Le Réseau Radio du Futur : Un outil de communication majeur pour les missions des forces de sécurité et de secours

Préfet Guillaume LAMBERT

Préfet, Conseiller au cabinet du Secrétaire Général
Responsable du programme Réseau Radio du Futur
Ministère de l'Intérieur

Les enjeux du programme Réseau Radio du Futur (RRF)

Les enjeux de sécurité et les risques, que notre pays doit prendre en compte, ont suscité une réflexion sur la nécessité de créer les conditions d'une sécurité globale, au-delà des traditionnelles césures entre services de l'État et ceux relevant des collectivités locales, entre les acteurs publics et les acteurs privés. Les attentes des concitoyens en matière de sécurité et secours exigent un décloisonnement de l'ensemble des services qui concourent au quotidien à leur protection.

Dans ce contexte d'émergence de nouvelles menaces (terroristes, violences urbaines, dérèglement climatique, crises sanitaires…) et de sollicitations croissantes des services de sécurité et de secours, disposer d'outils de communication adaptés est essentiel.

Les réseaux radio actuels des forces de sécurité et de secours actuels sont désormais vieillissants et méritent d'être renouvelés : le réseau RUBIS de la Gendarmerie a été créé en 1986, tandis que l'Infrastructure Nationale Partageable des Transmissions (INPT) a été lancée dans sa version ACROPOL pour la Police en 1994.

Ces réseaux proposent des fonctions qui ne sont plus aujourd'hui adaptées aux besoins des services de sécurité et de secours (interopérabilité très restreinte, partage de données et vidéo inexistantes à titre d'exemples). Ils reposent sur une technologie antérieure à la deuxième génération (2G) de la téléphonie mobile et sont devenus, avec le temps, coûteux en termes d'entretien et de maintenance. En effet les équipements d'infrastructure sont vieillissants, qu'ils s'agissent des ateliers d'énergie, des batteries de secours, de la centrale de gestion de l'infrastructure ou encore des climatiseurs et des extracteurs d'air. Ainsi, les coûts de maintenance de ces réseaux sont amenés à croitre avec le temps.

En synthèse, on observe un décalage technologique entre les outils de communication mis à disposition des services de secours et de sécurité (des terminaux radio bas débit) et les usages de la société qui utilise des smartphones fonctionnant en 4G et bientôt en 5G. En les remplaçant, le RRF répond doublement aux attentes du concitoyen car il fournit un service de communication au meilleur de la technologie et

transversal entre tous les acteurs de la sécurité et du secours, tout en réalisant des économies d'échelle.

C'est pourquoi l'évolution des moyens de radiocommunication en France est un tournant majeur à ne pas manquer, car leurs limitations actuelles nécessitent la création d'une solution offrant un ensemble d'applications, d'outils et de services adaptés à l'ensemble des utilisateurs et qui restent accessibles économiquement.

Un système de communications mobiles pour missions critiques s'appuyant sur les standards internationaux

L'objectif du RRF est d'offrir dès 2023 un système de communication haut débit, sécurisé, résilient et pleinement interopérable aux services de sécurité et de secours en s'appuyant sur les standards définis par le groupe 3GPP au titre des communications dédiées aux missions critiques.

De ce point de vue, le programme RRF représente une évolution profonde des moyens de communication des services de sécurité et de secours

Le RRF s'appuiera en effet sur les infrastructures des opérateurs privés de téléphonie mobile, en offrant un dispositif de priorité/préemption pour éviter toute saturation en cas de congestion du trafic, ainsi que sur des dispositifs projetables d'extension de couverture radio 4G pour garantir la résilience des communications haut débit.

La réalisation du système de télécommunication critique RRF passe par l'acquisition de trois éléments fondamentaux qui formeront le cœur technique de la future infrastructure de communication critique :

- une capacité d'accès à la couverture radio 4G (puis 5G) et aux services de téléphonie et d'internet auprès de deux opérateurs de réseaux mobiles ;
- l'acquisition des capacités techniques d'un opérateur de réseau mobile virtuel (MVNO) à savoir un « cœur » de réseau télécom, un système d'information de gestion du RRF et de ses abonnés, un centre d'opération du réseau RRF (NOC), une offre de terminaux mobiles ;
- l'acquisition d'une capacité à délivrer des services applicatifs de communications pour missions critiques (MCx), permettant d'organiser des communications multimédias de groupe au profit des abonnés du RRF en bénéficiant d'une qualité de service avec priorité et préemption dans les réseaux 4G.

Un service de communication dédié aux acteurs de la sécurité et des secours dans leur diversité

Le RRF s'adresse aux services qui ont en charge au quotidien les missions de sécurité et de secours, la protection des populations et la gestion des crises et des catastrophes.

Les communautés utilisatrices du RRF recouvrent donc une assez grande diversité d'organisations puisque parmi les futurs services éligibles on trouvera aussi bien les préfectures que les maires, la gendarmerie et la police nationales que les polices municipales ou le ministère des armées au travers de la mission Sentinelle, les SDIS (services départementaux d'incendie et de secours que les moyens nationaux de la sécurité civile ou les services d'aide médicale urgente (SAMU) mais aussi le ministère de la justice, les douanes, etc.

Le RRF a été conçu pour prendre en considération les besoins de chacune de ces communautés, tout en permettant la collaboration entre les différents acteurs. A ce titre, les communautés utilisatrices du RRF font partie intégrante de la gouvernance du programme, et seront représentées au conseil d'administration de la future structure porteuse. Elles ont été associées en détail à la conception de la solution, permettant à la maitrise d'ouvrage du RRF de

connaître précisément les besoins et contextes d'emplois de chacune d'elles.

Des usages inédits et innovants au bénéfice des communautés utilisatrices

La solution RRF offrira à ses communautés utilisatrices de nouveaux usages de captation et de diffusion de la donnée opérationnelle en temps réel, absolument inédits dans le quotidien des utilisateurs.

Le RRF permettra deux nouveaux usages principaux :

- De nouvelles fonctionnalités de communication critiques multimédias : le RRF repose sur des technologies standardisées, offrant des possibilités élargies à ses utilisateurs : communications vidéo de groupe ou interpersonnelles, géolocalisation des utilisateurs et points d'intérêt… Standardisés par le 3GPP, ces services de communications pour missions critiques sont accessibles à l'ensemble des utilisateurs du RRF, sur le terrain comme en salle de commandement.

  Les services missions critiques offrent trois types de fonctionnalités principales :

  - le MCPTT (Mission Critical Push-To-Talk) : service de conférence vocale ;
  - le MCVideo : service de conférence vidéo qui utilise les capteurs vidéo du smartphone pour échanger des vidéos soit en temps réel entre les utilisateurs d'une conférence MCx, soit en asynchrone dans des outils de type messagerie instantanée ;
  - le MCData : service de connectivités de données : fichiers, géolocalisation, informations sur les terminaux (couverture, niveau de batterie du terminal).

- Une interopérabilité complète et native : le RRF est par conception un système de communication commun à l'ensemble des acteurs de la sécurité et du secours et nativement interopérable. Les échanges en interservices bénéficient ainsi du même ensemble de fonctionnalités de communications multimédias de groupes que celui disponible au sein d'une communauté, avec les mêmes exigences de sécurité et de réactivité et dans le respect des doctrines d'emplois de chaque communauté.

Ce passage à l'ère de la donnée des communications opérationnelles des services de sécurité ou de secours devra se réaliser en respectant scrupuleusement les obligations européennes et nationales en matière de protection des données personnelles.

La possibilité de capter et de diffuser des données en temps réel n'impliquera pas son utilisation en continu. L'architecture du RRF empêche d'ailleurs par défaut le partage de données, qui n'est possible que par exception quand la situation opérationnelle l'impose. C'est le contexte de la mission, et donc la finalité, qui conduira à activer un partage en temps réel de données audio et vidéo, selon un principe de minimisation des données (respect du principe de proportionnalité). C'est ainsi qu'a été identifié un ensemble restreint de finalités où la criticité et la probabilité d'occurrence d'une situation justifieraient cet usage, comme par exemple la prévention des risques d'atteinte à l'intégrité physique d'un agent d'un service de sécurité ou de secours, les opérations de secours aux personnes, l'existence d'un péril imminent, la lutte anti-terroriste, la prévention des risques d'atteintes aux biens et aux personnes dans le cadre de troubles graves à l'ordre public.

L'usage de ces données opérationnelles d'environnement se traduira par des apports concrets pour les acteurs de la sécurité et du secours :

- **L'amélioration de l'intelligence situationnelle, à travers :**
  - **une meilleure efficacité opérationnelle** : la diffusion de vidéo avec audio permet de retranscrire de manière plus fiable et détaillée le contexte d'une intervention, au bénéfice des

opérateurs en salles ou des utilisateurs sur le terrain qui, habilités à accéder aux données, disposent tous du même niveau d'information ;

- **une identification facilitée** des situations et individus potentiellement à risques.

- **L'amélioration de la sécurité des utilisateurs lors d'une intervention, à travers :**
  - **une meilleure compréhension des situations de danger** pour les utilisateurs (appel de détresse géolocalisé, fonctionnalité de protection des travailleurs isolés (PTI) paramétrable, etc.), et des réponses plus adaptées à ces situations ;
  - **une levée de doute plus fiable** par les opérateurs des salles de commandement en cas d'appel de détresse (écoute d'ambiance, déclenchement des flux vidéo du terminal…).

- **L'amélioration de la sécurité des citoyens et du grand public** à travers des interventions plus rapides ou une meilleure sécurisation de grands évènements car mieux renseignées, un meilleur partage de l'information entre les différents services intervenant et la capacité de bénéficier de l'appui d'experts à distance et en temps réel.

Une approche « *privacy by design and by default* »

La protection des données a été prise en compte dès la conception de l'architecture du RRF. Le RRF sera compatible avec les exigences élevées du socle de sécurité du ministère de l'Intérieur afin, notamment, d'assurer un haut niveau de sécurisation de l'accès au service et de traçabilité des actions réalisées en son sein par les utilisateurs.

Cette démarche de sécurisation et de protection des données se déclinera en un ensemble de règles techniques et organisationnelles. Les dispositions techniques intègrent la sécurisation physique des composants du RRF, une sécurisation technique des données à toutes les étapes de son utilisation (intégrant l'authentification des utilisateurs et des terminaux et le chiffrement des données) et une supervision SSI opérée par le centre de cyberdéfense du ministère de l'Intérieur. Des règles organisationnelles complèteront ces dispositions et comporteront notamment des actions de sensibilisation des utilisateurs au bon usage de la donnée.

Le RRF est construit selon un principe de cloisonnement entre communautés utilisatrices, et au sein de ces dernières. Ce cloisonnement garantit la limitation de l'accès des utilisateurs aux communications qu'ils ont à connaître spécifiquement. Ainsi, chaque communauté dispose de son propre environnement de communication, par défaut fermé aux autres utilisateurs. Ces derniers sont strictement identifiés et authentifiés, et rattachés à une communauté.

Les communications s'organisent au sein de ces environnements à travers des groupes de communication fermés, appelés « conférences ». Ces conférences sont également fermées par défaut, et ne rassemblent que les utilisateurs habilités à accéder aux données. Au sein de ces conférences, les utilisateurs ont accès à des fonctionnalités d'échange multimédia, permettant une communication riche entre membres.

Chaque communauté organise son arborescence de conférences en fonction de sa doctrine d'emploi. Une conférence peut être permanente ou temporaire, active à tout moment ou à la demande. Des conférences peuvent ainsi être définies pour correspondre à des périmètres géographiques fixes (la zone d'intervention du centre d'incendie et de secours du département en question), à un service ou un ensemble de services (les services composants une direction départementale de la sécurité publique par exemple), à une intervention précise (les services engagés à la suite d'un accident de la route) ou à toute autre fin définie par la communauté.

Ces principes d'organisation des conférences s'appliquent aux communications au sein d'une communauté, comme entre plusieurs communautés. Vecteur d'interopérabilité, le RRF permet ainsi de créer, à la volée ou de manière pérenne, des conférences associant utilisateurs de différentes communautés, habilités à accéder aux données d'un même sujet d'intérêt ou d'une même intervention. Par exemple, il sera possible de créer une conférence associant des utilisateurs issus de l'escadron départemental de sécurité routière du Vaucluse, de la direction interrégionale des routes Méditerranée, du SDIS du Vaucluse et de l'opérateur des autoroutes du Sud de la France - dans les mêmes conditions d'accès et de cloisonnement que pour une conférence propre à une communauté. Une doctrine d'interopérabilité viendra définir les principes de communication interservices généraux et propres à chaque environnement (local ou thématique).

Trois types d'utilisateurs sont définis au sein du RRF, en fonction de leurs rôles et des droits qui leurs sont associés :

- Administrateur fonctionnel d'entité, en charge de créer et de gérer les conférences permanentes, et de créer et gérer les droits des utilisateurs de sa communauté. Un administrateur fonctionnel n'a, par défaut, pas accès aux contenus des échanges transitant sur une communauté ;
- Opérateur de salle de commandement, et dont la mission consiste à exploiter en temps réel les conférences dont il a la charge, d'autoriser leur accès aux utilisateurs et de définir les droits de ces derniers au sein des conférences. Il peut également créer des conférences à la volée s'il dispose des droits pour ce faire ;
- Opérationnel, qui correspond à la grande majorité des futurs utilisateurs ayant accès aux conférences définies dans leurs droits par l'administrateur fonctionnel, et dans les conditions définies par l'opérateur de salle de commandement.

Ces principes de cloisonnement et de gestion fine des droits et des accès garantissent une diffusion des données captées restreinte aux utilisateurs habilités à accéder aux données. Ces garanties restent applicables également dans le cadre d'un environnement plus complexe, par exemple lors d'une intervention en interopérabilité mobilisant un grand nombre d'acteurs issus de différentes communautés. Cette architecture garantit un accès exclusif de certains types de données aux seuls utilisateurs habilités à y accéder (comme, par exemple, les données de santé).

Une communication directe multimédia entre deux ou plusieurs utilisateurs d'une communauté est par ailleurs également possible, dans le respect des mêmes doctrines d'emplois et règles de gestion métier. Un utilisateur ne pourra contacter qu'un ensemble de destinataires définis par ces dernières. Ce type de communication est également possible entre utilisateurs de communautés différentes, si les règles de gestion définies en fonction des doctrines d'emplois le permettent.

Planning et Plan de déploiement du RRF

La démarche de déploiement du RRF vise prioritairement les territoires pilotes des grands évènements sportifs des années à venir. L'objectif principal en termes de déploiement du RRF est d'être au rendez-vous des deux échéances majeures que sont la coupe du monde rugby de 2023 et les jeux olympiques et paralympiques de 2024 sur les territoires hôtes de ces deux événements, prioritairement pour ce qui concerne les acteurs clés en charge de la sécurité et des secours : préfectures, services de police et de gendarmerie nationales, services d'incendie et de secours (SIS), SAMU/SMUR, militaires de l'opération Sentinelle, polices municipales.

Ces deux grandes échéances conditionnent la conception et le déploiement de ce projet. Ainsi, l'avis de marché en vue de sélectionner les industriels qui apporteront leur concours à la réalisation du cœur technique de RRF a été publié le 1er décembre 2020. La passation des marchés devrait intervenir en novembre prochain, ce qui permettra de déployer le RRF auprès des entités utilisatrices pilotes au premier semestre 2023. Un plan de construction de l'architecture par versions successives a ainsi été mis en place afin de sécuriser la disponibilité des principaux services en version 1 (premier opérateur raccordé, fonctionnalités essentielles et déploiement des 90 000 premiers abonnés mobiles) dès fin 2023 avant de gagner en fonctionnalités pour les versions suivantes du RRF. Puis raccordement du deuxième opérateur, déploiement de nouvelles fonctionnalités et extension du périmètre de déploiement à 100 000 abonnés mobiles supplémentaires pour la V2 disponible début 2024. Enfin, fonctionnalités complètes déployées sur l'ensemble du périmètre d'abonnés mobiles cible pour la V3 à compter de début 2025.

Au total, plus de 300 000 agents sont susceptibles d'être utilisateurs de ce système de communications. Le continuum des acteurs de sécurité et de secours est l'ambition d'offre de services et d'interopérabilité du RRF.

Dès octobre 2017, à l'occasion de son discours aux forces de sécurité et de secours, le Président de la République a lancé le programme RRF en soulignant les enjeux majeurs attachés à sa réalisation, *« Un des grands projets régaliens sera le réseau radio du futur à haut débit commun à la police, la gendarmerie et la sécurité civile qui devra bénéficier d'un haut niveau de résilience en cas de crise et des meilleures technologies numériques disponibles. Ce sera un grand projet industriel français et européen dont le déploiement doit se faire le plus rapidement possible et fait aussi l'objet d'un engagement clair en termes financiers dans le cadre du grand plan d'investissement. »*

Ce nouveau système offrira à celles et ceux qui nous protègent des bénéfices opérationnels majeurs. La capacité de partager une même information, notamment à l'aide de flux vidéo, sur le terrain et en salles de commandement, améliorera l'intelligence situationnelle des communautés utilisatrices, permettant un meilleur engagement et un meilleur pilotage des moyens. Les intervenants sur le terrain verront leur sécurité renforcée grâce au partage de leurs géolocalisations et à une meilleure compréhension de leurs environnements d'intervention. L'interopérabilité native du RRF permettra d'étendre au besoin ces capacités aux échanges entre services et facilitera la coopération au quotidien.

Les retombées et les impacts pour la société civile touchent tous les secteurs (tourisme, exportation, insécurité, …). Les gains directs et indirects sont nombreux : (sécurisation des interventions des agents, baisse du nombre de victimes, …) avec de réelles économies d'échelle qui seront détaillées en annexe en fin d'article.

Le RRF permettra à la France de rejoindre les quatre autres premiers pays au monde ayant mis à disposition de leurs services de sécurité et de secours des outils de communications de dernière génération : le Royaume Uni avec son réseau ESN et le projet ESMCP, les Etats-Unis avec FirstNet, la Finlande avec Virve 2.0 et la Corée du Sud avec SafeNet.

Les impacts positifs attendus du déploiement du Réseau Radio du Futur