Alerte attentat : quelles solutions pour remplacer SAIP, l'appli défectueuse du gouvernement ?

mercredi 9 août 2017, par Thémis

L'application SAIP, conçue par la société Deveryware pour prévenir la population en cas d'attentat, a été sévèrement critiquée pour son inefficacité dans un rapport du Sénat. Quelles autres solutions pourrait-on mettre en place ?

14 juillet 2016, 22h30. Alors que la promenade des Anglais, à Nice, est noire de monde pour célébrer la fête nationale, un camion fonce dans la foule, faisant 86 morts et plus de 450 blessés. Un mois plus tôt, pour l'Euro 2016, le gouvernement avait lancé SAIP (Système d'alerte et d'information des populations), une application censée envoyer des informations officielles en cas d'attentat, en moins de 15 minutes, pour éviter la confusion et la propagation des rumeurs, comme cela avait le cas le 13 novembre 2015.

Mais ce soir là, SAIP, créé par l'entreprise Deveryware, envoie son alerte à... 1h34, trois heures après les faits, et bien après le déclenchement du Safety Check de Facebook (à 0h25) et du plan ORSEC (Organisation de Réponse de Société Civile, à 0h40). Rebelote deux semaines plus tard. Alors qu'un nouvel attentat a lieu à Saint-Etienne-du-Rouvray, la préfecture décide de ne même pas déclencher SAIP.

Un rapport parlementaire au vitriol

Ces "dysfonctionnements" ont fait l'objet d'un rapport parlementaire d'information, mené par le sénateur Jean-Pierre Vogel (LR) et publié lundi 7 août. Le verdict est sans appel : le système d'alerte attentat est "inefficace" et "doit être revu". "Conçue dans l'urgence", l'application SAIP a présenté de nombreuses "défaillances" : déclenchement tardif à Nice, fausses alertes (en septembre 2016 à Paris suite à un canular, en mars 2017 à Grasse suite à une fusillade qui n'était pas de nature terroriste).

Autre point noir : les autorités n'y ont spontanément pas eu recours. Lors des attaques du Louvre (février 2017) et des Champs-Elysées (avril 2017), elles ont préféré Twitter. Il faut dire que l'application n'avait été téléchargée que 900.000 fois en avril 2017. Or, elle nécessiterait au moins 5 millions de téléchargements pour être efficace.

Le "cell broadcast", l'alerte par les opérateurs télécoms, une piste à considérer

Pour Jean-Pierre Vogel, cela ne veut pas dire qu'il faut jeter SAIP aux oubliettes. Le sénateur préconise d'évaluer d'ici à 2019 sa pertinence, et d'étudier d'autres options, à commencer par le "cell broadcast", ou "diffusion cellulaire".

Cette méthode, déjà employée par d'autres pays, notamment la Belgique, a prouvé son utilité. Elle consiste à envoyer directement des SMS officiels d'alerte et d'information, mais par l'intermédiaire des opérateurs télécoms. L'information touche ainsi tous les abonnés de l'opérateur, qu'ils se trouvent près de la zone de l'attentat ou non. Cela résout le problème de l'application à télécharger.

Le rapport indique que cette solution avait été envisagée en 2011 par le gouvernement, qui réfléchissait à un système d'alerte. Mais son coût de plusieurs millions d'euros a été jugé "non soutenable et non-compatible avec les enveloppes budgétaires existantes". Le projet s'était aussi heurté à la réticence des opérateurs télécoms, car il requiert "de forts investissements pour adapter les logiciels des équipements des réseaux". Autrement dit, les opérateurs télécoms doivent faire preuve de davantage de volonté sur ce dossier.

Les SMS géolocalisés, plus faciles à mettre en place mais moins sûrs

Une autre solution envisagée par le rapport est le recours aux SMS géolocalisés. Ils permettraient d'envoyer un message officiel uniquement aux personnes se trouvant à proximité d'une zone de danger, pour leur donner des consignes (se cacher, partir) et des informations sur la nature de l'attaque.

"La solution de recours aux SMS géolocalisés apparaît rapide et facile à mettre en œuvre", explique Jean-Pierre Vogel. Mais elle comporte aussi des faiblesses : du fait de la saturation des réseaux en cas d'attentat, "la vitesse d'acheminement des messages serait trop faible", pointe le rapport. Cette solution suppose aussi une "agrégation dynamique" des numéros de téléphone présents sur une zone d'alerte, "ce qui peut susciter des interrogations sur la gestion des données personnelles". Enfin, les SMS géolocalisés ne se distinguent pas des autres SMS et ne s'affichent pas forcément sur l'écran d'accueil. C'est pourquoi aucun pays étranger n'utilise cette solution, explique le rapport.

Le système API ou l'information par de multiples sources

Une autre piste, non envisagée dans le rapport, serait de recourir au système API (application programming interface). En cas d'attentat terroriste, le message d'information envoyé par le gouvernement est capté en priorité par les services les plus utilisés par la population, comme Facebook, Twitter, la RATP pour les Parisiens, Météo France, les applications bancaires etc, qui à leur tour propagent l'information, ce qui permet d'informer la population par de nombreuses sources.

Une autre solution très prometteuse de ce type avait été mise sur pied lors du hackathon sécurité organisé par la Mairie de Paris en janvier 2016. Baptisée "API-Alerte", elle a ensuite été testée, avec succès, par Vélib, le service de vélos parisiens. Elle permet en cas de danger de prévenir les personnes à proximité en faisant apparaître sur leur application une icône "Alerte", qui les informe que la zone est dangereuse. Ce système d'alerte pourrait être intégré à n'importe quelle application mobile.

S'inspirer d'Alerte Enlèvement, un dispositif qui fonctionne

Enfin, une autre piste, elle aussi absente du rapport, est de s'inspirer de ce qui marche déjà : le système Alerte Enlèvement, utilisé pour les disparitions d'enfants. Déployé depuis 2006 en France, il permet aux autorités d'envoyer de façon massive à la population un message pour retrouver rapidement l'enfant et/ou son agresseur, en mobilisant les médias TV et web, les réseaux sociaux, les écrans dans les lieux publics et mêmes les panneaux d'autoroute. Il faudrait adapter le dispositif au contexte de l'attentat, mais il a fait ses preuves une vingtaine de fois en dix ans.

Une chose est sûre : le système des sirènes est devenu "totalement obsolète". D'après Jean-Pierre Vogel, il faut "renoncer à la doctrine faisant des sirènes le vecteur principal de diffusion de l'alerte". En partie car les sirènes envoient un message (l'existence d'un danger) qui ne contient aucune information (nature et localisation du danger, attitude à adopter).

Date : 09/08/2017
Source : La Tribune
Auteur : Sylvain Rolland