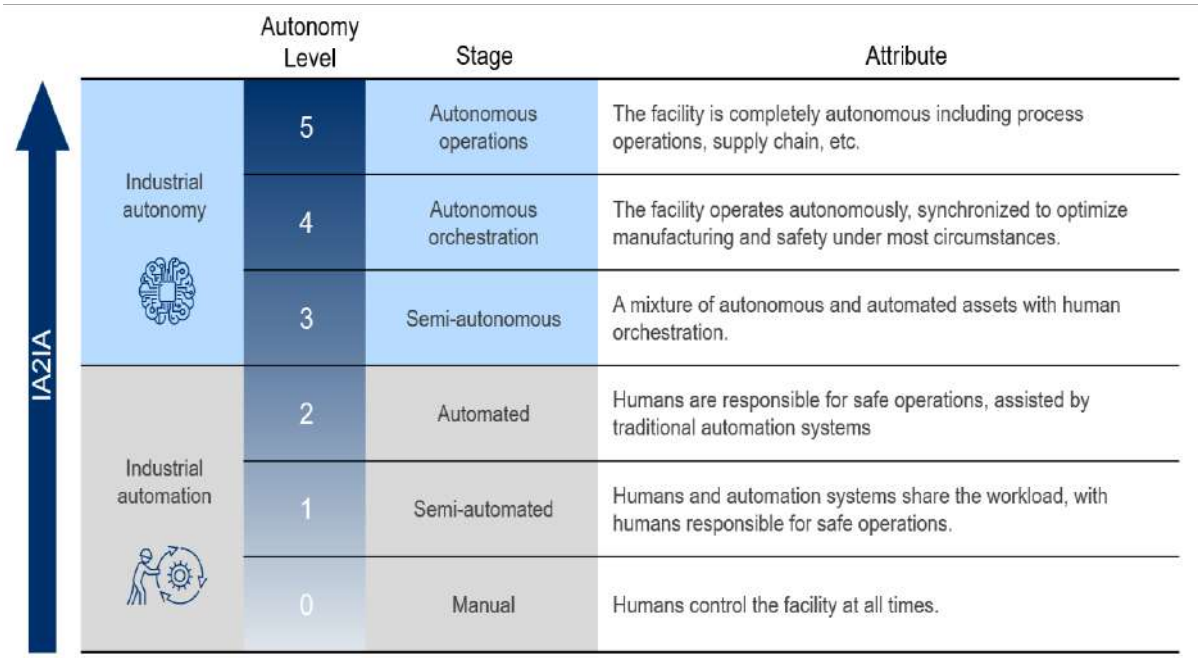
Le marché mondial des robots de sécurité est très fragmenté, avec la présence de plusieurs nouveaux entrants et start-ups dans les régions développées. Des barrières relativement élevées à l'entrée et à la sortie induisent un niveau de pénétration du marché plus élevé et plus complexe. Cependant, la tendance à s'intégrer verticalement dans différents segments de la chaîne de valeur a tendance à offrir un avantage concurrentiel aux principaux fournisseurs du marché. Parmi les principaux acteurs du marché des robots de sécurité on retrouve Lockheed Martin Corporation et Northrop Grumman.

- Octobre 2020 - SZ DJI Technology Co. Ltd, a dévoilé à INTERGEO, deux nouvelles solutions de charge utile DJI Zenmuse P1 et DJI Zenmuse L1 pour sa plateforme phare de drone commercial Matrice 300 RTK, destinée à servir les missions d'arpentage aérien les plus exigeantes. Les charges utiles twp devraient changer la donne pour l'industrie, apportant plus d'efficacité et de nouvelles perspectives à un coût abordable sans compromettre la qualité et la précision des données collectées pour des inspections aériennes précises et des missions de collecte de données.

- Septembre 2020 - Lockheed Martin lance une étude pour un navire à charge utile intégré et capable, qui sera capable de patrouiller pendant des durées prolongées, dans le cadre du concours Large Unmanned Surface Vessel (LUSV) de l'US Navy. Lockheed Martin s'est associé à Vigor Works, LLC, basé à Portland, en tant que constructeur naval de l'équipe. En tant que maître d'œuvre, Lockheed Martin gérera le programme, fournira l'intégration de la plate-forme, l'ingénierie des systèmes, la gestion du combat, l'automatisation et les solutions cyber associées.

Robots d'inspection et de sécurité en contexte industriel





	Autonomy Level	Stage	Attribute
Industrial autonomy	5	Autonomous operations	The facility is completely autonomous including process operations, supply chain, etc.
	4	Autonomous orchestration	The facility operates autonomously, synchronized to optimize manufacturing and safety under most circumstances.
	3	Semi-autonomous	A mixture of autonomous and automated assets with human orchestration.
Industrial automation	2	Automated	Humans are responsible for safe operations, assisted by traditional automation systems
	1	Semi-automated	Humans and automation systems share the workload, with humans responsible for safe operations.
	0	Manual	Humans control the facility at all times.

IA2IA

Acteurs majeurs de la robotique de sécurité

DEVELOPPEMENTS récents

- Décembre 2020 - Aerovironment a acquis Telerob pour étendre son offre de systèmes sans pilote multi-domaines et sa présence mondiale. Le partenariat de l'entreprise avec le ministère américain de la Défense et sa présence dans 50 pays alliés, combinés à la présence de Telerob dans 45 pays et à sa base de clients multisectoriels, peuvent créer d'importantes opportunités de croissance et de création de valeur.

- Janvier 2020 - Les robots de sécurité de SMP Robotic ont reçu l'autorisation d'être utilisés dans la ville de Dubaï avec l'Agence de réglementation de l'industrie de la sécurité de Dubaï délivrant l'autorisation d'utiliser des robots de sécurité. Les robots de sécurité patrouillaient sur le territoire de la communauté fermée.

Segmentation du marché des drones aériens (UAV)

Marché des drones, par système

- Marché des plateformes, par sous-système
  - Cellules, par type de matériau
    - Alliages
    - Plastiques
    - Composites, par type
      - Polymères renforcés de fibre de carbone
      - Polymères renforcés de fibres de verre
      - Polymères renforcés de fibres de bore
      - Polymères renforcés de fibres d'aramide
  - Avionique, par composant
    - Systèmes de commandes de vol, par sous-composant
      - Ordinateurs de données aériennes
      - Pilotes automatiques/Ordinateurs de contrôle de vol
    - Systèmes de navigation, par sous-composant
      - GPS/GNSS
      - INS/IMU
      - Systèmes de détection et d'évitement
    - Systèmes de communication
    - Autres
  - Systèmes de propulsion, par composant
    - Moteurs, par type
      - Gaz
      - Électrique
    - Sources d'alimentation, par type
      - Batteries

            - Cellules solaires
            - Réservoirs de carburant
        - Capteurs, par type
            - Capteurs de vitesse
            - Capteurs de lumière
            - Capteurs de proximité
            - Capteurs de position
            - Capteurs de température
        - Logiciel de drone
- Charges utiles, par type
    - Caméras, par type
        - Caméras haute résolution
        - Caméras multispectrales
        - Caméras hyperspectrales
        - Caméras thermiques
        - Caméras EO/IR
    - Capteurs CBRN
    - Charges utiles de renseignement électronique, par type
        - Intelligence des signaux
        - Renseignement électronique
        - Intelligence de la communication
        - Intelligence télémétrique
    - Radar UAV, par type
        - Radar d'ouverture synthétique
        - Radar actif à balayage électronique
    - LiDAR drone
    - Cardan de drone
    - Autres
- Liens de données UAV
- Stations de contrôle au sol d'UAV
- Systèmes de lancement et de récupération d'UAV

Marché des drones, par verticale

- Militaire, par application
    - Renseignement, surveillance et reconnaissance (ISR)
    - Opérations de combat
    - Gestion des dommages de combat
- Commercial, par application
    - Inspection et surveillance
    - Télédétection
    - Arpentage et cartographie
    - Livraison de produit
    - Entretien et réparation
    - Imagerie aérienne
    - Entreposage industriel
    - Autres

- Gouvernement et application de la loi, par vertical
    - Gestion des frontières
    - Surveillance du trafic
    - Lutte contre les incendies et gestion des catastrophes
    - Recherche et sauvetage
    - Opérations et enquêtes policières
    - Sécurité maritime
- Consommateur, par application
    - Prosommateurs
    - Amateurs

Marché des drones, par industrie

- Défense & Sécurité
- Agriculture
- Logistique et transport
    - Livraison postale et de colis
    - Soins de santé et pharmacie
    - Commerce de détail et alimentation
- Énergie & Puissance
    - La production d'énergie
    - Gaz de pétrole
- Construction et exploitation minière
- Médias et divertissement
- Assurance
- Faune et foresterie
- Universitaires et recherche

Marché des drones, par classe

- Petit UAV
    - Nano drones
    - Micro drones
    - Mini drones
- UAV stratégiques et tactiques
    - UAV à courte portée (CR)
    - UAV à courte portée (SR)
    - UAV à moyenne portée (MR)
    - UAV d'endurance à moyenne portée (MRE)
    - UAV à pénétration profonde à basse altitude (LADP)
    - UAV à basse altitude et longue endurance (LALE)
    - Moyenne Altitude Longue Endurance (MALE)
    - Haute altitude longue endurance (HALE)
- UAV à usage spécial
    - Véhicules aériens de combat sans pilote (UCAV)
    - Essaim de drones
    - UAV mortels

- UAV leurres
- UAV stratosphériques
- UAV exo-stratosphériques

Marché des drones, par type de drone

- UAV à voilure fixe
- UAV VTOL à voilure fixe
- UAV à voilure tournante
    - Rotor unique
    - Multi-rotor
        - Bicoptère
        - Tricoptères
        - Quadricoptères
        - Octocoptères

Marché des drones, par mode d'exploitation

- Piloté à distance, par verticale
- Piloté en option, Par Vertical
- Entièrement autonome, par vertical

Marché des drones, par gamme

- Ligne de visée visuelle (VLOS), par verticale
- Ligne de visée visuelle étendue (EVLOS), par verticale
- Au-delà de la ligne de mire (BLOS), par verticale

Marché des drones, par MTOW

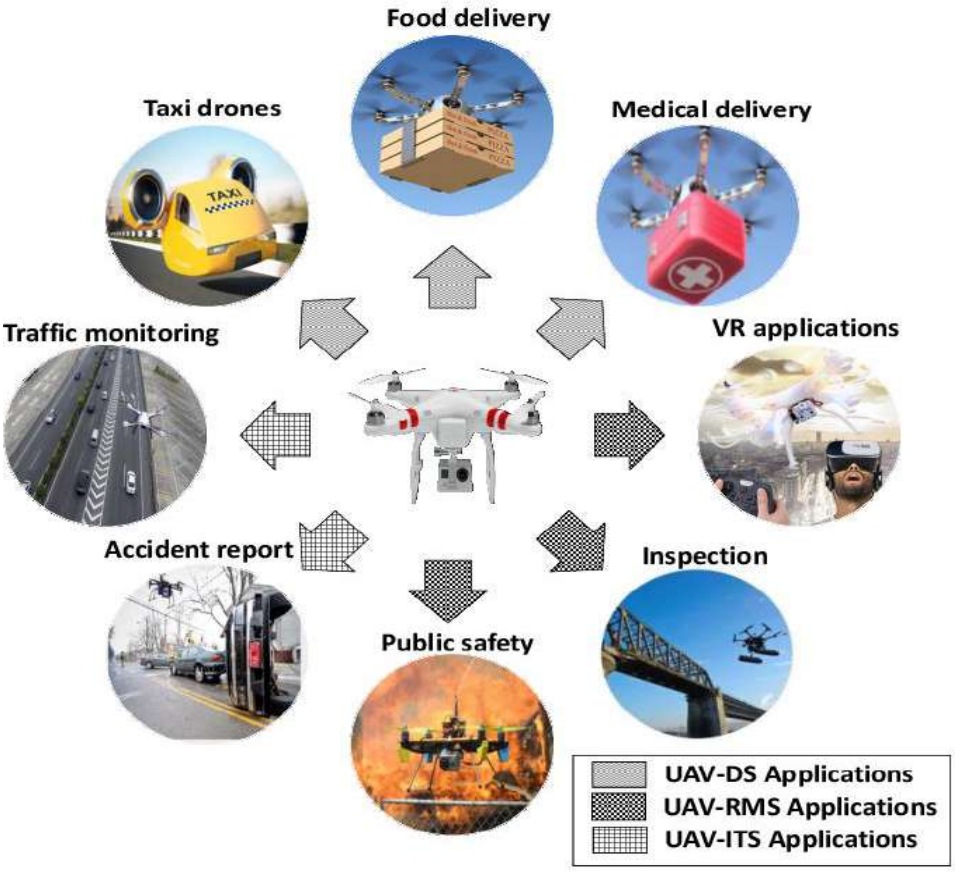
- <25 kilogrammes, par vertical
- 25-170 kilogrammes, par vertical
- >170 kilogrammes, par verticale

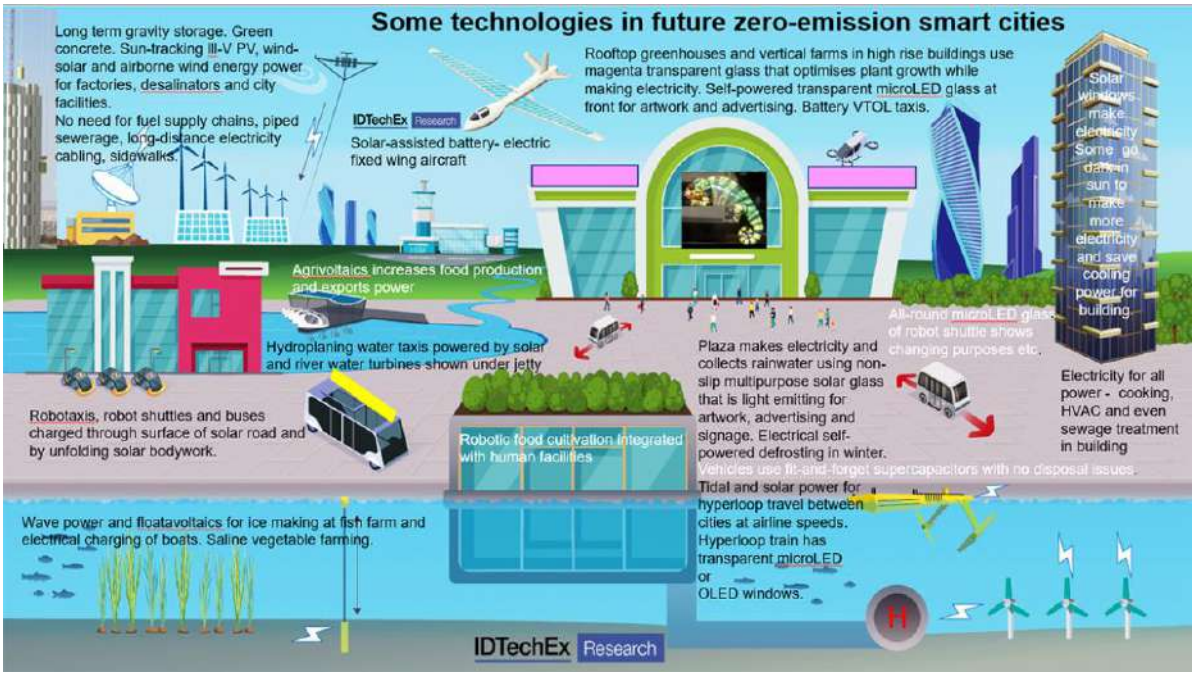
Marché des drones, par point de vente

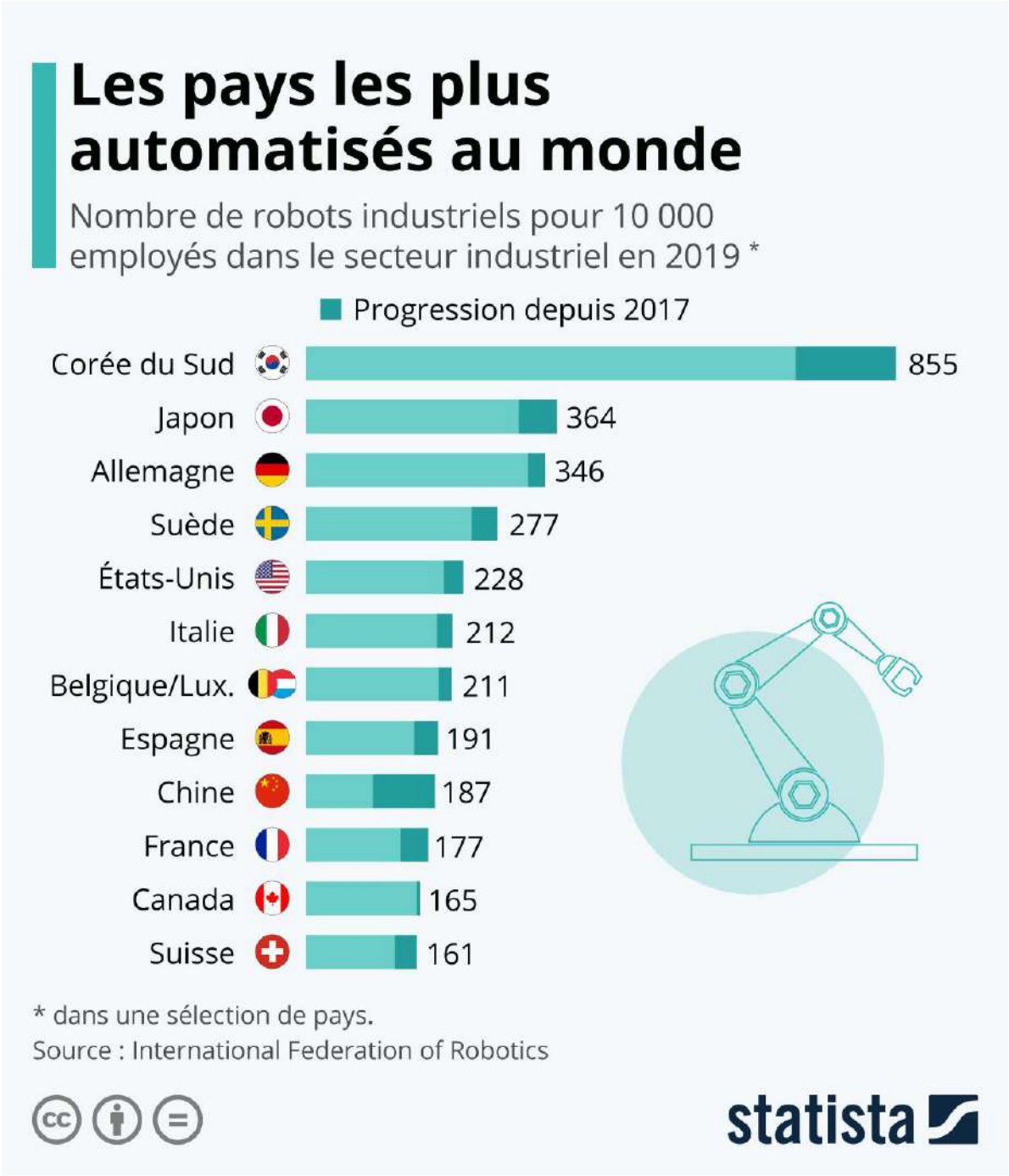
- Fabricants d'équipement d'origine (OEM)
- Marché secondaire

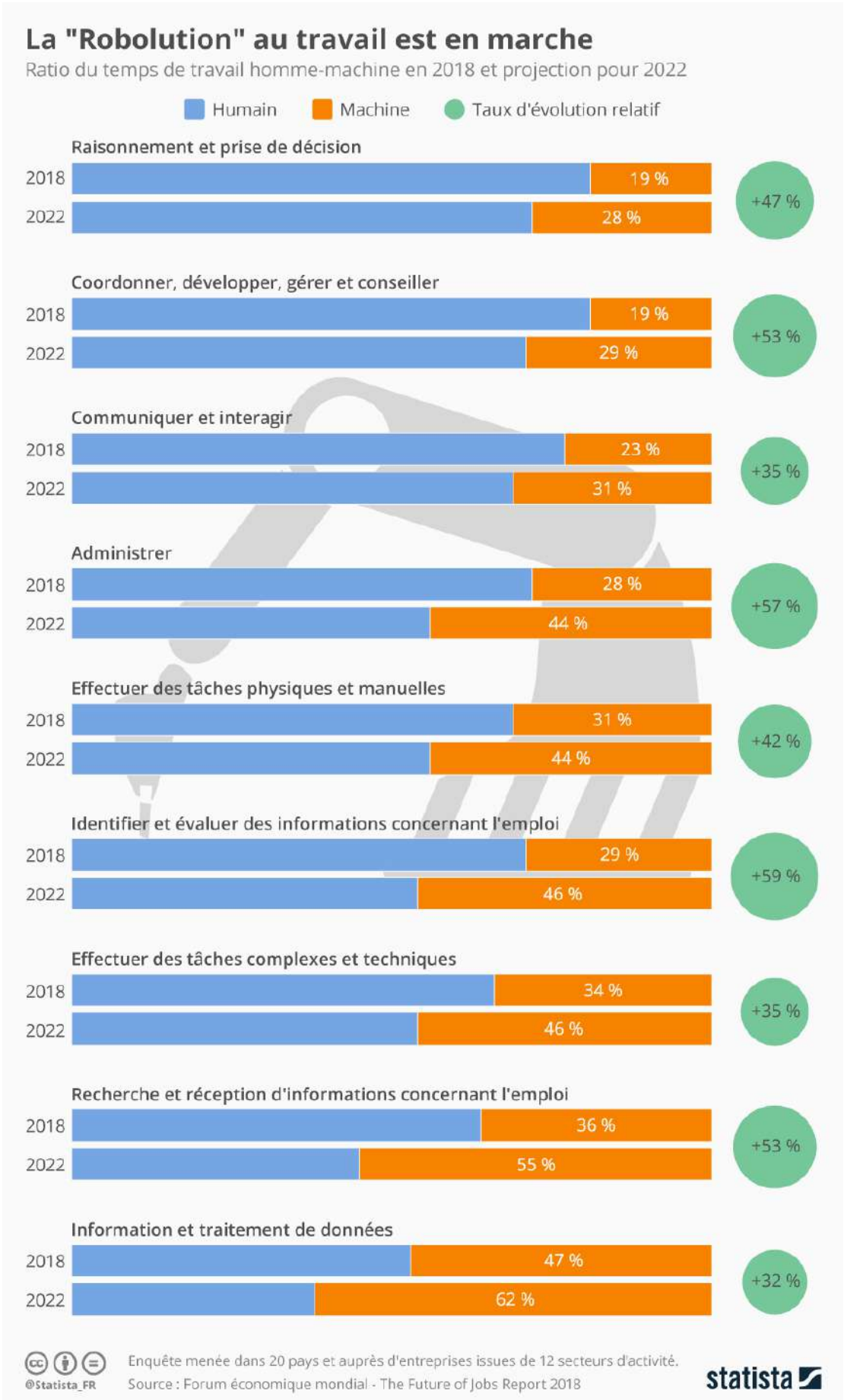
Marché des drones, par région

- Amérique du Nord
- L'Europe ·
- Asie-Pacifique
- Moyen-Orient
- l'Amérique latine
- Afrique


Food delivery
Taxi drones
Medical delivery
Traffic monitoring
VR applications
Accident report
Inspection
Public safety
UAV-DS Applications
UAV-RMS Applications
UAV-ITS Applications


Some technologies in future zero-emission smart cities
Long term gravity storage. Green concrete. Sun-tracking III-V PV, wind-solar and airborne wind energy power for factories, desalinators and city facilities.
No need for fuel supply chains, piped sewerage, long-distance electricity cabling, sidewalks.
IDTechEx Research
Solar-assisted battery- electric fixed wing aircraft
Rooftop greenhouses and vertical farms in high rise buildings use magenta transparent glass that optimises plant growth while making electricity. Self-powered transparent microLED glass at front for artwork and advertising. Battery VTOL taxis.
Solar windows make electricity. Some go down sun to make more electricity and save cooling power for building.
Agrivoltaics increases food production and exports power
Hydroplaning water taxis powered by solar and river water turbines shown under jetty
All-round microLED glass of robot shuttle shows changing purposes etc.
Plaza makes electricity and collects rainwater using non-slip multipurpose solar glass that is light emitting for artwork, advertising and signage. Electrical self-powered defrosting in winter.
Electricity for all power - cooking, HVAC and even sewage treatment in building
Robotaxis, robot shuttles and buses charged through surface of solar road and by unfolding solar bodywork.
Robotic food cultivation integrated with human facilities
Vehicles use fit-and-forget supercapacitors with no disposal issues.
Tidal and solar power for hyperloop travel between cities at airline speeds. Hyperloop train has transparent microLED or OLED windows.
Wave power and floatavoltaics for ice making at fish farm and electrical charging of boats. Saline vegetable farming.
IDTechEx Research

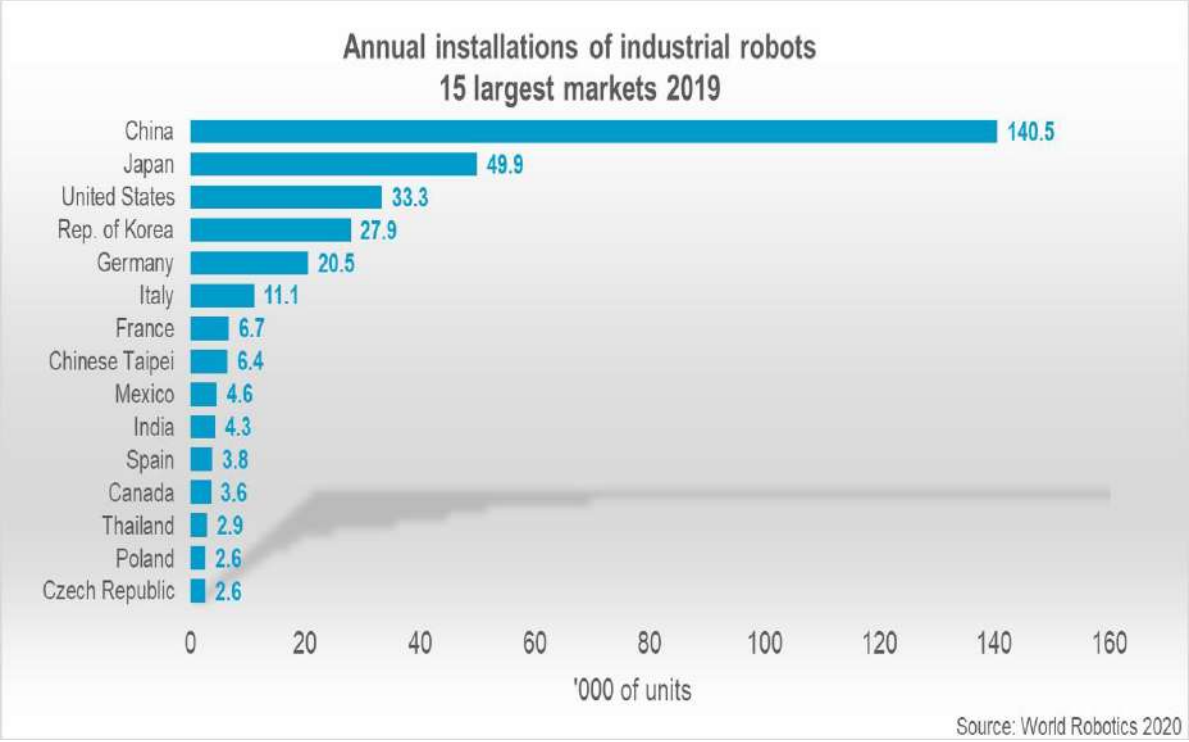

Les pays les plus automatisés au monde
Nombre de robots industriels pour 10 000 employés dans le secteur industriel en 2019 *
Progression depuis 2017
Corée du Sud 855
Japon 364
Allemagne 346
Suède 277
États-Unis 228
Italie 212
Belgique/Lux. 211
Espagne 191
Chine 187
France 177
Canada 165
Suisse 161
* dans une sélection de pays.
Source : International Federation of Robotics
statista


La "Robolution" au travail est en marche
Ratio du temps de travail homme-machine en 2018 et projection pour 2022
Humain
Machine
Taux d'évolution relatif
Raisonnement et prise de décision
2018
19 %
2022
28 %
+47 %
Coordonner, développer, gérer et conseiller
2018
19 %
2022
29 %
+53 %
Communiquer et interagir
2018
23 %
2022
31 %
+35 %
Administrer
2018
28 %
2022
44 %
+57 %
Effectuer des tâches physiques et manuelles
2018
31 %
2022
44 %
+42 %
Identifier et évaluer des informations concernant l'emploi
2018
29 %
2022
46 %
+59 %
Effectuer des tâches complexes et techniques
2018
34 %
2022
46 %
+35 %
Recherche et réception d'informations concernant l'emploi
2018
36 %
2022
55 %
+53 %
Information et traitement de données
2018
47 %
2022
62 %
+32 %
@Statista_FR
Enquête menée dans 20 pays et auprès d'entreprises issues de 12 secteurs d'activité.
Source : Forum économique mondial - The Future of Jobs Report 2018
statista

Dans le cadre de son plan de relance économique, le gouvernement a présenté début septembre un projet de soutien à la modernisation des usines françaises. Ce dernier se compose notamment de subventions et de prêts destinés aux investissements dans l'automatisation industrielle : robots, capteurs, logiciels, etc. Comme le rappelait la secrétaire d'État auprès du ministre de l'Économie dans Les Echos, « on s'aperçoit que dans un certain nombre de secteurs, les entreprises, notamment les PME et les ETI, n'ont pas nécessairement eu la capacité de se moderniser » et l'industrie française accuse globalement un retard en matière de robotisation par rapport à d'autres puissances industrielles.

Dans sa dernière étude parue hier, la Fédération internationale de robotique a calculé la densité de robots industriels dans une sélection de pays, mettant en lumière de fortes disparités à travers le monde. Le développement de l'automatisation est particulièrement dynamique en Asie, où environ deux tiers des robots vendus dans le monde l'année dernière ont été installés. La Corée du Sud comptait 855 robots industriels pour 10 000 salariés en 2019, alors que Singapour, non inclus dans ce graphique, détenait le ratio mondial le plus élevé (918). Quant à la Chine, qui concentre à elle seule plus du tiers des installations, elle a vu sa densité de robots industriels doubler en l'espace de deux ans. Avec une densité de 187 pour 10 000 employés, le pays passe devant la France au classement cette année.

En Europe, le pays le plus automatisé est l'Allemagne avec 346 unités recensées pour 10 000 employés en 2019. Quant à l'industrie française, elle enregistrait toujours une densité plus faible que la plupart de ses voisins européens : 177 robots pour 10 000 employés, contre respectivement 212 en Italie, 211 en Belgique (et Luxembourg) et 191 en Espagne. Toutefois, il est important de noter que cette statistique correspond à une moyenne multisectorielle pour l'ensemble de l'industrie. Dans la branche automobile, l'Hexagone est par exemple plutôt bien équipé en comparaison aux autres pays industrialisés.



Nombre record de robots installés en France - Rapports la Fédération Internationale de Robotique

• Le stock de robots atteint un nouveau record - plus 10 % - ventes en hausse de 15 %
• La France parmi les 3 premiers pays comptant le plus de robots au sein de l'Union européenne

Francfort, le 24 septembre 2020 - **Le nouveau rapport World Robotics 2020 Industrial Robots présenté par la Fédération Internationale de Robotique (IFR) révèle un record d'environ 42 000 robots industriels officiant dans des usines aux quatre coins de la France - une augmentation de 10 %. Les ventes de nouveaux robots ont augmenté de 15 % et ont atteint environ 6 700 unités en 2019 - un nouveau record d'installations.**

« La France réalise une incroyable réussite sur la production intelligente avec des robots industriels », déclare Milton Guerry, président de la Fédération Internationale de Robotique. « Les installations annuelles ont augmenté au cours de la période 2014-2019 de 18 % en moyenne par an. »
Depuis 2010, les initiatives gouvernementales de renforcement de la production en France ont engendré des investissements importants de la part de l'industrie automobile et de la plupart de l'industrie générale. L'industrie la plus importante est l'automobile avec une part de 40 % des installations en 2019. Dans l'industrie générale, les installations ont augmenté de 11 %.
Aujourd'hui, la France fait partie des 3 premiers utilisateurs de robots industriels au sein de l'Union européenne : leur stock opérationnel d'environ 42 000 unités est environ le double du stock du Royaume-Uni qui compte 21 700 unités. Le principal utilisateur de l'UE reste l'Allemagne qui dénombre un stock opérationnel d'environ 221 500 unités, soit environ cinq fois le stock de la France - suivi de l'Italie avec un stock opérationnel de 74 400 unités.

Perspective

À l'échelle mondiale, le COVID-19 a une forte incidence sur 2020 - mais offre également une chance de modernisation et de numérisation de la production en voie de reprise. À long terme, les avantages de l'augmentation des installations de robots restent identiques : la production rapide et la livraison de produits personnalisés à des prix compétitifs sont les principales incitations. L'automatisation permet aux fabricants de maintenir la production dans les économies développées - ou de la restituer - sans sacrifier la rentabilité. La gamme de robots industriels continue de s'étendre - des robots traditionnels en cage capables de gérer toutes les charges utiles rapidement et avec précision aux nouveaux robots collaboratifs qui travaillent en toute sécurité aux côtés des humains, entièrement intégrés dans les établis.

Liens et références

Word Robotics Report 2020 :

https://ifr.org/ifr-press-releases/news/record-2.7-million-robots-work-in-factories-around-the-globe

Security Robots Market 2020

https://www.mordorintelligence.com/industry-reports/security-robots-market

Contacter les contributeurs

Thierry BERTHIER :

thier.berthier@gmail.com

tb@drones4sec.eu

Victor VUILLARD :

Victor.vuillard@parrot.com

v@drones4sec.eu

Manon VERMENOUZE :

shark-robotics@drones4sec.eu

manon.vermenouze@shark-robotics.fr

Geoffroy DELTEL :

g.deltel@photonis.com

photonis@drones4sec.eu

Mission du député Jean-Michel Mis

« Pour un usage responsable et acceptable par la société des technologies de sécurité »

*

1/ Objectifs de la mission

La mission souhaite explorer, lors des auditions et via les contributions écrites, les axes suivants :

- Les **opportunités offertes par les nouvelles technologies au service d'une meilleure offre de sécurité** en analysant les besoins des forces de sécurité, entre autres dans la perspective des grands événements sportifs de 2023 et 2024.

- Les principes nécessaires à **la préservation des libertés** en définissant un cadre d'emploi global et cohérent des technologies de sécurité et en associant la société civile à cette définition pour renforcer la compréhension et l'acceptabilité des nouvelles technologies dans la société.

2/ Questions

Quelles sont les principales nouvelles technologies de sécurité selon vous ? *[Par exemple : applications d'IA et d'automatisation, traitement des données (textuelles, images, sonores), biométrie, équipements de l'agent en mobilité]*

Aujourd'hui, les technologies du numérique dont l'Intelligence Artificielle apportent les principales nouveautés au domaine de la Sécurité. Elles permettent de collecter les données sur les systèmes puis de les analyser afin d'étudier l'état du système en matière de sécurité. Les données peuvent être très nombreuses (big data) et apparaître sous de nombreuses formes (données structurées et non structurées : image, vidéo, parole, audio, texte). Ces technologies apportent des bénéfices mais aussi des risques surtout dans les cas où les données comprennent des données personnelles.

Pour quelles finalités ? *[Par exemple : détection de situations, analyse prédictive, suivi des personnes.]*

Les analyses sur les données collectées et historisées permettent notamment de : établir des modèles de comportement nominal des systèmes, détecter les écarts (faille de sécurité) et prévoir des problèmes de sécurité à venir ; rechercher des relations entre événements et remonter, à partir d'une situation particulière (ex : fraude), l'ensemble des événements ayant conduit à cette situation jusqu'à la source (cause, point de compromission) ; rechercher, dans des bases de situations de non-sécurité des regroupements de situations similaires ou des situations correspondant à certaines caractéristiques (search sur mots clés)… Beaucoup de ces techniques peuvent être déployées pour la cybersécurité.

Pensez-vous qu'elles permettraient d'anticiper les évolutions des missions de sécurité dans les 10 à 20 ans à venir ? Comment voyez-vous ces évolutions ?

Ces technologies évoluent très rapidement et, au vu des travaux de recherche très nombreux sur ces sujets, il est très certain que de nouveaux résultats vont apparaître dans les 10 ans à venir, que les applications de sécurité pourront exploiter.

Parmi les évolutions prévisibles : la possibilité d'analyser « sans couture » les sources de données non structurées de toutes sortes (par exemple, image, parole, texte) ; l'apparition de modèles d'intelligence artificielle pré-entraînés sur de très larges volumes de données disponibles sur étagère (exemple : modèle de fake news) ; l'apparition de plateformes de données disponibles sur des verticaux d'applications ; la possibilité de réaliser des analyses de sécurité en temps réel et en continu quel que soit le volume de données à collecter ; le développement de techniques IA pour combattre les cyberattaques.

Quels sont selon vous les principaux enjeux de liberté dont il est question face aux nouvelles technologies de sécurité ?

Face à ces technologies, il est important de s'assurer que les règles d'éthique (par exemple celles élaborées par le AI High Level Expert group de la commission Européenne[1]) sont assurées : la confiance des citoyens dans les systèmes mis en place est cruciale pour leur acceptabilité :

> *Veiller à ce que la mise au point, le déploiement et l'utilisation de systèmes d'IA répondent aux exigences d'une IA digne de confiance : 1) action humaine et contrôle humain, 2) robustesse technique et sécurité, 3) respect de la vie privée et gouvernance des données, 4) transparence, 5) diversité, non-discrimination et équité, 6) bien-être sociétal et environnemental, et 7) responsabilité.*

Quelles technologies et usages vous inspirent le plus d'interrogations quant au respect de ces libertés ?

Les technologies totalement automatiques, celles qui apprennent en continu (comme le chatbot Tay de Microsoft[2]). C'est-à-dire les technologies qui ne sont pas contrôlées par un être humain tout au long de leur cycle de vie.

Comment assurer l'équilibre, dans une société toujours plus imprégnée de technologies, entre les impératifs de liberté et de sécurité ?

Il faut acculturer le public sur les technologies pour qu'il puisse juger en connaissance de cause. Il faut respecter les principes de l'IA digne de confiance (indiqués ci-dessous). Il faut toujours être clair sur les objectifs visés et les moyens employés.

Le plan de régulation de la Commission européenne fournit un bon cadre de référence sur les applications « à haut risque »[3]

L'un des moyens de garantir un bon usage de ces technologies et de procéder avant tout à des expérimentations. Quelles seraient selon vous les conditions que ce cadre expérimental devrait réunir ?

Plus que les expérimentations (difficile de travailler « en vraie grandeur ») il convient de former des équipes pluridisciplinaires pour que les développeurs des applications

[1] https://digital-strategy.ec.europa.eu/en/library/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60427

[2] https://www.technologyreview.com/2018/03/27/144290/microsofts-neo-nazi-sexbot-was-a-great-lesson-for-makers-of-ai-assistants/

[3] https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-european-approach-artificial-intelligence

soient formés aux questions d'éthique et soient entourés d'experts en éthique, en droit, en sociologie. La mixité de ces équipes est également à rechercher.

*

Ce questionnaire est indicatif et ne prétend pas de couvrir l'intégralité des enjeux posés par les technologies de sécurité. La mission recueillera tout élément qui lui sera apporté afin de l'intégrer au mieux dans sa réflexion.

De l'information des citoyens & de la sécurité technique des données

L'information apportée à la société civile est fondamentale dans son acceptation des nouvelles technologies dans la sécurité publique, autant que les garanties de sécurité contribuant à un objectif de confiance.
Il conviendra sur le premier point de distinguer l'information liée à la **captation des données** : l'information issue du fait que ces données sont extraites, exploitées en temps réel ou différé selon les finalités. En ce sens il est possible de prendre appui sur le cadre administratif de la vidéoprotection pour les traitements immédiats et du cadre judiciaire pour les utilisations en temps différé.
Il faut distinguer ensuite la **protection des données extraites et utilisées**. C'est une question très actuelle mais dont la portée s'étendra par exemple aux territoires connectés. Les données seront de plus en plus importantes (en quantité) et sensibles. L'interrogation porte sur la façon de protéger les données à la fois dans le flux comme dans le stock. Il s'agit aussi de désigner les responsabilités en matière de collecte et de traitement.
En matière de sécurité, **tout développement d'une nouvelle technologie doit intégrer la sécurité et la protection des données dès la conception**. Sur les aspects techniques, le chiffrement apparaît indispensable. Pour autant, il risque d'être difficile à mettre en œuvre à l'avenir au regard de la démultiplication des données à chiffrer. Les solutions autour des blockchains présenteraient des garanties de protection mais sont également lourdes dans leur mise en œuvre. Les données ne peuvent cependant en aucun cas apparaître en clair ni ne bénéficier que de faibles garanties de sécurité.
Il est possible cependant d'envisager sur un horizon de dix ans le **quantique** en matière de protection des données qui sera alors plus répandu et donc à moindre coût.
L'autre solution complémentaire est la réponse à la question des audits pour garantir aux citoyens une exploitation loyale, basée sur le principe de la minimisation, aux finalités pertinentes et conformes avec un temps de conservation restreint au strict nécessaire.
Le ministère de l'intérieur devrait **aborder la question des données d'un point de vue basé sur les finalités et non différencier les technologies**. Un système d'IA identique peut être embarqué sur un drone ou être déployé sur des caméras fixes. Les risques diffèrent selon la finalité d'usage (et les sécurités mises en place), que l'on cherche à identifier un individu dangereux à un instant T par de la reconnaissance faciale ou que l'on veuille collecter tous les visages passant à un endroit précis sur une période donnée, le risque n'est pas le même et l'acceptabilité non plus.

L'information doit également parvenir au grand public (sauf dans le cas où elle est contraire à l'effet recherché). Sur la captation des données, toute personne doit pouvoir être informée qu'à un endroit ses données sont collectées, traitées en temps réel ou en différé. Un **affichage « loyal »** est suffisant, ni trop petit ni exagérément volumineux ; une communication par différents biais peut être menée mais surtout, il serait pertinent d'ajouter des éléments sur le site du ministère de l'Intérieur ou de **créer un site** à part entière (ce qui se révélera pertinent vu la progression des traitements de données à caractère personnel) indiquant les lieux/périodes/manifestations couverts par des nouvelles technologies de sécurité publique ainsi que les types de techs utilisées, les finalités et quels moyens pour exercer ses droits répondant à la législation en vigueur et surtout, à l'impératif de transparence induisant la confiance de la société civile.
Il conviendrait au mieux de limiter les finalités nécessitant le traitement de données personnelles à des cas très précis et sur un temps restreint. Le développement d'IA en mesure de capter des métadonnées et non des données est faisable et plus respectueux des libertés individuelles.
Il ne faudrait pas non plus tomber dans l'excès d'informations inutiles. Un site Internet dédié permettrait à une personne souhaitant davantage d'informations (qu'elle saurait où chercher d'après l'indication sur l'affichage et le logotage de certains vecteurs – inatteignables pour éviter les incivilités) de trouver facilement par simple indication du lieu par exemple, si le site

dispose bien d'une technologie susceptible d'avoir capté ses données et de formuler une demande (aux contours à déterminer).
L'information de la société civile sur leurs données personnelles est de toute évidence un problème de fond dont la solution se trouve dans l'éducation qui doit être généralisée.

Côté helvète

La France travaille sur un concept de souveraineté numérique. Il est bon de garder à l'esprit que même sur territoire européen (géographiquement parlant) tous les pays n'ont pas la même vision. La Suisse travaille par exemple non pas sur le concept de souveraineté mais d'**autodétermination numérique**. Il a d'ailleurs été adopté comme ligne stratégique 2021-2024 par le DFAE (affaires étrangères suisse). On remarque une maturité culturelle peut-être plus avancée. Ces concepts sont intéressants à plusieurs titres : protection englobant les notions de cybersécurité mais aussi de transparence citoyenne tout en permettant à l'industrie de développer de la valeur ajoutée. Une vision plutôt libérale finalement.

Existe également une théorie exprimant et explorant deux pistes. D'une part il est envisagé que dans le futur il sera criminel de récolter en masse des données de citoyens et de les exploiter tel qu'aujourd'hui cela se fait ; d'autre part il est mis en avant l'idée que détenir des données de citoyens sera trop dangereux économiquement parlant pour que cela reste un avantage à long terme (Etats exclus).

Lutte anti-drones

Légiférer pour se préparer aux événements sportifs internationaux de 2023 et 2024

« En matière de mise en oeuvre de moyens de lutte anti-drone, des outils règlementaires renforcés seront rapidement nécessaires afin de circonscrire efficacement les actes malveillants[1]. » Le nombre de drones en circulation augmente effectivement de façon exponentielle (environ vingt drones pour un avion en circulation aujourd'hui, et estimé à cinquante drones/avion d'ici 2025)[2].

Les besoins traduits par le général Cousin en avril 2020[3] visent le déploiement de « *radars qui voient le plus loin possible, une intelligence artificielle qui progresse encore, aussi bien pour la discrimination que pour la neutralisation. ».* Les outils devront aussi être en mesure de neutraliser des drones à la fois sur des distances étendues ou très réduites. Une nécessité de réponse aux défis sécuritaires posés par l'utilisation des systèmes de drones par la délinquance, criminalité et terrorisme. Des enjeux d'autant plus grands qu'approchent des grands événements en 2023 et 2024 exigeant le déploiement de nouvelles technologies de sécurité proportionnellement aux risques et menaces anticipés.

La loi dite Sécurité globale, promulguée le 25 mai 2021[4] suite à l'utilisation de l'article 45 alinéa 3 de la Constitution, partiellement censurée par la décision constitutionnelle du 21 mai 2021[5], préparait l'utilisation de drones par les forces de sécurité et pour la lutte anti-drones au cours de ces événements. En censurant certaines dispositions de l'article 47 le Conseil constitutionnel y a porté un coup d'arrêt.
Les dispositions contestées permettaient la captation et la transmission d'images concernant un nombre important de personnes (y compris leur déplacement) et, le cas échéant, sans que ces personnes ne soient informées de cette captation et transmission, portant donc atteinte au respect au droit de la vie privée.

Cette décision du Conseil constitutionnel paraît initialement incohérente au vu non seulement du projet de loi Renseignement et prévention des actes de terroriste adopté en première lecture par l'Assemblée nationale le 2 juin 2021 mais également de l'avis publié par la Direction générale de l'Armement le 2 mai dernier.[6]
L'article 12 de la loi dite Renseignement dispose en effet que « *l'utilisation par les services de l'État de dispositifs destinés à rendre inopérant l'équipement radioélectrique d'un aéronef circulant sans personne à bord est autorisée, en cas de menace imminente, pour les besoins de l'ordre public, de la défense et de la sécurité nationale ou du service public de la justice ou afin de prévenir le survol d'une zone en violation d'une interdiction prononcée dans les conditions prévues au premier alinéa de l'article L. 6211-4 du code des transports*.[7] »
L'avis publié par la DGA le 2 mai dernier est quant à lui relatif à une offre de marché public du programme PARADE (Protection déployAble modulaiRe Anti-DronEs), faisant suite au programme MILAD et visant à fournir des systèmes de lutte anti-drones aériens et à en assurer le maintien en condition opérationnelle et de sécurité. Ce système devra assurer la protection permanente et à 360° de sites militaires ou civils situés en France ou sur des théâtres d'opération extérieurs « *par tous les temps, jour et nuit* ».
Les drones de sécurité publique développés depuis plusieurs années risquent donc de se voir cloués au sol pour la Coupe du monde de rugby en 2023 et les Jeux Olympiques en 2024 sans proposition adéquate et proportionnelle au regard des finalités.

---

[1] Colonel Jean-François Morel, chargé de mission auprès de la Direction des opérations et de l'emploi de la gendarmerie
[2] *https://hologarde.com/menace/?lang=fr*
[3] *https://www.air-cosmos.com/article/focus-sur-la-lutte-anti-drones-22960*
[4] *https://www.legifrance.gouv.fr/dossierlegislatif/JORFDOLE000042563668/*
[5] *https://www.conseil-constitutionnel.fr/decision/2021/2021817DC.htm*
[6] *https://www.boamp.fr/avis/detail/21-58142/3*
[7] *https://www.assemblee-nationale.fr/dyn/15/textes/l15b4104_projet-loi#D_Article_12*

Un rapport d'information parlementaire déposé le 17 juillet 2019 par la commission de la défense nationale et des forces armées sur l'action aérospatiale de l'Etat[8] fait état des difficultés et des attentes du secteur en proposant de regrouper sous la conduite du SGDSN l'ensemble des acteurs de la défense aérienne afin de construire une capacité de lutte anti-drones cohérente et partagée au niveau interministériel.
La sûreté aérienne étant un défi majeur à relever, notamment au cours des événements à venir, le Commandement de la défense aérienne et des opérations aériennes (CDAOA) jouera un rôle prépondérant en matière de lutte anti-drones. Une convention de cinq ans signée en mai 2021 avec le Cnes et le groupe ADP (gestionnaire des aéroports de Paris-Orly et Roissy Charles De Gaulle) vise à partager capacités et experiences ainsi que le développement du système de detection Hologarde.
Outre le ministère des Armées, quatre acteurs étatiques sont impliqués : le ministère des Affaires étrangères, l'Intérieur, les douanes et les Transports à travers la DGAC. Les DPSA (Dispositif particulier de sûreté aérienne) et la lutte anti-drones (LAD) entrent pleinement dans leur mission de sûreté aérienne et sont donc au cœur des systèmes de sécurité envisagés pour 2023-2024. Leur système devrait d'ailleurs être interopérable avec le programme PARADE.
La décision constitutionnelle n'a pas pour vocation d'empêcher tout développement ou déploiement. C'est au contraire une reconnaissance des enjeux portés par la question du vecteur drone et de ses systèmes embarqués. Il s'agit d'exiger des garanties d'usage explicites, fondées, cadrées et proportionnelles aux atteintes que porteraient ces systèmes aux libertés individuelles.

L'exemple russe lors de la Coupe du monde de 2018 donne un éclairage sur les mesures de lutte anti-drones prises à l'étranger. Plusieurs mois avant le début de la Coupe, la Russie a mis en place des unités chargées du brouillage électronique autour des stades. Un usage déjà en vigueur en Syrie ou dans l'est de l'Ukraine et rendant impossible des éventuelles attaques par drone. Ce vecteur peut embarquer plusieurs kilos de TNT aisés à faire exploser à distance. Les unités de guerre électronique de la défense russe ont ainsi utilisé dans leur lutte anti-drones la station de contrôle technique « Svet-KU », la station automatisée de brouillage « Jitel » ainsi qu'environ soixante systèmes portatifs de protection radioélectronique « Arbalet ». Selon l'analyste Samuel Bendett[9], le succès de la défense anti-drone russe, fort de ses expériences en Syrie ou en Ukraine, se résume en trois points clefs : des radars perfectionnés capables de détecter de petits appareils à basse altitude, des brouilleurs électroniques et des missiles anti-aérien qui peuvent facilement cibler des engins de petite taille.

Bien que pour des raisons évidentes de sécurité il soit difficile de trouver des informations plus précises sur la sécurité anti-drones pour les JO de 2021, le Japon a promulgué des lois interdisant de faire voler des drones au-dessus des sites olympiques et légifère davantage dans le domaine du drone civil pouvant sous-entendre une avancée plus marquée en matière de sécurité publique.
La France semble être techniquement prête à déployer des mesures technologiquement supérieures à celles mises en place lors de l'Euro 2016. Les progrès des industriels ont été suivis de près, entre le système de CS Group mêlant plusieurs outils anti-drones ou le fusil anti-drones Chimera de la start-up Cerbair.
Il ne reste qu'à permettre aux forces de sécurité d'user de moyens de lutte anti-drone dans le respect des droits fondamentaux des personnes concernées en matière de vie privée et en vertu de l'article 34 de la Constitution, seule une loi peut légiférer sur un tel sujet.
Déterminer précisément les modalités d'utilisation du drone et de la caméra aéroportée, avec la fixation d'un délai maximal d'utilisation ainsi que d'un périmètre déterminé pourrait suffire à en autoriser l'usage.
Un point d'importance concerne également les contours des « dérogations » d'information au public selon les finalités visées.

---

[8] *https://www.assemblee-nationale.fr/dyn/opendata/RINFANR5L15B2166.html#_Toc256000050*
[9] *https://www.defensenews.com/opinion/commentary/2021/05/23/russias-real-world-experience-is-driving-counter-drone-innovations/*

Dans le respect des normes européennes et des conditions posées par le Conseil constitutionnel, les enjeux sécuritaires d'un événement comme la Coupe du monde de rugby 2023 et les Jeux Olympique 2024 nécessitent une adaptation législative et réglementaire rapide. Il pourrait s'agir d'un régime dérogatoire pour des événements à partir d'un certain nombre de personnes, en plein air.

L' « intelligence artificielle » au service de la sécurité publique

Synthèse

Constat

- Multitude de travaux publiant livres blancs, recommandations ou lignes directrices concentrés sur l'éthique de l'IA ;
- Absence de législation encadrante claire sur le développement et le déploiement des systèmes d'IA ;
- Craintes des acteurs judiciaires à l'égard des algorithmes (ex. du Conseil constitutionnel à travers les conditions d'exception énoncées à l'interdiction du profilage et qui a pointé indirectement la responsabilité des concepteurs dans l'explicabilité de ces décisions → tournant législatif) ;
- Domination des acteurs privés & publics à étrangers, développant les IA sans freins et utilisant les données publiques des français avec leur consentement mal éclairé ;
- Règlement européen à venir.

Enjeux

- Assurer la sécurité publique des grands événements sportifs 2023-24 au regard des nouvelles menaces ;
- Les données sont l'enjeu principal en matière d'IA : il faut reprendre la main ;
- Rééquilibrer le rapport de force avec un ennemi devenu protéiforme et parfaitement à l'aise avec les nouvelles technologies ;
- Risque de perte des compétences souveraines au profit des acteurs privés technologiquement plus avancés ;
- Adéquation des réponses des forces de l'ordre par l'élargissement et la rapidité de leurs capacités d'intervention en assurant leur propre sécurité, devenue elle aussi un enjeu fondamental ;
- Développer & soutenir l'innovation et la recherche française pour répondre aux enjeux politiques, économiques et technologiques du XXIème siècle ;
- Assurer le haut niveau technologique de la France sous couvert de fortes garanties pour la protection des droits fondamentaux.

Freins

- Problématiques financières & administratives engageant un « jeu de priorités » dans la sécurité ;
- Difficultés d'accès aux données par les chercheurs ;
- Méconnaissance des législateurs sur les systèmes d'intelligence artificielle ;
- Défiance de la société civile à l'égard de l'IA tenant à son manque de transparence et d'information ;
- Excès de travaux autour de l'éthique mais législation inadéquate au regard des enjeux ;
- Sécurité numérique des données traitées mais législation en la matière plutôt suffisante ;
- Risques de légiférer sur de mauvais fondements et finalités → perte de temps.

Propositions

- L'exploitation de données captées à des fins de *machine learning* dans le but de créer une intelligence artificielle de prévention des troubles à l'ordre public peut se justifier par un intérêt supérieur à l'atteinte possible à la vie privée des personnes concernées ;
- Mise en place de zones de libres d'expérimentation couplée à la consolidation du cadre juridique pour combler les « angles morts » démocratiques de mise en œuvre de systèmes d'IA de sécurité publique ;
- Faire des événements sportifs 2023-24 le cadre d'expérimentations de nouvelles technologies avant implémentation ;
- Développer les IA d'analyse comportementale, beaucoup moins intrusive que la reconnaissance faciale car anonyme ;
- Disposer et conserver – notamment à travers le maintien en poste des personnes compétentes – un haut niveau d'expertise en interne pour continuer à développer l'algorithme, à partir d'une architecture de base modelable potentiellement fournie par le privé ;
- Législation centrée sur l'humain et non la nature de la technologie dont les progrès ne sont pas toujours anticipés (ex : loi Godfrain de 1988) ;
- Mise en place d'une politique de transparence fondamentale pour favoriser l'acceptabilité de la société civile (« l'explicabilité de l'IA ») et favoriser son implication à différentes échelles ;
- Maintenir un contrôle humain aux étapes sensibles de prise de décision ;

Le 7 juin 1954 Alan Turing décédait à Wilmslow. Il a posé les bases scientifiques de l'informatique, grandement contribué à la victoire de 1945, impulsé ce que nous appelons « intelligence artificielle », et laisse une question qui n'a pas pris une ride 67 ans plus tard : « Les machines peuvent-elles penser ? » La seule définition de l'intelligence n'étant elle-même pas universelle, celle de l' « intelligence artificielle » (IA) non seulement ne l'est pas non plus, mais évolue aussi rapidement que ses usages, sa nature et ses objectifs. Pour en définir les contours, l'IA s'entendra dans ce rapport comme l' *« ensemble de sciences, théories et techniques (notamment logique mathématique, statistiques, probabilités, neurobiologie computationnelle, informatique) dont le but est de reproduire par une machine des capacités cognitives d'un être humain*[1]*. »* Le développement de cette discipline et de ses usages est étroitement lié à celle de l'informatique, amenant les ordinateurs à réaliser des tâches de plus en plus diverses et complexes auparavant réalisées par des humains. L'intelligence artificielle fait l'objet d'une distinction très actuelle entre l'IA connexionniste et l'IA symbolique. La première est incarnée par le *machine learning*, un apprentissage autonome supervisé ou non par un humain. La seconde est le *deep learning* (apprentissage profond) et répond à la formalisation et l'exécution d'un raisonnement basé sur des règles précises et fonctionne par bio-mimétisme, reproduisant le système neuronal humain. Cette dernière semble être mieux comprise mais donne parfois de moins bons résultats que l'IA connexionniste, qui ne permet pas toujours de comprendre comment elle en est arrivée à obtenir ce résultat, aussi précis et pertinent soit-il.
L'IA se distingue également en trois catégories : « faible », « modérée » ou « forte ». Cette dernière n'a pas encore été matérialisée, hormis dans la science-fiction, mais nécessiterait des progrès en recherche fondamentale - qui sont à notre portée - pour répondre à la règle de l'univers cybernétique où la réalité est vouée à dépasser la fiction. L'IA « forte » serait *« en capacité de contextualiser des problèmes spécialisés très différents de manière totalement autonome, […] de modéliser le monde dans son ensemble*[2]*. »* Or c'est une problématique centrale visant une automatisation aboutie qui n'est pas à confondre avec l'autonomisation. L'autonomisation totale est un risque majeur dont les premiers écueils viennent d'être rapportés par un groupe d'expert du Conseil de sécurité de l'ONU sur la Lybie. Un drone armé autonome de fabrication turque KARGU-2 aurait engagé différentes cibles, et abattu sans en avoir reçu l'ordre un soldat battant en retraite en mars 2020. Le rapport qualifie cet état de fait comme une *« prise d'initiative effrayante »*. Une initiative de l'IA embarquée par le vecteur drone qui semble confirmer les craintes soulevées par les usages de systèmes « trop » autonomes. Le développement comme l'usage d'IA dans la sécurité reste contextuellement indispensable mais souffre aussi de nombreux freins. Cela nécessite tout d'abord un cadre clair définissant des contours répondant aux enjeux de l'IA dans ce domaine. En ce sens le projet de règlement de la Commission européenne permet une avancée considérable.

Les systèmes d'IA visant l'autonomie tel celui du KARGU-2 sont développés et utilisés par des pays juridiquement moins protecteurs. En Europe, d'autres systèmes autonomes existent aussi, à l'instar du système Skeyetech, premier drone autonome homologué sur le territoire européen, non armé bien entendu. Cette IA a été développée pour « renforcer la sécurité des sites sensibles » et permet aux forces de sécurité de gagner en temps et en sécurité par la fourniture d'images instantanées et la détection d'événements anormaux. Une nouvelle technologie utilisée dans de nombreux domaines répondant à l'une des particularités de l'intelligence artificielle. Quelle que soit la première application d'une IA, du point de vue technologique elle est parfaitement transférable à d'autres applications. Exemple des IA développées pour la défense, tout à fait transférable à la sécurité[3]. Les points de convergences sont nombreux, principalement sur le traitement de l'information : analyse d'images, vidéos ou de sons. Au-delà de la convergence, les IA de sécurité, à l'instar de celles de défense, *« nécessitent bien sûr une déclinaison opérationnelle plus précise qui prenne en compte leurs singularités*[4]*. »*

1 Définition du Comité ad hoc sur l'intelligence artificielle (CAHAI)
2 Conseil de l'Europe, Histoire de l'intelligence artificielle (https://www.coe.int/fr/web/artificial-intelligence/history-of-ai)
3 Cédric Villani, Donner un sens à l'intelligence artificielle, Focus 5, mission parlementaire, 2017-2018
4 Ibid.

C'est en ce sens qu'il faut aborder les nombreuses questions posées par l'usage des intelligences artificielles dans la sécurité : dans un premier temps, en établissant un constat relatif aux enjeux de cet usage devenu nécessaire par les forces de sécurité intérieure, mais qui apportent dans un second temps des gains indéniables en matière de sécurité pour la société civile. Les risques persistent néanmoins et exigent une législation adéquate ainsi que des limites éthiques au-delà du textuel.

Actuellement un constat clair démontre que les intelligences artificielles sont développées à l'étranger, par des Etats et des collectivités amis ou ennemis, ou par des groupes criminels. Leurs freins ne sont pas les nôtres, et le déploiement de ces IA ne répond pas à nos propres règles éthiques ou en matière législative. Les dérives commencent à émerger alors même que les IA « fortes » n'existent pas encore, à l'instar du système de drone armé autonome turc précédemment cité ayant pris seul une décision d'attaque, tuant un être humain. Autrement, les dérives concernent largement le droit à la vie privée. Des Etats autoritaires développent des IA pour le contrôle de la population civile, voire l'élimination d'une partie de cette population. En France et en Europe, la recherche en intelligence artificielle fait l'objet d'une quantité très importante de Livres blancs, chartes, recommandations et lignes directrices où il est facile de se perdre. Il n'y a cependant pas encore de législation sur le développement et le déploiement de ces systèmes, global ou appliqués à la sécurité, mais un projet de règlementation européenne vient d'être présenté le 21 avril par la Commission européenne.

Les dérives existantes ou envisagées se traduisent en freins à plusieurs niveaux. Notamment, on observe un paradoxe entre protection des libertés fondamentales limitant strictement l'utilisation des données et manque réel de contrôle des technologies venant de l'étranger. Utiliser des systèmes d'intelligence artificielle étrangers[5] présente une sérieux problème en termes de souveraineté, mais aussi un manque de contrôle sur ladite technologie. L'IA est évolutive ; il s'agit de pouvoir la « régler », l'améliorer, ce que ne permettent pas les logiciels étrangers. *In fine*, les risques en matière de protection des libertés publiques et individuelles, voire de sécurité nationale, en sont accrus. L'histoire a démontré que disposer d'une technologie inférieure à celle d'Etats étrangers expose à des menaces que les nouvelles technologies d'ailleurs rendent encore plus dangereuses. Le mythe des cavaliers polonais chargeant sabre au clair les chars allemands au début de la Seconde Guerre mondiale illustrant la propagande de supériorité technologique de l'Allemagne nationale-socialiste, pourrait devenir une réalité si face à une armée de robots chinois, l'Europe présente une armée humaine. La France ne peut se permettre de perdre le contrôle des données de ses citoyens au profit de Puissances étrangères ni de recourir à de tels systèmes d'IA pour assurer la sécurité publique. De même, l'état actuel du rapport de force entre les forces de l'ordre et les groupes criminels/terroristes ou individus dangereux utilisant – illégalement – ces systèmes, exige un retournement de situation au plus tôt et un soutien technologique pour toute intervention de nature à mettre des personnes civiles ou des agents en danger.

L'intelligence artificielle et la sécurité est un enjeu de souveraineté. Mais en matière de développement et déploiement des systèmes d'intelligence artificielle, la sécurité ne se dissocie pas des autres sphères d'utilisation. Il est préférable de faire la distinction par types d'applications fonctionnelles. Cognilytica en présente sept[6] :

- L'hyperpersonnalisation : la génération d'un profil individuel notamment utilisé à des fins de recommandation et de ciblage ;
- La reconnaissance : l'utilisation de l'IA pour structurer de l'information (images, texte, audio, etc.) et pour y identifier des éléments particuliers ;

[5] Israéliens par exemple, tel le logiciel Any Vision en matière de reconnaissance faciale visant des présupposés « fichés S » à Nice lors d'une expérimentation en 2019

[6] Chaire transformations de l'action publique, séminaire « algorithmes, intelligence artificielle et monde public » séance 2 – prospective des grandes fonctions de l'intelligence artificielle (IA) et de ses usages (18 novembre 2020)

- La conversation et l'interaction avec l'humain : permettre aux machines d'interagir avec des humains de la même manière que ceux-ci interagissent entre eux, que cela soit à travers des formes écrites ou parlées ;
- Analyses prédictives : qui ont pour objectif principal d'aider les humains à prendre des décisions ;
- La détection de constantes et d'anomalies : où il s'agit, pour des ensembles de données, d'identifier des schémas constants ou de cibler des éléments anormaux ;
- Les systèmes autonomes : la conception de systèmes capables d'effectuer des tâches ou d'interagir avec leur environnement tout en minimisant l'intervention humaine ;
- Les systèmes tournés vers des objectifs précis (goal-driven) : dont l'objectif principal est de trouver la solution optimale à un problème donné (e.g. simulation de scénarios, etc.).

Si les sphères d'usages se confondent, une forte problématique concerne la domination des acteurs privés. Les conséquences dans le domaine de la sécurité sont et seront majeures, « génératrice d'un transfert d'activités régaliennes des États vers les géants du numérique[7]. » Le contrôle de la donnée est central, les entreprises privées ont des objectifs naturels de rentabilité, tandis que la sécurité publique n'en a qu'un, éponyme. Le développement des systèmes d'IA est ainsi crucial ; les données sensibles qui devraient nécessairement y être traitées seront soumises aux mêmes garanties qu'actuellement et contrôlées par le cadre administratif ou le cadre judiciaire. La confiance est une clef du développement des IA. Bénéfiques à l'humanité, en cas d'absence de contrôle ou de détournement, elles représentent une menace à anticiper sous deux angles : la continuité du service et de la capacité à agir/réfléchir. Une trop forte dépendance à ces systèmes priveraient les services de sécurité d'une partie de leurs capacités opérationnelles, les fragilisant nécessairement.

Développer l'IA implique de la comprendre et de la maîtriser tout en réservant les capacités décisionnelles aux humains, un enjeu majeur pour les forces de sécurité intérieure. Prévenir la délinquance, identifier les auteurs d'infractions, détecter des failles sur les systèmes d'informations, etc. Il s'agit bien d'offrir un niveau de sécurité accepté et acceptable par la société civile sans verser dans le contrôle disproportionné des citoyens. Ceux-ci ont des craintes justifiées exprimées par des décideurs ne comprenant pas l'intelligence artificielle et à la fois utilisant le terme d'éthique à l'extrême tout en menant une course à l'IA. La compréhension de celle-ci par ceux qui légifèrent, développent ou gèrent des programmes liés est primordiale. Les débats sont *« souvent plus idéologiques qu'éthiques pour interdire la reconnaissance faciale ou l'emploi de méthodes prédictives[8]. »* Il existe bien un cadre légal relatif aux données s'il ne l'est pas à l'IA. Ces données doivent rester sous le contrôle des forces de sécurité qui devraient obtenir les moyens de les utiliser dans le cadre d'expérimentations, à la fois pour connaître les perspectives comme les limites : *« l'IA ne peut être une boîte noire utilisée par les forces de l'ordre, elle est au cœur des enjeux de souveraineté et doit être envisagée comme le vecteur de la transformation capable d'appréhender, de comprendre et d'anticiper les nouvelles menaces sécuritaires. Mais pour pouvoir développer des applications, les évaluer, les confronter aux enjeux éthiques et en mesurer les limites, il faut aussi pouvoir travailler sur des données réelles, des données sensibles et disposer de moyens de calcul[9].* » En ce sens et comme préconisé par Cédric Villani dans son rapport « Donner du sens à l'intelligence artificielle : pour une stratégie nationale et européenne », il est nécessaire de faire émerger des « bacs à sable » d'innovation et développer une politique de la donnée spécifique à chaque sphère ou secteur.

La législation sur les données existe. Certains accès devraient cependant être facilités pour des expérimentations avant implémentation. Le manque de données ou des données biaisées sont un risque que ne peut prendre la recherche dans la sécurité publique en matière d'IA. Joy Buolamwini, chercheure au MIT, a mis en lumière les biais discriminatoires des IA de

[7] Colonel Patrick Perrot, coordonnateur pour l'IA à la Gendarmerie Nationale, Institut Sapiens, « Intelligence artificielle et sécurité, un enjeu de souveraineté », 6 mai 2021
[8] Ibid.
[9] Ibid.

reconnaissance faciale développées par les GAFA. Elle propose en ce sens le « code inclusif » qui limiterait les discriminations et les erreurs à l'instar de Nijeer Parks, cet américain noir qui a passé une semaine en prison à cause d'une erreur du logiciel de reconnaissance faciale en 2020[10]. Il faut cependant rappeler que l'IA n'est pas « pensante » et si les biais sont dans la base de données, elle les accentuera. Un contrôle humain (l'IA ne doit être qu'un appui complémentaire) et une amélioration continue doivent être des lignes directrices, l'IA n'est qu'un *« problème mathématique*[11] ». Toute législation en matière d'IA est appelée à prôner la transparence, clef de l'acceptabilité par la société civile. A noter que *« l'IA ne manque pas tant de transparence que d'humains capables de la comprendre. Alors certes, nous ne comprenons pas complètement le poids attribué à chaque connexion neuronale, mais cela ne nous empêche pas de connaître le niveau de performance d'un système automatique à travers ses taux de faux rejets et de fausses acceptations. C'est là que doit se situer la transparence, à l'accessibilité au niveau de performance des systèmes pour chaque base de données exploitée*[12]. » Une transparence et une éthique que font émerger les travaux de certains groupes de travail produisant des travaux essentiels en ce sens tel le Comité ad hoc sur l'intelligence artificielle[13] (CAHAI) donnant des orientations à l'intention des législateurs et décideurs, insistant sur la licéité (par exemple, *« le traitement de catégories particulières de données, telles que les données biométriques, n'est autorisé que s'il repose sur une base juridique appropriée et si des garanties complémentaires et appropriées sont inscrites dans la loi nationale »*) ou le cadre juridique pour chaque utilisation : explication détaillée de l'utilisation spécifique et de la finalité poursuivie, fiabilité minimale et la précision de l'algorithme employé, durée de conservation des photos utilisées, possibilité de contrôler ces critères, traçabilité du processus, garanties. Les limitations strictes de certaines utilisations par la loi, l'implication nécessaire des autorités de contrôle, la certification des IA utilisées par les services de sécurité ou la sensibilisation de chaque élément de la chaîne. Les lignes directrices sur l'intelligence artificielle et la protection des données[14] donnent également des éléments d'orientation à l'intention des législateurs et décideurs. De la confiance dans les produits et services de l'IA à travers le respect du principe de la responsabilité des développeurs en IA, l'adoption de procédures d'évaluation des risques et la mise en œuvre d'autres mesures appropriées. Les autorités de contrôle devraient également bénéficier de ressources supplémentaires pour accentuer les contrôles sur les programmes de vigilance algorithmiques des développeurs, fabricants et prestataires de service en IA. Le principe de limitation de la dépendance aux IA est aussi abordé ainsi que la nécessité d'impliquer la société civile et toute partie prenante *« dans le débat relatif au rôle que l'IA devrait jouer […] dans les processus décisionnels les affectant. »*

Dans la spécificité des forces de sécurité intérieure, le cas d'Israël donne un éclairage. La question des métiers nécessaires au développement des systèmes d'intelligence artificielle les plus impartiales possibles au sein même du service se pose. Une question dont nous devons nous saisir pour rester dans le cadre dans le cadre règlementaire applicable. La police israélienne diffère fondamentalement des autres agences de sécurité d'Israël. Ses opérations restent règlementées par un cadre légal garanti par la haute cour de justice et l'activité des tribunaux, une réglementation qui ne s'oppose pas au développement des IA. Israël fait partie des Etats les plus avancés en ce qui concerne la recherche sur l'IA à des fins de sécurité publique. Ces usages couvrent cinq catégories : la reconnaissance faciale ; l'analyse vidéo (algorithmes d'identification des personnes et des objets) ; la police prédictive (analyse des réseaux sociaux et lutte contre l'anonymat des cybercriminels) ; l'utilisation de robots et la lutte contre les crimes non-violents (fraudes, abus, …). Pour l'Etat hébreu comme pour la France, la première percée scientifique modifiant durablement les méthodes d'investigation et nécessitant une adaptation de la législation a été le test ADN. Selon Lior Rokach,

[10] https://www.01net.com/actualites/un-homme-arrete-et-incarcere-apres-une-reconnaissance-faciale-erronee-attaque-en-justice-2026023.html
[11] Colonel Patrick Perrot, coordonnateur pour l'IA à la Gendarmerie Nationale, « Faut-il avoir peur de l'IA ? », Parole d'expert, CyberCercle, mars 2021
[12] Ibid.

[13] https://www.coe.int/fr/web/artificial-intelligence/cahai-1
[14] https://rm.coe.int/lignes-directrices-sur-l-intelligence-artificielle-et-la-protection-de/168091ff40

directeur du centre de la criminologie computationnelle (partenariat entre la police israélienne et l'université Ben Gourion du Neguev), nous serions au seuil de la prochaine grande percée scientifique : « l'analyse des *big data* pour découvrir des modèles cachés aux fins de prédire puis prévenir la criminalité[15]. »
En Europe, la très proposition de règlementation présentée par la Commission européenne le 21 avril 2021 semble être le socle sur lequel les pratiques et mesures devront être basées. Elle insiste sur la confiance et distingue les systèmes d'IA en « risques inacceptables », « haut risques », « risques limites », « risques minimes ». Elle exclut donc tout d'abord les systèmes de notation sociale dans les Etats et rappelle que sont considérées à haut risques les technologies d'IA utilisées dans le domaine du maintien de l'ordre, susceptibles d'interférer avec les droits fondamentaux des personnes (par exemple, la vérification de la fiabilité des éléments de preuve). S'agissant de la gouvernance, la Commission propose que les autorités nationales compétentes de surveillance du marché veillent au respect des nouvelles règles dont la mise en œuvre sera facilitée par la création d'un comité européen de l'intelligence artificielle. La proposition prévoit des « bacs à sable réglementaires » afin de faciliter l'innovation responsable. Concernant les usages de l'IA en matière de sécurité, la Commission rappelle l'interdiction de l'utilisation des systèmes d'identification biométriques fondés sur l'IA dans l'espace public et en temps réel à des fins de maintien de l'ordre, hors exceptions strictement encadrées (enfant disparu, menace terroriste spécifique et imminente, détecter, localiser, identifier ou poursuivre l'auteur ou le suspect d'une infraction pénale grave).

Les risques pour les droits fondamentaux relevés par la Commission européenne et les groupes de travail dédiés comme le CAHAI sont réels et constituent un point de vigilance central mais dont les garanties devraient être adaptées la recherche, au moins interne aux forces de sécurité qui ne peuvent partager des données de travail sensibles à des organismes voués à rendre leurs recherches publiques à l'instar des universités. Développer des systèmes d'IA ne signifie pas les déployer. La souveraineté française et la sécurité nationale dépendent de la capacité de la France à se positionner à l'échelle internationale sur ces questions en répondant aux enjeux de fiabilité à travers l'efficacité effective de ces systèmes, de maintien du contrôle humain et de la sécurité dans l'usage. L'acceptabilité de la société civile restera tributaire de ces clefs de confiance. Cette sécurité dans l'usage doit être couplée à une forte sécurité numérique et une cybersécurité efficace et résiliente pour prévenir notamment des violations de données et des vols/détournements d'usage des IA.

En conclusion de ce rapport, il semble que le développement et le déploiement des systèmes d'intelligence artificielle sont inévitables et même nécessaires à la conduite de la mission des forces de sécurité intérieure. A ceci près que le retard accumulé sur ces deux points face au secteur privé et aux Etats étrangers place la France et l'Europe dans une situation dangereuse sur les plans politiques, économiques et sécuritaires. Il s'agit donc de développer les IA dans des zones d'expérimentation libres, de préférence en interne et d'encadrer leur éventuel déploiement en fonction d'une identification précise des besoins. La recherche et le déploiement devront faire preuve de transparence en tenant compte des particularités du *machine learning*. L'acceptation est également nécessaire dans l'autre sens : il s'agit d'admettre que les systèmes d'IA d'auto-apprentissage – plus efficaces que le *deep learning* dans certains domaines – donnent des réponses dont nous ne comprenons pas le cheminement qui y a conduit. Il faut également accepter que les IA fassent des erreurs et en feront toujours. La question de la responsabilité devra s'y pencher, même si l'IA produit par exemple moins de 1% d'erreur, elles sont moins tolérées qu'un humain en produisant 20%. Les systèmes d'intelligence artificielle ne sont que des mathématiques réalisées par des êtres humains, avec leurs biais et leurs erreurs, et parce qu'elles ne sont que cela, elles ne doivent jamais franchir la barre de l'autonomie totale (dont là encore, le curseur doit être placé) et rester perpétuellement sous un contrôle humain.
L'intelligence artificielle doit être développée, pensée et utilisée en fonction des finalités poursuivies, comme toute nouvelle technologie. Catégoriser, légiférer ou dessiner une doctrine d'emploi par

[15] Rebecca Stadlen Amir, « Israeli lab uses AI and big data to fight cyber crime », Israel21c, 18 mars 2018

technologie et non par finalité est une erreur qui se heurtera aux progrès à venir dont la portée est encore sous-estimée. Nous ignorons tout des technologies qui feront notre quotidien dans vingt ans. Encore une fois, Etats et collectivités alliés ou ennemis, criminels ou terroristes, n'ont aucun frein ni dans le développement ni dans l'usage de l'intelligence artificielle. La France doit être en mesure à la fois d'anticiper les bonds technologiques, d'en être à l'origine plutôt que les subir, et d'assurer la mission qui est la raison d'être de l'Etat : la sécurité de ses citoyens.

Différencier les finalités, propulser la recherche et le développement, encourager les expérimentations et encadrer fermement leur déploiement est ce qui fera de la France le leader européen en matière de nouvelles technologies.

Réflexions européennes et législation à venir en matière de réglementation de l'intelligence artificielle

Par Bertille Vallet

« En matière d'intelligence artificielle, la confiance n'est pas un luxe mais une nécessité absolue. »[16] Si l'intelligence artificielle (IA) figure parmi les trois priorités de la stratégie européenne pour une économie numérique et résiliente[17], une certaine confusion règne au sein des débats actuels à l'échelle européenne selon Cécile Crichton[18] : confusion entre algorithme et intelligence artificielle[19] ou encore manque de consensus international sur la définition de l'intelligence artificielle reconnu par le projet de livre blanc de la Commission européenne[20].

Les livres blancs, chartes, recommandations et lignes directrices sont très nombreux. Ces travaux sont produits par de nombreuses instances, conseils et comités : pour le seul Conseil de l'Europe, dix instances (d'expertes ou consultatives) s'intéressent et publient des recommandations à ce sujet, dont le fondamental Comité ad hoc sur l'intelligence artificielle (CAHAI)[21]. Il y a également le Conseil de l'Union européenne, la Commission Européenne comprenant six instances différentes [22]. Enfin, le Parlement européen, l'Autorité de marché et de sécurité européenne (ESMA), l'*European Union Agency for Cybersecurity* (ENISA), la *Fundamental Rights Agency* (FRA), ainsi qu'*Eurocontrol* et *Europol* sont également à l'origine de plusieurs travaux au sujet de l'intelligence artificielle. Le CAHAI a recensé les initiatives sur l'IA au sein d'une data visualisation très complète accessible au grand public.[23] L'Union européenne est en effet la zone géographique la plus prolifique en matière de recommandations et réglementations.[24] Ainsi, entre les années 2017 et 2021 sont dénombrés plus de 110 documents d'orientation, lignes directrices et études.

Sur l'IA il n'existe pas de texte juridiquement contraignant à l'échelle européenne. Le principal appui se fait par le biais des traitements de données dont la convention 108 (devenue la C108+) en est le socle. Les 47 Etats membres du Conseil de l'Europe, de même que Maurice, le Sénégal, la Tunisie, l'Argentine, le Cap-Vert, le Mexique et le Maroc et l'Uruguay, sont Parties à la « Convention 108 »; le Burkina Faso a été invité à y adhérer[25]. L'idée à retenir est que de nombreux Etats hors Europe utilisent les fondements la Convention pour l'élaboration de nouvelles lois sur la protection des données, s'approchant de l'harmonisation avec la règlementation européenne elle-même basée dessus ainsi que de la directive abrogée 95/46/CE.[26]

En 2020, le Parlement Européen a adopté trois résolutions de recommandations à la Commission européenne en matière d'intelligence artificielle, de robotique et de technologies connexes : en matière d'éthique, de responsabilité civile et de propriété intellectuelle, n'ayant aucune force contraignante mais permettant d'avoir un aperçu sur la position européenne en matière d'IA.[27] La très récente proposition de règlementation présentée par la Commission européenne le 21 avril 2021 semble être l'avenir pratique de ces résolutions.

---

[16] Margrethe Vestager, vice-présidente exécutive pour une Europe adaptée à l'ère du numérique
17 Ursula Van der Leyen , discours du Conseil Spécial, 2 octobre 2020
[18] https://www.dalloz-actualite.fr/flash/union-europeenne-et-intelligence-artificielle-etat-des-propositions#.YLaWiZMzZQI
[19] https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/IMCO/DV/2020/01-22/RE_1194746_EN.pdf
[20] https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/IMCO/DV/2020/01-22/RE_1194746_EN.pdf
[21] Autres instances : CDCJ, CEPEJ, la Commission pour les droits humains, le Comité des ministres, le comité consultatif de la convention. 108, DG1 et la Commission de Venise, l'ECRI, Eurimages, observatoire audiovisuel européen, MSI-AUT, MSI-NET, MSI-REF, l'assemblée parlementaire du Conseil de l'Europe
[22] AI HLEG, observatoire de l'AI, le groupe d'expert sur la responsabilité civile et les nouvelles technologies, le groupe européen sur l'éthique dans les sciences et les nouvelles technologies, le Comité économique et social européen (EESC), EDPS
[23] https://www.coe.int/fr/web/artificial-intelligence/national-initiatives
[24] https://www.cognilytica.com/2020/02/14/worldwide-ai-laws-and-regulations-2020/
[25] https://www.coe.int/fr/web/conventions/full-list/-/conventions/treaty/108/signatures
[26] Communiqué de presse du protocole d'amendement (STCE n°223) à la Convention pour la protection des personnes à l'égard du traitement automatisé des données personnelles (STE n ° 108)
[27] https://www.europarl.europa.eu/doceo/document/TA-9-2020-0275_FR.html

Dans le communiqué de presse, la commission européenne insiste sur la confiance : elle distingue les technologies d'IA en « risques inacceptables », « haut risques », « risques limites », « risques minimes.
Elle exclut donc tout d'abord les systèmes de notation sociale dans les Etats puis rappelle que **sont considérées à haut risques les technologies d'IA utilisées dans le domaine du maintien de l'ordre**, susceptibles d'interférer avec les droits fondamentaux des personnes (par exemple, la vérification de la fiabilité des éléments de preuve). Ces systèmes devront être fiables afin de traiter toute incohérence, de résister à une attaque en apportant des décisions protégeant l'utilisateur. A ce titre, il a été proposé dans le livre blanc d'**adapter la charge de la preuve aux** victimes afin de responsabiliser l'opérateur.
S'agissant de la gouvernance, la Commission propose que les autorités nationales compétentes de surveillance du marché veillent au respect des nouvelles règles dont la mise en œuvre sera facilitée par la **création d'un comité européen de l'intelligence artificielle.** La proposition prévoit des *« **bacs à sable réglementaires** »* afin de faciliter l'innovation responsable.

Concernant les usages de l'IA en matière de sécurité, la Commission rappelle l'**interdiction de l'utilisation des systèmes d'identification biométriques fondés sur l'IA dans l'espace public** et en temps réel à des fins de maintien de l'ordre, hors exceptions strictement encadrées (enfant disparu, menace terroriste spécifique et imminente, détecter, localiser, identifier ou poursuivre l'auteur ou le suspect d'une infraction pénale grave).

Le Comité ad hoc sur l'intelligence artificielle a adopté un rapport sur la faisabilité relative à un cadre juridique pour la création, le développement et l'application de l'IA sur la base des normes du Conseil de l'Europe le 17 décembre 2020. Selon ce rapport, *« le risque de voir les systèmes d'IA faciliter ou amplifier des biais injustes »,* comme indiqué plus haut, *« peut constituer une menace pour le droit à la liberté et à la sûreté, combiné au droit à un procès équitable (art. 5, 6 et 7 CEDH), lorsque ces systèmes sont utilisés dans des situations susceptibles de mettre en jeu la liberté physique des individus ou la sûreté de la personne (domaines de la justice et du maintien de l'ordre par exemple).* [28] »

Le futur règlement européen, pris sur le fondement du projet de règlementation publié par la Commission européenne le 21 avril 2021, donnera ainsi le premier cadre juridique aux utilisations de l'IA en matière de sécurité. Ce droit vertical serait complété par un droit horizontal de type convention, doté de droits fondamentaux communs aux Etats membres.

[28] Etude de faisabilité relative à un cadre juridique pour la création, le développement et l'application de l'IA sur la base des normes du Conseil de l'Europe, adoptée par le CAHAI le 17 décembre 2020 https://rm.coe.int/cahai-2020-23-final-etude-de-faisabilite-fr-2787-2531-2514-v-1/1680a1160f p.8

Règlementation et réflexions nationales

Par Bertille Vallet

Si, comme au niveau européen, les organes et rapports se multiplient au sujet de l'intelligence artificielle en France, le débat autour de la loi Sécurité globale a mis en lumière la question de leur développement et de leur usage au sein des forces de sécurité. Basés sur le cadre administratif et judiciaire, leur encadrement juridique national « par nature » n'est encore que très conceptuel. A l'instar des vecteurs, il se verra progressivement adapté à travers la règlementation européenne et les dérogations relatives à la compétence souveraine de la sécurité intérieure. Quelle qu'en soit la finalité d'usage, la Commission informatique et libertés (CNIL) a relevé les principes de vigilance, de loyauté et de finalité comme indispensables au traitement des données que l'IA suppose.

Selon un communiqué de presse du Premier ministre publié le 9 mars 2020, « *la stratégie nationale en intelligence artificielle a été lancée par le président de la République fin mars 2018, et vise à positionner la France comme un leader de l'intelligence artificielle en Europe et dans le monde. […] Dotée d'un budget de 1,5 milliard d'euros sur cinq ans, elle a (notamment) pour priorité de consolider un modèle éthique et équilibré entre innovation et protection des droits fondamentaux, au service de l'humanité* ». La mission parlementaire de Cédric Villani rendue en 2018[29] rapportait en ce sens la nécessité d'une synergie d'innovation interministérielle vers laquelle il faut continuer de se diriger.

Le cadre juridique règlementant l'IA en matière de sécurité publique est donc épars et souvent d'origine ou d'inspiration européenne. La proposition de règlement européen sur l'IA publié par la Commission le 21 mai dernier fait d'ailleurs état des problèmes que posent les règlementations nationales en matière d'IA, à savoir notamment la fragmentation des corpus juridiques applicables. Il est à noter tout de même certaines dispositions législatives.

Sur la **sécurité des données** du fait de l'utilisation des techniques d'intelligence artificielle, la loi n° 78-17 du 6 janvier 1978 dite Informatique et libertés[30] a été récemment révisée par la loi n° 2018-493 du 20 juin 2018[31] pour intégrer les exigences du règlement n° 2016/679/UE sur la protection des données personnelles en matière civile et commerciale (dit RGPD).
En outre, la directive 2016/680/EU 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 (dite Directive police-justice) été transposée par la loi du 20 juin 2018.

Saisi par soixante députés, le Conseil constitutionnel a du se prononcer sur la conformité de cette loi dans une décision du 12 juin 2018.[32]
Pris pour adapter le droit interne aux articles 58 et 83 du RGPD, le 2° du paragraphe I de l'article 7 de cette loi réécrit l'article 45 de la loi du 6 janvier 1978 afin de prévoir les différentes mesures et sanctions susceptibles d'être prises par la présidente de la CNIL ou par la formation restreinte de cette commission en vue de prévenir, mettre fin ou réprimer les manquements commis par les responsables de traitement de données personnelles ou leurs sous-traitants aux dispositions de ce règlement ou de cette loi.[33]

Ces textes ont été complétés par le décret n° 2018-687 du 1er août 2018 et l'ordonnance n° 2018-1125 du 12 décembre 2018.

De plus, la **transparence algorithmique** a été encouragée par la loi du 17 juillet 1978[34].

[29] https://www.aiforhumanity.fr/pdfs/9782111457089_Rapport_Villani_accessible.pdf
[30] https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000886460/
[31] https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000037085952
[32] https://www.conseil-constitutionnel.fr/decision/2018/2018765DC.htm
[33] Commentaire de la décision 2018-765 DC du 12 juin 2018 p.8
[34] https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000339241/

De manière anecdotique, une proposition de loi constitutionnelle a été déposée le 15 janvier 2021 relative à l'introduction, dans notre Constitution, d'une Charte de l'intelligence artificielle et des algorithmes[35] par M. Pierre-Alain Raphan.

Plus récemment, le projet de loi relatif à la prévention d'actes de terrorisme et au renseignement, dont la procédure accélérée a été engagée le 12 mai dernier, a été adopté en première lecture par l'Assemblée nationale le 2 juin 2021. Ce projet de loi prévoit tente de légiférer l'extension de la surveillance par algorithmes notamment par un allongement de la durée de conservation des renseignements à des fins de recherche et de développement et un allongement de la durée d'autorisation de la technique de recueil de données informatiques.
Cette loi pourrait également permettre le déchiffrement d'une URL (Uniform Resource Locator : adresse d'un site sur Internet) en étendant le champ d'application des *« boîtes noires »*, algorithmes de surveillance, en expérimentation depuis 2017.
Relativement à ce projet, le Conseil d'Etat a émis un avis le 6 mai 2021[36], la CNCTR a été consultée en application de l'article L. 833-11 du CSI sur ces dispositions, de même que la CNIL en application du a du 4° de l'article 8 de la loi du 6 janvier 1978 et l'ARCEP, en application de l'article L. 36-5 du CPCE.

A titre de réflexion, dans un rapport d'information sur les fichiers mis à la disposition des forces de sécurité de 2018[37], M. Éric Morvan, directeur général de la police nationale, a indiqué aux rapporteurs que les projets d'intelligence artificielle étaient très attendus au sein des services de la police nationale qui espèrent pouvoir être libérés de certaines tâches à faible valeur ajoutée.

D'après Éric Morvan, *« plus qu'une simple intelligence artificielle, les projets s'orienteront vers de l'intelligence augmentée pour dépasser la dimension strictement technologique et aller dans le sens d'une véritable assistance aux agents »* correspondant à la vision américaine de la gouvernance de l'intelligence artificielle, plutôt que de sa régulation par une réglementation trop contraignante.

[35] https://www.assemblee-nationale.fr/dyn/15/textes/l15b2585_proposition-loi
[36] https://www.assemblee-nationale.fr/dyn/15/textes/l15b4153_avis-conseil-etat.pdf
[37] https://www.assemblee-nationale.fr/dyn/15/rapports/cion_lois/l15b1335_rapport-information

De l'usage des drones de sécurité publique

Synthèse

Constat

- Des forces de sécurité publique exposées, faisant face à des individus/groupuscules utilisant les nouvelles technologies, dont des drones ;
- Recrudescence de guet-apens violents et de manifestations massives à fort potentiel de conflit ;
- Des pays alliés ou ennemis en supériorité technologique développant & utilisant sans freins les drones pour de la surveillance/reconnaissance faciale/suivi des personnes ;
- Perte du contrôle des données au profit des entreprises & Etats étrangers.

Enjeux

- Rééquilibrer le rapport de force avec les agitateurs/délinquants/criminels/terroristes ;
- Elargissement & rapidité des capacités d'intervention des forces de l'ordre ;
- Développer & soutenir l'innovation technologique et la recherche française ;
- Equilibrer les usages de drones par les forces de sécurité intérieure & la protection des droits fondamentaux ;

Freins

- Millefeuille législatif ;
- Déséquilibre entre proportionnalité des usages & protection des droits fondamentaux ;
- Difficultés d'accès aux données par les chercheurs malgré des démarches conformes ;
- Méconnaissance des législateurs sur les technologies existantes (capacité de l'IA de flouter en temps réel les visages) ;
- Cybersécurité relative des systèmes de drones.

Propositions

- Code regroupant la législation en matière ;
- Législation centrée sur l'humain et non la nature de la technologie dont les progrès ne sont pas toujours anticipés (ex : loi Godfrain de 1988) ;
- L'acceptabilité du déploiement des systèmes de drones repose sur la transparence, la renforcer ;
- Les moyens mis en œuvre (vecteur + dispositifs apposés) doivent être proportionnés avec l'objectif à atteindre.
- Limiter la captation de données personnelles à ce qui est strictement nécessaire pour l'exécution de la mission ;
- Faciliter les accès aux aides à l'innovation des start-up/PME/PMI spécialisées ;
- Adapter les appels à projets trop complexes & longs en termes de décision pour les start-up/PME/PMI spécialisées ;
- Réunir des groupes de travail réunissant des experts sur toutes les technologies sécuritaires ;
- Elargir le champ de compétence de la CNCTR et la CNIL sur les accompagnements & contrôles ;
- Ne jamais franchir la barre de l'autonomisation ni de la reconnaissance faciale de masse

Le drone, « aéronef sans équipage à bord », est au cœur du débat actuel – quoiqu'ancien – opposant la protection des libertés publiques aux nouvelles technologies. A prendre en considération qu'il est pourtant né peu ou prou en même temps que l'aviation au début du XIXème siècle. D'origine militaire, au même titre qu'Internet, la popularisation de son usage dans les années 2000 tant dans le versant défense que civil, a fait s'accroître les risques et menaces liés à cette utilisation. Ce vecteur s'étant miniaturisé pour correspondre à une demande de « loisir », il s'est effectivement éloigné de la perception de l'aéronef utilitaire qui le marquait pour adopter une réputation beaucoup plus « intrusive » induite par ses nouveaux usages : captation et traitement d'images, embarquement de caméras thermiques, etc. Les capacités des systèmes embarqués par les drones se perfectionnant et les usages de toutes les sphères de la société s'accroissant (défense, sécurité, professionnelle, de loisir), se pose avec raison la question de leur encadrement législatif.

Quel que soit le versant par lequel cet encadrement est abordé, il est essentiel de noter qu'actuellement *« le drone reste encore indissociable de la personne qui le met en œuvre, à savoir le « télépilote ». Ainsi, il n'est pas tant question de « drones » mais plutôt de « systèmes de drones », puisqu'il s'agit en réalité d'un ensemble plus complexe que le simple vecteur drone, dont l'Homme est au cœur*[1]*. »* Ainsi toute étude devra inclure cet aspect de l'humain trop souvent dissocié des nouvelles technologies dont il est pourtant : le créateur ; l'utilisateur ; le bénéficiaire et parfois la victime.

La France n'a pas saisi les opportunités dans l'immédiat et a tardivement exploité les capacités opérationnelles des drones au point d'être sous une américano-dépendance marquée tendant vers une sino-dépendance économico-technologique[2] de plus en plus prégnante et inquiétante. Les emplois dans la défense et dans la sécurité civile et publique sont récurrents et devenus indispensables à la stratégie en place dans la « lutte contre le terrorisme » avec pour précurseurs, les Etats-Unis. Employés militairement contre l'ennemi dès les années 2000, celui-ci réplique en usant de la même technologie. Les drones sont de plus en plus utilisés pour des frappes, notamment dans la guerre asymétrique, à l'instar des rebelles yéménites houtis ayant frappé avec une dizaine d'aéronefs en 2019 une usine et un gisement de pétrole au Yémen, paralysant un court moment la production mondiale de pétrole et 5% de la production mondiale du brut.

Des vidéos « pratiques » se diffusent sur des réseaux spécifiques ou traditionnels, adressées aux individus radicalisés en Occident apprenant à fabriquer un drone, disposer des charges utiles et le faire exploser à distance. Ce « transfert technologique » expose davantage la France déjà sous une menace terroriste quasi-permanente. La lutte contre cette menace s'étant étendue jusqu'à l'intérieur du territoire national, la stratégie de prévention, surveillance, traque et enquête doit nécessairement s'adapter.

En parallèle, les mouvements contestataires, devenus un enjeu majeur pour la sécurité publique, se font de plus en plus réguliers, massifs, avec des débordements récurrents (Gilets jaunes ; manifestations contre la loi de Sécurité globale, etc.). Ces *« manifestations à fort potentiel de conflit »* exposent à la fois les forces de sécurité en intervention et les manifestants pouvant être pris pour cible par des contre-manifestants, des personnes cherchant uniquement le conflit sans prise de position ou des terroristes cherchant à causer un maximum de victimes. Face à cette évolution, Cassandra Rotily a rédigé la thèse Drones et sécurité, soutenue le 7 décembre 2020. Réalisée dans le cadre du projet franco-allemand OPMoPS (Organized Pedestrian Movement in Public Spaces), *« visant à la préparation et à la gestion, par les forces de sécurité intérieure, des manifestations à fort potentiel de conflit avec l'aide des nouvelles technologies »*, de nombreuses références y sont faites dans ce document qui étudiera **comment la question des systèmes de drones peut être abordée dans le domaine de la sécurité publique à travers un rappel du contexte et du cadre juridique actuel et les différents usages qui peuvent en être faits au bénéfice de l'intérêt général, puis les risques et menaces liés et quelles propositions peuvent être faites en corrélation avec les nouvelles législations et évolutions technologiques en perspective.**

[1] Cassandra ROTILY, revue Riséo, Drones et sécurité – Positions de thèse, 2021-1

[2] https://portail-ie.fr/analysis/1941/les-drones-civils-au-cur-de-louragan-perpetuel-de-destruction-creatrice

La situation précédemment exposée rend donc nécessaire une élévation proportionnelle des outils et nouvelles technologies utilisés, notamment à travers l'usage de systèmes de drones prédéfinis avec des finalités précises et un encadrement solide. Or, trois éléments sont à prendre en compte : la doctrine se trouve en difficulté face au progrès technologique ; les problèmes que rencontrent les start-up/PME françaises dans l'innovation et les craintes de la société civile en matière de protection de la vie privée face aux besoins grandissants des agents de terrain.

Pour Cassandra Rotily, *« le recours aux nouvelles technologies (vidéoprotection fixe et mobile – à l'instar des caméras et drones) est apparu comme une solution performante pour assurer la prévention des atteintes à la sécurité […]»*. Les oppositions sont cependant fortes depuis le tournant des années 2013-2014, les révélations du lanceur d'alerte Edward Snowden et la portée de la surveillance de masse américaine. A contrario, les attentats terroristes menés sur le sol français dans la dernière décennie ont provoqué des divisions et relancé le débat Protection des libertés *vs* Sécurité, plus actuel qu'il ne l'a jamais été autour de la loi Sécurité globale. Pour autant, *« la liberté est fondée sur la sécurité, c'est un couple complémentaire*[3] *»*, la doctrine doit appuyer cet état de fait. En ce sens, les systèmes de drones devraient pouvoir être *« des garants de la liberté d'aller et venir sans crainte, de sortir, de travailler, etc. tout en permettant l'élimination des menaces et la sécurisation*[4] *»* et non des sources de menaces pour la population.

Dans leur ensemble, les doctrines de sécurité suivent difficilement l'évolution rapide de la société, des usages et des technologies[5]. Le premier frein en est l'aspect règlementaire qui, bien qu'évidemment nécessaire, prive les forces de l'ordre comme les personnes interpelées et les victimes, d'un appui aujourd'hui presque indispensable à leur sécurité et l'exercice de leurs missions ou de leurs droits. Par exemple, la majorité de la population possédant un téléphone portable, les vidéos d'interventions policières sont régulièrement filmées, mais de loin, avec des outils peu fiables, laissant parfois planer le doute quant aux faits réels par rapport à ce qu'en donne une image lointaine et de mauvaise qualité. Les Etats-Unis disposent de caméras embarquées éprouvées depuis un certain nombre d'années, sans omettre les limites de ces outils. Citons également la complexité de déploiement de systèmes de drones dans des zones urbaines où une surveillance physique met directement en danger l'intégrité des agents tandis qu'en face, les contrevenants en déploient à leur guise. Le rapport de force s'étant inversé, les nouvelles technologies permettraient de reprendre le contrôle de zones sensibles.

Un autre frein cible la latence du marché, affaiblissant l'innovation technologique française provenant d'un ensemble de jeunes et petites entreprises ne pouvant faire face à des appels d'offres s'étalant sur des cycles de décision à la durée difficilement tenable et complexes à monter. Les aides à l'innovation sont *« laborieuses à solliciter, à obtenir et à gérer (CIR / JEI / projets Européens), ce qui va à l'encontre de leur but premier de soutenir et accélérer l'innovation. Un indicateur fort de cette difficulté est directement visible de par le florilège de consultants prenant en charge ces dossiers à un coût exorbitant pour les petites sociétés*[6]*. »* Il y a dissonance entre les besoins des acteurs terrain que les nouvelles technologies peuvent accompagner dans le respect des libertés publiques vu les évolutions des missions de sécurité et l'opposition règlementaire/politique face aux nombreux freins de différentes natures. Ces acteurs terrain sont actuellement exposés à l'utilisation des nouvelles technologies embarquées par les drones sans pouvoir prendre de contre-mesure.

[3] Mireille COUSTON, échange du 26 mai 2021
[4] Ibid
[5] Sébastien PARIS, échange du 28 mai 2021
[6] Ibid

La décision du Conseil constitutionnel n° 2021-817 DC du 20 mai 2021[7] (cf. analyse en annexe 1) censurant deux dispositions met en évidence la complexité de mise en place de ces contre-mesures. Les dispositifs de surveillance nécessaires à la protection de l'ordre public doivent évidemment être encadrés afin de préserver les libertés et droits fondamentaux des personnes concernées. Or, il semble qu'il y ait méconnaissance sur les dispositifs en question, notamment concernant les systèmes de drones. Par exemple il est possible de flouter en temps réel les visages sur les images retransmises par un drone, avant transmission de l'image au poste de commandement. La « porte reste ouverte » à une prochaine soumission de loi. Le contexte actuel nécessitant l'usage des systèmes de drones, la conciliation entre les besoins et la nécessité de protéger la vie privée des personnes concernées est possible. Pour Cassandra Rotily le droit est prêt à évoluer mais un débat de société et des groupes de travail réunissant des experts sur toutes les technologies sécuritaires sont nécessaires.

Le cadre juridique applicable relatif à l'usage de systèmes de drones vient récemment de démontrer ses failles à travers la décision précitée du Conseil constitutionnel constituant une décision majeure. « Saisi *a priori* de la conformité à la Constitution de vingt-deux articles de la loi Sécurité globale, devenue loi pour un nouveau pacte de sécurité respectueux des libertés puis, finalement, loi pour une sécurité globale préservant les libertés, le Conseil constitutionnel s'est prononcé sur certaines dispositions pénales qu'il a censurées au nom des droits fondamentaux.

Concernant la censure de la surveillance par drone, l'article 47 visait à instaurer un cadre juridique pour l'utilisation des drones. Le Conseil constitutionnel a estimé que le texte ne présentait pas de garanties suffisantes. En cause notamment l'absence de limite maximale à la durée de l'autorisation de recourir à un tel moyen de surveillance, exceptée la durée de six mois lorsque cette autorisation est délivrée à la police municipale, ni aucune limite au périmètre dans lequel la surveillance peut être mise en œuvre, ni le principe d'un contingentement du nombre d'aéronefs circulant sans personne à bord équipés d'une caméra pouvant être utilisés, le cas échéant simultanément, par les différents services de l'État et ceux de la police municipale.
Il a donc censuré les dispositions relatives à l'usage des drones par les forces de l'ordre, que la proposition de loi avait pour objectif d'étendre de façon conséquente.
Les dispositions prévoyaient initialement de fournir un cadre légal en ajoutant au Code de la sécurité intérieure un nouveau chapitre "caméras aéroportées". L'usage des drones et le traitement des images était ainsi prévu pour *"les services de l'État concourant la sécurité intérieure et à la défense nationale, les services d'incendie et de secours et les formations militaires de la sécurité civile".* Le cadre d'utilisation était relativement étendu : rassemblements sur la voie publique ou dans les lieux ouverts au public, prévention d'actes terroristes, poursuite d'infractions, protection des bâtiments publics et des installations *"utiles à la défense nationale"*, ou encore régulation des flux de transport, surveillance des littoraux et des frontières, secours aux personnes, incendies.

Le Conseil constitutionnel a estimé qu'il y avait une atteinte disproportionnée de la surveillance par drone au droit à la vie privée en censurant l'article 22 (devenu l'article 47).Les drones ne pourront être utilisés que pour la sécurité civile (secours, pompiers), mais pas pour une surveillance généralisée de la population. Le Conseil constitutionnel a maintenu dans la loi l'interdiction du traitement des images des drones par des logiciels de reconnaissance faciale.

Malgré la censure du Conseil constitutionnel, le ministre de l'Intérieur envisage de proposer un nouveau texte permettant aux forces de l'ordre de faire appel à des drones. En France, la pandémie de Covid-19 a été l'occasion pour certaines entreprises et pour la puissance publique de s'essayer à des technologies pouvant être utilisées à des fins de surveillance. La CNIL[8] et le Conseil d'Etat[9] a enjoint à l'Etat de cesser de procéder aux mesures de surveillance

[7] https://www.conseil-constitutionnel.fr/actualites/communique/decision-n-2021-817-dc-du-20-mai-2021-communique-de-presse
[8] https://www.cnil.fr/fr/la-cnil-appelle-la-vigilance-sur-lutilisation-des-cameras-dites-intelligentes-et-des-cameras
[9]https://www.conseil-etat.fr/ressources/decisions-contentieuses/dernieres-decisions-importantes/conseil-d-etat-18-mai-2020-surveillance-par-drones

par drone, du respect, à Paris, des règles de sécurité sanitaire applicables à la période de déconfinement tant qu'il n'aura pas été remédié à l'atteinte caractérisée au point précédent, soit par l'intervention d'un texte réglementaire, pris après avis de la CNIL, autorisant, dans le respect des dispositions de la loi du 6 janvier 1978 applicables aux traitements relevant du champ d'application de la directive du 27 avril 2016, la création d'un traitement de données à caractère personnel, soit en dotant les appareils utilisés par la préfecture de police de dispositifs techniques de nature à rendre impossible, quels que puissent en être les usages retenus, l'identification des personnes filmées.

Concernant la censure du délit de provocation à l'identification des forces de l'ordre (art.52), l'article 52 (ex-article 24) de la loi Sécurité globale, visait à limiter la diffusion d'images des forces de l'ordre lors de leurs interventions. Le Conseil a jugé imprécis cet article qui ne définit pas suffisamment si la provocation doit être constatée pendant ou après une opération, ou même quel type d'*"opération"* entre dans le cadre de cette loi[10]. »

La question du traitement de la donnée se réfère à la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (loi Informatique et Libertés). Celle-ci a subi deux modifications majeures à travers, effectivement, le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel (RGPD), mais aussi la 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 (directive Police-Justice). C'est donc bien cette directive qui est appliquée et constitue le cadre légal en vigueur s'appliquant aux forces de sécurité lorsqu'elles recourent aux technologies dans le domaine de la sécurité publique avec le Code de la sécurité intérieure. En matière de données, la CEDH marque un tournant dans son arrêt du 25 mai 2021 où elle considère même que, *« compte tenu des multiples risques auxquels les Etats doivent faire face dans les sociétés modernes, le recours au régime d'interceptions de masse n'est pas en soi contraire à la Convention [européenne des droits de l'homme] »*. Toutefois, elle juge que *« pareil régime doit être encadré par des garanties de bout en bout ».*

A noter que nous sommes ici dans une compétence souveraine. Les règlementations européennes sur l'usage du drone le précisent. L'arrêté du 3 décembre 2020 sur les scénarios standards précisait les conditions applicables à ces missions qui sont exclues du règlement (UE) 2018/1139 du Parlement européen et du Conseil du 4 juillet 2018 concernant des règles communes dans le domaine de l'aviation civile et instituant une Agence de l'Union européenne pour la sécurité aérienne. L'arrêté note que pour certaines missions spécifiques de police, de sécurité civile, etc. il est possible d'évoluer en dérogation aux dispositions du présent arrêté qui est fixé pour les usages professionnels de drones.

(Contexte juridique complémentaire détaillé en annexe 2)

En termes de jurisprudence, précédant la récente décision du 20 mai détaillée ci-dessus, la jurisprudence traitant de la question est relativement courte. La décision n°446155 du Conseil d'Etat du 22 décembre 2020 est venue suspendre La décision du préfet de police de Paris de procéder à l'utilisation de drones et aux mesures de surveillance par drone pour la surveillance de rassemblements de personnes sur la voie publique. Cette décision fait suite à l'avis rendu public le 13 novembre 2020, req. n°401214 du Conseil d'Etat, estimant que *« eu égard aux enjeux qu'ils représentent pour la vie privée des citoyens, le recours, pour des missions de police administrative ou judiciaire, à des dispositifs aéroportés de captation d'images nécessite de recourir à la loi[11]. »*

[10] Analyse de Myriam Quemener, magistrat, senior advisor du CyberCercle.
[11] https://www.dalloz-actualite.fr/flash/il-faut-une-loi-sur-l-usage-des-drones-par-police

Des divergences entre les décisions rendues par les Cours européennes (CEDH/CJUE) et la jurisprudence française sont cependant à mettre en lumière. « Si les enregistrements issus des systèmes installés sur la voie publique sont utilisés dans des traitements automatisés ou contenus dans des fichiers structurés selon des critères permettant d'identifier, directement ou indirectement, des personnes physiques ; le système relève de la loi du 6 janvier 1978 dite « Informatique et libertés »[12]. Le système doit alors être autorisé par la Commission nationale de l'informatique et des libertés en vertu de l'article L. 252-1 du Code de la sécurité intérieure. Ainsi, l'article L.251-1 du Code de la sécurité intérieure prévoit donc une option entre la simple transmission et l'enregistrement d'images prises sur la voie publique, auquel cas le Code de la sécurité est applicable, et le cas dans lequel les données font l'objet de traitements automatisés ou dans des fichiers permettant l'identification de personnes physiques, auquel cas la loi Informatique et Libertés est applicable.

Pour Cassandra Rotily, « cette conception traditionnelle de la vidéoprotection prévue par le législateur en 1995 est largement remise en cause par la jurisprudence européenne. En effet, selon la jurisprudence de la Cour de justice de l'Union européenne, l'image d'une personne enregistrée par une caméra constitue une « *donnée à caractère personnel* », dès lors qu'elle permet d'identifier la personne concernée (arrêt *Buivids*)[13]. Par suite, dès lors qu'il est possible de voir ou d'entendre la personne sur la vidéo en cause, les images des personnes ainsi enregistrées constituent des données personnelles[14]. «

Par une ordonnance du 18 mai 2020[15], le juge des référés du Conseil d'État a enjoint à l'État de cesser les mesures de surveillance des règles de sécurité sanitaire par drone. Le juge a considéré que le dispositif en question constituait un traitement de données à caractère personnel et qu'en l'absence de moyens techniques rendant impossible l'identification des personnes ou de dispositions règlementaires encadrant ce traitement, une atteinte grave et manifestement illégale au droit à la vie privée était caractérisée. Le juge se permet de dire qu'il s'agissait bien d'un traitement de données à caractère personnel alors même que « *la finalité poursuivie par le dispositif litigieux n'était pas de constater les infractions ou d'identifier leur auteur* » mais seulement de détecter des attroupements[16]. »

Ces éléments révèlent cependant deux choses : la question centrale n'est pas la technologie en elle-même mais celle de la donnée et l'arsenal législatif est suffisamment complexe pour centrer les préoccupations sur la mise en œuvre. Une clarification à travers un Code rassemblant toute la règlementation applicable, comme recommandé par Cassandra Rotily, pourrait s'en trouver fort à propos. Concernant les drones précisément, encore une fois il ne s'agit pas de l'engin en lui-même qui, hormis des risques de chute ou de collision, ne porte pas atteinte aux droits fondamentaux, contrairement aux systèmes embarqués. Fonder une législation sur une technologie en particulier serait ainsi périlleux en plus d'être chronophage est coûteux. L'expérience a démontré que les lois basées sur des principes permettaient de suivre les rapides progrès technologiques sans perdre en efficacité à l'instar de la loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique (loi Godfrain). Ainsi il s'agirait non pas de restreindre le développement de nouvelles technologies qui doit au contraire être soutenu,, mais d'en encadrer la mise en œuvre en contexte réel. Les usages de ces technologies apportent des bénéfices indéniables pour la communauté. L'instantanéité des communications a été un premier pas majeur. Mais alors qu'auparavant un temps de latence entre leur développement à leur démocratisation permettait aux Etats de s'en saisir pour améliorer ses compétences régaliennes et d'assurer un contrôle de leur diffusion, aujourd'hui la plupart de ces nouvelles technologies – à l'exception de celles développées spécifiquement à l'intention de la défense – n'ont plus ce temps de latence. Cet état de fait a

[12] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, *JORF* du 7 janvier 1978
[13] CJUE, 14 février 2019, *Buivids*, n° C-345/17, pt. 31; CJUE, 11 décembre 2014, *Ryneš*, n° C212/13, pt. 22.
[14] Arrêt, *Buivids*, préc., pt. 32
[15] CE, ord., 18 mai 2020, *La Quadrature du Net* et *La Ligue des droits de l'Homme*, n° 440442, 440445
[16] Cassandra ROTILY, échange du 26 mai 2021

déséquilibré les rapports entre les forces de sécurité intérieure et les « agitateurs », rendant plus que nécessaire l'utilisation d'outils d'aide à la décision pour les assister.

Face à des menaces dont les protagonistes sont bien équipés en nouvelles technologies et sachant parfaitement les utiliser, le déploiement de systèmes de drones s'illustre dans trois cas de figure répondant à des règles différentes d'utilisation.
Tout d'abord la question des manifestations à haut potentiel de conflit. La sécurisation des rassemblements, tout en garantissant l'exercice des libertés fondamentales des manifestants, est un nouvel enjeu majeur. La Suisse semble avoir trouvé un équilibre entre acceptabilité et surveillance : elle positionne par exemple des drones plus volumineux mais éloignés de la manifestation, donnant une vision élargie aux forces de sécurité sans faire courir de risque aux personnes ou à l'engin. En ces conditions, pour préserver la sécurité des personnes et des biens, seuls les mouvements de foule devraient pouvoir être analysés, permettant une meilleure gestion des manifestations de plus en plus nombreuses, massives et à potentialité accrue de débordement. Un tel outil permettrait de déterminer plus facilement la manière dont les forces de l'ordre devront se positionner et évoluer au cours de la manifestation, à travers des modélisations et des essais combinés avec des méthodes de simulation permettant d'anticiper plusieurs scénarios de risques. Il reste à définir les contours de l'emploi de cette nouvelle technologie et ceux relatifss aux modalités de collecte, de visionnage et de conservation des données. Quasiment presque toutes les entreprises – à l'image de ONHYS - spécialisées sur ces systèmes peuvent déployer des systèmes floutant en « natif » (donc avant transmission de l'image au poste de commandement) les visages mais permettant de prédire les mouvements problématiques.
Les chercheurs du laboratoire INRIA de Rennes effectuent des recherches sur la simulation dans l'objectif de créer des algorithmes informatiques qui calculent le mouvement d'une foule, afin de comprendre, reproduire ou prédire son comportement. Julien Pettré, chercheur à l'INRIA, davantage centré sur la sécurité civile, ajoute que dans ce type mission il est préférable de s'intéresser à des technologies qui ne permettent pas l'identification individuelle pour des questions d'acceptabilité.

La reconnaissance faciale à des fins de surveillance de masse n'est pas et ne devrait pas être autorisée dans ce contexte : en sus d'être contre-productif en termes d'acceptabilité, elle entraîne un risque d'effet dissuasif sur des personnes qui auraient autrement exercé leur droit de manifester. En ce sens, la transparence devrait être un maître mot pour tout usage de nouvelles technologies.
Ensuite, l'analyse d'une zone avant une intervention dans l'objectif d'éviter les dommages collatéraux sur des civils se trouvant là « au mauvais endroit au mauvais moment » et bien entendu, de protéger les forces de l'ordre d'un ou plusieurs assaillants cherchant à provoquer un effet de surprise. Est particulièrement ciblé ici le guet-apens qui, depuis une vingtaine d'années, est devenu habituel les soirs de « fête ». Mais *« depuis quatre ou cinq ans, c'est quotidien. En grande couronne, toutes les nuits, ce genre de faits est constaté, sans compter les attaques des commissariats*[17] *»*, observe Yvan Assioma, secrétaire national Île-de-France du syndicat Alliance. L'attaque de Viry-Châtillon du 8 octobre 2016 a vu quatre policiers tomber dans un guet-apens où un groupe d'assaillants a brisé les vitres des voitures pour y jeter des cocktails Molotov en bloquant les portières pour empêcher les agents de fuir. La cour d'appel a reconnu en avril 2021 *« la volonté claire des assaillants de provoquer la mort des victimes »* mais a conclu par des peines allant de 6 à 18 ans de prison pour cinq des prévenus, et relaxé les onze autres. Une caméra fixe vandalisée qui « dérangeait » les délinquants est à la source du déplacement des policiers. Une caméra thermique embarquée sur un système de drone, sans reconnaissance faciale mais permettant d'identifier une situation à problème réduirait nettement ce type d'attaques, de plus en plus récurrentes et de plus en plus violentes envers les forces de sécurité intérieure.
Pendant une intervention « sensible », la captation d'image se révèle être un outil nécessaire aussi bien pour corréler les dires d'une victime, d'une personne interpelée ou des agents en

[17] Yvan Assioma, secrétaire national Île-de-France du syndicat Alliance, pour William Moliné, le 18 février 2021 https://www.lci.fr/justice-faits-divers/guet-apens-contre-la-police-des-videos-brandies-en-trophee-sur-les-reseaux-sociaux-snapchat-telegram-2178711.html

cas de contradictions sur les faits. L'usage systématique n'est pas recommandé : en fonction du contexte et des finalités l'usage de systèmes de drones peut être décidé.
Enfin, dans le cadre d'une intervention immédiate avec un auteur des faits identifié, l'usage de systèmes de drones permettrait de suivre l'individu en fuite, potentiellement dangereux. Les menaces évoluent, la criminalité s'adapte, les forces de sécurité intérieure ne peuvent pas être moins bien équipées, au risque de devenir David luttant contre Goliath.

Pour ces différents cas de figure, le développement d'outils performants européens, si ce n'est français, est l'une des garanties à apporter pour favoriser l'acceptabilité de la société civile, en sus des enjeux de souveraineté. Or, si des volontés fortes apparaissent, l'inadéquation des moyens reste quant à elle flagrante. Pour les chercheurs des laboratoires comme l'INRIA, l'Institut IRIMAS ou des start-up spécialisées dans ces nouvelles technologies le constat est le même : l'impossibilité d'accéder aux données nécessaires à leur perfectionnement. La recherche a besoin de données. Julien Lepagnot, Maître de conférences en informatique à l'Université de Haute-Alsace - Institut IRIMAS, a travaillé avec Cassandra Rotily sur le projet OPMoPS cité précédemment (préparation et gestion des manifestations à fort potentiel de conflit) et indique que ce qui leur a le plus manqué fut notamment *« la possibilité d'accéder aux systèmes de vidéoprotection urbains, malgré de nombreuses démarches. Cela aurait été en effet d'une grande aide pour perfectionner nos algorithmes d'IA. D'un autre côté, cela montre que le respect des libertés est actuellement déjà plutôt bien assuré, ce qui est une bonne chose. »*

Les freins imposés à la recherche, réduisant drastiquement leurs capacité innovatrices autant que régulatrices sur des systèmes étrangers, sont un reflet, d'une part de l'inadéquation des conditions d'exploitation des données dans ce secteur précis, d'autre part de l'angoisse des autorités en mesure de donner les autorisations nécessaires. L'inquiétude grandissante de la population face à ces nouvelles technologies en parallèle est l'une des raisons de ces freins apposés, indispensables mais qui devraient être proportionnés. Par exemple, l'usage de systèmes de drones pour collecter la plaque d'immatriculation d'une voiture qui aurait dépassé son autorisation de stationnement serait disproportionné au regard des finalités. Par contre, leur usage pour collecter, pendant une manifestation de quelque nature que ce soit, des images de foules en mouvement aux visages non identifiables à des fins de recherche, serait acceptable au regard des bénéfices quant à la sécurité des personnes. Ainsi, la finalité, la proportionnalité et la minimisation des données traitées (collectées, analysées, corrélées, conservées, transmises, archivées ou supprimées) sont des principes fondamentaux déjà inscrits dans la loi Informatique et Libertés qu'il convient de respecter dans le déploiement de systèmes de drones par les forces de sécurité intérieure. Ces principes appellent également un autre élément fondamental, clef de l'acceptabilité par la société civile de ces usages : la transparence.

La transparence doit être d'une limpidité exemplaire auprès des personnes concernées, à la fois sur la nature des systèmes utilisés, les données traitées, leur finalités, les éventuels moyens d'exercice des droits – ou pas, rappelons que les données personnelles n'appartiennent pas aux personnes concernées – mais aussi sur les risques encourus. Le curseur est à positionner à deux endroits différents, d'où une difficulté d'appréciation : l'équilibre entre nécessité à objectif sécuritaire et protection des droits fondamentaux ; l'équilibre entre nécessité à objectif sécuritaire et les risques et menaces encourus. Sur ce dernier point, la question de la fiabilité technique des systèmes et cybersécurité est en jeu. Les aéronefs sans équipage à bord ne sont pas réputés pour la solidité de leur cybersécurité. Un drone de surveillance côtière semble inoffensif au premier abord ; cependant son piratage peut amener des groupes criminels à envoyer des images « neutres » sur lesquelles aucune activité anormale n'est détectée tandis qu'en parallèle, un déchargement illégal de personnes, produits de contrebande, armes, est en train de se produire.

Se pose de manière intrinsèque (ou induite) l'inévitable question de l'automatisation/autonomisation du drone. Il s'agirait là d'une frontière à ne pas dépasser, en mars 2020 le drone turc Kargu-2 en a démontré la nécessité en attaquant et tuant délibérément un soldat battant en retraite sans en avoir reçu l'ordre d'après un rapport émanant du Conseil de sécurité des Nations Unies en Libye. L'humain doit nécessairement rester aux commandes et n'utiliser les nouvelles technologies et leurs vecteurs que comme un appui, et non en

remplacement de ses tâches de surveillance. L'autonomisation fait écho au « syndrome Terminator » qui reste à relativiser, à ceci près qu'existe une règle dans l'univers numérique, celle que toute technologie fantasmée est vouée à être dépassée par la réalité. Si l'on prend ainsi l'exemple du drone côtier, il doit être associé à d'autres technologies (système de vidéosurveillance fixe, outils de détection) et à une continuité de la surveillance humaine.

La proportionnalité dans le traitement des données contribue fortement à la sécurité numérique des systèmes de drones. Le fait de ne pas les conserver ou d'écourter au mieux la durée de conservation non seulement allège les obligations des forces de sécurité utilisant le vecteur, mais renforce l'acceptabilité de son usage - en cas de cyberattaque les conséquences sur la *privacy* seront réduites. Si l'on reprend l'exemple côtier, face à la transparence d'utilisation et les finalités clairement explicitées, rares seraient les personnes refusant un regard supplémentaire sur la baignade des enfants ou les risques liés à la navigation. La conception de systèmes traitant immédiatement et automatiquement les données, prompts à signaler une agitation anormale sur un bord de plage ou une embarcation en difficulté, serait tout à fait possible, dans la mesure ou les concepteurs auraient accès à des données pour entraîner leurs systèmes.

Dans le cas de systèmes de drones où la captation d'images/enregistrement de sons/voix à conserver engendre des risques pour les libertés individuelles, là encore, l'acceptabilité passant par la confiance de la société civile, les garanties devront être particulièrement solides. L'Estonie, pays aux services particulièrement numérisés, a été confrontée à cette défiance. Son maître mot est devenu la transparence. Chaque citoyen dispose d'un identifiant numérique unique contenant l'intégralité des données relatives à sa vie d'administré (identité, diplômes, données de santé, etc.). En allant sur un espace personnel, il peut savoir à chaque instant qui ou quelle administration a consulté quelles données. Tout un chacun doit donc pouvoir être en mesure, lorsque cela n'est pas contraire aux finalités, de savoir quelles données sont collectées puis traitées et par qui. Tout drone devant être numériquement identifié d'ici 2023 (règlement U-space), l'identification peut aussi être visuelle à quelques exceptions près et là encore, selon les finalités.

Face à ces enjeux, la France peut répondre en développant une stratégie à toutes les strates concernées. Dans un premier temps, communiquer auprès de la société civile sur les aéronefs sans équipage, existants depuis presque aussi longtemps que l'aviation elle-même et qu'elle utilise dans le cadre de la sécurité intérieure : ses bénéfices pour la sécurité publique (& civile), ses risques réels, le tableau de proportionnalité indiquant sur quel type de situation tel système de drone peut être utilisé. La transparence est encore une fois la clef de l'acceptabilité, à condition que l'information soit aisément accessible. Aucune nouvelle technologie - hors déviance éthique nette – ne devrait être freinée dans son développement. L'enjeu réside plutôt dans son déploiement à conduire, proportionnellement aux risques et menaces auxquels elle exposerait les personnes concernées.

La France dispose d'un maillage de laboratoires de recherches privés/publics et d'entreprises spécialisées dans les systèmes de drones et algorithmes d'intelligence artificielle mesure de traiter les données captées. Ils sont également tout autant en mesure de développer des technologies innovantes (sans verser dans l'innovation pour l'innovation). Leur faciliter l'accès aux données, notamment lorsqu'il s'agit de développer des outils propres à l'usage des forces de sécurité publique ou civile répond aux différents enjeux autour des nouvelles technologies en plus de récupérer un retard accumulé face aux géants américains et chinois. Dans le même sens, l'intérêt des start-up et PMI/PME ne devrait pas être négligé. Pour éviter leur rachat par des sociétés étrangères et renforcer la souveraineté française, un soutien économique destiné à ces entreprises et un accès facilité aux démarches (que ce soit pour les aides ou pour l'accès aux marchés publics) est nécessaire. Pour ne citer qu'un exemple, ONHYS a dû employer une personne dédiée au traitement des dossiers d'obtention des aides françaises et européennes. Si l'américano-dépendance est un problème, le risque à anticiper est celui de la Chine, qui pratique une politique d'étouffement des entreprises françaises et européennes par une

politique de « cassage » des prix, rentrant dans son objectif vraisemblable d' « étendre le "rêve chinois" à l'Europe[18] » dans une troisième phase de « conquête » prévue pour 2035-2055.

Pour préserver les droits fondamentaux, encourager la recherche et l'innovation à travers une politique de développement *security & privacy by design*, la clarté de la législation et de déploiement des systèmes de drones devraient faire l'objet d'un Code rassemblant la législation applicable classée par finalité. Le contrôle du déploiement de ces vecteurs pourrait se faire en élargissant les compétences de la Commission nationale de contrôle des techniques de renseignement (CNCTR) tandis que de la même façon la CNIL pourrait travailler en amont sur les mesures à mettre en place pour garantir un équilibre entre le développement et le déploiement des nouvelles technologies de sécurité avec la protection des droits fondamentaux.

Un travail en commun entre les différents organisations de l'Etat impliquées dans ces thématiques, les représentants de la filière, mais aussi d'organisations défenseuses des libertés, dans le cadre d'un process – cadre officiel lancé par l'Etat serait sur ce sujet tout à fait pertinent.

[18] https://www.lemonde.fr/international/article/2021/05/22/sayragul-sauytbay-formatrice-dans-un-camp-de-reeducation-du-xinjiang_6081101_3210.html

ANNEXE 1

Analyse de la décision constitutionnelle du 20 mai 2021

Loi pour une sécurité globale préservant les libertés

Par Bertille Vallet

Le 20 mai 2021, le Conseil Constitutionnel a rendu une décision n° 2021-817 portant sur la loi sécurité globale, perçue comme attentatoire aux libertés individuelles par ses opposants mais soutenue principalement par ses partisans y compris les syndicats de policiers.
La saisine du Conseil constitutionnel a été basée sur le fondement de l'article 61 alinéa 2 de la Constitution à savoir dans le cadre de la transmission d'une question prioritaire de constitutionnalité par au moins 60 députés et 60 sénateurs, et par le Premier ministre pour l'article -52 de la loi.

La décision rendue par le Conseil constitutionnel affirme les exigences pesant sur les forces de sécurité intérieure et de défense nationale, notamment dans l'utilisation des drones et des caméras embarquées.
Ainsi, respectivement certaines dispositions de l'article 47 et les dispositions de l'article 48 de cette loi ont été déclarés inconstitutionnels.

Sans condamner la légitimité de leur utilisation comme a pu le faire le Conseil d'Etat dans une ordonnance du 18 mai 2020 et un avis du 13 novembre 2020, le Conseil constitutionnel censure les modalités d'utilisation des drones et des caméras embarquées et les garanties afférentes jugées trop imprécises.
La rédaction des articles 47 et 48 de la loi pourra faire l'objet d'une nouvelle rédaction ou un prochain texte.

Sur certaines dispositions de l'article 47 de cette loi

L'article 47, paragraphe 1, insère un chapitre dans le Code de la sécurité intérieure permettant le traitement d'images aux moyens de drones par les services de l'Etat et la police municipale. Ainsi, sur autorisation d'un magistrat ou d'un représentant de l'Etat dans le département, les services de l'Etat et la police municipale peuvent être autorisés à recourir à ce moyen de surveillance dès lors que les circonstances le justifient et pour une durée adaptée, à l'exception de l'intérieur des domiciles et de leurs entrées.
Les images sont transmises en temps réel au poste de commandement. Le public est informé sauf lorsque les circonstances l'interdisent ou lorsque l'information entre en contradiction avec les objectifs poursuivis.

Selon les requérants, ces dispositions portent une atteinte disproportionnée au droit au respect de la vie privée.
Les motifs retenus par le législateur pour justifier la captation d'images sont trop larges, le dispositif ne présente pas un caractère nécessaire et les garanties encadrant cette technologie sont insuffisantes. Les requérants estiment que l'autorisation délivrée par l'autorité judiciaire ou administrative est sans limite de durée et de périmètre. De plus, les hypothèses de non-information du public dans la mise en œuvre d'une telle mesure de surveillance sont définies en des termes larges et imprécis. Eu égard à la mobilité des aéronefs sans personne à bord et à la hauteur à laquelle ils peuvent évoluer (120m), ces appareils sont susceptibles de capter, en tout lieu, et sans que leur présence ne soit détectée, des images d'un nombre très important de personnes et de suivre leurs déplacements dans un vaste périmètre. Dès lors, la mise en œuvre de tels systèmes de surveillance doit être assortie de garanties particulières de nature à sauvegarder le droit au respect de la vie privée.

S'agissant de l'usage par la police municipale, ces derniers peuvent y recourir afin d'assurer l'exécution de tout arrêté de police ce qui conduit à la surveillance généralisée et continue d'une commune selon les requérants.

Selon le Conseil constitutionnel, les dispositions contestées permettent, parmi d'autres motifs, que la captation et la transmission d'images concernent un nombre important de personnes (y compris leur déplacement) et, le cas échéant, sans que ces personnes ne soient informées de cette captation et transmission.

Les dispositions susvisées portent donc atteinte au respect au droit de la vie privée.

Au regard des motifs pouvant justifier le recours aux drones équipés de caméras et les conditions encadrant ce recours, le législateur n'a pas assuré la conciliation entre atteinte à l'ordre public et droit au respect de la vie privée.

Certaines dispositions de l'article 47 paragraphe 1 de la loi sont donc jugées contraires à la Constitution.

Sur l'article 48 de cette loi

Cet article insère un nouvel article au sein du Code de la sécurité intérieure relatif aux caméras embarquées, permettant aux forces de sécurité intérieure de procéder à la captation, l'enregistrement et la transmission d'images équipant leurs véhicules, aéronefs et embarcations à l'exception des aéronefs sans personne à bord.

Selon les requérants, ces dispositions portent une atteinte injustifiée au droit au respect de la vie privée sur plusieurs fondements.
Les requérants estiment que le législateur n'aurait pas clairement explicité les finalités de ces usages méconnaissant ainsi l'exigence de clarté de la loi, faute de définir suffisamment les exceptions à l'obligation d'informer le public de l'usage de ces caméras. Selon les sénateurs requérants, le législateur n'aurait pas suffisamment limité les finalités pouvant justifier l'accès à ces images ainsi que leur utilisation. L'usage des caméras embarquées n'ayant pas été réservé à la prévention ou à la constatation des infractions pénales les plus graves, et disproportionnée, faute d'interdire expressément que ces caméras filment l'entrée des domiciles

Selon le Conseil constitutionnel, les dispositions contestées permettent aux caméras embarquées de capter, enregistrer et transmettre les images sur la voie publique ou dans les lieux ouverts au public, y compris l'intérieur des immeubles et leurs entrées.
L'information générale du public est prévue par l'apposition d'une signalétique lorsque les véhicules sont équipés de caméras. Une dérogation est prévue à cette obligation dès lors que les circonstances l'interdisent ou si l'information est en contradiction avec les objectifs poursuivis.
La dérogation prévue est donc très large, particulièrement en matière d'investigations pénales. Les images captées peuvent être transmises en temps réel au poste de commandement.

En outre, les dispositions contestées peuvent être mises en œuvre pour prévenir les incidents, faciliter le constat des infractions et la poursuite de leurs auteurs, assurer la sécurité des rassemblements et faciliter la surveillance des zones frontalières (comprenant le secours aux personnes et la lutte contre les incendies).

En sus, la mise en œuvre de ces dispositions doit être déterminée pour une durée strictement nécessaire à la réalisation de l'opération mais le législateur n'a pas fixé de limite maximale de la durée, ni de périmètre.
De plus, la décision de recourir à des caméras embarquées n'est soumise à aucune autorisation, ni même à l'information d'une autorité autre que les agents des forces de sécurité intérieure et les services de secours.

Sur la base des motifs susvisés, le législateur n'a donc pas assuré de conciliation équilibrée entre la prévention des atteintes à l'ordre public et le droit au respect de la vie privée.

L'article 48 méconnaît donc le droit au respect de la vie privée et est ainsi contraire à la Constitution.

Relativement au rapport

Une prise en considération des craintes soulevées par ces dispositions

Il est important de noter, relativement au présent rapport, que les requérants présentent à la fois les craintes de la société civile et les atteintes majeures aux libertés fondamentales (droit au respect de la vie privée, droit de la liberté d'aller et venir notamment).

La délibération de la CNIL n°2021-011 du 26 janvier 2021 décrit ainsi le danger dans « ce changement de paradigme, en matière de captation d'images par les autorités publiques, [qui] ne doit pas être sous-estimé dans le contexte de la montée, au sein de notre démocratie, d'un débat autour de la mise en place d'une société dite de surveillance. »

Aussi, Alexis Corbière, dans une séance parlementaire du 15 avril 2021 parle de la « suspicion croissante sur le rôle de la police, en donnant le sentiment que ce service public indispensable ne peut être soumis à aucune critique citoyenne. En pleine crise sanitaire, alors que nous avons manqué de masques, de blouses, et que nous n'avons pas le nombre de vaccins nécessaire, votre ministère commande 170 000 munitions de LBD et 586 micro-drones du quotidien pour un montant de 4 millions d'euros. » La défiance publique doit être prise en compte.

Une régularisation possible

En filigrane de cette décision constitutionnelle sans précédent transparaissent les possibilités de régularisation à mettre en œuvre. La régularisation d'un tel texte est possible, en prenant en compte les points relevés par les décisions jurisprudentielles.
Ainsi, déterminer précisément les modalités d'utilisation du drone et de la caméra aéroportée, avec la fixation d'un délai maximal d'utilisation ainsi que d'un périmètre déterminé, proportionnés aux finalités, pourrait rendre les dispositions contestées conformes à la constitution.

Des difficultés persistantes relatives aux dérogations

Concernant les dérogations possibles, quant à l'information au public, cette difficulté soulevée par le Conseil constitutionnel demeure difficile à surmonter. Il est à craindre que toute utilisation de drone à des fins sécuritaires (surveillance de rassemblement par exemple) entre directement en opposition avec les objectifs de la mission.

Les dispositions contestées par les requérants, censurées par le Conseil constitutionnel dans sa décision du 20 mai 2021, et spécialement les articles 47 et 48 de la proposition de loi sécurité globale, devraient donc être largement explicitées afin d'être mis en conformité à la Constitution. Celle-ci suppose donc d'établir les modalités d'exercice de la surveillance par drone ou par caméra aéroportée ainsi que des précisions concernant les dérogations possibles à ces modalités.

Conclusion

La légitimité – comme l'acceptabilité – de l'utilisation de tels moyens par les forces de sécurité intérieure est un enjeu majeur sur lequel la législation nationale et européenne et la jurisprudence doivent s'accorder afin de préserver au mieux les libertés fondamentales.

Ainsi, les récentes divergences, entre l'ordonnance du Conseil d'Etat rendue le 18 mai 2020 relativement à l'utilisation des drones pour surveiller le respect des mesures de confinement, et l'avis du 13 novembre 2020 insistant sur le fait qu'une telle captation d'images par un drone constituait un traitement de données à caractère personnel, relevant alors de la compétence du législateur, ne peuvent continuer à coexister sans perdre tout un chacun.

La portée de cette décision sera certainement plus profonde que le seul cadre de la loi sécurité globale. Elle illustre ainsi l'importante évolution des moyens et techniques des forces de sécurité intérieure et les dangers que cela comporte. Les propositions visant à apaiser les craintes et à poser un cadre législatif clair sont nombreuses bien que longues à mettre en place. A cet égard, Cassandra Rotily, dans sa thèse « Drones et sécurité » plaide en faveur d'un Code rassemblant toute la règlementation applicable, mettant ainsi fin au millefeuille législatif. Elle pose toutefois la question d'une graduation dans la légitimité de l'utilisation des drones par la force de sécurité publique : celle du respect des règles de confinement le serait, quand celle de la surveillance des rassemblements de personne ne le serait pas.

La doctrine, la société civile et les experts techniques auront donc à se prononcer sur ces sujets dans les mois à venir. Un débat démocratique doit être lancée afin d'éviter - l'instauration d'une « société de surveillance » selon les mots de la CNIL. Dans le même temps, un équilibre reste à trouver entre, d'une part, la fixation d'un cadre règlementaire clair et la conservation des libertés fondamentales, et, d'autre part, la flexibilité pour le développement des nouvelles technologies et leur amélioration.

ANNEXE 2
Cadre juridique applicable aux drones de sécurité publique et perspectives

Par Bertille Vallet et Rémi de Francqueville

1. Etat de la règlementation applicable en France

a. Règlementation nationale

Sur le plan international, la convention de Chicago relative à l'aviation civile internationale, signée le 7 décembre 1944, Convention **confirme la souveraineté nationale en matière de règlementation aérienne** en conservant la possibilité de concertations régionales comme en Europe.

Sur le plan national, les normes sont supplantées au fur et à mesure par la réglementation européenne afin de donner un cadre normatif unique à l'utilisation des drones. Toutefois, pendant cette transition, plusieurs décrets et arrêtés tentent de mettre en place un cadre pour l'utilisation des drones de sécurité publique.

Chronologiquement, encore en vigueur à l'échelle nationale, il est à noter :

- deux décrets du 27 avril 2013
- l'arrêté du 3 mai 2013
- l'arrêté du 24 décembre 2013
- l'arrêté du 22 janvier 2020

Ainsi, le décret N°2013-366 du 27 avril 2013[19] crée la direction de la sécurité aéronautique de l'Etat auprès du ministre de la défense, exerçant également auprès du ministère de l'Intérieur.

Le décret N°2013-367[20] est relatif aux règles d'utilisation, de navigabilité et d'immatriculation des aéronefs militaires et des aéronefs appartenant à l'Etat et utilisés par les services de douanes, de sécurité publique et de sécurité civile. Au sein de ce décret, est considéré « aéronef militaire » les aéronefs appartenant à l'Etat et soit utilisés par les organismes relevant de l'autorité du ministre de la défense ou du ministre de l'intérieur s'agissant des aéronefs en service au sein de la gendarmerie nationale ; soit utilisés de façon temporaire par une personne morale, pour les besoins du ministère de la défense ou du ministère de l'intérieur s'agissant des aéronefs de la gendarmerie nationale (article 1 du décret).

Ce décret dispose des possibles délégations de pouvoirs en matière de délivrance d'autorisations de vol et dérogations notamment. Selon ce décret, un aéronef ne peut être utilisé que s'il dispose d'un document de navigabilité valide (certificat de navigabilité ou autorisation de vol), d'une immatriculation, des spécifications de navigabilité justifiant la délivrance de son document de navigabilité. Son utilisation doit être conforme au manuel de vol ou aux règles édictées et les personnes assurant sa conduite doivent détenir les qualifications requises.
Il est possible de déroger à ces conditions en cas de « circonstances exceptionnelles » ou de « nécessités opérationnelles urgentes » (article 10 du décret).
Les certificats de navigabilité et les autorisations de vols sont délivrés par le ministre chargé de l'aviation civile suivant les règles applicables aux aéronefs civils.

[19] https://www.legifrance.gouv.fr/loda/id/JORFTEXT000027379073
[20] https://www.legifrance.gouv.fr/loda/id/JORFTEXT000027379114

Subsidiairement, l'arrêté du 3 mai 2013[21] fixe les règles du maintien de navigabilité des aéronefs militaires et aéronefs appartenant à l'Etat et utilisés par les services de douanes, de sécurité publique et de sécurité civile.

Ensuite, l'arrêté du 24 décembre 2013[22] fixe les règles relatives à la conception et aux conditions d'utilisation des aéronefs militaires et des aéronefs appartenant à l'Etat et utilisés par les services de douanes, de sécurité publique et de sécurité civile qui circulent sans aucune personne à bord.

A titre informatif, l'arrêté du 22 janvier 2020[23] fixe la liste des zones interdites à la prise de vue aérienne.

Concernant le régime d'utilisation des drones par les forces de sécurité intérieure, par une ordonnance du 18 mai 2020[24], le Conseil d'Etat a pu délimiter la doctrine d'usage des drones de sécurité publique. En l'espèce, pendant le premier confinement national du à la pandémie de Covid-19, le préfet de police de la ville de Paris avait déployé des drones de sécurité publique afin de faire respecter les mesures de confinement.

Il y a été jugé que le simple accès à des données à caractère personnel constitue un traitement de données personnelles. Dès lors, expose le Conseil d'État, un arrêté autorisant un tel traitement doit être pris après avis motivé et publié de la CNIL, conformément à l'article 31 de la loi « Informatique et Libertés » n° 78-17 du 6 janvier 1978,[25] qui permet d'encadrer sa mise en œuvre et d'y assurer les garanties suffisantes pour la sauvegarde des droits et intérêts des personnes concernées.[26]

Au titre des opérations de surveillance par drones de sécurité publique, et en l'absence de dispositions spéciales, s'applique la règlementation du Code de la sécurité intérieure (article L. 251-1 à L. 263-1), étant précisé que l'utilisation de drones dans le cadre d'une mission de police reste également limitée par le droit au respect de la vie privée (art. 9 Code civil, article 226-1 Code pénal) mais surtout doit répondre à la législation en matière de protection des données personnelles (directive n° 2016/680 du 27 avril 2016, dite directive « Police-Justice »).[27]

La régularisation d'une telle situation était toutefois possible à travers un acte règlementaire**. Le Conseil d'Etat considérait donc comme légitime l'utilisation de drone à cette finalité.**

Ainsi l'article L.251-1 du Code de la sécurité intérieure prévoit une option entre la simple transmission et l'enregistrement d'images prises sur la voie publique, auquel cas le Code de la sécurité est applicable, et le cas dans lequel les données font l'objet de traitements automatisés ou dans des fichiers permettant l'identification de personnes physiques, auquel cas la loi Informatique et Libertés est applicable.
Cette conception traditionnelle de la vidéo protection prévue par le législateur en 1995 est largement remise en cause par la jurisprudence européenne. En effet, selon la jurisprudence de la Cour de justice de l'Union européenne, l'image d'une personne enregistrée par une caméra constitue une « *donnée à caractère personnel* », dès lors qu'elle permet d'identifier la personne concernée depuis un arrêt *Buivids*[28]. Par suite, dès lors qu'il est possible de voir ou d'entendre la personne sur la vidéo en cause, les images des personnes ainsi enregistrées constituent des données personnelles.

[21] https://www.legifrance.gouv.fr/loda/id/JORFTEXT000027386495/
[22] https://www.legifrance.gouv.fr/loda/id/JORFTEXT000028398844/
[23] https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000041459817/
[24] https://www.conseil-etat.fr/ressources/decisions-contentieuses/dernieres-decisions-importantes/conseil-d-etat-18-mai-2020-surveillance-par-drones
[25] https://www.legifrance.gouv.fr/loda/article_lc/LEGIARTI000037822860/
[26] https://actu.dalloz-etudiant.fr/a-la-une/article/surveillance-policiere-par-drones-le-oui-mais-du-conseil-detat/h/59f264b79b351e2f495b8844b7f6aa64.html
[27] https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016L0680
[28] https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:62017CJ0345

Récemment, la loi Sécurité globale, promulguée le 25 mai 2021 en application de l'article 49 alinéa 3 de la Constitution, a fait l'objet d'une censure partielle par le Conseil constitutionnel dans une décision du 20 mai 2021[29]. Cette décision marque un durcissement net de la position du Conseil constitutionnel et une accentuation des exigences pesant sur les forces de sécurité intérieure et sur la police municipale.[30] (voir annexe 1)

Ainsi, le Conseil constitutionnel a de fait interdit l'usage des drones par les forces de sécurité intérieure (article 47) ainsi que l'usage des caméras embarquées par les forces de sécurité intérieure (article 48) pour plusieurs finalités légitimes au motif qu'il n'y était pa apporté de garanties suffisantes (durée d'utilisation, périmètre et régime d'autorisation notamment dérogations). Cela laisse donc entière la question du régime permettant aux policiers, gendarmes et policiers municipaux de recourir à ces équipements nécessaires, même s'il offre quelques pistes pour une nouvelle rédaction.

b. Règlementation européenne

A l'échelle européenne, face aux risques que représente l'usage des drones de sécurité publique pour les libertés individuelles et les droits fondamentaux, les réponses sont d'ordres opérationnelles et juridiques.

En 2007, l'entreprise commune européenne SESAR (Single European Sky Air Traffic Management Research) a été créée par le Conseil de l'UE (Règlement n°219/2007) afin d'améliorer les performances de la gestion du trafic aérien (ATM) en modernisant et en harmonisant les systèmes ATM par la définition, le développement, la validation et le déploiement de solutions ATM technologiques et opérationnelles innovantes[31].

Ainsi, avec plus de 10 000 opérations drones chaque année en France et un nombre croissant de drones enregistrés, la Direction des services de la Navigation aérien (DSNA) a lancé en 2019 le programme U-Space Together[32] visant à garantir une insertion des drones dans les espaces aériens qui soit sûre, performante, respectueuse de l'environnement et des citoyens.[33]

Le Ciel unique européen (SES) est une initiative lancée par la Commission européenne en 2004 pour réformer l'architecture de l'ATM (Air Traffic Management) européen. Il propose une approche législative pour répondre aux futurs besoins de capacité et de sécurité au niveau européen plutôt que local.

En doctrine, le projet franco-allemand OPMoPS (Organized Pedestrian Movement in Public Spaces), vise à la préparation et à la gestion, par les forces de sécurité intérieure, des manifestations à fort potentiel de conflit avec l'aide des nouvelles technologies mais sa réalisation est aujourd'hui largement remise en cause en raison du contexte politique et de l'état du Droit.[34]

Il est dorénavant fait une **distinction selon le risque pour la sécurité aérienne liée à l'opération, et non selon sa finalité**. La règlementation européenne définit ainsi trois

[29] https://www.conseil-constitutionnel.fr/decision/2021/2021817DC.htm
[30] https://www.senat.fr/presse/cp20210520b.html
[31] https://ec.europa.eu/transport/modes/air/sesar_en
[32] https://www.sesarju.eu/sites/default/files/documents/reports/U-space%20Blueprint%20brochure%20final.PDF
[33] https://france.uspacekeeper.com/u-spacekeeper-est-deploye-au-sein-de-la-zone-aerienne-la-plus-dense-deurope/#:~:text=Avec%20plus%20de%2010%20000,l'environnement%20et%20des%20citoyens.
[34] Revue RISEO - Université et prétoire – Mélanges en l'honneur du Professeur Claude Lienhard (L'Harmattan, 2020) Drones et sécurité – Positions de thèse Cassandra ROTILY p.336

catégories d'opération : Ouverte, Spécifique et Certifiée par un règlement d'exécution de la Commission européenne du 24 mai 2019[35]

- ouverte : opérations à faible risque → vol en vue directe

- spécifique : opérations à risque modéré → vol en vue directe ou hors vue

- certifiée : opérations à haut risque nécessitant un niveau élevé de fiabilité de l'aéronef (transports de personnes, de marchandise dangereuse).

Le règlement du 20 février 2008[36], pris en application de la convention de Chicago précédemment citée, institue l'Agence européenne de la sécurité aérienne (AESA). L'objectif principal du règlement est d'établir et de maintenir un niveau uniforme élevé de sécurité de l'aviation civile en Europe.

Suite à cela, divers règlements européens déterminent les règles et procédures applicables à l'exploitation d'aéronefs sans équipage à bord notamment le règlement d'exécution n°923/2012 du 26 septembre 2012[37] établissant les règles de l'air communes et des dispositions opérationnelles relatives aux services et procédures de navigation aérienne, ou encore le règlement délégué 2019/945 du 12 mars 2019 relatif à la classification des drones en aéronefs sans équipage à bord de type C0 à C6.[38]

Le règlement d'exécution (UE) 2019/947 de la Commission du 24 mai 2019[39] concernant les règles et procédures applicables à l'exploitation d'aéronefs sans équipage à bord, dont l'entrée en vigueur initialement prévue au 1er juillet 2022 a été reportée au 1er juillet 2023 dû à la pandémie de Covid-19[40], prévoit notamment l'enregistrement des exploitants d'aéronefs sans personne à bord dès lors qu'ils présentent des risques pour la protection de la vie privée et des données à caractère personnel.

2. Etudes comparées

Il sera successivement envisagé l'usage des drones de sécurité publique aux Etats-Unis (i), en Belgique (ii) et enfin en Chine (iii).

i. L'utilisation des drones de sécurité publique aux Etats-Unis

Robert Mueller, directeur du FBI (2001 - 2013) reconnait l'usage en petite quantité et à titre expérimental de drones devant la commission de la justice du Sénat. Le département de la sécurité annonce en utiliser sur la frontière du Mexique. L'ATF (bureau contre les trafics d'armes, de tabac et d'alcool) s'en sont équipés ainsi que les services anti drogues. Il est alors question - dans les discours - d'expérimentations. Le Congrès imposait alors (en 2013) que l'espace aérien américain soit ouvert à la circulation des drones. [41]

S'agissant de la législation, sur le site NCSL (National Conference of State Legislature)[42] on trouve un historique précis de la manière dont depuis 2013, 44 Etats ont promulgués des lois afin de légiférer sur les UAS (Unmanned Aircraft Systems). Les lois promulguées peuvent aller dans le sens de la protection des libertés, de la propriété privée, comme elles peuvent spécifier les prérogatives des forces de l'ordre, le système juridique des Etats-Unis fonctionnant sur un modèle de permissivité (tout ce qui n'est pas interdit ou précisé comme étant l'action à mener, est permis).

[35] https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=PI_COM:C(2019)3824&from=FR
[36] https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32008R0216
[37] https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32012R0923&from=SK
[38] https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32019R0945&from=FR
[39] https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32019R0947&from=EN
[40] https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32020R0746
[41] Article « Le FBI reconnait l'usage de drones aux EU » 20 juin 2013, le Monde avec AFP
[42] https://www.ncsl.org/research/ transportation/current-unmanned-aircraft-state-law-landscape.aspx

Ainsi dès 2013, en Floride (SB 1221) il a fallu définir ce qu'était un drone, définir les circonstances dans lesquelles les forces de l'ordre pouvaient en faire usage. En 2020, l'Etat de Vermont interdit l'usage de la reconnaissance faciale couplée aux drones par les forces de l'ordre.

ii. L'utilisation des drones de sécurité publique en Belgique

La législation à ce sujet en vigueur est principalement concentrée dans la loi dite « caméra » entrée en vigueur le 25 mai 2018. En ce qui concerne les caméras mobiles elles ne sont autorisées à l'extérieur que pour la captation des plaques d'immatriculation en cas d'infractions et afin de prévenir des incivilités, se limitant ainsi à l'aspect routier.
Pour les particuliers le ciel est ouvert aux drones en Belgique (4 000 utilisateurs) avec des zones préservées.

iii. L'utilisation des drones de sécurité publique en Chine

Le modèle social chinois, qui repose sur « la collecte des données de sa population via les différents réseaux numériques mis en œuvre par les entreprises technologiques qu'elles soient *publiques ou privés »*[43] a une vision différente des libertés fondamentales. La sécurité collective et l'unité nationale priment sur l'expression de libertés individuelles.

À titre d'exemple récent a été mis en place durant la crise de Covid 19 l'utilisation de drones à capteurs thermiques afin de contrôler les températures corporelles ; de drones vérifiant l'effectivité port du masque, aptes à sommer les individus en défaut de rentrer chez eux via un haut-parleur ; a couplé ses systèmes de caméras à des programmes d'intelligence artificielle de reconnaissance faciale (biométrie), Ainsi que le rappelle Alice Ekman *« Sous Xi Jinping les autorités chinoises utilisent à grande échelle les technologies (vidéosurveillance, reconnaissance faciale, collecte et analyse des données agrégées big data), et continuent à investir massivement dans ces outils qu'elles considèrent comme des outils de « gestion de la société » »*[44].

Dans ce contexte l'usage de drone de surveillance, préalable à l'affaire des drones-pigeons en 2018, s'est intensifié.

Si un texte a été voté en 2017 afin d'encadrer pour la première fois la captation et l'usage des données[45] celui-ci est particulièrement controversé. De fait s'il légifère sur le droit des entreprises à accaparer les données il facilite la capacité du gouvernement à les saisir avec, notamment, une obligation du stockage sut le territoire national.

3. Perspectives d'évolution

L'intense prospective autour du drone s'explique par l'étendue et la variété des tâches qui pourraient lui incomber à terme. En effet, après avoir été principalement affecté à des usages de « loisirs[46] » et non professionnels, ce type d'aéronef sans équipage a divisé l'opinion au travers de la *« Loi pour une sécurité globale préservant les libertés »*.

Cette loi s'appuie sur l'arrêté du 27 juillet 2005[47] qui donne aux drones le pouvoir de prendre des prises de vues aériennes[48]et sur celui du 22 janvier 2020, qui recense les lieux où celles-

[43] Zubeldia, Océane. « Entre résilience et rupture : l'émergence d'un nouveau modèle technologique chinois ? », *Monde chinois*, vol. 61, no. 1, 2020, pp. 39-53.
[44] Alice Edman (2020), Rouge vif, l'idéal communiste chinois, Paris, Editions de l'Observatoire
[45] Morgane Tual, « En Chine, une loi controversée sur les données personnelles et la cybersécurité », *Le Monde*, 1er juin 2017.
[46] NIEDERCORN Frank, GEORGES Benoît, « Pourquoi la donnée est l'avenir des drones », *Les Echos*, https://www.lesechos.fr/2016/03/pourquoi-la-donnee-est-lavenir-des-drones-1110322
[47] https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000446845/
[48] «Article D133-10, Section 2 : Usage aérien des appareils photographiques, cinématographiques, de télédétection et d'enregistrement de données de toute nature (Articles D133-10 à D133-14) », *Légifrance*,

ci sont formellement interdites[49] .Elle autorise les autorités militaires et judiciaires à capter des images sur la voie publique [50]depuis un drone . Si la surveillance de citoyens par voie de drones s'est justifiée depuis le motif de prévenir les atteintes à l'ordre public, cette aptitude vient d'être censurée par le Conseil constitutionnel dans sa décision du 20 mai 2021. Ses requérants ont invoqué une atteinte au droit à la vie privée. En effet, est fondamentalement crainte une occlusion de la sécurité publique, car le drone se substitue au personnel humain. Parfois indicible, au déploiement quasi-instantané, sa caméra visuelle permet de remplir des missions de filature, de contrôle des foules, et complète plus largement les opérations policières. Cette loi met en avant la conjonction croissante voire l'interdépendance capacitaire observable depuis plusieurs années, entre maintien de l'ordre propre aux forces de police et préservation des intérêts stratégiques de l'Etat depuis l'armée. Ce glissement technique est en l'espèce contenu par l'édification d'une compétence partagée entre police et armée de surveillance depuis des drones. Conformément à l'évolutivité de la notion de sécurité publique sur le territoire national, le drone civil appelle à son tour à la mutation du traitement des menaces d'ordre intérieur. Malgré son rejet, le contenu de cette loi démontre l'évolutivité [51] permanente du drone, système qui mérite distinction.

Ce sont en l'espèce moult problématiques qui nécessitent d'être explicitées, afin de règlementer le drone et de l'insérer au sein du trafic aérien. Les aptitudes du drone civil se multiplient, avec par exemple[52] des capacités d'inspection des voies ferrées, de lignes électriques ou des incendies de forêts.

Ces compétences ont ouvert le débat sur le transport de produits voire de personnes, ce qui a permis de discuter de la taille des aéronefs. La crainte d'accidents depuis des drones civils plus lourds que ceux militaires (2000 kilos[53]), compte tenu des frictions imprévisibles dans les airs telles que des collisions, du brouillage ou des interférences, étaye l'arrêté du 24 décembre 2013[54]. Ce dernier a défini les conditions d'utilisation des volumes de drones possibles, qui se portent à la limite d'un poids égal ou 45 supérieur à 150kg, ce qui laisse une importante largeur d'interprétation pratique.

A compter du 1er janvier 2021, les drones civils sont dorénavant règlementés non plus selon leur type d'utilisation, mais depuis leur poids. Dès 800 grammes, tout drone doit être corrélé à un signalement électronique accompagné d'une carte grise d'identification. A partir de 250 grammes, et ceci au niveau européen, l'engin doit être déclaré auprès de la DGAC et l'exploitant « télépilote » doit s'identifier.

La notion de poids explique ces modifications de régime. En effet, la retombée d'aéronefs d'envergure plus importante pourrait créer des accidents mortels. Si le drone civil, dans l'ampleur de ses caractéristiques, demeure distinct de celui militaire, l'éventualité discutée d'un transport de produits voire de personnes imposerait non seulement une prise en responsabilité

https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000006843701/

[49] Arrêté du 22 janvier 2020 fixant la liste des zones interdites à la prise de vue aérienne par appareil photographique, cinématographique ou tout autre capteur", *Légifrance*, Annexe, https://www.legifrance.gouv.fr/jorf/jo/2020/01/24/0020

[50]" Loi n° 2021-646 du 25 mai 2021 pour une sécurité globale préservant les libertés (1)", *Légifrance*, Article 47, https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000043530276/

[51]" Loi n° 2021-646 du 25 mai 2021 pour une sécurité globale préservant les libertés (1)", Article 48, op.cit.

[52] BOURKE Robbie, DOUGLAS Steve, MARCONTELL Dave, THIBAULT Guillaume, « The hurdles drones face », *Oliver Wyman*, https://www.oliverwyman.com/our-expertise/insights/2018/sep/oliver-wyman-transport- and-logistics-2018/the-hurdles-drones-face.html

[53] Ibid

[54] « Arrêté du 24 décembre 2013 fixant les règles relatives à la conception et aux conditions d'utilisation des aéronefs militaires et des aéronefs appartenant à l'Etat et utilisés par les services de douanes, de sécurité publique et de sécurité civile qui circulent sans aucune personne à bord», *Légifrance*, Article 3, https://www.legifrance.gouv.fr/loda/id/JORFTEXT000028398844/

humaine très forte, mais aussi une redéfinition technique qui risquerait de créer une confusion peut-être physique entre drones civils et militaires. De tels drones seraient naturellement beaucoup plus robustes et imposants que ceux actuellement dépêchés dans le monde civil. La probabilité de défaillances est démultipliée par la prolifération des drones, avec 4 millions d'appareils d'ici 2022[55].

Ce danger créé un « brouillard » qui érode la crédibilité de potentielles normes de navigabilité sûres. L'accès, la propriété, la libre exploitation et la régulation de drones de grande taille sont peu perceptibles.

Reste l'acceptation sociétale[56], qui pourrait y percevoir une robotisation dangereuse[57]. L'enjeu à venir pour la mécanique du drone repose aussi sur la confiance des entreprises, afin qu'elles fournissent des données pour accélérer leur règlementation. Le drone civil sera tributaire d'un marché français à hauteur de 25 à 40% en 2025 par rapport à celui mondial[58]. A l'échelle européenne, le drone reflètera 10% du marché de l'aviation en 2050 pour 150000 emplois. L'Agence européenne de la sécurité aérienne se doit donc d'unifier les législations nationales eu égard au commerce transfrontalier[59] qui est un vecteur de motivation dans le développement de systèmes de drones utilitaires. Cette prolifération pourrait créer un effet de saturation entre drones civils et militaires dans le trafic aérien. En cela, l'édification de systèmes radars qui détecteraient des drones au sein du trafic 56aérien commence à être discutée en France. Si ce processus tend vers une égalisation des moyens entre drones civils et militaires, une réglementation législative séparée doit en découler et permettre de strictement séparer les champs d'actions de ces deux catégories pour empêcher un empiètement. Malgré le risque de confondre ces aéronefs et de juridiquement leur octroyer des moyens d'identification semblables, il semble que des capacités radars seront nécessaires à terme, au vu de la prolifération du nombre d'appareils. Au regard de l'interdépendance à l'œuvre entre personnels intérieurs de police et forces militaires, ce partage de compétences pourrait à son tour affecter les drones. La domination très large de la prospective sur la règlementation des drones doit donc rapidement amener à une régulation, au regard de la multiplication des aéronefs sans personnel, celle-ci n'en étant qu'à ses prémices.

Aujourd'hui, le drone civil est représentatif de la « nouvelle économie » (IA, Big Data, électronique, miniaturisation, réalité augmentée) qui bouleverse l'écosystème de défense. D'ores et déjà, l'analyse de données est renforcée par les effets de la numérisation, avec la dotation de drones en capteurs de télédétection, de topographie ou infrarouge laser. Epaulé par l'IA dans la transmission des données collectées, les algorithmes du drone civil permettent de nuancer la contraction des boucles décisionnelles. Intelligente et rapide, l'innovation au drone offre de larges prospectives expérimentales, comme le transport de poches de sang au Rwanda lors de la Covid-19[60]. Si ce foisonnement de perspectives sur le drone contribuent à l'illisibilité quant à ses limites, il pourrait aussi en accélérer la légifération. Cet esprit d'innovation respecte l'arrêté du 11 avril 2012, qui soutient l'évolutivité des opérations des drones civils eu égard aux progrès qu'ils seront amenés à connaître[61].

[55] Ibid
[56] BOURKE Robbie, DOUGLAS Steve, MARCONTELL Dave, THIBAULT Guillaume, op.cit.
[57] BOURKE Robbie, DOUGLAS Steve, MARCONTELL Dave, THIBAULT Guillaume, op.cit.
[58] NIEDERCORN Frank, GEORGES Benoît, op.cit.
[59] Ibid
[60] « Rwanda : des drones livreurs de sang pour sauver des milliers de vies », *Le Point International*, https://www.lepoint.fr/monde/rwanda-des-drones-livreurs-de-sang-pour-sauver-des-milliers-de-vies-14-10- 2016-2075940_24.php
[61] « Arrêté du 11 avril 2012 relatif à la conception des aéronefs civils qui circulent sans aucune personne à bord, aux conditions de leur emploi et sur les capacités requises des personnes qui les utilisent », *Légifrance*, https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000025834953/

La capacité en système de drones intègre désormais les champs de la stratégie militaire contemporaine. La possibilité de piratage, de détournement ou de sabotage sur drone, qu'il soit civil ou militaire[62],est prégnante en ce qu'il s'agit d'un appareil dont les circonférences et la valeur stratégique sont amenées à s'accroître. Au-delà des frictions naturelles et du risque de cyberterrorisme, leur prolifération requiert un contrôle spécifique afin de pallier toute dérive. Le drone civil doit faire l'objet du principe de proportionnalité, car il pourrait supposer à terme une réelle collusion dans ses tâches avec les personnels militaires (maintien de l'ordre, contrôle des populations) ces derniers ayant vu leurs prérogatives empiéter sur la sécurité domestique au pays. Si les retombées qualitatives du drone civil sont évidentes, celui-ci aggrave aussi la volatilité du domaine aérien. Le développement de normes de certification et la protection de l'informatique embarquée à bord de ces aéronefs garantiront la sûreté aérienne de demain.

[62] BOURKE Robbie, DOUGLAS Steve, MARCONTELL Dave, THIBAULT Guillaume, op.cit.

Liste des participants & contributeurs

Ont directement contribué aux travaux :
Bénédicte Pilliet, présidente du CyberCercle ;
Bertille Vallet, étudiante en droit ;
Jules-Henri Palleschi, diplômé en relations internationales, sécurité & défense ;
Matthias Popoff, étudiant en relations internationales, sécurité & défense ;
Migena Dushaj, juriste spécialisée en droit financier ;
Myriam Quéméner, magistrate et senior advisor du CyberCercle ;
Rémi de Francqueville, étudiant en relations internationales, expertise & risques internationaux.

Ont répondu aux questions :
Adrien Paillard, juriste spécialisé & ingénieur chez Orbitalize (Suisse) ;
Cassandra Rotily, docteure en droit, responsable du pôle Nouvelles technologies chez Air Space Drone ;
Julien Lepagnot, Maître de conférences en informatique, Université de Haute-Alsace - Institut IRIMAS;
Julien Pattré, chercheur à l'INRIA ;
Michael Barocco, fondateurs d'Orbitalize, société suisse proposant des solutions d'identification des drones de sécurité publique ou privés ;
Mireille Couston, Professeur des universités, directrice du Centre du droit des espaces et des frontières (Lyon 3), directrice "droit spatial" en la RFDAS (Paris) ;
Sébastien Paris, président et directeur de la R&D d'ONHYS, société spécialisée dans la gestion des flux de personnes.

De l'audit et de la certification des algorithmes

Par Matthias Popoff

La transparence des algorithmes est une composante nécessaire à l'édification d'une intelligence artificielle (IA) de confiance. Le concept d'audit des algorithmes est né en écho à l'utilisation croissante de systèmes d'IA dans des domaines sensibles. Il convient de préciser que ce concept bien que très répandu n'a, en soi, que peu de sens. Des algorithmes identiques peuvent en effet être utilisés de diverses façons sans pour autant revêtir la même sensibilité. Il est donc préférable de parler d'**audit des systèmes dans leur environnement applicatif** plutôt que d'audit des algorithmes.

Concrètement, l'auditabilité consiste en la possibilité d'évaluer et de certifier des algorithmes et autres jeux de données afin d'identifier les erreurs, les corriger et détecter les risques lors du développement d'une IA. Cela passe par le contrôle et le test des algorithmes tout au long du cycle de vie d'une intelligence artificielle afin d'analyser son fonctionnement ainsi que ses résultats et effets. Le concept d'auditabilité implique alors un **volet éthique** (appréhender les risques d'atteintes aux libertés fondamentales) et un **volet technique** consistant à mesurer la performance du système selon plusieurs critères[1]. Une mesure qui se divise en deux parties : l'**évaluation** et la **certification**.

L'évaluation s'effectue largement en interne, c'est-à-dire au sein des organismes développant et utilisant les systèmes d'IA, ce qui en soit est assez normal. En revanche, il est largement **préférable que la certification soit réalisée par un organisme extérieur, public** de préférence surtout lorsqu'il s'agit d'IA de sécurité publique utilisant des données souvent sensibles, afin de garantir un maximum de transparence. Une norme qui est encore loin d'être universelle sans être pour autant inexistante (LNE, AFNOR[2], …) et qui pourrait à l'avenir s'étendre à d'autres organismes (COFRAC[3], …). Certifier des algorithmes ne se base pas pour l'instant à partir d'un sens clair et précis. Et pour cause, la fiabilité des résultats d'un système d'algorithmes dépend en très grande partie de la qualité des données fournies. Une qualité pas toujours garantie. Pour beaucoup, le recours à l'IA amène souvent une difficulté, voire une impossibilité quant à auditer les systèmes algorithmiques[4]. Cela s'explique notamment par le fait que COBIT, le référentiel des auditeurs informatiques, ne dit rien des algorithmes. Il est donc parfois délicat de saisir ce qui est auditable ou non. Il n'empêche que les besoins de transparence et de contrôle n'en sont alors que renforcés afin d'assurer la crédibilité des certificats délivrés.

Un autre point important à évoquer concerne la question de la cadence qui diffère selon que l'on parle d'évaluation ou de certification. En effet, la fréquence plus importante de l'évaluation permet de disposer de trois niveaux sur un système d'intelligence artificielle : l'**utilisation**, l'**évaluation** et la **certification**. *« Cela présente l'avantage d'une plus grande implication des*

[1] https://hellofuture.orange.com/fr/auditer-lia-quand-les-algorithmes-sont-passes-au-crible/
[2] Laboratoire National d'Essai, Association Française de Normalisation, …
[3] Comité français d'accréditation
[4] https://gouvsi.blogspot.com/2019/04/laudit-et-la-certification-des.html

responsables en matière d'évaluations et de connaissances des systèmes, ce qui permet à terme de prévenir les effets "boîtes noires"[5]*.* »

Un avantage amplifié si tant est que les organismes publics conservent un contrôle efficace. En effet, cela est dû au fait que l'audit de la fiabilité des algorithmes d'IA et de leurs données ne constitue pas le seul socle de l'assurance délivrée par les auditeurs internes. Elle doit et devra être renforcée par la participation d'organismes externes, or ces derniers, selon qu'ils soient publics ou privés, ne fondent pas la crédibilité des certificats fournis sur les mêmes exigences. En d'autres termes, une plus grande implication des responsables doit s'accompagner d'une fiabilité croissante quant aux certificats délivrés, ce que peuvent garantir de manière plus sûre les organismes publics. Une cadence d'évaluations importante n'a de sens que si elle est accompagnée par une certification fiable.

L'enjeu principal que pose la question des audits vis-à-vis du public ; comment garantir aux citoyens que leurs données sont exploitées à des fins pertinentes et conformes et qu'elles ne sont conservées que le temps nécessaire. En ce sens, l'implication croissante d'organismes publics apporterait une réponse forte là où les organismes relevant du privé proposeraient une solution économique. Ces derniers, il est important de le rappeler, ayant pour objectif principal de dégager du bénéfice tandis que les organismes publics sont liés à des critères de qualité et de transparence plus élevés.

In fine et en précision complémentaire, il est important que la décision relève de l'humain surtout dans le cadre des applications dites à haut risque. Dès lors, il apparait aussi intéressant d'évaluer le niveau d'expertise du *pool* d'experts humain au sein de l'institution ou de la société privée capable d'exploiter ou d'évaluer les systèmes. Cette évaluation peut se faire sur présentation d'un niveau de diplôme. Tous les utilisateurs de l'IA ne peuvent être des docteurs mais il est essentiel que dans la structure **au niveau des instances dirigeantes** il y ait ce niveau d'expertise. La connaissance des systèmes ne peut être qu'au niveau exécutif, elle doit absolument se situer là ou est endossée la responsabilité. Certes ces éléments sortent du strict audit des systèmes mais, parce que dans le cas de l'IA on souhaite que la part de l'humain soit prépondérante, il parait pertinent de s'interroger sur ce sujet[6].

[5] Colonel Patrick PERROT (ST DGGN)

[6] Colonel Patrick PERROT (ST DGGN)

Ce document est la contribution de Palantir France aux réflexions de la mission « Pour un usage responsable et acceptable par la société des technologies de sécurité ».

Sur chaque technologie prioritaire évoquée, quel est le cadre juridique et doctrinal en cours ou envisagé? -> Un socle SECURITE 2022 Legal and Privacy by Design

Les plateformes de données dans le domaine de la sécurité sont utilisées dans certains des environnements **les plus sensibles et les plus sécurisés au monde**, c'est pourquoi elles nécessitent une protection et une gouvernance des données exemplaires. C'est pourquoi, les nouvelles technologies du numérique dans le domaine de la sécurité, doivent constamment être jugées par le biais de la façon dont elles aident analystes et décideurs à prendre des décisions éclairées, reposant sur des données empiriques, en vue d'objectifs de sécurité spécifiques, explicites et légitimes, permettant de minimiser les risques encourus par la France, les Français et les forces de l'ordre.

Les enjeux de sécurité, en France comme dans d'autres pays européens, peuvent aujourd'hui s'articuler autour des trois défis suivants:

- la prise de décision basée sur des données est excessivement complexe à cause de la faible qualité des données à disposition,
- les données risquent d'être partagées de façons inappropriées, soit trop peu pour mener à bien la mission, soit au-delà de ce qui est nécessaire et proportionné aux delà du traitement,
- et les décisions prises sur ces données peuvent demeurer opaques aux analystes et aux autorités de contrôle.

Le premier défi est un problème de confiance dans la qualité des données à disposition, le second un problème de collaboration sécurisée et le troisième un problème de transparence et de responsabilité. Ainsi, nous recommandons d'évaluer ces nouvelles technologies à l'aune des trois objectifs suivants :

- Fournir des analyses exactes, opportunes et utiles en vue d'informer la prise de décisions des autorités compétentes,
- Encourager une culture de partage et de collaboration responsable quant aux données au sein des administrations chargées de la sécurité en France.
- Inspirer la confiance des Français et des autorités compétentes (CNIL, ANSSI,...) grâce aux principes de transparence et de responsabilité.

Il est indispensable pour **concilier utilisation des technologies d'aide à la décision et garanties pour les libertés (graduation des règles d'engagement, instauration de contrôles, etc.) de respecter les principes suivants :**

- **Qualité et traçabilité des données** : Les analystes doivent être en mesure d'évaluer la véracité et la fiabilité des données. Toute décision prise sur la base d'informations inexactes risque d'impacter le succès opérationnel, et peut aboutir à des erreurs lourdes de conséquences, comme une surveillance accrue ou, pire, une arrestation d'individus ne pouvant être justifiées raisonnablement par les faits. Ainsi, il en va des libertés individuelles et publiques de garantir que les analystes puissent s'appuyer sur des technologies fournissant les capacités suivantes :
    - **Provenance** : Les utilisateurs peuvent indépendamment vérifier la provenance des données à leur disposition et déterminer d'eux-mêmes si ces données sont fiables. En respectant les permissions d'accès, les utilisateurs peuvent évaluer l'historique des données, suivre les ajouts, modifications et suppressions successives qu'elles ont suivies, permettant ainsi de ne pas répéter les mêmes erreurs.

- **Source Unique et Gestion des Versions** : Les solutions technologiques doivent maintenir une version unique et canonique de la donnée, plutôt que de laisser se propager de multiples copies au sein d'une organisation. Afin de préserver cette unicité, ces solutions doivent offrir des outils de gestion des versions (ou branching en anglais), permettant aux utilisateurs de rapidement proposer par eux- mêmes des modifications de données, une fois que celles-ci ont été vérifiées et approuvées. Ainsi, lorsque des erreurs sont identifiées dans les données, ces dernières sont rapidement corrigées et partagées avec tous les utilisateurs, réduisant ainsi la probabilité que des erreurs se répètent dans les données.
- **Santé des Données** : Les consommateurs de données doivent pouvoir s'assurer que ces dernières sont cohérentes et à jour. Pour ce faire, des contrôles automatiques doivent permettre de vérifier que les données respectent certaines conditions préétablies. De plus, les consommateurs doivent pouvoir vérifier si les données sont fraiches et les rafraichir le cas échéant. Ainsi, il sera garanti que les décisions prises ont été basées sur les meilleurs informations à disposition.

- **Une Meilleure Collaboration** : Paradoxalement, pour pouvoir partager des données, il faut être capable de les sécuriser. Plus la granularité dans la sécurisation des données est permise, plus le partage granulaire sera possible. Ainsi, les nouvelles technologies digitales se doivent de mettre en place un contrôle des accès de haute précision. Les principes suivants permettront de sécuriser les données de façon efficace :
  - **Contrôle des accès granulaire :** Les agences, direction et service en charge de la sécurité en France doivent pouvoir organiser leurs données selon les différents niveaux de classification. Le principe de proportionnalité requiert que les utilisateurs aient uniquement accès aux données strictement nécessaires aux vues de la finalité légitime de leur traitement. Accomplir cela, nécessite tout d'abord des contrôles d'accès hautement configurables (allant jusqu'au jeux de données, la ligne, la colonne ou même la cellule), mais cela requiert également un niveau d'orchestration permettant de configurer dynamiquement ces permissions dans la mesure du minimum nécessaire aux utilisateurs (peut-être basé sur leur rôle ou leur finalité de traitement, et limité dans le temps).
  - **Une Minimisation des Données Dynamique** : Le principe de minimisation des données implique que les utilisateurs ont accès aux données les moins sensibles nécessaires à leur finalité de traitement. Une approche avancée de la minimisation des données doit être dynamique : la même donnée doit apparaître à différents niveaux de rédaction en fonction de l'identité de l'utilisateur, mais aussi en fonction de la finalité spécifique au moment de l'accès à cette donnée. Cela permet de ne révéler que le minimum de données confidentielles et donc de protéger la vie privée de traitement ou corrélation abusives.
  - **Compartimentation des Données et Gouvernance** : Afin d'être conforme aux exigences de gouvernance des données et se protéger contre le risque de ré-identification des données, les administrateurs ont besoin d'avoir une compréhension claire des activités de traitement sur leurs plateformes. Savoir exactement où sont les données personnelles est un pré-requis permettant de s'assurer que des données qui ne doivent pas être croisées ne le soient, ni le seront.
- **Transparence et Responsabilité** : Afin de garantir les confiances entre les administrés et les administrations qui les protègent, il est crucial que l'utilisation de technologies digitales sur des données sensibles se fassent de façon transparente et responsable. Palantir croit profondément qu'il ne saurait y avoir de compromis entre sécurité et libertés individuelles et publiques. Il est donc nécessaire de promouvoir une utilisation des technologies qui préserve la confiance entre les citoyens et l'État. Ainsi, les fournisseurs de solutions technologiques se doivent de respecter les principes suivants :
  - **Des machines qui accompagnent mais une responsabilité humaine** : La première étape vers la transparence est de garantir que toutes les décisions reposant sur des données soient prises exclusivement par des agents. Les technologies doivent responsabiliser les agents et fonctionnaires et toutes les décisions importantes doivent être prises par des personnes et non des ordinateurs.

- **Auditabilité**: Tout système d'information doit fournir un journal d'audit robuste ainsi que des capacités d'analyse de ce journal. Ainsi, les personnes autorisées peuvent s'assurer de la conformité du traitement des données en analysant, filtrant et visualisant d'une façon intuitive et efficace toutes les données d'audit des systèmes d'information d'une organisation.
- **Relations avec le Autorités de Protection des Données** : Ces autorités ont une très bonne expertise des conditions à mettre en œuvre au service de la protection des données. Ainsi pour en arriver à ce qu'on appelle "privacy by design", les fournisseurs technologiques doivent pouvoir interagir avec ces autorités à toutes les étapes du développement, dès le design et la conception et jusqu'au déploiement sur des cas d'usages réels. Idéalement, ces relations pourraient être facilité par les administrations utilisant ces technologies, afin que leurs défis opérationnels soient constamment mis en perspective avec ces solutions. Enfin, une telle relation pourrait aussi aider, dans une certaine mesure, à communiquer de façon pédagogique des détails sur les solutions technologiques utilisées aux communautés qui seront impactées, renforçant aussi le lien de confiance entre les citoyens et leurs institutions.

Tous les principes décrits ci-dessus ne peuvent être vus isolement, comme autant d'outils déconnectés car cela conduirait à aggraver les risques de sécurité et de conformité. Ainsi, la base d'une utilisation efficace et responsable des technologies digitales dans le contexte de la sécurité doit reposer sur des systèmes cohérents permettant de gouverner les données de façon dynamique et rigoureuse. En ajoutant à cela une organisation forte et des garanties structurelles de la part de ces institutions au service des citoyens, de telles technologies seraient en mesure d'aider à préserver les sécurités des Français tout en en protégeant les libertés individuelles et publiques, sans modification du cadre légal.

En effet, **les service de sécurité doivent conserver la maitrise de l'utilisation qu'elles veulent avoir des logiciels et services de Palantir** : ce sont elles qui déterminent ce qui peut et ne peut pas être fait avec leurs données.

Les fournisseurs ne doivent pas pouvoir réutiliser ne transférer les données métiers pour ses propres besoins.

C'est pourquoi, chez Palantir, des équipes interdisciplinaires (Privacy & Civil Liberties) constituées de philosophes, de data scientists, d'avocats, d'ingénieurs travaillent en étroite collaboration sur les questions d'éthique et accompagnent les ingénieurs et développeurs dans la création et le développement des plateformes pour garantir que les questions de **confidentialité et de protection** soient intégrées 'by design' dans nos produits.

Nos solutions intègrent nativement les obligations de la norme RGPD :

- Découverte des données et classification : Foundry permet aux entreprises d'appliquer à leurs sets de données des metadonnées complètes et de les conserver afin de dresser rapidement le registre des données qu'elles détiennent (art. 30 du RGPD) et ainsi de comprendre leur exposition au risque (art. 35 du RGPD).
- Focus sur les données d'une personne : Foundry permet aux entreprises d'intégrer des données issues de systèmes sources différents et déconnectés, d'identifier et résoudre les doublons et de créer une vue unique et complètes des informations personnelles associées avec des sujets de données individuels dans le système. Cette capacité à générer une vue unique pour chaque sujet de données garantit aux entreprises d'être bien préparée pour répondre aux requêtes liées aux droit de la donnée prévus par le RGPD, notamment les droits d'accès (art. 15), de rectification (art. 16), d'effacement (art. 17) et à la portabilité des données (art. 20).
- Contrôles d'accès solides et précis : Les contrôles d'accès de Foundry se déclinent à différents niveaux de granularité métadonnées, dataset et sous-dataset et permettent d'opérationnaliser la collaboration sur des projets liés à la donnée, sans exposer les données personnelles à des

utilisateurs qui n'auraient pas un niveau d'autorisation suffisant. Ces contrôles peuvent permettre de se conformer à des politiques générales de limitation des accès, ou bien à des contraintes spécifiques à un projet particulier. Ceci permet aux contrôleurs d'assurer la sécurité et la confidentialité des données personnelles (article 32) mais aussi qu'elles soient traitées en accord avec la raison initiale pour laquelle elles ont été collectées.

- Minimisation dynamique des données : Au-delà des contrôles d'accès, Foundry permet aux entreprises et organisations d'appliquer des procédures de minimisation dynamiques des données, comme la pseudonymisation automatique, le chiffrement et le masquage sélectif pour répondre aux contraintes complexes et dépendantes du contexte qui sont issues du RGPD. Ceci permet aux entreprises de rendre leurs opérations de traitement des données compatibles avec les principes de minimisation des données (art. 5 alinéa 1c) tout en contribuant à la limitation par objectif (art. 5 alinéa 1b) et à la sécurité des données (art. 5 alinéa 1f et art. 32).
- Traçabilité de la provenance et du traitement des données : La transparence est un principe clé de la protection des données dès la conception et par défaut (Art. 25). Afin de rendre le traitement des données transparent pour les personnes concernées et les autorités de régulation, les entreprises ont besoin d'une infrastructure gardant trace de la provenance de toutes les données, incluant toute modification effectuée, la date de modification et la personne l'ayant effectuée. Foundry maintient automatiquement un tel journal de provenance des données et de leurs transformations, de sorte qu'il est possible de retracer l'histoire de la donnée à travers sa durée de vie, de la collecte à l'analyse puis à la suppression.
- Effacement des données : L'importance d'une bonne gouvernance des données devient immédiatement apparente dans le contexte de l'effacement, qui devient un défi technique significatif dans les cas des systèmes distribués et des déploiements sur le cloud. Foundry est livrée avec un outil permettant de définir des règles pour la gestion de l'effacement des données, de sorte que les organisations peuvent être sûres qu'elles ont effacé les données personnelles en accord avec la loi. Ainsi, Foundry aide par exemple un important client Européen du secteur de la finance dans la mise en oeuvre du "droit à l'oubli" (Art. 17), à la fois pour les données vivant dans Foundry mais aussi celles vivant dans d'autres systèmes.
- Journalisation d'audit et analyse : Le RGPD impose au responsable du traitement de démontrer qu'il respecte la loi (Art. 5 para. 2). L'infrastructure IT doit donc permettre d'enquêter aisément sur toutes les activités de traitement des données. Foundry - avec ses outils de traçabilité de la provenance, de versionnage et de journal d'audit - offre la vue d'ensemble requise par le RGPD.
- Gouvernance des données : Foundry offre un environnement unifié dans lequel délégué à la protection des données, gestionnaire des données, analystes et utilisateurs business peuvent interagir pour collecter, analyser, gouverner et protéger les données de l'entreprise. Cette plateforme unique diminue très fortement les coûts liés à l'utilisation des données et encourage une plus grande collaboration entre différents acteurs, tout en garantissant conformité vis-à-vis du RGPD et autres règlementations en matière de protection des données.
- Anonymisation et minimisation des données : Nos systèmes permettent aux administrateurs de la plateforme de s'assurer que chaque donnée est uniquement accessible aux utilisateurs autorisés, ceci en n'exposant que ce qui est nécessaire aux utilisateurs concernés (Art. 5 para. 2 du RGPD). En utilisant les outils de transformation de Foundry, la donnée peut être pseudonymisée, agrégée ou anonymisée puis sécurisée en applicant des contrôles d'accès granulaires. Ainsi, en utilisant les outils à disposition sur Foundry il est par exemple possible de chiffrer une colonne (ou un champ) sur tous les sets de données existants dans la plateforme et ne permettre son déchiffrement qu'à certains utilisateurs, de façon sélective (une valeur à la fois) et en justifiant la finalité de traitement qui sera sauvegardée. La combinaison de ces outils permet donc aux administrateurs de s'assurer que la donnée n'est accessible qu'aux utilisateurs autorisés mais aussi respectant des finalités légitimes de traitement.

La transparence et la sécurité sont au cœur de nos préoccupations : les clients ont accès aux logs, peuvent effectuer des audits réguliers, des tests de pénétration et avoir accès à toutes les versions du code de transformation de la donnée.

9 juin 2021

Technologies de sécurité :
Sans un contrôle effectif, pas de confiance des citoyens

-

Contribution du think tank Renaissance Numérique

Préambule

La note ci-après vise à contribuer aux travaux de la mission « Pour un usage responsable et acceptable par la société des technologies de sécurité », confiée par le Premier ministre au député Jean-Michel Mis.
Cette mission a vocation à étudier deux axes en particulier :

- "*Les opportunités offertes par les nouvelles technologies au service d'une meilleure offre de sécurité en analysant les besoins des forces de sécurité, entre autres dans la perspective des grands événements sportifs de 2023 et 2024.*
- *Les principes nécessaires à la préservation des libertés en définissant un cadre d'emploi global et cohérent des technologies de sécurité et en associant la société civile à cette définition pour renforcer la compréhension et l'acceptabilité des nouvelles technologies dans la société.*"[1]

Cette note a également été partagée avec les sénateurs Agnès Canayer et Marc-Philippe Daubresse, en tant de rapporteurs du projet de loi relatif à la prévention d'actes de terrorisme et au renseignement.

La position partagée ici est issue d'une réflexion collective au sein de Renaissance Numérique[2].

[1] Source : questionnaire de la mission.
[2] La liste des contributeurs est mentionnée à la fin du document.

I. Les technologies numériques de sécurité sont en quête d'une gouvernance de confiance

Le champ de la sécurité connaît une multiplication des usages des technologies numériques. Usages publics, privés, voire publics-privés, les applications sont multiples et relancent avec une vive acuité le débat ancien de l'équilibre entre le droit à la sécurité et les libertés publiques.

La multiplication des textes législatifs visant à favoriser le déploiement de technologies toujours plus intrusives dans le champ de la sécurité est un marqueur des attaques successives à cet équilibre. Sur les trente-cinq premières années de l'application de la Loi Informatique et Libertés, douze textes principaux ont été consacrés à la création de fichiers de police ou de justice ou à la régulation de technologies de sécurité (vidéoprotection, empreintes ADN), contre vingt-neuf textes sur les dix dernières années pour introduire ou réguler *a posteriori* des technologies numériques de sécurité (géolocalisation, accès élargi aux données de trafic, nouvelles techniques de renseignement, *IMSI catchers*, drones, consultations élargies de fichiers centraux, nouveaux champs de l'identification génétique, reconnaissance faciale, etc.). Si cette tendance a accompagné l'essor même de l'innovation dans le champ de la sécurité, ce dernier ne suffit pas à justifier cet écart. Rien que sur cette dernière année, on dénombre trois textes liés aux enjeux de sécurité : la proposition de loi pour une sécurité globale préservant les libertés, le projet de loi relatif à la prévention d'actes de terrorisme et au renseignement, et enfin la proposition de loi d'expérimentation créant un cadre d'analyse scientifique et une consultation citoyenne sur les dispositifs de reconnaissance faciale par l'intelligence artificielle, portée par le député Didier Baichère.

Exécutifs et législateurs successifs semblent engagés dans une course en avant pour accroître le champ des usages des technologies numériques dans le domaine de la sécurité et les exceptions juridiques afférentes. Si cette tendance participe d'un affaiblissement progressif des libertés publiques, l'apport efficient pour la sécurité n'est, lui-même, pas toujours démontré. Il semblerait qu'il en soit de même de la mission parlementaire à laquelle répond cette position. Le besoin de ces technologies et leur apport incrémental au regard des moyens, des formations nécessaires et des capacités d'analyse ou de corrélation, est faiblement interrogé dans la lettre de mission. Qu'est-ce que l'on ne peut pas faire sans avoir recours à ces technologies ? A-t-on évalué leur performance au regard du besoin de sécurité dans un environnement où les formes de criminalité ou d'infractions se multiplient, en diversité et en volume ?[3] Ces technologies ne sont d'ailleurs pas décrites, ni même mentionnées en exemples ou en "cas d'usage" précis. Quelles sont les technologies concernées par les termes de "technologies de sécurité" ? La mémoire est-elle une technologie de sécurité ? La multiplication des accès à des bases de données aussi ? Les nouveaux "capteurs"

[3] À ce titre, les technologies de reconnaissance faciale sont un exemple particulièrement illustratif des limites de ces technologies, dont on ne peut en particulier garantir une fiabilité à 100 %. Voir le rapport de Renaissance Numérique sur ce sujet : "Reconnaissance faciale : Porter les valeurs de l'Europe", juin 2020, 104 p.

d'informations sont-ils en soi utiles sans interroger la capacité d'analyse ? Quelles données vont être traitées ? Qui va les utiliser ? Dans quel contexte ? Pour quel motif initial ? Pour quelle évolution des besoins ? Pendant combien de temps ? Cette analyse que l'on précipite en amont de plusieurs rendez-vous sportifs internationaux, mériterait ainsi une réflexion plus approfondie, qui dépasse la création d'un "produit" pour adresser un "besoin" particulier. Renaissance Numérique redoute que l'urgence de rendez-vous sportifs internationaux contribue à modifier durablement nos perceptions en la matière, sans que des justifications solides soient apportées à cette urgence.

Le dur constat que fait le think tank est que le débat a peu progressé depuis sa dernière position en 2015, relative à loi Renseignement, qui a notamment créé la Commission nationale de contrôle des techniques de renseignement (CNCTR)[4]. Renaissance Numérique alertait alors sur l'accumulation des exceptions juridiques relatives aux usages numériques dans le champ de la sécurité, notamment en matière de surveillance. Le think tank appelait notamment à ce que la CNCTR devienne un *"réel organe de contrôle, indépendant, autonome et compétent face aux risques de dérives liés à une surveillance accrue"*. Malgré une forte mobilisation des défenseurs des droits, cet appel n'a eu que peu d'effet et, six ans plus tard, la question est à nouveau posée par le législateur : comment mieux encadrer ce déploiement ?

II. Un prérequis : respecter la méthode instaurée par notre État de droit

Avant d'envisager toute évolution du cadre juridique, il conviendrait déjà d'établir un diagnostic fin du cadre existant et de l'effectivité de son application. Une réflexion récente du think tank relative aux technologies de reconnaissance faciale a par exemple démontré que le cadre juridique entourant ces technologies était relativement bien fourni (droits fondamentaux, textes européens - Règlement général sur la protection des données et Directive Police-Justice -, et nationaux - Loi Informatique et Libertés, réglementation relative à la vidéoprotection -). Or, ce cadre pâtit de faiblesses dans son application qui le rendent peu efficient[5], puisque peu respecté. Qu'en est-il concernant les autres technologies dites "de sécurité" ?

Donner les moyens aux forces de l'ordre d'assurer leur mission passe par un renforcement de la confiance des citoyens envers eux. Pour ce faire, le respect des procédures qui existent au sein notre État de droit est un prérequis. L'objectif de sécurité est nécessaire, mais il ne se suffit pas en soi - pas davantage que d'autres objectifs légitimes -, tant qu'on n'examine pas ses modalités de mise en œuvre. Cela paraît tellement évident qu'il est étonnant de se poser

[4] Renaissance Numérique, "Projet de loi Renseignement. Pas de garantie des droits sans un pouvoir de contrôle effectif", Position, Mai 2015.
[5] Renaissance Numérique, " Reconnaissance faciale : Porter les valeurs de l'Europe", juin 2020, 104 p.

encore la question des modalités de mise en œuvre de technologies de sécurité. Les technologies de sécurité ne relèvent pas - pas davantage que les règles d'engagement des forces de l'ordre -, d'une liberté consistant à "essayer pour voir".

L'innovation exploratoire est néanmoins possible pour déterminer quelle amélioration d'efficacité, quel coût de fonctionnement, quelle intégration opérationnelle et réglementaire, est applicable à ces technologies. Pour ce faire, toute "technologie de sécurité" se déploie dans un contexte opérationnel et réglementaire qui exige une justification préalable de la proportionnalité et de la pertinence de son usage. L'analyse d'impact est une méthode prescrite par les textes en vigueur. Elle ne consiste pas à être d'accord avec soi-même, mais à justifier préalablement auprès d'un organe indépendant ou légitime (le législateur, le Conseil constitutionnel, le Conseil d'État, la Commission nationale de l'informatique et des libertés (CNIL)) d'un certain nombre de critères objectifs : finalité légitime, modalités de collecte d'information, limitation à des données pertinentes et nécessaires, possibilité de filtres et de rejets des données collectées, destinataires limités et justifiés, durée proportionnée, analyse d'impact du recoupement avec d'autres sources, droit d'accès direct ou indirect, mécanisme de contrôle *a posteriori*, voie de recours à caractère juridictionnel, sanctions en cas de violation des règles établies.

À ce titre, nombre de questions de la mission parlementaire se rapportent au principe de proportionnalité. Or, il existe un cadre juridique très clair qui le régit : le devoir de proportionnalité consiste à opérer une mise en balance et réaliser un équilibre entre chacun des principes juridiques en cause – généralement un pouvoir reconnu à l'État (ordre public, force publique) - et des droits fondamentaux des personnes, ou entre plusieurs droits fondamentaux. Le respect du principe de proportionnalité impose qu'une mesure restreignant les droits et libertés respecte ce qu'on appelle le triple test, c'est-à-dire qu'elle soit à la fois : appropriée, en ce qu'elle doit permettre de réaliser l'objectif légitime poursuivi ; nécessaire, c'est-à-dire qu'elle ne doit pas excéder ce qu'exige la réalisation de cet objectif ; et proportionnée, en ce qu'elle ne doit pas, par les charges qu'elle crée, être hors de proportion avec le résultat recherché.[6] Le principe de proportionnalité doit permettre d'évaluer la nécessité ou les apports mesurables (en qualité, en pertinence, en efficacité) des technologies utilisées au regard des objectifs visés, afin de garantir les libertés publiques qui s'expriment dans la vérification que les finalités correspondent aux missions qui sont dévolues, qu'il n'y a pas notamment des données qui sont traitées plus longtemps ou à destination d'autres acteurs que ceux qui sont déclarés. Quels que soient les usages technologiques de sécurité, ils peuvent être traités au travers de la même méthode et répondre à la même question : ces usages passent-ils le triple test et permettent-il de garantir l'équilibre sécurité / libertés publiques ? Renaissance Numérique considère qu'il n'y a donc pas lieu de créer de nouvelles instances pour garantir ces équilibres. Le droit constitutionnel, la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, la Charte des droits

[6] Renaissance Numérique, " Reconnaissance faciale : Porter les valeurs de l'Europe", juin 2020, 104 p.

fondamentaux de l'Union européenne, la jurisprudence de la Cour de justice de l'Union européenne (CJUE), de la Cour européenne des droits de l'homme (CEDH) et du Conseil d'État[7], le Règlement général sur la protection des données (RGPD), l'ensemble de ce *corpus* juridique intègre le principe de proportionnalité, qui n'est pas un principe d'interdiction, mais une condition de validité.

Ainsi, des instances sont déjà en place pour garantir l'application de ce principe. À ce titre, même s'il ne faut pas limiter ce contrôle à la protection des données personnelles, de nombreux droits fondamentaux pouvant être mis en cause[8], il convient de noter que l'analyse de la conformité des technologies de sécurité aboutira toujours à cette question. Dans toutes les circonstances, il y aura un moment où il s'agira d'imputer un comportement (atypique ou criminogène) à une personne ou à un groupe de personnes, même si on part de données comportementales, anonymes, pseudonymes, ou de géolocalisation, qui ne sont pas rattachées à un individu *a priori* identifiable. On arrivera donc toujours à des questions de protection des données personnelles relevant du RGPD ou de la Directive Police-Justice. La CNIL joue ainsi un rôle essentiel dans la régulation de ces technologies par l'application du principe de proportionnalité, qui consiste d'abord à plaider sa cause dans une analyse d'impact pouvant faire l'objet d'un débat contradictoire, afin d'éclairer la décision publique. *A priori*, c'est la CNIL qui est consultée quand sont en cause des données susceptibles d'être qualifiées de personnelles ou de relever de la vie privée des personnes. Quand il s'agit des droits des personnes, c'est aussi cette commission qui est consultée, notamment dans la procédure de droit d'accès indirect[9].

Or, de manière récurrente, exécutifs et législateurs cherchent à remettre en cause ce cadre avec l'argument que ce dernier contraindrait les possibilités de sécurité. Un dernier exemple en date est la proposition de loi pour une sécurité globale préservant les libertés pour laquelle nombre d'acteurs, en dépit de son intitulé, ont soulevé les risques pour les libertés publiques. Dans sa décision du 20 mai 2021, le Conseil constitutionnel a invalidé plusieurs articles de la proposition de loi (7 articles sur 22), dont plusieurs relatifs à l'emploi de technologies numériques par les forces de l'ordre[10]. Le juge constitutionnel a relevé ainsi plusieurs atteintes à l'équilibre entre *"les objectifs de valeur constitutionnelle de prévention des atteintes à l'ordre public et de recherche des auteurs d'infractions et le droit au respect de la vie privée"*.

[7] Dans le cadre d'un rapport État-citoyen, ou administration-citoyen.
[8] Voir sur ce sujet le rapport de l'Agence des droits fondamentaux de l'Union européenne sur les technologies de reconnaissance faciale : 2019, « Facial recognition technology: fundamental rights considerations in the context of law enforcement », 36 pp. : https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law
[9] La CNIL définit ce droit ainsi : *"Toute personne peut demander que la CNIL vérifie les renseignements qui peuvent la concerner dans les fichiers intéressant la sûreté de l'État, la Défense et la Sécurité publique."* Source : https://www.cnil.fr/fr/definition/droit-dacces-indirect
[10] Conseil constitutionnel, Décision n° 2021-817 DC du 20 mai 2021 : https://www.conseil-constitutionnel.fr/decision/2021/2021817DC.htm

Un autre exemple est la difficulté du gouvernement à bâtir une doctrine sur la conservation des données de trafic, de connexion, de localisation ou de mise en ligne de contenus numériques, afin de se mettre en conformité avec les décisions de la CJUE et de la CEDH. Si, dans plusieurs arrêts, cette dernière a reconnu la surveillance de masse, elle exige des *"garanties de bout en bout"*, dont une autorisation *a priori* et un contrôle *a posteriori* par des autorités indépendantes, et l'appréciation à chaque étape du processus de surveillance de *"la nécessité et* (de) *la proportionnalité des mesures prises"*[11]. Il n'y a pas de sécurité sans finalité de sécurité. Or, subsiste dans la loi française une faiblesse de ce contrôle, qui fait qu'une donnée peut être conservée alors que les raisons de sa collecte s'avèrent inexistantes. Il convient de savoir pourquoi les données doivent être captées, la façon dont elles le seront, qui y aura accès et dans quelles conditions, et connaître le tri *a posteriori* sur l'utilité à court ou long terme des données collectées.

Par ailleurs, au-delà des textes, c'est le respect même du cadre en pratique qui fait défaut aujourd'hui. Le temps qui a été par exemple laissé à la CNIL afin qu'elle rende son avis sur la dernière loi Renseignement est assez significatif en la matière. Il est nécessaire de permettre à ces autorités de contrôle de jouer pleinement le rôle que la loi leur consacre afin de construire une stratégie prévisible, c'est-à-dire efficace.

III. Trois voies d'amélioration pour maintenir l'équilibre sécurité / libertés

Comment faire en sorte que le cadre juridique soit pleinement appliqué et le principe de proportionnalité respecté quand il s'agit de déployer des "technologies de sécurité" ? Pour ce faire, Renaissance Numérique entrevoit trois voies d'amélioration.

1. Partager une culture juridique et technique avec les décideurs publics et potentiels utilisateurs des "technologies de sécurité"

Au-delà des aspects purement politiques ou des intérêts privés au financement de telle ou telle technologie de sécurité, la mauvaise application du cadre juridique peut s'entendre également par un défaut de connaissance juridique et technique de la part des décideurs publics et des potentiels utilisateurs, qu'ils soient publics ou privés. Du point de vue de la conception de la loi, peu de législateurs appréhendent des notions comme le "triple test" ou les spécificités techniques de ces technologies, d'autant plus qu'elles sont multiples et évolutives. Il s'ensuit une méfiance, corollaire de la méconnaissance, des contraintes juridiques et des modalités techniques entourant les technologies de sécurité. Ces décisions devraient être éclairées par la réunion de différents types d'expertises et ce, de manière systématique, afin qu'il ne soit pas "trop tard" pour aboutir à un projet charpenté sur l'ensemble des enjeux en présence. Rien que sur le plan juridique, il conviendrait de réunir des experts

[11] Lire à ce sujet la synthèse de Nicolas Hervieu :
https://twitter.com/N_Hervieu/status/1397128120654778370

du droit constitutionnel, de la protection des données personnelles, du droit international ou encore de la sécurité / du renseignement, chaque champ juridique ayant ses particularités. Alors que l'on réfléchit à l'évolution de la formation des agents de l'État et notamment de la haute fonction publique avec la transformation de l'École nationale d'administration en Institut du service public, il conviendrait d'intégrer cette nécessaire diversité et montée en compétences dans les nouveaux programmes.

2. Donner (enfin) un pouvoir de contrôle effectif à la CNCTR

Dans sa position de 2015 sur la création de la Commission nationale de contrôle des techniques de renseignement, Renaissance Numérique invitait à donner à cette instance un pouvoir de contrôle effectif et les moyens financiers, humains et techniques afférents. Or, telle qu'instituée par la loi de 2015, la CNCTR n'a la possibilité ni d'effectuer un contrôle d'opportunité, ni de proportionnalité, ni d'injonction, ni de correction, sur les mesures de renseignement. Pour maintenir les équilibres fondamentaux, notamment entre la sécurité et la vie privée, il est nécessaire que ce contrôle porte sur un examen au préalable de tout dispositif de surveillance avant que ceux-ci ne puissent être employés par les services de renseignement, et le refus que pourrait émettre la CNCTR doit s'imposer aux administrations. Concernant son pouvoir de contrôle *a posteriori*, ce dernier doit s'exercer sans devoir passer par une saisie hypothétique du Conseil d'État manquant de contexte et de matière pour constituer une voie effective à un recours juridictionnel. Aujourd'hui, la CNCTR est enfermée dans un principe de recommandation. Pour être en conformité avec le droit de l'Union européenne, il conviendrait que cette instance soit dotée d'un véritable pouvoir de contrôle. Dans une décision récente, le Conseil d'État a, à ce titre, ordonné au gouvernement "*de réévaluer régulièrement la menace qui pèse sur le territoire pour justifier la conservation généralisée des données et de subordonner l'exploitation de ces données par les services de renseignement à l'autorisation d'une autorité indépendante.*"[12] Il s'inscrit non seulement dans la lignée des exigences de la CJUE[13], mais aussi de celles de la CEDH sur les "garanties de bout en bout".

En 2015, le think tank invitait également à l'existence d'une voie de recours accessible à tout citoyen. Cette dernière doit être simplifiée, digitalisée et la notoriété de la CNCTR renforcée.

[12] Conseil d'État, "Données de connexion : le Conseil d'État concilie le respect du droit de l'Union européenne et l'efficacité de la lutte contre le terrorisme et la criminalité", 21 avril 2021 : https://www.conseil-etat.fr/actualites/actualites/donnees-de-connexion-le-conseil-d-etat-concilie-le-respect-du-droit-de-l-union-europeenne-et-l-efficacite-de-la-lutte-contre-le-terrorisme-et-la

[13] Cour de Justice de l'Union européenne, "La Cour de justice confirme que le droit de l'Union s'oppose à une réglementation nationale imposant à un fournisseur de services de communications électroniques, à des fins de lutte contre les infractions en général ou de sauvegarde de la sécurité nationale, la transmission ou la conservation généralisée et indifférenciée de données relatives au trafic et à la localisation", Communiqué de presse n° 123/20, 6 octobre 2020 : https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-10/cp200123fr.pdf

Le mécanisme d'interpellation en vigueur, qui s'exerce par courrier postal, ne peut aboutir qu'à un débat stérile entre une réclamation et l'absence de réponse utile, la CNCTR n'ayant, en pratique, aucune réponse substantielle à fournir à un justiciable, ni pour estimer infondée sa demande, ni pour l'instruire d'une manière susceptible d'être corrective.

Par ailleurs, il est nécessaire de donner à ces autorités de contrôle (CNCTR, CNIL) les moyens nécessaires à leur mission. Leurs capacités demeurent encore trop limitées et surtout en décalage par rapport à l'élargissement de leur champ de contrôle.

Renaissance Numérique invite les parlementaires à se saisir du projet de loi Renseignement en discussion au Parlement pour donner toute son effectivité à un pouvoir de contrôle de la CNCTR, organisant une compatibilité entre les objectifs de respect du secret de la défense et de la sécurité nationale, et le questionnement légitime de dérives ou d'imprécisions inconciliables avec le devoir de proportionnalité.

3. Renforcer la voie d'accès du citoyen et instaurer une réponse publique

Le droit d'accès indirect qui constitue une autre voie de recours à la disposition des citoyens doit également être renforcé. Il s'agirait de faire évoluer le rôle du commissaire de la CNIL chargé de garantir l'effectivité de ce droit par l'interrogation des organismes publics détenant des informations sur un requérant. En l'état, il faut notamment lui donner les moyens juridiques et techniques nécessaires à ce contrôle, pour que la simple consultation de documents triés par l'administration puisse être assortie d'une capacité à tester - dans le respect des secrets en cause - l'effectivité des mécanismes de purge, lorsqu'il est établi que des informations auraient été stockées sans aucune pertinence.

Depuis 1978, ce droit s'exerce par le truchement d'un commissaire de la CNIL, qui a une fonction juridictionnelle par ailleurs. Il exerce auprès des administrations concernées des droits d'accès des personnes. Cette procédure est sous le contrôle du Conseil d'État et peut faire l'objet d'un contrôle de la Commission d'accès aux documents administratifs (CADA). Un tel mécanisme de contrôle indépendant n'a jamais mis en cause les missions dévolues aux services de police et de justice ni l'efficacité du renseignement policier. Il n'y a dès lors pas lieu de craindre qu'une voie d'interrogation effective ouverte aux justiciables remette en cause l'équilibre sécurité / libertés, sauf à s'exposer à des cycles de construction législative et de destruction jurisprudentielle, qui nuisent profondément à l'efficacité des politiques publiques en matière de sécurité et fragilisent les équilibres démocratiques en suscitant la défiance de l'ensemble de nos concitoyens, qu'ils soient réputés "libertaires" ou "sécuritaires".

Rédaction

Etienne Drouard, Associé, Hogan Lovells
Jennyfer Chrétien, Déléguée générale, Renaissance Numérique

Contribution

Henri Isaac, Président, Renaissance Numérique
Samuel Le Goff, Consultant, CommStrat
Marine Pouyat, Présidente, W Talents
Nicolas Vanbremeersch, Président, Spintank

Utilisation des nouvelles technologies par les forces de sécurité intérieure

Contribution du SCSI-CFDT dans le cadre de la mission confiée par le Premier ministre à M. Jean-Michel Mis

Avant d'examiner les différentes opportunités offertes dans le cadre des missions de la police nationale par les dernières avancées technologiques, il convient de rappeler que notre administration fait malheureusement preuve d'une maîtrise insuffisante des technologies d'ores et déjà accessibles. Ainsi à titre d'exemple, le développement d'un nouveau logiciel de rédaction de procédure, « Scribe », a été annoncé par le DGPN d'alors en novembre 2017. Sa généralisation était promise aux fonctionnaires de police en…2019. Censé intégrer des fonctions de dictée et être interconnecté avec les autres applications numériques métier, ce logiciel Scribe n'a toujours pas vu le jour… Si certaines avancées telles que le déploiement des tablettes et téléphones NEO améliorent le quotidien de la grande majorité des policiers, d'autres chantiers semblent s'enliser durablement.

Il est important de garder à l'esprit le vécu de nos collègues dans les commissariats, qui incarnent la police du quotidien pour nos concitoyens. Ils doivent être intégrés à cette réflexion avec l'objectif d'un gain de temps dans certains tâches répétitives, au risque sinon d'accréditer l'idée d'une police à deux vitesses où seuls quelques services spécialisés bénéficieraient de technologies de pointe tandis que la plupart des policiers n'auraient accès qu'à des outils obsolètes et dépassés.

Comme le relevait le *Livre blanc de la sécurité intérieure* rendu public en novembre 2020, il est impératif d'investir afin de « porter le ministère de l'Intérieur à la frontière technologique ». Cette ambition implique l'adaptation des forces de sécurité intérieure à la société numérique et la modernisation des outils mis à disposition des policiers.

Affilié à la CFDT, le SCSI n'ignore rien des enjeux juridiques et éthiques que soulève la recherche appliquée au domaine de la sécurité. Ils doivent être pris en compte dans un souci permanent d'équilibre avec l'efficacité opérationnelle afin de ne pas obérer l'action des services de police. La police nationale devra être capable d'expliquer clairement et de façon décomplexée au grand public pourquoi et dans quel cadre elle emploie certaines technologies innovantes (drones, intelligence artificielle, reconnaissance faciale…) afin d'améliorer leur acceptabilité sociale.

Pour mettre à la disposition des services d'investigation les outils adaptés aux enjeux contemporains de la mission de police judiciaire, il convient notamment d'explorer les multiples possibilités ouvertes par la biométrie afin d'améliorer l'identification des individus mis en cause. L'intelligence artificielle pourra, elle, permettre de traiter et de croiser des volumes de données très importants afin de gagner un temps précieux dans leur exploitation. Certains logiciels sont déjà utilisés pour aider à l'analyse des interceptions téléphoniques ou de longues séquences de vidéo mais il faudra aller à l'avenir beaucoup plus loin. Cependant, aussi performante soit-elle, la technologie ne constituera jamais qu'une aide à l'enquêteur. Certes précieuse, elle ne peut remplacer son expérience ni ses qualifications.

Les technologies de reconnaissance faciale devront également être expérimentées dans les lieux publics, en commençant par les nœuds de communication que sont les gares et les aéroports, afin de contribuer entre autres à la sécurisation des Jeux Olympiques de 2024. En

cas de résultats concluants, il pourrait s'agir d'une aide importante pour anticiper les troubles à l'ordre public et appréhender des individus recherchés.

Les ressources du ministère telles que le centre de recherche de l'ENSP pourraient être davantage mobilisées dans des projets à finalité opérationnelle. La cartographie prédictive afin d'adapter la présence des équipages sur le terrain en fonction des faits constatée est ainsi une piste intéressante. Dans le registre des équipements, les casques de réalité augmentée auront certainement vocation également à être testés dans les prochaines années.

D'une manière générale, il conviendra d'intégrer à chaque étape de la conception de nouveaux outils les besoins des services et des utilisateurs finaux que sont les policiers. Les supports du futur devront être à la fois simples, fiables et intuitifs. La formation initiale et continue de l'ensemble des corps actifs devra évoluer pour intégrer les avancées technologiques en temps réel.

Dans le domaine des évolutions législatives nécessaires, il est particulièrement important de donner un cadre aux expérimentations qui devront être menées par les services de police. Dans l'immédiat, le SCSI regrette la censure par le Conseil constitutionnel d'une large partie des dispositions de la loi « pour une sécurité globale préservant les libertés » qui sécurisaient juridiquement l'usage de drones et de caméras embarquées sur les véhicules de police. Nous retenons cependant que le principe de l'utilisation de drones par la police n'est pas remis en cause, il faut donc trouver rapidement une formulation qui concilie les finalités de cet usage (prévention des atteintes à l'ordre public et recherche d'auteurs d'infractions notamment) et la protection de la vie privée.

L'utilisation de caméras aéroportées par drones permet en effet aux policiers d'intervenir par exemple pour repérer la préparation d'éventuels guet-apens à travers l'accumulation sur des toits d'immeubles d'objets destinés à être jetés sur les équipages de police en amont des nuits sensibles (14 juillet, nouvel an…). Elles sont également utiles aux unités d'intervention spécialisées telles que le RAID dans la prise d'information qui précède le déploiement des opérateurs. Les drones présentent aussi une plus-value opérationnelle en matière de maintien de l'ordre. Au regard du contexte actuel où des groupes violents intègrent les cortèges de manifestants, ils peuvent aider à leur repérage plus efficace en vue d'une intervention ciblée plus rapide en amont des débordements.

Plus largement, les drones sont utiles dans le cadre de la mission de police judiciaire pour procéder à des constatations et pour les missions de sécurisation générale et de secours. Ils permettent ainsi par exemple de rechercher une personne disparue ou de surveiller plus efficacement une plage. Les forces de sécurité intérieure ne sauraient toutefois se passer de leurs apports sans préjudice pour leurs capacités d'action, d'autant que de nouveaux progrès techniques sont prévisibles dans les années à venir. Les dotations sont encore en revanche trop limitées tout comme les formations des personnels amenés à les piloter.

Concernant les instances de contrôle de l'utilisation des nouvelles technologies par la police, il ne nous apparaît pas nécessaire de créer une nouvelle autorité administrative en sus de celles qui existent déjà (Défenseur des droits, CNIL, CNCTR, etc…). La formation tant des policiers que des agents en charge des contrôles internes et externes devra en revanche intégrer pleinement les doctrines et cadres juridiques d'emploi de ces technologies.

Mission du député Jean-Michel Mis

« Pour un usage responsable et acceptable par la société des technologies de sécurité »

*

1/ Objectifs de la mission

La mission souhaite explorer, lors des auditions et via les contributions écrites, les axes suivants :

- Les **opportunités offertes par les nouvelles technologies au service d'une meilleure offre de sécurité** en analysant les besoins des forces de sécurité, entre autres dans la perspective des grands événements sportifs de 2023 et 2024.

- Les principes nécessaires à **la préservation des libertés** en définissant un cadre d'emploi global et cohérent des technologies de sécurité et en associant la société civile à cette définition pour renforcer la compréhension et l'acceptabilité des nouvelles technologies dans la société.

2/ Questions

La notion de « technologies de sécurité » est large. Quelles sont les principales selon vous ? [Par exemple : traitement des données (textuelles, images, sonores), biométrie, mobilité.]

En automatisant différentes tâches d'analyse traitant des informations actuellement non corrélées, des technologies existantes peuvent être rendues plus efficientes. Il faut considérer ces technologies comme une « augmentation de la capacité opérationnelle » des solutions en place tendant vers une efficience maximale. Si ces technologies « d'augmentation de la capacité » embarquent des fonctions de contrôle de la compromission, elles deviennent un moyen de reprendre la main sur des technologies non-souveraines.

Par exemple, analyser en temps réel des informations de type nombre de personnes dans un lieu (capteur IOT), mouvement de foule (vidéo-protection), séquence de sons anormaux (capteur d'anormalité sonore) et trafic internet issu des équipements télécom (sondes sur le réseau opérateur) permet d'anticiper un événement connu, soit par une action humaine ou automatique (régulation des flux).

De même, dans le cyberespace, savoir qu'un vecteur d'attaque cyber est déjà présent dans de nombreux équipements rebonds permet de le bloquer automatiquement pour éviter son action. Ce sont par exemple des caméras de vidéo-protection qui extraient de très faibles données sans autorisation vers des serveurs étrangers de manière très régulière. La technologie permet ainsi de détecter et de contrer des tentatives de compromission des systèmes.

Pour quelles finalités ? *[Par exemple : détection de situations, analyse prédictive, suivi des personnes.]*

En étant capable de détecter et d'analyser des situations anormales dans le monde réel ou dans le monde cyber et de les corréler, la capacité de protection s'en trouve accrue. Avec une technologie déployée massivement, une protection globale est alors possible lors de grands événements. Dans le cyberespace, des technologies leurres peuvent être déployées en amont des futures infrastructures pour apprendre et comprendre les processus d'attaque pour mieux les contrer sur les infrastructures de production de service. En outre, identifier l'origine des attaques permet de riposter sur les rebonds d'attaque pour inhiber les vecteurs d'attaques. La massification de ces solutions ne peut être réalisée qu'avec des solutions simples, automatisées et à faible coût. Elles doivent permettre de faire évoluer les acteurs en place sur les technologies traditionnelles sans chercher à remplacer l'existant, visant une amélioration permanente.

Pensez-vous qu'elles permettraient d'anticiper les évolutions des missions de sécurité dans les 10 à 20 ans à venir ? Comment voyez-vous ces évolutions ?

Les technologies de sécurité peuvent clairement rendre plus efficientes les technologies actuelles en réalisant à haute fréquence des actions actuellement manuelles. Par exemple :

- La détection d'anormalité sonore couplée à des solutions de vidéoprotection permet de rendre plus performante la détection de situation dégradant la sécurité (anticipation) ou nécessitant une intervention instantanée. Les missions pourraient ainsi évoluer en permettant l'envoi de secours adaptés à la situation avant l'arrivée sur place.
- En automatisant certains traitements basiques aujourd'hui réalisés par des ressources humaines, la technologie (machine learning) permet une meilleure efficience de traitement des événements ainsi qu'une possibilité de concentration des ressources disponibles sur des tâches à haute valeur ajoutée.
- Une base de connaissance des événements analysés en amont permet d'être plus réactif sur le traitement d'événements similaires lors de leur survenu sur de nouvelles infrastructures (détection des signaux faibles).

La détection et la connaissance du contexte sont fondamentales pour permettre aux organisations de s'adapter à l'évolution de la menace, de manière commune pour éviter les failles sur l'ensemble de la chaîne de valeur.

Ces évolutions ouvrent des perspectives de création de nouveaux métiers, à la croisée des chemins entre technologies physiques et cyber (supervision mutualisée des événements cyber…) sans nécessité de haut niveau de formation pour les opérateurs.

Sur chaque technologie prioritaire évoquée, quel est l'état de développement de l'industrie française ? Que lui manque-t-il pour se perfectionner ?

Sur les technologies évoquées, de nombreuses technologies innovantes existent, mais rencontre un problème majeur lors de la phase de développement commercial : la facilitation et l'accompagnement sur le marché pour atteindre un seuil de rentabilité à même de dégager des moyens de continuer la R&D.

Ainsi, plusieurs freins impactent le développement des technologies innovantes :

- Le financement de la commercialisation en phase d'amorçage n'existe pas. Ainsi, un inventeur technologique ou un développeur informatique doit être expert en analyse de marché et commerce pour assurer le développement de son projet.
- La commande publique bloque l'accès à son marché en imposant des références sur 3 ans, antinomique avec l'innovation.
- Les grands groupes demandent une solidité financière sur 3 bilans comptable pour référencer de nouveaux fournisseurs.
- Le paiement des aides à l'innovation peut prendre plusieurs mois lors de phases critiques de la vie d'une jeune structure, alors que de nombreuses sollicitations par des fonds étrangers entrainent soit une perte d'énergie soit un rachat de la technologie.
- A contrario, les solutions étrangères profitent d'une exclusivité sur leur marché permettant d'assurer un développement complet des solutions avant de les exporter (DARPA) et de venir concurrencer les solutions innovantes. Citons le GPS en exemple, ou ARPANET ancêtre d'internet pour lequel le français Louis Pouzin a participé à l'invention.

Aussi, permettent d'accéder au marché cible au technologie émergeante tout en simplifiant l'accès au financement de la commercialisation des solutions permettrait à de nombreuses pépites de passer le cap de la startup.

Comment les configurations techniques peuvent-elles concilier une utilisation de ces technologies et des garanties pour les libertés (protection des données, contrôles automatisés, etc.) ?

Avec la notion d'extra territorialité des lois et aussi les expériences avérées d'espionnage entre « alliés », nous constatons que le droit ne nous protège pas ou peu. Il faut donc opter pour des dispositifs technologiques permettant de garantir le secret des échanges et l'automatisation des contrôles. En outre, il serait souhaitable que les acteurs en charge de la garantie des libertés soient accompagnés par de véritable experts des technologies actuelles issu de la société civile, en visant un accompagnement pour une co-construction de solutions plutôt que des contrôles entraînant des sanctions bloquant l'accès au marché.

Les cadres d'expérimentation sont souvent mis en avant pour le perfectionnement de ces technologies. Quelles sont selon vous les priorités ? Quels seraient les contours de ces cadres ? A quelles fins ?

Les cadres d'expérimentation sont fondamentaux pour l'expérimentation de technologies dont on ne sait pas a priori quels pourraient être les avantages sociétaux et concurrentiels. Il faut donc introduire rapidement la possibilité de créer simplement un cadre d'expérimentation qui doit être borné dans le temps mais doit laisser un périmètre assez large et souple afin de pouvoir opérer sur tout type de données ou de traitement afin de faire avancer la recherche. Ces cadres doivent être pilotés par des structures indépendantes de tout lobbie technologique, politique ou industriel afin que l'on puisse faire progresser la technologie mais aussi certains règlements complétement obsolètes. Nous tenons à citer en exemple l'arrêt d'une expérimentation sur des capteurs de détection d'anormalités sonores 12 mois après son lancement par une collectivité suite à un contrôle juste avant le déploiement de la solution. Les retours de l'organisme ont démontré l'absence de cadre juridique sur cette nouvelle technologie, mais aucune proposition d'accompagnement sur l'adaptation de la solution ou de la loi. La collectivité a stoppé l'expérimentation, n'a pas honoré la totalité des budgets d'expérimentation programmés argumentant un arrêt du projet, mettant en difficulté la trésorerie de la startup. In fine, le projet stoppé a vu le jour en Angleterre pour lutter contre les nuisances sonores…

*

Ce questionnaire est indicatif et ne prétend pas de couvrir l'intégralité des enjeux posés par les technologies de sécurité. La mission recueillera tout élément qui lui sera apporté afin de l'intégrer au mieux dans sa réflexion.

Paris, le 11 Juin 2021

Monsieur le Député,

Vous trouverez ci – dessous notre contribution à votre demande par mail du 21 Mai 2021.

Composante technique et scientifique majeure de l'enquête judiciaire ou de la surveillance de Police, les biométries sont depuis longtemps indispensables à la recherche d' auteurs d' infractions. Leur rôle n a jamais cessé de s'étoffer depuis un siècle.
Tout service public moderne de sécurité doit s'y adapter et y recourir dans le respect des valeurs et des normes de l état de droit

Nos services PTS disposent actuellement de caméras 360° THETA Z1 qui permettent une visite virtuelle de la scène de crime, de scanners infra rouge DOT PRODUCT qui permettent de capter la scène en 3D mais aussi des drones pour effectuer des recherches sur de larges périmètres de constatations des scènes d infractions.

Cependant, bon nombre de ces moyens sont en dotation dans les services centraux PTS. Une plus large attribution permettrait à certains services territoriaux (SRPTS ou SDPTS) de répondre à des demandes ou besoins de plus en plus fréquents dans un délai toujours plus réduit.

Concernant la biométrie, elle recouvre l'ensemble des techniques permettant de reconnaître un individu à partir de ses caractéristiques physiques biologiques voire comportementales : empreintes papillaires et génétiques, visage, iris de l œil, la voix ou encore récemment l'odeur corporelle et le contour de l'oreille qui permettent d'observer la façon de se mouvoir.
Deux grandes catégories de données se distinguent donc :
- les traces collectées en milieux non contrôlés
- les données biométriques (empreintes) qui sont conservées et liées à une personne ou identité connue.

Il est indispensable de mettre ces possibilités émergentes, offerte par la science, au service des agents PTS (Traitement automatisé de l'image, de la voix, du texte en commande vocale, compte rendu vocal, analyse des bandes vidéos etc...)

Nous vous confirmons que la Police Technique et Scientifique évolue vers une organisation efficiente et cohérente.
Face à une délinquance de plus en plus complexe, la PTS moderne fait partie des appuis judiciaires développés pour concourir à la réussite des investigations : faire face à la délinquance du quotidien, à la criminalité organisée voire au terrorisme.

Au travers de ces méthodes, les magistrats pourront trouver une meilleur lisibilité afin d' intensifier les recours aux laboratoires publics plutôt qu' aux structures privées

Pour cela, il faut innover, optimiser et harmoniser.

Plusieurs institutions de Police Technique et Scientifique à l'étranger (Allemagne, Royaume - Uni), se sont engagées dans l' approche multi biométrique en utilisant la donnée dite « pivot ».
L'ensemble de leurs fichiers utilisent des ensellements biométriques interconnectés, via l'élément pivot dans le strict respect des conditions d'inscription et de la durée de conservation.

La Police Technique et Scientifique française ainsi que les services en charge des fichiers de documentation criminelle, gagneraient en efficacité à adopter la même approche multi – biométrique.
Une coopération européenne devrait être recherchée afin que les agents puissent disposer d' outils adéquats leur permettant d'interroger via une interface unique, l'ensemble des systèmes nationaux et européens (données alphanumériques et biométriques).
L'objectif est de pouvoir déterminer de manière rapide et fiable si la personne concernée (identité vérifiée) est inscrite à un ou plusieurs fichiers.

L'architecture des principaux fichiers de police judiciaire FPR, TAJ, FAED, FNAEG devra par ailleurs être restructurée.

Il est important de rappeler que le renforcement des dispositifs biométriques de sécurité intérieure passe par la modernisation des outils criminalistiques existants

Il subsiste encore une lourdeur inutile de certaines méthodes de prélèvements désormais désuètes. Celles ci pourraient être simplifiées grâce à la dématérialisation complète des opérations :
Concernant les prélèvements des traces sur scènes d'infraction, nous devons obtenir des appareils spécialisés pour les prises de vue, ainsi que pour le recueil des empreintes sur les personnes.

En matière de biométrie du visage, l'objectif scientifique et technique d'une façon générale doit être de hisser cette biométrie au niveau des deux biométries historiques : papillaire et génétique.

La biométrie du visage présente des avantages spécifiques car elle permet un traitement dématérialisé de la scène d'infraction. Elle constitue une approche complémentaire des biométries papillaire et génétique qui nécessitent un traitement physique de la scène d infraction.

Les pré-requis indispensables à la montée en puissance de la biométrie faciale seront d'améliorer la qualité des images de référence.

Expérimenter la reconnaissance du visage dans l'espace public à l'instar de ce qui se pratique dans plusieurs pays européens, est une réflexion sérieuse sur laquelle il faudra positionner un cadre pour éviter les dérives.

L'odorologie et le traitement d'une biométrie complémentaire nécessitent une recherche d'amélioration des performances d' identification et la convergence d'un moyen de prélèvement commun PN/GN.

Il faut renforcer la capacité d'innovation technologique dans la PTS en développant une recherche et une innovation ouverte à l'ensemble des agents, en partenariat avec les systèmes européens.
Nous vous proposons la création d une plate-forme qui fédérerait de manière souple l' ensemble des acteurs de la PTS.

Pour conclure, il faut conserver « la main humaine » dans la prise de décision et le contrôle des technologies. Les algorithmes d'intelligence artificielle sont en premier lieu des outils d'aide à la décision. Ils peuvent intervenir à des degrés variables dans la prise de décision selon la

complexité des enjeux, mais leur potentiel en autonomie doivent toujours être sous contrôle direct ou a posteriori de la part d'opérateurs.