N° 454

SÉNAT

SESSION ORDINAIRE DE 2021-2022

Enregistré à la Présidence du Sénat le 7 février 2022

RAPPORT D'INFORMATION

FAIT

au nom de la délégation aux collectivités territoriales et à la décentralisation (1)
sur le **Numérique, protection des populations et territoires***,*

Par M. Antoine LEFÈVRE, Mme Anne-Catherine LOISIER et M. Jean-Yves ROUX,

Sénateurs et Sénatrice

(1) Cette délégation est composée de : Mme Françoise Gatel, *présidente* ; MM. Rémy Pointereau, Guy Benarroche, Jean-Pierre Corbisez, Bernard Delcros, Mmes Corinne Féret, Michelle Gréaume, MM. Charles Guené, Éric Kerrouche, Antoine Lefèvre, Mme Patricia Schillinger, M. Pierre-Jean Verzelen, *vice-présidents* ; M. François Bonhomme, Mme Agnès Canayer, M. Franck Montaugé, *secrétaires* ; Mmes Nadine Bellurot, Céline Brulin, MM. Bernard Buis, Laurent Burgoa, Thierry Cozic, Mmes Chantal Deseyne, Mme Catherine Di Folco, MM. Thomas Dossus, Jérôme Durain, Mme Dominique Estrosi Sassone, MM. Fabien Genet, Hervé Gillet, Jean-Michel Houllegatte, Mmes Muriel Jourda, Sonia de La Provôté, Christine Lavarde, Anne-Catherine Loisier, MM. Pascal Martin, Hervé Maurey, Franck Menonville, Jean-Marie Mizzon, Philippe Mouiller, Olivier Paccaud, Philippe Pemezec, Didier Rambaud, Mme Sylvie Robert, MM. Jean-Yves Roux, Laurent Somon, Lucien Stanzione, Cédric Vial, Jean Pierre Vogel.

SOMMAIRE

Pages

RECOMMANDATIONS DU RAPPORT 5

AVANT-PROPOS 7

I. LES BONNES PRATIQUES LOCALES 9

A. EN MATIÈRE DE PROTECTION DE L'ORDRE PUBLIC 9

B. EN MATIÈRE DE SÉCURITÉ CIVILE – PRÉVENTION DES RISQUES 15

II. LES RECOMMANDATIONS 27

A. LE RECOURS AUX TECHNOLOGIES : UNE DÉMARCHE QUI DOIT ÊTRE FONDÉE SUR UNE MÉTHODE RIGOUREUSE ET UN BILAN COÛT / AVANTAGES ACTUALISÉ ET PUBLIC 27

B. LA SENSIBILISATION DES ÉLUS ET DU PERSONNEL AUX ENJEUX DE LA CYBERSÉCURITÉ 28

C. DÉVELOPPER LES USAGES NUMÉRIQUES EN PLEINE CONFORMITÉ AVEC LE PRINCIPE DE SUBSIDIARITÉ 32

D. DONNER UNE BASE LÉGALE À L'USAGE DES DRONES PAR LA POLICE MUNICIPALE 34

E. RENFORCER LA COOPÉRATION ENTRE LES COLLECTIVITÉS TERRITORIALES ET LES SERVICES DÉCONCENTRÉS DE L'ETAT DANS LE DOMAINE DE LA PROTECTION DES POPULATIONS 35

CONCLUSION 39

EXAMEN EN DÉLÉGATION 41

LISTE DES PERSONNES AUDITIONNÉES 53

LISTE DES CONTRIBUTIONS ÉCRITES 56

RECOMMANDATIONS DU RAPPORT

Recommandations	Nature de la recommandation	Destinataire	Échéance
1. **Recourir aux nouvelles technologies de manière rigoureuse** par un bilan coûts/avantages actualisé et public	Bonne pratique	Élus locaux	6 mois
2. **Sensibiliser les élus et le personnel** aux enjeux de la cybersécurité par la mise en place de procédures de continuité et de reprise d'activité et par la valorisation des fonctions de RSSI	Bonne pratique	Élus locaux et leurs services	6 mois
3. **Développer les usages numériques en pleine conformité avec le principe de subsidiarité** en déterminant l'échelon pertinent d'intervention	Bonne pratique	Élus locaux	6 mois
4. **Donner une** base légale **à** l'usage des drones **par la police municipale**	Législative	Parlement, en lien avec l'Association des Maires de France	1 an
5. **Renforcer la coopération** entre les collectivités territoriales et les services déconcentrés de l'État s'agissant de la protection des populations.	Bonne pratique	Élus locaux	6 mois

AVANT-PROPOS

En 2017, notre délégation rendait public un rapport intitulé *« les nouvelles technologies au service de la modernisation des territoires »*[1].

« Dans le cadre de leurs compétences locales, que ce soit en matière d'aménagement numérique, d'énergie, de transport et de mobilité, de gestion des déchets, de santé ou encore de sécurité, les collectivités peuvent tirer un grand bénéfice des nouvelles technologies » faisaient alors valoir les rapporteurs MM. Jacques Mézard et Philippe Mouiller. Ces derniers soulignaient, exemples concrets à l'appui, les **nombreux apports du digital** : efficacité de l'action publique, meilleur service aux usagers, économies budgétaires, développement durable, attractivité des territoires…

Notre délégation a souhaité, cinq ans plus tard, porter son attention sur cette même thématique mais en circonscrivant son périmètre à la **protection des populations.** Vos rapporteurs sont en effet convaincus que le numérique apporte en ces domaines une **plus-value très significative** et que les **potentiels de développement** y sont très élevés au sein des collectivités.

Deux axes ont donc été étudiés : la protection de l'**ordre public** ainsi que la **sécurité civile**.

Deux objectifs ont présidé à cette mission « flash » :

- identifier et analyser les **bonnes pratiques locales** dans ces deux champs de l'action publique locale, à la fois en milieu rural et dans les zones urbaines ;

- formuler des **recommandations** visant, d'une part, à encourager et sécuriser ces initiatives numériques locales, d'autre part, à supprimer ou limiter d'éventuelles entraves à leur réalisation.

---

[1] *Rapport d'information de MM. Jacques Mézard et Philippe Mouiller, fait au nom de la délégation aux collectivités territoriales, rapport n° 509 (2016-2017) en date du 19 avril 2017 :* http://www.senat.fr/notice-rapport/2016/r16-509-notice.html

I. LES BONNES PRATIQUES LOCALES

Comme le relève régulièrement notre délégation, les élus locaux agissent, en permanence, comme des « *inventeurs de solutions* ». Ils mènent ainsi, dans le cadre de leurs attributions, **diverses initiatives pragmatiques** pour apporter à leurs administrés, jusqu'au **dernier kilomètre**, le meilleur service au meilleur coût, y compris dans les zones les **plus isolées**.

Convaincus que le concept de « smart city » (ou « ville intelligente ») ne doit pas être exclusivement réservé aux espaces urbains, vos rapporteurs ont souhaité, à travers cette mission, recenser les **bonnes pratiques locales** en matière de numérique, **sans distinction de seuil démographique**.

Parce que l'exigence de protection des populations n'est évidemment pas l'apanage des agglomérations, il convenait d'analyser le niveau d'appropriation de diverses solutions numériques par les élus de petites villes, voire de communes rurales.

Il appartient en effet à toutes les collectivités, quelle que soit leur taille, d'envisager, en lien avec les acteurs privés et, le cas échéant, d'autres collectivités, des **solutions nouvelles adaptées à leurs territoires et fondées sur le numérique**. C'est pourquoi vos rapporteurs ont souhaité privilégier, dans le présent rapport, le concept de « **territoire connecté** », **plus large que celui de « smart city » qui renvoie exclusivement à des espaces urbains**.

Vos rapporteurs ont souhaité étudier les apports du numérique dans deux champs essentiels de l'action publique locale : la protection de l'ordre public (A) et la sécurité civile (B).

A. EN MATIÈRE DE PROTECTION DE L'ORDRE PUBLIC

Comme l'a souligné un récent rapport de la délégation[1], les maires, **pivots de la sécurité dans leur commune**, sont au cœur du « *continuum de sécurité* ». Leur tâche est cruciale dans un contexte marqué à la fois par une défiance entre forces de sécurité et population et par la montée des risques terroriste et sanitaire.

Pour accomplir leurs missions de protection de l'ordre public et de prévention de la délinquance, les maires **peuvent utilement s'appuyer sur les outils numériques** au travers, notamment, des **centres de supervision urbain** (1) et du **recours aux drones** (2). Par ailleurs, de nombreuses communes sont partenaires du **dispositif « voisins vigilants »**, dont l'efficacité est avérée (3).

---

[1] *« L'ancrage territorial de la sécurité intérieure » : Rapport d'information de M. Rémy POINTEREAU et Mme Corinne FÉRET, fait au nom de la délégation aux collectivités territoriales ; rapport n° 323 (2020-2021) - 29 janvier 2021*

1. Les centres de supervision urbain

Un **centre de supervision urbain** (CSU) est une salle équipée d'écrans affichant en direct les images filmées par des caméras de vidéo-protection, qui peuvent parfois être manipulées à distance.

La vidéo-protection permet de surveiller en temps réel la voie publique et de déclencher l'intervention des services de police ou de secours. Elle permet également une « *surveillance a posteriori* » de la voie publique, par le biais de la relecture et l'extraction d'images sur réquisition d'un magistrat ou d'un enquêteur de la Police ou Gendarmerie Nationale.

L'objectif est de prévenir les atteintes aux biens et aux personnes, identifier les auteurs, réguler la circulation urbaine, sécuriser les bâtiments et les sites communaux.

Les CSU constituent ainsi une illustration particulièrement intéressante de **l'intérêt du numérique** pour la protection de l'ordre public. Vos rapporteurs ont souhaité saluer diverses initiatives menées sur ce sujet.

a) l'exemple d'une ville moyenne investie dans la vidéo-surveillance : Charleville-Mézières

Face aux difficultés de l'État pour déployer des effectifs suffisants de policiers nationaux dans les **villes moyennes**, de nombreux maires décident d'installer des centres de supervision urbains.

Tel est le cas de la **ville de Charleville-Mézières**, qui compte près de 50.000 habitants. La commune a voulu répondre aux exigences de sécurité sur la voie publique en installant en 2016 un **centre de supervision urbain** fonctionnant pendant les heures de présence de la police municipale et comportant une fonctionnalité de transfert des images à la police nationale le reste du temps.

Ce centre est aujourd'hui composé de deux entités : d'une part, une unité vidéo regroupant quatre opérateurs équipés chacun d'un mur de huit écrans, d'autre part, un poste de commandement réunissant trois policiers chargés de coordonner les agents sur le terrain, rédiger des mains-courantes, assurer le lien entre les équipes et la hiérarchie et avertir les services de secours ou de police nationale en cas de besoin.

Chaque année, la commune consacre environ **150.000 € à des dépenses d'acquisition de caméras,** ce qui place la commune en dessous de la moyenne. En effet, d'après l'association « Villes de France », interrogée par vos rapporteurs, une ville moyenne consacre environ **215.000 €** chaque année à des investissements dans le **domaine de la sécurité,** que ces investissements concernent le numérique ou non.

b) l'exemple du département des Yvelines : un CSU intelligent et interconnecté

Le conseil départemental des Yvelines a lancé, début 2019, un **dispositif de vidéo-protection.** Ce dernier centralise les images de collèges, d'une caserne de pompiers et d'un bâtiment départemental. Le département a fait installer des **caméras innovantes** de très haute définition dont certaines sont des caméras thermiques permettant de détecter de jour comme de nuit le passage de personnes. Il ne s'agit pas d'une surveillance constante où les agents employés par le Département contrôlent en permanence les images des caméras. Dans les faits, les agents regroupés dans ce centre de surveillance sont la plupart du temps face à des écrans noirs, qui ne s'allument que lorsque les **algorithmes détectent une situation anormale dans l'un des lieux surveillés**.

La vidéosurveillance conjuguée à l'intelligence artificielle : une voie prometteuse

Lors des auditions menées par vos rapporteurs, nombreux sont ceux qui ont loué les algorithmes d'intelligence artificielle utilisés dans le cadre de la vidéosurveillance intelligente (VSI), encore appelée « Video Analytics » ou « Détection automatique d'anormalités » (DAA). Ces technologies se fondent sur des logiciels qui exploitent les capacités de calcul embarquées dans les caméras ou dans les serveurs pour analyser, si possible en temps réel, les images qu'elles enregistrent. L'objectif est clair : identifier des situations, prévues à l'avance, considérées *a priori* comme anormales. Ensuite, des algorithmes complexes aident les opérateurs de sécurité, soit en temps réel, soit en temps différé (élucidation) en lui envoyant automatiquement les alertes les plus pertinentes possibles lorsque la VSI a détecté un événement anormal : intrusion, dépassement d'une ligne ou d'un mur virtuels, intrusion, objet abandonné, personnes en situation horizontale, bruit d'explosion, personne à terre, bris de vitre…)… L'analyse VSI va alors s'atteler à des tâches de reconnaissance automatique de critères spécifiques de couleurs, de formes, de direction…

Un des objectifs qui a présidé à la mise en place du dispositif par le Conseil départemental est la connexion aux images des communes qui le souhaitent. Cette possibilité de raccordement a été ouverte par la loi n° 2021-646 du 25 mai 2021 dite « sécurité globale » qui permet désormais aux communes, rurales comme urbaines, équipées de caméras de surveillance d'être reliées au **centre de supervision départemental** (articles L.132-14 et L.132-14-1 du code de la sécurité intérieure).

Ainsi le centre de supervision du syndicat mixte « *Seine et Yvelines Numériques* »[1] qui comprend les départements voisins des Yvelines et des Hauts-de-Seine, en Ile-de-France, peut désormais être mutualisé au bénéfice des communes et intercommunalités de ces départements.

[1] *Il s'agit du premier opérateur interdépartemental dans le domaine du numérique à voir le jour.*

2. Istres : une commune pionnière dans le recours à des drones

La ville d'Istres (43.000 habitants) a acquis **deux drones au début de l'été 2020**. Elle est la **première commune de France à doter sa police municipale de tels outils**. Ces drones, équipés de caméras haute définition, permettent à la police, d'une part, d'identifier les auteurs de méfaits en temps réel avec des informations précises, mais également, suite aux incendies de l'été 2017, de surveiller plus efficacement les **massifs forestiers**.

Comme l'ont souligné les élus istréens entendus par vos rapporteurs, les images des drones sont non seulement visibles par l'agent-pilote mais également diffusées en streaming sur les écrans des quinze opérateurs du centre de supervision urbain (CSU) de la commune. Elles s'ajoutent donc aux caméras fixes installées sur la voie publique.

Plusieurs policiers municipaux suivent une formation théorique et pratique leur donnant l'habilitation pour faire voler ces drones.

« Nous sommes dans une ville relativement sereine, sans gros incident, mais tout cela est très fragile. Nous connaissons une délinquance importée et des trafics dirigés d'ailleurs qui n'existaient pas il y a dix ans », ont expliqué les élus lors de leur audition, ajoutant que les drones avaient par exemple prouvé leur efficacité dans le repérage des dépôts sauvages.

Ils ont toutefois regretté certaines contraintes tenant, d'une part, à la proximité de la base aérienne d'Istres, d'autre part à l'impossibilité de faire décoller les drones lorsque le mistral souffle à plus de 50 km/h.

3. Numérique et participation citoyenne

Vos rapporteurs se sont également intéressés au **rôle des communes** dans le déploiement d'initiatives citoyennes utilisant les outils numériques dans le but de renforcer la **protection des biens et personnes**.

Rappelons, à cet égard, que le rapport précité sur l'ancrage territorial de la sécurité encourage les citoyens à devenir **des acteurs à part entière de la sécurité** (10ème recommandation). Le rapport cite en particulier le dispositif innovant « *Voisins vigilants et solidaires* », directement inspiré du concept anglo-saxon « *Neighbourhood watch* » ou « Surveillance de quartier ».

Ce dispositif repose sur un site web communautaire permettant de mettre en relation les habitants d'un même quartier pour **lutter ensemble contre les cambriolages** de manière simple et gratuite.

La première communauté de Voisins Vigilants est née en 2002 à St-Paul-de-Vence. Cette **initiative citoyenne** a ensuite essaimé progressivement dans la France entière. Initialement créé pour les particuliers, le concept intègre, en 2014, **les mairies**. Contacté par vos rapporteurs, Thierry Chicha, Président et co-fondateur du site « voisinsvigilants.org » a indiqué que ce

dernier comptait aujourd'hui près de **700 mairies adhérentes.** Il a également précisé qu'une nouvelle commune adhérait tous les deux jours en moyenne. Le coût d'adhésion est variable selon la taille des communes.

Répartition des communes adhérentes au dispositif « voisins vigilants »

	Communes de moins de 2.000 habitants	**Communes entre 2.000 et 20.000 habitants**	**Communes de plus de 20.000 habitants**
Nombre de communes concernées	Environ 300 communes	Environ 300 communes	Environ 100 communes
Montant de l'adhésion[1]	Entre 250 et 800 € TTC	Entre 800 et 3.000 € TTC	Plus de 3.000 € TTC

Les communes ont deux **rôles principaux** : **financer la signalétique** et conduire des opérations de **communication et de sensibilisation** auprès des habitants, notamment dans les zones exposées au risque de cambriolage ou de violences.

Source : https://www.voisinsvigilants.org/voisin

Interrogé par vos rapporteurs, le Président du site « voisinsvigilants.org » a également souligné l'intérêt **d'interconnecter l'outil avec le centre de supervision urbain de la commune,** s'il existe. Il a ainsi cité l'exemple de la commune de Rognard, première commune en

[1] *Ce montant couvre les formations, la réalisation des plans de communication, le paramétrage des outils, l'inscription des personnes âgées, le contrôle de toutes les alertes, la vérification de tous les justificatifs de domicile, le support utilisateur, la maintenance technique, l'application mobile ainsi que l'envoi illimité de SMS et de messages vocaux sur téléphone fixe.*

France à avoir procédé à une telle interconnexion, à l'initiative de notre collègue Stéphane Le Rudulier, conseiller municipal de cette commune des Bouches-du-Rhône qui compte près de 12.000 habitants. **D'autres projets similaires sont en cours de déploiement**, ce dont vos rapporteurs ne peuvent que se réjouir.

Ce dispositif parait présenter un **bilan coût/avantages** très intéressant.

D'une part, il repose sur un procédé **simple et peu coûteux**. Comme le souligne le site « voisinsvigilants.org », nul n'est besoin d'être expert en nouvelles technologies en ce sens que le système fonctionne essentiellement par une application intuitive et par l'envoi de SMS : « *le système d'alertes Voisins Vigilants a été conçu pour être accessible à tous. Performant et innovant, il informe instantanément chaque Voisin Vigilant dès qu'un danger potentiel est signalé par un voisin ou par la police municipale.* ».

D'autre part, le dispositif « voisins vigilant » semble avoir **démontré son efficacité**. En effet, alors qu'en France, un cambriolage se produit toutes les 90 secondes, le ministère de l'Intérieur constate **une baisse des cambriolages de - 40% par an**. C'est pourquoi a été signée le 2 février 2021 une convention de partenariat entre la direction centrale de la sécurité publique (DCSP) et le site « voisinsvigilants.org ». Une note du 24 février 2021 adressée aux préfets expose l'objectif de ce partenariat : *« améliorer la lutte contre les délits d'appropriation et de constituer un maillage territorial permettant de démultiplier les relais locaux ».* Elle ajoute que cette convention *« s'inscrit pleinement dans le cadre de la Sécurité du Quotidien et vise à assurer, sur tout le territoire national, une meilleure prise en compte des attentes de la population en favorisant le rapprochement police/population par l'inclusion des « coordinateurs de quartiers » du site « voisinsvigilants.org » et en « renforçant la visibilité des services de police et en leur permettant de disposer d'une source d'information élargie et de nature opérationnelle ».*

Vos rapporteurs estiment que ce **partenariat novateur** répond opportunément à la philosophie du continuum de sécurité et aux besoins de sécurité de la population.

Source : https://www.voisinsvigilants.org/voisin

B. EN MATIÈRE DE SÉCURITÉ CIVILE – PRÉVENTION DES RISQUES

Comme l'a souligné la délégation à la prospective dans un rapport rendu public en 2019[1], l'adaptation aux changements climatiques constitue pour notre pays **un enjeu à la fois urgent et majeur**, qui va nécessiter une mobilisation soutenue durant plusieurs décennies. Ainsi, les climatologues estiment que les décennies à venir devraient être marquées par une *« augmentation de l'intensité des **précipitations intenses** sur la partie nord du bassin méditerranéen ».*

Le recours aux solutions numériques permet-il aux élus **de mieux gérer** et de **mieux anticiper** les **risques naturels majeurs** dont **la fréquence et la violence** semblent **s'intensifier** du fait du dérèglement climatique ?

C'est pour répondre à cette question que vos rapporteurs ont étudié certaines bonnes pratiques locales en matière de prévention des risques d'inondation (1), d'incendie (2) et d'avalanche (3). Enfin, le rapport présente un dispositif, facilement transposable, de téléalerte « multirisques » (4).

1. Le risque inondation

Les inondations représentent le **premier risque naturel en France** : elles menacent des vies, des habitations, des emplois et tous les territoires sont concernés.

Les chiffres-clés du risque inondation en France

- **17,1 millions** d'habitants permanents exposés aux différentes conséquences des inondations par débordement de cours d'eau, dont 16,8 millions en métropole.
- **1,4 million** d'habitants exposés au risque de submersion marine.
- Plus de **9 millions** d'emplois exposés aux débordements de cours d'eau et plus de **850 000** emplois exposés aux submersions marines.
- **20%** des habitations exposées aux submersions marines sont de plain-pied.

Source : https://www.ecologie.gouv.fr/generalites-sur-risque-inondation-en-france

On distingue **différents types d'inondation** :

- crue ou débordement de cours d'eau ;
- ruissellement ;
- submersion marine ;
- remontée de nappe phréatique ;
- rupture d'ouvrage.

[1] « Adapter la France aux dérèglements climatiques à l'horizon 2050 : urgence déclarée » : rapport d'information n° 511 (2018-2019) de MM. Ronan Dantec et Jean-Yves Roux, fait au nom de la Délégation sénatoriale à la prospective, déposé le 16 mai 2019.

Ces différents types d'inondation **peuvent être liés entre eux.** Par exemple, le ruissellement contribue au débordement des cours d'eau, une submersion marine peut causer un débordement de cours d'eau, ce dernier peut causer la rupture partielle ou totale d'un ouvrage...

Au plan juridique, la gestion des milieux aquatiques et la prévention des inondations (GEMAPI) est une compétence confiée, **depuis le 1er janvier 2018**, aux EPCI (métropoles, communautés urbaines, communautés d'agglomération et communautés de communes).

Vos rapporteurs ont souhaité saluer **quelques actions exemplaires** menées par les élus locaux dans la gestion de ce risque.

a) L'exemple de Nîmes : une commune-référence dans la gestion du risque inondation

La ville de Nîmes est souvent citée comme une référence en matière de **prise en charge du risque inondation**.

Interrogé par vos rapporteurs, Guillaume PLA, chef de projet « prévision des inondations » à la mairie de Nîmes, a rappelé que « *de par sa configuration, le territoire nîmois est fortement exposé au risque inondation par ruissellement urbain torrentiel, associé à une problématique de cours d'eau temporaires appelés cadereaux*.»

Confrontée à cette situation à risques, la municipalité a décidé, **à la suite de la crue catastrophique de 1988,** de mettre en place un système de prévision, d'observation et d'alerte. Développé à partir de la fin des années 1990 et déployé en **2005**, le dispositif de surveillance des crues éclairs urbaines baptisé « **ESPADA**[1] » est une **première en France** à un niveau communal et se décline en plusieurs phases.

Dans un premier temps, la **surveillance** de l'évolution des précipitations et du ruissellement sur l'ensemble du territoire s'opère aux moyens de **trois outils** : stations de mesures hydrométéorologiques, radars et caméras de surveillance.

Dans un deuxième temps, ces données sont exploitées afin **d'évaluer localement le risque d'inondation sur le territoire en temps réel**. Si le dispositif détecte un débordement en cours ou à venir, un indicateur alerte le prévisionniste de crue et identifie la zone impactée. Cette analyse permet aux autorités locales de décider des actions à déployer dans le cadre du Plan Communal de Sauvegarde. Ces décisions peuvent, par exemple, consister en des opérations de barriérage, à l'information et alerte de la population (réseaux sociaux et site internet de la mairie, automate d'appels) ou à la mise en place d'opérations de soutien à la population. Le lien opérationnel est assuré par la proximité immédiate entre l'espace dédié aux prévisionnistes ESPADA et le Poste de Commandement Communal (PCC) de la collectivité.

[1] *Évaluation et Suivi des Pluies en Agglomération pour Devancer l'Alerte*

Dès le début de l'année 2014 et dans le cadre de sa démarche PAPI[1], la municipalité a souhaité **moderniser son dispositif** d'observation pour le rendre **plus efficace** grâce à un réseau radio et un outil radar. Les données sont produites toutes les 5 minutes afin de représenter au mieux les phénomènes. La nouvelle phase de modernisation lancée en 2017 consistait à moderniser les interfaces utilisateur et à optimiser les performances du modèle de prévision, désormais réajusté en permanence sur la base des observations réalisées. D'une façon générale, le dispositif est régulièrement amélioré au gré des retours d'expérience et des évolutions technologiques, par exemple actuellement par l'exploitation des images de vidéo-protection pour l'estimation des débits dans une logique de mutualisation des moyens et une démarche « smart city ».

La collectivité projette, à terme, de permettre au public **d'accéder aux données collectées.** Le représentant de la mairie de Nîmes a souligné en effet que la marie envisage de *« s'appuyer sur les outils open data en cours de déploiement au sein de la collectivité plutôt que de développer une plate-forme supplémentaire qui risquerait d'alourdir l'offre numérique proposée au grand public ».*

S'agissant du coût de fonctionnement d'ESPADA, il est **compris entre 50.000 et 75.000 € par an,** correspondant au coût d'entretien d'une cinquantaine de capteurs et aux frais de maintenance logicielle.

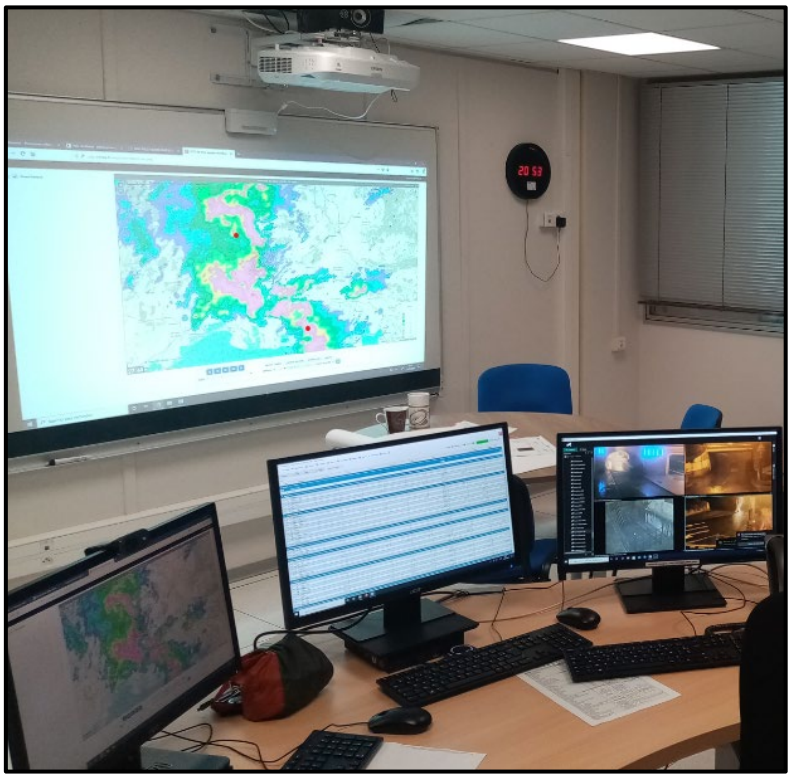
Il a été indiqué à vos rapporteurs que le dispositif pourrait, à court terme, être **étendu à l'échelle de la communauté d'agglomération** dans un double souci de cohérence avec la compétence GEMAPI et de mutualisation des charges, des moyens et de l'expertise.

Quelle est **l'efficacité d'un tel dispositif** d'observation ? Peut-on affirmer qu'il a permis de sauver des vies ? de protéger des biens ? des habitations ? Il est difficile de répondre avec précision à ces questions. La ville de Nîmes fait valoir que *« l'un des points majeurs remontés par les décideurs en poste lors de la catastrophe de 1988 est l'absence totale d'informations sur le phénomène en cours : des torrents dévalaient en centre-ville depuis les collines et la gestion de crise était alors uniquement en réaction. Via l'outil ESPADA, non seulement le Directeur des Opérations de Secours dispose d'un état des lieux complet sur le territoire à tout instant, mais surtout il dispose d'une anticipation sur ces impacts qui, même si elle n'est que **d'une heure environ**, permet de lancer les actions de sauvegarde avant qu'il ne soit trop tard ».*

[1] *Lancés en 2002, les Programmes d'Actions de Prévention des Inondations (PAPI) visent à promouvoir une gestion intégrée des risques d'inondation afin d'en réduire les conséquences dommageables sur les territoires, les habitations, les biens et les activités. Outil de contractualisation entre l'État et les collectivités territoriales, le dispositif PAPI permet le financement et la mise en œuvre d'une politique globale de gestion du risque d'inondation, menée à l'échelle d'un bassin de risque.*

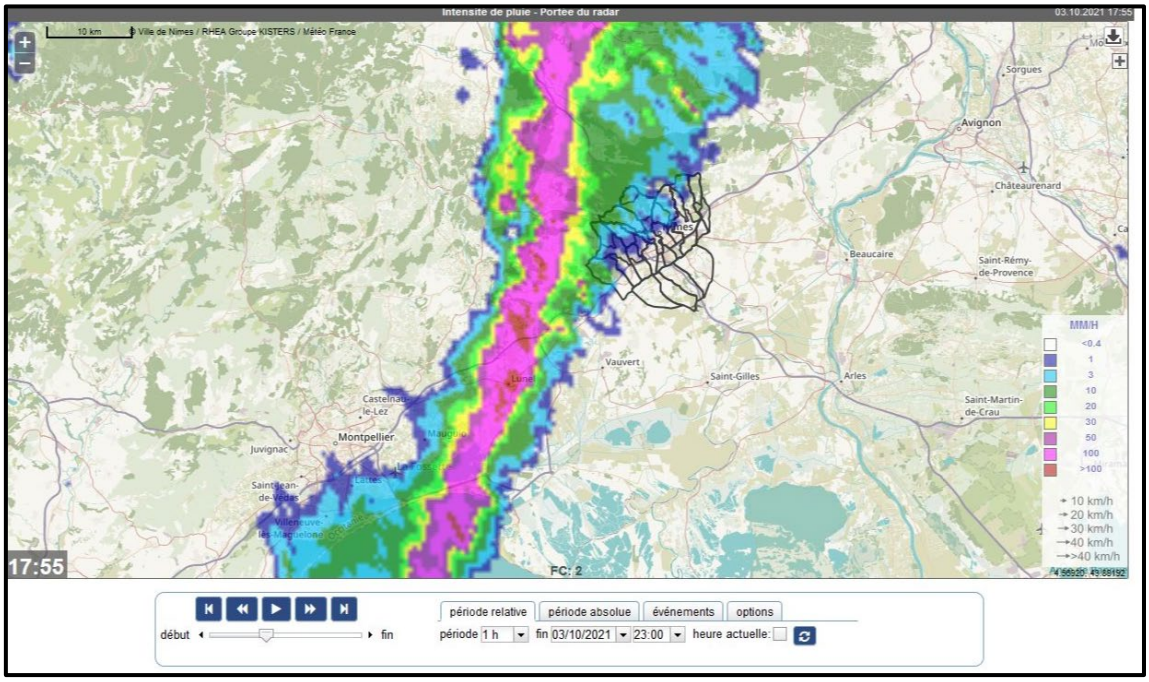
L'outil constitue donc indéniablement une aide à la prévention des risques, même s'il apparaît malaisé de la **mesurer** ou **de la quantifier avec certitude.**

Dispositif de surveillance ESPADA



Source : Commune de Nîmes

Intensité de pluie – données issues du radar



Source : Commune de Nîmes

b) L'exemple du Pays de Lourdes et des vallées des Gaves

Tout aussi sophistiqué est le **dispositif numérique d'alerte des crues** géré par le Pays de Lourdes et des Vallées des Gaves (PLGV). Ce Pôle d'Équilibre Territorial et Rural (PETR), créé le 1er janvier 2014, exerce notamment la compétence GEMAPI. Ce dispositif d'alerte, dont le coût d'installation s'est élevé à 30.000 €, a été élaboré dans le cadre de la prévention des risques d'inondations avec le soutien de l'État et en lien avec Météo-France et les chercheurs de l'université de Pau. Les informations et alertes peuvent notamment être envoyées aux habitants par téléphone, via internet, ou directement sur leur application mobile.

Parallèlement à ce système d'alerte, le PETR a mis en place des **outils d'observation** de ses cours d'eau afin de mieux comprendre le déplacement des sédiments. Ainsi, des galets sont **équipés de puces RFID** pour étudier les déplacements des sédiments à l'origine de crues. Nommé « O2H », ce projet à caractère expérimental est un **partenariat public-privé**. Lors de son audition, Mme Corinne Galey, 1ère vice-présidente du PLGV, s'est dite convaincue que le projet, en dépit de son coût (environ 30.000 € par an) constituerait une précieuse **aide à la décision** pour les élus.

Les galets connectés « communiquants »

Source : Pays de Lourdes et des Vallées des Gaves

c) L'exemple de la commune de Sommières (Gard)

Si les systèmes mis en place à Nîmes et dans le pays de Lourdes reposent sur une technologie très élaborée, d'autres communes ont mis en place des systèmes d'alerte au moyen de **technologies plus rudimentaires**.

Tel est le cas de la commune de Sommières, située dans le Gard, à une quarantaine de kilomètres de Nîmes. Cette commune de près de 5.000 habitants est l'une des plus exposées au risque inondation en France, en raison des crues fréquentes du fleuve Le Vidourle.

Crue d'octobre 2014

(Crédit photo : commune de Sommières)

Après la crue de 1958, la ville a mis en place des sirènes, système doublé, en 2004, de **nouvelles méthodes d'alerte par SMS ou message vocal**, pour un coût annuel d'environ 4.000 €, financés entièrement par la commune sans subvention[1]. Ce système fait partie intégrante du plan communal de sauvegarde (PCS).

Lors de leur audition, les représentants de la commune ont confirmé à vos rapporteurs que ce système simple de notification avait **démontré son efficacité** puisque la ville n'a jamais déploré de décès des suites d'une inondation.

2. Le risque incendie : l'exemple des drones utilisés par le conseil départemental des Bouches du Rhône

Le Service départemental d'incendie et de secours (SDIS) des Bouches-du-Rhône a été, en 2014, **le troisième de France**, après les Landes et le Haut-Rhin, **à s'équiper de drones,** après une expérimentation concluante lancée en 2012.

En effet, en prévision des fortes chaleurs de l'été 2014, les sapeurs-pompiers du département des Bouches-du-Rhône ont décidé d'intégrer des drones dans le **dispositif préventif de surveillance des incendies** sur le territoire, en particulier pour les zones présentant un fort risque pour la

[1] *Comme indiqué plus haut, les intercommunalités sont exclusivement compétentes en matière de GEMAPI. En l'espèce, la Communauté de communes du Pays de Sommières exerce et finance les missions suivantes : aménagement de bassins, entretien et aménagement de cours d'eau, défense contre les inondations, protection et restauration des sites, des écosystèmes aquatiques et des zones humides. En revanche, le système d'alerte est financé par la seule commune de Sommières, de la même façon que le dispositif ESPADA est, pour l'instant, pris en charge financièrement par la seule commune de Nîmes.*

sécurité des populations (forêts, zones industrielles, zones inondables, zones à risque de pollution…).

Avec le soutien du département, la brigade des sapeurs-pompiers des Bouches-du-Rhône a eu recours à des drones de seconde génération, dotés de **capteurs infrarouges** détectant de façon **plus précise les départs de feu.**

Complémentaires des moyens traditionnels d'intervention, les drones présentent de **nombreux atouts pour la gestion du risque incendie** :

- ils améliorent la coopération des équipes sur le terrain (pour les opérations de sauvetage nautique ou de recherche de personnes disparues) ;
- ils facilitent le passage dans des endroits dangereux et difficile d'accès ;
- ils réduisent l'exposition des sapeurs-pompiers à des risques mortels (feu, gaz toxiques…) ;
- ils permettent à des agents inaptes pour cause de handicap d'intervenir opérationnellement et d'être de nouveau pleinement mobilisés comme pilotes de drones ;
- ils représentent une source considérable d'économies au regard du coût d'un hélicoptère, qui s'élève à environ 3.000 € par heure ;
- lorsqu'ils sont équipés d'une caméra thermique, ils s'avèrent très utiles pour couvrir les dizaines de kilomètres de terrain incendiés et éviter les reprises de feu en identifiant les points chauds sur lesquels les pompiers peuvent agir en priorité. Outre une intervention rapide, cette identification plus fine permet de rationaliser la ressource en eau.

Entendu par vos rapporteurs, le Commandant Éric RODRIGUEZ, chef de groupement au SDIS des Bouches-du-Rhône, a souligné l'efficacité du recours au drone, considéré comme « *l'œil déporté* » du commandant des opérations de secours, en ce sens qu'il aide à parfaire la reconnaissance de ce dernier. Il permet d'identifier des enjeux particuliers ou des points sensibles dans la phase de lutte contre l'incendie.

S'agissant d'opération de recherche de personnes, il a été indiqué à vos rapporteurs qu'aucune victime **n'a été retrouvée par ce moyen**. Pour autant, la complémentarité du drone avec l'hélicoptère, sous réserve d'une coordination aérienne efficace, ne fait pas de doute, en particulier pour la reconnaissance des zones dangereuses ou difficiles d'accès.

Le représentant du SDIS s'est félicité du **très bon rapport performance / coût des drones**, rapport en constante progression. Un drone représente aujourd'hui un coût d'acquisition compris entre 5.000 et 10.000 €

et de faibles coûts de la formation des télépilotes, assurée par la Direction générale de l'aviation civile.

Ce coût raisonnable, conjugué aux capacités des drones, explique la généralisation du recours aux drones. Lors de leur audition, les représentants de l'ADF ont d'ailleurs souligné qu'*« en cas d'incendie, la majorité des SDIS possède des drones pour intervenir et estimer l'ampleur du phénomène »*.

Notons, pour conclure, que **la performance des drones ne cesse de s'améliorer**. Le SDIS des Bouches du Rhône expérimente ainsi des drones **dotés eux-mêmes de moyens d'extinction**. Ils pourraient ainsi, d'ici quelques années, être utilisés, non plus seulement à des fins d'observations, mais **dans le but d'éteindre des feux nés dans des zones difficiles d'accès**. Il s'agit là d'une très bonne illustration des formidables potentialités des drones dans un proche avenir.

3. Le risque avalanche : l'exemple des drones utilisés à Val Thorens

La station de sports d'hiver Val Thorens constitue le plus grand domaine skiable au monde. Elle s'est dotée de **deux drones à partir de l'hiver 2018-2019**. Les appareils sont dotés de **caméras très performantes :** l'une est thermique, l'autre est munie d'un zoom grossissant 200 fois.

Le drone exerce de multiples fonctions :

- il assure des **missions de secours aux personnes**. À cette fin, l'appareil vole au-dessus des skieurs et mène des missions d'observation et de reconnaissance. Il est équipé d'un outil de transmission de la voix pour rassurer et préparer à l'arrivée des secours ;

- il permet **d'analyser le terrain en cas d'avalanche** et de repérer les victimes ensevelies sous la neige (traces de ski, de bâtons, présence d'un bonnet…) ;

- hors saison, il participe aux **opérations de maintenance** de la station, notamment pour la vérification de l'état des remontées mécaniques et du dispositif de déclenchement d'avalanche.

Source : cellule drone de Val Thorens

Lors de son audition, M. Benjamin Blanc, directeur Général du service des pistes de Val Thorens, a souligné le **bilan performance / coût très positif** du recours aux drones.

Concernant le **coût**, il paraît raisonnable :

- environ 53.000 € en coût d'investissement ;
- environ 5.600 € par an en budget de fonctionnement (coût salarial et formation des télépilotes saisonniers, assurance responsabilité civile)[1].

S'agissant de la **performance** des drones, si ces derniers n'ont évidemment pas vocation à se substituer aux interventions humaines, ils constituent un **précieux moyen de soutien** aux équipes du service des pistes. M. Benjamin Blanc a fait en effet valoir notamment :

- que les opérations par drone avaient permis de sauver une personne ensevelie dans une avalanche du fait de sa rapidité d'intervention mais également de la forte capacité d'observation ;
- que les drones avaient permis de protéger les sauveteurs : « *En 2020, Val Thorens a recensé 15 avalanches. Auparavant, nous devions envoyer une équipe pour reconnaître la zone de l'avalanche et rechercher des traces de victimes. C'est une tâche particulièrement dangereuse parce que le terrain est accidenté et le risque d'une suravalanche présent* » ;
- que les appareils pouvaient voler malgré des vents de 90 km/heure ;
- qu'ils disposaient d'un haut-parleur puissant permettant de communiquer avec les personnes secourues ;
- que leur autonomie limitée (40 minutes de vol) pouvait être compensée par un système filaire permettant une alimentation permanente (dans le cas d'un vol stationnaire) ;
- qu'ils pouvaient désormais porter jusqu'à 15 kg de charge et pouvaient ainsi larguer une radio ou un défibrillateur.

En conclusion, M. Benjamin Blanc a souligné la **constante augmentation** du rapport performance /coût des drones et leur **immense potentiel d'utilisation** dans les années à venir par les élus locaux.

4. Un **dispositif numérique « multirisques » : l'exemple d'Ajaccio**

Exposée à de multiples **risques naturels et technologiques**, la commune d'Ajaccio a su pleinement tirer profit du numérique pour répondre à ces défis.

---

[1] *Il a été indiqué à vos rapporteurs que si le budget de fonctionnement peut rester fixe, l'investissement est d'environ 15 000€ tous les 3 ans afin de renouveler un drone tous les 3 ans.*

En premier lieu, la ville s'est dotée de divers outils **d'observations et de contrôle préventif**. Ainsi, une plateforme dénommée « WikiPredict » et un radar placé sur les hauteurs d'Ajaccio permettent à la commune de réaliser des prévisions météorologiques précises et fiables. De même, la commune recourt à un prestataire extérieur pour identifier la quantité, la qualité et l'implantation des points d'eau incendie sur sa commune (publics et privés)[1]. Ce prestataire réalise les contrôles des points d'eau incendie en se servant du logiciel de gestion patrimoniale lié au système d'information géographique d'Ajaccio. Aussi, le fichier est exporté du système du prestataire et quotidiennement importé dans les serveurs informatiques de la ville.

En second lieu, la ville a déployé en 2019 une plateforme multicanal de téléalerte afin de prévenir sa population en cas de crises. Ce dispositif, qui repose sur une démarche volontaire d'inscription, permet aux usagers, résidents permanents ou ponctuels, de recevoir une alerte en cas de situations d'urgence **liées à divers risques majeurs : tempêtes, inondations, canicule**… Cette notification prend la forme de SMS, de messages vocaux et de courriels. Hébergé sur une plateforme technique sécurisée, ce service de TéléAlerte permet de joindre dans un délai extrêmement court les personnes inscrites sur le fichier afin de leur délivrer un message clair et précis.

Interrogée par vos rapporteurs sur **l'efficacité** de ce dispositif de téléalerte, la commune d'Ajaccio a répondu :

- que les ajacciens se sont massivement inscrits à ce dispositif **(**51 531 inscriptions)[2] ;
- que le système, fiable et simple d'utilisation, a déjà servi **à plusieurs reprises** depuis sa mise en place en 2019, en particulier pour un incident sur une cuve de chlore de la Station d'Épuration des Eaux Usées ou pour l'interdiction d'emprunter les voies inondées lors d'une tempête et d'une crue qui avaient entraîné la fermeture de l'aéroport.

Il s'agit donc indéniablement d'une **bonne pratique locale,** sans doute **transposable** dans de très nombreuses communes.

---

[1] *Voir le rapport d'information de MM. Hervé MAUREY et Franck MONTAUGÉ, fait au nom de la délégation aux collectivités territoriales, rapport n° 760 (2020-2021), publié le 8 juillet 2021 et intitulé « Défense extérieure contre l'incendie : assurer la protection des personnes sans nuire aux territoires ».*

[2] *Ce chiffre est à mettre en relation avec la population de la ville, qui avoisine les 70.000 habitants. À noter que le système intègre d'office les informations de l'annuaire téléphonique, contenant majoritairement des numéros de téléphones fixes. À noter enfin que l'inscription est possible pour les résidents, les entreprises, les travailleurs et personnes de passage (touristes, étudiants...) dont l'adresse est située sur le périmètre de la commune d'Ajaccio. Pour les personnes de passage, une option leur permet de définir une période limitée d'activation (par exemple du 1er au 15 août).*

Source : commune d'Ajaccio

II. LES RECOMMANDATIONS

Les exemples concrets d'innovations technologiques au service de la protection des populations sont infinis et vos rapporteurs ne prétendent évidemment pas en avoir dressé une liste exhaustive.

Toutefois, au travers de la diversité des quelques exemples concrets fournis, vos rapporteurs souhaitent marteler une évidence : les collectivités territoriales, **véritables « incubateurs » de l'innovation,** recourent toujours davantage aux nouveaux outils pour rendre leurs territoires sans cesse **plus connectés** et **plus « intelligents »**. À l'image du corps humain, ces systèmes sont reliés au système nerveux central, qui a en charge la mémoire et l'analyse de millions de données collectées. L'émergence de collectivités « smart » ne doit pas être redoutée mais au contraire encouragée.

Pour autant, vos rapporteurs sont pleinement conscients que ces innovations ne sauraient être envisagées **comme des expériences à généraliser partout**, avec les mêmes méthodes et au même moment. Les dynamiques de modernisation varient non seulement en fonction de l'histoire, de la géographie, des fragilités et des ressources des territoires, mais aussi en fonction des élus qui, au sein des collectivités, les initient et les portent.

S'il n'existe pas de « solution uniforme » applicable à tous les territoires, l'analyse des bonnes pratiques locales a fait émerger la nécessité de **formuler des recommandations** de nature à accentuer et à sécuriser le mouvement de numérisation des collectivités.

A. LE RECOURS AUX TECHNOLOGIES : UNE DÉMARCHE QUI DOIT ÊTRE FONDÉE SUR UNE MÉTHODE RIGOUREUSE ET UN BILAN COÛT / AVANTAGES ACTUALISÉ ET PUBLIC

Lors des auditions, vos rapporteurs ont constaté que les solutions numériques sont parfois lancées par les élus locaux sans **objectifs clairement définis** et sans **communication efficace** auprès des habitants.

En premier lieu, vos rapporteurs insistent sur la nécessité de conduire une **démarche rigoureuse fondée sur une réflexion préalable approfondie**. Quels sont les objectifs attendus de tel ou tel outil numérique ? Quel est le bilan coût / avantages espéré de la technologie déployée ? Quels sont les critères d'évaluation qui permettront d'apprécier le succès ou non de l'initiative ? Faut-il privilégier l'achat ou la location des équipements ? Ce bilan, qui incombe à la collectivité, doit être sans cesse actualisé puisque le rapport performance/coût des outils numérique s'améliore constamment au fil du temps.

En second lieu, vos rapporteurs encouragent vivement les élus à **communiquer** sur la démarche engagée et sur son évaluation. Il est en effet

essentiel d'associer la population à la gestion des risques pour la rendre **actrice de sa propre protection :** il ne saurait y avoir de prévention efficace sans **information préalable des populations concernées par les risques majeurs**. Comme le souligne avec pertinence le ministère de l'environnement, interrogé par vos rapporteurs, *« une population bien informée est un maillon essentiel de la chaîne de réponse de sécurité civile.»*. C'est l'article L. 125-2 du code de l'environnement qui prévoit ce droit à l'information, droit renforcé récemment par la loi dite « Matras »[1] qui a étendu l'obligation de cette information **à toutes les communes concernées par un risque majeur** et pas uniquement aux communes couvertes par un plan de prévention des risques comme précédemment. Ainsi, les communes doivent mettre à la disposition du public le **document d'information communal sur les risques majeurs** (DICRIM). En pratique, de nombreuses communes vont au-delà de cette obligation de « mise à disposition » et utilisent le numérique et les réseaux sociaux pour permettre l'anticipation et la préparation des populations aux risques naturels et technologiques. Pour ce qui concerne les moyens financiers, les actions visant à assurer et promouvoir l'information préventive sur les risques naturels majeurs peuvent bénéficier de financements du fonds de prévention des risques naturels majeurs (FPRNM, dits « Fonds Barnier »). Le taux de financement maximum est de 80 % pour les collectivités (en application de l'article L.1111-10 du code général des collectivités territoriales).

Cet effort de communication dématérialisé doit concerner non seulement **l'état des risques** auxquels sont exposés les habitants, mais également le **bilan précité coût/avantages** des solutions numériques mises en place pour y faire face. En effet, **les outils numériques ne doivent pas apparaître aux yeux des habitants comme des « gadgets »** mais comme des solutions efficaces, protectrices et inscrites dans le cadre d'une réflexion stratégique.

B. LA SENSIBILISATION DES ÉLUS ET DU PERSONNEL AUX ENJEUX DE LA CYBERSÉCURITÉ

Vos rapporteurs sont convaincus que le recours au numérique améliore **l'efficacité de l'action publique locale** dans des domaines très importants pour nos concitoyens, aux premiers rangs desquels la préservation de **l'ordre public** et la **prévention des risques**.

Ils sont tout autant persuadés d'une **nécessité impérieuse** : à mesure que les usages numériques se développent, notre devoir de **vigilance et de protection** s'intensifie. En effet, les collectivités territoriales sont responsables de la sécurité des données qu'elles traitent et de leurs services numériques vis-à-vis des autorités et des citoyens. En conséquence, elles

---

[1] *Loi n° 2021-1520 du 25 novembre 2021 visant à consolider notre modèle de sécurité civile et valoriser le volontariat des sapeurs-pompiers et les sapeurs-pompiers professionnels.*

doivent garantir à leurs usagers un niveau optimal de protection et une mise à jour **permanente des systèmes de protection.** En d'autres termes, les démarches « développement des usages » / « renforcement du bouclier » apparaissent **indissociables** avec un objectif clairement identifié pour les collectivités locales : marcher sur « deux jambes » et se garder de créer des « *colosses numériques aux pieds d'argile* ».

Or, le dernier rapport de votre délégation, réalisé conjointement avec la délégation aux entreprises, souligne **l'ampleur du défi de la cybersécurité** que les élus doivent relever[1]. Ainsi, **en 2020, près de 30 % des collectivités territoriales ont été victimes d'une attaque au rançongiciel**[2] selon une étude du Clusif[3]. En effet, cette même année a vu le nombre de cyberattaques contre des collectivités territoriales **augmenter de 50 %** par rapport à 2019.

Comme le souligne le Groupement d'intérêt public « Action contre la cybermalveillance » sur son site Internet : « ***L'explosion des usages numériques ces dernières années****, qui s'est encore accentuée avec la crise sanitaire par le télétravail massif, le téléenseignement, le commerce en ligne, a vu en corollaire une recrudescence sans précédent des faits de cybermalveillance. Contrairement à l'image souvent véhiculée, les cybercriminels ne sont plus aujourd'hui les seuls adolescents immatures que l'on peut imaginer.* ***Ils s'organisent sur le darknet en équipes très structurées et compétentes pour maximiser leurs profits****. Leur seule idéologie est de chercher à gagner le plus d'argent possible, peu importent les conséquences pour les victimes qui peuvent avoir leurs systèmes d'information chiffrés, pillés, sabotés etc. Particuliers, entreprises, collectivités, associations et mêmes hôpitaux et États,* ***plus personne n'est aujourd'hui, et ne sera demain, épargné*** ».

Au regard de ces enjeux, le rapport précité évoque **plusieurs pistes de réflexion** :

- **sensibiliser les élus et leurs services** aux enjeux de la cybersécurité. En particulier, un travail d'information doit être mené sur l'ampleur des menaces numériques et sur l'existence de lourdes conséquences en cas d'attaques (dysfonctionnement des services publics locaux, perte de données, conséquences humaines et financières…) ;

---

[1] *« Les collectivités territoriales face au défi de la cybersécurité » ; Rapport d'information de M. Serge BABARY et Mme Françoise GATEL, fait au nom de la délégation aux entreprises et de la délégation aux collectivités territoriales n° 283 (2021-2022) - 9 décembre 2021*

[2] *Un rançongiciel (ou ransomware) est un logiciel malveillant ou virus qui bloque l'accès à l'ordinateur ou à ses fichiers et qui réclame à la victime le paiement d'une rançon pour en obtenir de nouveau l'accès. Certaines de ces attaques visent parfois simplement à endommager le système de la victime pour lui faire* ***subir des pertes d'exploitation et porter atteinte à son image****.*

[3] *https://clusif.fr/newspaper/le-risque-associe-aux-rancongiciels-demeure-sous-evalue-dans-les-collectivites-territoriales-clusif/. Le Clusif est l'association de référence de la sécurité du numérique en France.*

- mettre en place des procédures de **continuité et de reprise d'activité** en cas de survenance d'une crise d'origine numérique ;
- valoriser les fonctions de RSSI[1] dans les collectivités d'une certaine taille et en faire un véritable « directeur stratégique de la Sécurité numérique » en **lien direct** avec les élus et en charge d'une **veille permanente** sur la cybersécurité.

Les auditions menées par vos rapporteurs ont confirmé **l'entière pertinence de ces propositions**, que vos rapporteurs font leurs. Elles s'imposent d'autant plus dans le cadre **d'outils d'aide à la protection des populations,** qui doivent naturellement bénéficier d'un très haut niveau de protection.

À cet égard, vos rapporteurs saluent l'initiative de notre collègue Laurent LAFON, auteur d'une proposition de loi pour la mise en place d'une **certification de cybersécurité** des plateformes numériques destinée au grand public, texte actuellement en cours de discussion au Parlement[2]. L'exposé des motifs du texte présente les enjeux du sujet et salue en particulier les travaux de la commission d'enquête du Sénat sur la **souveraineté numérique** qui a *« montré l'importance d'adopter une réelle stratégie de maîtrise et de protection des données publiques, face aux attaques quotidiennes contre leurs systèmes d'information, qui menacent la continuité du service public et la sécurité des données de nos concitoyens »*[3].

Sur proposition de la commission des affaires économiques et en accord avec l'auteur de la proposition de loi, le Sénat a complété le texte afin de créer **« un cyberscore » des solutions numériques**. Le rapport souligne qu'un tel dispositif bénéficierait indirectement aux *« collectivités rurales en renforçant leur niveau d'information sur les solutions grand public qu'ils sont susceptibles d'utiliser »*[4].

Vos rapporteurs ont mesuré, lors des auditions, combien cette proposition séduisait les élus locaux, en particulier ceux des petites

---

[1] *Responsable de la sécurité des systèmes d'information*

[2] *Cette proposition de loi a été déposée au Sénat le 15 juillet 2020. Le dossier législatif est accessible sur cette page.*

[3] *« Le devoir de souveraineté numérique » - rapport de M. Gérard LONGUET, fait au nom de la commission d'enquête n° 7 tome I (2019-2020) – 1er octobre 2019. Le président de cette commission d'enquête, Franck MONTAUGE, a d'ailleurs été entendu par vos rapporteurs.*

[4] *Rapport n° 38 (2020-2021) de Mme Anne-Catherine LOISIER, fait au nom de la commission des affaires économiques, déposé le 13 octobre 2020. Le rapport précise que « ce dispositif reste très largement à construire, c'est pourquoi la proposition de loi renvoie à des textes d'application. La difficulté résidera sans doute dans la définition des indicateurs pertinents. On peut, par exemple, penser au chiffrement de bout en bout pour les services numériques impliquant des communications. On peut également imaginer des critères de nature moins technique et se rapprochant de la logique de « name and shame », comme le nombre de condamnations par une autorité en charge de la protection des données personnelles ou le nombre de failles mises à jour ».*

communes. En effet, ces derniers se trouvent souvent démunis face **aux choix multiples qui s'offrent à eux en matière de services numériques,** car ils ne bénéficient pas d'une information intelligible et accessible sur le niveau de protection dont bénéficient les outils numériques qui existent sur le marché.

Lors de table-ronde organisée par votre délégation et la délégation aux entreprises[1], Mme Gwenaëlle Martinet, cheffe de projet France Relance a jugé « *intéressante* » l'initiative du cyberscore tout en appelant à une certaine prudence : « *elle doit être manipulée avec précaution, car c'est une photo à l'instant T, qui varie très rapidement. Il faut garder une* ***attention constante*** *en matière de cybersécurité, étant donné qu'un cyberscore satisfaisant à un moment ne durera que si l'on continue d'investir* ».

Vos rapporteurs souscrivent pleinement à cette analyse. Ils recommandent aux élus et aux agents territoriaux de faire preuve, en matière de sécurité des données, d'une **vigilance permanente** lorsqu'ils développent les usages numériques, en particulier dans le domaine de la protection des populations.

Si cette vigilance est évidemment de mise pour les données issues des dispositifs de protection de l'ordre public, elle a également toute sa pertinence en matière de **risques naturels**.

Le ministère de l'environnement a ainsi souligné deux conséquences pouvant résulter d'une action de cybermalveillance :

- la **non-disponibilité de l'information sur les risques**, notamment en période de vigilance ou de crise ;
- l'altération de **l'information** (atténuation par exemple), ce qui pourrait avoir des conséquences catastrophiques.

Il est donc essentiel de sécuriser tous les outils numériques de protection des populations et de prévoir des **plans de continuité d'activité** en cas d'attaque.

Vos rapporteurs appellent en particulier les collectivités locales à veiller à la **sécurisation des données,** soit au moyen de « **data centers** », soit via la solution, encore expérimentale, du « **cloud souverain** ». Ce dernier est constitué d'un ensemble de ressources « serveurs » disponibles sur le territoire national et appartenant à un acteur **français**. Cette solution présente de nombreux atouts par rapport à un data center : d'une part, elle offre des moyens de stockage et de traitement quasiment illimités ; d'autre part, le cloud est bien mieux sécurisé qu'un data center dans la mesure où les « cloud providers » ont mis au point des techniques sophistiquées de sécurisation des données qui leur sont confiées.

---

[1] *Le compte-rendu est disponible sur ce lien : http://www.senat.fr/compte-rendu-commissions/20211104/2021_10_28.html#toc3*

C. DÉVELOPPER LES USAGES NUMÉRIQUES EN PLEINE CONFORMITÉ AVEC LE PRINCIPE DE SUBSIDIARITÉ

1. Un principe général : déterminer l'échelon pertinent d'intervention

En application du principe de subsidiarité inscrit à l'article 72 de la Constitution depuis 2003[1], *« les collectivités territoriales ont vocation à prendre les décisions pour l'ensemble des compétences qui peuvent être mises en œuvre à leur échelon »*. Le principe de subsidiarité implique ainsi d'organiser les politiques publiques à l'échelon le plus proche des citoyens, au plus près des territoires. Ainsi, la commune doit, en principe, être préférée à l'intercommunalité et au département, sauf s'il est établi que l'action de ces derniers est plus efficace. Ce principe a naturellement **toute sa pertinence dans la conduite des projets numériques.**

Ainsi, le rapport précité, intitulé « *les collectivités territoriales face au défi de la cybersécurité* » souligne la nécessité de réfléchir à l'application du principe de subsidiarité en matière de politique de **sécurité numérique**.

Deux critères doivent être pris en compte pour apprécier le niveau pertinent d'intervention et la « taille critique » : la soutenabilité financière et la technicité requise par le projet. En effet, il apparait nécessaire de confier la compétence numérique à l'échelon qui assure la **meilleure veille technologique** et qui dispose des **meilleures compétences**. Cette exigence se justifie d'autant plus dans un contexte marqué par un **foisonnement de l'offre numérique**, foisonnement qui a été souvent relevé lors des auditions.

Ce principe de subsidiarité, indique le rapport, permettrait aux petites collectivités, identifiées comme des « *maillons faibles* », de bénéficier, par l'effet de la mutualisation, d'une **protection numérique renforcée**. L'échelle de pertinence doit être appréciée *in concreto* selon les réalités territoriales. Il peut s'agir soit du niveau **intercommunal,** soit **départemental**.

Comme l'a souligné Mme Françoise GATEL, présidente de notre délégation, lors de la table-ronde précitée du 28 octobre 2021, *« il n'est pas possible de définir a priori une échelle de pertinence. L'intercommunalité peut être extrêmement pertinente alors que, dans d'autres cas, le sujet est porté par les départements. Il est surtout important que le sujet soit traité au niveau du territoire le plus pertinent, en confiant le sujet à des collègues compétents sur les sujets de cybersécurité »*.

Le principe de subsidiarité vaut non seulement pour les projets de **sécurisation des données,** mais aussi pour ceux visant à **développer les usages en matière de protection des populations.** La mutualisation répond

[1] *Loi constitutionnelle n° 2003-276 du 28 mars 2003 relative à l'organisation décentralisée de la République.*

ainsi à l'objectif de **renforcement de l'expertise locale**, « d'interopérabilité » et de « sobriété » des outils numériques. Vos rapporteurs ont souhaité, en particulier, insister sur l'intérêt de mutualiser les **centres de supervision urbain**.

2. mutualiser les centres de supervision urbain

Le rapport précité de notre délégation consacré à l'« *ancrage territorial de la sécurité intérieure* » préconise de **mettre en commun des agents de police municipale** dans le cadre des **centres de supervision urbain**. L'objectif est double : d'une part, amortir le coût de réalisation de ces centres, d'autre part, de suivre des images dans une zone géographique aussi étendue que possible. Toutefois, cette nécessité se heurte à **certaines réticences** liées à la crainte des maires de se voir dépossédés de leur pouvoir de police[1].

Contactée par vos rapporteurs, l'association « Villes de France » a ainsi souligné le faible nombre de villes moyennes qui mènent des **projets mutualisés de centres de supervision urbain[2]**. L'association a simplement cité des projets en cours au sein des communautés d'agglomération d'**Ajaccio** et de **Mont-de-Marsan**.

De même l'association n'a constaté, à ce stade, aucun effet positif résultant de la simplification opérée par la loi du 25 mai 2021 dite « sécurité globale ». En effet, dans sa rédaction antérieure à cette loi, le code de la sécurité intérieure prévoyait un seuil de 80.000 habitants au-delà duquel des communes formant un **seul tenant**[3] mais **non membres d'un même EPCI,** ne pouvaient pas mettre en commun leurs agents de police municipale (art 512-1 du code de la sécurité intérieure). Dès lors que cette mutualisation fonctionne sur la base du volontariat, ce seuil démographique a été opportunément supprimé par le législateur. Les possibilités de **mutualisation des centres de supervision urbains** ont donc été élargies. Vos rapporteurs encouragent donc les **communes à faire un usage actif de ces nouvelles dispositions** qui ne semblent pas encore utilisées.

Enfin, vos rapporteurs encouragent les élus à mobiliser le Fonds interministériel de prévention de la délinquance (FIPD) ainsi que la dotation d'équipement des territoires ruraux (DETR).

---

[1] *Voir la recommandation n°9 du rapport « ancrage territorial de la sécurité ».*

[2] *L'association « Villes de France » regroupe les villes et intercommunalités de taille infra-métropolitaine (villes moyennes dont la population est comprise entre 10.000 et 100.000 habitants).*

[3] *La notion « d'un seul tenant » a été définie en référence au principe de continuité territoriale : chaque commune doit être limitrophe d'au moins une des autres communes qui composent l'ensemble.*

En premier lieu, il y a lieu de rappeler que le FIPD, créé par la loi du 5 mars 2007 relative à la prévention de la délinquance, est géré essentiellement par les préfets. Il a vocation à financer des actions qui déclinent localement la stratégie nationale de prévention de la délinquance 2020-2024. La circulaire du ministère de l'intérieur en date du 5 mars 2020[1] souligne l'intérêt de financer, via ce fonds, des projets de vidéo-protection : « *Le développement de la vidéo-protection depuis ces dernières années s'est inscrit dans le cadre d'une* ***politique de modernisation des outils au service de la sécurité****. Elle peut également permettre aux enquêteurs de s'appuyer sur les images enregistrées dans le cadre d'une enquête judiciaire. (…) Pourront être soutenus dans ce cadre les projets* ***d'installation de caméras sur la voie publique*** *ou aux abords de lieux ouverts au public [et] les* ***projets de centre de supervision urbain*** *(..). Une attention particulière sera portée aux projets de vidéo protection disposant* ***d'innovations technologiques*** ».

En second lieu, cette même circulaire recommande également aux préfets de « *mobiliser la dotation d'équipement des territoires ruraux (…) pour le financement de ces systèmes de vidéo protection* ».

Ajoutons que la circulaire du 30 avril 2021 relative aux orientations budgétaires du FIPD pour l'année 2021 invite les préfets à consacrer au moins **75 % des crédits** qui leur sont délégués au titre du programme S (sécurisation) à des projets de **vidéo-protection**[2]. Cette même instruction insiste sur la nécessité de « *subventionner les projets portés par les collectivités intégrant nécessairement les* ***transferts d'images*** *vers les commissariats et brigades* ». Enfin, cette circulaire recommande aux représentants de l'État « *d'expérimenter le traitement automatisé de l'image (…), par exemple grâce à des logiciels de* ***détection des situations*** *comportant un danger manifeste (mouvement de foule inhabituel, intrusion dans un espace interdit, départ d'incendie…)* ». Cette recommandation correspond à l'initiative menée, par exemple, par le syndicat mixte « *Seine et Yvelines Numériques* » dont le dispositif de surveillance ne s'allume que **lorsque les algorithmes détectent une situation anormale** dans l'un des lieux surveillés, comme indiqué *supra*.

D. DONNER UNE BASE LÉGALE À L'USAGE DES DRONES PAR LA POLICE MUNICIPALE

Au cours des auditions, de nombreux élus municipaux ont regretté **l'absence de base légale** pour l'usage des caméras aéroportées par la police municipale.

Force est de constater que les « bonnes pratiques » décrites dans le présent rapport se sont développées sur des **bases juridiques fragiles**. C'est

---

[1] *Voir la circulaire-cadre du 5 mars 2020 relative à la déclinaison territoriale des politiques de prévention de la délinquance et de prévention de la radicalisation pour les années 2020 à* 2022 *ainsi que la circulaire du 30 avril 2021 relative aux orientations budgétaires du FIPD pour l'année 2021.*

[2] *Ce programme bénéficie de crédits de 15 millions d'euros pour l'année 2021.*

pourquoi le Parlement a adopté un amendement, dans le cadre de l'examen du projet de loi relatif à la responsabilité pénale et à la sécurité intérieure, ouvrant la possibilité aux services de police municipale de **recourir à des drones, à titre expérimental pour une durée de cinq ans.** Trois finalités ont été prévues par l'amendement :

- la sécurité des manifestations et des périmètres de protection auxquels les policiers municipaux peuvent être affectés ;
- la régulation des flux de transport dans l'exercice des pouvoirs de la circulation exercés par le maire ;
- la surveillance des espaces naturels.

Le Parlement a prévu que l'utilisation des drones serait soumise à l'obtention d'une autorisation préfectorale délivrée dans les mêmes conditions que pour les forces de sécurité intérieure ainsi qu'à l'existence d'une **convention de coordination** des interventions de la police municipale et des forces de sécurité de l'État. Cette condition est conforme à la 4ème recommandation du rapport précité sur l'ancrage territorial de la sécurité. En effet, cette recommandation, intitulée « *renforcer les liens opérationnels entre les polices municipales et les forces régaliennes de sécurité* », souligne l'importance des conventions de coordination, créées par la loi n° 99-291 du 15 avril 1999 relative aux polices municipales.

Toutefois, le dispositif a été **censuré par le Conseil constitutionnel** le 20 janvier 2022 au motif qu'il n'était pas assorti de **garanties suffisantes** de nature à sauvegarder le droit au respect de la vie privée. Le juge constitutionnel a en effet insisté sur le caractère intrusif des drones : « *Eu égard à leur mobilité et à la hauteur à laquelle ils peuvent évoluer, ces appareils sont susceptibles de capter, en tout lieu et sans que leur présence soit détectée, des images d'un nombre très important de personnes et de suivre leurs déplacements dans un vaste périmètre* ».

Vos rapporteurs soulignent donc la nécessité de donner rapidement une **nouvelle base juridique** au recours aux drones, eu égard à leur intérêt incontestable en matière de protection des populations. Afin de tirer tous les enseignements de la décision du Conseil constitutionnel, il appartiendra au législateur, en lien étroit avec l'association des maires de France, de garantir un **équilibre satisfaisant** entre **opérationnalité de l'usage des caméras aéroportées** et **protection du droit au respect de la vie privée.**

E. RENFORCER LA COOPÉRATION ENTRE LES COLLECTIVITÉS TERRITORIALES ET LES SERVICES DÉCONCENTRÉS DE L'ETAT DANS LE DOMAINE DE LA PROTECTION DES POPULATIONS

Vos rapporteurs ont acquis la conviction, lors de leurs travaux, que la coopération entre les **collectivités territoriales** et les **services déconcentrés** mérite d'être **renforcée**.

Cette exigence concerne, en premier lieu, la protection de la sécurité publique. Les auditions ont en effet confirmé la pertinence des recommandations du rapport précité de notre délégation sur l'ancrage territorial de la sécurité : la réussite des politiques de sécurité sur le terrain requiert une articulation renforcée entre les communes et les services déconcentrés de l'Etat. Le numérique n'échappe pas à cette nécessité impérieuse de coordination intelligente, bien au contraire. Les bonnes pratiques locales, exposées dans le présent rapport, fondées sur le recours aux drones ou à la vidéo-protection, illustrent de manière emblématique cette exigence de synergie entre tous les acteurs.

La coopération communes/Etat apparait également déterminante dans le domaine de la **prévention des risques**. En effet, certaines auditions ont mis en lumière un **dialogue insuffisant** dans ce domaine, préjudiciable à la protection des populations. L'insuffisance de cette coopération a pu même être relevée par vos rapporteurs sur des projets numériques locaux pourtant financés par l'État. Or, la réussite des politiques de lutte contre les risques majeurs repose sur une très bonne articulation entre tous les acteurs. Rappelons, à cet égard, que l'article L. 125-2 du code de l'environnement impose autant **aux communes qu'à l'Etat** de contribuer à **l'information** du public sur les risques majeurs auxquels celui-ci est exposé.

La concertation est essentielle, en particulier, dans le domaine de l'**alerte des populations.** Les auditions menées dans le cadre du présent rapport ont montré que certains élus ont mis en place des dispositifs d'alerte en cas d'imminence d'un risque grave (inondation par exemple). Ces systèmes sont souvent imparfaits en ce qu'ils reposent sur des **démarches volontaires d'inscription préalable** (cf exemples de Sommières et d'Ajaccio). Ils doivent donc être **complétés** par l'action de l'Etat qui dispose d'outils bien plus puissants. Ainsi, le Système d'Alerte et d'informations aux populations (SAIP), souvent évoqué lors des auditions, constitue un ensemble d'outils permettant d'avertir la population d'une zone donnée, d'un danger imminent et de l'informer sur la nature du risque et le comportement à tenir. Basé sur la multidiffusion des messages, il rassemble donc différents vecteurs ainsi qu'un logiciel de déclenchement permettant aux maires et aux préfets d'assurer la protection de leur population. Toutefois, ce système, lancé en 2016 après les attentats de Paris, présente de nombreuses limites. Il sera complété en juin 2022 par un **nouveau dispositif bien plus performant**, le « cell broadcast », en français « diffusion cellulaire ». Il s'agit d'un système d'alerte sur téléphones mobiles utilisé dans de nombreux pays.

La diffusion cellulaire, un système prometteur

Les alertes par diffusion cellulaire prennent la forme de mini messages (SMS) prioritaires qui arrivent en même temps sur tous les mobiles. Ils s'affichent sur l'écran du mobile, même si celui-ci est verrouillé. Le système présente de nombreux avantages.

En premier lieu, nul n'est besoin de connaître les numéros des destinataires car les messages sont envoyés au niveau d'une « cellule » télécom ce qui permet de toucher tous les mobiles situés dans une zone, à l'instar d'un programme radio ou télé. Il est ainsi possible de cibler une zone géographique en particulier.

En second lieu, le système fonctionne, en principe, sur tous les mobiles, même les anciens, quel que soit l'opérateur, ainsi que sur les mobiles étrangers, ce qui permet d'informer les touristes de passage.

Enfin, le « cell broadcast » est opérationnel même lorsque les réseaux voix ou données sont saturés – ce qui peut être le cas lors d'événements importants – car ils utilisent des canaux spécifiques.

Le déploiement de ce système d'alerte localisé, très attendu, nécessitera, à l'évidence, une **très bonne coordination entre les élus et l'Etat**. Si vos rapporteurs estiment que ce système devra rester à la main de l'Etat, ne serait-ce que pour des raisons opérationnelles et techniques, il reposera sur une **communication efficace et hyper-réactive** entre les maires et les services préfectoraux.

CONCLUSION

La ville et le village de demain seront **nécessairement numériques**. Quelle que soit leur taille, ils mettront en œuvre, seuls ou accompagnés par d'autres collectivités, de nombreux **projets d'intelligence territoriale** au service de la protection des populations, mission placée au cœur de l'action publique locale.

Nos territoires sont aujourd'hui autant de laboratoires où se construit l'avenir, grâce aux capacités d'innovation des élus locaux. Véritables « inventeurs de solutions », ces derniers sont en quête permanente de solutions **performantes, agiles, pragmatiques et adaptées** aux besoins de la population.

À travers cette contribution, votre délégation a souhaité montrer l'existence de bonnes pratiques locales dans la **diversité de nos territoires connectés** : grâce à la pédagogie par l'exemple, l'objectif de ce travail est de diffuser des « pépites » technologiques qui pourront inspirer, demain, les décideurs publics locaux dans le domaine de l'ordre public et de la gestion des risques.

Surtout, votre délégation a souhaité montrer que la transformation numérique **n'est pas l'apanage des grandes agglomérations**. Elle est à la portée des territoires **péri-urbains et ruraux**.

Trois conditions essentielles doivent toutefois être **remplies**.

En premier lieu, les collectivités doivent miser sur la « **force du collectif** ». Il parait en effet hasardeux de se lancer dans l'aventure numérique sans une expertise solide, ce qui nécessite, bien souvent, de privilégier l'échelon **intercommunal** ou **départemental**.

En deuxième lieu, les innovations technologiques ne seront bénéfiques pour tous que si et seulement si elles s'opèrent dans un **environnement de confiance :** on ne saurait construire de territoires intelligents **sans sécurité**. Comme le souligne l'adage, *« Quand on construit une maison, on met des portes et des serrures ».* Une collectivité territoriale qui n'a pas encore été attaquée pourra l'être, et une collectivité territoriale attaquée une fois pourra l'être de nouveau deux ou trois fois. Il convient donc de développer les outils **avec un souci constant de protection**, y compris dans les territoires ruraux, souvent présentés comme « les maillons faibles » de la sécurité numérique.

Enfin, si le présent rapport porte sur les « usages » et non sur les « tuyaux », vos rapporteurs relèvent que les deux sujets sont indissociablement liés. En conséquence, ils appellent de leurs vœux la **résorption des fractures numériques**. En effet, la crise sanitaire et le confinement ont confirmé l'ampleur des inégalités d'accès au numérique en France. Un tiers des habitants des communes de moins de 1.000 habitants ne

peut accéder à un internet de qualité minimale et le débit internet en zone rurale est de deux à cinq fois plus faible qu'en ville. Le télétravail imposé durant le confinement a également révélé que 5 millions de salariés rencontraient de fortes difficultés face au numérique. Vos rapporteurs souligne qu'une fracture numérique sociale et générationnelle représente un handicap dans notre société toujours plus numérisée et que ceux qui en sont exclus ont le sentiment d'être des « citoyens de seconde zone ».

Face à cette situation préoccupante, le gouvernement a affirmé, en réponse à une question posée par notre collègue M. Stéphane Demilly, que le déploiement « *de la fibre optique et de la 4G pour l'ensemble des Français est le socle indispensable pour résorber les fractures numériques*. (…) *C'est pour cette raison que le Gouvernement a fixé des objectifs ambitieux pour le déploiement du très haut débit pour tous et vise, en particulier, la couverture générale en fibre optique du territoire d'ici* **2025**[1] ».

Vos rapporteurs ajoutent que la **solution satellitaire** mérite un examen attentif par les collectivités territoriales, en particulier dans les zones blanches, sans connexion, ou dans les zones grises, mal desservies. On pense notamment à certaines zones de montagne qu'il sera difficile de couvrir jusqu'au dernier kilomètre. Or, le satellite offre un mode de connexion dont le **rapport performance/coût** s'est significativement amélioré depuis quelques années.

En tout état de cause, vos rapporteurs saluent l'ambition du Plan France Très Haut Débit et espère que les espoirs qu'elle fait naitre, notamment dans les territoires ruraux, ne seront pas, une nouvelle fois, déçus.

[1] *Question écrite n° 22156 publiée dans le JO Sénat du 15 avril 2021 ; réponse du Gouvernement publiée le 27 mai 2021 : http://www.senat.fr/questions/base/2021/qSEQ210422156.html*

EXAMEN EN DÉLÉGATION

COMPTE-RENDU DE LA RÉUNION PLÉNIERE DU 20 JANVIER 2022

Mme Françoise Gatel, présidente. – Bonjour à tous. Nous avons aujourd'hui un moment essentiel, avec l'examen du rapport portant sur les territoires connectés et la protection des populations, sujet dont se sont saisis nos trois collègues, Anne-Catherine Loisier, Antoine Lefèvre, vice-président de la délégation, et Jean-Yves Roux. Je les remercie d'avoir investi ce sujet auquel les élus sont de plus en plus sensibles et qu'il nous convient de valoriser et d'approfondir, puisqu'il s'inscrit dans la thématique qui nous est chère : les élus inventeurs de solutions. De manière générale, les élus qui sont confrontés régulièrement à des sujets complexes et des difficultés de toute nature ont cet art exceptionnel, souvent méconnu par l'État, d'inventer des solutions. Nous pensons que ce sujet des territoires connectés y contribue très fortement. Cette délégation souhaite valoriser, faire connaître et diffuser des bonnes pratiques qui peuvent inspirer d'autres collectivités, mais aussi nourrir les propositions de loi. Je souhaite donc les remercier pour ce rapport flash, qui a le mérite de se concentrer sur l'essentiel et de formuler des propositions qui interpellent le gouvernement. Nous souhaitons en effet pouvoir communiquer ces rapports aux ministres concernés, considérant que le travail réalisé par la délégation est un travail de fond très important, qui n'est pas soumis à des contingences de processus législatif ou de contexte électoral. Nous avons vu l'intérêt du rapport des déserts médicaux, lui aussi un rapport flash.

Je ne peux que faire mention du risque cybersécurité. Nous avons conduit un travail avec la délégation aux entreprises. Nous avons organisé une table ronde extrêmement intéressante et pertinente à ce sujet. Tout établissement public, y compris une commune, quelle que soit sa taille, peut être gravement paralysé par un problème de cybersécurité.

Je vous remercie, au nom de la délégation et en mon nom personnel, et vous cède la parole. La présentation de ce rapport sera suivie d'une conférence de presse.

M. Antoine Lefèvre, vice-président. – Merci, Madame la Présidente.

En 2017, notre délégation rendait public le rapport intitulé « Les nouvelles technologies au service de la modernisation des territoires ». Les rapporteurs Jacques Mézard et Philippe Mouiller soulignaient d'ailleurs, exemples concrets à l'appui, les nombreux apports du digital : efficacité de l'action publique, meilleur service aux usagers, économies budgétaires, développement durable, attractivité des territoires. Notre délégation a souhaité, cinq ans plus tard, porter son attention sur cette même thématique, mais en circonscrivant son périmètre à la protection des populations, dans la

mesure où, d'une part, le numérique apporte dans ce domaine une plus-value très significative, et où, d'autre part, les potentiels de développement sont très élevés. Deux axes ont été étudiés : la protection de l'ordre public ainsi que la sécurité civile. Deux objectifs ont présidé à cette mission flash : à la fois identifier les bonnes pratiques locales dans ces deux champs de l'action publique locale, en milieu rural comme dans les zones urbaines, et formuler des recommandations vivant à encourager et sécuriser ces initiatives locales, mais aussi supprimer ou limiter l'éventuelle entrave à leur réalisation.

Nous allons avant tout évoquer les bonnes pratiques locales en matière de protection de l'ordre public, en rappelant que les maires, pivots de la sécurité dans leur commune, sont au cœur du continuum de sécurité. Afin d'accomplir au mieux leurs missions de protection de l'ordre public et de prévention de la délinquance, ils peuvent tirer un grand profit du numérique. Le rapport en fournit trois exemples. D'abord, les centres de supervision urbains (CSU) peuvent être mutualisés entre plusieurs collectivités. Il s'agit de salles équipées d'écrans affichant en direct les images filmées par des caméras de vidéo-protection. Les CSU ont pour objectif de prévenir les atteintes aux biens et aux personnes, d'identifier les auteurs, de réguler la circulation urbaine et de sécuriser les bâtiments et les sites communaux. La mission a d'ailleurs salué l'exemple d'un CSU de ville moyenne, Charleville-Mézières, qui bénéficie d'une unité vidéo et d'un poste de commandement. De même, le CSU du département des Yvelines possède, depuis 2019, un dispositif de vidéo-protection avec une connexion aux images des communes qui le souhaitent depuis l'entrée en vigueur de la loi sécurité globale. En outre, les écrans noirs utilisent une technologie fondée sur l'intelligence artificielle. Ils ne s'allument que lorsque les algorithmes détectent une situation anormale dans l'un des lieux surveillés. Les drones constituent également une pratique locale intéressante en matière de protection de l'ordre public. À titre d'illustration, la ville d'Istres (43 000 habitants), qui a acquis deux drones au début de l'été 2020, est la première commune de France à doter sa police municipale de tels outils. Les drones sont équipés de caméras de haute définition et permettent à la police l'identification des auteurs de méfaits en temps réel. Bien sûr, il y a également le dispositif « Voisins vigilants ». Le rapport salue l'efficacité du dispositif fonctionnant via un site web permettant de mettre en relation les habitants d'un même quartier pour lutter ensemble contre les cambriolages de manière simple et gratuite. Il compte aujourd'hui 700 mairies adhérentes chargées de deux missions principales : d'une part financer la signalétique et, d'autre part, conduire des opérations de communication et de sensibilisation auprès des habitants, notamment dans les zones exposées aux risques de cambriolage ou de violence. Ce procédé simple et peu coûteux fonctionne essentiellement par une application intuitive et par l'envoi de SMS. De plus, son efficacité est avérée, puisqu'une baisse des cambriolages de 40 % par an a été constatée par le ministère de l'Intérieur.

M. Jean-Yves Roux. – Le rapport met en exergue certaines bonnes pratiques locales en matière de prévention des risques. En premier lieu, il salue quelques actions exemplaires menées par les élus locaux dans la gestion du risque inondation, qui constitue le premier risque naturel en France et concerne plus de 17 millions d'habitants permanents. Le rapport cite ainsi le dispositif d'évaluation et de suivi des pluies en agglomération pour devancer l'alerte (« ESPADA ») mise en place par la ville de Nîmes. Il permet la surveillance de l'évolution des précipitations et du ruissellement par réseaux de stations de mesure hydrométéorologiques et de caméras de surveillance. De même, le sophistiqué dispositif numérique d'alerte des crues, géré par le Pays de Lourdes et des Vallées des Gaves, permet d'alerter les habitants par téléphone, via internet ou directement sur leur application mobile. En outre, la mise en place d'outils d'observation grâce à des galets équipés de puces RFID contribue à étudier les déplacements des sédiments à l'origine des crues. Ce projet expérimental a constitué une précieuse aide à la décision pour les élus. Enfin, la commune de Sommières, dans le Gard, a mis en place un système d'alerte au moyen de technologies plus rudimentaires.

En deuxième lieu, le rapport cite, s'agissant du risque incendie, l'action du conseil départemental des Bouches-du-Rhône, qui s'est muni, en partenariat avec le SDIS, depuis 2014, de drones de seconde génération dotés de capteurs infrarouges détectant de façon plus précise les départs de feu, constituant un dispositif préventif de surveillance des incendies.

Concernant le risque avalanche, l'exemple des drones utilisés à Val Thorens, le plus grand domaine skiable au monde, démontre la performance du recours à ces aéronefs dotés de caméras très performantes : l'une est thermique et l'autre dotée d'un zoom grossissant 200 fois. En assurant des missions de secours aux personnes, ces caméras permettent d'analyser le terrain en cas d'avalanche et, hors saison, participent aux opérations de maintenance de la station. Les drones n'ont pas vocation à se substituer aux interventions humaines, mais constituent un précieux moyen de soutien aux équipes du service des pistes. Le rapport souligne la constante augmentation du rapport performances/coûts des drones et leur immense potentiel d'utilisation dans les années à venir par les élus locaux.

Enfin, le rapport met en avant la possibilité, à travers l'exemple de la commune d'Ajaccio, de mettre en place un dispositif numérique multirisques. En effet, cette commune exposée à de multiples risques naturels et technologiques a su pleinement tirer profit du numérique pour répondre à ces défis. En premier lieu, la ville s'est dotée de divers outils d'observation et de contrôle, afin notamment de prévenir les risques incendie et inondation. En second lieu, elle a déployé en 2019 une plateforme multicanale de télé-alerte afin de prévenir sa population en cas de crise. Ce dispositif qui repose sur une démarche volontaire d'inscription permet aux usagers résidents permanents ou ponctuels de recevoir une alerte en cas de

situation d'urgence liée à divers risques majeurs. Cette bonne pratique locale serait transposable dans d'autres communes.

Mme Anne-Catherine Loisier. – Nous arrivons aux recommandations, au nombre de cinq, que nous avons pu tirer de ces différents témoignages et expériences. La première consiste à préconiser de recourir aux technologies numériques suivant une démarche rigoureuse, c'est-à-dire après un bilan coûts/avantages actualisé, partagé et rendu public. L'enjeu est de mettre en valeur la plus-value numérique et de légitimer le recours à la démarche numérique. Les solutions numériques doivent être lancées par les élus avec des objectifs clairement définis et s'accompagner d'une communication attentive auprès des habitants, selon une démarche rigoureuse, fondée sur une réflexion préalable et approfondie. Il est essentiel d'informer en amont les populations concernées par les risques majeurs, l'état des risques auxquels elles sont exposées et le bilan coûts/avantages d'une démarche numérique.

La deuxième recommandation consiste à sensibiliser les élus et le personnel aux enjeux de la cybersécurité. L'efficacité de la démarche numérique repose sur un numérique de confiance, donc sécurisé, qui doit s'appuyer sur une montée en compétence des élus, mais aussi des services en responsabilité. Les usagers doivent également être assurés d'un niveau optimal de protection et de mise à jour permanente des systèmes de protection de leurs données. Le développement des usages du numérique doit aller de pair avec la prévention et le renforcement du bouclier de protection. Ces deux piliers sont essentiels pour que les communes locales se préservent de ce qui pourrait autrement devenir un colosse numérique aux pieds d'argile, à savoir un système avec des failles numériques grandissantes et donc une vulnérabilité non maîtrisée. Pour ce faire, il convient de sensibiliser les acteurs et d'assurer une veille permanente, qui doit associer véritablement les élus et les services à ces enjeux de cybersécurité. Ceci passe par un travail d'information des opportunités, mais aussi des menaces numériques et des potentielles conséquences en cas d'attaque. Il s'agit donc de familiariser l'ensemble des acteurs aux bonnes pratiques ainsi qu'aux procédures de continuité et de reprise d'activité en cas de survenance d'une crise d'origine numérique. En cela, nous insistons sur le rôle du responsable sécurité des systèmes d'information (RSSI), et nous conseillons vivement aux élus de positionner le RSSI comme un véritable directeur stratégique de la sécurité numérique, en lien direct et permanent avec les élus et les directeurs des services stratégiques, afin d'assurer une veille décisionnelle efficace en matière de cyberattaque.

La troisième préconisation serait de développer ces usages numériques en privilégiant le principe de subsidiarité et de mutualisation. Il apparaît pertinent de confier la compétence numérique à l'échelon en capacité d'assurer à la fois cette veille technologique, mais aussi la veille de sécurisation et d'adaptation, à savoir la collectivité ou l'échelon de

collectivité qui dispose des compétences les plus adaptées et qui sera donc le plus efficace en termes d'ajustement et de prévention. Il s'agit souvent des niveaux intercommunal ou départemental, qui sont également les plus pertinents pour mutualiser. Nous avons été frappés par l'exemple des agents de police municipale dans le cadre des CSU mutualisés. Ces derniers permettent en effet d'amortir les coûts d'investissement, de fonctionnement et de mise à jour de ces centres, et d'utiliser les bénéfices, en l'occurrence les images, dans un périmètre géographique plus étendu, et donc plus pertinent au regard de conséquences qui ne s'arrêtent pas aux frontières de nos communes.

M. Jean-Yves Roux. – La quatrième recommandation concerne le recours aux drones par les services de police municipale. Nous avons vu combien les drones pouvaient être utiles dans le cadre de la protection des populations. Il s'agit toutefois d'une technologie par nature intrusive. Il convient donc de donner une base juridique solide à cette pratique en garantissant un équilibre satisfaisant entre opérationnalité de l'usage des caméras aéroportées et protection du droit au respect de la vie privée, tout en prévoyant l'existence d'une convention de coordination des interventions de police municipale et des forces de sécurité de l'État.

Mme Anne-Catherine Loisier. – Enfin, la cinquième et dernière recommandation consiste à s'appuyer davantage sur une coopération entre les collectivités et les services déconcentrés de l'État dans le domaine de la protection des populations. Cette coopération mérite en effet d'être renforcée pour optimiser les atouts des deux entités, à la fois proximité et supervision. Elle s'impose même en matière de sécurité publique, pour des raisons pratiques, réglementaires, voire juridiques, notamment dans l'usage des drones ou de la vidéo-protection, mais également en matière de prévention des risques ou d'alerte des populations. Je pense par exemple au déploiement, en juin 2022, du système d'alerte dit *cell broadcast*, ou diffusion cellulaire, qui nécessitera une parfaite coordination entre les collectivités locales et l'État. Ce système devra rester à la main de l'État pour des raisons opérationnelles et techniques mais, pour son efficacité, reposera sur un partenariat et une communication étroite et réactive avec les élus locaux, les seuls à même de garantir la réelle couverture et le message jusqu'à la population.

M. Antoine Lefèvre, vice-président. – Je vous propose à présent de vous présenter la conclusion de notre rapport.

La ville et le village de demain seront nécessairement numériques. Quelle que soit leur taille, ils mettront en œuvre, seuls ou accompagnés par d'autres collectivités, de nombreux projets d'intelligence territoriale au service de la protection des populations, mission placée au cœur de l'action publique locale. Nos territoires sont aujourd'hui autant de laboratoires où se construit l'avenir, grâce aux capacités d'innovation des élus locaux. Véritables inventeurs de solutions, ces derniers sont en quête permanente de

plans d'actions performants, agiles, pragmatiques et adaptées aux besoins de la population. À travers notre rapport, nous avons souhaité montrer l'existence de bonnes pratiques locales dans la diversité de nos territoires connectés. Grâce à la pédagogie par l'exemple, l'objectif de ce travail est de diffuser les pépites technologiques qui pourront inspirer, demain, les décideurs publics locaux dans le domaine de l'ordre public et de la gestion des risques. Surtout, nous avons souhaité montrer que la transformation numérique n'est pas l'apanage des grandes agglomérations ; elle est à la portée des territoires périurbains et ruraux. Trois conditions essentielles doivent toutefois être remplies. En premier lieu, les collectivités doivent miser sur la force du collectif. Il apparaît en effet hasardeux de se lancer dans l'aventure numérique sans une expertise solide, ce qui nécessite bien souvent de privilégier l'échelon intercommunal ou départemental. En deuxième lieu, les innovations technologiques ne seront bénéfiques pour tous que si elles s'opèrent dans un environnement de confiance. On ne saurait construire de territoire intelligent sans sécurité, et nous devons éviter de créer des colosses numériques aux pieds d'argile. Enfin, si le présent rapport porte sur des usages et non des tuyaux, les deux sujets sont évidemment liés. C'est pourquoi nous appelons à la résorption des fractures numériques. En effet, la crise sanitaire et le confinement ont confirmé l'ampleur des inégalités d'accès au numérique en France. Nous soulignons donc que la solution satellitaire mérite un examen attentif par les collectivités territoriales, en particulier dans les zones blanches, sans connexion, ou dans les zones grises, mal desservies. Nous pensons notamment à certaines zones de montagne. Quoi qu'il en soit, nous saluons l'ambition du plan de relance très haut débit et espérons que les espoirs qu'il fait naître, notamment dans les territoires ruraux, ne seront pas une nouvelle fois déçus.

Pour terminer, je souhaite, au nom des co-rapporteurs, remercier Bruno Lehnisch, notre administrateur, qui nous a accompagnés tout au long de l'élaboration de ce rapport, ainsi que les équipes de la délégation. Merci pour leur patience et leur coopération.

Mme Françoise Gatel, présidente. – Merci beaucoup à tous les trois. Je souhaite encore vous remercier de vous être emparés d'un sujet essentiel. Avant de laisser la parole aux collègues, je suis heureuse des remerciements que vous adressez à l'équipe de la délégation, qui porte un travail colossal, nous accompagne et nous appuie et est remarquable en termes de disponibilité et de qualité de travail.

Ce rapport traite de sujets absolument essentiels, à savoir l'amélioration du service aux habitants, la lutte contre les fractures numériques et la nécessaire vigilance face à la cybermalveillance. À chaque échelle, dès lors que nos collègues pratiquent l'intelligence territoriale de la mutualisation, nous devons trouver des solutions. Vous avez montré combien ces outils pouvaient être d'importance pour prévenir la population de risques d'avalanche et d'inondation et permettre aux élus de développer

un plan d'action ou de réaction à des événements soudains. Ce rapport est donc majeur. Au-delà des communications au ministre, nous pourrions échanger avec les associations d'élus locaux sur ce rapport pour que, au-delà des actions qu'elles entreprennent auprès de leurs adhérents, notre délégation puisse contribuer à une action de sensibilisation, par votre intermédiaire.

Je laisse la parole à nos collègues.

M. Franck Montaugé. – Merci Madame la Présidente. Merci à nos collègues pour ce travail très intéressant sur ce sujet fondamental pour l'avenir de nos territoires et de nos populations.

Je souscris pleinement à la nécessité d'une gestion de ces enjeux, où le raccordement et la question de la sécurité doivent être traités à des mailles adaptées. Dans le milieu rural, où les petites mairies manquent de moyens, la maille départementale est la plus appropriée pour développer, notamment en direction des collectivités locales, des services de sécurité adaptés.

La dimension technologique est prépondérante dans ces questions, avec notamment un domaine en forte évolution, la 5G. Je me pose la question de la réutilisation du réseau de télévision numérique terrestre, dont certains spécialistes avancent qu'il pourrait être mobilisé pour proposer de l'hertzien à très haut débit, jusque dans les zones les plus reculées. Cette piste me semble importante.

Ces questions de sécurité, à l'égard des collectivités comme des particuliers et des entreprises, posent en outre la question de l'équipement du territoire en *data centers*. Un plan national d'équipement est nécessaire. Il s'agit d'une des conditions de la sécurisation des utilisateurs du numérique, au regard des agressions que nous constatons et qui, hélas, se développent.

Mme Anne-Catherine Loisier. – Merci beaucoup. Notre rapport souligne l'importance d'accompagner nos collègues élus dans l'instauration d'une culture numérique sur tout le territoire. Nous voyons aujourd'hui que certains territoires sont très innovants, alors que d'autres sont quelque peu frileux, car ils ne comprennent pas nécessairement toutes les opportunités offertes par les outils ni leurs risques potentiels. Ce rapport traduit donc la volonté de sensibiliser nos collègues, mais également le gouvernement, sur la nécessité d'accompagner l'ensemble du territoire dans une culture du numérique qui prospèrera dans les années à venir.

Sur la question des *data centers*, il se pose effectivement la question du stockage. Nous voyons un certain nombre de *data centers* se mettre en place sur les territoires. Pour répondre à la demande des entreprises, peu de *data centers* accueillent des données publiques. À ma surprise, nos interlocuteurs, qui étaient de grands acteurs comme Atos, ne semblent pas particulièrement attirés par les *data centers* et privilégient l'option du stockage dans les *clouds*. Il s'agit certainement d'un sujet à approfondir, en

termes de sécurisation. Nous savons qu'une démarche de *cloud* européen est actuellement conduite avec Atos et OVH.

Mme Céline Brulin. – Merci aux trois co-rapporteurs pour leur travail très intéressant. Je suis particulièrement sensible à deux aspects qu'ils ont traités. Le premier concerne les risques technologiques majeurs et le *cell broadcast*. Après l'expérience que nous avons connue avec l'incendie du Lubrizol, dans notre département, il a été révélé au grand public que nous étions très en retard en matière de prévention et de communication en direction des populations. Le *cell broadcast* a l'intérêt de prévenir l'ensemble des personnes qui se trouvent dans une zone par leur téléphone portable, même éteint. Les autres systèmes, en dehors des sirènes, reposent sur la base du volontariat. Les personnes exposées aux risques majeurs pouvaient ainsi indiquer souhaiter être contactées, mais une personne qui se trouverait à l'endroit pour une raison quelconque ne l'était pas. La métropole de Rouen est retenue pour être une zone d'expérimentation. Nous devons continuer de plaider, comme le faisait le rapport de la commission d'enquête de Lubrizol, pour une accélération du développement de ces systèmes. L'accident a eu lieu en septembre 2019. Nous sommes en janvier 2022 et nous n'avons pas encore abouti à une expérimentation, alors que les populations ont une sensibilité particulière et légitime.

Deuxièmement, je suis particulièrement en accord avec vous s'agissant des potentialités de ces nouvelles technologies et des risques de fractures territoriales et numériques qu'elles peuvent engendrer. Vous l'avez parfaitement développé sous l'angle de la crise que nous venons de vivre. Dans certains territoires, la 3G fonctionne encore à peine, alors que les maisons France Services proposent elles-mêmes des services numériques, comme la télémédecine. Nous devons être attentifs à ce que ces fractures ne s'accroissent pas.

M. Antoine Lefèvre, vice-président. – Merci d'avoir souligné la nécessité d'accélérer ces développements. Les outils technologiques sont aujourd'hui performants. Dans les systèmes d'alerte actuels, il est effectivement possible de s'inscrire et de recevoir un SMS. L'objectif est de donner davantage de garanties pour prévenir toute personne présente dans le périmètre de manière efficace. Pour les élus comme pour la population, l'enjeu est celui de la sensibilisation et de la formation à ces nouvelles techniques et à la réaction dans ces périodes de crise. Nous ne sommes pas assez formés sur ces questions. Beaucoup de pays européens ont cette culture de la catastrophe. En Allemagne, par exemple, des dispositifs conduisent à rassembler la sécurité civile et les pompiers et à mutualiser les moyens, mais aussi à développer chez les citoyens et les élus une véritable culture pour bien réagir en cas de catastrophe industrielle ou naturelle.

M. Jean-Yves Roux. – Rouen devrait effectivement être choisi par le gouvernement en tant que pilote du développement du *cell broadcast*. Dans nos auditions, nous avons soulevé des réflexions sur la ruralité et le

numérique. Le téléphone doit absolument être en veille pour recevoir une alerte. Le message que les téléphones portables vont recevoir doit en outre être très clair.

Mme Anne-Catherine Loisier. – Ces technologies du numérique évoluent en permanence, d'où l'importance de la notion de veille, et donc de l'adaptation permanente de nos technologies les plus adaptées pour tirer parti des progrès. Nous avons été impressionnés par l'attention de nos collègues élus et leur capacité à s'emparer de technologies innovantes et émergentes, mais aussi la capacité de nos grandes entreprises à faire progresser nos outils. En termes d'actualité, il existe sur mon territoire un site CEA. En matière d'information des populations, nous n'utilisons pas du tout ces technologies, qui seraient pourtant appropriées.

La fracture numérique peut être un véritable frein au déploiement de ces outils, ce qui m'amène à insister de nouveau sur l'outil satellitaire. Un projet est en cours depuis deux ans avec Eutelsat, concernant un satellite dédié au numérique, avec un numérique haut débit, à 100 Mo. Le satellitaire permettra de désenclaver les territoires pour lesquels nous n'avions pas, aujourd'hui, de solution filaire ou terrestre.

Mme Françoise Gatel, présidente. – Cette responsabilité de chaque citoyen sur la culture du risque est apparue dans un autre rapport, portant quant à lui sur la défense incendie. Nous devons, dans notre pays, développer cette culture. La protection des populations relève certes essentiellement du rôle des pouvoirs publics, mais nous devons aussi y éduquer et sensibiliser l'ensemble de nos citoyens.

Cette exigence que vous évoquez, qui doit être diffusée largement, suppose que les territoires disposent d'un responsable de la sécurité des systèmes d'information (RSSI), et donc d'un élu, peut-être à l'échelle de l'intercommunalité ou du département, qui soit porteur de ce sujet. Nous devons intégrer dans les stratégies des collectivités cette dimension qui ne l'est pas aujourd'hui. Avec l'exemple de la Rochelle, nous avons vu que l'incident de piratage ne devrait plus se produire car un élu responsable de la sécurité des systèmes d'information a été nommé. Il y a aujourd'hui dans le champ de la compétence des départements de nouvelles thématiques. Celle-ci est une thématique d'avenir, qui devient absolument indispensable. Des mutualisations sont possibles à l'échelle des départements, qui ont aussi des compétences en matière de SDIS. Nous devons sensibiliser nos partenaires des associations d'élus à ce sujet. Il s'agit d'un beau défi pour les départements qui feront preuve d'une capacité à être entreprenants et à protéger leur population.

Mme Anne-Catherine Loisier. – Le sujet des RSSI a beaucoup été soulevé. Il s'agit effectivement d'un élément important dans la montée en compétence sur les territoires. Ce RSSI doit effectivement avoir un accès direct à l'exécutif, via un élu décisionnaire et différents chefs de service. En

effet, la sécurité numérique se diffuse dans tous les services. L'organigramme qui est mis en place dans la collectivité est déterminant pour l'efficacité et la solidité du dispositif numérique.

Sur le volet de la compétence numérique, nous ne devons pas brider les initiatives émergentes, mais prendre conscience que le numérique suppose une acquisition d'équipements, des mises à jour permanentes et des questions essentielles de cybersécurité, d'où l'intérêt de mutualisations et d'une gestion à l'échelle d'un département, qui semble être la maille adaptée.

Mme Françoise Gatel, présidente. – Je vous remercie pour la clarté de votre propos et les solutions que vous proposez. Nous devons nous en emparer au niveau national. Nous disposons d'un outil rapide et efficace permettant d'endiguer des catastrophes.

M. Antoine Lefèvre, vice-président. – Lors de la COP21, nous avions évoqué un certain nombre d'outils et de technologies, notamment dans le domaine numérique. Nous avions parlé de toutes les applications en matière de sécurité et de protection des populations. Tous ces outils sont aujourd'hui efficaces pour tous les territoires. Ils n'apparaissent plus comme de simples gadgets, notamment grâce aux évolutions technologiques et à l'abaissement du coût de ces matériels. Les agents comme les élus ont en outre une appétence à ces nouvelles technologies. Ce rapport a pour intérêt de s'inscrire dans la pédagogie et la logique d'un guide de bonnes pratiques. Il présente des réponses très concrètes à des problématiques propres aux territoires. Nous devons alerter les élus et les agents des collectivités quant aux problèmes de risques, en termes de sécurisation. Le titre, « Les élus, inventeurs de solutions », nous importait de ce point de vue.

Mme Anne-Catherine Loisier. – Je souhaitais souligner une expérience qui m'a frappée et illustre les progrès technologiques permanents. Le témoignage que nous avons reçu sur l'usage des drones en montagne m'a permis de découvrir que les drones pouvaient transporter un certain nombre d'objets, par exemple pour des soins.

M. Jean-Yves Roux. – Nous envoyons actuellement beaucoup de secouristes en territoires de montagne, lors d'avalanches. Il sera désormais possible d'envoyer un drone qui repèrera le lieu de l'avalanche, ce que l'humain faisait auparavant. Nous protégeons ainsi les secouristes et les intervenants dans des situations très difficiles. Dans la région Provence-Alpes-Côte d'Azur, nos sapeurs-pompiers ne peuvent malheureusement pas intervenir sur certains sites. Peut-être les drones pourraient-ils éteindre des petits feux non accessibles par les sapeurs-pompiers.

Mme Françoise Gatel, présidente. – Le numérique peut être un outil extraordinaire pour des territoires qui ne sont pas urbains. Un drone n'est pas qu'un outil de surveillance, mais aussi de livraison. Nous avons vu certains pays mettre en place des livraisons de médicaments par drone dans des zones éloignées.

Merci encore pour ce sujet majeur. Je vous invite à faire connaître à vos collègues l'existence de ce rapport, voire à la diffuser auprès des associations d'élus locaux, qui peuvent à leur tour inviter des sénateurs à venir échanger sur ces sujets. Ce rapport est très pédagogique et nous avons la capacité de contribuer au développement de ces sujets. Nous mobiliserons nos contacts pour rencontrer les élus porteurs de ces sujets. Cela démontrera que le Sénat est inventeur de solutions.

M. Bernard Buis. – Merci pour ce rapport très intéressant. L'utilisation du drone peut effectivement être un atout important sur nos collectivités. Nous observons actuellement une importance notable dans la protection de la population suivant les collectivités. Le drone peut être une solution pour les inondations, les incendies, les tsunamis, les tremblements de terre ou encore les éruptions volcaniques. Nos collectivités doivent s'approprier cette nouvelle technologie quand elles en ont les moyens. Ces solutions peuvent être relativement peu coûteuses, par rapport à des solutions plus lourdes.

Mme Françoise Gatel, présidente. – Merci beaucoup. Merci encore d'avoir proposé ce sujet, qui avait déjà été travaillé par la délégation en 2017 mais reste un sujet du présent et d'avenir.

Nous avons lancé une mission conjointe de contrôle qui sera présidée par Rémi Pointereau, premier vice-président de la délégation, très attaché au sujet de la revitalisation des centres villes et centres bourgs. Il sera en binôme avec Sonia de La Provôté pour notre délégation. Ce travail se fait en coordination avec la délégation aux entreprises. Le 3 février, à 9 heures 45, une réunion conjointe avec la délégation aux entreprises sera l'occasion de lancer ce sujet, qui est au cœur des préoccupations de la délégation. Je remercie Rémi Pointereau de sa ténacité et sa constance.

Je vous souhaite une très bonne journée. Merci à nos trois rapporteurs.

LISTE DES PERSONNES AUDITIONNÉES

Mardi 19 octobre 2021

Hélène Martin, adjointe au sous-directeur de la direction générale des collectivités locales (DGCL), ministère de la Cohésion des territoires et des Relations avec les collectivités territoriales,

Karine Delamarche, sous-directrice des compétences et des institutions locales de la direction générale des collectivités locales (DGCL),

Émilie Vouillemet, cheffe du bureau du contrôle de légalité et du conseil juridique de la direction générale des collectivités locales (DGCL),

Claire Gonzague, adjointe de la cheffe du bureau du contrôle de légalité et du conseil juridique de la direction générale des collectivités locales (DGCL),

Taline Aprikian, cheffe du bureau des services publics locaux de la direction générale des collectivités locales (DGCL)

Mardi 26 octobre 2021

Cyril Cotonat, président, association des maires ruraux du Gers, association des maires ruraux de France (AMRF),

Céline Vincent, chargée du numérique, association des maires ruraux de France (AMRF)

Mardi 9 novembre 2021

Yves Le Breton, Directeur Général, agence nationale de la cohésion des territoires (ANCT),

Stéphanie Maringe, conseillère chargé des relations institutionnelles, agence nationale de la cohésion des territoires (ANCT)

Mercredi 10 novembre 2021

Valérie Nouvel, vice-présidente de la Manche, assemblée des départements de France (ADF)

Mercredi 24 novembre 2021

- Table ronde « risque inondation »

Patrick Campabadal, adjoint au maire chargé de la prévention des risques, mairie de Sommières,

Nathalie Tardieu, directrice générale des services, mairie de Sommières,

Michèle Lelou, chargée de la mise à jour et du suivi du plan communal de sauvegarde, mairie de Sommières

Marie-France Beaufils, présidente, centre Européen pour la Prévention du Risque Inondation (CEPRI),

Rodolphe Pannier, chargé de mission, centre Européen pour la Prévention du Risque Inondation (CEPRI)

Guillaume Delai, PDG, société Ogoxe

- Audition « risque sismique »

Gilles Dawidowicz, responsable des offres Google Maps, Google France,

Floriane Fay, responsable des relations institutionnelles et politiques publiques, Google France

Mercredi 8 décembre 2021

- Audition « expérience alpine »

Olivier Gardet, directeur technique de la régie des pistes de la vallée des Belleville, commune des Belleville (Val thorens)

Benjamin BLANC, directeur général de la patrouille de ski, commune des Belleville (Val Thorens)

- Audition « ordre public »

François Bernardini, maire d'Istres,

Alain Aragneau, 4ème adjoint au maire d'Istres, délégué à la sécurité publique et civile

Mardi 14 décembre 2021

- Table ronde « risque incendie »

Commandant Éric RODRIGUEZ, chef de groupement « volontariat » (engagement citoyen), conseiller technique, service départemental d'incendie et de secours (SDIS) 13

Murielle Auneau, directrice de l'urbanisme, foncier, accessibilité et gestion des risques, mairie d'Ajaccio,

Landine Salini, collaboratrice de la directrice de l'urbanisme, foncier, accessibilité et gestion des risques, mairie d'Ajaccio,

Laurent Leca, directeur général adjoint en charge du pôle Ressources et Moyens, communauté d'agglomération du pays ajaccien,

Michel Mattei, directeur des systèmes d'informations et du numérique, communauté d'agglomération du pays ajaccien,

Pascal Peraldi, expert de la direction des systèmes d'informations et du numérique, communauté d'agglomération du pays ajaccien

- Audition financement projets

Emmanuel Passily, responsable d'investissements « villes et territoires intelligents », Caisse des Dépôts et Consignations

Jeudi 6 janvier 2022

- Audition du Ministère de l'Intérieur

Yves Hocdé, sous-directeur de la préparation, de l'anticipation et de la gestion des crises

Hélène Halbrecq, adjointe au chef du bureau de l'alerte et de la sensibilisation et de l'éducation des populations

Michel Monneret, Directeur, Agence nationale de la sécurité civile

- Audition d'ATOS

Philippe Bouchet, Directeur Collectivités

Thierry Siouffi, VP groupe en charge du secteur

LISTE DES CONTRIBUTIONS ÉCRITES

- Guillaume PLA, chef de projet « prévision des inondations » à la mairie de Nîmes
- Ministère de l'environnement - Direction générale de la prévention des risques
- Société « voisinsvigilants.org »
- Association « Villes de France »
- Association des Directeurs Généraux des Communautés de France (ADGCF)