N° 595

SÉNAT

SESSION ORDINAIRE DE 2016-2017

Enregistré à la Présidence du Sénat le 28 juin 2017

RAPPORT D´INFORMATION

FAIT

au nom de la commission des finances (1) sur le **système** *d'***alerte** *et d'***information** *des* **populations** (**SAIP**),

Par M. Jean Pierre VOGEL,

Sénateur

(1) Cette commission est composée de : Mme Michèle André, *présidente ;* M. Albéric de Montgolfier, *rapporteur général ;* Mme Marie-France Beaufils, MM. Yvon Collin, Vincent Delahaye, Mmes Fabienne Keller, Marie-Hélène Des Esgaulx, MM. André Gattolin, Charles Guené, Francis Delattre, Georges Patient, Richard Yung, *vice-présidents ;* MM. Michel Berson, Philippe Dallier, Dominique de Legge, François Marc, *secrétaires ;* MM. Philippe Adnot, François Baroin, Éric Bocquet, Yannick Botrel, Jean-Claude Boulard, Michel Canevet, Vincent Capo-Canellas, Thierry Carcenac, Jacques Chiron, Serge Dassault, Bernard Delcros, Éric Doligé, Philippe Dominati, Vincent Éblé, Thierry Foucaud, Jacques Genest, Didier Guillaume, Alain Houpert, Jean-François Husson, Roger Karoutchi, Bernard Lalande, Marc Laménie, Nuihau Laurey, Antoine Lefèvre, Gérard Longuet, Hervé Marseille, Claude Nougein, François Patriat, Daniel Raoul, Claude Raynal, Jean-Claude Requier, Maurice Vincent, Jean Pierre Vogel.

S O M M A I R E

Pages

LES PRINCIPALES OBSERVATIONS ET RECOMMANDATIONS DU RAPPORTEUR SPÉCIAL

Les principales observations

- Le choix de remplacer le Réseau national d'alerte, vieillissant et principalement conçu pour répondre au risque d'attaque aérienne, par un nouveau système d'alerte et d'information adapté aux risques contemporains était pleinement justifié ;

- Le système d'alerte et d'information des populations (SAIP) vise à permettre aux acteurs de la gestion de crise de lancer l'alerte par une unique opération sur différents vecteurs (sirènes, téléphonie mobile, et autres moyens : par exemple Radio France, France Télévisions, panneaux à message variable des gestionnaires d'infrastructures et des collectivités territoriales) dans une zone géographique donnée. À l'heure actuelle, toutefois, seules les sirènes sont connectées au SAIP ;

- Ce projet est marqué par des choix stratégiques contestables. Le choix de conserver les sirènes comme principal vecteur de l'alerte, alors même que leur pertinence n'a pas fait l'objet d'une réelle évaluation n'apparaît pas opportun, tant la nature des risques et les vecteurs disponibles ont changé. Le volet « sirènes » concentre la quasi-totalité des crédits du SAIP, alors même que leur impact est désormais moindre que celui de l'alerte et de l'information par téléphonie mobile ;

- La mise en œuvre du volet « sirènes » est marquée par un retard de 36 mois dans la livraison du logiciel central de commande, qui aurait pu être en partie évité si le besoin avait été mieux spécifié (dans le cahier des charges). Si ce logiciel constitue en principe un atout important, l'absence de connexion prévue à court terme avec les autres moyens d'alerte en relativise l'intérêt ;

- S'agissant du volet « mobile », l'abandon de la technologie *Cell Broadcast*, initialement envisagée, au profit d'une application *smartphone* pour des raisons budgétaires et d'absence de volonté des opérateurs, est regrettable. Cette décision découle directement du choix contestable de privilégier le volet « sirènes » plutôt que le volet « mobile » ;

- La conception de l'application *smartphone*, tant dans la dimension technique que dans la gestion du projet, a été menée dans un délai trop contraint eu égard à sa complexité, alors même qu'une plus grande anticipation aurait été possible puisque la téléphonie mobile était envisagée comme un possible vecteur de l'alerte depuis 2011 ;

- Des défaillances nuisant à la fiabilité et à l'ergonomie de l'application subsistent encore aujourd'hui.

Les principales recommandations

Recommandation n° 1 : afin de favoriser le développement d'autres moyens d'alerte (*smartphones*, médias, etc.) et pour en améliorer la diffusion, renoncer à la doctrine faisant des sirènes le « vecteur principal » de diffusion de l'alerte.

Recommandation n° 2 : rééquilibrer les crédits de la phase 2, en renforçant le financement du volet « mobile » pour garantir la mise en place soit d'une application *smartphone* pleinement efficace (scénario 2) soit le recours au *Cell Broadcast* (scénario 1).

Recommandation n° 3 : pour permettre au ministère de l'intérieur de faire face aux projets informatiques d'envergure, prévoir une procédure exigeant la formulation d'un cahier des charges précis élaboré en amont de la notification du marché et un éventuel appui de la direction interministérielle du numérique et du système d'information et de communication de l'État (DINSIC), lorsque la complexité le commande, même si le coût du projet est inférieur au seuil réglementaire.

Recommandation n° 4 : effectuer, d'ici 2019, une évaluation de l'application SAIP, afin de déterminer sa pertinence en comparaison du *Cell Broadcast*, et réajuster le déploiement de la phase 2 en conséquence, afin de garantir la fiabilité et l'efficacité de l'alerte par téléphonie mobile.

→ Scénario 1 : en cas d'abandon, à la suite de cette évaluation, de l'application *smartphone* comme vecteur principal de l'alerte par téléphonie mobile, assurer son remplacement par la technologie *Cell Broadcast*, en lien avec les opérateurs, dans le courant des années 2020 et 2021.

→ Scénario 2 : en cas de confirmation du principe de l'application comme principal vecteur de l'alerte par téléphone mobile, fiabiliser l'application SAIP et poursuivre la publicité en sa faveur afin d'augmenter le nombre de téléchargements en vue d'atteindre une masse critique permettant d'en faire un vecteur efficace de l'alerte (objectif de 5 millions de téléchargements fin 2020).

Recommandation n° 5 : corriger en urgence les principales défaillances persistantes de l'application SAIP qui nuisent à sa fiabilité et à son ergonomie, comme les géolocalisations inopinées, la consommation excessive de batterie et, surtout, la nécessité de conserver l'application ouverte en tâche de fond.

Recommandation n° 6 : modifier la doctrine d'emploi de l'application afin d'y relayer, même lorsqu'ils semblent maîtrisés, l'ensemble des évènements pouvant mettre en cause la sécurité des personnes sur un territoire, afin notamment d'éviter une désaffection de la part du public pour ce dispositif.

PREMIÈRE PARTIE
LE SAIP : UNE MODERNISATION DU SYSTÈME D'INFORMATION ET D'ALERTE FRANÇAIS JUSTIFIÉE, QUOIQUE MARQUÉE PAR DES CHOIX STRATÉGIQUES CONTESTABLES

I. LA MISE EN PLACE D'UN NOUVEAU SYSTÈME D'ALERTE : UNE ÉVOLUTION INDISPENSABLE POUR RÉPONDRE À L'OBSOLESCENCE DU RÉSEAU NATIONAL D'ALERTE (RNA)

A. L'ALERTE ET L'INFORMATION DES POPULATIONS : UNE NÉCESSITÉ FACE AUX RISQUES GRAVES ET IMMÉDIATS

Le système d'alerte et d'information des populations (SAIP), initié en 2009 par le ministère de l'intérieur, est constitué du regroupement **de plusieurs moyens d'alerte et d'information au sens de la sécurité civile**.

Ces deux termes sont en effet entendus dans un sens précis et spécifique au secteur de la sécurité civile. Ils se distinguent donc des alertes « enlèvement », des mesures de vigilance comme les alertes météorologiques établies par Météo France, ou encore des alertes sanitaires.

L'alerte vise ainsi à « *accompagner les populations en temps de crise en leur diffusant des consignes de comportement leur permettant de prendre une part active à leur protection. Elles sont ainsi directement destinées aux populations mises en danger et diffusées par les autorités qui ont connaissance d'un péril et qui sont chargées de prendre les mesures permettant d'y faire face* »[1].

L'alerte, au sens du SAIP, est ainsi :

- **réservée aux événements graves**, c'est-à-dire lorsqu'une atteinte aux personnes est pressentie ;

- **déclenchée pour un événement imminent ou en cours de réalisation** ;

- **véhiculée par un signal facilement identifiable**, visant à appeler l'attention des populations, potentiellement distraites par leurs activités quotidiennes. Le vecteur traditionnel est la **sirène**.

L'information a pour objet de « *diffuser des consignes de comportement de sauvegarde, par anticipation ou concomitamment à un danger susceptible de porter atteinte à l'intégrité physique d'individus* »[2] et de notifier, si nécessaire, la fin de l'alerte.

---

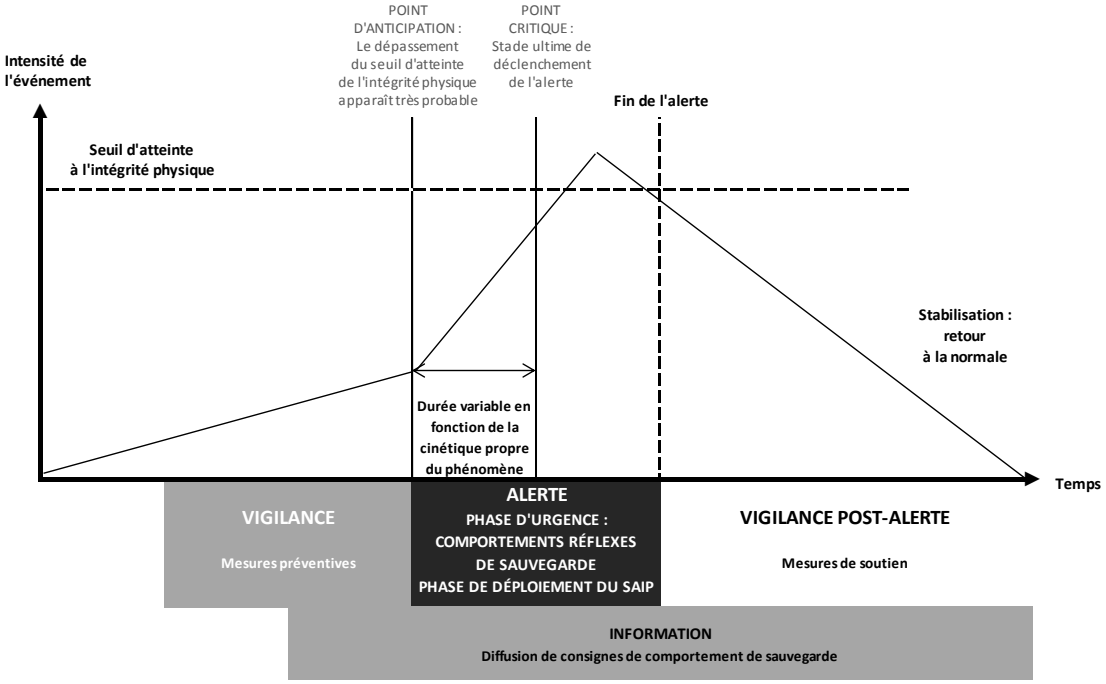
[1] *Guide ORSEC, Alerte et information des populations, juin 2013.*
[2] *Ibid.*

Le SAIP (système d'alerte et d'information des populations) se cantonne ainsi, dans son principe, à deux objectifs : alerter la population en visant un comportement réflexe et l'informer sur la conduite à tenir pendant la durée de l'alerte.

Ces mesures doivent être distinguées de la vigilance, antérieure à la crise, ou encore de la communication. Dans le domaine de la sécurité civile, la communication vise à relater les événements ou à présenter les mesures prises par les autorités pour en limiter les effets, c'est-à-dire à relayer des messages destinés à des populations le plus souvent spectatrices des événements, sans que leur finalité soit de les faire participer à leur propre sécurité.

Les mesures de sensibilisation aux risques (par exemple en milieu scolaire), quoiqu'indispensables et complémentaires à l'alerte, car conditionnant les comportements réflexes, ne sont pas davantage incluses dans le champ du SAIP et du présent rapport.

Chronologie de la diffusion de l'alerte et de l'information des populations en situation de crise



Source : commission des finances du Sénat, d'après le guide ORSEC 2013

Le SAIP vise ainsi à propager l'alerte et à véhiculer l'information pertinente en cas de réalisation de risques qui le justifient. Il porte donc principalement sur des risques à cinétique rapide, tels que les explosions et leurs éventuelles conséquences (nuages toxiques, projection de débris, etc.), les intempéries soudaines, les prises d'otage ou encore les attaques

terroristes. À l'inverse, les risques à cinétique lente, comme les crues de la Seine, ne justifient pas son activation.

B. UN RÉSEAU DE SIRÈNES DEVENU TOTALEMENT OBSOLÈTE

Le système d'alerte et d'information des populations succède au réseau national d'alerte (RNA), dont l'obsolescence a été mise en évidence par le rapport « Hirel », remis en novembre 2002[1].

La RNA a été institué après la seconde guerre mondiale par le service de la protection civile pour répondre à des risques de nature militaire. L'arrêté du 9 février 1954, qui porte création de ce réseau, n'envisageait que les bombardements comme motif de déclenchement. L'arrêté du 8 mai 1973 a, par la suite, élargi les hypothèses d'utilisation aux risques nucléaires, bactériologiques et chimiques (NBC).

Il était, dans les années 2000, constitué d'environ 4 500 sirènes et 48 sites de déclenchement, interconnectés par des liaisons filaires, situés sur 6 bureaux généraux de l'alerte (centres de détection et de commandement de l'armée de l'air) et 42 bureaux de diffusion et de l'alerte (implantés dans les locaux des préfectures).

La technologie de ce réseau était analogique, et les équipements (armoires de commande et meubles de déclenchement des sirènes) répondaient aux normes électriques de l'époque. **Votre rapporteur spécial a constaté par lui-même la vétusté de ces armoires de commande, ainsi que les éventuels risques d'incendie qu'ils impliquaient.**

Le rapport « Hirel » relevait que, n'ayant été que maintenu à niveau, **le RNA avait incontestablement vieilli, tandis que le risque auquel avait répondu son institution s'était fortement atténué suite à l'effondrement du bloc soviétique. Par ailleurs, les évolutions de la démographie et de la nature des risques ont également rendu la localisation des sirènes obsolète.**

En outre, plusieurs limites à son maintien demeuraient :

- sa doctrine d'emploi restait imprécise car le décret[2] qui en dressait les contours demeurait largement inappliqué ;

- faute de granularité suffisante, le RNA ne pouvait être utilisé à l'occasion d'une menace ou de la réalisation d'un risque affectant une zone géographique bien précise (logique du « tout ou rien ») ;

---

[1] *Rapport sur le réseau national d'alerte de l'inspection générale de l'administration, l'inspection générale des finances, le conseil général des technologies de l'information, le contrôle général des armées et l'inspection générale de l'environnement, novembre 2002.*

[2] *Décret n° 90-394 du 11 mai 1994 relatif au code national de l'alerte.*

- malgré les efforts indéniables de remise en état des sirènes, leur état de fonctionnement variait sensiblement d'un département à l'autre (impossibilité de déclencher les sirènes à distance lors des essais des premiers mercredis du mois, déclenchements intempestifs, usage en mode dégradé ou réseau inutilisable laissé à l'abandon...). En Corse, par exemple, les essais du premier mercredi du mois n'avaient même plus lieu faute d'installations satisfaisantes. Par ailleurs, à la suite de sa transformation en société privée, France Telecom, qui avait initialement la responsabilité de l'entretien du réseau, a interrompu toute prestation sur le RNA en 2011, faute d'indemnisation de la part du ministère de l'intérieur.

Au total, **le RNA devenait coûteux[1] à maintenir en état de fonctionnement, sans que son intérêt opérationnel ne soit établi.** Le rapport « Hirel » relève d'ailleurs qu'il n'avait jamais fait l'objet d'une utilisation en un demi-siècle, en dehors des essais des premiers mercredis du mois. Par ailleurs, s'agissant des catastrophes naturelles les plus récentes, des sirènes existaient (comme lors de la tempête Xynthia[2] ou des inondations dans les Alpes-Maritimes en octobre 2015), mais en nombre insuffisant et n'ont pas été déclenchées.

Partant de ces observations, le *Livre blanc sur la défense et la sécurité nationale* de 2008 a fixé comme objectif la mise en place d'un « *nouveau système d'alerte des populations, conçu sur le plan national et sur la base d'une approche centrée sur les bassins de risques* ». Ce dernier devait faire partie des six grands chantiers identifiés pour la sécurité civile[3]. Il prévoit notamment que le nouveau réseau « *doit être entièrement modernisé, pour utiliser au mieux la diversité des supports aujourd'hui possibles : sirènes, SMS, courriels, panneaux d'affichage public dans les villes, gares, aéroports, réseaux routier et autoroutier. Les potentialités du réseau Internet doivent également être exploitées* »[4].

Observation : le choix de remplacer le RNA, vieillissant, par un nouveau système d'alerte était pleinement justifié.

[1] *Le rapport « Hirel » évoque un coût annuel d'environ 70 millions de francs en 2000 et 2001.*
[2] *Cour des comptes, Tempête Xynthia : retour d'expérience, évaluation et propositions d'action, 2010.*
[3] *Livre blanc pour la défense et la sécurité civile, p. 232.*
[4] *Ibid. p. 188-189.*

C. LE SAIP : UN PROJET DESTINÉ À REMPLACER PLEINEMENT LE RNA

1. Un projet visant à permettre le déclenchement de l'ensemble des moyens d'alerte pertinents sur une plate-forme unique

Le SAIP vise à permettre aux acteurs de la gestion de crise de lancer l'alerte en une unique opération sur différents vecteurs (sirènes, téléphonie mobile, et autres moyens : Radio France, France Télévisions, panneaux à message variable des gestionnaires d'infrastructures et des collectivités territoriales...) dans une zone géographique donnée.

Une expérimentation, menée le 18 juin 2009 dans trois départements de la zone de défense Sud-Est (Ain, Allier et Rhône), mobilisant 300 personnes (sapeurs-pompiers, techniciens, réservistes du RNA, employés communaux) avait permis de **confirmer la faisabilité de la solution technique envisagée en remplacement du RNA : un cœur de dispositif constitué par un logiciel, pilotant un réseau de sirènes, et diffusant des messages d'alerte ou d'information sur un ensemble d'autres moyens d'alerte (les panneaux à message variable, notamment).**

Afin de limiter le coût du **volet « sirènes »**, qui devait demeurer, conformément au rapport « Hirel », le moyen d'alerte « numéro un »[1], il a été décidé de s'appuyer en partie sur les sirènes existantes. Le SAIP repose ainsi, en plus de nouvelles sirènes sur le raccordement des sirènes du RNA, des sirènes des collectivités locales, et des sirènes des industriels soumis à obligation de disposer d'un plan particulier d'intervention dont la localisation géographique est jugée pertinente par les préfectures et la direction générale de la sécurité civile et de la gestion des crises. Un travail de recensement des bassins à risque effectué en 2010 a abouti à l'identification de 1 743 bassins d'alerte, à couvrir par 5 338 sirènes à raccorder ou installer.

Le second volet du SAIP devait initialement reposer sur une solution technique permettant la diffusion, en toutes circonstances, de SMS d'alerte et d'information, en liaison avec les opérateurs de téléphonie mobile. Il a été remplacé, en 2015, et dans la perspective de l'« Euro 2016 », par le développement d'une application *smartphone* en libre téléchargement sur l'*Apple Store* et sur *Google Play*.

Enfin, il devait reposer sur des partenariats nationaux et locaux permettant aux différents médias de relayer les messages transmis par le cœur du SAIP[2].

---

[1] *Rapport sur le réseau national d'alerte, p. 31.*

[2] *Conformément à l'article R. 732-28 du code de la sécurité intérieure, les services de radiodiffusion sonore et de télévision diffusent à titre gracieux les consignes de sécurité, à la demande des autorités.*

Le partenariat du ministère de l'intérieur avec les médias en matière d'alerte

Le ministère de l'intérieur a signé, en 2006, une convention de partenariat avec France Télévisions renouvelée en date du 3 septembre 2009, et actuellement en cours de renégociation. Celle-ci avait été déclinée par des conventions conclues avec France 2, France 3 et Réseau France Outre-mer (RFO).

La convention nationale de 2004 conclue avec Radio France a quant à elle été renouvelée le 16 juillet 2015. Elle est accompagnée de messages préformatés comprenant les consignes de sauvegarde pour treize types de risques différents. Les modules sonores prescrivant les comportements adaptés ont été enregistrés et mis à disposition de l'ensemble des stations émettrices de Radio France.

La pratique a révélé que les réseaux France Bleu et France Info étaient les mieux armés pour répondre à la diffusion de l'alerte par leur granularité optimale et la participation des équipes aux exercices. L'efficacité et la souplesse du dispositif ont permis la mise en œuvre d'une ligne spécialisée de transmission des messages via le centre opérationnel de gestion interministérielle des crises (COGIC). Il a donc été décidé de décliner localement la convention dans chaque département. Cela permet d'identifier les acteurs de diffusion de l'alerte dans les territoires et d'entretenir une mise à jour permanente des contacts entre préfectures et stations de diffusions.

Source : DGSCGC

Au total, le SAIP devait être constitué :

- d'un réseau de sirènes, interconnectées et déclenchables à distance, via l'infrastructure nationale partageable de télécommunication (réseau Antares[1]) afin de garantir un niveau de sécurisation satisfaisant ;

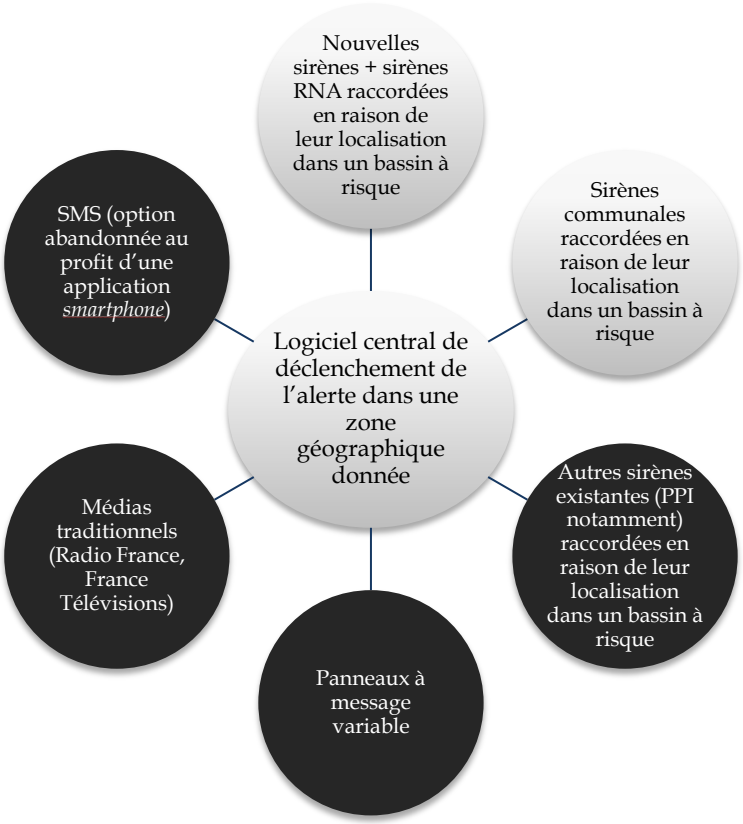
- d'une fonctionnalité permettant l'envoi de messages sous forme de SMS sur les téléphones mobiles des populations ;

- d'une fonctionnalité permettant aux acteurs disposant de moyens d'alerte et d'information de relayer l'alerte (automates d'appels des collectivités locales, panneaux à message variable de gestionnaires d'infrastructures de transport et de collectivités locales, médias partenaires…).

L'ensemble de ces vecteurs d'alerte et d'information devait pouvoir être activé depuis un logiciel pilote.

[1] *Rapport d'information de M. Jean Pierre Vogel, fait au nom de la commission des finances, n° 365 (2015-2016) - 3 février 2016.*

Architecture technique initiale du projet SAIP



Note de lecture : Les parties noircies correspondent aux volets dont la mise en œuvre n'a pas commencé.

Source : commission des finances du Sénat

La direction générale de la sécurité civile et de la gestion des crises indique que le SAIP devrait s'appuyer sur la norme « CAP », qui « *permettra de garantir la multidiffusion, sécurisée et sourcée, des messages d'alerte, en dehors de l'administration* (*site Internet spécialisé sur l'alerte et l'information des populations, médias, médias sociaux, opérateurs d'applications informatiques proposant des fonctionnalités de géolocalisation sur leurs produits…) sous des modalités, techniques et juridiques, qui restent à préciser* ». À l'heure actuelle, toutefois, seul le volet « sirènes » est en cours de raccordement au logiciel central.

2. Un système d'alerte national déclenché par l'État, en complément des dispositifs communaux

Le projet SAIP s'inscrit dans un cadre juridique et organisationnel largement inchangé, dans lequel l'alerte et l'information des populations demeure principalement une responsabilité de l'État[1].

Cette responsabilité est toutefois partagée avec les maires, qui exercent des missions de sécurité civile dans le cadre de leurs pouvoirs de police administrative générale[2]. La jurisprudence administrative a précisé qu'il incombait au maire, au titre de ces pouvoirs de police, de préparer les situations de crise susceptibles de se présenter sur le territoire de sa commune, et notamment de mettre en œuvre les mesures d'alerte et d'information des populations (Conseil d'État, 22 juin 1987, *Ville de Rennes*).

Les préfets de département interviennent en cas d'accident, sinistre ou catastrophe dont les conséquences peuvent dépasser les limites ou les capacités d'une commune[3], en cas de carence du maire (pouvoir de substitution du préfet), ou en cas d'événement de vaste ampleur qui justifie à ses yeux qu'il prenne la direction des opérations de secours.

Concrètement, les préfectures pourront, en tant qu'autorités chargées du déclenchement, permettre aux SDIS d'accéder à la plate-forme d'activation du SAIP en leurs noms[4] par le biais d'une convention. La première a été signée en juin 2017 dans l'Hérault.

L'application *smartphone* SAIP ne peut, quant à elle, être déclenchée que depuis le centre opérationnel de gestion interministérielle des crises (COGIC). Des procédures sont mises en place pour permettre aux préfectures de saisir ce dernier rapidement et donner l'ordre du déclenchement.

Pour les communes, le SAIP ne constitue pas, en tout état de cause, le vecteur exclusif de l'alerte, chaque commune étant libre de retenir d'autres moyens d'alerte et d'information des populations en complément de ce dispositif. Elles peuvent notamment disposer de sirènes communales (dont certaines ont également été raccordées au SAIP), de panneaux à messages variables, ou de moyens plus artisanaux (mégaphones, etc.) puisqu'elles ne sont soumises qu'à une obligation de résultat et non de moyen.

---

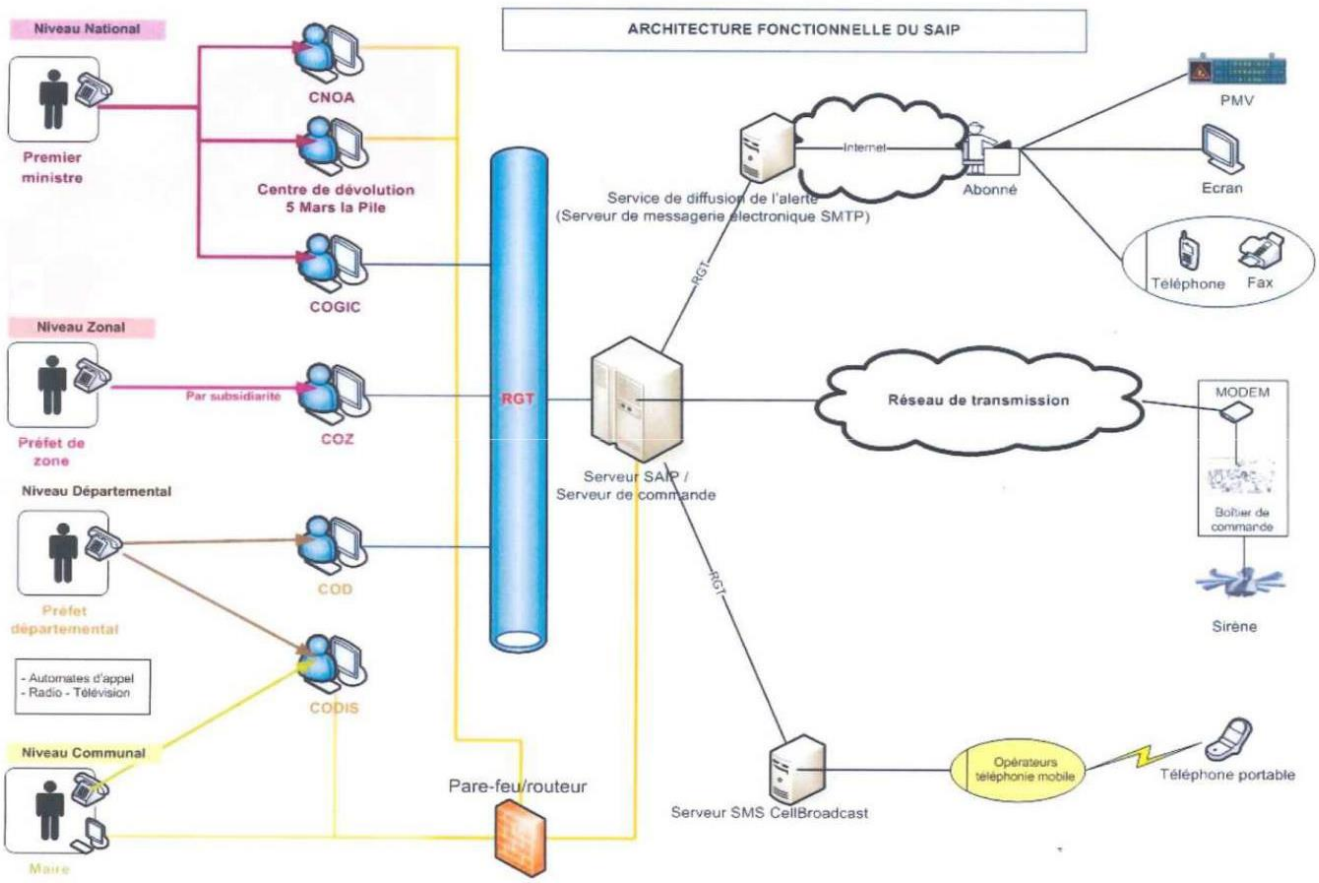
[1] *Selon l'article L. 112-2 du code de la sécurité intérieure,* « l'État est garant de la cohérence de la sécurité civile au plan national […] Il veille à la mise en œuvre des mesures d'information et d'alerte des populations ».

[2] *Article L. 2212-2, 5° du code général des collectivités territoriales.*

[3] *Articles L. 747-2 et L. 742-3 du code général des collectivités territoriales.*

[4] *Arrêté du 28 janvier 2014 relatif à l'utilisation du système d'alerte et d'information des populations par les services départementaux d'incendie et de secours.*

Architecture fonctionnelle du SAIP



Source : ministère de l'intérieur

II. UN CHOIX PEU PERTINENT : RÉNOVER LES SIRÈNES PLUTÔT QUE DE PRIVILÉGIER LES TÉLÉPHONES MOBILES COMME PRINCIPAUX VECTEURS DE L'ALERTE

A. UN FINANCEMENT EN DEUX PHASES, DEVANT ATTEINDRE 81 MILLIONS D'EUROS

Le coût du projet SAIP a été estimé initialement à 78 millions d'euros, divisé en deux phases. La première court de 2012 à 2019, tandis que la seconde, dont la durée reste à définir, débutera en 2020.

La loi n° 2011-267 du 14 mars 2011, d'orientation et de programmation pour la performance de sécurité intérieure a affecté au projet dans un premier temps une enveloppe de 44,7 millions d'euros d'autorisations d'engagement, devant être complétée par une seconde vague ultérieure. Son financement dépend de l'action « Prévention et gestion de crises » du programme « Sécurité civile » de la mission « Sécurités ».

Calendrier prévisionnel du financement de la première vague du SAIP

(en millions d'euros)

	Prévision		Exécution		Taux de consommation	
	AE	**CP**	**AE**	**CP**	**AE**	**CP**
2012	5,4	0,9	5,3	0,9	99,6%	100,0%
2013	6,6	4,2	6,8	3,9	98,3%	93,6%
2014	6,9	4,7	7,4	3,6	103,9%	77,7%
2015	8,7	8,7	8,5	8,04	92,2%	92,4%
2016	8	7,7	6,1	7,1	75,9%	92,6%
2017	9	7	8,1	7,8	99,7%	112,6%
2018	0	7				
2019	0	4,4				
Total	**44,7**	**44,7**	**42,1**	**31,5**		

Source : commission des finances du Sénat, d'après la DGSCGC et les documents budgétaires

En 2017, l'enveloppe nécessaire au projet a été revue à 81,5 millions d'euros[1], impliquant un dépassement de 4,5 % du montant initial.

Pour finaliser le déploiement, 33 millions d'euros seront nécessaires à partir de 2018, pour financer principalement la poursuite de l'installation des sirènes sur le territoire et « renforcer » le volet « mobile ». Les crédits de la deuxième phase seront, selon les informations transmises par la direction générale de la sécurité civile et de la gestion des crises, également largement dédiés au volet « sirènes », même si ce second volait devrait également prévoir le raccordement effectif d'autres moyens d'alerte.

[1] *Projet annuel de performances de la mission « Sécurités » annexé au projet de loi de finances pour 2017.*

Exécution des crédits de la première phase du déploiement du SAIP

(en millions d'euros)

	2009-2011		2012		2013		2014		2015		2016		(prévisionnel)		Total par actions	
	AE	**CP**	**AE**	**CP**	**AE**	**CP**	**AE**	**CP**	**AE**	**CP**	**AE**	**CP**	**AE**	**CP**	**AE**	**CP**
Études opérationnelles (marché relatif à l'assistance technique organisationnelle, financière et juridique pour l'élaboration, la passation et l'exécution du futur marché SAIP)	2,08	1,66	0,00	0,28	0,00	0,14									**2,08**	**2,08**
Logiciel pilote			2,43	0,00	0,00	0,00	0,00		0,31	1,53	0,01	0,32	0,91	0,57	**3,66**	**2,42**
Études liées au logiciel (audits, prestations SSI…)							0,11	0,11	0,00	0,00	0,08	0,08	0,04	0,04	**0,23**	**0,23**
Déploiement des sirènes			2,95	0,70	6,49	3,79	7,07	3,55	7,22	6,26	4,99	5,78	6,40	5,43	**35,12**	**25,52**
Volet mobile											0,56	0,31	1,22	1,47	**1,78**	**1,78**
Dépenses de fonctionnement (prestations en T3)									0,50	0,25	0,44	0,63	0,39	0,37	**1,33**	**1,25**
Total	**2,08**	**1,66**	**5,38**	**0,98**	**6,49**	**3,93**	**7,17**	**3,65**	**8,02**	**8,04**	**6,07**	**7,13**	**8,97**	**7,88**	**44,19**	**33,27**

Source : DGSCGC, données transmises en juin 2017

B. UN FINANCEMENT PRINCIPALEMENT DÉDIÉ AU VOLET « SIRÈNES », DONT L'INTÉRÊT OPÉRATIONNEL APPARAÎT POURTANT LIMITÉ

1. Les sirènes : vecteur traditionnel de l'alerte dont la primauté est contestable

Les sirènes, avec les cloches des églises, sont, en France, le vecteur historique de diffusion de l'alerte à la population. Sa primauté est aujourd'hui largement consacrée, la direction générale de la sécurité civile et de la gestion des crises estimant qu'elle constitue « *le principal vecteur de l'alerte* ».

En 2002, le rapport « Hirel » établissait ainsi qu' « *un réseau dense de sirènes rest*[ait] *le moyen le plus approprié pour prévenir, à tout moment et dans les meilleurs délais, le maximum de populations de l'occurrence d'un événement grave. Les technologies nouvelles permettant d'obtenir une grande fiabilité, d'adapter la granulométrie du système en fonction des bassins de risque et d'inscrire le système dans une véritable chaîne de commandement* »[1].

Il précisait que les sirènes présentaient principalement trois séries d'avantages :

- elles sont faciles à mettre en œuvre ;

- une grande partie de la population est susceptible de les entendre, la quasi-totalité en zone urbaine, une proportion notable en zone rurale ;

- elles peuvent délivrer un message clair (« confinez-vous et allumez telle radio ou telle chaîne de télévision »).

Cette analyse doit, aujourd'hui, être largement relativisée.

La sirène en elle-même, qu'elle soit mécanique ou électronique, constitue certes une installation simple et peu onéreuse. Les coûts d'entretien et d'exploitation (de l'ordre de 50 euros d'électricité par an et par sirène, selon les informations recueillies par votre rapporteur) restent faibles. **Les moyens d'activation de la sirène peuvent toutefois être facteurs de complexité.** L'obsolescence du RNA s'expliquait notamment par le vieillissement des liaisons filaires et des équipements de télécommande[2]. S'agissant du SAIP, et dès lors que l'entretien du réseau repose sur Antares, des coûts d'entretien sont également à prévoir. Le chiffrement des boîtiers d'émission-réception, qui assurent la liaison entre le réseau et la sirène, devront par exemple être mis à jour tous les deux ans, impliquant des allers et retours entre les sirènes et les services des préfectures. **En tout état de**

---

[1] *Rapport sur le réseau national d'alerte de l'inspection générale de l'administration, l'inspection générale des finances, le conseil général des technologies de l'information, le contrôle général des armées et l'inspection générale de l'environnement, novembre 2002, p. 41.*

[2] *Ibid, p. 6.*

cause, la relative simplicité d'utilisation de la sirène doit être examinée à l'aune de l'émergence des nouveaux moyens de communications beaucoup plus souples, tels que ceux offerts par la téléphonie mobile.

Par ailleurs, l'efficacité du message délivré doit être largement nuancée. Si la conduite à tenir implicite est de rester chez soi et de se tenir informé (sur les radios et chaînes de télévision publiques), un sondage réalisé sur un échantillon représentatif de 1 000 personnes a en effet montré que seuls 22 % des français savaient comment réagir dans les cas où les sirènes hurlaient[1]. Par ailleurs, un réseau de sirènes n'est efficient que si une véritable politique de communication, sur les risques existants et sur les mesures d'autoprotection adéquates à tenir en cas d'alerte, est convenablement menée.

Le signal des sirènes d'alerte

Le signal national d'alerte, défini par l'arrêté du 23 mars 2007 relatif aux caractéristiques techniques du signal national d'alerte, et consistant en trois cycles successifs d'une durée de 1 minute et 41 secondes chacune et séparés par un intervalle de 5 secondes, prescrit un comportement réflexe de mise en sécurité.

Plus spécifiquement, pour les aménagements hydrauliques, le signal d'alerte, comportant un cycle d'une durée minimum de 2 minutes composé d'émissions sonores de 2 secondes séparées par un intervalle de 3 secondes, prescrit uniquement une évacuation.

Dans les deux cas, le signal continu de 30 secondes annonce la fin d'une alerte. Il peut être diffusé dans les situations de danger clairement identifié dont les effets cessent instantanément.

L'émission du signal national d'essai comporte un cycle unique d'une durée de 1 minute et 41 secondes.

Le signal d'essai des dispositifs d'alerte des aménagements hydrauliques comporte, pour sa part, un cycle d'une durée de 12 secondes composé de trois émissions sonores de 2 secondes séparées par un intervalle de 3 secondes.

Source : Guide ORSEC 2013

Enfin, les sirènes ne constituent pas un moyen approprié d'alerte dans de nombreux cas. Leur efficacité dépend en premier lieu des conditions météorologiques (elles sont inopérantes en cas de forts vents, par exemple) et des lieux et populations concernées par l'alerte (espaces clos, personnes malentendantes ou n'étant pas dans le rayon d'action d'une sirène sont de fait exclues de ce moyen d'alerte). Même des scénarios dans lesquels les sirènes apparaissaient *a priori* comme le moyen d'alerte le plus pertinent, à l'instar des accidents industriels, ont montré que les sirènes n'étaient pas nécessairement adaptées. Ainsi, lors de l'explosion de l'usine AZF de

[1] *Sondage IFOP,* Que faire si les sirènes hurlent ?*, 2013.*

Toulouse le 21 septembre 2001, le bruit de l'explosion a suffi à alerter les populations avoisinantes. Dans ce cas, l'utilisation de moyens d'alerte pouvant également véhiculer de l'information aurait été bien plus pertinente. En cas d'attaque terroriste, les sirènes peuvent par ailleurs amplifier les mouvements de panique et entrer en contradiction avec d'autres consignes (fuir plutôt que se confiner) et n'ont donc jamais été déclenchées en de pareils cas.

Au total, considérer les sirènes comme « principal moyen d'alerte » constitue une doctrine datée, qui n'est plus en phase avec les nouveaux risques et les nouveaux moyens d'alerte. Les sirènes devraient, en conséquence, être considérées comme un moyen d'alerte parmi d'autres.

Recommandation n° 1 : afin de favoriser le développement d'autres moyens d'alerte (*smartphones*, médias, etc.) et pour en améliorer la diffusion, renoncer à la doctrine faisant des sirènes le « vecteur principal » de diffusion de l'alerte.

2. Un financement qui aurait dû porter davantage sur les autres vecteurs d'alerte et d'information, notamment la téléphonie mobile

Tant le rapport « Hirel » que les travaux récents menés sur les moyens d'alerte et d'information des populations insistent sur la nécessité de combiner plusieurs moyens pour véhiculer l'alerte. **Au plan national, la direction générale de la sécurité civile et de la gestion des crises estime que « *si le vecteur principal de l'alerte est constitué par la sirène, l'alerte et l'information des populations ne sont cependant pas circonscrites à ce seul moyen* ». Pourtant, les choix de financement du SAIP ne reflètent pas cette stratégie.**

Si les sirènes, les télévisions et radios restent très utilisées dans les pays étrangers, beaucoup de systèmes nationaux d'alerte reposent également depuis longtemps sur la téléphonie mobile (SMS géo-localisés en Norvège depuis 2007, *Cell Broadcast*[1] aux Pays-Bas, au Japon et en Corée depuis 2012, applications *smartphone* en Allemagne depuis 2012…)[2]. La téléphonie mobile, qui permet, en plus de l'alerte, d'assurer l'information est dans la plupart des cas plus pertinente. Par ailleurs, l'augmentation tendancielle du taux d'équipement en téléphones mobiles, qui atteint aujourd'hui 93 % de la population (contre 63 % pour les *smartphones*, qui connaissent toutefois une

[1] *Technologie proche du SMS géolocalisée, explicitée* infra *p. 31.*

[2] *European Emergency Numbers Associations, Public warnings, 15 juillet 2015.*

forte hausse depuis 2011)[1], tend à accroître la force de pénétration de ce moyen d'alerte.

Les initiatives locales prises dans les bassins de risque, antérieurement ou indépendamment du SAIP, démontrent cette prise de conscience de l'insuffisance des sirènes. À proximité de certains sites classés Seveso et soumis à des plans particuliers d'intervention (PPI)[2], des systèmes d'alerte par téléphone permettent d'alerter et informer les populations avoisinantes sont mis en place. Plusieurs préfectures disposent de moyens d'avertissement des maires en cas d'événement nécessitant des réactions urgentes de leur part.

En tout état de cause, le financement du SAIP, très largement concentré sur les sirènes, ne prend pas suffisamment en compte cette logique multi-vectorielle. La première phase du déploiement du SAIP a en effet été répartie comme suit :

- réalisation du logiciel pilote, cœur du dispositif, pour 2,4 millions d'euros ;

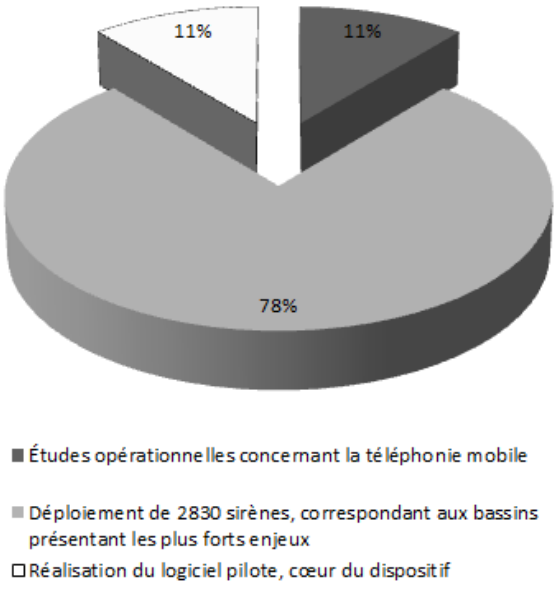
- déploiement de 2 830 sirènes, correspondant aux sites présentant les plus forts enjeux, pour 35,5 millions d'euros ;

- études opérationnelles concernant la téléphonie mobile, pour 5 millions d'euros.

[1] *CREDOC, enquête « Conditions de vie et aspirations », juin 2016.*

[2] *Le PPI définit l'organisation des secours en cas d'accidents susceptibles d'affecter les populations dans une installation classée (installations nucléaires, usines chimiques, stockages souterrains de gaz, barrages de plus de 20 mètres de hauteur et pouvant stocker plus de 15 millions de mètres cube d'eau, infrastructures liées au transport des matières dangereuses et laboratoires utilisant des micro-organismes).*

Répartition initiale des crédits de la première vague de financement



Source : commission des finances du Sénat

Observation : eu égard à son impact opérationnel, le volet « mobile » apparaît trop largement négligé. Une augmentation substantielle de la part des crédits alloués à cette partie du budget est nécessaire, au moins pour la seconde phase[1].

Recommandation n° 2 : rééquilibrer les crédits de la phase 2, en renforçant le financement du volet « mobile » pour garantir la mise en place soit d'une application *smartphone* pleinement efficace (scénario 2) soit le recours au *Cell Broadcast* (scénario 1).

[1] *Cf* infra, *partie du rapport relative à l'application mobile.*

DEUXIÈME PARTIE
UNE MISE EN ŒUVRE PERFECTIBLE DES DEUX PRINCIPAUX VOLETS DU SAIP, MARQUÉS PAR D'IMPORTANTS RETARDS

I. LE VOLET « SIRÈNES » ET LE LOGICIEL DE DÉCLENCHEMENT : UNE MISE EN ŒUVRE DÉFAILLANTE AYANT ENGENDRÉ UN IMPORTANT RETARD DE DÉPLOIEMENT

A. UN VOLET MIS EN ŒUVRE PAR LE BIAIS DE DIFFÉRENTS MARCHÉS PUBLICS, S'APPUYANT FORTEMENT SUR LES SIRÈNES EXISTANTES

1. Un volet reposant sur plusieurs marchés publics

Le volet « sirènes » a, en grande partie, été mis en œuvre par des prestataires auxquels ont été attribués des marchés publics. Lancés en avril 2011, ces marchés courent pour certains jusqu'en 2022.

S'agissant du logiciel central, les marchés conclus par la direction générale de la sécurité civile et de la gestion des crises ont été transférés fin 2011 à la direction des systèmes d'information et de communication (DSIC). Dans ce contexte, la DSIC est devenue à la fois maître d'œuvre du projet et pouvoir adjudicateur.

La phase préparatoire a été en grande partie réalisée avec l'assistance de la société Deloitte Conseil, qui avait remporté l'appel d'offres pour des prestations relatives à l'assistance à maîtrise d'ouvrage.

Les différents marchés publics du volet « sirènes » du SAIP

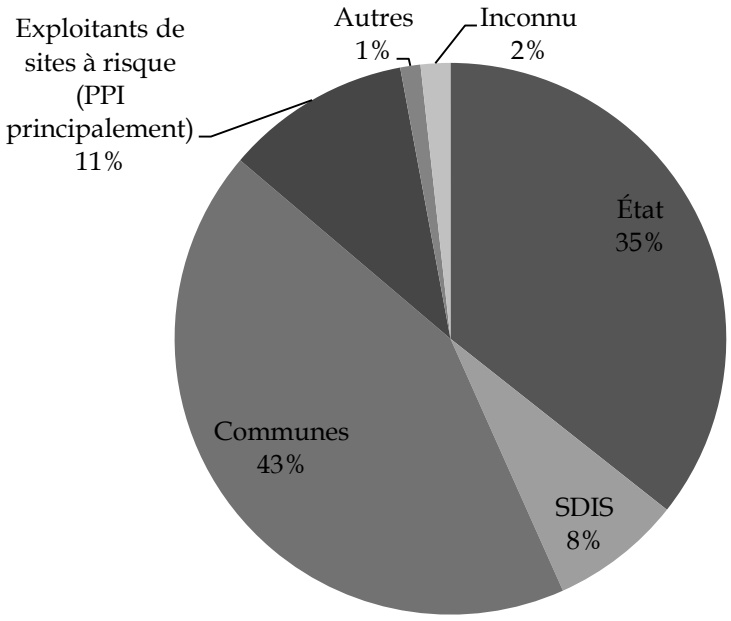
Marchés	Lots	Société retenue	Début	Fin
Marché relatif à l'assistance technique, organisationnelle, financière et juridique pour l'élaboration, la passation et l'exécution d'un futur marché de réalisation du SAIP		Deloitte Conseil	2009	31/05/2014
Marché relatif à la réalisation du SAIP	lot n° 1- Développement, intégration et maintien en condition opérationnelle du logiciel de déclenchement de l'alerte. Intégration des composants du SAIP	Cassidian SAS	2011	30/11/2021
	lot n° 2- Fournitures des sirènes	Moteurs Fox	2011	30/11/2021
	lot n° 2- Fournitures des sirènes	Ineo Cabalec	2011	30/11/2021
	lot n° 2- Fournitures des sirènes	AE&T	2011	30/11/2021
	lot n° 4- Fournitures des armoires électriques	Fournié Grospaud Synerys	2011	30/11/2021
	lot n° 4- Fournitures des armoires électriques	AE&T	2011	2021
	lot n° 4- Fournitures des armoires électriques	Ineo Cabalec	2011	2021
Marché relatif à la fourniture de boitiers émission réception pour le déclenchement des sirènes via l'infrastructure nationale des transmissions par le SAIP		Cassidian SAS	2012	2022
Marché relatif à la réalisation du SAIP via l'infrastructure nationale des transmissions (INPT)	lot n° 1- Fournitures des armoires de commande permettant la mise en réseau des sirènes	Fournié Grospaud Synerys	2012	2022
	lot n° 2- Installation et maintien en condition opérationnelle des fournitures sirènes, armoires électriques, armoires de commande et boîtiers d'émission-réception SAIP	Eiffage	2012	2022

Source : ministère de l'intérieur, DGSCGC

2. Un déploiement satisfaisant de la première phase de l'installation et du raccordement des sirènes

Le déploiement du SAIP s'appuie tant sur les sirènes existantes, dont le raccordement a été jugé pertinent par les préfectures, que sur des nouvelles sirènes. Afin de tirer au mieux profit du parc existant, le ministère de l'intérieur a organisé un inventaire en 2010 qui a permis de comptabiliser 10 306 sirènes.

Parc de sirènes recensées en 2010



Source : commission des finances, d'après le ministère de l'intérieur, DGSCGC

En tout, la direction générale de la sécurité civile et de la gestion des crises a prévu le raccordement au SAIP de 5 338 sirènes sur 1 743 bassins d'alerte. Ce déploiement doit être réalisé en deux vagues :

- la première est constituée de **2 830** sirènes correspondant aux anciennes sirènes réhabilitées du réseau national d'alerte (RNA) et de nouvelles sirènes afin de couvrir les zones considérées comme les plus à risques ;

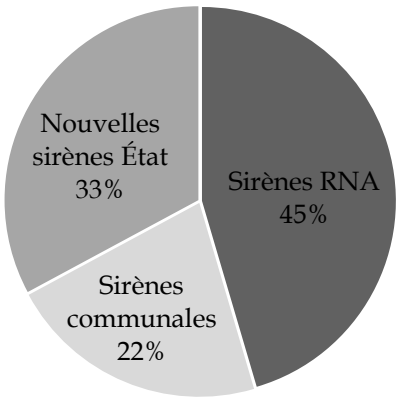
- la seconde est constituée de **2 508** sirènes correspondant aux sirènes situées sur les autres bassins de risques (d'intensité légèrement moindre) ainsi que des sirènes installées par les industriels exploitants dans le cadre d'un plan particulier d'intervention (PPI).

Origine des sirènes raccordées lors des deux phases du SAIP

	Sirènes RNA	Sirènes Communales	Nouvelles Sirènes État	Sirènes PPI	Total
Vague 1 (2010-2020)	1 286	614	930	0	2 830
Vague 2 (À partir de 2020)	0	533	854	1 121	2 508
Total	**1 286**	**1 147**	**1 784**	**1 121**	**5 338**

N.B. : les chiffres ci-dessus sont issus du recensement de 2010 et la répartition a donc pu évoluer en fonction des risques et de l'état des lieux.

Origine des sirènes raccordées lors de la première phase du SAIP



Source : ministère de l'intérieur, DGSCGC

Le déploiement des sirènes a été engagé sur le terrain à compter de septembre 2013 (suite à la passation des marchés publics). Il concerne à ce stade les sirènes de la seule première vague. **Ce déploiement ne semble, à ce stade, donner lieu qu'à des problèmes mineurs.**

Début 2016, les visites de préinstallation avaient commencé dans 68 départements. La société Eiffage est chargée de l'installation et du raccordement de sirènes avec l'appui des préfectures. **1 922 visites de site** (soit 68 % des sites retenus pour une première vague de déploiement) ont été effectuées à ce stade. À la fin du mois d'avril 2017, 1 459 sirènes sont installées et raccordées sur les 2 830 prévues en vague 1, soit 51 % de la

première vague, ce qui correspond à un avancement conforme aux prévisions.

L'objectif est de terminer l'installation de cette vague en 2019-2020 avec un nombre d'installations par an s'étendant entre 400 et 500.

Les choix de déploiement prennent par ailleurs en compte les priorités issues des crises récentes. Ainsi, à la suite des intempéries de l'automne 2015, il a été décidé début 2016 de privilégier le déploiement des sirènes dans les départements de l'arc méditerranéen. Les préfets de ces départements ont été sensibilisés à l'importance d'accélérer le déploiement des sirènes (ou leur raccordement au SAIP lorsque cela n'a pas encore été fait) dans les zones à risque et non couvertes par des moyens d'alerte et d'information des populations.

B. D'IMPORTANTS RETARDS DANS LA RÉALISATION DU LOGICIEL CENTRAL : UNE DOUBLE RESPONSABILITÉ DE L'ADMINISTRATION ET DU PRESTATAIRE

Si l'installation des sirènes, à proprement parler, n'a pas connu un retard important, ce volet n'a pas pu être opérationnel à temps en raison des difficultés liées à la réalisation du logiciel central de commande, qui a connu un important retard, de 37 mois. Environ 1 500 sirènes installées sont aujourd'hui prêtes à être raccordées au logiciel. Le 3 mai 2017, les préfectures pilotes ont pu tester le déclenchement des sirènes pour l'essai mensuel en utilisant le logiciel, mais ce dernier n'est toujours pas déployé dans les SDIS, les préfectures et les communes.

1. Un retard de 37 mois dans la livraison du logiciel permettant le déclenchement à distance des sirènes

L'élaboration du logiciel de déclenchement, cœur du dispositif, a été confiée à *Airbus Defence and Space* (ex *Cassidian*).

L'offre de cette société a été retenue comme étant la plus adaptée, Airbus ayant mis en avant ses nombreuses références en Amérique du Nord dans le domaine des systèmes de notification de masse pour des clients publics (*Federal Bureau of Investigation*, département de la santé de la ville de New York) et privés (Citigroup, Mellon Financial, etc.).

Par ailleurs, la solution proposée par Airbus devait être commune à la France et aux Émirats Arabes Unis, qui avaient également fait appel à l'industriel pour la réalisation de leur système national d'alerte.

Le marché correspondant, d'un montant de 2,82 millions d'euros, a été notifié le 30 novembre 2011.

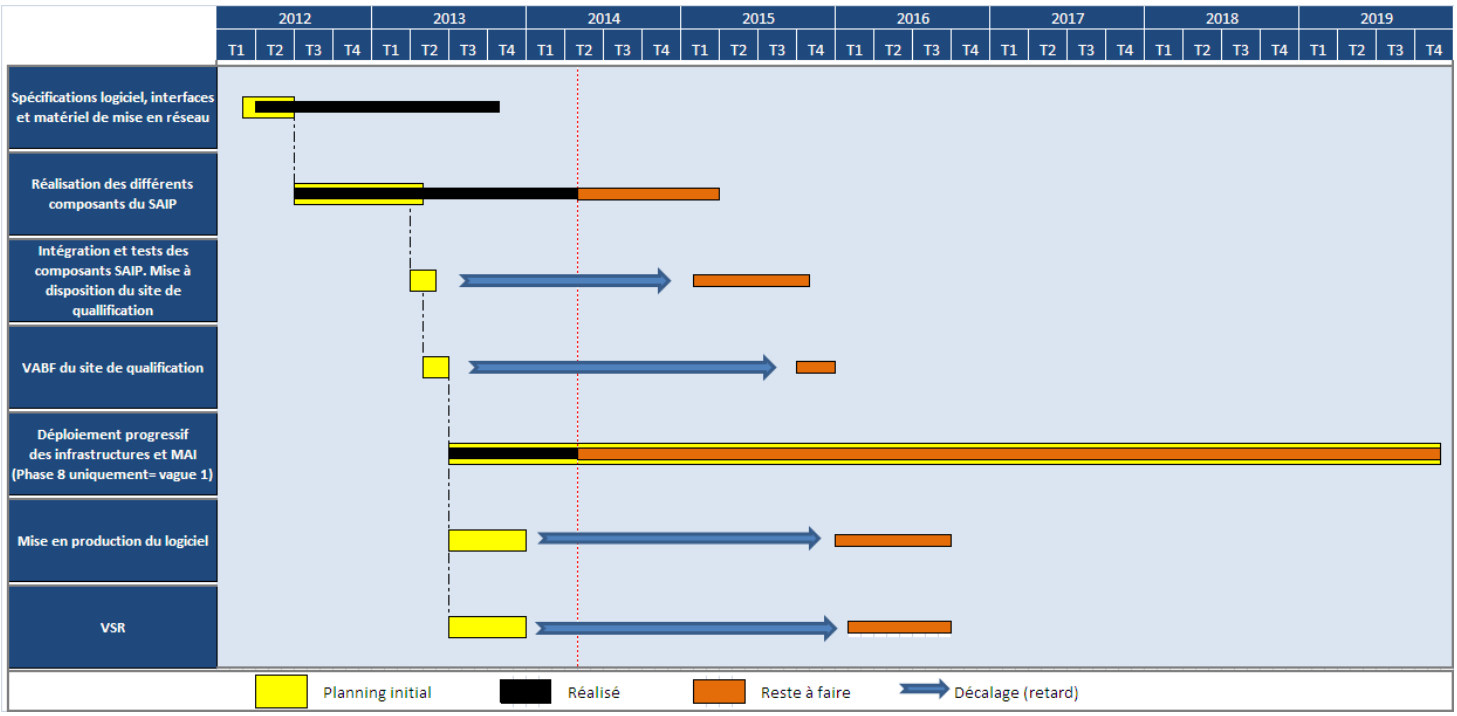
Le choix d'*Airbus Defence and Space* par la direction générale de la sécurité civile et de la gestion des crises, maître d'ouvrage du projet, n'est, a priori, pas dépourvu de pertinence ; la collaboration nouée entre cet industriel et l'État dans le cadre de la mise en place et de l'exploitation de l'infrastructure nationale partageable des transmissions (INPT) plaidait en sa faveur. Le marché excluait par ailleurs les PME et SSII de taille moyenne[1], en raison de la technicité importante exigée pour y répondre.

Le bon de commande relatif aux unités d'œuvre permettant l'élaboration du logiciel fut ainsi adressée le 20 mars 2012 à l'industriel, le logiciel devant être fourni à l'administration le 21 juin 2013 (début de la phase de vérification d'aptitude au bon fonctionnement). Il n'a toutefois été finalement été livré qu'en avril 2015, **avec 37 mois de retard, avec une vérification de mise en service régulier (essais préfigurant la mise en service du logiciel) effectuée à compter de septembre 2016 au lieu d'août 2013**.

L'allongement de la durée de déploiement du volet « sirènes » du SAIP a conduit à reporter l'échéance de fin de réalisation de la première vague à 2019, ce qui est, selon le ministère de l'intérieur, **préjudiciable au projet tant en termes de mobilisation des acteurs qu'au regard de son coût total.** Ce report conduit à un surcoût de déploiement (coûts de pilotage annuel plus importants et hausse économique sur les différents marchés) estimé à près de 2 millions d'euros sur un projet de 81,5 millions d'euros, à la charge de l'État.

[1] *Les exigences spécifiées dans le règlement pour répondre au lot 1 étaient de 30 millions d'euros de chiffre d'affaires annuel minimum.*

Les retards dans la mise en œuvre du volet « sirènes »



Source : ministère de l'intérieur, DISIC

2. Une double responsabilité de l'administration et du prestataire

Des torts partagés entre le prestataire et l'administration expliquent cet important retard.

Du côté d'*Airbus Defence and Space*, le choix de recourir à des équipes basées aux États-Unis pour le développement de l'application apparaît comme une des explications du retard. Le prestataire reconnaît également que la montée en compétence des équipes a été plus lente que prévue. De même, le projet de développement commun avec les Émirats Arabes Unis ne fut jamais lancé, et Airbus dût renoncer aux économies d'échelles qu'aurait permis un développement du logiciel vendu aux deux pays, ce qui a favorisé les retards, les équipes chargées du SAIP n'ayant pas pu le développer à partir d'un progiciel préexistant. L'équipe d'Airbus est restée mobilisée en dépit des surcoûts importants apparus au cours de l'exécution du contrat, qui ont sans doute engendré des pertes financières pour l'entreprise.

Les délais de livraison du logiciel ont également souffert des retards de validation par l'administration des dossiers d'architecture technique et fonctionnelle du projet. Selon le prestataire, une des principales difficultés rencontrées a été **l'absence de doctrine d'emploi** lors de la phase de conception. Alors que le contrat prévoyait cinq jours de réunions avec les services utilisateurs pour valider les fonctionnalités de l'outil, les groupes de

travail se sont échelonnés de mars 2012 à janvier 2013 avec une remise en cause fin 2012 des principes de base de l'application tels que, par exemple, la définition du déclenchement d'une alerte.

La complexité des fonctionnalités de logiciel, ainsi que la gestion des droits et des profils des utilisateurs (préfectures, service départemental d'incendie et de secours (SDIS), centre opérationnel de gestion interministérielle des crises (COGIC), etc.) a nécessité une spécification dense, de plus de 1 400 pages, modifiée en cours d'exécution du contrat, rendant les adaptations difficiles pour le prestataire.

Par ailleurs, le ministère de l'intérieur a abandonné en mai 2015 la fonction qui devait permettre l'envoi de SMS *Cell Broadcast* dans la même zone d'alerte que celle des sirènes actionnées. L'abandon de cette fonctionnalité en cours de projet, alors même qu'elle était, à juste titre, jugée critique par le ministère de l'intérieur lui-même traduit bien le manque de préparation du projet[1].

Si des éléments exogènes (perte du marché émirati par Airbus, défauts d'organisation des équipes) ont contribué aux retards, une partie des difficultés aurait pu être évitée si l'administration avait davantage préparé le projet en amont et précisé ses exigences.

Ces retards et ces difficultés s'expliquent également par les effectifs particulièrement restreints affectés au projet SAIP. Ainsi, au sein de la direction générale de la sécurité civile et de la gestion des crises, le projet est suivi par cinq personnes dont une à temps plein et deux aux trois quarts, et, à la direction des systèmes d'information et de communication, par quatre personnes à temps également partiel.

Aussi, si seuls les projets informatiques d'un montant supérieur à 5 millions d'euros[2] doivent faire l'objet d'un avis de la direction interministérielle des systèmes d'information et de communication (DINSIC), une saisine volontaire du ministère de l'intérieur de cette dernière aurait été justifiée, eu égard aux faibles effectifs dédiés en interne à ce projet et à sa complexité, même si son montant s'élevait à 2,43 millions d'euros.

---

[1] *Selon les informations recueillies par votre rapporteur spécial, la possibilité de déclencher l'application* smartphone *SAIP depuis le logiciel pourrait être à nouveau envisagée dans le cadre d'un futur marché.*

[2] *Décret n° 2011-193 du 21 février 2011 portant création d'une direction interministérielle des systèmes d'information et de communication de l'État. Ces seuils de coût ont été fixés par arrêté du 1er juin 2011 pris pour l'application de l'article 7 du décret du 21 février 2011 précité.*

Cette procédure apparaît vertueuse car elle permet aux projets concernés de bénéficier de l'expertise et de l'appui de cette direction (mesures telles que des formations ou des activités d'animation de communautés professionnelles afin de partager les meilleures pratiques)[1].

Recommandation n° 3 : pour permettre au ministère de l'intérieur de faire face aux projets informatiques d'envergure, prévoir une procédure, exigeant la formulation d'un cahier des charges précis élaboré en amont de la notification du marché et un éventuel appui de la direction interministérielle du numérique et du système d'information et de communication de l'État (DINSIC), lorsque la complexité le commande, même si le coût du projet est inférieur au seuil réglementaire.

II. LE VOLET « MOBILE » : UN ABANDON REGRETTABLE DU CELL BROADCAST AU PROFIT D'UNE APPLICATION *SMARTPHONE*, MOINS EFFICACE ET DEVELOPPÉE HÂTIVEMENT, NÉCESSITANT ENCORE D'IMPORTANTES AMÉLIORATIONS

A. UN ABANDON DES TECHNOLOGIES SMS ET CELL BROADCAST AU PROFIT DE L'APPLICATION SMARTPHONE *REGRETTABLE*

1. Trois technologies concurrentes pour diffuser l'alerte et l'information par téléphonie mobile

Trois technologies principales permettent de diffuser l'alerte par téléphonie mobile : les SMS géolocalisés, le « *SMS Cell Broadcast* » et le recours à une application *smartphone* en libre téléchargement.

L'objectif initial du projet, en 2011, visait à mettre en œuvre, en liaison avec les opérateurs de téléphonie mobile, la diffusion des messages d'alerte par le biais de la technologie dite du « *SMS Cell Broadcast* ».

Ce choix devait permettre de garantir la diffusion, en toute circonstance, des messages d'alerte, indépendamment de la charge supportée par les réseaux des opérateurs, et offrait la possibilité de les différencier immédiatement des SMS classiques.

Des négociations ont donc été engagées en 2011 avec les opérateurs de téléphonie mobile français en vue d'explorer la faisabilité technique et le coût de la mise en œuvre de cette solution. Toutefois, la direction générale de la sécurité civile et de la gestion des crises a estimé que celles-ci n'avaient pu

[1] L'informatique publique : quels moyens pour l'administration de demain ?, *Rapport d'information n° 76 (2016-2017) de M. Michel Canevet, fait au nom de la commission des finances, déposé le 26 octobre 2016, p. 24.*

aboutir « *pour des raisons* ***de volonté des opérateurs ou de coûts non soutenables et non compatibles avec les enveloppes budgétaires existantes*** ».

Le ministère de l'intérieur, pour lequel les sirènes doivent en tout état de cause rester le principal vecteur de la diffusion de l'alerte, a donc décidé de privilégier le développement d'une application *smartphone* en libre téléchargement plutôt que de s'appuyer sur le *Cell Broadcast* ou sur les SMS géolocalisés.

Deux principales raisons expliquent le choix de ne pas recourir à la technologie *Cell Broadcast* :

- cette technologie n'est pas systématiquement intégrée dans les *smartphones* et n'est à ce stade pas encore compatible avec la 4G. Ainsi, aux États-Unis, Apple, qui ne fournissait pas cette fonctionnalité, n'aurait accepté de l'introduire sur ses iPhones qu'après une demande des autorités fédérales américaines à la suite de l'ouragan Sandy de 2012 ;

- elle requiert par ailleurs un fort investissement des opérateurs, puisque les logiciels des équipements des réseaux doivent comprendre une fonctionnalité particulière (elle doit être paramétrée, testée et installée). Si, à l'origine, l'inclusion de la fonction *Cell Broadcast* aux réseaux était courante en technologie 2G, il est possible qu'elle ne soit plus présente sur les réseaux postérieurs. Des travaux seraient toutefois en cours pour l'installer rapidement sur les réseaux 4G.

La solution de recours aux SMS géolocalisés apparaît, au contraire, rapide et facile à mettre en œuvre mais souffre également de plusieurs lacunes jugées, à juste titre, rédhibitoires par le ministère de l'intérieur :

- la vitesse d'acheminement des messages d'alerte dans un contexte de crise serait trop faible, du fait de la saturation des réseaux ;

- elle suppose une agrégation dynamique par l'opérateur des numéros de téléphones présents sur une zone d'alerte, ce qui peut susciter des interrogations sur la gestion de ces données personnelles ;

- le SMS d'alerte ne se distingue pas des autres SMS. Contrairement au *Cell Broadcast* qui est « prioritaire » et fait l'objet d'une présentation distincte, il n'y a pas systématiquement d'affichage immédiat du SMS sur l'écran du téléphone et il faut, comme pour n'importe quel SMS, aller consulter sa boîte de réception pour le lire. L'envoi de faux SMS d'alerte est par ailleurs aisée et l'utilisateur n'a que peu de moyens de les détecter.

Au total, il apparaît qu'aucun pays étranger n'utilise l'envoi de SMS géolocalisés pour la diffusion de messages d'alerte au niveau national, même si des études sont en cours au Royaume-Uni.

En tout état de cause, l'ensemble des moyens d'alerte par téléphonie mobile suppose, pour être pleinement opérationnel, que les efforts de réduction des zones blanches menés par les opérateurs soient accrus.

2. Un choix contestable de recourir à l'application *smartphone*

Le ministère de l'intérieur a préféré recourir à une application smartphone plutôt qu'au *Cell Broadcast*. Pourtant, cette technologie présente plusieurs inconvénients qui conduisent à douter de sa pertinence :

- **son activation nécessite un téléchargement de la part de l'utilisateur**, ainsi qu'une activation des notifications et de la géolocalisation. Elle doit, par ailleurs, être conservée en tâche de fond sous iOS ;

- elle n'est, par définition, disponible que sur *smartphone*. Par ailleurs, elle n'est disponible que pour les *smartphones* fonctionnant sous Android et iOS (ce qui exclut notamment les téléphones de la marque BlackBerry et ceux fonctionnant sous le système d'exploitation de Windows) ;

- **elle s'appuie sur des données transmise par internet. Or ce réseau peut être vulnérable en cas de crise** (saturation, comme en cas de sur-sollicitation imprévue d'internet après un attentat, endommagement des antennes-relais suite à un phénomène naturel, etc.) ;

- **elle entre en concurrence avec d'autres applications poursuivant le même objet**, ou celle des médias traditionnels et des réseaux sociaux, également susceptibles de générer des « notifications *push* » en cas d'alerte. Par ailleurs, elle ne devrait être téléchargée en nombre significatif que par les personnes habitant régulièrement en France, et exclut de fait les personnes en voyage en France[1], ces dernières n'ayant qu'un faible intérêt à procéder à un téléchargement. Cette lacune revêt une gravité particulière s'agissant des alertes concernant des lieux touristiques fréquentés par des étrangers.

Au contraire, le *Cell Broadcast* aurait sans doute mérité de plus amples réflexions avant d'être abandonné si promptement. Déjà utilisé dans de nombreux pays, tels que les États-Unis, le Chili, le Japon, ou encore les Pays-Bas, il permet la diffusion rapide d'un message intelligible et facilement identifiable à l'ensemble des téléphones situés dans un espace géographique donné.

L'argument tenant aux lourdeurs liées à la nécessaire pré-programmation des téléphones pour exclure le *Cell Broadcast* ne paraît par ailleurs pas convaincant, dès lors que le choix de l'application nécessite lui aussi un téléchargement de la part des utilisateurs.

Enfin, la réticence de certains opérateurs à mettre en œuvre cette technique aurait aisément pu être surmontée par l'introduction d'une disposition législative prévoyant l'obligation, pour ces derniers, d'acheminer

[1] *Selon la Direction générale des entreprises, 84,5 millions de touristes étrangers ont ainsi séjourné en France en 2015.*

les communications des pouvoirs publics destinés à l'alerte et à l'information des populations[1].

Certes, cette technologie présenterait un coût budgétaire pour l'État, qui aurait dû indemniser les opérateurs des coûts d'adaptation du système et des coûts de fonctionnement[2]. À titre illustratif, aux Pays-Bas, 25 millions d'euros ont été dépensés depuis 2012 pour un parc de 17 millions d'abonnés répartis entre trois opérateurs. **Néanmoins, les bénéfices (rapidité, robustesse) auraient largement excédé ces coûts. À ce titre, les 81,5 millions d'euros programmés pour financer le SAIP auraient pu être plus utilement employés pour poursuivre les études préparatoires relatives au volet « mobile » et à financer une éventuelle mise en place du *Cell Broadcast* comme vecteur de l'alerte.**

Toutefois il peut être difficile de remettre en cause les choix antérieurs, étant donné les investissements engagés en faveur de l'application. Il serait cependant nécessaire que la pertinence de cette application dans sa version aboutie fasse l'objet d'une évaluation indépendante d'ici la fin de 2019. Il conviendrait, dans l'hypothèse où cette évaluation ne serait pas concluante, de reprendre les travaux visant à mettre également en place le *Cell Broadcast*.

Observation : le choix d'avoir abandonné le *Cell Broadcast*, initialement envisagé, au profit d'une application *smartphone* pour des raisons budgétaires et d'absence de volonté des opérateurs, est critiquable. Cette décision découle directement du choix contestable de privilégier le volet « sirènes » plutôt que le volet « mobile ».

[1] *Un amendement en ce sens avait d'ailleurs été déposé en commission par notre collègue Daniel Raoul en 2016, lors de la discussion du projet de loi pour une République numérique.*

[2] *Le Conseil d'État a indiqué, dans un avis rendu le 6 mars 2012, que si la gratuité de la diffusion des messages peut être imposée aux opérateurs, le déploiement de la solution technique du Cell broadcast, non prévue par les obligations du service universel, devait par contre donner lieu à une « juste rémunération » de la part de l'administration.*

Recommandation n° 4 : effectuer, d'ici 2019, une évaluation de l'application SAIP, afin de déterminer sa pertinence en comparaison du *Cell Broadcast*, et réajuster le déploiement de la phase 2 en conséquence, afin de garantir la fiabilité et l'efficacité de l'alerte par téléphonie mobile.

→ Scénario 1 : en cas d'abandon, à la suite de cette évaluation, de l'application *smartphone* comme vecteur principal de l'alerte par téléphonie mobile, assurer son remplacement par la technologie *Cell Broadcast*, en lien avec les opérateurs, dans le courant des années 2020 et 2021.

→ Scénario 2 : en cas de confirmation du principe de l'application comme principal vecteur de l'alerte par téléphone mobile, fiabiliser l'application SAIP et poursuivre la publicité en sa faveur afin d'augmenter le nombre de téléchargements en vue d'atteindre une masse critique permettant d'en faire un vecteur efficace de l'alerte (objectif de 5 millions de téléchargements fin 2020).

B. UNE APPLICATION IMPARFAITE RÉALISÉE DANS UN CALENDRIER TROP CONTRAINT

L'application trouve son origine dans une décision du Premier ministre. À la suite des attentats du 13 novembre 2015, ce dernier a voulu que le dispositif d'alerte par application mobile soit mis en place avant la compétition « Euro 2016 », prévue en juin 2016. L'application *smartphone* a ainsi été conçue dans l'urgence, ce qui a nui à la qualité du produit final.

Le marché a été notifié à Deveryware le 27 mai 2016, soit moins de deux semaines avant la date de mise en production et le début de l'« Euro 2016 ». Cette société, spécialisée dans les services s'appuyant sur la géolocalisation en temps réel était déjà, comme d'autres, en relation d'avant-vente avec la DGSCGC depuis plus d'un an.

De fait, cinq mois se sont écoulés entre la phase d'expression des besoins, en janvier 2016, et la mise en ligne de l'application, le 8 juin 2016. Cette courte période a dû être mise à profit pour formuler le cahier des charges, sélectionner un prestataire qui a lui-même dû concevoir l'application, en prenant en compte la contrainte forte exprimée par la direction générale de la sécurité civile et de la gestion des crises, qui souhaitait garantir l'absence de remontée des données de géolocalisation vers un serveur central afin de garantir le respect de la vie privée des usagers et d'éviter de susciter la méfiance du public.

Compte tenu de cette exigence, le prestataire a conçu une architecture originale basée sur le principe du *geofencing*, qui exclut toute remontée des données de géolocalisation des utilisateurs vers les serveurs. À l'inverse, l'ensemble des événements recensés sur le territoire justifiant une alerte sont téléchargés sur le téléphone, qui diffuse l'alerte par une notification si ce dernier est localisé dans un endroit concerné.

Ce calendrier particulièrement contraint traduit l'impréparation dans laquelle s'est déroulée la phase de conception de l'application, alors même que le choix de recourir à la téléphonie mobile comme vecteur de l'alerte était arrêté depuis 2011 et que l' « Euro 2016 » était prévu à Paris depuis 2010.

Observation : le projet, dans ses dimensions techniques, de définition du besoin et de passation du marché, a été mené un délai trop contraint eu égard à sa complexité, alors même qu'une plus grande anticipation aurait été possible, la téléphonie mobile étant envisagée comme vecteur de l'alerte depuis 2011.

C. UNE APPLICATION PEU ERGONOMIQUE ET UNE DOCTRINE D'EMPLOI TROP TIMIDE RISQUANT D'ENGENDRER UN DÉLAISSEMENT PAR LE PUBLIC AU PROFIT DES MOYENS D'ALERTE PLUS CLASSIQUES

1. Une ergonomie et une solidité technique perfectible, malgré la prise en compte des principales défaillances

Le 14 juillet 2016, au moment de l'attentat de Nice, alors que le dispositif est utilisé pour la première fois en conditions réelles, un dysfonctionnement technique retarde de plus de deux heures l'envoi de l'alerte. À la suite de cet incident, le ministère de l'intérieur a commandé un rapport d'audit au cabinet Wavestone, qui a imputé ce dysfonctionnement à la conjonction de quatre éléments dorénavant maîtrisés.

Cet audit technique conclut que « ***les actions mises en œuvre pour traiter les causes primaires du dysfonctionnement (passage d'une mise à jour corrigeant le bug, correction du développement spécifique, renforcement de la supervision, formalisation de la procédure de démarrage) sont jugées satisfaisantes et de nature à éviter la reproduction d'un incident du même type*** ».

L'audit a par ailleurs permis de compléter le plan d'action de Deveryware en formulant des recommandations techniques, à travers notamment la mise en place d'un deuxième site d'hébergement, afin de fiabiliser l'existant et de limiter les risques.

Des « bugs » résiduels, laissant une impression de manque de maîtrise de la part du ministère de l'intérieur et de Deveryware, subsistent toutefois (cas de réception d'alerte bien que l'utilisateur ne se trouve pas dans une zone de danger, message de fin d'alerte à Nice renvoyé plus d'un mois après l'événement, à la suite du redémarrage des serveurs du *back-office*).

Surtout, des défauts structurels de l'application doivent être corrigés : la haute consommation de batterie, l'application géolocalisant le mobile de manière quasi-continue en cas d'alerte, et la nécessité, sous iOS (système d'exploitation des iPhones d'Apple), de garder l'application en tâche de fond (c'est-à-dire ouverte, mais sans être nécessairement active au premier plan).

Recommandation n° 5 : corriger en urgence les principales défaillances persistantes de l'application SAIP qui nuisent à sa fiabilité et à son ergonomie, comme les géolocalisations inopinées, la consommation excessive de batterie et, surtout, la nécessité de conserver l'application ouverte en tâche de fond.

Des évolutions devraient pouvoir être mises en œuvre dans le cadre du marché passé sous l'égide de l'Union des groupements d'achats publics (UGAP) le 1er mars 2017 pour une durée d'une année renouvelable une fois. Ce dernier vise à pérenniser l'application et élargir les cas dans lesquels elle peut être actuellement déclenchée (alertes attentat, nucléaire, produits dangereux, rupture d'ouvrage hydraulique) aux crises de sécurité civile à cinétique rapide (inondations rapides, feux de forêts, intempéries, séisme, submersion marine, cyclones, éruptions volcaniques).

2. Un nombre de téléchargements insuffisant et une doctrine d'emploi trop timide risquant d'engendrer une désaffection de la part du public

a) Revoir la doctrine d'emploi

S'agissant de la doctrine d'emploi, le ministère de l'intérieur a précisé que le « *SAIP* [était] *un vecteur parmi d'autres. L'information peut être diffusée par voie de presse ou par les réseaux sociaux, via les comptes de la préfecture de police ou du ministère de l'intérieur. L'important, c'est que l'information soit diffusée, d'une manière ou d'une autre* […] *Pour que SAIP reste une application efficace, il faut la déclencher à bon escient. Ce déclenchement est décidé par le préfet, en fonction des éléments qu'il a en sa possession* »[1].

De fait, lors des attaques terroristes récentes, le compte Twitter de la Préfecture de Police de Paris a commencé à diffuser des messages d'information et d'alerte dans les instants suivants les attaques, que ce soit lors de l'attentat du 20 avril 2017 (fusillade sur les Champs-Élysées, message « Nous vous conseillons d'éviter le secteur des Champs-Élysées » diffusé à 21 h 06) ou lors de l'attaque ayant eu lieu au musée du Louvre le 3 février 2017**. La multiplication des canaux d'information et d'alerte entre**

[1] *Réponses aux questionnaires.*

toutefois en contradiction avec l'objectif initial affiché par l'application SAIP, de centraliser l'ensemble des messages d'alerte relatifs à une zone donnée. L'utilisation de l'application devant relever d'une démarche positive des usagers, une doctrine d'emploi trop timide fait encourir un risque de désaffection de la part du public pour l'application, qui pourrait renoncer à la télécharger ou la désinstaller, surtout si les moyens plus classique (réseaux sociaux, médias) ne nécessitant pas de téléchargement supplémentaire, s'avèrent plus fiables.

La justification du non recours à l'application par le ministère de l'intérieur, reposant sur la cinétique lente ou le fait que la situation ait pu être figée rapidement (comme lors de la fusillade des Champs-Élysées) apparaît d'autant plus contestable que le manque de diffusion de l'alerte accroît la charge de travail des forces de l'ordre sanctuarisant le secteur de l'attaque. La diffusion de l'alerte apparaît également pertinente dans une situation supposée figée, la possibilité qu'un assaillant non identifié ait réussi à prendre la fuite ou qu'une autre équipe de terroristes effectuent une réplique dans les instants suivant la première attaque n'étant pas négligeables.

Recommandation n° 6 : modifier la doctrine d'emploi de l'application afin d'y relayer, même lorsqu'ils semblent maîtrisés, l'ensemble des évènements pouvant mettre en cause la sécurité des personnes sur un territoire, afin notamment d'éviter une désaffection de la part du public pour ce dispositif.

b) En cas de confirmation de sa pertinence, augmenter le nombre de téléchargements de l'application

Le nombre de téléchargements de l'application, de l'ordre de 900 000 à mi-2017 et stable depuis lors[1] n'apparaît pas suffisant pour atteindre la masse critique permettant d'alerter toute la population présente sur un site concerné par une alerte. Ce nombre de téléchargement a pu être atteint grâce à l'effet de notoriété engendré par campagne de publicité organisée par le service d'information du Gouvernement pendant l'« Euro 2016 ».

Si, à la suite de l'évaluation préconisée par votre rapporteur, le principe de l'application *smartphone* devait être conservé, une augmentation significative des personnes l'ayant activée sur leur *smartphone*, à environ 5 millions (soit un peu moins de 10 % de la population), apparaît souhaitable. Il constitue le minimum permettant de garantir un nombre suffisant de personnes alertées par *smartphone* sur une zone de danger donnée et susceptibles de prévenir les personnes en danger avoisinantes.

[1] *Rapport d'audit de Wavestone.*

Une nouvelle campagne de communication devrait donc être envisagée en ce sens en 2019.

3. La contribution des autres applications *smartphone* à l'alerte et à l'information des populations

Les applications *smartphone* qui bénéficient d'une grande diffusion et peuvent générer des notifications push sur les *smartphones* constituent des vecteurs potentiellement très efficaces, en raison de leur grand nombre d'usagers actifs. Les principales applications susceptibles de contribuer à l'alerte et à l'information des populations sont celles des réseaux sociaux, des médias ou encore des applications de cartographie dynamique. À titre illustratif, Facebook comprend en France 32 millions d'utilisateurs, dont 28 millions depuis un mobile et dispose donc d'une force de frappe particulièrement remarquable.

Ces réseaux peuvent contribuer au déclenchement de l'alerte de deux manières :

- par le biais des contenus publiés par les utilisateurs, qui peuvent être individuels ou institutionnels, publics ou privés. La préfecture de Police de Paris utilise ainsi son compte Twitter, qui dispose de 340 000 abonnés en juillet 2017, pour relater des alertes (cf. *supra*). Des comptes associatifs inscrits sur ces réseaux sociaux se spécialisent également dans la diffusion de messages d'alertes, comme ceux de l'association VISOV, qui a noué des partenariats avec différents SDIS et avec la direction générale de la sécurité civile et de la gestion des crises[1] ;

- par l'utilisation de dispositifs mis en place par le concepteur de l'application lui-même, permettant d'envoyer un message d'alerte aux utilisateurs. Le Facebook Safety Check, créé à la suite de l'accident nucléaire de Fukushima en 2011, permet ainsi aux utilisateurs de se signaler comme étant en sécurité en cas de crise[2]. Il permet également de diffuser des consignes de comportement aux utilisateurs concernés. D'autres types d'applications, tels que le service de cartographie Google Maps[3], peuvent également contribuer efficacement à la diffusion de l'alerte et de l'information.

Ces dispositifs épars ne font l'objet d'aucune réelle coordination au niveau de l'État et aucune convention formalisée n'existe pour l'heure même si des sollicitations ponctuelles (issues principalement du Service

---

[1] *European Emergency Numbers Associations, Public warnings, 15 juillet 2015.*

[2] *Lors de l'attentat du 13 novembre 2015 à Paris, 4 millions de personnes se sont signalées comme étant en sécurité.*

[3] *Lors de l'attaque sur les Champs-Élysées le vendredi 21 avril 2017, l'application Google Maps a ainsi signalé cette avenue comme bloquée très rapidement après l'attaque, alors même que l'application SAIP était muette.*

d'information du Gouvernement, ou des cabinets ministériels[1]) ont toutefois lieu. **Le renforcement de la coopération et des échanges entre l'État et les gestionnaires de ces applications apparaît souhaitable. Toutefois, cette coopération ne saurait remettre en cause la nécessité, pour le ministère de l'intérieur, de disposer d'un dispositif d'alerte par téléphonie mobile dont il a la pleine maîtrise.**

[1] *Facebook a ainsi été sollicité par le secrétariat d'État chargé du numérique et de l'innovation lors de l'attentat du 14 juillet 2016 à Nice.*

EXAMEN EN COMMISSION

Réunie le mercredi 28 juin 2017, sous la présidence de Mme Michèle André, présidente, la commission a entendu une communication de M. Jean Pierre Vogel, rapporteur spécial, sur le système d'alerte et d'information des populations (SAIP).

M. Jean Pierre Vogel, rapporteur spécial. – Le système d'alerte et d'information des populations, ou SAIP, initié en 2009, constitue un projet de modernisation piloté par la Direction générale de la sécurité civile et de la gestion des crises, la DGSCGC, visant à mettre en place un système moderne d'alerte et d'information des populations et mettant en réseau les différents vecteurs d'alerte disponibles.

L'alerte a vocation à être donnée en cas de risques exigeant un comportement-réflexe de la part des populations en cas de danger. Le SAIP doit permettre, dans son principe, aux acteurs de la gestion de crise, c'est-à-dire principalement les préfets, les maires et les SDIS, de lancer l'alerte sur un territoire donné en une unique opération, en utilisant un logiciel permettant d'activer différents vecteurs de diffusion. Il s'appuie aujourd'hui sur un réseau de 2 830 sirènes qui devrait en compter plus de 5 000 d'ici à 2020 et constituer, selon la doctrine de la DGSCGC, le « principal vecteur de l'alerte ». D'ici à 2020, il doit être connecté à d'autres vecteurs, tels que la téléphonie mobile, mais aussi aux panneaux à messages variables des différentes collectivités ou encore aux radios, la redondance des moyens d'alerte étant, à juste titre, considérée par la DGSCGC comme un facteur d'efficacité.

Ce projet découle du constat dressé par plusieurs rapports qui ont relevé la nécessité de remanier l'ancien réseau de sirènes, le réseau national d'alerte, ou RNA, construit après-guerre, qui visait à prévenir le risque d'attaque aérienne.

Ce projet, d'un montant total de 81,5 millions d'euros, est donc financé par le programme « Sécurité civile » de la mission « Sécurités ». Il comporte deux phases. La première, qui a été lancée en 2010 et court jusqu'en 2019, porte principalement sur la réalisation du logiciel central et sur l'installation des sirènes dans des « bassins à risques », pour un montant d'un peu moins de 45 millions d'euros. Elle comprend également un volet téléphonie mobile, qui s'appuie aujourd'hui sur une application *smartphone*, portant le nom SAIP, en libre téléchargement. La seconde phase, qui commencera en 2020, devrait, selon la DGSCGC, porter sur la poursuite de l'installation des sirènes et sur la connexion d'autres moyens d'alerte au logiciel central.

Même si le projet SAIP était rendu nécessaire par l'obsolescence du RNA, il est marqué par des choix stratégiques contestables.

Le choix de conserver les sirènes comme principal vecteur de l'alerte apparaît en effet comme une importante erreur stratégique. Le volet « sirènes » concentre 78 % des 81,5 millions d'euros consacrés au SAIP, alors même que leur impact apparaît beaucoup plus faible que celui de la téléphonie mobile, lequel bénéficie pourtant seulement de 11 % des crédits consommés ou prévus pour ce projet.

Les sirènes ne sont quasiment jamais utilisées dans d'autres contextes que ceux des essais hebdomadaires. Les sondages montrent que seule une infime minorité de Français sait comment réagir lorsque les sirènes se déclenchent. Par ailleurs, de nouveaux vecteurs plus efficaces, comme la téléphonie mobile, ont émergé ; ils permettent non seulement d'assurer la fonction d'alerte, mais peuvent également informer les populations concernées en délivrant un message clair. La nature des risques a également changé, et aurait justifié une réflexion plus globale sur la stratégie d'alerte et d'information, qui n'a pas été suffisamment menée.

De même, le volet téléphonie mobile est également marqué par des revirements qui ont conduit à revoir fortement à la baisse ses ambitions initiales. Alors que le ministère de l'intérieur privilégiait initialement le recours à la technologie dite du *Cell Broadcast*, qui devait permettre de diffuser un message sur l'ensemble des téléphones mobiles présents sur une zone d'alerte, cette dernière a été a été remplacée en 2015 par le développement d'une application *smartphone*, dénommée SAIP, en libre téléchargement sur *Apple Store* et sur *Google Play*, pour des raisons principalement budgétaires. L'application *smartphone* apparaît pourtant beaucoup moins efficace, notamment car elle ne fonctionne que si l'utilisateur a effectivement téléchargé l'application, qui n'est elle-même disponible que sur des types précis d'appareils, contrairement au *Cell Broadcast*, qui est fiable et utilisé aujourd'hui dans divers pays – c'est le cas aux États-Unis, aux Pays-Bas, au Japon, en Corée... – et peut être reçu sur tous les appareils correctement paramétrés.

Au-delà des choix stratégiques, la mise en œuvre des deux principaux volets, ceux concernant la téléphonie mobile et celui concernant les sirènes, a connu d'importantes défaillances. La conception de l'application *smartphone*, tant dans la dimension technique que dans la gestion du projet, a été menée un délai trop contraint eu égard à sa complexité, alors même qu'une plus grande anticipation aurait été possible, la téléphonie mobile étant envisagée comme vecteur de l'alerte depuis 2010. L'abandon tardif du *Cell Broadcast* et la volonté du Premier ministre de disposer d'un moyen d'alerte par téléphone avant l'Euro 2016 a en effet fortement contraint les délais de conception de l'application, qui continue à pâtir de certaines lacunes, comme la nécessité qu'elle soit ouverte en tâche de fond, ou la forte consommation de batterie. Par ailleurs, l'application, dont le

coût s'élève à 300 000 euros, n'a pas pu être déclenchée dans un délai raisonnable lors de l'attentat du 14 juillet 2016 survenu à Nice, en raison de défaillances techniques ; je le rappelle, elle ne s'est déclenchée que deux heures après l'attentat.

Il me paraît nécessaire, en plus d'une correction rapide de ces défaillances, qu'une évaluation indépendante de l'application SAIP soit menée d'ici à la fin 2019, afin d'envisager un éventuel retour à la technologie *Cell Broadcast* initialement envisagée.

Toutefois, si l'application *smartphone* devait être maintenue à terme, il me semble également nécessaire qu'elle soit disponible sur tous les types de *smartphones* et que soit faite une publicité plus grande visant à augmenter le nombre d'utilisateurs, aujourd'hui limités à environ 500 000, pour qu'elle constitue un vecteur efficace de l'alerte.

L'atteinte de cet objectif pourrait d'ailleurs faire l'objet d'un indicateur de performance du programme « Sécurité civile ».

La mise en œuvre du volet « sirènes », qui comprend l'installation des sirènes et la conception du logiciel de commande est également marquée par un retard important, de trente-six mois, lié aux difficultés de conception de ce logiciel. Ce retard provient notamment du manque de préparation du projet et de l'absence d'un cahier des charges précis élaboré suffisamment en amont de la notification du marché. Ce raté n'est pas sans rappeler celui d'autres projets informatiques de l'État de plus grande ampleur, comme celui de Louvois au ministère de la défense, celui de Sirhen au ministère de l'éducation nationale, ou encore l'opérateur national de paye.

Il me semblerait donc souhaitable qu'une procédure applicable aux projets informatiques du ministère soit élaborée, exigeant la formulation d'un cahier des charges précis conçu en amont de la notification du marché. Cette procédure pourrait en outre comprendre un éventuel appui de la Direction interministérielle du numérique et du système d'information et de communication de l'État, la DINSIC, dont la capacité à appuyer les projets informatiques complexes a été rappelée dans le rapport de notre collègue Michel Canevet au mois d'octobre 2016.

Tous ces constats me conduisent à recommander, plus globalement, de procéder à un changement doctrinal en renonçant aux sirènes comme vecteur principal de diffusion de l'alerte et de favoriser le développement de vecteurs alternatifs.

Je propose en conséquence que les crédits de la seconde phase de déploiement du SAIP – ils s'élèvent à 36,8 millions d'euros –, qui commencera en 2020 portent bien davantage qu'aujourd'hui sur le financement du volet « mobile », et non plus quasi intégralement sur le déploiement des plus de 2 000 sirènes restantes, dont le nombre pourrait être revu à la baisse.

Mme Catherine Troendlé. – Je partage l'analyse de notre collègue sur l'inefficacité du dispositif ; elle a été prouvée de manière dramatique par l'attentat de Nice.

Je souhaite simplement adresser une mise en garde. Le redéploiement des moyens sur le mobile que Jean Pierre Vogel propose a pour préalable indispensable une bonne couverture en réseaux, notamment en milieu rural. Dans mon département, quatre petites communes sont encore en zone blanche ! Il est donc nécessaire de travailler en interministériel, en mobilisant le ministère chargé du numérique pour compléter le maillage.

M. Albéric de Montgolfier, rapporteur général. – Le sujet est malheureusement d'une actualité brûlante. Il faut trouver un système qui permette l'alerte des populations dans les meilleurs délais. Cela pose des problèmes techniques.

Qu'en est-il à l'étranger ? Nous voyons les limites des sirènes ou de la téléphonie mobile en France. Des pays confrontés à des événements climatiques ou à des tremblements de terre ont-ils conçu ou mis en œuvre des dispositifs d'alerte efficaces dont nous pourrions nous inspirer ? Le Japon a-t-il tiré les conséquences des défaillances après l'accident nucléaire ?

Y a-t-il des réflexions à l'échelon européen sur un système d'alerte commun ? Certes, il existe déjà un numéro européen pour l'accès aux services de secours, le 112. Mais, compte tenu de la mobilité au sein de l'Union européenne, il serait utile d'avoir un système standardisé et compréhensible par l'ensemble des populations.

M. Daniel Raoul. – Les sommes dépensées en matière de téléphonie mobile pour mettre en place un système qui n'a jamais fonctionné, ou alors avec beaucoup de retard – je vous renvoie à l'attentat du 14 juillet –, sont un véritable scandale !

Pour ma part, j'avais proposé d'appliquer la solution retenue par le Japon. Il n'y avait pas besoin d'une application spécifique. Certes, la Direction de la protection civile voulait son propre logiciel ; nous avons vu à quoi cela menait… C'est du gaspillage !

Il suffisait – malheureusement, l'article 40 de la Constitution a été opposé à mon amendement – d'autoriser la géolocalisation en cas d'alerte. C'est tout simple. Les opérateurs sont capables d'envoyer un signal d'alerte à tout le monde.

Dans le système SAIP téléphonie mobile, il faut d'abord télécharger l'application, qui par ailleurs consomme beaucoup de batterie et ne fonctionne qu'avec un délai.

La technique existe. Il suffit que le ministère donne l'ordre, évidemment avec compensation financière, aux opérateurs de géolocaliser les clients dans une zone donnée. C'est ce qui est utilisé au Japon. Je ne

comprends pas pourquoi le ministère s'obstine dans son erreur. C'est absurde !

M. Michel Canevet. – La révolution numérique nous appelle à nous approprier l'ensemble des ressources pour pouvoir développer les dispositifs d'urgence et d'alerte.

Peut-être pourrait-on profiter des possibilités offertes par le déploiement de Galileo – le dispositif est maintenant opérationnel – pour initier un certain nombre d'applications, y compris de géolocalisation, afin d'être plus efficaces en matière de secours.

Je souscris à la proposition du rapporteur spécial sur le recours aux installations téléphoniques. D'ailleurs, cela permettrait peut-être de résorber le problème des zones blanches dans nos départements.

M. Jean Pierre Vogel, rapporteur spécial. – Je recommande non pas de supprimer les sirènes, mais de les concentrer sur les zones à risques. Au SDIS de Rennes, il nous a été indiqué qu'une dizaine ou une quinzaine de sirènes étaient déployées sur la ville de Saint-Malo face aux risques de submersion. Cela peut se comprendre. Mais il faut alors une information suffisante des populations sur les réactions à avoir en cas de déclenchement des sirènes, ce qui n'est pas forcément le cas aujourd'hui.

Au Japon, c'est le *Cell Broadcast* qui est développé. Cela fonctionne très bien. De même, aux Pays-Bas, 25 millions d'euros ont été dépensés sur ce système depuis 2012, pour un parc de 17 millions d'abonnés répartis entre trois opérateurs. Ceci est à mettre en perspective avec les 81,5 millions d'euros qui sont dépensés pour la mise en œuvre du SAIP en France ; ils pourraient aussi permettre de résoudre les problèmes de zone blanche dans notre pays.

Dans mon rapport, j'indique qu'il aurait fallu introduire une disposition législative prévoyant l'obligation pour les opérateurs d'acheminer les communications des pouvoirs publics destinées à l'alerte et l'information des populations.

Les préconisations vont dans le même sens, surtout eu égard aux nouveaux risques, notamment chimiques, bactériologiques, nucléaires, sans parler des attentats et des actes de tuerie de masse.

M. Daniel Raoul. – L'obligation pour les opérateurs existe déjà ; il suffit que le ministère passe commande, moyennant évidemment compensation.

Il faut permettre la géolocalisation sans l'avis abonné. Pour une intervention de ce type, elle devrait être de droit. Inscrivons-le dans la loi.

Mme Catherine Troendlé. – Il faudrait consulter la CNIL, non ?

M. Daniel Raoul. – Non ! En cas de sinistre, on peut géolocaliser les abonnés dans une zone donnée.

M. Philippe Dallier. – Je souhaite obtenir une précision. Permettre à un opérateur de détecter tous les téléphones accrochés à une borne donnée dans un secteur, ce n'est pas la même chose qu'autoriser à géolocaliser l'utilisateur ; on sait ce que Google ou d'autres en font.

M. Jean Pierre Vogel, rapporteur spécial. – La technologie du *Cell Broadcast*, qui a été retenue dans un certain nombre de pays, repose sur de la diffusion ; l'expéditeur du message ne connaît donc pas les destinataires du message.

Dans ce cadre-là, il n'y a pas besoin de légiférer. Cette technologie ne nécessite pas la mise en place d'un annuaire. Elle ne permet pas non plus à l'émetteur de savoir si le message a été bien reçu, car il n'y a pas d'accusé de réception. Il n'y a donc aucune atteinte à la vie privée. Ce n'est pas le cas des SMS géolocalisés, qui nécessitent un annuaire de diffusion.

La commission a donné acte de sa communication à M. Jean Pierre Vogel, rapporteur spécial, et en a autorisé la publication sous la forme d'un rapport d'information.

LISTE DES PERSONNES ENTENDUES

Ministère de l'intérieur

- *Direction des systèmes d'information et de communication(DSIC)*

  - M. Laurent HOTTIAUX, directeur ;

  - M. Vincent NIEBEL, adjoint au directeur.

- *Direction générale de la sécurité civile et de la gestion des crises (DGSCGC)*

  - M. Philippe LEMOING-SURZUR, sous-directeur de la planification et de la gestion des crises ;

  - M. Karim KERZAZI, chef du bureau de l'alerte de la sensibilisation et de l'éducation des publics ;

  - Mme Hélène HALBRECQ, adjointe au chef du bureau de l'alerte de la sensibilisation et de l'éducation des publics.

Airbus

- M. Éric DAVALO, vice-président, directeur de la stratégie, du portfolio et de la R&D, Airbus DS/ SLC ;

- M. Thierry BECKER, directeur Europe de l'Ouest & Afrique, Airbus DS/ SLC ;

- M. Gérard MOISSELIN, conseiller sécurité et territoires du résident d'Airbus Group ;

- Mme Annick PERRIMOND-du BREUIL, directrice des relations avec le Parlement.

Service d'information du Gouvernement

- M. Romain PIGENEL, directeur adjoint au numérique.

Fédération nationale des sapeurs-pompiers de Paris (FNSPF)

- Lieutenant-colonel Christophe MARCHAL, trésorier général.

Deveryware

- M. Stéphane SCHMOLL, directeur général ;

- Mme Delphine ARIAS BUFFARD, directrice des relations institutionnelles.

Déplacement à Rennes

Préfecture d'Ille-et-Vilaine

- M. Christophe MIRMAND, préfet ;

- Mme Agnès CHAVANON, directrice de cabinet ;

- Colonel Pierre PATET, directeur départemental des services d'incendie et de secours (SDIS) ;

- M. Olivier QUEMENER, chef du pôle risques technologiques et infrastructures de la DSC ;

- M. Thomas PAPIN, adjoint au directeur de la Direction de la sécurité civile.