PROJET

Conformément à l'article 116, paragraphe 6, de la loi sur les communications électroniques (UL RS nº 130/22 et 18/23 — ZDU-1O), l'agence des réseaux et des services de communication de la République de Slovénie, en vertu de la procédure d'information instaurée par la directive (UE) 2015/1535 du Parlement européen et du Conseil du 9 septembre 2015 prévoyant une procédure d'information dans le domaine des réglementations techniques et des règles relatives aux services de la société de l'information (JO L 241 du 17.9.2015, p. 1), établit ce qui suit

LOI GÉNÉRALE
sur les exigences et restrictions supplémentaires en matière de sécurité

Article 1er
(Contenu de la loi générale)

La présente loi générale définit:

1. les lignes directrices à suivre par les opérateurs de réseaux de communications mobiles (ci-après dénommés les «opérateurs») qui fournissent ces réseaux à des entités essentielles, qui sont soit des gestionnaires d'infrastructures critiques dans d'autres domaines de la réglementation des infrastructures critiques, tels que définis par la loi sur le domaine des infrastructures critiques (ci-après dénommés les «gestionnaires d'infrastructures critiques»), soit des prestataires de services essentiels, tels que définis par la loi sur la sécurité de l'information (ci-après dénommés les «prestataires de services essentiels»), soit des organes administratifs de l'État, tels que définis par la loi sur la sécurité de l'information (ci-après dénommés les «organes d'administration de l'État»), soit des transporteurs d'éléments essentiels du système de sécurité du pays; et
2. les éléments critiques du réseau et des systèmes d'information associés avec leurs fonctionnalités visées à l'article 116, paragraphe 6, de la loi sur les communications électroniques (UL RS nº 130/22 et 18/23 — ZDU-1O), ci-après dénommée la «loi»), telle qu'elle figure en annexe, qui fait partie intégrante de la présente loi générale et qui est élaborée en coopération avec l'organe chargé de la sécurité de l'information.

Article 2
(Signification des termes)

(1) Les termes utilisés dans la présente loi générale répondent aux définitions ci-dessous.

1. Une chaîne d'approvisionnement est l'ensemble du système de processus, de personnes, d'organisation et de distribution intervenant dans la conception, la production, le stockage, la distribution et l'approvisionnement, ainsi que l'installation et la maintenance de composants d'éléments critiques installés sur le réseau de l'opérateur ou chez son prestataire de services cloud.

2. Les éléments critiques du réseau sont les éléments, fonctions, services et systèmes d'information supports du réseau, sous forme physique, logicielle ou virtuelle, au

niveau de l'opérateur ou du prestataire de services cloud, tels qu'ils sont énumérés à l'annexe de la présente loi générale.

3. Les entités essentielles sont soit des gestionnaires d'infrastructures critiques dans d'autres domaines de la réglementation des infrastructures critiques, soit des prestataires de services essentiels, tels que définis par la loi sur la sécurité de l'information, soit des organes d'administration de l'État, tels que définis par la loi sur la sécurité de l'information, soit des transporteurs d'éléments essentiels du système de sécurité du pays.

(2) Les autres termes utilisés dans la présente loi générale ont la même signification que celle définie par la loi et par la loi générale sur la sécurité des réseaux, des services et des données.

Article 3
(Orientations générales)

(1) Les opérateurs de la chaîne d'approvisionnement des composants d'éléments critiques du réseau, et des services de support de troisième niveau pour ces composants, doivent observer au moins les lignes directrices suivantes tout au long du cycle de vie desdits composants:

1. en vertu des relations et des accords conclus entre eux, chaque fabricant individuel, fournisseur et prestataire de services de support de troisième niveau procède à une évaluation des risques d'approvisionnement et d'incidences potentielles par des personnes physiques ou morales tierces de droit public ou privé (ci-après dénommés les «tiers»), ainsi que des risques de compatibilité avec les équipements d'autres fabricants, de qualité et de sécurité des produits et d'incidences négatives potentielles sur l'exploitation des services de l'opérateur et des entités essentielles;
2. la sécurité est intégrée et mise en œuvre dès la conception et les contrats prévoient des délais pour l'élimination des vulnérabilités perçues;
3. les principales caractéristiques de sécurité (disponibilité, confidentialité, intégrité et authenticité) sont assurées tout au long du cycle de vie de leur utilisation;
4. la sécurité et l'alimentation continue sont garanties et il est confirmé que le système prend en charge des dispositifs de sécurité élevée conformément aux normes internationalement reconnues (3GPP) et aux normes techniques européennes (ETSI);
5. les lignes directrices visées aux points 2 à 4 du présent paragraphe sont vérifiables dans la documentation contractuelle avec le fabricant ou avec le fournisseur;
6. pour chaque fabricant ou fournisseur, les risques liés aux droits d'utilisation des technologies clés, qui sont nécessaires à la fabrication et à l'utilisation des équipements, ainsi que les risques liés à la fourniture d'équipements, de pièces de rechange ou de services de support de troisième niveau, sont également évalués et pris en compte;
7. les composants utilisés ne présentent pas de vulnérabilités critiques connues non résolues ou exploitées activement;
8. lorsque cela est techniquement réalisable et économiquement viable, il convient d'éviter le recours à un fabricant ou à un fournisseur unique, afin de réduire la dépendance et d'accroître la résilience en cas de vulnérabilités de composants

critiques, de défaillance catastrophique du réseau ou d'une menace pour la sécurité des réseaux et des services d'entités essentielles par des entités physiques ou juridiques tierces de droit public ou privé.

(2) Lorsqu'ils fournissent des équipements, des systèmes et des services d'information et de communication, les opérateurs doivent respecter dans leur intégralité les lignes directrices de l'Agence de l'Union européenne pour la cybersécurité (ci-après dénommée «ENISA») et les règlements en vigueur de l'Union européenne concernant les exigences fondamentales en matière de sécurité lors de l'acquisition de produits et de services TIC sécurisés. L'agence publie sur son site internet des liens à jour vers les documents de l'ENISA et les règlements de l'UE pertinents.

(3) Lors de la fourniture de composants d'éléments critiques du réseau ou de l'utilisation de services en nuage, la priorité est donnée au choix de composants parmi les fabricants, fournisseurs ou prestataires de services cloud qui ont été certifiés par des organismes d'évaluation de la conformité accrédités et, si nécessaire, autorisés sur la base de l'article 60, paragraphe 3, du règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) nº 526/2013 (ci-après dénommé le «règlement») pour la délivrance de certificats européens de cybersécurité à un certain niveau d'assurance, conformément à l'article 52 du règlement.

(4) Aux fins du paragraphe précédent, l'opérateur doit se référer à un site internet dédié, établi par l'ENISA conformément à l'article 55 du règlement, qui fournit des informations sur les schémas européens de certification de cybersécurité, les certificats de cybersécurité européens et les déclarations de conformité de l'Union européenne, y compris des informations relatives aux schémas européens de certification de cybersécurité qui ne sont plus valables, aux certificats de cybersécurité européens qui ont été retirés ou ont expiré et aux déclarations de conformité de l'Union européenne, ainsi qu'au répertoire de liens vers des informations relatives à la cybersécurité.

Article 4
(Évaluation des risques)

(1) L'opérateur doit tenir compte et évaluer les aspects ci-dessous afin de déterminer les risques affectés au fabricant ou au fournisseur de composants et au prestataire de services de troisième niveau pour les éléments critiques du réseau.

(2) Aux fins de l'évaluation visée au paragraphe précédent, l'opérateur doit évaluer et tenir compte au moins des critères suivants:

1. la qualité globale (y compris les aspects de sécurité) et la fiabilité;
2. le niveau d'utilisation des normes et des interfaces ouvertes qui empêchent la dépendance et le verrouillage des produits d'un fabricant ou d'un fournisseur particulier;
3. la conformité aux normes techniques internationales et européennes reconnues (3GPP, ETSI), à la réglementation de l'Union européenne et aux paramètres de sécurité par défaut conformément aux recommandations professionnelles (association GSMA);

4. le niveau de compatibilité avec les équipements tiers et les fonctions réseau;
5. la capacité à fournir des mises à niveau et des personnalisations;
6. le processus de gestion et de divulgation des vulnérabilités, avec mises à jour et correctifs;
7. la disponibilité et la transparence de la documentation concernant:
   - les fonctions clés et les informations sur la sécurité et les autres caractéristiques du composant, avec les paramètres possibles, et
   - les logiciels utilisés, y compris le code open source (nomenclature logicielle — SBOM);
8. le degré de dépendance vis-à-vis des services de support de troisième niveau pour la gestion et l'entretien des équipements, si l'opérateur ne réalise pas lesdits services seul avec ses employés;
9. une évaluation préliminaire de la conformité des équipements ou d'une entité qui fournirait un service de support de troisième niveau par des organismes accrédités dans l'Union européenne conformément aux systèmes européens de certification de cybersécurité, les organismes accrédités étant publiés au Journal officiel de l'Union européenne.

(3) L'opérateur doit documenter et mettre régulièrement à jour les facteurs de risque et les résultats de l'évaluation des risques pour chaque fabricant, fournisseur ou prestataire de services de troisième niveau sélectionné visé aux paragraphes 2 et 3 du présent article.

Article 5
(Lignes directrices générales sur le fonctionnement des éléments critiques du réseau)

(1) Les composants des éléments critiques du réseau, leur fonctionnement et leurs paramètres par défaut ne doivent pas contenir de caractéristiques techniques susceptibles d'affecter négativement la sécurité ou le fonctionnement d'entités essentielles, notamment en raison d'activités de sabotage, d'espionnage, de vol de propriété intellectuelle ou de terrorisme.

(2) Les éléments critiques du réseau sont généralement réalisés en République de Slovénie ou, sous réserve qu'une évaluation de tous les risques de sécurité garantisse un niveau de sécurité élevé, et si cela n'est pas spécifié autrement par la réglementation applicable, dans l'Union européenne. L'opérateur doit informer l'agence des réseaux et services de communication de la République de Slovénie (ci-après dénommée l'«agence») et l'organe chargé de la sécurité de l'information de toute relocalisation en dehors de l'Union européenne au moins 30 jours avant ladite relocalisation.

(3) Les services de support de troisième niveau pour les éléments critiques du réseau sont généralement réalisés en République de Slovénie ou, sous réserve qu'une évaluation de tous les risques de sécurité garantisse un niveau de sécurité élevé, et si cela n'est pas spécifié autrement par la réglementation applicable, dans l'Union européenne. L'opérateur doit notifier à l'agence et à l'organe chargé de la sécurité de l'information toute relocalisation de ses services de support de troisième niveau en dehors des pays de l'Union européenne au moins 30 jours avant ladite relocalisation.

(4) La mise en œuvre de services de support de troisième niveau ne doit pas compromettre la sécurité ou le fonctionnement des services d'entités essentielles ni la sécurité nationale.

(5) L'opérateur doit établir et mettre régulièrement en œuvre le processus d'identification des éléments critiques du réseau. Cette procédure doit être effectuée au moins une fois par an, ou lors de l'acquisition de composants d'éléments critiques du réseau.

(6) Si un composant individuel ne représente que partiellement un élément critique du réseau, il est considéré comme faisant partie d'un élément critique du réseau.

(7) L'opérateur doit tenir à jour une liste de tous les composants des éléments critiques du réseau, ainsi que de leurs fonctionnalités, emplacements, et des administrateurs, gestionnaires, prestataires de services de support de troisième niveau, fabricants et fournisseurs associés. Sur demande, la liste est mise à la disposition de l'agence et d'un organe chargé de la sécurité de l'information.

Article 6
(Mesures de sécurité pour la fourniture de composants d'éléments critiques du réseau)

(1) L'opérateur doit connaître l'ensemble de la chaîne d'approvisionnement et des risques qui y sont associés, y compris les sous-traitants de composants individuels d'éléments critiques du réseau, qui comprennent également les clés de chiffrement, UICC/eUICC et d'autres éléments de sécurité, dont l'utilisation abusive pourrait compromettre la sécurité des entités essentielles.

(2) L'opérateur doit veiller à ce que les exigences de sécurité entre l'opérateur et les fabricants ou fournisseurs de composants d'éléments critiques du réseau ou ses prestataires de services de support de troisième niveau soient convenues contractuellement et documentées et exigent des fabricants ou des fournisseurs qu'ils respectent les mesures de sécurité convenues tout au long de la chaîne d'approvisionnement.

(3) Afin de prévenir en temps utile l'exploitation des vulnérabilités par des acteurs malveillants, l'opérateur doit veiller à ce que le fabricant ou le fournisseur de composants d'un élément critique du réseau s'engage contractuellement à informer immédiatement l'opérateur de toute vulnérabilité détectée, ainsi qu'à indiquer des mesures d'atténuation des risques, de protection ou de réparation que l'opérateur peut adopter en réponse à ladite menace.

(4) L'opérateur doit vérifier au moins une fois par an l'adéquation des droits d'accès aux éléments critiques du réseau, et les mettre à jour sans délai en cas de changement intervenu dans l'organisation ou du côté des prestataires de services de support de troisième niveau.

(5) L'opérateur doit prévenir toute dépendance vis-à-vis d'un fournisseur individuel ou d'un prestataire de services de troisième niveau («effet de verrouillage»), lorsque cela est techniquement faisable et économiquement viable, dans le but de réduire la dépendance et

d’accroître la résilience en cas de vulnérabilités de composants critiques. Il doit également à cette fin éviter les contrats à long terme avec des fabricants ou fournisseurs ou prestataires de services de support de troisième niveau, sauf s'il a la possibilité de les modifier dans le but de réduire au maximum les risques de perturbations de la fourniture de services aux entités essentielles.

Article 7
(Conditions contractuelles avec les fabricants, les fournisseurs ou les prestataires de services de support de troisième niveau)

Afin d’assurer un niveau élevé de sécurité, l’opérateur doit inclure au moins, dans de nouvelles conditions contractuelles, les éléments suivants avec les fabricants, les fournisseurs ou les prestataires de services de support de troisième niveau:

1. une déclaration du fabricant ou du fournisseur selon laquelle le composant ou ses paramètres par défaut n’ont pas de vices cachés non documentés ni n’ont aucune incidence négative sur le fonctionnement des entités essentielles;
2. l’engagement du fabricant, du fournisseur ou du prestataire de services de troisième niveau à protéger les données dont ils ont connaissance lors de la fourniture de services ou de l’accès à ceux-ci dans le cadre de la prestation du service d’accès;
3. l’engagement du fabricant, du fournisseur ou du prestataire de services de troisième niveau à informer immédiatement l’opérateur en cas de violation de la protection des données de communication ou des données relatives au trafic qui affectent ou sont susceptibles d’affecter l’opérateur ou les entités essentielles visées à l’article 1er, point 1, de la présente loi générale;
4. l’engagement du fabricant, du fournisseur ou du prestataire de services de troisième niveau à informer immédiatement l’opérateur de tout incident de sécurité et de toute vulnérabilité susceptible d’affecter la sécurité du réseau, des services associés ou des données de l’opérateur;
5. l’engagement du fabricant, du fournisseur ou du prestataire de services de troisième niveau à se conformer aux normes et aux règles de sécurité fixées par l’opérateur et à prendre les mesures de sécurité appropriées pour assurer la sécurité des systèmes et des réseaux d’information, ainsi que des données de l’opérateur ou de l’entité essentielle;
6. la capacité de l’opérateur à examiner continuellement les environnements, les procédures, les mesures de sécurité et les outils utilisés par le prestataire de services de support de troisième niveau lors de l’accès au réseau et aux données de l’opérateur;
7. la responsabilité du fabricant, du fournisseur, ou du prestataire de services de support de troisième niveau en cas de dommages qui seraient causés par des vulnérabilités identifiées ou par une utilisation abusive de composants d’éléments critiques du réseau, en raison d'un réglage par défaut défectueux, ou que le fabricant, le fournisseur ou le prestataire de services de support de troisième niveau a mis en œuvre intentionnellement ou par négligence lors de la prestation de services de support de troisième niveau;
8. l’obligation de former régulièrement le personnel du fabricant, du fournisseur ou du prestataire de services de support de troisième niveau dans le domaine de la sécurité des données et des systèmes et réseaux d’information.

Article 8
(Règles relatives à l'accès et à l'utilisation des éléments critiques du réseau)

(1) Lorsqu'il accède physiquement ou logiquement aux composants des éléments critiques du réseau, à leurs paramètres et aux données de l'opérateur qui y sont stockées, traitées ou modifiées, l'opérateur doit veiller à ce que:

1. l'accès soit strictement limité aux personnes qui y ont été préalablement autorisées;
2. tous les travaux sur des éléments critiques du réseau réalisés sur site ou via un accès à distance soient contrôlés par l'opérateur;
3. l'authentification multifacteur soit effectuée pour les utilisateurs auxquels les droits les plus élevés sont attribués pour accéder à des composants individuels d'éléments critiques du réseau, à leurs paramètres ou aux données qui y sont stockées ou traitées;
4. chaque personne autorisée à qui l'accès est accordé dispose d'un compte utilisateur unique et d'un mot de passe unique;
5. tous les mots de passe soient modifiés régulièrement ou immédiatement en cas de mauvaise utilisation détectée, contiennent au moins 15 caractères et comprennent des lettres majuscules et minuscules, des chiffres et des caractères spéciaux, si le logiciel le permet;
6. dans la mesure du possible, l'accès soit soumis au concept de confiance ou de tolérance zéro;
7. la sécurité de la connexion de communication de l'utilisateur autorisé aux composants individuels soit protégée par l'utilisation du cryptage, en tenant compte des derniers développements technologiques et des bonnes pratiques industrielles dans le domaine de la sécurité de l'information, ou recommandées par des institutions établies dans le domaine de la sécurité de l'information;
8. un enregistrement indélébile des accès et des tentatives d'accès soit effectué, puis conservé, ainsi qu'une copie de sauvegarde, pendant au moins six mois, voire pendant une période plus longue lorsque cela est préconisé par l'analyse de la gestion des risques et par l'évaluation du niveau acceptable de risques;
9. l'enregistrement et le suivi de toutes les interventions logicielles sur les composants, y compris des changements de configuration, soient effectués dans la mesure du possible. Les enregistrements, y compris une copie de sauvegarde de ces données, soient conservés pendant la période indiquée au point précédent;
10. l'accès aux composants individuels et aux données qui y sont stockées ou traitées soit limité dans le temps et ouvert uniquement pour la durée nécessaire des travaux.

(2) Dans le cas de l'accès à des composants individuels d'éléments critiques du réseau par le personnel ou les employés d'un prestataire de services de support de troisième niveau, ces derniers doivent:

1. utiliser exclusivement un poste de travail intermédiaire dédié sécurisé («serveur jump»), qui fait l'objet de contrôles de sécurité réguliers;
2. installer sur ce poste de travail dédié uniquement les outils, composants et services actifs absolument nécessaires pour accéder à d'autres ressources du réseau, mis à jour avec les derniers correctifs de sécurité;
3. utiliser des opérations cryptographiques sécurisées et des clés sur un poste de travail dédié, situé dans le réseau de l'opérateur et sous son contrôle exclusif;
4. chaque accès est approuvé et activé manuellement par l'opérateur, uniquement pour la durée de l'accès;

5. tous les accès et toutes les activités sont contrôlés et enregistrés physiquement par l'opérateur;
6. utiliser une authentification à deux facteurs et des mots de passe d'au moins 15 caractères et comportant des lettres majuscules et minuscules, des chiffres et des caractères spéciaux, qui doivent être modifiés en fonction des risques évalués.

(3) Avant que l'opérateur ne transfère le service de gestion, de maintenance ou de mise à jour d'éléments critiques du réseau ou de leurs composants individuels à un tiers, il doit vérifier et s'assurer qu'il dispose au moins de mécanismes de sécurité et de processus de gestion de la sécurité identiques ou améliorés par rapport à ses mécanismes et processus. Il doit informer immédiatement l'entité essentielle concernée, l'agence et l'organe chargé de la sécurité de l'information de toute intention de transfert.

(4) L'opérateur doit vérifier l'état réel des processus de sécurité avant le début de la prestation de service, puis au moins une fois par an. L'opérateur doit tenir des registres des examens et contrôles internes relatifs à la fourniture de services de support par des tiers, et conserver ces registres pendant toute la durée de la prestation des services et pendant un an après leur réalisation, dans la limite de cinq ans.

DISPOSITIONS TRANSITOIRES ET FINALE

Article 9
(Dispositions transitoires)

(1) L'opérateur doit notifier les emplacements existants des éléments critiques du réseau à l'agence et à l'organe chargé de la sécurité de l'information dans un délai de trente jours à compter de l'entrée en vigueur de la présente loi générale.

(2) L'opérateur doit notifier les emplacements existants des services de support de troisième niveau pour les éléments critiques du réseau à l'agence et à l'organe chargé de la sécurité de l'information dans un délai de 30 jours à compter de l'entrée en vigueur de la présente loi générale.

(3) L'agence doit publier pour la première fois les documents visés à l'article 3, paragraphe 2, de la présente loi générale, à compter de la date de son entrée en vigueur.

Article 10
(Entrée en vigueur)

La présente loi générale entrera en vigueur le trentième jour suivant sa publication au Journal officiel de la République de Slovénie. Les opérateurs peuvent utiliser l'équipement et maintenir la fourniture de services de support de troisième niveau jusqu'à l'expiration des délais prévus à l'article 312, paragraphes 2 et 3, de la loi.

nº _____ mag. Marko Mišmaš

Ljubljana, le _____ directeur

EVA 2023-3150-0034

PROJET

Annexe

Liste des éléments critiques du réseau et des systèmes d'information associés:

Éléments critiques du réseau	**Fonctionnalités du réseau et des systèmes d'information**
Gestion des abonnés et mécanismes de cryptage	- gestion des sessions (voix et données), - authentification des utilisateurs et des équipements avec le réseau, - gestion et stockage des clés d'autorisation des abonnés et des composants du réseau (UICC/eUICC, certificats numériques/HSM), - fonctions d'authentification sécurisée, de protection de l'intégrité de la communication (cryptage) et de stockage des clés d'utilisateur, des composants réseau et de gestion, - gestion des droits d'accès.
Interconnexion	- fonctions d'hébergement et interfaces vers d'autres réseaux et services.
Services de réseau gérés	- enregistrement et autorisation des services de réseau, - stockage et traitement des données de communication, de localisation et de trafic, - exposition du réseau et des fonctionnalités du réseau à des applications et à des services externes.
Gestion et orchestration des fonctions réseau virtualisées (NFV) et de l'orchestration de réseau (MANO), y compris de l'infrastructure de virtualisation	- fonctions de gestion de l'orchestration et de la configuration des NFV quel que soit le type de mise en œuvre (VM, conteneur, microservices), - fonctions de virtualisation pour la mise en œuvre et l'utilisation des NFV, - fonction de sélection des tranches de réseau (NSSF)
Réseau d'accès radio	- stations de base qui prennent en charge la technologie 5G ou plus.
Systèmes de gestion et autres systèmes de support	- suivi de l'exploitation et de la gestion du réseau de communication mobile, y compris la partie «accès» (RAN/O-RAN), - systèmes de détection d'événements de sécurité, d'anomalies, de menaces et prenant en charge leur gestion (fonctions de sécurité, y compris SIEM/SOAR).
Interception légale	- fonctions d'accès au contenu de la communication et aux données relatives au trafic des utilisateurs par l'autorité compétente.