INSTITUT BELGE DES SERVICES POSTAUX
ET DES TÉLÉCOMMUNICATIONS

DÉCISION DU CONSEIL DE L'IBPT DU 01/04/2014 FIXANT LES HYPOTHÈSES DANS LESQUELLES LES OPÉRATEURS DOIVENT NOTIFIER À L'IBPT UN INCIDENT DE SÉCURITÉ ET LES MODALITÉS DE CETTE NOTIFICATION

TABLE DES MATIÈRES

1. OBJET ET BASES JURIDIQUES

1 La loi du 10 juillet 2012 portant des dispositions diverses en matière de communications électroniques[1] a introduit entre autres un article 114/1, § 2, dans la loi du 13 juin 2005 relative aux communications électroniques (ci-après la LCE). Cet article se lit comme suit (c'est nous qui soulignons):

> «*Les entreprises fournissant des réseaux publics de communications ou des services de communications électroniques accessibles au public notifient sans délai à l'Institut toute atteinte à la sécurité ou perte d'intégrité ayant eu un impact significatif sur le fonctionnement des réseaux ou des services. Après autorisation préalable du ministre, l'Institut précise dans quelles hypothèses l'atteinte à la sécurité ou perte d'intégrité a un impact significatif au sens du présent alinéa*. »

2 La présente décision exécute entre autres la dernière phrase de la disposition précitée.

3 Par ailleurs, l'article 114/2 de la LCE, tel qu'inséré dans la LCE par la loi du 10 juillet 2012 susmentionnée, prévoit ce qui suit :

> « *§ 1er. L'Institut a le pouvoir de donner des instructions contraignantes, y compris concernant les dates limites de mise en œuvre, aux entreprises fournissant des réseaux publics de communications électroniques ou des services de communications électroniques accessibles au public, en vue de l'application des articles 114 et 114/1.* »

4 Sur base de l'article 114/2 et de l'article 114/1, § 2, première phrase, précité, l'IBPT fixe par la présente décision des instructions contraignantes quant à l'obligation pour les opérateurs de notifier sans délai à l'IBPT toute atteinte à la sécurité ou perte d'intégrité ayant eu un impact significatif sur le fonctionnement des réseaux ou des services.

5 La présente décision fixe dès lors les modalités pratiques de la notification par les opérateurs à l'IBPT d'incidents de sécurité et détermine ainsi les points suivants :

- le délai dans lequel la notification doit être faite ;
- le mode de transmission de la notification ;
- le contenu de la notification.

6 La présente décision ne concerne pas l'obligation des entreprises fournissant un service de communications électroniques accessible au public d'informer les abonnés et l'IBPT d'un risque de violation de la sécurité du réseau comme indiqué dans l'article 114/1, § 1, de la LCE :

> « *Lorsqu'il existe un risque particulier de violation de la sécurité du réseau, les entreprises fournissant un service de communications électroniques accessible au public informent les abonnés et l'Institut de ce risque et, si les mesures que peuvent prendre les entreprises fournissant le service ne permettent pas de l'écarter, de tout moyen éventuel d'y remédier, y compris en en indiquant le coût probable.* » (c'est nous qui soulignons)

7 La notification à l'IBPT d'une atteinte à la sécurité d'un service de communications électroniques accessible au public en matière de données à caractère personnel qui doit être faite en vertu de l'article 114/1, §3, de la LCE n'est pas traitée dans la présente décision et fera l'objet, si nécessaire, de directives distinctes de l'IBPT[2].

[1] Moniteur belge du 25 juillet 2012, p. 40969.

[2] La présente décision ne traite pas non plus des indemnités que les opérateurs devraient verser aux abonnés en cas d'interruption du service conformément à l'arrêté royal qui pourrait être pris sur base de l'article 113/2 de la LCE.

2. PROCÉDURE

2.1. Consultation publique

8 Du 7 mai 2013 au 7 juin 2013, l'IBPT a organisé une consultation publique concernant le projet de la présente décision, sur base de l'article 14, § 2, 1°, 1ière phrase, de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges (ci-après la loi-statut).

9 Ont répondu à cette consultation les opérateurs suivants : Belgacom, Mobistar, Plateform, Telenet et Verizon.

10 La synthèse des résultats de la consultation publique se trouve en annexe 2 à la présente décision.

2.2. Consultation des régulateurs des médias

11 En vertu de l'article 3 de l'accord de coopération du 17 novembre 2006[3], le 3 septembre 2013, l'IBPT a transmis le projet de la présente décision aux régulateurs média des communautés, à savoir le CSA, le Medienrat et le VRM. Le Medienrat et le VRM ont réagi en répondant qu'ils n'avaient pas de commentaires. Le CSA n'a pas réagi.

2.3. Autorisation du ministre

12 Par courrier du 21 mars 2014, M. Johan Vande Lanotte, Vice-Premier Ministre et Ministre de l'Economie, des Consommateurs et de la Mer du Nord, a donné l'autorisation préalable visée à l'article 114/1, §2, de la LCE pour ce qui concerne les aspects de la présente décision qui traitent des hypothèses dans lesquelles l'atteinte à la sécurité ou perte d'intégrité a un impact significatif sur le fonctionnement des réseaux ou des services, soit concernant la section 4 de la présente décision.

3. CONTEXTE EUROPÉEN

13 La directive 2009/140/CE[4] a introduit entre autres les articles 13*bis* et 13*ter* dans le chapitre III*bis* « Sécurité et intégrité des réseaux et services » de la directive « cadre » de 2002[5]. Les articles 114/1, § 2, et 114/2 de la LCE susmentionnés ont été adoptés dans le cadre de la transposition en droit belge de ces nouveaux articles 13*bis* et 13*ter*.

14 L'ENISA (European Network and Information Security Agency) a publié sur son site Internet[6] un document intitulé « *Technical Guidelines on Incident Reporting. Technical guidance on the incident reporting in Article 13a . Version 2.0, January 2013* » (ci-après « les lignes directrices de l'ENISA »). Ce document adresse une série de recommandations aux autorités réglementaires nationales (ci-après « ARN ») en ce qui concerne la mise en œuvre de l'article 13*bis* de la directive « cadre » et en particulier en

[3] Accord de coopération du 17 novembre 2006 entre l'Etat fédéral, la Communauté flamande, la Communauté française et la Communauté germanophone relatif à la consultation mutuelle lors de l'élaboration d'une législation en matière de réseaux de communications électroniques, lors de l'échange d'informations et lors de l'exercice des compétences en matière de réseaux de communications électroniques par les autorités de régulation en charge des télécommunications ou de la radiodiffusion et la télévision. Moniteur belge du 28.12.2006, p. 75371.

[4] Directive 2009/140/CE du Parlement européen et du Conseil du 25 novembre 2009 modifiant les directives 2002/21/CE relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques, 2002/19/CE relative à l'accès aux réseaux de communications électroniques et aux ressources associées, ainsi qu'à leur interconnexion, et 2002/20/CE relative à l'autorisation des réseaux et services de communications électroniques.

[5] Directive 2002/21/CE du Parlement européen et du Conseil du 7 mars 2002 relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques (directive "cadre").

[6] Voir https://resilience.enisa.europa.eu/article-13/guideline-for-incident-reporting

ce qui concerne l'obligation contenue dans cet article 13*bis* pour les ARN de fournir une fois par an à la Commission européenne et à l'ENISA un rapport succinct sur les notifications d'incidents de sécurité reçues des opérateurs et sur l'action envisagée par ces ARN[7].

15 La présente décision s'inspire[8] des lignes directrices de l'ENISA en vue d'assurer une certaine cohérence entre les notifications des opérateurs vers l'IBPT et le rapport annuel sur les incidents de sécurité que l'IBPT envoie l'ENISA et à la Commission européenne.

4. HYPOTHÈSES DANS LESQUELLES LES OPÉRATEURS DOIVENT NOTIFIER À L'IBPT UN INCIDENT DE SÉCURITÉ

4.1 Introduction

16 Selon l'article 114/1, §2, de la LCE, « *les entreprises fournissant des réseaux publics de communications ou des services de communications électroniques accessibles au public notifient sans délai à l'Institut toute atteinte à la sécurité ou perte d'intégrité ayant eu un impact significatif sur le fonctionnement des réseaux ou des services.* »

17 Les différents éléments de cette disposition sont analysés ci-dessous.

4.2 Opérateurs soumis à la notification

18 Il ressort de cette disposition qu'elle s'applique tant aux entreprises fournissant des réseaux publics de communications qu'aux entreprises fournissant des services de communications électroniques accessibles au public.

19 Si plusieurs opérateurs sont concernés par un même incident, chacun de ces opérateurs fera une notification à l'IBPT, pour autant que les seuils indiqués au point 28 et aux points suivants soient atteints.

4.3 Incident de sécurité

20 Comme indiqué dans les lignes directrices de l'ENISA, faisant par ailleurs référence à la littérature technique sur les réseaux et les réseaux interconnectés, il faut entendre, pour l'application de la présente décision, par « *intégrité* » « *la capacité du système de conserver ses caractéristiques spécifiques en termes de performances et de fonctionnalité* »[9].

21 Par « *incident de sécurité* » ou par « *incident* », il faut entendre, pour l'application de cette décision, toute atteinte à la sécurité ou à la perte d'intégrité qui a un impact sur le bon fonctionnement d'un réseau public de communications électroniques (ci-après « réseau ») ou sur la fourniture d'un service de communications électroniques accessible au public (ci-après « service »)[10].

22 Par « *atteinte à la sécurité* », il faut entendre toute atteinte physique ou logicielle (software - virus – via internet – via le réseau – coupure de câble – dérangement sur câble – inondation – court-circuit, etc), à un réseau ou à l'exploitation d'un service, impactant la sécurité physique ou logicielle de fonctionnement, ou le fonctionnement même, de ce réseau ou service. Il s'agit donc d'une notion très large.

23 *Par* « *perte d'intégrité* », il faut entendre la perte de la capacité du système de conserver ses caractéristiques spécifiques en termes de performances et de fonctionnalité.

---

[7] Voir l'article 13*bis.3,* alinéa 3, de la directive "cadre".
[8] Ceci en particulier pour ce qui concerne le contenu des notifications.
[9] Traduction libre de « *the ability of the system to retain its specified attributes in terms of performance and functionality* ». Voir lignes directrices de l'ENISA, p. 5.
[10] Cette définition est inspirée des lignes directrices de l'ENISA, p. 5.

4.4 Incident et risque d'incident

24 Le fait de simplement soupçonner qu'un incident s'est produit ne génère pas l'obligation de notifier à l'IBPT cet incident en vertu de l'article 114/1, § 2, alinéa 1er, de la LCE [11]. Le constat d'un incident est considéré comme établi, et l'incident doit être notifié à l'IBPT, dès que l'opérateur dispose d'assez d'éléments indiquant qu'il s'est produit un incident de sécurité.

4.5 Réseaux et services concernés

25 Le terme « *réseaux de communications électroniques* » est défini à l'article 2, 3°, de la LCE. Le terme « *service de communications électroniques* » est quant à lui défini à l'article 2, 5°, de la LCE.

26 La liste des réseaux et des services à considérer est la suivante[12]:

- Réseaux : fixe, mobile
- Service de téléphonie (voix)
- Service de lignes louées
- Services de transmission de données : Service d'accès à Internet, SMS
- Services d'accès partagé ou dégroupé à la boucle locale et services de gros d'accès à la large bande.

Cette liste n'est pas exhaustive.

4.6 Seuils d'impact

4.6.1 Principes

27 Un incident doit être notifié à l'IBPT si un des seuils suivants est atteint (critères non cumulatifs). Ces critères s'inspirent de ceux de l'ENISA, en tenant compte du nombre d'utilisateurs finaux en Belgique.

28 L'incident affecte un nombre supérieur à 700 000 (téléphonie voix fixe), 1 900 000 (téléphonie voix mobile et SMS), 540 000 (accès internet fixe), 310 000 (accès internet mobile) ou 2000 (lignes louées) utilisateurs finals pendant une heure ou plus (« seuil 1 »).

29 L'incident affecte un nombre supérieur à 460 000 (téléphonie voix fixe), 1 250 000 (téléphonie voix mobile et SMS), 350 000 (accès internet fixe), 210 000 (accès internet mobile) ou 1330 (lignes louées) utilisateurs finals pendant 2 heures ou plus (« seuil 2 »).

30 L'incident affecte un nombre supérieur à 230 000 (téléphonie voix fixe), 625 000 (téléphonie voix mobile et SMS), 175 000 (accès internet fixe), 105 000 (accès internet mobile) ou 670 (lignes louées) utilisateurs finals pendant 4 heures ou plus (« seuil 3 »).

31 L'incident affecte un nombre supérieur à 95 000 (téléphonie voix fixe), 250 000 (téléphonie voix mobile et SMS), 70 000 (accès internet fixe), 41 000 (accès internet mobile) ou 270 (lignes louées) utilisateurs finals pendant 6 heures ou plus (« seuil 4 »).

32 L'incident affecte un nombre supérieur à 48 000 (téléphonie voix fixe), 125 000 (téléphonie voix mobile et SMS), 35 000 (accès internet fixe), 21000 (accès internet mobile) ou 130 (lignes louées) utilisateurs finals pendant 8 heures ou plus (« seuil 5 »).

33 L'incident affecte un nombre supérieur ou égal à 160 stations de base, fixes ou temporaires, indépendamment du nombre d'utilisateurs finals affectés ou de la durée de cet incident (« seuil 6 »).

---

[11] On rappellera cependant que l'article 114/1, § 1er, de la LCE impose d'informer les abonnés et l'IBPT en cas de risque particulier de violation de la sécurité du réseau (voir ci-dessus).

[12] Voir page 9 des lignes directrices de l'ENISA.

4.6.2 Explications

34 Chaque opérateur est tenu d'examiner l'impact de l'incident sur ses utilisateurs finals et non sur les utilisateurs finals d'autres opérateurs. Les seuils 1 à 5 se calculent donc par opérateur et non en tenant compte des utilisateurs finals de différents opérateurs qui seraient affectés par l'incident[13].

35 Un utilisateur final est affecté par un incident lorsque l'incident a un effet tel que la disponibilité ou la continuité du réseau ou service ne peut plus être assurée.

36 Chaque ligne, numéro d'appel ou carte SIM affecté par un incident correspond à un utilisateur final.

37 Sont considérés comme étant affectés par un incident non seulement les utilisateurs finals qui ont utilisé le service concerné par l'incident et qui ont été dans les faits affectés par l'incident mais également les utilisateurs finals qui auraient été affectés par l'incident s'ils avaient décidé d'utiliser le service concerné.

38 Pour les seuils 1 à 5, il se peut que l'incident dépasse à plusieurs reprises les chiffres (par exemple les 700 000 téléphonie voie fixe) indiqués dans ces seuils, à chaque fois pendant une durée inférieure à la durée (1, 2, 4, 6 et 8 heures) reprise dans ces seuils. Dans ce cas, il faut aditionner les différentes durées pendant lesquelles ces chiffres ont été dépassés pour déterminer si le seuil est atteint. A titre d'illustration, pour ce qui concerne le seuil 1, si le chiffre de 700 000 (téléphonie voix fixe)a été dépassé quatre fois pendant un quart d'heure, l'incident doit être notifié à l'IBPT.

39 Pour le calcul du seuil 6, il y a lieu de déterminer quelles ont été les stations de base affectées par l'incident pendant toute sa durée.

40 Tout incident ne répondant pas aux critères susmentionnés peut être notifié à l'IBPT sur l'initiative de l'opérateur si ce dernier considère que l'impact de l'incident est tel qu'il doit être porté à la connaissance de l'IBPT.

5. DÉLAI DANS LEQUEL LA NOTIFICATION DOIT ÊTRE FAITE

41 L'article 114/1, § 2, de la LCE prévoit que «*Les entreprises fournissant des réseaux publics de communications ou des services de communications électroniques accessibles au public notifient sans délai à l'Institut toute atteinte à la sécurité ou perte d'intégrité ayant eu un impact significatif sur le fonctionnement des réseaux ou des services.* » (c'est nous qui soulignons)

42 Pour déterminer quand un incident de sécurité doit être notifié à l'IBPT, les opérateurs respecteront les principes suivants :

1) La notification doit être adressée à l'IBPT selon le mode de transmission prévu ci-dessous dès que l'opérateur dispose de toutes les informations visées à la section 7 et en tout cas dans les 72h00 à partir du moment où un des seuils a été atteint.. Pour le calcul du délai de 72h00, seuls les jours ouvrables sont pris en considération.

2) Si la notification envoyée à l'IBPT n'est pas complète ou contient des éléments ayant changé, un complément de notification doit être adressé à l'IBPT dans les 15 jours.

6. MODE DE TRANSMISSION DE LA NOTIFICATION

43 Pour la transmission des notifications à l'IBPT, les opérateurs ont le choix entre les modes suivants :
- courrier par porteur ;
- courrier recommandé postal ;
- fax ;
- plate-forme électronique mise à disposition de l'IBPT et renseignée par ce dernier.

44 Dans leur choix entre ces différents modes, les opérateurs tiendront compte de l'urgence éventuelle.

[13] Un même incident peut affecter des réseaux ou services de différents opérateurs.

45 Dans le cas d'une notification par courrier recommandé postal et par porteur, l'adresse utilisée sera :

IBPT
A l'attention du Président du Conseil
Notification « security incident report »
Ellipse Building - Bâtiment C
Boulevard du Roi Albert II 35
1030 Bruxelles

7. CONTENU DE LA NOTIFICATION

46 Les informations à communiquer dans le cadre de la notification sont détaillées en annexe 1.

8. ENTRÉE EN VIGUEUR

47 La présente décision entre en vigueur trois mois après sa publication sur le site internet de l'IBPT.

9. VOIES DE RECOURS

48 Conformément à l'article 2, §1 de la loi du 17 janvier 2003 concernant les recours et le traitement des litiges à l'occasion de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et télécommunications belges, vous avez la possibilité d'introduire un recours contre cette décision devant la Cour d'appel de Bruxelles, Place Poelaert 1, B-1000 Bruxelles. Les recours sont formés, à peine de nullité prononcée d'office, par requête signée et déposée au greffe de la Cour d'appel de Bruxelles dans un délai de soixante jours à partir de la notification de la décision ou à défaut de notification, après la publication de la décision ou à défaut de publication, après la prise de connaissance de la décision.

49 La requête contient, à peine de nullité, les mentions requises par l'article 2, §2 de la loi du 17 janvier 2003 concernant les recours et le traitement des litiges à l'occasion de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et télécommunications belges. Si la requête contient des éléments que vous considérez comme confidentiels, vous devez l'indiquer de manière explicite et déposer, à peine de nullité, une version non-confidentielle de celle-ci. L'Institut publie sur son site Internet la requête notifiée par le Greffe de la juridiction. Toute partie intéressée peut intervenir à la cause dans les trente jours qui suivent cette publication.

Charles Cuvelliez
Membre du Conseil

Axel Desmedt
Membre du Conseil

Luc Vanfleteren
Membre du Conseil

Jack Hamande
Président du Conseil

ANNEXE 1 : FORMULAIRE DE NOTIFICATION

Information	Description
DATE ET HEURE	
Date de début	Date et heure à laquelle l'incident a (eu) lieu (en heure nationale). Ces indications temporelles peuvent être considérées comme le moment où l'incident a été découvert. L'heure doit être exprimée tant en zone horaire CET qu'en zone horaire locale.
IMPACT DE L'INCIDENT ET SOURCE DU PROBLEME	
Services touchés: - **Téléphonie fixe** - **Téléphonie mobile** - **Services de messages (courts)** - **Internet fixe** - **Internet mobile** - **Lignes louées**	Le ou les services qui sont touchés par l'incident.
Paramètres d'impact: - **Nombre de lignes, numéros d'appel ou cartes SIM affectés** - **Nombre de lignes, numéros d'appel ou cartes SIM qui sont fournis grâce au service ou réseau affecté par l'incident**	Nombre total de lignes, numéros d'appel ou cartes SIM affectés lorsque l'incident a lieu. Ce nombre doit être exprimé en valeur absolue (p. ex. « 250 000 d'utilisateurs finals » est accepté) et non pas de manière relative (p. ex. « 75% des cartes pre-paid» est refusé).
Durée	La durée de l'incident. Il s'agit de la durée pendant laquelle le seuil a été dépassé[14]. La durée totale de l'incident doit également être indiquée, lorsque cette donnée est disponible. La durée totale de l'incident est le laps de temps entre le début de l'incident et le moment où l'incident a été tout à fait résolu.
Impact sur les appels d'urgence	Si disponible, service d'urgence touché par l'incident.
Détails sur l'impact	[*Facultatif*] Détails sur l'impact de l'incident.
Source du problème[15]: - **Catastrophe ou phénomène naturel** - **Erreur humaine** - **Attaques ou actions malveillantes** - **Défaillance matérielle ou logicielle** - **Défaillance d'une tierce partie ou partie externe**	La cause à l'origine de l'incident
Détails sur la source du problème	[*Facultatif*] Les incidents à rapporter doivent se focaliser sur l'intégrité du réseau et la continuité du service. Il pourrait s'agir de sous-catégories des sources du problème, répertoriées dans la section pertinente.
AUTRES INFORMATIONS SUR L' INCIDENT	
Description générale	Résumé de l'incident
Gestion de l'incident et plans d'intervention[16]	Toutes les interventions effectuées après la découverte de l'incident et des mesures adoptées pour rétablir les conditions/le niveau d'origine du service.
Actions après l'incident	Description de toute disposition prise afin de minimizer le

[14] Voir lignes directrices de l'ENISA, p. 12.

[15] Lignes directrices de l'ENISA, pp.. 13 et 14. Indépendamment que cette cause ou origine soit une défaillance de sécurité ou une perte d'intégrité.

[16] Mesures d'intervention et de rétablissement prises par les fournisseurs tant pendant qu'après l'incident.

	niveau de risque..
Interconnexions nationales touchées	Si le service touché peut causer des dommages/changements à un bien (ou service) appartenant à un autre opérateur ou fournisseur, une interconnexion est touchée. (exemples : liens d'interconnection entre réseaux, lignes louées, etc.) Si applicable, détails sur les opérateurs belges concernés.
Interconnexions internationales touchées	En cas d'incidents transfrontaliers, il se peut qu'une brèche de sécurité dans un Etat membre touche les biens d'un autre Etat membre 'interconnecté'. Certaines concentrations d'infrastructure sont vulnérables et des perturbations significatives peuvent être causées par une faille locale; les systèmes interconnectés peuvent faire l'objet de failles techniques en cascade. Si applicable, détails sur les opérateurs concernés des autres Etats Membres.
Portée géographique /région touchée	Si disponible, la région (commune, ville, province, partie de territoire, etc.) touchée par l'incident.
Enseignements tirés	Décrire toutes les interventions effectuées après l'incident pour améliorer la sécurité du bien et les procédures (ou les mesures prises) qui seront suivies à partir de ce moment-là. La différence entre ce champ et le champ des "Actions après l'incident" est que dans ce champ, nous renvoyons aux actions à long terme.
Autres observations	Informations à compléter sur l'incident ou la notification de l'incident

ANNEXE 2 : RÉSULTATS DE LA CONSULTATION PUBLIQUE

1. Du 7 mai 2013 au 7 juin 2013, l'IBPT a organisé une consultation publique concernant le projet de la présente décision, sur base de l'article 14, § 2, 1°, 1ière phrase, de la loi statut.

2. Ont répondu à cette consultation les opérateurs suivants : Belgacom, Mobistar, Plateform, Telenet et Verizon.

3. La présente synthèse reprend uniquement les parties non confidentielles des réponses reçues.

4. Pour la bonne compréhension de la présente annexe, il est précisé qu'à la suite de la consultation publique, l'IBPT a décidé de ne pas reprendre le seuil 1 du projet de décision soumis à consultation et qui était le suivant : « L'incident affecte un service (par exemple, une ligne louée, un accès de gros à la large bande ou un accès dégroupé à la boucle locale) que rend un opérateur à un ou plusieurs utilisateurs, qui ne sont pas des utilisateurs finaux, pour autant qu'un des seuils (« seuils 2 à 6 ») ci-dessous soit atteint ».

5. Deux répondants attirent l'attention sur le fait que dans le texte en néerlandais, il est demandé au point 5 aux opérateurs de notifier à l'IBPT tout risque d'atteinte à la sécurité ou perte d'intégrité. Ce répondant émet des réserves sérieuses quant à l'évaluation effective et uniforme de cette notion de risque. Il faut remarquer qu'il s'agit d'une erreur de traduction dans la version néerlandaise et que cette notion de risque n'est pas présente dans le point 5 de la version française du texte.

6. Un répondant est d'accord avec les seuils d'impact 2 à 6 (actuellement seuils 1 à 5) mais émet des réserves quant au seuil d'impact n° 1 (actuellement supprimé). Ce répondant, ainsi qu'un autre, mentionne qu'un opérateur wholesale n'est pas au courant du nombre de clients impactés de son client.

7. A propos du seuil d'impact n° 7 (actuellement seuil 6), trois répondants mentionnent que le nombre choisi de stations de base est trop peu élevé et que le seuil d'impact n° 7 est moins élevé que les seuils 2 à 6 (actuellement seuils 1 à 5). Ces répondants proposent dès lors soit de supprimer ce seuil d'impact, soit d'augmenter le nombre de stations de base à 150 / 200. A ce propos, un autre répondant fait remarque qu'en tant que MVNO, il n'a pas d'information concernant ce seuil.

8. Un répondant fait remarquer que ces notifications ne visent pas les services d'e-mail ou de distribution de TV.

9. Un répondant est d'avis que l'obligation de transmettre l'information dans les 24 h 00 à partir du début de l'incident est trop rapide par rapport à l'usage effectif de cette information par l'IBPT, d'autant plus qu'il n'est pas prévu de distinction entre jours ouvrables, weekend et jours fériés. Ce répondant est d'avis qu'un délai d'une semaine voir un mois est suffisant, et demande avec insistance qu'un délai de minimum 72 heures ouvrées (business hours) soit d'application. Au cas où ce délai de 24 h serait maintenu, ce répondant demande que seul un minimum d'informations doive être transmis dans ce délai, le reste étant alors transmis endéans la semaine.

10. Trois répondants demandent de prévoir un délai de minimum trois mois de mise en application de la décision, en vue de pouvoir s'organiser en interne.

11. Deux répondants demandent de prévoir l'envoi de l'information via envoi à une boite e-mail sécurisée de l'IBPT. Un répondant est d'avis que l'usage du site tel que préconisé par l'IBPT est trop compliqué et trop lent. De plus, cela pose des problèmes d'accès par différentes personnes depuis différents endroits. Un autre répondant note de problème de flexibilité quant à l'usage du site de l'IBPT.

12. Un répondant mentionne une apparente contradiction entre le fait que chaque opérateur est responsable pour identifier les notifications à opérer et le seuil d'impact n° 1 (actuellement supprimé). Des clarifications sont demandées.

13. Un répondant mentionne comprendre que tous les opérateurs présents sur le marché sont concernés et demande à l'IBPT de bien contrôler ce point.

14. Un répondant mentionne que ni les lignes directrices de l'ENISA ni le projet de décision ne définit la notion d'atteinte à la sécurité et demande de la clarté quant à cette notion.

15. Un répondant constate que l'IBPT a ajouté le service des lignes louées et les services d'accès partagé ou dégroupé à la boucle locale et services de gros d'accès à la large bande, par rapport à ce que est prévu dans la liste de l'ENISA. Ce répondant se montre d'accord avec l'ajout du service des lignes louées mais se montre sceptique quant à l'ajout des services d'accès partagé ou dégroupé à la boucle locale et services de gros d'accès à la large bande. Si ces derniers devaient être repris dans la décision, ce répondant demande à ce que le service de revente d'accès broadband soit concerné aussi.

16. Un répondant émet des réserves quant au seuil d'impact n° 1 (actuellement supprimé). Ce répondant mentionne qu'un opérateur n'est pas au courant du nombre d'utilisateurs (finals) impactés de son client, et ce spécialement lorsqu'il s'agit d'une ligne louée. Ce répondant mentionne la complexité de ce seuil n° 1 et dénote une contradiction avec le point 4.2. du projet de décision. Ce répondant se demande aussi comment appliquer cette disposition dans le cas « mobile » et MVNO en particulier. Ce répondant demande le retrait de ce seuil n° 1 ou, à défaut, des explications plus détaillées et complètes de la part de l'IBPT.

17. En ce qui concerne les seuils d'impact 2 à 6 (actuellement seuils 1 à 5), un répondant invite l'IBPT à mieux cerner la notion d'utilisateurs affectés et demande que l'on ne tienne compte que des utilisateurs réellement affectés et non ceux potentiellement affectés. En cas de service mobile, ce répondant mentionne une difficultés d'interprétation en cas de roaming. En cas de service mobile, ce répondant propose de tenir compte des utilisateurs finaux susceptibles d'utiliser le service, en se basant sur des données historiques. En cas de service fixe, la situation n'est pas toujours claire.

18. Un répondant mentionne une difficulté d'interprétation des seuils d'impact en cas d'impact variant dans le temps. Si le nombre d'utilisateurs affectés décroit avec le temps, il se peut qu'une notification ne soit plus nécessaire.

19. Un répondant est d'avis que le délai de 24 h 00 pour transmettre la notification est trop court et ne permet pas à l'opérateur de collecter les diverses informations et contrôles nécessaires. A cet égard, un délai de 72 h est proposé, ce délai commençant à courir au moment où l'opérateur a collecté les informations nécessaires pour déterminer si une notification doit être faite.

20. Un répondant mentionne que l'usage d'un site comme préconisé par l'IBPT est compliqué, et que le fait de devoir confirmer la notification par une confirmation écrite et signée par une personne pouvant engager l'opérateur complique encore davantage la procédure. Ce répondant demande de pouvoir utiliser des méthodes de notifications pouvant être automatisées (via e-mail ou XML)

21. En ce qui concerne l'annexe 1 du projet de décision, un répondant formule diverses remarques de détails, avec des demandes de précisions. Il demande aussi de prévoir un champ « référence » en vue de pouvoir préciser de quelle notification il s'agit lorsque cette notification fait l'objet de précisions ultérieures.

22. Un répondant propose de prévoir une période de transition en vue de pouvoir implémenter la décision. Cette période est nécessaire afin de pouvoir s'assurer auprès de l'IBPT de la bonnne compréhension de la décision et afin de développer en interne les solutions techniques pour mettre en œuvre la décision.

23. Un autre répondant est d'avis que le délai de 24 h 00 pour transmettre la notification est trop court et ne permet pas à l'opérateur de collecter les diverses informations et contrôles nécessaires. Un délai d'un mois est préconisé. Au cas où ce délai de 24 h serait maintenu, ce répondant demande que seul un minimum d'informations doive être transmis dans ce délai, le reste étant alors transmis endéans la semaine.

24. Un autre répondant mentionne le fait de devoir confirmer la notification par une confirmation écrite et signée par une personne pouvant engager l'opérateur comme compliquant encore davantage la procédure. Il demande que ceci puisse être fait par e-mail.

25. En ce qui concerne les seuils d'impact 2 à 6 (actuellement seuils 1 à 5), un autre répondant invite aussi l'IBPT à mieux cerner la notion d'utilisateurs affectés et demande que l'on ne tienne compte que des utilisateurs réellement affectés et non de ceux potentiellement affectés. Ce répondant insiste aussi qu'il ne peut donner que les chiffres concernant ses propres utilisateurs.

26. Un répondant mentionne qu'il a déjà mis en place des mesures spécifiques harmonisées pour l'Europe, et que ces mesures sont différentes de celles proposées par le projet de décision visé ici. Néanmoins, ce répondant estime satisfaire à ses obligations légales en Belgique. Il insiste sur le fait qu'étant un opérateur pan-européen, il est important de savoir mettre en place des procédures harmonisées pan-européenne.