RÉPUBLIQUE ET CANTON DE GENÈVE

POST TENEBRAS LUX

Genève, le 16 septembre 2026

Le Conseil d'Etat

2322-2026

Département fédéral de l'environnement
des transports, de l'énergie et de la
communication DETEC
Monsieur Albert Rösti
Conseiller fédéral
Palais fédéral Nord
3003 Berne

Concerne : renforcement de la sécurité des réseaux et protection contre les cybermenaces (révision partielle de l'ordonnance du 9 mars 2007 sur les services de télécommunication [OST], de l'ordonnance du 25 novembre 2015 sur les installations de télécommunication [OIT] et de l'ordonnance du 6 octobre 1997 sur les ressources d'adressage dans le domaine des télécommunications [ORAT])

Monsieur le Conseiller fédéral,

Notre Conseil a bien reçu votre lettre du 27 mai dernier, par laquelle vous l'invitez à se prononcer dans le cadre de la procédure de consultation citée en titre, et il vous en remercie.

Après un examen attentif de l'ensemble des documents transmis, nous souhaitons vous faire part des observations suivantes.

Notre Conseil accueille favorablement les modifications proposées, qui contribuent au renforcement de la protection des réseaux de télécommunication face à des cybermenaces croissantes. Cette révision s'inscrit dans une évolution déjà bien établie à l'étranger et permet à la Suisse de renforcer son dispositif réglementaire en la matière.

Nous soutenons également le principe selon lequel les centres d'opérations du réseau et de sécurité doivent être exploités en Suisse. Il nous semblerait judicieux de préciser le régime applicable aux accès à distance par des maisons-mères ou des sous-traitants établis à l'étranger. Une attention particulière pourrait également être portée à la mise en place de délais transitoires adaptés au degré de maturité des différents types d'opérateurs.

Notre Conseil est en revanche plus réservé quant à la possibilité de recourir à des systèmes redondants situés hors du territoire national. Dès lors que ces systèmes ont précisément vocation à prendre le relais en cas d'indisponibilité des dispositifs primaires, leur hébergement hors de la sphère de compétence de notre État pourrait soulever certaines difficultés au regard de la maîtrise d'infrastructures critiques. Il nous paraîtrait dès lors souhaitable de supprimer cette exception.

S'agissant des exigences de sécurité applicables aux installations critiques, une articulation explicite avec la loi fédérale sur la sécurité de l'information du 18 décembre 2020 (LSI) ainsi qu'avec l'obligation d'annonce des cyberattaques au *National Cyber Security Centre* (NCSC) nous paraîtrait utile, notamment afin de limiter les risques de doublons en matière d'audits et de *reporting*.

Nous relevons par ailleurs que l'obligation d'annoncer sans délai tout danger imminent aux polices cantonales et aux autorités fédérales concernées, bien qu'évoquée dans le rapport explicatif, ne ressort pas du texte même de l'ordonnance, qui prévoit en l'état uniquement une annonce à la Centrale nationale d'alarme. Compte tenu de l'importance d'une telle information pour la protection de la population, il est nécessaire de prévoir l'inscription expresse de cette obligation dans l'ordonnance, ainsi que la désignation de ses destinataires.

Notre Conseil accueille également favorablement la limitation de la sous-attribution des numéros à un seul niveau ainsi que le renforcement des mesures préventives contre l'usurpation de numéros suisses. Ces évolutions rejoignent les pratiques développées à l'étranger. Le spoofing constituant aujourd'hui un vecteur important de fraude au préjudice de la population, il nous semble indispensable de préciser les modalités de collaboration entre les fournisseurs et les autorités de poursuite pénale dans ce domaine.

Nous souhaitons également attirer votre attention sur la durée minimale de maintien en fonction des réseaux de télécommunication en cas de pénurie d'électricité, actuellement fixée à quatre heures. Cette durée ne prend pas en compte l'hypothèse d'une panne électrique généralisée, dont les conséquences pour la population seraient importantes, en particulier s'agissant du maintien de la possibilité d'effectuer des appels d'urgence. Dans cette perspective, il nous paraîtrait indiqué de porter cette durée à 72 heures, ce qui correspond aux données des scénarios de *black-out* retenus en la matière.

Enfin, compte tenu de l'hétérogénéité du degré de maturité des acteurs concernés, la publication par l'Office fédéral de la communication de directives techniques d'exécution, accompagnée d'un dialogue régulier avec la branche, pourrait contribuer à faciliter une mise en œuvre homogène et proportionnée des nouvelles exigences.

Vous trouverez en annexe un tableau synoptique qui détaille nos observations, article par article et inclut l'ensemble des présentes remarques.

Nous vous remercions d'ores et déjà de l'attention que vous voudrez bien prêter aux observations de notre Conseil et vous prions de croire, Monsieur le Conseiller fédéral, à l'assurance de notre haute considération.

AU NOM DU CONSEIL D'ÉTAT

Le vice-chancelier :

Patrick Ferraris

La présidente :

Anne Hiltpold

Annexe mentionnée

Copie à : tp.secretariat@bakom.admin.ch

Procédure de consultation concernant le renforcement de la sécurité des réseaux et protection contre les cybermenaces (révision partielle des ordonnances dans le domaine des télécommunications)

Prise de position du Conseil d'Etat de la République et canton de Genève

---

Remarques générales

1. Soutien de principe au projet

Cette révision s'inscrit dans la tendance internationale : NIS2 et la 5G Toolbox dans l'UE, le Telecommunications Security Act britannique, les exigences allemandes (BSI/TKG). La Suisse comble un retard réglementaire et il convient de clairement soutenir cette révision.

2. Installations de réseau critiques : demander la cohérence réglementaire

Nous soutenons les exigences renforcées (acquisition, exploitation, contrôles de conformité), mais nous souhaiterions une articulation explicite avec la Loi fédérale sur la sécurité de l'information (ci-après : LSI).

Nous suggérons une obligation d'annonce des cyberattaques au National Cyber Security Centre (NCSC), afin d'éviter les doublons d'audits et de reporting pour les opérateurs.

Nous prônons une approche fondée sur les risques plutôt que des contrôles uniformes.

3. NOC/SOC en Suisse : soutien avec précision

L'obligation d'exploiter les centres d'opérations et de sécurité en Suisse suit la logique de souveraineté numérique adoptée ailleurs (Allemagne, exigences américaines).

Nous exprimons deux recommandations :

- clarifier le traitement de l'accès à distance par des maisons-mères ou sous-traitants étrangers (risque d'extraterritorialité, type CLOUD Act), sinon l'obligation de localisation perdrait son effet ;
- prévoir des délais transitoires proportionnés. En effet, si les grands opérateurs sont matures, les Full MVNO et petits FST le sont beaucoup moins.

4. Numéros suisses et spoofing :

La limitation de la sous-attribution à un seul niveau et la lutte préventive contre le spoofing correspondent aux meilleures pratiques (STIR/SHAKEN aux États-Unis, mécanisme d'authentification MAN en France, mesures Ofcom au Royaume-Uni).

Nous souhaitons vivement que les canaux de collaboration entre fournisseurs et autorités de poursuite pénale (signalement, blocage rapide, traçabilité de la sous-attribution) soient explicitement prévus, car le spoofing est aujourd'hui un vecteur majeur de fraude au préjudice de la population.

5. Proportionnalité et accompagnement

Le succès du TSA britannique a été obtenu grâce à un dialogue avec la branche. En ce sens, il sera demandé que l'Office fédéral de la communication (ci-après : OFCOM) publie des directives techniques d'exécution et prévoie un dialogue similaire, au vu de l'hétérogénéité de maturité des acteurs.

6. Différence entre le rapport explicatif et la concrétisation dans l'ordonnance

Le rapport détaille abondamment des éléments techniques tels que les principes zero trust, la segmentation réseau, les pare feux, les listes précises de normes 3GPP/GSMA/ENISA, l'obligation d'informer « sans délai » la Police en cas de danger imminent. Il mentionne également les ateliers annuels avec l'Office fédéral de la cybersécurité (OFCS) et l'OFCOM et les réunions plusieurs fois par an entre départements cybersécurité.

Or, à l'exception du filtrage de signalisation mentionné à l'article 96f bis, alinéa 6 AP_OST, presque aucun élément technique n'apparaît comme obligation juridiquement contraignante dans le texte de l'ordonnance lui-même. L'art. 96 OST en vigueur prévoit une obligation d'annonce auprès de la CENAL uniquement.

Compte tenu de l'importance d'une telle annonce, ces obligations doivent figurer expressément dans le texte avec la mention de ses destinataires.

Résumé :

Nous insistons sur trois demandes :

- cohérence avec la LSI/NCSC
- encadrement de l'accès étranger aux NOC/SOC
- intégration formelle des autorités pénales dans le dispositif anti-spoofing.

Commentaire sur les articles :

Les Ordonnances sur les installations de télécommunication (OIT), l'Ordonnance de l'OFCOM sur les installations de télécommunication (OOIT) et l'Ordonnance sur les ressources d'adressage dans le domaine des télécommunications (ORAT) n'appellent aucune remarque. Nos observations portent exclusivement sur l'Ordonnance sur les services de télécommunications (OST) qui sont reportées ci-après sur un tableau synoptique.

Proposition Ordonnance sur les services de télécommunications (OST)	**Commentaire CE**
Titre précédant l'art. 96d **Section 5: Sécurité de l'infrastructure des réseaux de radiocommunication mobile**	
Art. 96*d* Champ d'application 1 Les dispositions de la présente section s'appliquent aux réseaux de radiocommunication mobile qui répondent aux spécifications techniques définies au niveau international pour toutes les générations de réseaux. 2 Elles s'appliquent aux fournisseurs de services de télécommunication suivants : a. les concessionnaires de radiocommunication mobile ; b. les opérateurs de réseau mobile virtuel complet.	
Art. 96*e al. 1* 1 Les concessionnaires de radiocommunication mobile et les opérateurs de réseau mobile virtuel complet développent, mettent en œuvre et réexaminent en continu un système de gestion de la sécurité de l'information en se fondant sur une analyse des risques et sur les objectifs de sécurité qui découlent de celle-ci. 2 [...]	**Commentaire :** quelles sont les mesures qui permettront de vérifier que les systèmes sont continuellement réexaminés d'un point de vue sécurité de l'information ?
Art. 96*f* 1 Les concessionnaires de radiocommunication mobile et les opérateurs de réseaux mobiles virtuels complets s'assurent que les installations de télécommunication qu'ils exploitent et qui sont critiques du point de vue de la sécurité correspondent à l'état de la technique. L'OFCOM peut déterminer les installations concernées. 2 Les concessionnaires de radiocommunication mobile et les opérateurs de réseaux mobiles virtuels complets exploitent exclusivement en Suisse leurs centres d'opération du réseau (*Network Operations Center [NOC]*), leurs centres de gestion de la sécurité (*Security Operations Center [SOC]*) et les installations de télécommunication essentielles pour l'exploitation, la commande et la gestion de leurs réseaux. 3 Pour assurer la continuité de l'exploitation, ils peuvent disposer à l'étranger de systèmes qui assurent la redondance pour les centres et les installations visés à l'al. 2 et qui sont prévus exclusivement pour l'exploitation de secours, pour autant que : a. les systèmes et les installations soient exploités dans des États dont la législation garantit un niveau de protection des données adéquat ;	**Ad art. 96f al. 3**: La mise en place de systèmes redondants hors du territoire national, même s'il s'agit uniquement de solutions de secours, est absolument à éviter. C'est précisément parce qu'ils constituent des moyens de substitution pour pallier une indisponibilité des dispositifs primaires qu'on ne peut se permettre de les héberger hors de la sphère de compétence de notre Etat. Le moindre risque de prise d'influence étrangère sur ces équipements critiques **n'est pas acceptable**. **Proposition** : supprimer la possibilité d'une implantation des dispositifs redondants des réseaux hors du territoire helvétique.

b. toutes les connections vers les installations de télécommunication en Suisse soient cryptées et journalisées ; c. le contrôle et la gestion des systèmes redondants et des clés cryptographiques qui leur sont associées soient assurés depuis la Suisse; et d. le service téléphonique public et le service d'accès à Internet continuent d'être assurés en Suisse même en cas d'interruption des connexions vers des installations redondantes à l'étranger. 4 L'exploitation de secours visée à l'al. 3 est limitée dans le temps. L'OFCOM en fixe la durée maximale et les conditions de prolongation. 5 Les concessionnaires de radiocommunication mobile et les opérateurs de réseaux mobiles virtuels complets qui recourent à un système redondant visé à l'al. 3 doivent en informer l'OFCOM au plus tard 48 heures après le début de l'exploitation de secours. 6 Les systèmes redondants visés à l'al. 3 et qui sont situés à l'étranger peuvent être exploités uniquement avec des clés cryptographiques et des certificats dérivés ou temporaires. Les clés sont générées, activées et désactivées exclusivement par des modules de sécurité matérielle exploités en Suisse et certifiés selon des normes reconnues. 7 Tout accès au matériel de cryptage doit être consigné. Les documents doivent être conservés au moins trois ans et remis à l'OFCOM sur demande.	
Art. 96*fbis* *Mesures de sécurité* 1 Les concessionnaires de radiocommunication mobile et les opérateurs de réseaux mobiles virtuels complets prennent les mesures techniques, organisationnelles et opérationnelles nécessaires pour garantir la sécurité des infrastructures de télécommunication et prévenir les cybermenaces. 2 Les concessionnaires de radiocommunication mobile et les opérateurs de réseaux mobiles virtuels complets veillent à mettre en service des infrastructures matérielles et logicielles de leurs réseaux qui ne soient pas compromises. Ils installent et appliquent toutes les options de sécurité standardisées. 3 Ils effectuent en temps réel une surveillance permanente et systématique de détection des vulnérabilités, des anomalies et des intrusions dans leurs réseaux. 4 Ils partagent les informations concernant les vulnérabilités, les anomalies et les intrusions qu'ils ont détectées et s'accordent sur les meilleures pratiques actuelles. En cas de cyberattaque, ils s'informent mutuellement de l'état de leurs réseaux. Ils coopèrent pour en atténuer les conséquences et supprimer la menace. 5 Ils utilisent un système de redirection des messages SMS forçant ceux-ci à transiter dans tous les cas par la Suisse. 6 Ils effectuent des filtrages des messages de signalisation en utilisant des outils de filtrage et en se basant sur des méthodologies conformes aux recommandations et normes reconnues au niveau international. L'OFCOM peut préciser les recommandations et normes reconnues.	**Commentaires :** Les alinéas 1 à 4 restent formulés de manière trop générale (« mesures techniques, organisationnelles et opérationnelles nécessaires », « toutes les options de sécurité standardisées », « surveillance permanente », « coopèrent pour... supprimer la menace »). Il serait judicieux qu'une ordonnance propose des dispositions plus précises et non des formulations générales qui auraient leur place dans une loi et non dans une ordonnance. **Ad art. 96fbis al. 3**: Le rapport explicatif fait état, en lien avec cette disposition, d'une obligation d'annonce aux polices et autorités fédérales concernées de tout danger imminent. Cette obligation d'annonce ne figure pas dans l'art. 96fbis du projet OST, alors qu'elle le devrait.

Art. 96g al. 2 1 [...] 2 S'il existe un soupçon fondé de violation du droit et que cela s'avère nécessaire pour constater les faits, l'OFCOM peut obliger les concessionnaires de radiocommunication mobile et les opérateurs de réseaux mobiles virtuels complets à se soumettre à leurs frais à un audit réalisé par un organisme qualifié ou à faire contrôler leurs installations de télécommunication. .	
Art. 96h Obligation de préparation et étendue de la garantie **(EN VIGUEUR)** 1 En cas de panne d'électricité ne dépassant pas 4 heures, suivie d'une phase d'alimentation au moins deux fois aussi longue que la panne, les concessionnaires de radiocommunication mobile doivent prendre les mesures nécessaires pour assurer les services de télécommunication visés à l'art. 94a, al. 4 et 5, ainsi que le service d'accès à Internet. 2 En cas de panne d'électricité visée à l'al. 1, ils doivent garantir que, dans chaque commune, au moins 99% de leurs clients disposent d'un accès aux services de télécommunication mobile à l'adresse figurant sur leur contrat. 3 Si la couverture n'atteint pas 99% en situation normale, ils doivent au moins garantir la couverture habituelle. 4 En cas d'autres perturbations de l'approvisionnement en électricité, les services de télécommunication doivent être assurés autant que possible.	**Ad art. 96h OST en vigueur :** Cette disposition n'est pas concernée par le projet de révision. En revanche, elle fixe la durée minimale de maintien en fonction des réseaux de télécommunication. L'exigence porte sur une durée de 4 heures : elle correspond au scénario de délestage en cas de pénurie d'électricité qui table sur des périodes de coupure de courant de 4h pour 8h de fonctionnement. Cependant, il y a une insuffisance de prise en compte de l'aspect énergétique et le scénario du black-out n'est absolument pas couvert avec cet objectif de durée. La rupture massive d'électricité est une menace qui doit être dûment prise en considération compte tenu de sa probabilité et de ses conséquences lourdes pour la population. Les appels d'urgence doivent tout particulièrement être possibles en pareille situation, sous peine d'atteinte grave à l'intégrité de la population. Les données du scénario d'un black-out tablent **sur une durée de 72h**, c'est cette durée qui doit dicter l'objectif de maintien d'une alimentation de secours. Cette réflexion s'inscrit pleinement dans le cadre du rapport explicatif, dans le passage consacré à l'art. 2 al. 1 let. c et cbis du projet d'OIT qui insiste sur la définition des installations critiques dont la défaillance peut mettre en danger la sécurité publique. **Proposition** : Compléter le projet de révision par une adaptation de l'art. 96h OST, afin de passer à une durée de 72h.