PRINCIPES DE FONCTIONNEMENT ET DIFFÉRENCES ENTRE LB-SMS ET CB

Rapport technique - Livrable 1.2.a

Partenaires du projet

Avec le soutien financier de

Rédacteurs : Esteban BOPP, Johnny DOUVINET & Margaux DUMONTEIL (UMR ESPACE 7300 CNRS), Amélie GRANGEAT (GEDICOM-F24)

Participants : Aurélien DOUSSERON, Matthieu COULON (ESPACE)

Novembre 2021

Sommaire

Synthèse des résultats obtenus et recommandations

Cette étude a permis de mettre en avant plusieurs constats et de formuler plusieurs recommandations, qu'il faut considérer à l'horizon des JOP 2024, pour améliorer la diffusion de l'alerte à la population en France. Aucune hiérarchie n'est retenue dans les propositions ci-dessous.

CONSTATS	RECOMMANDATIONS
Des confusions sont souvent observées (dans différents médias) entre le LB-SMS et le CB, qui sont pourtant des technologies différentes sur de nombreux aspects.	**Il faut donc accentuer la communication sur leurs différences, à travers différents supports, pour clarifier les principes de fonctionnement de ces deux technologies.**
La vulnérabilité structurelle, le risque de congestion et le risque de piratage sont des risques bien connus et souvent rappelés dans les publications techniques et/ou scientifiques concernant les LBAS.	**Il faut donc redonder les solutions pour en assurer le fonctionnement en cas de catastrophes majeures.**
Au-delà de leur différence technique, le LB-SMS et le CB ne renvoient pas aux mêmes cas d'usage ni aux mêmes droits utilisateurs.	**Il faut donc concevoir une matrice de droits et de responsabilités, pour espérer un usage opérationnel approprié à chaque situation nécessitant l'activation d'une alerte.**

1. Introduction

Cap-4-MultiCan'Alert est un projet de développement expérimental s'inscrivant dans le cadre des Jeux Olympiques et Paralympiques de 2024. Il avait pour but de concevoir une **solution d'alerte innovante**, qui combinerait différents canaux de diffusion, adaptés aux contextes réglementaire et technologique se profilant en France, et qui intègrerait les besoins des utilisateurs finaux et les réactions à attendre des populations. Le consortium, inédit, a été composé de deux industriels (ATRISC et GEDICOM-F24) et deux laboratoires de recherche publics (ESPACE et CHROME).

Dans le même moment, le gouvernement et les autorités compétentes ont avancé sur le développement de la nouvelle solution d'alerte nationale « FR-Alert », attendue au plus tard le 21 juin 2022 sur l'ensemble de la métropole et les territoires d'outre-mer[1]. Comme quelques autres pays de l'Union Européenne, la France a opté pour **une plateforme qui combinera deux technologies** : les SMS géolocalisés (LB-SMS, pour *Location-Based Short Message Service*) et la diffusion cellulaire (CB, pour *Cell Broadcast*). Ces technologies permettent toutes les deux la diffusion de messages textuels d'alerte sur les téléphones des individus, localisés en temps réel, mais leurs modes de fonctionnement diffèrent (Chapitre 2). L'adoption de ce système d'alerte basé sur la localisation des individus (LBAS, pour *Location-Based Alerting System*) marque un tournant majeur dans les choix politiques opérés en France, puisque l'alerte à la population n'est diffusée jusque-là que par les sirènes dites « SAIP » (Système d'Alerte et d'Information des Populations), qui d'ailleurs seront intégrées à FR-Alert en complément des deux nouvelles technologies.

Dans le fonctionnement actuel (Vogel, 2017 ; Douvinet, 2020), **les 2 100 sirènes SAIP couvriraient à peine 29% des résidents** si l'on considère un rayon d'audibilité de moins d'1km. Les 4 500 sirènes de l'ancien RNA (Réseau National d'Alerte, mis en place en 1954 sur ordonnance du Général de Gaulle, mais dont la fin a été officiellement actée en 2010) couvraient de leur côté 42% des résidents en théorie mais étaient tombées en désuétude : seulement 32% des sirènes émettaient encore un signal conforme aux attendus, 35% étaient alimentées par un réseau électrique obsolète. Sur une période de 60 ans, les sirènes ont réellement été activées moins de 10 fois (Douvinet, 2020). C'est en comparaison à ce mode de diffusion de l'alerte en France que seront présentés ci-après les avantages et la plus-value des LB-SMS et du CB (Chapitre 3). Seront ensuite évoquées les limites et pistes d'améliorations de ces deux technologies (Chapitre 4).

[1] Annonces du Ministre de l'Intérieur, G. Darmanin, lors de son discours du 24 septembre 2020.

2. Les technologies de l'alerte géolocalisée

2.1. Les méthodes de localisation des téléphones

La localisation des individus peut se faire par bornage GSM, par technologie cellulaire, par localisation satellitaire, ou par Internet (Küpper, 2005). La localisation par satellite (GNSS, pour *Géolocalisation et Navigation par un Système de Satellites*) est la première technique de géolocalisation à avoir été utilisée au début des années 1960 (Aloudat, 2010). Le GPS (*Global Positioning System*) a été lancé en 1964, pour une utilisation militaire, avant d'être disponible dans le domaine civil à partir des années 1990. Ce système a permis le développement d'une grande diversité d'applications, comme par exemple les services d'urgence pour localiser des individus en difficulté (Spiekermann, 2004). Le récepteur détecte plusieurs satellites (au moins 4) dont les positions sont connues avec précision. Il mesure la distance qui le sépare de ces satellites, ce qui lui permet de connaître la position, l'altitude, sa vitesse de déplacement et l'heure.

De leur côté, les technologies cellulaires utilisent des stations (des antennes de télécommunication) qui communiquent avec le récepteur cible situé à l'intérieur d'une cellule. Chaque antenne est rattachée à une cellule qui lui est propre et dont la surface varie ; la méthode d'identification cellulaire (« Cell-ID ») consiste ainsi à récupérer les identifiants des antennes auxquelles le terminal est connecté. La connaissance de la position de l'antenne permet alors de localiser le terminal à l'échelle de la cellule. Le Cell-ID est la principale technique utilisée mais d'autres méthodes existent comme par exemple la triangulation, qui est plus précise (Ahriz Roula, 2010).

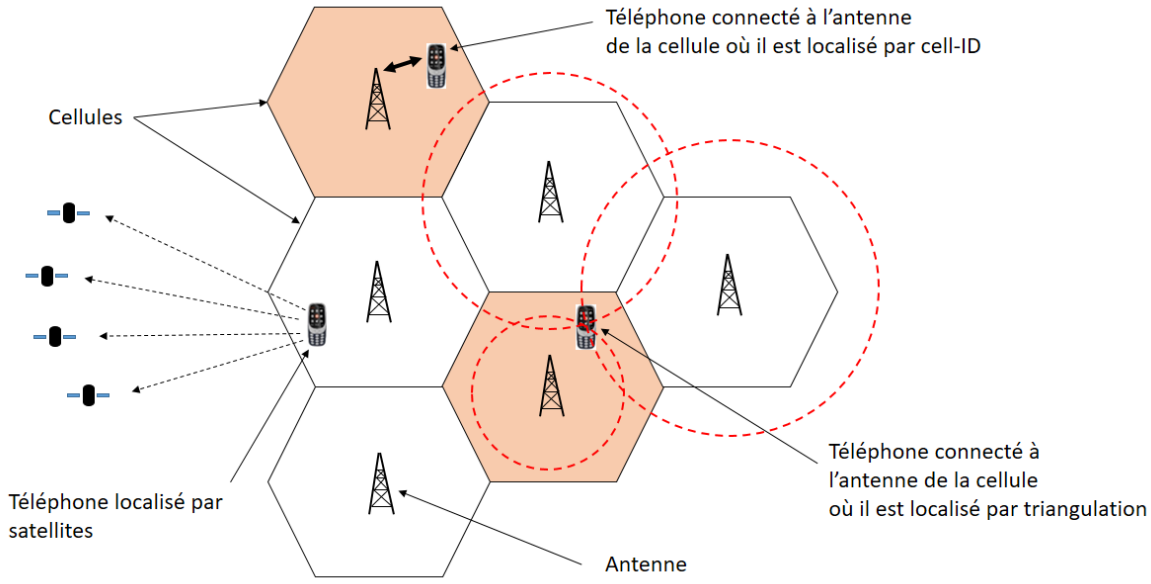

Figure 1. Illustration de trois méthodes de géolocalisation des téléphones

Le CB et le LB-SMS reposent tous les deux sur ces méthodes cellulaires de localisation des téléphones, ce qui explique peut-être qu'ils sont souvent confondus (Vogel, 2017 ; Santoni, 2021). Pourtant, le mode de diffusion des messages et la couverture de l'alerte diffèrent entre ces deux technologies. C'est ce que nous allons voir en détail ci-après.

2.2. La diffusion cellulaire, ou *Cell Broadcast* (CB)

La diffusion cellulaire (*Cell Broadcast*) consiste en la diffusion d'une notification dans une zone appelée « zone de diffusion cellulaire » (ETSI, European Telecommunication Standard Institute, 1996). Cette technologie est opérationnelle depuis 1997 (Udu, 2009), et elle ne nécessite pas la connaissance préalable des numéros des téléphones cibles (Aloudat and Michael, 2011; Aloudat et al., 2007). Le message passe par les antennes de télécommunication sous formes d'ondes radio via un équipement dédié au CB, puis il est ensuite diffusé à tous les mobiles situés dans la cellule : on parle ici d'un mode de diffusion « *point-to-area* » (Sillem, 2006; Choy et al., 2016). Son spectre a une capacité d'environ 64 000 canaux différents, avec possibilité de dédier un canal à chaque type de message (Aloudat, 2010; Chochilouros et al., 2008). Par conséquent, le CB n'est pas soumis au risque de congestion comme peuvent l'être les messages diffusés sur les canaux traditionnels de télécommunication (Jagtman, 2010; Sillem et al., 2006).

Le principal avantage du CB est de pouvoir alerter rapidement un nombre élevé d'individus (Jagtman, 2010; Jayasinghe et al., 2006; Song et al., 2014). La connexion à un **réseau spécifique** (fonctionnant uniquement sur la 4G pour la France) est nécessaire (**Figure 2**). L'unité de base pour la zone de diffusion est la cellule (espace couvert par une antenne relais), mais la zone de diffusion peut inclure plusieurs cellules, ce qui permet de diffuser l'alerte sur de larges emprises spatiales (Sillem and Wiersma, 2006). Le téléphone doit néanmoins être en capacité de supporter la technologie pour pouvoir recevoir des notifications (Samarajiva and Waidyanatha, 2009), ce qui est le cas des smartphones iOS > 6 ou Android > version 11 en France. Les notifications peuvent être accompagnées d'une alarme sonore, qui ne s'arrête qu'une fois le message vu par l'utilisateur, y compris si le téléphone est en mode veille ou en mode avion. Le CB permet aussi de détecter la nationalité des utilisateurs des smartphones via leur numéro de téléphone, et donc d'adapter l'alerte, traduite dans la langue de l'utilisateur. Par ailleurs, l'autorité émettrice est en capacité de paramétrer à l'avance l'heure de diffusion du message.

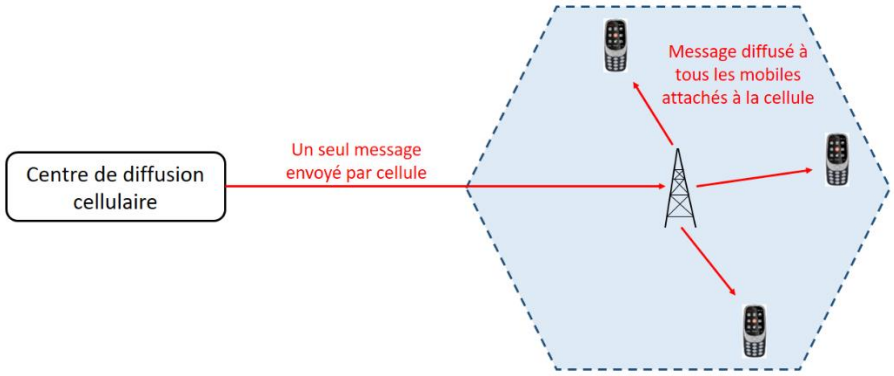

Figure 1. Architecture d'une alerte diffusée par CB (modifié d'après BEREC, 2019)

En revanche, il n'est pas possible pour l'émetteur de savoir combien d'individus ont reçu et lu le message d'alerte, contrairement aux SMS géolocalisés. Un individu sortant de la zone de diffusion cellulaire (ou zone d'alerte) ne sera pas non plus averti ; il n'a donc aucun moyen de savoir s'il est en sécurité (sauf précisions dans le contenu du message, sur la localisation d'un abri par exemple). Le CB a aussi pour limite que tous les téléphones mobiles ne sont pas compatibles et qu'une défaillance technique pourrait toucher le centre de diffusion cellulaire (Song et al., 2014). En dernier lieu, le CB ne doit pas être utilisé en cas d'attaque terroriste car le son émis par le téléphone portable lors de la réception du message pourrait révéler la position d'individus cachés.

2.3. Les SMS géolocalisés (LB-SMS)

Le SMS géolocalisé (LB-SMS pour « *Location-Based Short Message System* ») permet l'envoi d'un SMS à n'importe quel téléphone situé dans une zone prédéfinie comme « zone d'envoi » (Leo et al., 2015). Le SMS passe par les réseaux traditionnels (2G, 3G, 4G et plus) via les antennes relais identifiées dans la zone à alerter par le Centre SMS (**Figure 3**), puis il est délivré à chacun des téléphones autour des antennes sélectionnées : on parle d'un mode de diffusion « *point-to-point* » (Sillem, 2006). Comme le CB, l'unité de diffusion de base est la cellule, et la zone d'alerte peut englober plusieurs antennes. En revanche, contrairement au CB, il n'est pas nécessaire d'avoir une infrastructure spécifique ; le coût de mise en œuvre est donc faible. Sur le plan technique, le LB-SMS comporte deux avantages majeurs (Akanmu and Rabiu, 2012; Bonaretti and Fischer-Preßler, 2021). Par un recensement des cartes SIM, les acteurs de l'alerte peuvent savoir combien d'individus ont reçu le SMS sur différentes échelles de temps, et ils peuvent envoyer plusieurs SMS successifs, ce qui permet d'informer clairement de la fin de crise par exemple (alors que les sirènes se limitent à un signal sonore).

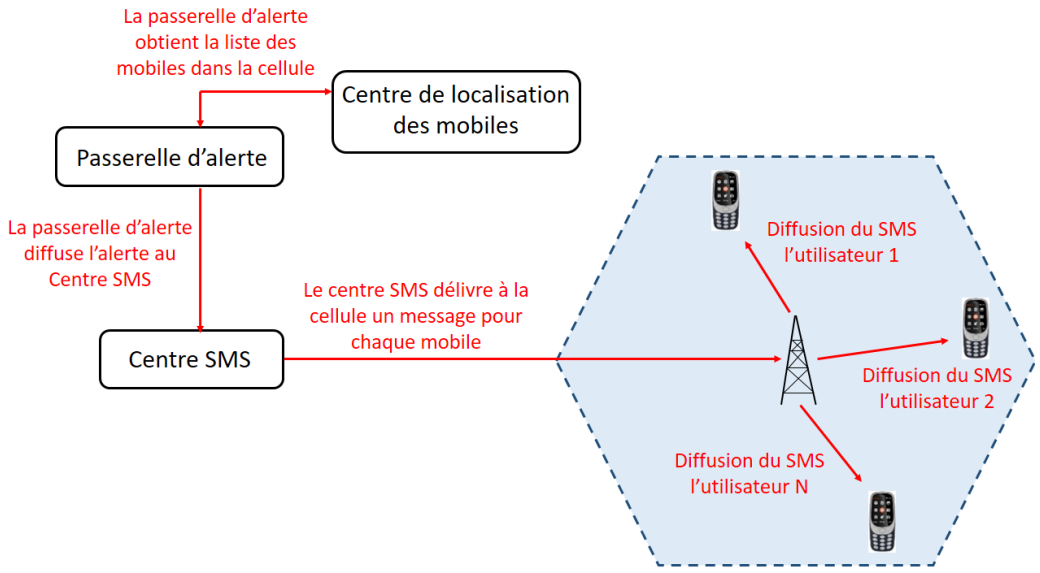

Figure 3. Architecture d'une alerte diffusée par LB-MS (modifié d'après le rapport du BEREC, 2019)

Vu son principe de fonctionnement, le LB-SMS est toutefois sensible au risque de congestion, ce qui est problématique, d'autant plus que les périodes de crises sont caractérisées par une forte augmentation de la communication (Pries et al., 2006). Ce risque est en réalité lié à l'envoi de « paquets » de SMS envoyés par les opérateurs, et du nombre d'individus rattachés aux antennes de télécommunication. C'est pourquoi le nombre de personnes pouvant être alertées simultanément n'est pas aussi important qu'avec le CB. En revanche, la consommation de bande passante d'un SMS est faible et le risque de congestion n'est à considérer que dans les cas où il faudrait alerter en même temps un grand nombre de personnes. Si le réseau est temporairement indisponible, le message est stocké puis délivré quand le réseau redevient disponible (Aloudat, 2010). Ainsi, le LB-SMS est un outil d'alerte efficace localement ou quand le nombre d'individus à informer est limité mais son usage est en revanche déconseillé pour une diffusion à large échelle ou quand les individus à alerter son très nombreux.

Commentaires de l'équipe projet : Le CB ou LB-SMS sont deux technologies de diffusion cellulaire, mais elles ne reposent pas du tout sur les mêmes infrastructures et n'ont pas les mêmes avantages ni les mêmes inconvénients. Le choix annoncé en France (une solution hybride) doit permettre de pallier les limites identifiées pour chacune d'entre elles.

3. Avantages et attendus du CB et du LB-SMS

Dans le cadre du projet Cap Alert, une étude des apports et des limites des LBAS a été menée en intégrant différentes dimensions, à savoir le volet humain, social, contextuel, organisationnel et opérationnel. Ici, on se focalise essentiellement sur des avantages techniques.

3.1. Alerter plus vite, plus précisément, plus massivement

Grâce à la forte démocratisation de la téléphonie mobile et des outils de géolocalisation, il est désormais possible de diffuser des alertes à la population de façon à la fois plus ciblée et plus intensive. En 2018, un message test CB, envoyé par les autorités étatsuniennes, a atteint 75% de la population du pays, soit près de 180 millions d'individus. Aux Pays-Bas, 85% de la population ont pu être atteints lors d'un test en 2019 (soit environ 12,6 millions d'individus). Il s'agit là de chiffres importants, notamment dans les pays où la couverture spatiale des sirènes est insuffisante pour faire de l'alerte massive. La géolocalisation des individus à l'échelle de la cellule garantit également une précision spatiale assez fine des alertes (**Figure 4c**). La plus petite zone d'alerte est la cellule pour les LBAS cellulaires (CB ou LB-SMS) et quelques mètres carrés pour les prototypes d'alerte par satellite (solutions à l'état de prototypes actuellement). Cela limite le nombre d'individus qui reçoivent une alerte alors qu'ils sont situés hors de la zone de danger ainsi que le nombre d'individus qui sont situés dans la zone de danger, mais qui ne reçoivent pas l'alerte. Il est également possible de différencier le contenu du message selon l'endroit où est situé l'individu (toujours à l'échelle cellulaire). Ainsi, il peut être demandé à un individu situé proche du danger d'évacuer, mais à un autre individu situé plus loin du danger de se confiner (et inversement). Pour cela, il faut que les autorités délimitent un zonage de l'alerte.

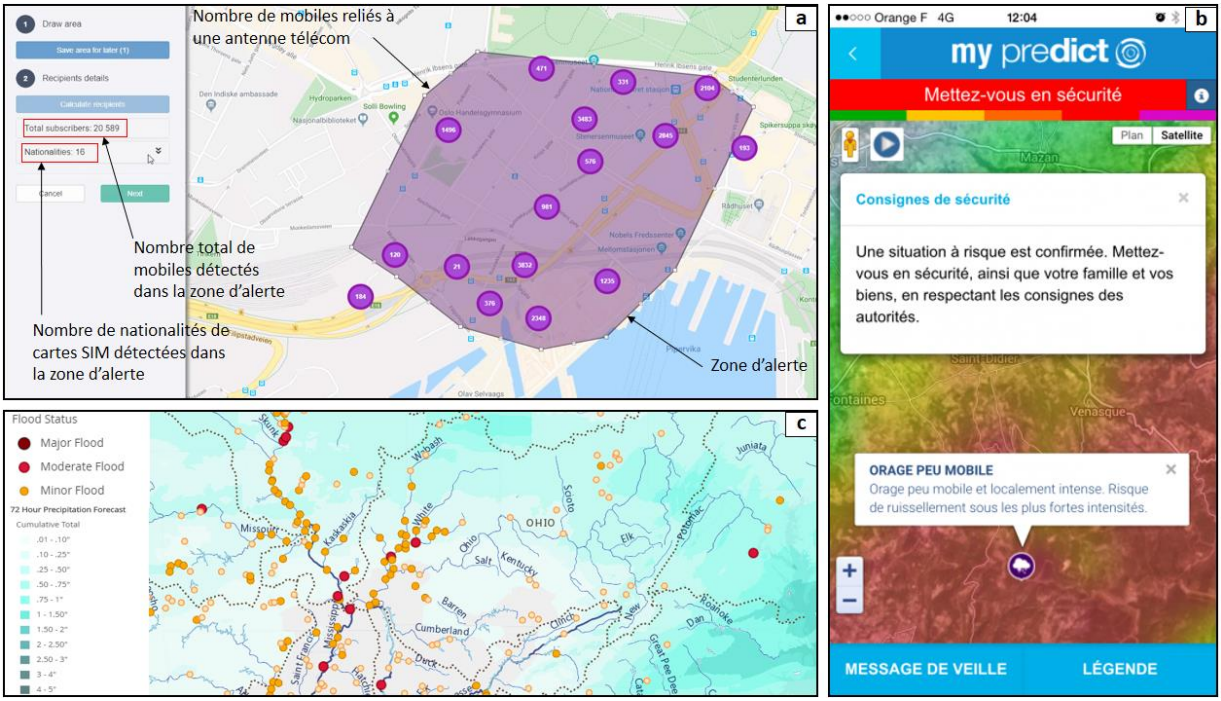

Figure 4. Trois visuels de géolocalisation pour l'alerte : a) capture de la plateforme de lancement d'alerte d'Everbridge® ; b) localisation d'un aléa avec des consignes associées sur l'application MyPredict® ; c) USA Flood Map de Esri®, plateforme de suivi des précipitations et des crues

De plus, le LB-SMS donne la possibilité de connaître avec exactitude le nombre d'individus atteints, et ceux qui n'ont pas reçu le message. Dès que les individus reçoivent l'alerte, l'information remonte vers les autorités impliquées par un recensement des cartes SIM. Les autorités peuvent alors renvoyer plusieurs fois l'alerte vers ceux ne l'ayant pas reçu jusqu'à ce qu'ils l'aient vu. En dernier lieu, il est possible d'alerter en temps réel les individus pénétrant dans la zone d'alerte et ceux qui en sortent (**Figure 4a**).

3.2. Accompagner l'alerte d'un message d'information

Du côté des citoyens, les messages reçus grâce aux LBAS sont plus riches d'information que le signal sonore d'une sirène (Sillem et al., 2006). La langue des messages d'alerte peut varier en fonction de la nationalité de la carte SIM de l'utilisateur. Des illustrations (photographies et cartes localisant le danger) et liens de redirection peuvent également être diffusés (notamment via une application mobile). Cela augmente la richesse des informations mises à disposition des individus confrontés à une situation de danger (**Figure 5**). En 2019, une étude menée par Grant et Smith à l'université de Hull a démontré que la localisation de la zone affectée par un danger était l'élément le plus important que les individus souhaitent voir dans un message texte (60% des participants à un test sur la diffusion d'une alerte CB le souhaitaient). Selon l'enquête menée du 12 au 17 novembre 2020 au sein d'Avignon Université, 94% des enquêtés ont déclaré souhaiter avoir la localisation du danger dans le message d'alerte. Les autres contenus jugés importants lors du test CB à l'université Hull sont intéressants : 58% des participants souhaitent avoir des informations sur la sévérité de la menace, 51% sur les consignes à tenir et 40% sur la durée de la crise (Grant and Smith, 2019). Par ailleurs, le recours aux capteurs connectés accroit la qualité des prévisions sur l'aléa, voire assure un suivi en temps réel de la situation sur le terrain.

3.3. Des premiers retours opérationnels concluants

En complément de l'étude rendue en parallèle en juillet 2020 pour le CHEMI (qui avait pour but d'étudier plus en détails les pratiques observées aux USA, en Belgique, en Indonésie et en Australie), nous avons étudiés les retours aux Pays-Bas, qui ont été le 1er pays européen à se doter de la technologie CB (Udu, 2009). Des tests effectués entre 2005 et 2007 ont montré des taux de pénétration faible au départ (entre 0 et 29% des mobiles visés selon les tests), expliqués par des erreurs dans la diffusion de certains messages et des téléphones peu compatibles (Jagtman, 2010). Après corrections, des tests réalisés en 2008 ont affiché des taux de pénétration meilleurs (72% ; Jagtman, 2010). En 2012, les États-Unis ont lancé le « *Wireless Emergency Alerts* » qui permet de diffuser des alertes via CB. Ce système a été intégré dans IPAWS (*Integrated Public Alert and Warning System*) et il a été utilisé pour la première fois, avec succès, en 2012 lors d'un « *Tornado Warning* » à Elmira proche de New York (GSMA, 2013). La même année, la ville de New York a utilisé IPAWS lors du passage de l'ouragan Sandy (Scott, 2016).

La Belgique a fait le choix du LB-SMS suite aux attentat de Bruxelles en 2016, et a acté l'abandon des sirènes, avec un démantèlement progressif sur l'année 2018 (Douvinet, 2020). En novembre 2017, un SMS a été envoyé à tous les individus situés dans un rayon de 20km autour de la ville de Drogenbos, où un conteneur de batteries lithium était en feu (Douvinet, 2020). En octobre 2019, un test grandeur nature a été réalisé au cours duquel plus de 400 000 SMS, 50 000 appels vocaux et 120 000 emails ont été envoyés, et impliquant 204 communes. De nombreuses communes ont affiché un taux de réussite technique à 99,9% (en nombre de téléphones mobiles atteints). Seules quatre communes (Comines-Warneton, Estines, Wemmel, Wezembeek-Oppem) ont présenté des chiffres légèrement plus faibles (de 93 à 99,9%).

En Australie, *l'Emergency Alert* a été utilisé dès 2011 lors d'inondations qui frappèrent l'État du Queensland (Brisbane City Council, 2011). Malgré un message insuffisamment explicite (ce qui a engendré des phénomènes de confusion et de panique), le recours au SMS d'alerte est aujourd'hui une solution largement utilisée dans ce pays. Le système a d'ailleurs été utilisé plusieurs fois en 2020, lors des incendies en janvier 2020 et des inondations en juin 2020.

En Suisse, l'application mobile *Alertswiss*® a été développée pour compléter les 7700 sirènes nationales. Un test national impliquant la diffusion d'une alerte sur l'ensemble des canaux (sirènes, application SwissLife, et site internet) a eu lieu en 2019. L'application compte plus de 100 000 téléchargements en 2020 d'après GooglePlay®. Un nouveau test a été effectué en 2020 durant lequel 98% des sirènes ont bien fonctionné mais des retards de diffusion de l'alerte sur l'application ont été notés. En Allemagne, l'application Katwarn® est utilisée pour alerter la population depuis 2016. Lors de la fusillade du 22 juillet 2016 à Munich, l'application a diffusé un message demandant à la population de se confiner chez elle, et elle a été utilisée plus de 50 fois lors de l'épidémie de la COVID-19.

3.4. Autre avantage en amont : réduire le délai d'activation

Les LBAS permettent aux autorités d'envoyer une alerte de manière « plus rapide et plus massive ». La rapidité de diffusion des messages via le CB ou le LB-SMS est associée au développement d'une interface accessible via n'importe quel ordinateur ou smartphone et d'une bibliothèque de modèles créés à l'avance. Dès lors, les autorités peuvent, en quelques minutes, adapter un modèle et diffuser l'alerte à la population ciblée (Nagarajan et al., 2012). Lors du colloque Cap'Alert organisé en 2019 à l'Université d'Avignon, l'un des membres du Centre de Gestion de crise en Belgique nous avait confié qu'avec son smartphone, il avait la possibilité d'envoyer un SMS d'alerte (sur ordre d'une autorité compétente) à tout ou partie de la Belgique, en moins de 5 minutes. Des tests réalisés à Avignon en janvier 2021 (journée d'expérimentation du projet Cap-4-MultiCan'Alert) ont montré la rapidité dans la réception et la diffusion d'un SMS auprès d'étudiants et personnels de l'université (quelques secondes pour l'envoi et la réception d'un message préenregistré)[2].

En cas d'extrême urgence, les LBAS peuvent aussi supprimer le temps nécessaire à la validation de la prise de décision. En cas de tremblement de terre par exemple, Alphonsa et Ravi (2016) ou Auclair et Bertil (2008) ont montré qu'une alerte automatisée déclenchée par un réseau de capteurs sismiques pouvait atteindre la population quelques secondes avant l'arrivée d'un séisme, grâce à la détection des ondes S (ondes non détectables par un humain mais qui se déplacent plus rapidement que les ondes P destructrices). L'alerte automatisée (sans prise de décision humaine) reste néanmoins rare et réservée à des risques ayant une cinétique ultra rapide. Même lorsque la technologie permet cette automatisation et malgré le bénéfice de rapidité, les autorités peuvent choisir, politiquement, de ne pas supprimer l'intervention humaine de leur système d'alerte. En Indonésie, bien que le BMKG, le bureau chargé de la surveillance des aléas météorologiques et géodynamiques, dispose d'un outil appelé « *Warning Recifal System* », qui permet d'envoyer automatiquement des SMS dès qu'un aléa à cinétique rapide est détecté (typiquement un tsunami), la validation humaine de la détection de l'aléa doit être néanmoins faite par un centre opérationnel en veille permanente.

[2] Pour en savoir plus sur les expérimentations menées dans le cadre du projet Cap Alert, nous vous invitons à lire les livrables du Work Package 2, et en particulier le livrable 2.5.a sur les journées de test à Avignon Université.

3.5 Autre avantage en aval : inciter encore plus les individus

En l'état actuel, les LBAS restent utilisés comme des outils d'alerte « *top-down* », parfaitement adaptés à l'organisation nationale et pyramidale des systèmes d'alerte à l'échelle mondiale. Les citoyens sont cantonnés dans un rôle de « simple récepteur », même s'ils disposent avec leur téléphone d'un pouvoir de communication considérable et souvent sous-estimé par les acteurs opérationnels. Mais le recours aux moyens d'alerte géolocalisée pourraient renverser les codes, ou du moins, rendre possible la structuration d'une d'alerte montante qui ne viendrait pas des prévisionnistes, mais des citoyens eux-mêmes. D'autant plus que les habitants, travailleurs, et autres usagers sont les premiers témoins et observateurs des phénomènes impactant leur territoire.

La recherche scientifique s'est attachée à mettre en avant ce potentiel. Dès 2007, Goodchild introduit le concept de citoyen-capteur et de VGI (« *Volunteered Geographic Information* ») qui traduit la capacité des citoyens à remonter des informations à travers leurs téléphones mobiles ou divers médias sociaux (Goodchild, 2007). Les médias sociaux en gestion d'urgence (MSGU, SMEM en anglais) sont un champ scientifique largement étudié depuis les années 2010 (Alexander, 2014; Cao et al., 2018; Cavalière et al., 2016; De Longueville et al., 2009; Laverdet et al., 2018 ; Houston et al., 2015 ; Martin and Blay, 2014; Wellington Region Emergency Management Group, 2012)). Preis et al. (2013) ont démontré que les médias sociaux pouvaient être un excellent indicateur de l'intensité d'un phénomène. En se fondant sur le cyclone Sandy au moment où il impacta le New Jersey (USA) en 2012, les chercheurs ont observé une corrélation entre la chute de la pression atmosphérique et l'augmentation du nombre de photos publiées sur le média social Flickr® (**Figure 5a**). Ils ont ainsi démontré qu'il est possible de calculer l'intensité d'un phénomène naturel au travers des réactions qu'il suscite dans les médias sociaux.

Il est donc possible d'exploiter ce genre d'information pour améliorer la précision des alertes montantes, sans nécessairement modifier les doctrines en place, ni la verticalité du système d'alerte. Il faut pour cela mettre en place des outils de communication officiels (application smartphone, comptes dédiés sur les réseaux sociaux) afin de capter les informations provenant du terrain et des individus.

Certaines applications mettent d'ailleurs le citoyen au cœur du dispositif d'alerte : on parle d'applications « proactives » (Bopp et al., 2019 ; Kouadio, 2016) par opposition aux applications informatives (qui se limitent à diffuser une information aux personnes les ayant téléchargées). La plupart de ces applications proactives guident l'utilisateur dans les remontées d'informations (**Figure 5b**). L'utilisateur choisit l'aléa qu'il est en train d'observer, puis il peut ensuite décrire l'intensité et prendre une photo pour l'illustrer. Souvent, ces applications proactives localisent automatiquement la remontée d'informations (Santoni, 2021). Elles contribuent ainsi à augmenter les ressources et données disponibles pour les gestionnaires, et à augmenter leur conscience situationnelle (avec une appréhension d'un événement à distance ; **Figure 6**). Les individus, s'ils en ont conscience, seraient alors investis d'un rôle actif durant les crises, ce qui pourrait améliorer la conscience collective des risques (Gourine, 2013).

Commentaires de l'équipe projet :
Le recours aux LBAS apparaît comme une solution efficace au vu des retours d'expérience collectés. Si les premières utilisations ont révélé certains problèmes (paramétrage des antennes-relais, contenu des messages), ces systèmes centrés sur la localisation sont aujourd'hui inévitables, tant les avantages sont indéniables, ne serait-ce qu'en termes de population atteignable et de temporalité d'alerte.
Pour plus d'informations sur les systèmes d'alertes mis en œuvre dans différents pays, nous vous invitons à lire les livrables 1.2.b (Etat des lieux et études de cas) et 3.1.a (rapport pour le CHEMI), ainsi que le livrable 1.1 (interfaçage avec le standard *Common Alerting Protocol*).

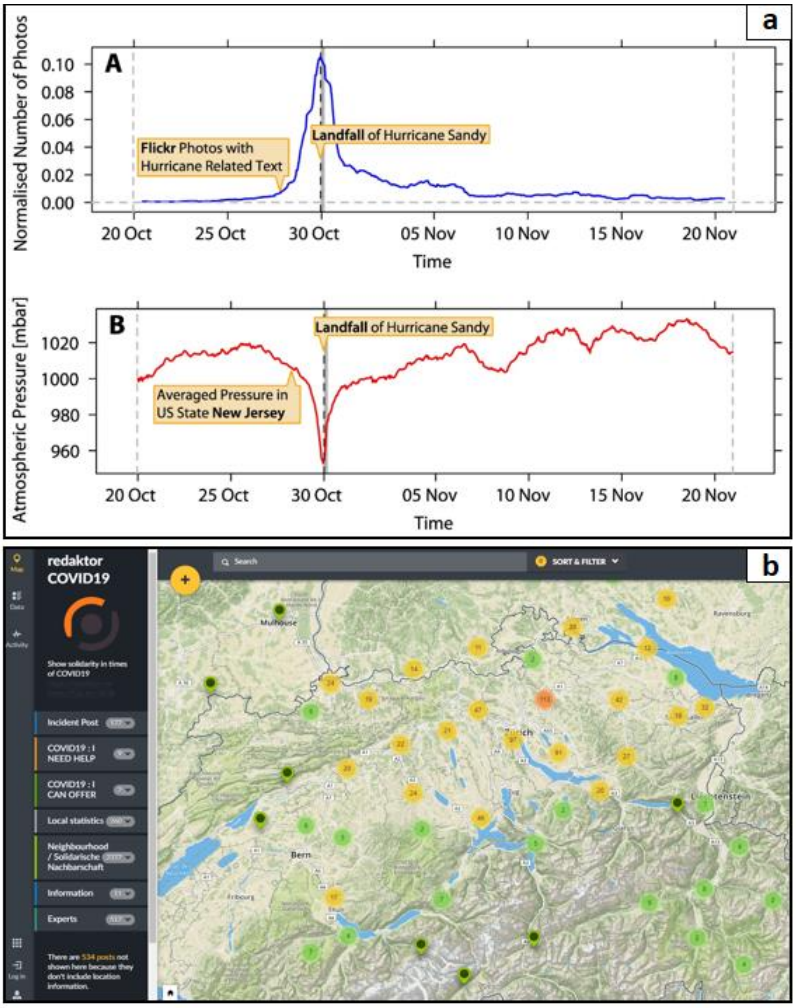

Figure 5. Deux exemples de remontée d'information à travers les réseaux sociaux :
a) Corrélation négative des courbes de pression de l'ouragan Sandy et des photos de l'évènement postées dans Flickr® (Preis et al., 2013)
b) Capture d'écran de la plateforme Ushahidi lors de la pandémie du Covid-19 en Suisse.

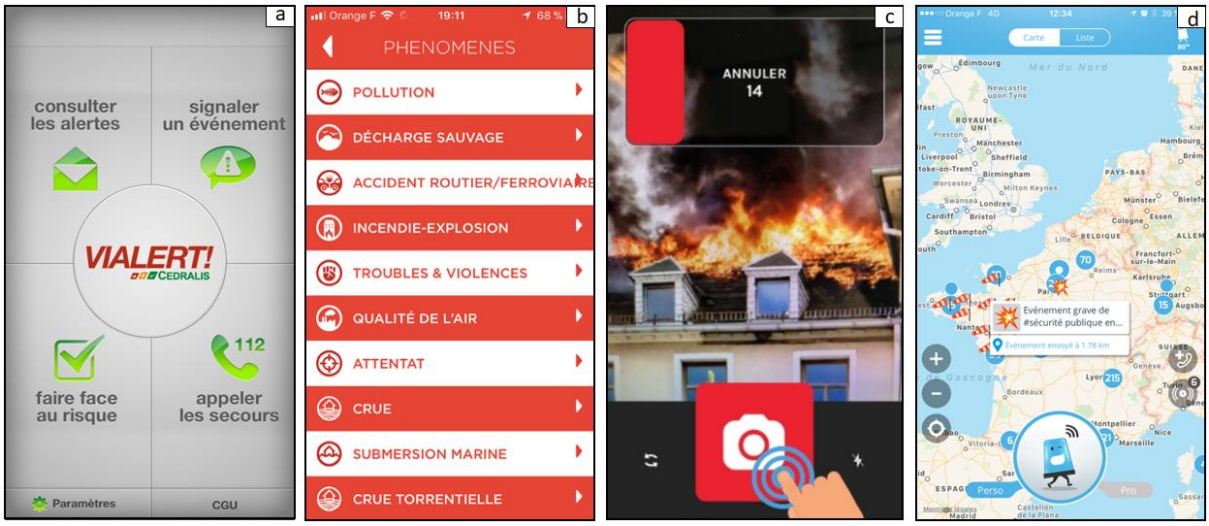

Figure 6. Exemples d'interface via une application mobile :
a) Interface d'accueil de l'application Vialert® ; b) Choix des aléas sur l'application Signalert® ;
c) Photographie de l'aléa sur l'application Swelp® ; d) Géolocalisation des remontées d'autres utilisateurs sur l'application Quidam®

4. Des solutions perfectibles

Malgré les nombreux avantages des LBAS relevés dans cette étude, il est également important de mettre en lumière certains éléments qui restent à améliorer. Des points d'ouverture et de discussions sont aussi mis en exergue, pour cette fois-ci dépasser une lecture purement technique.

4.1. Des solutions vulnérables

Une vulnérabilité structurelle importante

Les LBAS dépendent du maintien opérationnel de plusieurs réseaux (électriques, Internet, antennes de télécommunication), or ces derniers restent vulnérables aux aléas. Durant l'ouragan Irma qui frappa Saint-Martin les 5 et 6 septembre 2017, l'ensemble des communications Internet et mobiles furent impossible car les réseaux électriques et les réseaux de télécommunications avaient été touchés (Moatty et al., 2019; Rey et al., 2019). La coupure a duré de quatre jours à trois mois selon les endroits. Il s'agit là d'un problème majeur dans l'utilisation des réseaux numériques en période d'urgence (Douvinet et al., 2017). Paradoxalement, ce sont d'anciens moyens de communication qui sont les plus fiables juste après une catastrophe, et notamment les communications par ondes radio (Higgins and Smith, 1985). Ces solutions ont déjà été testées avec succès pour la communication post-catastrophe (Hajdarevic and Konjicija, 2015; Nollet and Ohto, 2013). Gaël Musquet, cofondateur de l'association Hand (*Hackers Against Natural Disasters*) affirmait dans Ouest-France[3] au retour d'une mission à Saint-Martin que : « *Dès qu'il n'y a plus d'énergie, toutes les communications sont rompues. Avec des moyens simples comme la radio amateure ou des antennes mobiles rapides à monter et exploiter, en communicant par satellite, il est possible d'éviter de telles situations, à moindre coût* ».

L'effet « mise en réseaux » des Technologies d'Information et de Communication (Weill and Souissi, 2010) accroît aussi cette vulnérabilité structurelle. La vulnérabilité des réseaux de communication face aux aléas se manifeste le plus souvent par une coupure de l'alimentation électrique occasionnée par des dégâts sur les infrastructures dont elle dépend (Kwasinski and Krein, 2007). Cette vulnérabilité varie selon les aléas. Une étude de l'OCDE affirme qu'en cas de crue historique de la Seine, un quart des infrastructures électriques pourraient être impactées en Ile-de-France, la surface d'impact étant 1,5 fois supérieure à la surface inondée (OCDE, 2014). Cette vulnérabilité structurelle est d'autant plus importante que les réseaux de télécommunication constituent un système de système, et un seul point de vulnérabilité suffit à porter atteinte à l'entièreté du réseau (Kwasinski, 2010).

Kwasinki (2010) suggère d'identifier les principaux points de faiblesses, pour y mettre en place une diversification en alimentation électrique via des générateurs. En région Sud-PACA 33,4% des antennes de télécommunication sont situées en zone inondable. Cette vulnérabilité doit être prise en compte et les points de vulnérabilité des réseaux doivent être identifiés afin de les redonder. C'est ce que s'attache à faire l'application locale de la Directive Inondation, mais les collectivités ont plusieurs fois remonté des difficultés à discuter de ces questions avec les gestionnaires de réseaux (Bopp, 2021) et l'inondation n'est pas le seul aléa menaçant les réseaux électriques et les réseaux de télécommunication.

[3] Ouest-France, consulté le 30 mars 2020 : https://www.ouest-france.fr/normandie/catastrophes-un-normand-saint-martin-5489923.

Des risques de congestion qui subsistent dans les grandes agglomérations

Si le CB n'est pas soumis à la congestion des réseaux de télécommunication, le LB-SMS, lui, y est très vulnérable. Sans aller jusqu'à une impossibilité totale de diffuser des messages SMS d'alerte, le temps d'acheminement du SMS vers le mobile dépend du nombre d'individus devant être alerté sur chaque cellule. Ainsi, la congestion est davantage un problème de temporalité de diffusion de l'alerte que de nombre d'individus alertés. Une application mobile peut également être soumise au même problème, d'autant que la consommation en bande passante est nettement supérieure pour faire fonctionner une application que pour recevoir un simple SMS. Ces problèmes peuvent limiter l'utilisation de ces solutions à grande échelle ou dans un délai très rapide, au contraire du CB. L'envoi le 17 mars 2020 d'un SMS d'alerte sur les dangers liés au Covid-19 par le gouvernement français a été délivré de manière très inégale parmi la population, et le temps d'acheminement a pris entre 6h et 24h (estimations observées mais non validées par les opérateurs). En fonction des opérateurs, des décalages de plusieurs heures peuvent être constatés, tout en sachant que ceux-ci peuvent prendre la décision d'échelonner la diffusion des messages SMS, sans l'indiquer publiquement.

Afin de voir si des différences existaient spatialement, nous avons cartographié les risques de congestion à l'échelle de la région Sud-PACA (**Figure 7**), en fonction du nombre d'individus résidant dans chaque cellule. Les estimations des risques de congestion ont été déterminées pour chaque antenne-relais via la méthode des polygones de Voronoï (Audric et al., 2018). La grande majorité des cellules ne présentent pas de risque, mais celui-ci existe dans certaines, densément peuplées, situées dans les principales agglomérations (Marseille, Toulon, Cannes). Plus la densité de population est élevée, plus la superficie couverte par les cellules doit être faible, pour éviter le rattachement d'un grand nombre d'individus à une antenne. Cela nécessite donc un maillage resserré dans les grandes agglomérations.

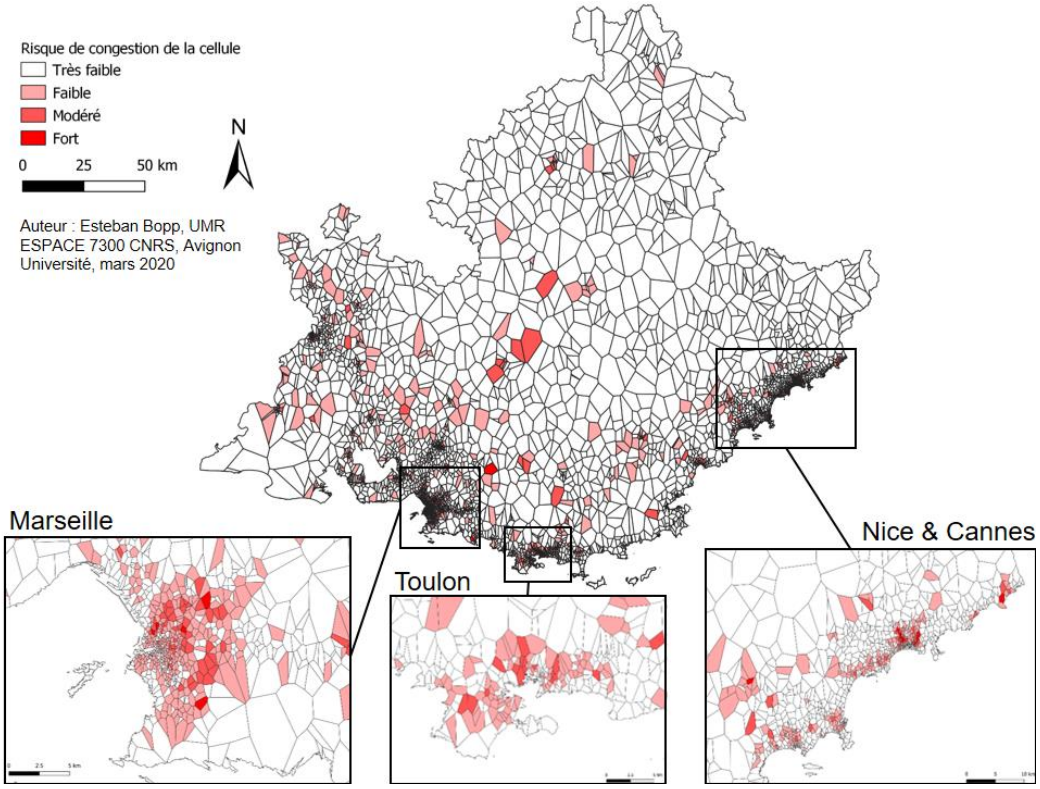

Figure 7. Risque de congestion des cellules de télécommunication en région PACA

Alerte manquée et fausse alerte

Sans pouvoir le quantifier précisément, l'utilisation des LBAS n'échappe pas non plus à un risque de diffusion d'une alerte trop tardive (alerte manquée) ou d'une fausse alerte. Lors de l'attentat du 14 juillet 2016 à Nice, l'ancienne application SAIP® (2016 – 2018) a émis une alerte vers 1h30 du matin alors que l'attaque s'est déroulée entre 22h et 22h20. Ce problème a été provoqué par la mise à jour des serveurs devant diffuser l'alerte, l'ordre d'alerter ayant déjà été envoyé sans possibilité de l'annuler. L'alerte est arrivée sur les téléphones à la fin de la mise à jour soit plus de trois heures après la fin de l'attentat. Début 2020 au Canada, une fausse alerte diffusée via le CB, reportant un incident dans une centrale nucléaire, a provoqué une indignation de la part des populations locales qui avaient ingérées des pastilles d'iode à la lecture du message. Le message a été envoyé par erreur au cours d'un exercice. A Hawaï, lors d'un exercice de crise (janvier 2018), un message d'alerte CB mentionnant une menace balistique a été envoyée à l'ensemble de la population. Cela a créé un sentiment de panique à travers toute la population d'autant plus que le message n'a été démenti que 42 minutes après la fausse alerte. Si cet événement n'est pas directement lié à la performance du CB, cela remet toutefois en question la réception et la compréhension d'une telle technologie pour les usagers.

Piratage et méfiance des utilisateurs

Des failles dans la sécurité des LBAS pourraient aussi être explorées, et l'envoi à la population de fausses alertes ou de messages frauduleux est ainsi tout à fait envisageable. C'est d'ailleurs ce qui s'est passé le 1er décembre 2020, lors de l'envoi du SMS incitant la population à télécharger l'application mobile TousAntiCovid® (avec une action de « fisching » observée dès le 4ème jour par exemple). La possibilité de récupération des données privées est également un sujet qui doit être pris en compte (Egelman et al., 2013). Aux Pays-Bas, deux mois après le lancement de l'application NL-Alert®, le gouvernement a demandé aux citoyens de désinstaller l'application car des données personnelles avaient été piratées[4]. Le problème a été résolu depuis, mais il a pu entacher la confiance envers cette solution.

En France, l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), rattachée au SGDSN (Secrétariat Général de Défense et de Sécurité Nationale), a pour mission de défendre les systèmes d'information de l'État. Elle est dotée du CERT-FR (centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques), qui dirige un système d'alerte focalisé sur le risque cyber à l'échelle de la France. Le prochain système d'alerte FR-Alert pourrait donc bénéficier des services de l'ANSSI et des services de surveillance du CERT-FR pour réduire les risques de piratages et d'envoi d'alerte malveillant à la population. Récemment, un consortium de scientifiques a d'ailleurs publié un article de vulgarisation sur l'application Stop-COVID® intitulé « *Le traçage anonyme, dangereux oxymore* » (Bonnetain *et al.*, 2020). Cet article montre que les données récoltées par l'application sont « pseudonymisées » (et non anonymisées). D'une manière générale, les technologies de géolocalisation donnent aux smartphones un caractère intrusif mal perçu par la population (Weill and Souissi, 2010b).

Commentaires de l'équipe projet :
La vulnérabilité structurelle, le risque de congestion et le risque de piratage sont des risques bien connus et souvent rappelés dans les publications techniques et/ou scientifiques concernant les LBAS. Il faut ajouter à cela le fait que les LBAS, comme n'importe quel moyen d'alerte, n'empêchent pas le risque pour les opérationnels de rater des alertes ou de diffuser de fausses alertes. Mais d'autres menaces et problématiques liées à l'usage des LBAS ne sont pas systématiquement considérés dans les rapports et articles publiés : il convient donc de les rappeler et de les prendre en considération.

[4] Crisis.nl, consulté le 8 mai 2020 : https://crisis.nl/nl-alert/nieuws/update-over-onderzoek-datalek/

4.2. Des solutions pas toujours ubiquitaires

Malgré un fort taux de pénétration des mobiles en France (95% en 2019, pour 72% en 2013 selon le Baromètre du Numérique), une certaine partie de la population ne sera jamais alertée par un LBAS car elle ne possède pas de téléphone mobile et/ou de smartphone. Le terme de « non-usagers » (Kellner et al., 2010 ; Wyatt, 2002) désigne les individus qui n'utilisent pas une technologie. Selon Jauréguiberry (2012), les études statistiques cherchant à cerner les variables expliquant l'usage d'une innovation (au sens large) ont montré que « *les non-usagers sont moyennement plus pauvres, plus isolés, plus vieux, ont de plus faibles compétences techniques et ont moins fait d'études* ». Goniewicz et Burkle (2019) précisent de leur côté que face aux risques naturels, les individus dépourvus de technologie sont aussi les plus vulnérables.

La question des inégalités d'usage est plus forte que celle des inégalités d'accès (Jauréguiberry, 2012). Granjon (2010) définit la fracture numérique comme « *un ensemble d'écarts de pratiques constitutifs d'inégalité sociale* ». Parmi les « non-usagers », Kellner et al., (2010) différencient : les « *abandonnistes volontaires* » (ils n'utilisent plus la technologie par choix personnel) ; les « *abandonnistes involontaires* » (qui ont été obligés de stopper l'utilisation de la technologie) ; les « *exclus* » qui n'ont pas accès par manque d'infrastructure ou de moyens ; les « *résistants* », qui ne souhaitent pas du tout utiliser une nouvelle technologie par choix (Granjon, 2010). Pour Kellner et al. (2010), les trois principaux facteurs des non-usages des TIC sont l'absence de besoin, le manque d'intérêt et le manque de motivation.

Bergier (2016) préfère, parler de « non-possession ». Selon lui, la non-possession est davantage choisie que subie (pour 84% d'un échantillon de 527 personnes ne possédant pas de portables). Ce fait s'explique par la grande méfiance qu'inspirent ces objets (37% de l'échantillon), par le fait que les téléphones mobiles sont perçus comme inutiles (35% de l'échantillon) ou par leurs coûts trop élevé (33% de l'échantillon). L'exposition aux ondes (22%) et l'incapacité réelle ou supposée à utiliser ces outils (14%) sont également avancés par les individus n'utilisant pas volontairement les téléphones mobiles. Bergier (2016) souligne néanmoins que la non-possession de téléphone mobile n'empêche pas les individus de rester connecter via d'autres outils de communication (ordinateur et téléphone fixe).

Par ailleurs, étant donné l'existence de zones blanches et de zones à faible connectivité en milieu rural, la question de « l'alertabilité » (terme discuté dans le livrable 1.3.a) des territoires ruraux isolés en cas d'utilisation d'un LBAS pourrait se poser : même si les technologies de communications participent à la revitalisation des zones rurales (Brachotte, 2011), l'existence d'espaces ruraux « inalertables » pourrait remettre en question l'adoption d'un LBAS à l'échelle nationale.

5. Conclusions et perspectives

Ce rapport a permis d'aborder les caractéristiques (techniques, fonctionnelles) et les enjeux relatifs aux outils d'alerte centrés sur la localisation des individus, en se focalisant sur le CB ou le LB-SMS. Ces LBAS pourraient révolutionner l'alerte en France et venir compléter les sirènes SAIP. Ainsi, ces solutions sont spatialement plus précises, peuvent fournir des messages plus explicites et plus riches en information, et garantir une procédure d'alerte plus rapide. Tout système centré sur la localisation doit aujourd'hui se calquer sur l'existant (téléphone portable, smartphone, objets connectés), sans pour autant pousser à l'achat massif d'outils spécialement dédiés. Le coût (équipement, fonctionnement, maintenance) doit aussi être une composante dans le choix.

De nombreux pays, développés ou émergents, se sont tournés avec succès vers les LBAS. La Directive européenne de décembre 2018 rend obligatoire l'adoption d'un LBAS pour tous les pays membre de l'Union Européenne d'ici 2022, et le mix entre le CB et LB-SMS a en train de faire l'objet d'un consensus dont a pris acte la Commission Européenne. Après plusieurs mois de réunions et de discussions (entre différents services et différents ministères), le Ministre de l'Intérieur a annoncé le 24 septembre 2020 la mise en place d'une telle solution hybride en France. En 2021, Malte, la Slovaquie et la Croatie ont eux aussi annoncé la même direction. D'autres pays pourraient rapidement rejoindre cette liste en 2022.

Toutefois, le non-usage volontaire ou subi des solutions sur lesquelles repose un LBAS, la vulnérabilité physique des infrastructures, les risques de piratage, la congestion des réseaux de télécommunication en période de crise ou les problèmes liées aux libertés privées et l'impact environnemental des LBAS invitent à reconsidérer l'hégémonie de ces solutions, et invitent surtout à ne pas dépendre du « fétichisme technologique ». **Ce n'est pas parce que l'outil existe qu'il sera accepté ou utilisé par les acteurs décisionnaires…**

Liste des figures et des tableaux

Liste des références bibliographiques

Alexander, D. E. (2014). Social media in disaster risk reduction and crisis management. *Science and engineering ethics*, *20*(3), 717-733.

Aloudat, A., Michael, K., & Yan, J. (2007). Location-based services in emergency management-from government to citizens: Global case studies.

Aloudat, A. (2010). Location-based mobile phone service utilisation for emergency management in Australia.

Aloudat, A., & Michael, K. (2011). Toward the regulation of ubiquitous mobile government: a case study on location-based emergency services in Australia. *Electronic Commerce Research*, *11*(1), 31-74.

Alphonsa, A., & Ravi, G. (2016). Earthquake early warning system by IOT using Wireless sensor networks. In *2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET),* 1201-1205)

Ardelet, C., Veg-Sala, N., Goudey, A., & Haikel-Elsabeh, M. (2017). Entre crainte et désir pour les objets connectés: comprendre l'ambivalence des consommateurs. *Décisions Marketing*, (2), 31-46.

Auclair, S., & Bertil, D. (2009). *Systèmes d'alerte sismique : principes et faisabilités aux Antilles françaises*, Rapport final, BRGM/RP-5663-FR, 92p.

Bergier, B. (2016). *Sans «mobile» apparent*. Chronique sociale.

Bonaretti, D., & Fischer-Preßler, D. (2021). The problem with SMS campus warning systems: an evaluation based on recipients' spatial awareness. *International Journal of Disaster Risk Reduction*, *54*, 102031.

Bonnetain, X., Canteaut, A., Cortier, V., Gaudry, P., Hirschi, L., Kremer, S., ... & Vuillot, C. (2020). Le traçage anonyme, dangereux oxymore.

Bopp, E. (2021). *Évaluation et spatialisation du potentiel offert par les moyens d'alerte centrés sur la localisation des individus. Expérimentations à différentes échelles en France* (Doctoral dissertation, Avignon Université).

Brachotte, G. (2011). Les TIC en zone rurale : de la fracture numérique à la revitalisation d'un territoire. *에피스테메*, (5), 137-157.

Cavalière, C., Davoine, P.-A., Lutoff, C., & Ruin, I. (2016). Analyser des tweets géolocalisés pour explorer les réponses sociales face aux phénomènes météorologiques extrêmes. *Actes de SAGEO*, Nice, France, 15p.

Chochliouros, I. P., Spiliopoulou, A. S., & Agapiou, G. (2009). Cell Broadcasting Opportunities of Modern Mobile Communications and Its Usage in Emergency Warning Facilities. In *Handbook of Research in Mobile Business, Second Edition: Technical, Methodological and Social Perspectives* (pp. 375-387). IGI Global.

Choy, S., Handmer, J., Whittaker, J., Shinohara, Y., Hatori, T., & Kohtake, N. (2016). Application of satellite navigation system for emergency warning and alerting. *Computers, Environment and Urban Systems*, *58*, 12-18.

De Longueville, B., Smith, R. S., & Luraschi, G. (2009). " OMG, from here, I can see the flames!" a use case of mining location based social networks to acquire spatio-temporal data on forest fires. In *Proceedings of the 2009 international workshop on location based social networks* (pp. 73-80).

Douvinet, J. (2018). Alerter la population face aux crues rapides en France : compréhension et évaluation d'un processus en mutation. *Université d'Avignon*.
Douvinet, J. (2020). L'alerte par sirènes : une priorité discutable en France. *Annales de géographie* 731(1), 5p.
Douvinet, J., Gisclard, B., Kouadio, J. S., Saint-Martin, C., & Martin, G. (2017). Une place pour les technologies smartphones et les Réseaux Sociaux Numériques (RSN) dans les dispositifs institutionnels de l'alerte aux inondations en France?. *Cybergeo: European Journal of Geography*.
Egelman, S., Felt, A. P., & Wagner, D. (2013). Choice architecture and smartphone privacy: There'sa price for that. In *The economics of information security and privacy* (pp. 211-236). Springer, Berlin, Heidelberg.
European Telecommunication Standard Institute (1996). Digital cellular telecommunications system (Phase 2+); Technical realization of Short Message Service Cell Broadcast (SMSCB). Sophia Antipolis, France, 29p.
Goniewicz, K., & Burkle, F. M. (2019). Challenges in implementing Sendai framework for disaster risk reduction in Poland. *International journal of environmental research and public health*, *16*(14), 2574.
Goodchild, M. F. (2007). Citizens as sensors: the world of volunteered geography. *GeoJournal*, *69*(4), 211-221.
Gourine, R. T. T. M. (2013). *Enjeux et performance socio-économique d'actions proactives et innovantes de gestion des risques qui s' appuient sur la tradition de solidarité* (Doctoral dissertation, Conservatoire national des arts et metiers-CNAM).
Granjon, F. (2010). Le « non-usage» de l'internet: reconnaissance, mépris et idéologie. *Questions de communication*, (18), 37-62.
Grant, S., & Smith, K. (2019). *Emergency Alerting in England. Warning simulation exercise,* University of Hull.
GSMA. (2013). Mobile Network PWS and Rise of Cell-Broadcast. https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2013/01/Mobile-Network-Public-Warning-Systems-and-the-Rise-of-Cell-Broadcast.pdf
GSMA (2015). Disaster Response, DEWN - Dialog's Disaster and Emergency Warning Network, 18p.
Hajdarevic, K., & Konjicija, S. (2015). A low energy computer infrastructure for radio VOIP supported communication and SDR APRS in education and disaster relief situations. In *2015 38th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)* (pp. 556-561). IEEE.
Houston, J. B., Hawthorne, J., Perreault, M. F., Park, E. H., Goldstein Hode, M., Halliwell, M. R., & Griffith, S. A. (2015). Social media and disasters: a functional framework for social media use in disaster planning, response, and research. *Disasters*, *39*(1), 1-22.
Jagtman, H. M. (2010). Cell broadcast trials in The Netherlands: Using mobile phone technology for citizens' alarming. *Reliability Engineering & System Safety*, *95*(1), 18-28.
Jauréguiberry, F. (2012). Retour sur les théories du non-usage des technologies de communication. *Connexions: communication numérique et lien social*, 335-350.
Jayasinghe, G., Fahmy, F., Gajaweera, N., & Dias, D. (2006). A GSM alarm device for disaster early warning. In *First International Conference on Industrial and Information Systems* (pp. 383-387). IEEE.
Kellner, C., Massou, L., & Morelli, P. (2010). *(Re) penser le non-usage des tic* (No. 18, pp. 7-20). Presses universitaires de Nancy.
Kouadio, S. J. A. (2016). *Les technologies smartphone comme outils d'aide à l'alerte face aux crues rapides en France: Expérimentations dans le Vaucluse et le Var* (Doctoral dissertation, Université d'Avignon).
Küpper, A. (2005). *Location-based services: fundamentals and operation*. John Wiley & Sons.
Laverdet, C., Weiss, K., Bony-Dandrieux, A., Tixier, J., & Caparos, S. (2018). Digital Training for Authorities: What is the Best Way to CommunicatDuring a Crisis?. *Decision-making in Crisis Situations: Research and Innovation for Optimal Training*, 149-173.
Leo, Y., Sarraute, C., Busson, A., & Fleury, E. (2015). Taking Benefit from the User Density in Large Cities for Delivering SMS. In Proceedings of the 12th ACM Symposium on Performance Evaluation of Wireless Ad Hoc, Sensor, & Ubiquitous Networks - PE-WASUN '15, Cancun, Mexico: ACM Press, 55–61.
Martin, G., & Blay, L. (2014). Le citoyen au coeur de sa sauvegarde grâce à l'utilisation des médias sociaux en gestion de l'urgence. *Risques Infos*, 34, 22–24.
Moatty, A., Grancher, D., Virmoux, C., & Cavero, J. (2019). Bilan humain de l'ouragan Irma à Saint-Martin: la rumeur post-catastrophe comme révélateur des disparités socio-territoriales. *Géocarrefour*, *93*(93/1).
Nollet, K. E., & Ohto, H. (2013). When all else fails: 21st century Amateur Radio as an emergency communications medium. *Transfusion and apheresis science*, *49*(3), 422-427.
OCDE (2014). Étude de l'OCDE sur la gestion des risques d'inondation : la Seine en Île-de-France 2014. https://doi.org/10.1787/9789264207929-fr
Preis, T., Moat, H. S., Bishop, S. R., Treleaven, P., & Stanley, H. E. (2013). Quantifying the digital traces of Hurricane Sandy on Flickr. *Scientific reports*, *3*(1), 1-3.
Pries R., Hobfeld T., Tran-Gia P. (2006). On the Suitability of the Short Message Service for Emergency Warning Systems, 991-995 in: 2006 IEEE 63rd Vehicular Technology Conference. Melbourne, Australia, IEEE.
Rey, T., Leone, F., Candela, T., Belmadani, A., Palany, P., Krien, Y. & Zahibo, N. (2019). Coastal Processes and Influence on Damage to Urban Structures during Hurricane Irma (St-Martin & St-Barthélemy, French West Indies). *Journal of Marine Science and Engineering*, *7*(7), 215.
Samarajiva, R., & Waidyanatha, N. (2009). Two complementary mobile technologies for disaster warning. *info*.

Santoni V (2021). *Utilisation des réseaux sociaux numérques dans un contexte de gestion territorialisée des crises. Comparaison entre l'Ile de France et la région de Bruxelles-Capitale*, Thèse de Géographie, Cergy Université, 332p.
Scott, K. (2016). Digital urban health and security: NYC's got an app for that. *In Digital Futures & the City of Today: New Technologies and Physical Space*, G.A. Caldwell, C.H. Smith, and E.M. Clifs, eds.
Sillem, S., & Wiersma, E. J. W. F. (2006). Comparing cell broadcast and text messaging for citizen warning. In *Proceedings of the 3rd International ISCRAM Conference*. ISCRAM.
Sillem, S., Jagtman, H. M., Wiersma, J. W. F., & Ale, B. J. M. (2006). Using cell broadcast in citizens warning: Characteristics of messages.
Song, M., Jun, K., & Chang, S. (2014). An efficient multiplexing method of T-DMB and cell broadcast service in emergency alert systems. *IEEE Transactions on Consumer Electronics*, *60*(4), 549-557.
Spiekermann, S. (2004). General Aspects of. *Location-based services*, *9*, 14-33.
Udu, N. (2009). Mobile Cell Broadcasting for Commercial Use and Public Warning in the Maldives. 43p.
Vogel, J. P. (2017). Rapport d'information sur le système d'alerte et d'information des populations (SAIP). *Rapport public pour le Sénat*, *595*, 48.
Weill, M., & Souissi, M. (2010). L'Internet des objets : concept ou réalité?. In *Annales des Mines-Réalités industrielles* (No. 4, pp. 90-96). Eska.
Wellington Region Emergency Management Group (2012). Social Media in a Emergency, a best practice guide. Wellington Region *Emergency Management*. 58p.
Wyatt, S. (2010). Les non-usagers de l'internet. Axes de recherche passés et futurs. *Question de communication 18* (2010), pp. 21-36.

.