



Genève, le 16 septembre 2026

Le Conseil d'Etat

2321-2026

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 : révision partielle de la loi sur les télécommunications (LTC) dans le domaine de la sécurité

Monsieur le Conseiller fédéral,

Notre Conseil a bien reçu votre courrier du 27 mai 2026, par lequel vous l'avez invité à se prononcer dans le cadre de la procédure de consultation relative à la révision partielle de la loi du 30 avril 1997 sur les télécommunications (LTC) dans le domaine de la sécurité, et il vous en remercie.

Ce projet de révision est, dans son principe, favorablement accueilli. Des infrastructures de télécommunication sûres, disponibles et résilientes sont en effet essentielles pour la population, l'économie et les autorités, notamment pour garantir une communication efficace en situation d'urgence. La numérisation croissante, la complexité technique et l'évolution du contexte des menaces démontrent la nécessité de renforcer la robustesse des communications d'urgence sur les plans juridique, technique et organisationnel.

Notre Conseil salue le renforcement des communications d'urgence prévu aux art. 20 à 20e LTC, notamment la clarification des fonctions système, les mécanismes de secours, la redondance des réseaux, la coordination centralisée et les tests de bout en bout obligatoires. Il soutient également l'utilisation du Real-Time Text (RTT) et de la « Total Conversation », qui améliorent l'accès aux services d'urgence pour les personnes en situation de handicap ou en danger.

Cependant, la rédaction des articles 6a et 6b du projet nous apparaissent insatisfaisantes et ont généré d'importantes critiques de fond au point que nous recommandons qu'elles soient complètement réécrites, notamment en ce qui concerne la situation des lignes téléphoniques et des autres services de communication sous écoute.

Il est notamment impératif que le Service de surveillance de la correspondance par poste et télécommunication (Service SCPT) soit dans l'obligation de consulter l'autorité de poursuite pénale qui a ordonné la mesure de surveillance, car ce n'est pas au Service SCPT qu'appartient le pouvoir de décider si le blocage peut avoir lieu ou non.

De même, le rôle que la loi prévoit de donner à l'Office fédéral de la police (fedpol) n'est pas adéquat, car il consacre une intrusion massive et excessive de la Confédération dans les compétences des autorités cantonales. Ces dernières doivent pouvoir ordonner elles-mêmes le blocage. Si une instance de coordination est souhaitée, fedpol devra se limiter strictement à cette fonction.

Il n'est, de plus, pas nécessaire que le numéro de téléphone ou le nom de domaine reste bloqué "jusqu'à la clôture" de la procédure pénale, car il est envisageable qu'un blocage soit ordonné pendant une certaine période avant d'être levé.

Enfin, notre Conseil souhaite que la possibilité de blocage de numéros de téléphone et de noms de domaine soit étendue à d'autres infractions que la seule escroquerie et que leur durée soit augmentée. Cinq jours est un délai considéré comme trop court d'un point de vue opérationnel.

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

En vous remerciant de l'attention que vous voudrez bien prêter à nos observations, nous 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 Hiltbold

Annexe mentionnée

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

Tableau de travail – avant-projet et remarques du CE

Source : présentation synoptique des modifications prévues par rapport au droit en vigueur, DETEC/OFCOM, 27 mai 2026.

Avant-projet (modification)	Remarques du CE
I. Loi du 30 avril 1997 sur les télécommunications¹	
Préambule vu les art. 92, 97, al. 1, et 173, al 2, de la Constitution fédérale	
<i>Remplacement d'une expression</i> Dans tout l'acte, « assistance administrative » est remplacé par « assistance administrative et entraide judiciaire ».	
Art. 1, al. 1 et 2, let. b et f ¹ La présente loi a pour but d'assurer aux particuliers et aux milieux économiques des services de télécommunication variés, avantageux, de qualité, sûrs et concurrentiels sur le plan national et international. ² Elle doit en particulier : a. [...]; b. assurer que le trafic des télécommunications ne soit pas perturbé, qu'il soit sûr, qu'il respecte les droits de la personnalité et les droits immatériels et qu'il garantisse une protection contre les cybermenaces ; c. [...]; d. [...]; e. [...]; f. garantir la sécurité et la résilience des infrastructures de télécommunication	Art. 1 alinéa 1 (Buts) L'introduction de la protection contre les cybermenaces est favorablement accueillie. Let. b) Il est peut-être avantageux de reprendre in extenso les définitions figurant dans la LSI ce qui permettrait de rendre autonome le champ d'application de la LTC et d'en augmenter au besoin la portée. Actuellement, la cybermenace est constituée par tout événement pouvant entraîner un incident qui nuit à la confidentialité, à la disponibilité ou à l'intégrité des informations ou à la transparence de leur traitement lors de l'utilisation de techniques de l'information et de la communication. La protection contre les cyberattaques devrait être expressément mentionnées pour affirmer l'importance de la LTC d'un point de vue de la défense stratégique du pays.
Art. 3, let. d Au sens de la présente loi, on entend par a. [...]; b. [...]; c. [...]; c ^{bis.} [...]; c ^{ter.} [...]; d. installation de télécommunication : les appareils, y compris leurs logiciels, les lignes ou équipements destinés à transmettre des informations au moyen de techniques de télécommunication ou utilisés à cette fin; d ^{bis.} et d ^{ter.} [...]; e. [...]; e ^{bis.} [...]; e ^{ter.} [...]; f. [...]; g. [...]; h. [...].	

Avant-projet (modification)	Remarques du CE
Insérer avant le titre du chapitre 2 Art. 3a Droits et obligations des propriétaires et des exploitants d'installations de télécommunication ou de canalisations de câbles ¹ Les droits et obligations des fournisseurs de services de télécommunication, tels que prévus aux art. 35 à 37, s'appliquent par analogie aux : a. propriétaires et exploitants d'installations de télécommunication destinées à la fourniture de services de télécommunication qui mettent celles-ci à la disposition de tiers ou envisagent de le faire ; b. propriétaires de canalisations de câbles qui mettent celles-ci à la disposition de tiers ou envisagent de le faire. ² Dans la mesure où une concurrence efficace en matière de services de télécommunication l'exige, le Conseil fédéral peut prévoir que d'autres dispositions de la présente loi qui règlent les droits et les obligations des fournisseurs de services de télécommunication s'appliquent par analogie aux propriétaires et aux exploitants d'installations de télécommunication ou de canalisations de câbles visés à l'al. 1.	
Art. 3b Ex-art. 3a	
Art. 3b Rapport d'évaluation ¹ Tous les trois ans, le Conseil fédéral rend compte à l'Assemblée fédérale: a. de l'évolution des investissements réalisés à l'échelle de la Suisse; b. de l'évolution du service universel; c. de la qualité et des prix des services de télécommunication proposés; d. de l'évolution de la concurrence en matière de réseaux; e. des coûts et de la garantie de l'accès aux raccordements d'abonné, quelle que soit la technologie utilisée pour ces raccordements. ² Le cas échéant, il soumet à l'Assemblée fédérale des propositions visant à promouvoir une concurrence efficace.	
Art. 4 Enregistrement ¹ L'Office fédéral de la communication (OFCOM) enregistre les fournisseurs de services de télécommunication qui utilisent l'une des ressources suivantes destinées à la fourniture de services de télécommunication : a. fréquences de radiocommunication soumises à concession ; b. ressources d'adressage gérées au niveau national. ² Les fournisseurs enregistrés ne peuvent accorder l'utilisation des ressources visées à l'al. 1 à d'autres fournisseurs de services de télécommunication que si ceux-ci se sont fait préalablement enregistrer. ³ L'OFCOM peut enregistrer d'autres fournisseurs de services de télécommunication qui proposent des services d'importance technique ou économique majeure dans le domaine des télécommunications. Il peut également enregistrer les propriétaires et exploitants d'installations de télécommunication destinées à la fourniture de services de télécommunication, ainsi que les propriétaires de canalisations de câbles qui mettent ces installations et canalisations à disposition de tiers pour une utilisation en Suisse. ⁴ Il tient une liste des fournisseurs, propriétaires et exploitants enregistrés, y compris les propriétaires et exploitants visés à l'art. 4a, et de leurs offres de services ou d'installations de	L'article 4 ne traite pas des communications directes par satellite de type Starlink. Il serait sans doute opportun de le mentionner ce type de fournisseur (fournisseur par satellite) de manière explicite, ce d'autant plus que le rapport explicatif n'évoque pas ce type de fournisseur en lien avec l'alinéa 3.

Avant-projet (modification)	Remarques du CE
télécommunication ; il peut publier cette liste. ⁵ Le Conseil fédéral règle les modalités de l'enregistrement. Il peut prévoir des exceptions à l'enregistrement prévu à l'al. 1 si la fourniture de services de télécommunication est limitée temporellement ou géographiquement.	
Art. 4a Obligation d'annoncer ¹ Les propriétaires ou exploitants d'installations de télécommunication qui sont destinées à la fourniture de services de télécommunication et qui raccordent des bâtiments doivent s'annoncer à l'OFCOM. Celui-ci enregistre les propriétaires et exploitants annoncés. ² Le Conseil fédéral règle les modalités de l'annonce.	
Art. 6a Blocage de l'accès à la téléphonie et à internet ¹ Les fournisseurs de services de télécommunication bloquent l'accès à la téléphonie et à internet des personnes : a. qui, auprès du fournisseur : 1. ont utilisé une identité fictive ; 2. ont utilisé l'identité d'une personne qui ne voulait pas conclure de contrat avec le fournisseur ; b. qui se sont identifiées auprès du fournisseur au moyen d'un document qui ne remplit pas les exigences de la loi fédérale du 18 mars 2016 sur la surveillance de la correspondance par poste et télécommunication (LSCPT) ; c. si, pour des raisons techniques ou juridiques, le document au moyen duquel la personne s'est identifiée auprès du fournisseur à l'étranger n'a pas été transmis aux autorités compétentes en Suisse. ² Les autorités compétentes veillent à ne pas procéder à un blocage si elles ont connaissance que l'accès à internet ou à la téléphonie fait l'objet d'un mandat de surveillance du Service de surveillance de la correspondance par poste et télécommunication (Service SCPT). Dans ce cas, une consultation avec le Service SCPT a lieu.	Art. 6a (Blocage de l'accès à la téléphonie et à internet) Ce nouvel article qui étend l'obligation de blocage à la charge des fournisseurs de services de télécommunication répond à la lacune de la situation actuelle qui limite cette obligation aux seules offres de produits hors abonnement, ce qui est en effet largement insatisfaisant. L'article 6a alinéa 1 n'inclut pas la possibilité de faire bloquer l'accès à la téléphonie même lorsque le numéro de téléphone a bien été enregistré correctement, mais qu'il est manifestement utilisé à des fins abusives. L'article 6a alinéa 1 devrait être complété par une lettre d) libellée comme suit : « Lorsque le numéro de téléphone a bien été enregistré correctement, mais qu'il est manifestement utilisé à des fins abusives. » L'article 6a al. 2 n'est pas satisfaisant et il serait nécessaire de le reformuler de manière à ce que l'objectif soit clair. Est-il voulu que seules les autorités puissent procéder à ces blocages et non les fournisseurs de services de télécommunication ? Est-il possible de procéder quelles autorités sont compétentes ? Plus largement, les autorités compétentes ne peuvent avoir connaissance d'un mandat de surveillance sans le concours du SCPT. Dès lors, il faudrait inverser la logique en allant dans le sens suivant : dans le cadre de procédure de blocage, les autorités compétentes consultent systématiquement le SCPT afin de déterminer si l'accès à internet ou à la téléphonie fait l'objet d'un mandat de surveillance. L'obligation du Service SCPT de consulter l'autorité de poursuite pénale qui a ordonné la mesure de surveillance doit impérativement être mentionnée dans la loi. Ce n'est en effet pas au Service SCPT seul de décider si le blocage peut avoir lieu ou non : seule l'autorité de poursuite pénale qui a ordonné la surveillance doit pouvoir trancher cette question.
Art. 6b Blocage de numéros de téléphone et de noms de domaine ¹ En cas de soupçons fondés d'escroquerie présumée au sens de l'art. 146 du Code pénal (CP)⁷, les fournisseurs de services de télécommunication sont tenus, sur signalement de l'Office fédéral de la police (fedpol), de bloquer le numéro de téléphone suisse concerné ; le blocage dure cinq jours au maximum. ² L'al. 1 s'applique également aux registres d'un domaine s'agissant du blocage d'un nom de domaine de deuxième niveau subordonné à un domaine internet, dont la gestion relève de la	Art. 6b Blocage de numéros de téléphone et de noms de domaine Cet article est approuvé dans son principe, mais le dispositif prévu est bancal et il est nécessaire de le repenser dans le détail. Le Pouvoir Judiciaire estime qu'un important travail de réflexion doit être conduit avant une réécriture complète de cette disposition. 6b Alinéa 1 à 5 : • La notion de "soupçons fondés" n'est pas adéquate. Il est évident qu'en début d'enquête, un soupçon est un soupçon. Si l'on exige un niveau d'indice trop élevé, aucun blocage ne

Avant-projet (modification)	Remarques du CE
compétence de la Suisse. ³ L'Office fédéral de la cybersécurité (OFCS) assiste fedpol dans l'évaluation des conditions énoncées aux al. 1 et 2, et lui transmet à cette fin des informations provenant de signalements au sens de l'art. 73d de la loi fédérale du 18 décembre 2020 sur la sécurité de l'information. ⁴ Le ministère public ou le tribunal compétent peut ordonner que le numéro de téléphone ou le nom de domaine reste bloqué jusqu'à la clôture de la procédure pénale. ⁵ Les autorités compétentes veillent à ne pas procéder au blocage d'un numéro de téléphone si elles ont connaissance que celui-ci fait l'objet d'un mandat de surveillance du Service SCPT. Dans ce cas, une consultation avec le Service SCPT a lieu.	sera jamais ordonné. • Il est totalement injustifié de limiter l'obligation de blocage au seul cas d'escroquerie (art. 146 CP). De nombreuses autres infractions sont susceptibles d'être commises par le biais des services de télécommunication, telles que la diffusion de pédopornographie, par exemple. De manière générale, tous les crimes et délits devraient pouvoir donner lieu à un tel blocage. • Le rôle qu'il est prévu de donner à fedpol n'est pas adéquat. Si l'on peut concevoir que l'office fédéral de la police soit informé d'un certain nombre de situations, notamment qui lui seraient signalées par l'OFCS, la majorité des cas seront connus par les autorités de poursuite pénale cantonales, compétentes pour la poursuite des escroqueries (et de la plupart des autres infractions, si la liste des infractions donnant lieu au blocage est étendue comme souhaité). Cela signifie que si des autorités de poursuite pénale cantonales (police ou ministère public) sont informées de situations devant donner lieu à des blocages, elles devront saisir fedpol. Outre que la loi ne le prévoit pas, cela signifie une intrusion massive de la Confédération dans les compétences cantonales, ce qui n'est pas acceptable. Les autorités de poursuite cantonales doivent pouvoir ordonner elle-même le blocage. Subsidiairement, si l'on souhaite une instance de coordination, le rôle de fedpol devra alors être strictement limité à cette fonction, sans aucune possibilité de rejeter les requêtes. A tout le moins, non seulement fedpol peut présenter une demande, mais aussi les autorités cantonales et communales compétentes. • La durée du blocage est de cinq jours. Rien n'est dit de ce qui est censé se produire pendant le délai en question. Or, pour que le blocage ait une quelconque utilité, il faut que les autorités de poursuite pénale, compétentes pour ordonner le maintien du blocage au sens de l'alinéa 4, en soient informées (un peu sur le modèle du blocage institué par la LBA). Il est impératif de le mentionner expressément dans la loi. • Par ailleurs, ce délai de cinq jours est trop court. L'autorité qui a ordonné le blocage devra, pour saisir l'autorité judiciaire compétente pour ordonner le maintien du blocage au sens de l'alinéa 4, réunir les informations disponibles sur le cas, de manière à permettre l'ouverture d'une enquête. Le ministère public concerné devra ensuite prendre les dispositions nécessaires. Pour l'ensemble de ces actes, un délai d'au moins 10 jours est à prévoir, sinon davantage. • Le rôle du ministère public compétent au sens de l'alinéa 4 n'est pas suffisamment défini. On comprend qu'il s'agit de lui donner la compétence d'ordonner le maintien du blocage. Cela suppose que cette compétence soit concrètement donnée aux ministères publics, ce qui suppose une modification du CPP. On ne voit pas, sans cela, par quel acte de procédure le ministère public pourrait ordonner la prolongation du blocage. Une telle prolongation doit en effet prendre la forme d'un acte formel sujet à recours. L'on ne voit pas non plus pourquoi le ministère public devrait nécessairement ordonner que le numéro de téléphone ou le nom de domaine reste bloqué "jusqu'à la clôture" de la procédure pénale. Il est parfaitement envisageable qu'un numéro ou un nom de domaine soit bloqué pendant une certaine période, puis le blocage levé. • Enfin, la même remarque prévaut, s'agissant de l'alinéa 5, que pour l'alinéa 2 de l'article 6a. Il est impératif que le Service SCPT soit systématiquement consulté avant toute mesure de blocage et qu'il ait lui-même l'obligation de consulter l'autorité qui a ordonné une mesure de surveillance. 6b alinéa 5 : le titre de l'article 6b et son alinéa 4 font référence aux numéros de téléphone et aux noms de domaine Internet. L'alinéa 5 devrait également couvrir ces deux cas et il serait opportun d'adapter l'alinéa 5 de manière à ce que la surveillance des noms de domaine Internet soit

Avant-projet (modification)	Remarques du CE
	également couverte.
<i>Art. 13, al. 1 et 3</i> ¹ Pour autant qu'aucun intérêt public ou privé prépondérant ne s'y oppose, l'OFCOM fournit à la personne qui en fait la demande les informations suivantes : a. le nom et l'adresse : 1. des fournisseurs, propriétaires et exploitants enregistrés ; 2. des fournisseurs de services à valeur ajoutée ; b. le type de services proposés par les fournisseurs, les propriétaires et les exploitants ; c. les poursuites ou sanctions administratives et pénales dans le domaine des télécommunications concernant les fournisseurs, les propriétaires et les exploitants. ² [...]. ³ Abrogé	
<i>Art. 13a, al. 1</i> ¹ La ComCom, l'OFCOM et les délégataires visés aux art. 12c, 20b, 28a et 58, al. 1, peuvent traiter les données personnelles, y compris les données sur les poursuites ou sanctions administratives et pénales dans le domaine des télécommunications, si ces données sont nécessaires à l'exécution de leurs tâches au sens de la présente loi. ² [...]. ³ [...].	
<i>Art. 13b titre et al. 1 à 2bis et 4</i> Assistance administrative et entraide judiciaire ¹ La ComCom, l'OFCOM et les délégataires visés aux art. 12c, 20b, 28a et 58, al. 1, transmettent aux autorités suisses les données personnelles dont celles-ci ont besoin pour accomplir les tâches qui leur incombent de par la loi. Ils sont autorisés à communiquer des données sur les poursuites ou sanctions administratives et pénales dans le domaine des télécommunications, à condition que les autorités disposent d'une base légale leur permettant de traiter ces données. ² Ils peuvent transmettre à des autorités étrangères les données dont celles-ci ont besoin pour exercer la surveillance des fournisseurs de services de télécommunication, y compris des données sur les poursuites ou sanctions administratives et pénales dans le domaine des télécommunications. La transmission n'est autorisée que si les autorités étrangères sont liées, conformément à la loi de leur Etat, par le secret de fonction ou par le secret professionnel. ^{2bis} La transmission visée à l'al. 2 nécessite l'approbation préalable de la ComCom, de l'OFCOM et des délégataires visés aux art. 12c, 20b, 28a et 58, al. 1, ou doit être prévue dans un accord international. ³ [...]. ⁴ Les autorités suisses transmettent à la ComCom, à l'OFCOM et aux délégataires visés aux art. 12c, 20b, 28a et 58, al. 1, les données nécessaires à l'exécution de la législation sur les télécommunications, y compris des données sur les poursuites ou sanctions administratives et pénales dans le domaine des télécommunications.	13b alinéa 1 : la limitation aux données à caractère personnel risque de faire disparaître la base légale permettant la mise à disposition des cartes dites de couverture. L'Office fédéral de la communication (ci-après : OFCOM) doit ici préciser sur quelle base légale les cartes de couverture seront mises à disposition à l'avenir dans le cadre des recherches d'urgence. Il convient d'étendre cette disposition à la mise à disposition de cartes de couverture pour les recherches d'urgence et de ne pas la limiter à la seule mise à disposition de données personnelles. La problématique de la collecte de données sensibles et de leur transmission, notamment à des autorités étrangères pose question par rapport aux objectifs de la loi et à la protection de la sphère privée des citoyens. Les articles 13b al. 2, 30a al. 4, 34b et 48 d offrent de larges possibilités de collectes de données à des fins de profilage et de transmission des données sensibles à des autorités étrangères sans garde-fou apparent : des restrictions à ces collectes sont attendues pour préserver la sphère privée des citoyens.
<i>Art. 13c</i> Traitement et transmission des données de personnes morales ¹ Les art. 13a et 13b s'appliquent également au traitement et à la transmission des données de	

Avant-projet (modification)	Remarques du CE
personnes morales. ² La ComCom, l'OFCOM et les délégataires visés aux art. 12c, 20b, 28a et 58, al. 1, peuvent, dans le cadre de l'exécution de la législation sur les télécommunications, traiter des données relatives aux secrets professionnels, d'affaires et de fabrication.	
<i>Titre précédant l'art. 20</i> Section 3 Communication d'urgence	
Art. 20 Principes ¹ Les fournisseurs du service téléphonique public garantissent que la communication entre les utilisateurs et les centrales gérées par les services d'urgence et les services d'aide et de conseil (communication d'urgence) est possible en tout temps. ² Ils doivent garantir en particulier l'acheminement, la localisation et la redondance (solution de repli minimale). ³ Le Conseil fédéral peut, en tenant compte des intérêts respectifs de la population et des fournisseurs ainsi que de l'état de la technique et de l'harmonisation internationale : a. étendre aux fournisseurs d'autres services de télécommunication les obligations visées aux al. 1 et 2, dans la mesure où les services sont accessibles publiquement et largement utilisés ; b. prévoir des exceptions aux obligations visées à l'al. 2 ; c. prévoir que les fonctionnalités de localisation des terminaux puissent être utilisées sans l'accord exprès de l'utilisateur.	La disponibilité des réseaux d'appels d'urgence est essentielle pour garantir l'engagement rapide des moyens de secours. Les nouveaux art. 20ss du projet de LTC sont importants à cet égard et leur objectif est expressément approuvé.
Art. 20a Tâches systémiques ¹ La communication d'urgence est garantie, par un ou plusieurs fournisseurs, au moyen des tâches d'ordre supérieur suivantes (tâches systémiques) : a. l'exploitation d'un réseau destiné uniquement aux communications d'urgence et disponible en tout temps ; b. l'exploitation redondante par un deuxième fournisseur de tout ou partie du réseau visé à la let. a ; c. l'exploitation d'un service de localisation ; d. l'exploitation d'un organe de coordination central, disponible en tout temps, pour les communications d'urgence critiques ; e. l'exploitation d'une plateforme de test et d'intégration permettant de réaliser des tests de bout en bout ; f. la collecte des données pour le contrôle des exigences qualitatives. ² Pour garantir la communication d'urgence, les fournisseurs sont tenus de respecter les exigences techniques découlant des tâches systémiques. ³ L'OFCOM édicte les prescriptions techniques et administratives relatives aux tâches systémiques et définit les exigences que les fournisseurs concernés doivent remplir pour garantir la disponibilité des tâches systémiques	La disponibilité des réseaux d'appels d'urgence est essentielle pour garantir l'engagement rapide des moyens de secours. Les nouveaux art. 20ss du projet de LTC sont importants à cet égard et leur objectif est expressément approuvé. La volonté exprimée dans le rapport explicatif d'une disponibilité permanente des appels d'urgence et l'objectif énoncé par l'art. 1 al. 2 let. f du projet LTC de garantir la sécurité des infrastructures de communication en les préservant de toute panne doit impérativement intégrer la dimension énergétique (alimentation électrique des équipements des réseaux). Cet élément est insuffisamment pris en compte. Proposition : compléter le projet de révision de l'OST pour intégrer cette dimension, notamment par une adaptation de l'art. 96h OST, afin de passer à une durée de 72h. Article 20a, alinéa 1, lettre b doit être considéré comme une condition impérative au regard du critère de résilience
Art. 20b Obligation d'offrir des tâches systémiques ¹ Si l'OFCOM constate qu'une ou plusieurs tâches systémiques ne sont pas assurées, il peut contraindre un ou plusieurs fournisseurs à les garantir. ² Si plusieurs fournisseurs entrent en considération pour la réalisation d'une tâche systémique, l'OFCOM organise une procédure d'appel d'offres ou d'invitation à soumissionner. Le droit des marchés publics ne s'applique pas. ³ Il peut désigner un fournisseur sans procédure d'appel d'offres ou d'invitation à soumissionner, si	Article 20b, alinéa 1 : le choix de la forme potestative peut laisser entendre qu'une lacune dans l'exécution de tâches dites systémiques pourrait découler d'une absence d'intervention de l'OFCOM. Pour lever cette ambiguïté, nous proposons de remplacer le verbe « pouvoir » par le verbe « devoir » ou par « contraint » à l'indicatif présent. Recommandation : « Si une ou plusieurs tâches systémiques ne sont pas assurées, l'OFCOM

Avant-projet (modification)	Remarques du CE
l'une des conditions suivantes est remplie : a. aucune procédure d'appel d'offres ou d'invitation à soumissionner ne peut être organisée pour cause d'urgence ; b. une étude de marché a été réalisée et montre qu'aucun appel d'offres ne peut se dérouler dans des conditions de concurrence ; c. une procédure d'appel d'offres a été organisée, mais aucune offre répondant aux exigences n'a été soumise.	contraint/doit contraindre un ou plusieurs fournisseurs à les garantir. » Article 20b, alinéa 3, lettre a : si l'alinéa 1 est adapté, cette lettre n'est plus nécessaire et peut être supprimée. « aucune procédure d'appel d'offres ou d'invitation à soumissionner ne peut être organisée pour cause d'urgence »
Art. 20c Prise en charge des coûts ¹ Les fournisseurs tenus de garantir la communication d'urgence prennent en charge les coûts imputables aux tâches systémiques. ² Les utilisateurs de la plateforme de test et d'intégration visée à l'art. 20a, al. 1, let. e, prennent en charge une partie appropriée des coûts imputables.	Article 20c, alinéa 2 : cette prise en charge des coûts est le seul moyen de garantir le financement de la plateforme tout au long de son cycle de vie. De plus, elle permet de faire supporter les coûts par ceux qui les génèrent et non par la collectivité. La notion de coût imputable peut être remplacée en mentionnant expressément le critère de la consommation. Nous suggérons la rédaction suivante : « <i>Les utilisatrices et utilisateurs de la plateforme de test et d'intégration visée à l'article 20a alinéa 1er lettre e prennent en charge une part des coûts totaux liés à l'utilisation de cette plateforme, proportionnelle à leur consommation.</i> »
Art. 20d Tests de bout en bout Les tests de bout en bout concernant l'accès à la communication d'urgence doivent être réalisés sur la plateforme de test et d'intégration visée à l'art. 20a, al. 1, let. e, et coordonnés par l'organe de coordination visé à l'art. 20a, al. 1, let. d.	L'article 20d est considéré comme très positif dans la mesure où il permet de soulager les centrales d'appel concernées, qui peuvent ainsi se concentrer sur leurs missions essentielles.
Art. 20e Protection de l'intégrité de la communication d'urgence ¹ Les fournisseurs de services de télécommunication tenus de garantir la communication d'urgence prennent des mesures visant à protéger l'intégrité de la communication d'urgence. ² Ils s'appuient en particulier sur les indications de l'organe de coordination visé à l'art. 20a, al. 1, let. d. Ils prennent des mesures immédiatement et les maintiennent aussi longtemps que nécessaire. ³ Ils sont autorisés à déconnecter les utilisateurs du réseau aux fins prévues à l'al. 1. ⁴ Le Conseil fédéral définit les mesures techniques et organisationnelles que les fournisseurs visés à l'al. 1 doivent prendre.	Article 20e, alinéa 1 : les fabricants d'installations de télécommunications et de terminaux doivent également être tenus responsables en raison du risque de plus en plus important pour l'intégrité des communications d'urgence. Nous suggérons la rédaction suivante. « <i>Les fournisseurs de services de télécommunications, les fabricants d'installations de télécommunications et de terminaux tenus d'assurer les communications d'urgence prennent, dans la mesure de leur influence, des mesures visant à protéger l'intégrité des communications d'urgence.</i> »
<i>Titre précédent l'art. 21</i> Section 3a Obligations découlant de la fourniture de certains services	
Art. 29 ¹ Les titulaires de ressources d'adressage et les délégataires visés à l'art. 28a sont tenus de fournir à l'autorité compétente les renseignements dont celle-ci a besoin pour gérer les ressources d'adressage attribuées. ² Les services privés et publics reconnus chargés de la cybersécurité peuvent collaborer entre eux et avec les délégataires visés à l'art. 28a, dans le but d'identifier et d'évaluer les risques liés aux cybermenaces. ³ Le Conseil fédéral fixe les critères de reconnaissance des services privés et publics.	

Avant-projet (modification)	Remarques du CE
Art. 30a Traitement des données, assistance administrative et entraide judiciaire ¹ Pour l'exécution des tâches prévues à l'art. 28d, let. a, et la mise en œuvre de l'art. 28e, let. c, l'OFCOM et les délégataires visés à l'art. 28a sont habilités à effectuer des profilages, au besoin sans que la personne concernée n'en ait connaissance, et à traiter les données personnelles sensibles suivantes : a. données biométriques permettant l'identification univoque d'une personne physique ; b. données sur les poursuites ou sanctions administratives et pénales. ² Ils peuvent transmettre ces données et les résultats des profilages aux autorités suisses chargées de la protection contre les cybermenaces et à d'autres services privés et publics reconnus chargés de la cybersécurité, pour autant que ces autorités disposent d'une base légale correspondante dans le cadre de l'exécution de tâches liées à la protection contre les cybermenaces. ³ Le Conseil fédéral règle les modalités du traitement des données personnelles sensibles et de la réalisation de profilages. ⁴ Les art. 13a et 13b s'appliquent au traitement de ces données et à leur transmission à des autorités suisses ou étrangères.	La problématique de la collecte de données sensibles et de leur transmission, notamment à des autorités étrangères, pose question par rapport aux objectifs de la loi et à la protection de la sphère privée des citoyens. Les articles 13b al. 2, 30a al. 4, 34b et 48 d offrent de larges possibilités de collectes de données à des fins de profilage et de transmission des données sensibles à des autorités étrangères sans garde-fou apparent : des restrictions à ces collectes sont attendues pour préserver la sphère privée des citoyens.
Art. 32a Interdiction des installations de radiocommunication et autres installations et dispositifs perturbateurs ¹ La fabrication, l'importation, l'offre, la mise à disposition sur le marché, la possession, la mise en service, la mise en place ou l'exploitation d'installations de radiocommunication ou d'autres installations et dispositifs destinés à perturber ou à empêcher le trafic des télécommunications ou la radiodiffusion, sont interdites. ² Sont également considérés comme des installations et dispositifs perturbateurs : a. les dispositifs destinés à rendre des installations de télécommunication ou des installations à fort et à faible courant inutilisables au moyen d'ondes électromagnétiques ; b. les installations de télécommunication destinées à empêcher, à des fins autres que leur propre protection, le trafic des télécommunications de tiers. ³ L'interdiction prévue à l'al. 1 ne s'applique pas aux installations et dispositifs utilisés par les autorités pour garantir la sécurité publique. L'art. 32b est réservé.	
Art. 32b Installations de télécommunication et autres installations et dispositifs destinés à garantir la sécurité publique ¹ Le Conseil fédéral réglemente l'importation, l'offre, la mise à disposition sur le marché, la mise en service, la mise en place et l'exploitation des installations de télécommunication et des autres installations et dispositifs au sens de l'art. 32a dont les autorités doivent disposer pour garantir la sécurité publique. ² Les autorités suivantes peuvent mettre en place, mettre en service ou exploiter une installation perturbatrice aux fins ci-après : a. les autorités de police, de poursuite pénale et d'exécution des peines, pour garantir la sécurité publique et l'administration de la justice pénale ; b. le Service de renseignement de la Confédération, pour garantir la protection et la sécurité de ses collaborateurs, de ses informations et de ses installations ; c. l'armée, pour garantir la défense du pays ; d. les autorités compétentes, pour effectuer des recherches en cas d'urgence ou des recherches de personnes condamnées, aux fins de ces recherches. ³ Quiconque offre ou met à disposition sur le marché de telles installations et dispositifs doit fournir à l'OFCOM toutes les informations dont celui-ci a besoin. Les informations mises à disposition, les installations et dispositifs en question ainsi que les informations concernant les autorités qui utilisent ces installations et dispositifs, sont classés « confidentiels » par l'OFCOM.	

Avant-projet (modification)	Remarques du CE
Art. 34 Perturbations ¹ La mise en place et l'exploitation d'installations de télécommunication dans le but de perturber ou d'empêcher le trafic des télécommunications ou la radiodiffusion sont interdites. ² Si une installation de télécommunication ou une installation à fort ou à faible courant perturbe ou empêche le trafic de télécommunications ou la radiodiffusion, l'OFCOM peut contraindre l'exploitant à modifier l'installation à ses propres frais ou à en suspendre l'exploitation, même si elle répond aux prescriptions relatives à l'importation, à l'offre, à la mise à disposition sur le marché, à la mise en service, à la mise en place et à l'exploitation. ³ L'OFCOM peut limiter ou interdire l'offre et la mise à disposition sur le marché d'installations de radiocommunication qui perturbent ou peuvent perturber les utilisations du spectre des fréquences nécessitant une protection accrue. Il peut prendre ces mesures même si ces installations répondent aux prescriptions relatives à l'offre et à la mise à disposition sur le marché. ⁴ L'al. 2 est applicable lorsque des perturbations licites au sens de l'art. 32b portent atteinte de manière excessive à d'autres intérêts publics ou aux intérêts de tiers.	
Art. 34a Localisation des perturbations ¹ Pour déterminer l'origine des perturbations du trafic des télécommunications, de la radiodiffusion ou d'une installation à fort ou à faible courant, l'OFCOM a accès à toutes les installations de télécommunication et installations à fort et à faible courant. Sur demande, les fournisseurs, les propriétaires et les exploitants d'installations destinées à la fourniture de services de télécommunication doivent mettre à la disposition à l'OFCOM l'ensemble des informations techniques pertinentes relatives à la période en question, notamment sur les caractéristiques et paramètres de rayonnement des installations concernées. ² L'OFCOM peut, à des fins d'identification, détecter optiquement et de manière automatisée les véhicules émettant un signal perturbateur et si nécessaire les faire arrêter et les contrôler. Les données ainsi recueillies sont immédiatement supprimées si elles ne constituent pas des moyens de preuve. ³ Le Conseil fédéral règle les modalités relatives au système de détection optique automatisée à acquérir et les conditions d'anonymisation. Il fixe la durée de conservation des données constituant des moyens de preuve. ⁴ L'OFCOM règle les modalités relatives à l'obligation de mise à disposition des informations sur demande.	Art. 34a alinéa 1 : dans le cadre d'une intervention, les autorités compétentes ne sont pas toujours en mesure de fournir ces informations. Les exceptions prévues à l'article 32b alinéa 2 s'appliquent-elles également ici ? Si ce n'est pas le cas, il convient de prévoir une exception correspondante.
Art. 34b <i>Ex-art. 34a</i>	
Art. 34b Les art. 13a et 13b s'appliquent au traitement par l'OFCOM de données personnelles, y compris les données sur les poursuites ou sanctions administratives et pénales dans le domaine des télécommunications, nécessaires à l'exécution de ses tâches au sens des art. 31 à 34a, ainsi qu'à la transmission de ces données à des autorités suisses ou étrangères.	La problématique de la collecte de données sensibles et de leur transmission, notamment à des autorités étrangères pose question par rapport aux objectifs de la loi et à la protection de la sphère privée des citoyens. Les articles 13b al. 2, 30a al. 4, 34b et 48d offrent de larges possibilités de collectes de données à des fins de profilage et de transmission des données sensibles à des autorités étrangères sans garde-fou apparent : des restrictions à ces collectes sont attendues pour préserver la sphère privée des citoyens.
Art. 35b, al. 6 ¹ [...]. ² [...]. ³ [...].	

Avant-projet (modification)	Remarques du CE
⁴ [...]. ⁵ [...]. ⁶ L'OFCOM règle les modalités techniques de la co-utilisation. Il peut édicter des prescriptions techniques et administratives relatives à la construction et à la mise en place d'installations domestiques, pour autant que cela soit adéquat et nécessaire pour garantir un accès sûr, sans perturbation et non discriminatoire aux services de télécommunication publics.	
<i>Art. 46, al. 2</i> ² Il peut, en tenant compte des intérêts de la population, des personnes appelées et appelantes et des fournisseurs ainsi que de la technique et de l'harmonisation internationale, définir des exceptions et prévoir, pour les raccordements au réseau fixe de la police, des pompiers, des services sanitaires et de sauvetage, et des services d'aide et de conseil, la levée de la suppression de l'affichage des numéros même sans l'accord exprès des appelants.	
<i>Art. 46a</i> Protection des enfants et des jeunes ¹ Les fournisseurs d'accès à internet doivent conseiller leurs clients sur les possibilités qui existent en matière de protection des enfants et des jeunes et leur proposer des moyens pour protéger efficacement ceux-ci contre les contenus pornographiques. ² Le Conseil fédéral peut édicter d'autres dispositions en vue de protéger les enfants et les jeunes des dangers liés à l'utilisation des services de télécommunication. ³ L'OFCOM, fedpol et les services compétents des cantons coordonnent les mesures à prendre pour effacer rapidement et à l'échelon international les informations à caractère pornographique au sens de l'art. 197, al. 4 et 5, CP10. À cette fin, ils peuvent faire appel à des instances d'alerte gérées par des tiers ainsi qu'à des autorités à l'étranger, ou aider ces instances et ces autorités. Le Conseil fédéral règle les modalités. ⁴ Les fournisseurs de services de télécommunication suppriment les informations à caractère pornographique au sens de l'art. 197, al. 4 et 5, CP qui leur sont signalées par fedpol. Les fournisseurs de services de télécommunication signalent à fedpol les cas suspects d'informations à caractère pornographique au sens de l'art. 197, al. 4 et 5, CP qu'ils découvrent fortuitement dans le cadre de leurs activités ou que des tiers ont portés à leur connaissance par écrit.	L'art. 46a développe une approche trop libérale de la protection des enfants et jeunes. En lien avec la précédente prise de position du Conseil d'Etat sur la nouvelle loi sur les plateformes de communication (LPCom), il est attendu un cadre de protection plus marqué vis-à-vis des enfants et des jeunes. Les fournisseurs ont un pouvoir d'action et celui-ci va au-delà de la question de la pornographie. Art. 46a alinéa 1 : nous proposons d'inscrire « solutions » plutôt que « moyens », car la notion de « moyen » n'oblige à aucune garantie de résultat. Nous suggérons : « Les fournisseurs d'accès à internet doivent conseiller leurs clients sur les possibilités qui existent en matière de protection des enfants et des jeunes et leur proposer des moyens pour protéger efficacement ceux-ci contre les contenus pornographiques. »
<i>Art. 48a</i> Résilience des infrastructures de télécommunication et protection contre les cybermenaces ¹ Les fournisseurs de services de télécommunication prennent des mesures techniques, opérationnelles et administratives pour lutter contre toute manipulation non autorisée d'infrastructures de télécommunication par des transmissions au moyen de techniques de télécommunication, pour renforcer la résilience de ces infrastructures et pour garantir une protection contre les cybermenaces. Pour ce faire, ils sont autorisés à dévier ou à empêcher des communications et à supprimer des informations. ² L'OFCOM surveille, identifie et évalue les facteurs de risque susceptibles de menacer la résilience des infrastructures de télécommunication ou d'affecter la protection contre les cybermenaces. Il évalue en particulier s'il existe un risque pour la sécurité des infrastructures au sens de l'art. 48b. ³ Les fournisseurs de services de télécommunication doivent communiquer à l'OFCOM les informations, y compris les données relatives au trafic, nécessaires à l'exécution de ses tâches au sens de l'al. 2, dans la mesure où ils disposent de ces informations. Ils peuvent collaborer entre eux et avec les services privés et publics reconnus chargés de la cybersécurité pour identifier et évaluer les risques liés aux cybermenaces. ⁴ Le Conseil fédéral précise les mesures visées à l'al. 1. A des fins de protection contre les dangers,	

Avant-projet (modification)	Remarques du CE
de prévention des dommages et de réduction des risques, il peut édicter des dispositions sur la sécurité des informations et des infrastructures et services de télécommunication, en particulier concernant : a. la disponibilité ; b. l'exploitation ; c. la garantie d'infrastructures redondantes ; d. l'annonce de perturbations ; e. la traçabilité d'incidents ; f. la déviation ou l'empêchement de communications et la suppression d'informations au sens de l'al. 1.	
<i>Insérer avant le titre du chapitre 9</i> Art. 48b Sécurité des infrastructures de télécommunication ¹ Les fournisseurs de services de télécommunication doivent utiliser des infrastructures qui garantissent la confidentialité, l'intégrité et la disponibilité des services de télécommunication. Les paramètres de sécurité doivent être configurés et activés par défaut et tenus à jour. ² Les composants critiques de l'infrastructure d'un fournisseur de services de télécommunication doivent provenir de différents fabricants, dont au moins un doit avoir son siège dans un Etat dont la législation garantit une protection des données adéquate. Le Conseil fédéral règle les modalités ; il peut fixer des catégories, des parts et des pourcentages minimaux. ³ Si l'OFCOM constate un risque fondé pour la sécurité, il interdit aux fournisseurs de services de télécommunication de mettre en service les composants concernés. Il publie une liste des composants interdits, dont il peut ordonner la mise hors service ou le retrait. Concernant les composants nécessaires à la surveillance de la correspondance par poste et télécommunication au sens de la LSCPT11, il consulte au préalable le Service SCPT.	Les articles 48b al. 2 et 48 c al. 2 et 3 abordent la question de la souveraineté. Elles posent toutefois des exigences qui ne semblent pas propre à atteindre les objectifs visés : soit l'ensemble des composants doit être issue d'un Etat donc la législation garantit un niveau de protection des données adéquat, soit aucun... mais le fait d'avoir un seul composant n'apporte aucune garantie par rapport à l'objectif visé.
Art. 48c Mesures concernant les infrastructures de télécommunication face aux risques géopolitiques ¹ Le Conseil fédéral peut interdire l'acquisition, la mise en service et l'exploitation de composants d'une infrastructure de télécommunication qui proviennent de fabricants présentant un risque géopolitique pour la Suisse ou qui sont détenus, contrôlés ou sous l'influence d'un Etat étranger présentant un risque géopolitique pour la Suisse. ² Dans l'évaluation du risque géopolitique, il tient compte de la sécurité intérieure et extérieure ainsi que de la protection de la place industrielle, économique et financière de la Suisse en prenant en considération : a. les sanctions directes ou indirectes infligées aux fabricants en vertu de la loi du 22 mars 2002 sur les embargos; b. les dépendances économiques, technologiques et sécuritaires à l'égard des fabricants ou de la chaîne d'approvisionnement; c. les menaces pour la sécurité liées à des cyberattaques, des actes de sabotage et des activités de services de renseignement; d. la menace de sanctions ou d'embargos qui mettraient en péril la sécurité ou l'économie de la Suisse. ³ Le Conseil fédéral peut contraindre les fournisseurs de services de télécommunication à retirer de leur infrastructure de télécommunication les composants provenant des fabricants visés à l'al. 1. Ce faisant, il tient compte des conséquences économiques.	Les articles 48b al. 2 et 48 c al. 2 et 3 abordent la question de la souveraineté. Elles posent toutefois des exigences qui ne semblent pas propre à atteindre les objectifs visés : soit l'ensemble des composants doit être issue d'un état donc la législation garantit un niveau de protection des données adéquat, soit aucun...mais le fait d'avoir un seul composant n'apporte aucune garantie par rapport à l'objectif visé. Par ailleurs, si la pesée d'intérêt économique vient dans la balance, il conviendrait de développer, au moins dans le rapport explicatif, de quelle manière elle vient s'appliquer sans quoi les considérations économiques risquent de primer systématiquement sur les considérations sécuritaires.
Art. 48d Traitement des données et collaboration ¹ Pour exécuter les tâches visées aux art. 48a et 48b, l'OFCOM est habilité, au besoin sans que la personne concernée n'en ait connaissance, à effectuer des profilages et à traiter les données personnelles sensibles suivantes : a. données biométriques permettant l'identification univoque d'une personne physique ;	La problématique de la collecte de données sensibles et de leur transmission, notamment à des autorités étrangères pose question par rapport aux objectifs de la loi et à la protection de la sphère privée des citoyens. Les articles 13b al. 2, 30a al. 4, 34b et 48 d offrent de larges possibilité de collectes de données à des fins de profilage et de transmission des données sensibles à des autorités étrangères sans garde-fou apparent : des restrictions à ces collectes sont attendues pour préserver la sphères privée des citoyens.

Avant-projet (modification)	Remarques du CE
b. données sur les poursuites ou sanctions administrative et pénales. ² Il peut transmettre ces données et les résultats des profilages aux autorités suisses chargées de la protection contre les cybermenaces et à d'autres services privés et publics reconnus chargés de la cybersécurité visés à l'art. 29, pour autant que ces autorités disposent d'une base légale correspondante dans le cadre de l'exécution de tâches liées à la protection contre les cybermenaces. ³ Les fournisseurs de services de télécommunication peuvent collaborer entre eux et avec les services privés et publics reconnus chargés de la cybersécurité visés à l'art. 29 pour identifier et évaluer les risques liés aux cybermenaces. ⁴ Le Conseil fédéral règle les modalités du traitement des données personnelles sensibles et de la réalisation de profilages. ⁵ Les art. 13a et 13b s'appliquent au traitement de ces données par l'OFCOM et à leur transmission à des autorités suisses ou étrangères.	
<i>Art. 52, al. 1, let. g à j</i> ¹ Est puni d'une amende de 100 000 francs au plus quiconque : a. [...] b. [...] c. [...] d. [...] e. [...] f. [...] g. fabrique, importe, offre, met à disposition sur le marché, possède, met en service, met en place ou exploite des installations de radiocommunication ou d'autres installations et dispositifs destinés à perturber ou à empêcher le trafic des télécommunications ou la radiodiffusion ; h. rend inutilisables des installations de télécommunication ou des installations à fort et à faible courant au moyen d'ondes électromagnétiques ; i. empêche le trafic des télécommunications de tiers à des fins autres que leur propre protection ; j. met en place ou exploite des installations de télécommunication dans le but de perturber ou d'empêcher le trafic des télécommunications et la radiodiffusion. ² [...].	L'extension à l'ensemble du domaine des télécommunications est nécessaire.
<i>Titre précédant l'art. 58</i> Chapitre 11 Outils de surveillance et sanctions administratives	
Art. 59, al. 2 et 2bis, let. e ¹ [...]. ² Elles sont tenues de fournir régulièrement à l'OFCOM les informations nécessaires à l'élaboration d'une statistique fédérale sur les télécommunications. ^{2bis} Les données collectées ou communiquées à des fins statistiques ne peuvent être utilisées à d'autres fins que dans les cas suivants: a. [...]; b. [...]; c. [...]; d. [...]; e. ces données sont nécessaires pour actualiser les informations contenues dans la liste des enregistrements effectués en vertu des art. 4 et 4a. ^{2ter} [...]. ³ [...].	

Avant-projet (modification)	Remarques du CE
Art. 59a Atlas national de la large bande	
¹ Les fournisseurs de services de télécommunication et les propriétaires soumis à l'obligation d'annoncer visés à l'art. 4a sont tenus de fournir à l'OFCOM des données sur le raccordement des bâtiments par des installations de télécommunication. ² L'OFCOM utilise les données pour établir et publier un atlas national de la large bande. ³ Il peut publier les données également sous une autre forme. ⁴ Le Conseil fédéral détermine les données à fournir.	
Annexe	
II. Modification d'un autre acte	
Loi du 24 juin 1902 sur les installations électriques ¹³	
Art. 3, al. 1, 2, let. d, 2bis et 2ter ¹ Le Conseil fédéral édicte des prescriptions en vue de prévenir les dangers, les dommages et les perturbations causés par les installations à fort et à faible courant. ² Il règle : a. [...]; b. [...]; c. [...]; d. la protection du trafic des télécommunications et de la radiodiffusion ainsi que des installations à fort et à faible courant contre les perturbations électromagnétiques; il peut en particulier définir les exigences essentielles en matière de compatibilité électromagnétique des installations de ce type. ^{2bis} Il édicte les prescriptions visées à l'art. 2, let. d en tenant compte des réglementations internationales reconnues. ^{2ter} Il peut déléguer à l'Office fédéral de la communication (OFCOM) le soin d'édicter des prescriptions administratives et techniques. Celui-ci peut élaborer lui-même ou désigner des normes techniques qui, lorsqu'elles sont respectées, permettent de présumer que les exigences essentielles sont remplies, ou déclarer obligatoires des normes techniques, des actes juridiques de l'Union européenne ou d'autres règles. Il tient compte des normes internationales dans ce domaine. ³ [...]. ⁴ [...].	
Art. 21, al. 1, phrase introductive, et 2 ¹ Le contrôle de l'exécution des prescriptions mentionnées à l'art. 3, al. 2, let. a à c, est confié: a. [...]: 1. [...], 2. [...], 3. [...]; b. [...]. ² Le contrôle de l'exécution des prescriptions mentionnées à l'art. 3, al. 2, let. d, 2bis et ^{2ter}, est confié à l'OFCOM.	
Art. 22	

Avant-projet (modification)	Remarques du CE
Le Conseil fédéral peut substituer une inspection unique aux deux organes de contrôle prévus à l'art. 21, al. 1.	
Titre précédant l'art. 26b IVa. Perturbations	
Insérer avant le titre du chapitre V. Art. 26b ¹ Si une installation à fort ou à faible courant perturbe ou empêche l'utilisation d'une autre installation de ce type, l'OFCOM peut contraindre l'exploitant à modifier l'installation perturbatrice à ses propres frais ou à en suspendre l'exploitation. ² Pour déterminer l'origine des perturbations d'une installation à fort ou à faible courant, l'OFCOM a accès à toutes les installations de ce type. ³ Le Conseil fédéral règle les modalités.	