ÉDITORIAL

Petit à petit, sans nous en rendre compte, les systèmes d'alarmes sont devenus omniprésents. D'un côté, il y une augmentation des systèmes d'alarmes que nous utilisons au quotidien et, de l'autre, une prolifération des systèmes d'alarmes préventifs et de surveillance. Mais encore faut-il s'entendre sur le terme alarme. Depuis longtemps nous avons pris goût au fait que nos outils informatiques nous informent au moyen d'alertes, d'alarmes, de l'arrivée de nouveaux messages, d'un événement, comme un rendez-vous, ou de la fin d'une tâche réalisée par la machine. Aujourd'hui, ce mode d'interaction se propage que cela soit par des alertes sur des sujets qui intéressent l'utilisateur, comme celles générées par des outils de curation, ou par des réseaux sociaux et des applications mobiles de géolocalisation. La plupart des réseaux sociaux disposent de fonctionnalités pour avertir leurs utilisateurs de l'activité de leurs contacts ou de la publication de nouveaux contenus tels que des actualités, des images ou des vidéos, suivant les critères d'intérêt de l'utilisateur. Couplées à la géolocalisation, ces alarmes peuvent dépendre des déplacements des utilisateurs et être générées lors du passage à proximité de lieux d'intérêt.

Nous pouvons dresser un parallèle entre les alertes issues d'applications grand public et celles utilisées par des organisations en vue de prévenir de divers types de risques. En effet, concernant les systèmes de prévention, que cela soit pour la prédiction de catastrophes naturelles (inondations, avalanches, etc.), la veille sanitaire ou la surveillance du ciel et de l'espace, de plus en plus d'acteurs se retrouvent impliqués au sein de systèmes d'information dont l'un des buts est la diffusion d'alarmes. Ces systèmes visent, pour la plupart, à générer des alarmes en vue de prévenir d'un risque par exemple un tsunami ou une potentielle épidémie. Dans un monde globalisé, ces systèmes peuvenet être déployés à des échelles variables ; à un niveau locale dans le cas de la surveillance des crues, régionale, continentale voire mondiale, dans le cas de la surveillance de risques sismiques.

Cependant, la frontière tend à devenir poreuse entre les systèmes de prévention de risques dédiés et les systèmes d'alarmes grand public (lorsque par exemple les contenus publiés sur les réseaux sociaux sont analysés en flux tendu pour y déceler la naissance de phénomènes tels que les épidémies, les risques de mouvements de panique, etc.). Il serait à l'avenir illusoire de continuer à étudier ces types de systèmes séparément ou de chercher à maintenir une frontière étanche entre les deux. Par exemple, le réseau social Facebook, avec son alarme « safety check » en cas de catastrophe naturelle ou d'attentat, peut-il encore être considéré comme simple fournisseur d'un service grand public, non critique et sans garantie d'efficacité ? Twitter, en proposant aux organisations gouvernementales de diffuser sur son réseau leurs messages d'alarmes, comme les alertes enlèvement, ne doit-il

pas être aussi vu comme un moyen de prévenir les populations en cas de risque ? Brouillant un peu plus la frontière, certaines applications mobiles proposent non seulement de jouer le rôle de vecteur d'alarmes pour certains types de risques précis, gérés par des organismes gouvernementaux, mais aussi aux utilisateurs grand public de participer à la surveillance du risque. Ainsi, l'application mobile de la Japan Meteorological Agency, Yurekuru Call, permet d'être averti à l'avance d'une secousse sismique, mais aussi de collecter des informations que les utilisateurs partagent sur l'intensité sismique ressentie.

Face à cette prolifération des systèmes avec alarmes, il nous semble important de mener une réflexion sur les enjeux entourant ces systèmes, en prenant en compte leurs particularités afin d'identifier et de qualifier leur impact sur leurs utilisateurs, ou les populations associées, concernées ou sollicitées, parfois à tort, ou malgré elles, de plus en plus souvent via des communautés, cercles, cliques, cohortes, etc. En effet, parce que les systèmes d'alarmes visent de plus en plus à la gestion de risques, il convient de s'interroger sur leur pertinence et sur les garanties qu'ils peuvent offrir quant à la mission de prévention ou de gestion de crise qu'ils contribuent à réaliser. Ainsi, la bonne marche de tout système d'alarme dépend de propriétés que nous pourrions qualifier de fondamentales, telles que (parmi d'autres) la vivacité, la réactivité ou la résilience. Toute alerte doit absolument être acheminée à un destinataire pertinent, au bon moment et au bon endroit (vivacité et réactivité), et ce malgré les diverses contraintes liées d'une part à des événements externes, comme des défaillances matérielles, des défauts de connexion, des ruptures dans les canaux de communication (résilience).

Étudier ces systèmes nous amène à évoluer dans un contexte de Big Data, contexte dans lequel la réflexion ne peut se borner aux seuls aspects de performance (volume et vélocité par exemple) : il faut aussi s'interroger sur les aspects liés à la confidentialité et au risque de manipulation de ces systèmes à des fin de désinformation ou de déclenchement de réactions de panique massive par exemple. Ainsi, la véracité et la vérité de la donnée sont plus que tout essentielles ici. Les systèmes d'alarmes manipulant de plus en plus d'information concernant les individus, la question du respect de la vie privée et de la gestion de données personnelles se doit d'être abordée : doit-on réellement abandonner la protection de la vie privée pour la sécurité, où se situe le compromis idéal entre protection de la vie privée et prévention de risques ? En suivant cet axe de réflexion, on peut s'interroger sur la légitimité pour un système d'alarme d'avoir un accès sans restrictions aux données personnelles de ses utilisateurs, de pouvoir collecter ces données (avec ou sans le consentement de l'utilisateur, par exemple via les mécanismes de bris de glace). Comment assurer un contrôle de la collecte et de l'utilisation des données personnelles des utilisateurs ? Ces systèmes d'alarme pouvant avoir une influence extrême sur leurs utilisateurs, comment aborder la question de leur protection par rapport aux utilisations détournées visant à la propagation de rumeurs, à la manipulation du comportement ou de l'opinion de ses utilisateurs ? De plus en plus présents sur les réseaux sociaux, sur les plateformes de

partage et sous la forme d'applications mobiles, ces systèmes de diffusion d'alarmes ne doivent pas devenir des vecteurs d'instigation ou d'amplification de phénomènes de panique : comment détecter et se prémunir contre ces risques de propagations de fausses alertes ou bien de rumeurs, les rumeurs pouvant mener à des mouvements de paniques ? C'est peut-être ici qu'interviendra un cinquième V du Big Data qui traduira la volonté de l'utilisateur engagé, par exemple *via* les mécanismes de *crowdsourcing*, volontaire et « validant ».

Le but de ce numéro de la revue ISI est donc de lancer une réflexion collective et d'inciter le lecteur à participer à cette réflexion en présentant un ensemble de travaux récents pertinents vis-à-vis du cadre défini ci-dessus. Ainsi le premier article, proposant une « roadmap » architecturale pour la construction d'un système de diffusion d'alarme, s'interroge sur les exigences fonctionnelles, mais aussi de qualité de service, propres à tout type de système de diffusion d'alarmes et propose une architecture de référence pour la conception de tels systèmes. Le propos est illustré au travers d'un exemple de système de contrôle aérien anti-collision (*Traffic Collision Avoidance System*).

Le deuxième article propose un cadre formel pour exprimer une politique d'échange d'information entre organisations dans le but de produire des alarmes. Le but de ce cadre générique est de disposer d'un langage formel permettant la spécification des règles de diffusion d'information et l'expression de propriétés souhaitées à un niveau organisationnel.

Tourné sur l'étude d'un cas pratique, le troisième article se situe à la frontière entre les systèmes d'alarmes des organisations et les liens qu'ils pourraient entretenir avec le grand public, au travers d'applications mobiles. Partant du cas concret d'un système d'alertes pour les crues rapides dans les petits bassins versants, ce papier étudie la faisabilité d'une application pour téléphone mobiles visant à réduire les temps d'acheminement d'alertes à destination de populations, mais qui permettrait aussi la collecte d'informations auprès des utilisateurs pour améliorer la vigilance grâce à la participation active des citoyens, et d'améliorer ainsi les connaissances sur les dommages observés en temps réel.

Le quatrième article s'intéresse aux phénomènes « parasites » de la diffusion d'information dans les écosystèmes sociaux. Il constitue un travail préliminaire sur les travaux de détection de *spammeurs*, d'analyse de polémiques, de rumeurs, et la prise en charge du *buzz*. Il s'agit plus précisément ici, à partir d'une étude du réseau social Delicious, d'analyser l'influence de l'enrichissement de profils utilisateurs sur la propagation de *buzz* dans les médias sociaux.

Le dernier article de ce numéro présente une méthode de traitement des alarmes pour faciliter leur gestion dans le cas d'une grande masse de données. Cette approche se base sur une ontologie ainsi qu'un système de règles de filtrage et a été appliquée à l'étude de déplacements des populations de mammifères marins, dont la détection de certains comportements anormaux ou atypiques pourrait constituer une alerte écologique.

Ce numéro est le fruit d'une collaboration, entreprise dans différents contextes et qui ne cesse de s'enrichir, entre membres de la communauté, représentants de la diversité des domaines que ces travaux associent, que nous remercions chaleureusement pour leur implication et leur contribution :

– Rocio Abascal-Mena – UAM, Mexico, Mexique

– Agnès Front – LIG, Grenoble, France

– Sergio Ilarri – Universidad de Zaragoza, Zaragoza, Espagne

– Jamal Malki – L3I, La Rochelle, France

– Andre Miralles – UMT Tétis, Montpellier, France

– Arnaud Quirin – CNCA, Crédit Agricole Data Lab., France

– Didier Richard – IRSTEA, France

Florence SÈDES
IRIT, Toulouse

Rémi DELMAS
Thomas POLACSEK
ONERA, Toulouse