



## CONSEIL D'ETAT

Château cantonal  
1014 Lausanne

Madame la Conseillère fédérale  
Simonetta Sommaruga  
Cheffe du DETEC  
Palais fédéral Nord  
3003 Berne

*Envoi par courriel :*  
*Tp-secrétariat@bakom.admin.ch*

Réf. : ID/DES/Polcant

Lausanne, le 17 mars 2022

### **Modification de l'Ordonnance sur les services de télécommunication (OST) - Ouverture de la procédure de consultation**

Madame la Conseillère fédérale,

Par courrier du 3 décembre 2021, vous nous avez invités à prendre position sur le projet mentionné sous rubrique. Le Canton de Vaud vous remercie de la possibilité ainsi offerte. Vous trouverez ci-après notre prise de position.

#### **GENERALITES**

Nous souscrivons fondamentalement au projet soumis d'Ordonnance sur les services de télécommunication (OST).

Du point de vue des services « feux bleus », il est important de tenir compte de la manipulation illicite possible du réseau 5G et d'adopter des mesures supplémentaires permettant de garantir la protection du réseau. Nous rendons également attentif à la nécessité de mettre en place un système de communication à large bande (Projet MSK) afin d'éviter à l'avenir des pannes sur les réseaux existants. Pour rappel, 70% des appels reçus par les centrales d'urgence sont faites par les appareils mobiles.

Nous suggérons que les processus d'alerte et de notification soient décrits en détail. Afin d'améliorer le traitement et la distribution des messages d'incident reçus, le règlement révisé prévoit de renforcer le rôle de la centrale nationale d'alarme d'alerte (CENAL). La réception des messages de cyber-attaques doit devenir une tâche essentielle de la CENAL, car elle dispose d'une infrastructure informatique sécurisée et d'une exploitation 24 heures sur 24. La création d'un Single Point of Contact (SPOC) est un objectif, car elle facilite la gestion des crises.

Il y a d'autres organisations qui s'occupent de cyber-attaques. Il n'est pas possible que seul l'OFCOM soit informé par la CENAL des perturbations signalées. Par exemple, le National Cyber Security Center (NCSC), l'unité de signalement et d'analyse de l'AI (MELANI) ainsi que les centres cantonaux d'appel d'urgence de la police, des pompiers et des services sanitaires doivent être inclus. Leur rôle dans l'ensemble du processus de notification et d'alerte dans le domaine de la cyber doit être indiqué dans le rapport explicatif. Les processus d'information doivent donc être ancrés dans l'ordonnance (OST).

## COMPLEMENTS ET MODIFICATIONS

Nous demandons les modifications suivantes au projet de l'OST :

### **Art. 96**

Les interférences dans le secteur de la téléphonie mobile ont des effets immédiats. Par exemple, les numéros d'urgence peuvent ne plus être disponibles ou les forces de police, de secours et de lutte contre les incendies peuvent être entravées par le manque de moyens de transmission de données. Dans de nombreux cantons, des points de rencontre d'urgence ont été installés et peuvent être occupés en cas de panne dans la zone de communication. Cela suppose toutefois que les centres cantonaux d'urgence soient immédiatement et immédiatement informés des pannes, déjà dans le secteur à bas niveau. La taille de 30 000 clientes et clients concernés par une défaillance, telle que formulée à l'article 96, est nettement trop élevée. De plus une jauge fixe ne nous paraît pas idéale. Un seuil d'alerte paramétrable selon la région, le site, l'émetteur, la population, la topographie, la présence d'infrastructures critique ou autres nous paraîtraient plus appropriés (sous réserve de faisabilité technique).

#### Demande :

*Lors d'une défaillance du système de plus de 15 minutes concernant des clients et clientes (pas de jauge fixe, mais un seuil paramétrable), les prestataires de services de télécommunications doivent informer en priorité les centres d'appel d'urgence cantonaux de la police, des services sanitaires et des pompiers (112, 117, 118, 144). On doit diminuer au maximum les intermédiaires.*

### **Art. 96a**

Au paragraphe 1, il est question spécifiquement et en dernier lieu d'attaques de la DDoS. En raison de l'évolution rapide de la technologie, il est possible que d'autres types d'attaques puissent être envisagées dans le futur.

Au paragraphe 3, on autorise les fournisseurs d'accès à Internet à bloquer ou à restreindre les accès à Internet et les éléments d'adressage qui affectent les systèmes. Ils peuvent maintenir les mesures tant que la menace persiste. Cela peut entraîner des interruptions dans le domaine des appels d'urgence et donc des risques pour les personnes nécessitant une assistance.

#### Demandes :

- a) *Par. 1 : Dans le paragraphe susmentionné, il ne s'agit pas de parler d'attaques DDoS, mais de mentionner les attaques DDoS comme exemples.*
- b) *Par. 1 : Les détails des mécanismes d'attaque potentiels ne doivent pas être réglés de manière exhaustive dans l'OST, mais dans les règles technico-administratives (LTC). Cela permet d'agir de manière adéquate et d'adapter les règles à prendre en considération de manière relativement peu contraignante.*

- c) *Par. 3 : Les restrictions en cas de menace doivent être très sélectives et ne conduire qu'à titre exceptionnel à l'impossibilité de composer des numéros d'urgence sur les lignes concernées.*

#### **Art 96f**

Au paragraphe 2, il est précisé que des centres d'exploitation du réseau et de leurs centres d'exploitation de la sécurité peuvent se trouver hors de la Suisse dans l'Espace économique européen et au Royaume-Uni. Lorsqu'un exploitant opère principalement en dehors de la Suisse, il est difficile, voire impossible, de parvenir à un accord opérationnel et juridique en cas d'événement ou de dysfonctionnement. Outre les difficultés d'accès à l'étranger, la priorisation des mesures et des ressources est également nettement plus difficile. Il est suggéré d'exiger une représentation permanente en Suisse.

#### Demande :

*En ce qui concerne notamment l'exploitation d'installations de télécommunications critiques pour la sécurité, il convient d'accorder une grande importance au siège ou à une représentation permanente en Suisse. Ceci doit être ancré dans l'OST.*

#### **CE QUI MANQUE**

Deux sujets qui ont été remontés à plusieurs reprises par le Comité de pilotage intercantonal des centrales d'urgence (Steuerungsausschuss Notrufe) n'ont pas été pris en compte dans le cadre de l'ordonnance. Il s'agit de la gratuité d'utilisation pour les services d'urgence à la SOS-DB (base de données d'urgence) et à l'application de transfert dynamique des appels (DLWL). Ceci ne doit pas être un enjeu commercial.

#### Demande :

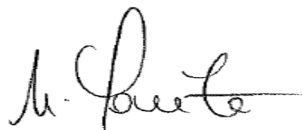
*Intégrer dans l'OST la notion de gratuité d'accès pour toutes les centrales d'urgence à la SOS-DB et à l'application DLWL.*

Nous vous prions de croire, Madame la Conseillère fédérale, à l'assurance de nos sentiments les meilleurs.

AU NOM DU CONSEIL D'ETAT

LA PRESIDENTE

LE CHANCELIER



Nuria Gorrite



Aurélien Buffat

#### **Copies**

- OAE
- Polcant