Institut belge des services postaux et des télécommunications

Version traduite de la décision du Conseil de l'IBPT du 23/08/2022 concernant l'absence de mesures de sécurité adéquates prises par Telenet pour son site à [confidentiel]

Version publique

Institut belge des services postaux et des télécommunications
Bâtiment Ellipse C | Boulevard du Roi Albert II 35 bte 1 | 1030 Bruxelles
T +32 2 226 88 88 | **F** +32 2 226 88 77 | **www.ibpt.be**

TABLE DES MATIÈRES

1. Objet

1. Il est reproché à Telenet de ne pas avoir pris les mesures de sécurité adéquates comme exigé à l'article 107/2 de la loi du 13 juin 2005 relative aux communications électroniques (ci-après la « loi télécoms ») pour son site établi à [confidentiel] (ci-après le « site de [confidentiel] »). Plus particulièrement, Telenet n'est pas parvenue à :

   1.1. protéger ce site contre la tempête Eunice du 18 février 2022 ;

   1.2. sécuriser l'accès physique à ce site, conformément à ce qui a été constaté lors d'une visite de deux membres du personnel de l'IBPT sur ce site le 21 février 2022.

2. L'IBPT somme Telenet :

   2.1. de renforcer la sécurité physique de l'accès à ce site, dans la mesure où cela n'a pas encore été effectué ;

   2.2. d'informer l'IBPT dans les 15 jours suivant la présente décision concernant le calendrier des travaux de reconstruction du site de [confidentiel], en incluant des détails sur les travaux et délais prévus.

3. L'IBPT impose une amende de 190 000 € à Telenet.

2. Cadre légal

2.1. La loi télécoms

4. L'article 2, 62/2°, de la loi télécoms définit la « sécurité des réseaux et services » comme suit :

   « *la capacité des réseaux et services de communications électroniques de résister, à un niveau de confiance donné, à toute action qui compromet la disponibilité, l'authenticité, l'intégrité ou la confidentialité de ces réseaux et services, de données stockées, transmises ou traitées ou des services connexes offerts par ces réseaux ou services de communications électroniques ou rendus accessibles via de tels réseaux ou services*. »

5. L'article 6 de la loi télécoms prévoit ce qui suit :

   « *Art. 6. Dans l'accomplissement des tâches qui lui incombent en vertu de la présente loi, l'Institut : [...] promeut les intérêts des citoyens, [...] en préservant la sécurité des réseaux et services ;* ».

6. Les obligations imposées aux opérateurs concernant la sécurité des réseaux et services se trouvent à l'article 107/2 (mesures de sécurité) et 107/3 (notification d'incidents et de menaces) de la loi télécoms. L'article 107/2, § 1er, prévoit ce qui suit :

« § 1er. Les opérateurs analysent les risques pour la sécurité de leurs réseaux et services. L'Institut peut fixer les modalités de cette analyse de risque.

Les opérateurs prennent les mesures d'ordre technique et organisationnel adéquates et proportionnées, y compris le cas échéant le chiffrement, pour gérer ces risques de manière appropriée ainsi que pour prévenir et limiter l'impact des incidents de sécurité tant pour les utilisateurs que pour d'autres réseaux et services.

Compte tenu des possibilités techniques les plus récentes, ces mesures garantissent un niveau de sécurité adapté aux risques existants.

Le Roi, sur proposition de l'Institut ou d'initiative, sur avis de l'Institut, peut préciser les mesures visées à l'alinéa 2, lorsque le risque visé à cet alinéa découle de l'organisation des opérateurs.

Sous réserve de l'alinéa 4 et après avis de l'Institut, le Roi peut préciser les mesures visées à l'alinéa 2. »

7. L'article 107/4 de la loi télécoms contient les compétences de l'IBPT afin de préserver la sécurité des réseaux et des services et notamment les dispositions suivantes :

« *Art. 107/4. § 1er. En vue de l'application des articles 107/2, 107/3 et du présent article, l'Institut peut donner des instructions contraignantes à un opérateur, y compris les mesures requises pour remédier à un incident de sécurité ou empêcher qu'un tel incident ne se produise lorsqu'une menace importante a été identifiée, ainsi que les dates limites de mise en œuvre de ces instructions. […]*

§ 2. L'opérateur fournit à l'Institut, à sa demande, toutes les informations nécessaires pour évaluer la sécurité de ses réseaux et services, y compris les documents relatifs à sa politique de sécurité. L'Institut peut fixer les modalités à respecter pour la fourniture de ces informations.

À la demande de l'Institut, un opérateur se soumet à un contrôle de sécurité effectué par l'Institut lui-même, par un organisme ou en partie par l'Institut et en partie par cet organisme. L'Institut fixe l'objet et les modalités du contrôle et, lorsque le contrôle est effectué par un organisme, le délai dans lequel il doit être effectué. Lorsque le contrôle est effectué par l'Institut, ce contrôle peut inclure des inspections sur place. […] » (nous soulignons)

2.2. La loi sur le statut de l'IBPT

8. L'article 14, § 1er, 3°, a), de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges (ci-après la « loi sur le statut de l'IBPT ») confie à l'IBPT la tâche de veiller au respect de la loi télécoms.

9. La présente décision est prise sur la base de l'article 21 de la loi sur le statut de l'IBPT, qui prévoit ceci :

« *Art. 21. § 1er. Si le Conseil dispose d'un faisceau d'indices qui pourraient indiquer un manquement à la législation ou à la réglementation dont l'Institut contrôle le respect, à une décision prise par l'Institut en exécution de cette législation ou réglementation ou à une décision visée à l'article 105, § 6, alinéa 1er, de la loi du 13 juin 2005 relative aux communications électroniques, il fait part le cas échéant de ses griefs à l'intéressé ainsi que des mesures envisagées visées au paragraphe 5 qui seront appliquées en cas de*

confirmation du manquement. Les sanctions ainsi prévues sont appropriées, effectives, proportionnées et dissuasives.

§ 2. Le Conseil fixe le délai dont dispose l'intéressé pour consulter le dossier et présenter ses observations écrites. Ce délai ne peut être inférieur à dix jours ouvrables.

§ 3. L'intéressé est invité à comparaître à la date fixée par le Conseil et communiquée par lettre recommandée. Il peut se faire représenter par le conseil de son choix.

§ 4. Le Conseil peut entendre toute personne pouvant contribuer utilement à son information, soit d'office, soit à la demande de l'intéressé.

§ 5. Si le Conseil conclut à l'existence d'un manquement, il peut adopter, en une ou plusieurs décisions, une ou plusieurs des mesures suivantes :

1° l'ordre qu'il soit mis fin au manquement, soit immédiatement, soit dans le délai raisonnable qu'il impartit, pour autant que ce manquement n'ait pas cessé; l'Institut prend à cet égard des mesures appropriées et proportionnées pour garantir le respect de ces conditions ;

1°/1. des prescriptions relatives à la manière dont il faut remédier au manquement ;

2° le paiement dans le délai imparti par le Conseil d'une amende administrative au profit du Trésor public d'un montant maximal de 5 000 euros pour les personnes physiques et de 5 % au maximum du chiffre d'affaires consolidé du contrevenant, avant impôts et hors T.V.A., réalisé au cours de l'exercice complet le plus récent dans le secteur des communications électroniques ou des services postaux en Belgique ou si le contrevenant ne développe pas d'activités lui faisant réaliser un chiffre d'affaires, d'un montant maximal de 1 000 000 d'euros pour les personnes morales. Pour les manquements au chapitre 2 de la loi du 5 mai 2017 relative aux services de médias audiovisuels en région bilingue de Bruxelles-Capitale, le montant de l'amende administrative est de maximum 5 % du chiffre d'affaires consolidé du contrevenant, avant impôts et hors T.V.A., réalisé dans le secteur en question au cours de l'exercice complet le plus récent, plafonné à 125 000 euros ;

2°/1 en vue de faire respecter une ou plusieurs de ses décisions, le paiement dans le délai imparti par le Conseil d'une astreinte au profit du Trésor public d'un montant maximal de 500 euros par jour de retard pour les personnes physiques et de 5 % du chiffre d'affaires journalier par jour de retard pour les personnes morales. L'astreinte est due à compter de la date que le Conseil fixe dans sa décision ;

3° l'ordre de cesser ou de suspendre la fourniture d'un service ou d'un ensemble de services qui, si elle se poursuivait, serait de nature à entraver la concurrence de manière significative, jusqu'au respect, selon les modalités fixées par le Conseil, des obligations imposées en matière d'accès à la suite d'une analyse de marché réalisée conformément à la loi du 13 juin 2005 relative aux communications électroniques ou à la loi du 5 mai 2017 relative aux services de médias audiovisuels en région bilingue de Bruxelles-Capitale.

Le chiffre d'affaires journalier visé à l'alinéa 1er, 2° /1, est le chiffre d'affaires annuel total consolidé avant impôts et hors T.V.A., réalisé en Belgique, dans le secteur des communications électroniques ou des services postaux, au cours de l'exercice comptable le plus récent, divisé par 365.

En l'absence de données concernant le chiffre d'affaires visé à l'alinéa 1er, 2° et 2° /1, l'Institut peut déterminer un chiffre d'affaires sur la base de données obtenues de tiers ou sur la base du chiffre d'affaires d'une personne comparable.

§ 5/1. Les amendes et astreintes visées au paragraphe 5, alinéa 1er, 2° et 2/1°, ne sont pas fiscalement déductibles.

§ 6. Si les mesures prises conformément au paragraphe 5 n'ont pas permis de remédier au manquement, le Conseil peut, après avoir suivi la procédure prévue aux paragraphes 1er à 5, imposer une amende administrative ou une astreinte dont le montant ou le pourcentage maximum représente le double du montant ou du pourcentage visé au paragraphe 5, alinéa 1er, 2° et 2° /1.

§ 7. Si les mesures prises conformément au paragraphe 5 n'ont pas permis de remédier au manquement et s'il s'agit d'un manquement grave ou répété, le Conseil peut en outre :

1° suspendre ou retirer les droits d'utilisation attribués, dont les conditions n'ont pas été

respectées ou

2° ordonner la suspension de tout ou partie de l'exploitation du réseau ou de la fourniture du service en question ainsi que de la commercialisation ou de l'utilisation de tout service ou produit concerné ;
§ 7/1. L'Institut ne prévoit des sanctions dans le cadre de la procédure visée à l'article 49/2 de la loi du 13 juin 2005 relative aux communications électroniques, que lorsqu'une entreprise ou une autorité publique fournit, en connaissance de cause ou du fait d'une négligence grave, des informations trompeuses, erronées ou incomplètes.
Lors de la détermination du montant des amendes ou des astreintes imposées à une entreprise ou à une autorité publique en application de l'alinéa 1er, l'Institut tient compte notamment de l'effet négatif du comportement de l'entreprise ou de l'autorité publique sur la concurrence et, en particulier, si, contrairement aux informations initialement communiquées ou à toute actualisation de ces informations, l'entreprise ou l'autorité publique soit a déployé un réseau ou procédé à une extension ou à une mise à niveau d'un réseau, soit n'a pas déployé de réseau et elle n'a pas fourni de justification objective à ce changement de plan.
§ 8. Toute décision prise en application du présent article est notifiée sans retard à l'intéressé ainsi qu'au ministre et publiée sur le site Internet de l'Institut. La notification à l'intéressé se fait par lettre recommandée.
La décision fait mention du délai raisonnable dans lequel l'intéressé doit satisfaire à la mesure ou aux mesures imposées. »

2.3. L'importance de la sécurité des réseaux et services

10. Les dispositions susmentionnées de la loi télécoms et de la loi sur le statut de l'IBPT démontrent qu'un cadre juridique a été instauré pour veiller à ce que les opérateurs prennent les mesures adéquates afin de garantir la sécurité de leurs réseaux et services de communications électroniques. En effet, il est essentiel pour la société dans son ensemble d'éviter toute perturbation du fonctionnement de ces réseaux et services et de pouvoir compter sur des réseaux et services fiables. Il ressort également des dispositions susmentionnées que l'IBPT doit jouer un rôle spécifique afin de garantir la sécurité des réseaux et services (examen des notifications d'incidents, instructions contraignantes, contrôle, sanction, etc.).

11. L'action de l'IBPT est soulignée dans son plan stratégique 2020-2022 de l'IBPT :

« 4.5 Sécurité des réseaux
Contexte
Les derniers développements technologiques, par exemple la 5G, offrent d'énormes possibilités de tout connecter, partout et toujours. D'une part, ces développements impliquent une forte augmentation de la dépendance de notre société à l'égard des communications électroniques. D'autre part, ils augmentent considérablement la complexité des réseaux de communications électroniques. La nécessité de disposer de réseaux de communications électroniques bien gérés et sûrs se fait donc de plus en plus sentir.

Travaux de l'IBPT
Via son service « Sécurité des réseaux », l'IBPT veille à la sécurité des réseaux publics de communications électroniques et des services de communications électroniques accessibles au public.

Ainsi, l'IBPT travaille en permanence avec les opérateurs pour prendre les mesures de sécurité appropriées afin de garantir la disponibilité, la confidentialité et l'intégrité de leurs réseaux. L'accent est mis à cet effet sur les infrastructures critiques, les principaux nœuds du réseau en Belgique. Si un incident survient malgré les mesures en place, l'IBPT en assurera le suivi et vérifiera si les mesures complémentaires nécessaires ont été prises.

L'IBPT encourage également la coopération entre les opérateurs et les services publics tels que la police, les services de sécurité et de renseignement et le Centre pour la Cybersécurité en Belgique.

L'IBPT surveille également l'accessibilité des services d'urgence et veille à ce que les opérateurs prennent les mesures nécessaires pour garantir l'accès à ces services. »

3. Procédure

12. La procédure qui a été suivie est la suivante :

12.1. Le 4 mai 2022, l'IBPT a envoyé le projet de la présente décision à Telenet (ci-après « le projet de décision ») ;

12.2. Telenet a réagi dans un e-mail du 20 mai 2022 (ci-après les « remarques écrites de Telenet du 20 mai 2022 ») ;

12.3. Le 23 mai 2022, Telenet a été entendue par le Conseil de l'IBPT ;

12.4. Le 7 juillet 2022, le projet de décision a été soumis aux régulateurs des médias. Ces derniers ont fait savoir à l'IBPT qu'ils n'avaient pas de remarque par rapport au projet de décision.

4. Griefs

4.1. Introduction : importance du site de Telenet de [confidentiel] pour le fonctionnement de son réseau

13. Il ressort de l'e-mail envoyé par Telenet à l'IBPT le 4 février 2022 que son site de [confidentiel] comprend les deux sections suivantes :

- la « headend » (HE) [confidentiel]. Les headends sont des points d'agrégation des réseaux coaxiaux et de fibre optique au niveau local. Selon l'e-mail précité de Telenet, mais sans tenir compte d'une redondance éventuelle, une interruption du fonctionnement de cette headend entraînerait [confidentiel] , et ;
- un des [confidentiel] « switching offices » (SO) de Telenet. Les « switching offices » agrègent le trafic fixe et mobile des accès locaux (headends) et assurent la connectivité avec les centres de données. Selon l'e-mail précité de Telenet, mais sans tenir compte d'une redondance éventuelle, un mauvais fonctionnement du switching office de

[confidentiel] aurait un impact [confidentiel]. La zone touchée comprendrait donc [confidentiel].

14. La figure ci-dessous illustre la position du switching office de [confidentiel] dans le backbone et son importance pour la connectivité [confidentiel] :

[confidentiel]

15. La figure suivante affiche les réseaux d'agrégation secondaires :

[confidentiel]

16. Cette figure illustre également l'importance du site de [confidentiel] pour [confidentiel]. Le site de [confidentiel] assure la connectivité des réseaux indiqués dans le schéma en orange et en vert, avec les centres de données.

17. Selon un e-mail de Telenet du 1er avril 2021, les clients non résidentiels critiques desservis par le switching office de [confidentiel] comprennent notamment [confidentiel]. Dans son e-mail du 27 avril 2022, Telenet a confirmé que [confidentiel] étaient également connectés au site.

18. À la suite d'une lettre de l'IBPT du 7 avril 2022, Telenet a communiqué dans son e-mail du 27 avril 2022 une estimation des clients qui sont connectés au site de [confidentiel]:

Services	**Switching office (SO)**	**Headend (HE) de [confidentiel]**
Mobile	+/- [confidentiel] clients. Telenet souligne que ces clients ne seraient pas touchés par la défaillance du switching office [confidentiel].	+/- [confidentiel] clients.
Fixe	[confidentiel] clients. Telenet souligne que ces clients ne seraient pas touchés par la défaillance du switching office [confidentiel].	[confidentiel] clients, dont [confidentiel] clients résidentiels. Les autres clients sont les clients de gros et B2B via câble coaxial.

19. L'IBPT ne prend pas en compte les mesures de sécurité, notamment d'éventuelles mesures de redondance, pour déterminer l'importance du site de [confidentiel] pour la fourniture des services de communications électroniques de Telenet. En effet, ces mesures de sécurité ne sont pas une mesure de l'importance de ce site (mais peuvent refléter son importance) mais permettent de réduire les risques de sécurité du site lorsqu'elles sont correctement mises en œuvre et testées régulièrement.

20. En ce qui concerne les services mobiles de Telenet, +/- **[confidentiel]** clients sont connectés au site de [confidentiel] en 2022, sur un total de **[confidentiel]** clients mobiles de Telenet le 31 décembre 2021. Le chiffre de [confidentiel] clients représente un peu plus

d'un [confidentiel]des clients des services mobiles de Telenet en 2021 (un [confidentiel] correspond à [confidentiel]).

21. En ce qui concerne les services fixes de Telenet, **[confidentiel]** clients sont connectés au site de [confidentiel] en 2022, sur un total de **[confidentiel]** clients au haut débit de Telenet le 31 décembre 2021. Le chiffre de **[confidentiel]** clients représente un peu moins d'un [confidentiel] des clients des services haut débit de Telenet en 2021 (un [confidentiel] correspond à [confidentiel], ce chiffre est arrondi).

22. [Confidentiel]. Les services de communications électroniques offerts par Telenet via ce site n'ont pas été touchés, mais les risques d'indisponibilité des services étaient élevés et Telenet a dû intervenir pour migrer les fonctionnalités ou veiller à la redondance.

23. Après cet incident, le site de [confidentiel] a été couvert d'une grande tente afin de le protéger des intempéries. La vulnérabilité du site a ainsi considérablement augmenté, car une tente implique davantage de risques de sécurité qu'un bâtiment ou un conteneur.

24. Dans ses remarques écrites du 20 mai 2022, Telenet explique que « *préalablement à la tempête* [Eunice du 18 février 2022]*, tous les équipements actifs avaient déjà été désactivés dans la partie endommagée du bâtiment de [confidentiel], et qu'il ne reste donc plus de services actifs dans la partie endommagée.* »

25. L'IBPT comprend sur la base de l'audition de Telenet et du « work breakdown » de Telenet (annexe à la pièce 1) que des équipements actifs ont été déplacés vers la partie intacte du bâtiment et que certains services ont été transférés dans des conteneurs sur le site.

26. Dans ses remarques écrites du 20 mai 2022, Telenet explique ce qui suit : « *Telenet a consenti des* efforts considérables *(au total environ 3000 heures-hommes externes et internes) afin de veiller à la redondance du site de [confidentiel] . Telenet a agi immédiatement après [confidentiel - l'incident]. [Confidentiel], tous les services critiques avaient été dupliqués de sorte que, en cas de nouvel [confidentiel - incident], ces services essentiels continueraient de fonctionner. [Confidentiel], cela était déjà le cas pour plus de 80 % des services critiques.* »

27. Il ressort de l'audition que la redondance du switching office a toujours été prévue : auparavant « site-redundant » (deux exemplaires de tout sur un même site), mais la géoredondance est appliquée depuis l'incident à [confidentiel] (un deuxième exemplaire de tout également sur un autre site, en l'occurrence sur le site du switching office de [confidentiel]).

28. Selon l'IBPT, il convient de relativiser l'argument de Telenet selon lequel il aurait fourni des efforts considérables. En effet, la redondance sur site (site-rendundant) mise en place sur le site de [confidentiel] avant l'incident [confidentiel] était insuffisante par rapport aux bonnes pratiques en matière d'architecture réseau pour le backbone du réseau. Un incident aurait pu affecter l'ensemble du site de [confidentiel], de sorte que la redondance sur site ne fonctionne pas. Les efforts effectués par Telenet pour mettre en place une redondance géographique étaient dès lors de toute manière nécessaires.

4.2. Premier grief : risque que la tente sur le site de [confidentiel] s'envole lors de la tempête Eunice du 18 février 2022

29. Le 17 février 2022, l'IBPT a envoyé un e-mail à Telenet lui demandant de tenir compte de la situation particulière du site de [confidentiel], étant donné que de mauvaises conditions météorologiques (tempête Eunice) étaient annoncées pour le 18 février 2022.

30. Le matin du 18 février 2022 (à 9h25), Telenet a envoyé par e-mail à l'IBPT la réponse suivante :

« Nous avons fait venir hier une société externe afin de soumettre la tente à un contrôle supplémentaire et ce contrôle était en ordre.

De plus, la sécurité effectue un contrôle permanent pour surveiller de près la situation.

En ce qui nous concerne, tout est sous contrôle. »

31. Le même jour, à savoir le 18 février 2022, mais dans l'après-midi (à 15h28), en pleine tempête, Telenet contacte l'IBPT, sans passer par le service de garde pour la sécurité des réseaux de l'IBPT (disponible 24h sur 24 et 7 jours sur 7), expliquant qu'il y a un danger imminent que la tente s'envole et que l'aide des pompiers est requise.

32. L'IBPT a transmis cette demande au Centre de crise du gouvernement et les pompiers ont été envoyés prioritairement sur place dans les 45 minutes. Lors de l'intervention des pompiers, les bâches à l'avant et à l'arrière de la tente ont été retirées afin de diminuer la prise au vent. Les précipitations sur le site étaient heureusement limitées.

33. Il est reproché à Telenet de ne pas avoir réalisé une analyse correcte du risque que la tente s'envole (Telenet s'est basée sur un seul sous-traitant qui a fait une mauvaise estimation) et de ne pas avoir pris les mesures de précaution nécessaires pour éviter ce risque, comme requis par les paragraphes 1er et 3 de l'article 107/2 de la loi télécoms :

« § 1er. Les opérateurs analysent les risques pour la sécurité de leurs réseaux et services. L'Institut peut fixer les modalités de cette analyse de risque.
Les opérateurs prennent les mesures d'ordre technique et organisationnel adéquates et proportionnées, y compris le cas échéant le chiffrement, pour gérer ces risques de manière appropriée ainsi que pour prévenir et limiter l'impact des incidents de sécurité tant pour les utilisateurs que pour d'autres réseaux et services.
Compte tenu des possibilités techniques les plus récentes, ces mesures garantissent un niveau de sécurité adapté aux risques existants.
Le Roi, sur proposition de l'Institut ou d'initiative, sur avis de l'Institut, peut préciser les mesures visées à l'alinéa 2, lorsque le risque visé à cet alinéa découle de l'organisation des opérateurs.
Sous réserve de l'alinéa 4 et après avis de l'Institut, le Roi peut préciser les mesures visées à l'alinéa 2. » (nous soulignons)

« § 3. Les opérateurs prennent toutes les mesures nécessaires, y compris préventives, pour assurer la disponibilité la plus complète possible des services de communications vocales et des services d'accès à l'internet en cas de défaillance exceptionnelle des réseaux

ou de force majeure.
Le Roi, sur proposition de l'Institut ou d'initiative, sur avis de celui-ci, peut préciser ces mesures, lorsque le risque de défaillance ou de force majeure découle de l'organisation des opérateurs.
Sans préjudice de l'alinéa 2, le Roi peut, après avis de l'Institut, préciser ces mesures. » (nous soulignons)

34. Dans ses remarques écrites du 20 mai 2022, Telenet explique ce qui suit : « *Le 16 février 2022, Telenet a fait venir dans une optique préventive et proactive une société de tentes professionnelle (confidentiel) sur le site pour contrôler la tente et sécuriser davantage l'installation le cas échéant, vu la tempête annoncée.* »

35. Cette affirmation (intervention de [confidentiel] le 16 février 2022) n'est cependant pas cohérente avec l'e-mail précité de Telenet à l'IBPT du 18 février 2022, selon lequel cette intervention a eu lieu le 17 février 2022.

36. Selon Telenet, il n'y avait à aucun moment un risque concernant la prestation de services pour les utilisateurs finaux. Tous les équipements actifs dans la partie endommagée du bâtiment avaient déjà été désactivés avant les tempêtes de février. Il n'y avait plus de services actifs ni passifs dans la partie endommagée. En raison de ces mesures, le fait que la tente s'envole totalement n'aurait eu aucune conséquence pour la sécurité des réseaux et services. L'intervention des pompiers était uniquement nécessaire car il y avait un risque éventuel que la tente cause des dommages pour les passants et les riverains.

37. Contrairement à ce qu'avance Telenet, il n'est pas certain que la tente, si elle s'était envolée à cause de la tempête, n'aurait pas affecté le fonctionnement de ses réseaux et services de communications électroniques.

38. En effet, vu le poids et la taille de la tente et le fait qu'elle recouvre l'entièreté du bâtiment (et donc également les parties du bâtiment qui ne sont pas abîmées et qui abritent des éléments actifs), elle aurait pu, lors de son envol, abîmer le bâtiment, des conduits d'évacuation ou le système de climatisation, ce qui aurait pu affecter la fourniture de réseaux ou services de communications électroniques de Telenet. On peut difficilement imaginer que la tente s'envole « à la verticale », sans toucher le bâtiment, ses conduits d'évacuation ou son système de climatisation, pour retomber en dehors du site de Telenet. En revanche, on peut raisonnablement estimer que la tente, lors de son envol, aurait touché le bâtiment, ses conduits d'évacuation ou son système de climatisation et aurait occasionné des dégâts sur le site même.

39. En vertu de l'article 107/2, § 1er, de la loi télécoms les opérateurs doivent prendre les mesures techniques et organisationnelles adéquates et proportionnées afin de bien maîtriser les risques pour la sécurité de leurs réseaux et services. L'article 107/2 vise donc les risques pour la sécurité des réseaux et services. Or, il y avait un risque que l'envol de la tente affecte la fourniture des réseaux ou services de communications électroniques de Telenet.

40. Exiger pour l'établissement du grief un incident (envol effectif de la tente) qui ait eu un impact réel sur le fonctionnement du réseau ou du service, signifierait que l'IBPT ne pourrait pas jouer à plein sa tâche de contrôle de l'article 107/2 précité.

41. En conclusion, l'IBPT considère que le premier grief (le fait de ne pas avoir pris à temps des mesures pour éviter l'envol de la tente) est établi et que Telenet n'a pas respecté l'article 107/2, § 1er, de la loi télécoms :

« § 1er. Les opérateurs analysent les risques pour la sécurité de leurs réseaux et services. L'Institut peut fixer les modalités de cette analyse de risque.
Les opérateurs prennent les mesures d'ordre technique et organisationnel adéquates et proportionnées, y compris le cas échéant le chiffrement, pour gérer ces risques de manière appropriée ainsi que pour prévenir et limiter l'impact des incidents de sécurité tant pour les utilisateurs que pour d'autres réseaux et services.
Compte tenu des possibilités techniques les plus récentes, ces mesures garantissent un niveau de sécurité adapté aux risques existants.
Le Roi, sur proposition de l'Institut ou d'initiative, sur avis de l'Institut, peut préciser les mesures visées à l'alinéa 2, lorsque le risque visé à cet alinéa découle de l'organisation des opérateurs.
Sous réserve de l'alinéa 4 et après avis de l'Institut, le Roi peut préciser les mesures visées à l'alinéa 2. »

4.3. Deuxième grief : mesures insuffisantes pour la sécurité physique de l'accès au site de [confidentiel]

4.3.1. Introduction

42. Après une demande du Centre de crise du gouvernement de fournir un rapport et vu l'importance du site de [confidentiel] pour le fonctionnement du réseau de Telenet, l'IBPT a demandé ce qui suit à Telenet :

Objet de la demande	Échanges entre l'IBPT et Telenet
- Une description des mesures de lutte contre les catastrophes prises par Telenet [confidentiel];	L'IBPT a posé ses différentes questions via différents e-mails [confidentiel] et Telenet y a répondu au cours du même mois.
- Une analyse de l'impact potentiel de la perte totale du bâtiment ([confidentiel] et en date du 1er février 2022, avec la redondance prévue) ;	L'IBPT a posé cette question dans un e-mail du 1er février 2022 et Telenet y a répondu dans son e-mail du 4 février 2022.
- Pouvoir visiter le site de [confidentiel];	L'IBPT a posé cette question à Telenet dans un e-mail du 16 février 2022 et des e-mails ultérieurs. Telenet a proposé d'organiser cette visite le 20 avril 2022, suggérant des travaux à réaliser.

- Donner un aperçu des mesures relatives à la sécurité physique du site de [confidentiel] et en fournir quelques photos à l'IBPT.	L'IBPT a posé cette question dans un e-mail du 17 février 2022. Telenet y a répondu dans son e-mail du 21 février 2022, à 15h51 (sans fournir de photos).

43. En raison de l'absence de réponse de Telenet avant le 21 février 2022 concernant les mesures relatives à la sécurité physique du site de [confidentiel], du risque que la tente ait pu s'envoler le 18 février 2022 et de l'intervention des pompiers (voir section 4.2), deux membres du service Sécurité des réseaux de l'IBPT se sont rendus le 21 février 2022 au matin sur le site de [confidentiel], afin d'évaluer la situation.

44. Dans ses remarques écrites du 20 mai 2022, Telenet déclare qu'il n'est pas raisonnable « *que l'IBPT donne d'abord l'impression de vouloir attendre jusqu'à la mi-avril pour effectuer une visite sur place, reçoive ensuite le 21 février 2022 un aperçu des mesures relatives à la sécurité physique de Telenet, pour ensuite conclure au paragraphe [43] qu'une visite immédiate était nécessaire "en l'absence d'une réponse de Telenet".*»

45. Il est vrai que Telenet a proposé une visite le 20 avril 2022, mais l'IBPT a avancé la visite vu les faits présentés au paragraphe 43 et parce que Telenet a proposé une date située plus d'un mois et demi plus tard que les dates proposées par l'IBPT. Au moment de la visite, l'IBPT n'avait toujours pas reçu de réponse de Telenet concernant les mesures en matière de sécurité physique du site de [confidentiel].

46. De plus, rien n'empêche l'IBPT de réaliser des contrôles inopinés auprès des opérateurs. La visite inopinée à [confidentiel] a également prouvé son utilité étant donné qu'elle a révélé que l'accès physique au site n'était pas en ordre.

47. Ce contrôle repose sur les deux bases légales suivantes :

47.1. Comme expliqué précédemment, l'article 14, § 1er, 3°, a), de la loi sur le statut de l'IBPT confère à l'Institut la tâche de veiller au respect de la loi télécoms ;

47.2. L'article 107/4, § 2, alinéa 2, de la loi télécoms prévoit ce qui suit :

« À la demande de l'Institut, un opérateur se soumet à un contrôle de sécurité effectué par l'Institut lui-même, par un organisme ou en partie par l'Institut et en partie par cet organisme. L'Institut fixe l'objet et les modalités du contrôle et, lorsque le contrôle est effectué par un organisme, le délai dans lequel il doit être effectué. Lorsque le contrôle est effectué par l'Institut, ce contrôle peut inclure des inspections sur place. »

4.3.2. Le rôle de [confidentiel]

48. Sur place, les deux membres du service Sécurité des réseaux de l'IBPT ont constaté que le site était protégé par [confidentiel] (24/7), mais :

48.1. [confidentiel]

48.2. [confidentiel]

48.3. [confidentiel]

49. Dans ses remarques écrites du 20 mai 2022, Telenet explique ce qui suit :

> « *- L'agent de sécurité sur place n'a pas appliqué la procédure convenue (voir annexe 1 : contrôle d'accès [confidentiel]) en ne contrôlant pas l'identité des inspecteurs de l'IBPT. Cela s'explique notamment par le fait que le site de [confidentiel] était encore fréquemment visité juste avant la visite de l'IBPT par des visiteurs externes dans le cadre de l'expertise légale [confidentiel], faisant que de nombreux avocats et experts d'assurances ont visité le site. L'agent de sécurité sur place a probablement pensé à tort que les inspecteurs de l'IBPT visitaient le site dans le cadre de l'expertise légale. Dans tous les cas, l'agent de sécurité aurait dû contrôler sur place l'identité des inspecteurs de l'IBPT. Telenet a entendu son sous-traitant [confidentiel] pour qu'il se justifie et a très récemment répété que l'identité des visiteurs externes devait toujours être contrôlée (voir annexe 2 : e-mail du 11 mai 2022 de Telenet à [confidentiel]).*
>
> *- Vu les larges compétences légales de l'IBPT, Telenet demande de recevoir les lignes directrices nécessaires de l'IBPT et demande d'éclaircir si les inspecteurs de l'IBPT peuvent entrer sur les sites de Telenet sans encadrement par Telenet. La mise en demeure insinue que l'IBPT s'attend à ce qu'une visite du site ne soit possible qu'avec l'encadrement par Telenet.* »

50. L'IBPT ne conteste pas que Telenet ait convenu d'une procédure avec [confidentiel]. Toutefois, cette procédure n'a pas été appliquée lors de la visite des membres du personnel de l'IBPT (et potentiellement pas non plus pour les avocats, les experts d'assurances et les sociétés qui se sont présentés à l'agent de sécurité). Il est reproché à Telenet de ne pas s'être assurée que cette procédure soit effectivement appliquée. Cela était d'autant plus important vu le nombre important de visiteurs sur le site à la suite des expertises légales et des travaux de démolition qui ont eu lieu.

51. L'IBPT ne s'attend pas à ce que sa visite soit uniquement possible avec l'encadrement de Telenet ou d'un agent de sécurité de [confidentiel], mais les conséquences négatives possibles d'une absence d'identification d'un visiteur sont encore plus importantes si le visiteur n'est pas encadré lors de sa visite.

52. Lors de leur visite, les membres du personnel de l'IBPT étaient capables d'entrer dans la partie intacte du bâtiment (via une porte ouverte sous la structure de la tente).

4.3.3. Accès au site, caméras et alarmes

53. Lors de leur visite, les membres du personnel de l'IBPT ont constaté ce qui suit :

53.1. [confidentiel] ;

53.2. [confidentiel].

54. Dans ses remarques écrites du 20 mai 2022, Telenet répond ce qui suit :

- « *Telenet n'a pas attendu la mise en demeure de l'IBPT pour prendre des mesures supplémentaires afin d'améliorer la sécurité physique du site de [confidentiel]. Ainsi, Telenet était déjà en train d'installer des caméras supplémentaires (installation prévue dans le courant du mois de mai 2022) afin de compléter à nouveau la vue sur le site, en ce compris sur la zone à l'arrière du site. Une partie des caméras se trouvaient en effet avant [confidentiel- l'incident] dans la partie endommagée du site ainsi que du côté du mur extérieur [confidentiel]* » ;

- « *afin d'optimiser encore davantage la sécurité du site, Telenet avait aussi, avant la mise en demeure de l'IBPT, entrepris de faire installer une nouvelle centrale anti-intrusion et un système d'alarme anti-intrusion (pour mai 2022). Grâce à ces mesures de sécurité supplémentaires, [confidentiel]. Dès lors, l'accès au site de [confidentiel], ainsi qu'à la plupart des autres infrastructures critiques de Telenet, sera uniquement validé selon les protocoles appliqués généralement.* »

55. Lors de l'audition, Telenet a ajouté que les caméras ne pouvaient naturellement être installées qu'après la démolition du site et que Telenet devait donc attendre la concrétisation du planning pour la reconstruction et la reconstruction effective avant de faire installer de nouvelles caméras et une alarme.

56. L'IBPT note que Telenet a communiqué le projet de planning suivant concernant les mesures de reconstruction dans ses remarques écrites du 20 mai 2022 (sous réserve notamment de la disponibilité des ressources nécessaires et de l'obtention des autorisations nécessaires) :

56.1. [confidentiel]

56.2. [confidentiel]

56.3. [confidentiel]

56.4. [confidentiel]

56.5. [confidentiel]

56.6. [confidentiel]

57. L'IBPT ne trouve pas acceptable qu'aucune caméra n'ait encore été installée, étant donné la longue période de temps concernée [confidentiel].

4.3.4. L'infrastructure de climatisation

58. Sur place, les deux membres du service Sécurité des réseaux de l'IBPT ont constaté que l'infrastructure de climatisation se trouvait à l'extérieur dans une prairie à proximité et était facilement accessible.

59. La réponse de Telenet dans ses remarques écrites du 20 mai 2022 est la suivante : « *Au moment de l'inspection, l'infrastructure de climatisation se trouvait en effet en dehors du*

périmètre du site afin de faire de la place pour la démolition de la partie endommagée du site. Entre-temps, Telenet a pris toutes les mesures nécessaires pour déplacer à nouveau la climatisation et celle-ci se trouve à nouveau dans le périmètre du site (voir photo ci-dessous). »

60. Lors de l'audition, Telenet a indiqué que la climatisation n'était pas nécessaire pour le refroidissement de la partie placée sous tente, mais que cette climatisation pouvait être utilisée en tant que capacité de refroidissement supplémentaire dans le switching office de [confidentiel] si nécessaire (si le switching office atteint des températures trop élevées en été).

61. L'IBPT estime que si un système de climatisation était au départ nécessaire pour le bon fonctionnement du site, il l'est également après le déplacement des éléments actifs de la partie abîmée du bâtiment vers d'autres parties du site et a fortiori plus encore, vu que le déplacement de ces éléments actifs implique plus de matériel dans un même espace. En tout état de cause, il ne peut pas être exclu qu'à un moment donné ce système de climatisation ait été nécessaire pour le bon fonctionnement du site (par exemple en cas de températures extérieures élevées ou du fait de la concentration d'équipements dans un local à la suite du déplacement des éléments actifs).

62. L'explication de Telenet n'enlève pas le fait que la climatisation, au moment où l'installation de refroidissement se trouvait en dehors du périmètre sécurisé, était relativement accessible et donc susceptible d'être manipulée de manière nuisible par un passant. Une telle manipulation aurait pu avoir une incidence sur la sécurité des réseaux et du service.

4.3.5. Conclusion

63. Le deuxième grief est retenu. Telenet n'a pas pris des mesures de sécurité suffisantes concernant l'accès physique au site comme l'exigeait l'article 107/2, paragraphe 1er, de la loi télécoms :

« § 1er. Les opérateurs analysent les risques pour la sécurité de leurs réseaux et services. L'Institut peut fixer les modalités de cette analyse de risque.
Les opérateurs prennent les mesures d'ordre technique et organisationnel adéquates et proportionnées, y compris le cas échéant le chiffrement, pour gérer ces risques de manière appropriée ainsi que pour prévenir et limiter l'impact des incidents de sécurité tant pour les utilisateurs que pour d'autres réseaux et services.
Compte tenu des possibilités techniques les plus récentes, ces mesures garantissent un niveau de sécurité adapté aux risques existants.
Le Roi, sur proposition de l'Institut ou d'initiative, sur avis de l'Institut, peut préciser les mesures visées à l'alinéa 2, lorsque le risque visé à cet alinéa découle de l'organisation des opérateurs.
Sous réserve de l'alinéa 4 et après avis de l'Institut, le Roi peut préciser les mesures visées à l'alinéa 2. »

5. Mesures à prendre par Telenet pour sécuriser l'accès physique au site de [confidentiel]

64. Vu le deuxième grief formulé à l'encontre de Telenet (point 4.3 Mesures insuffisantes pour la sécurité physique de l'accès au site de [confidentiel]) et pour autant que cela n'ait pas déjà été effectué dans l'intervalle, l'IBPT somme Telenet de prendre immédiatement les mesures adéquates et proportionnées d'ordre technique et organisationnel visées à l'article 107/2, § 1er, de la loi télécoms, afin de sécuriser l'accès physique à son site de [confidentiel], à savoir : [confidentiel].

65. Ces instructions reposent sur les bases suivantes :

65.1. Art. 21, § 5, de la loi sur le statut de l'IBPT : *« Si le Conseil conclut à l'existence d'un manquement, il peut adopter, en une ou plusieurs décisions, une ou plusieurs des mesures suivantes :*
1° l'ordre qu'il soit mis fin au manquement, soit immédiatement, soit dans le délai raisonnable qu'il impartit, pour autant que ce manquement n'ait pas cessé; l'Institut prend à cet égard des mesures appropriées et proportionnées pour garantir le respect de ces conditions ;
1°/1 des prescriptions relatives à la manière dont il faut remédier au manquement ; »

65.2. Art.107/4 de la loi télécoms : *« § 1er. En vue de l'application des articles 107/2, 107/3 et du présent article, l'Institut peut donner des instructions contraignantes à un opérateur, y compris les mesures requises pour remédier à un incident de sécurité ou empêcher qu'un tel incident ne se produise lorsqu'une menace importante a été identifiée, ainsi que les dates limites de mise en œuvre de ces instructions. »*

66. L'IBPT effectuera de nouveaux contrôles sur ce site pour vérifier si ces mesures ont été prises.

67. De plus, l'IBPT somme Telenet de communiquer à l'IBPT dans les 15 jours suivant la présente décision le calendrier des travaux de reconstruction du site de [confidentiel], en détaillant les travaux prévus et les délais.

68. Le fait que le site de [confidentiel] ait été mis sous tente entraîne en effet plus de risques en matière de sécurité que si le site se trouvait dans un bâtiment. Ce risque doit être limité le plus possible.

69. Cette demande d'informations se base sur les dispositions suivantes :

69.1. L'article 107/ 4, § 2, de la loi télécoms : « *§ 2. L'opérateur fournit à l'Institut, à sa demande, toutes les informations nécessaires pour évaluer la sécurité de ses réseaux et services, y compris les documents relatifs à sa politique de sécurité. L'Institut peut fixer les modalités à respecter pour la fourniture de ces informations.* » ;

69.2. L'article 14, § 2, 2°, de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges, selon lequel : *« Dans le cadre de ses compétences, l'Institut : [...] 2° peut exiger, par demande motivée, de toute personne concernée toute information utile. L'Institut fixe le délai de communication des informations demandées ».*

6. Imposition d'une amende administrative

6.1. Nécessité d'imposer une amende

70. L'IBPT considère que l'imposition d'une amende administrative à Telenet est justifiée, tant vu les griefs que l'impact (possible) d'un incident sur le site de [confidentiel] sur le bon fonctionnement de son réseau et par conséquent sur les intérêts des utilisateurs finaux (voir section 4.1).

71. L'absence d'une amende pourrait laisser penser que la loi télécoms pourrait simplement être enfreinte sans que l'opérateur ne soit puni. Il n'est pas acceptable qu'un opérateur puisse violer la loi télécoms et ensuite échapper à toute sanction dès lors qu'il prend les mesures nécessaires après que l'IBPT ait attiré son attention sur cette violation.

6.2. Principes de calcul du montant de l'amende

72. L'article 21, § 1er, de la loi sur le statut de l'IBPT prévoit ceci : *« Les sanctions ainsi prévues sont appropriées, effectives, proportionnées et dissuasives.* »

73. En outre, la loi sur le statut de l'IBPT fixe uniquement les plafonds pour le montant des amendes, mais ne précise pas la méthode que l'IBPT doit suivre pour le calcul de ces amendes. Mis à part ces plafonds, la définition du montant de l'amende relève de la compétence discrétionnaire de l'IBPT.

74. Le montant de l'amende est déterminé à l'aide des lignes directrices que l'IBPT a établies à cet effet dans sa communication du 31 mars 2020 concernant les lignes directrices relatives au calcul du montant des amendes administratives imposées par l'IBPT (ci-après les « lignes directrices »).

75. D'une part, les amendes visent à réagir de manière appropriée au non-respect de la réglementation et, d'autre part, à avoir un effet dissuasif. Il ne s'agit pas ici de l'indemnisation de la victime à la suite du comportement irrégulier. L'effet dissuasif comprend deux volets : le but est d'encourager le contrevenant à ne plus commettre l'infraction (effet dissuasif spécifique) et d'inciter des tiers à ne pas commettre l'infraction ou une infraction similaire (effet dissuasif général).

76. En vertu du principe de proportionnalité, le montant de l'amende doit être suffisamment élevé pour réaliser les objectifs poursuivis sans aller plus loin que nécessaire pour atteindre ces objectifs.

77. Le montant maximal de l'amende est « de 5 % au maximum du chiffre d'affaires du contrevenant réalisé au cours de l'exercice complet le plus récent dans le secteur des communications électroniques ou des services postaux en Belgique » (article 21, § 5, 2°, de la loi sur le statut de l'IBPT). L'exercice complet le plus récent connu de l'IBPT est l'exercice 2021.

78. Le montant de l'amende pris en compte dans ce cas-ci est bien inférieur au montant maximal.

79. Dans les paragraphes suivants, l'IBPT détaille les éléments dont il a tenu compte dans le cadre du calcul du montant de l'amende.

6.3. Calcul du montant de base

6.3.1. Chiffre d'affaires pertinent

80. La première phase du calcul du montant de base de l'amende consiste à déterminer le chiffre d'affaires du contrevenant. L'IBPT estime opportun de tenir compte du chiffre d'affaires annuel réalisé par le contrevenant sur le marché sur lequel l'infraction s'est produite et, par conséquent, sur le(s) marché(s) où les conséquences de l'infraction se font sentir (« chiffre d'affaires pertinent »).

81. Via le site de [confidentiel], Telenet offre « tous » les services :

- données mobiles et fixes ; et
- téléphonie mobile et fixe.

82. Par conséquent, l'IBPT tient compte du chiffre d'affaires réalisé en 2021 par Telenet pour ses différents services, à savoir [confidentiel] € :

Objet	
Total net retail revenues of which revenues related to telecommunication	[confidentiel]
Total wholesale revenues	[confidentiel]
Total	[confidentiel]

83. Le switching office de [confidentiel] est l'un des [confidentiel] seuls switching offices de Telenet. C'est la raison pour laquelle l'IBPT tient compte d'un [confidentiel] du chiffre d'affaires précité, à savoir [confidentiel] € (arrondi à [confidentiel] €).

84. L'IBPT tient compte du chiffre d'affaires réalisé par Telenet pendant un an pour les raisons suivantes. La tente a été installée sur le site de [confidentiel] après qu'une partie de l'infrastructure sur ce site [confidentiel]. L'inspection par les deux membres du personnel de l'IBPT sur ce site avait eu lieu le 21 février 2022, à savoir un peu moins [confidentiel].

85. Lors du mois de mai 2022 (confidentiel), Telenet a entrepris certaines actions afin d'améliorer le niveau de sécurité de l'accès physique au site :

85.1. e-mail du 11 mai 2022 à [confidentiel] rappelant une nouvelle fois le protocole convenu en matière de contrôle d'accès au site de [confidentiel];

85.2. calendrier concret de l'installation de caméras supplémentaires, d'une nouvelle centrale anti-intrusion et d'un système d'alarme anti-intrusion ;

85.3. la réinstallation de la climatisation dans le périmètre du site.

86. Dans le cadre du calcul du chiffre d'affaires pertinent, Telenet demande que l'IBPT tienne compte de la géoredondance avec le switching office de [confidentiel]. En cas de panne complète du switching office et du site headend de [confidentiel], maximum [confidentiel] clients mobiles pouvaient être touchés selon Telenet, ainsi que [confidentiel] clients fixes, à savoir les clients connectés au site headend de [confidentiel].

87. L'IBPT ne suit pas ce raisonnement pour les raisons suivantes :

87.1. Il est toujours possible qu'un incident au sein du switching office de [confidentiel] puisse également entraîner une défaillance de la géoredondance (par exemple parce que le switching office de [confidentiel] est déjà saturé). De plus, il ressort de la pratique que la redondance ne fonctionne pas toujours.

87.2. Lors de l'audition du 23 mai 2022, Telenet a indiqué que le switching office de [confidentiel] (avec celui [confidentiel]) assure la géoredondance pour le switching office de [confidentiel]. En cas d'interruption du switching office de [confidentiel], il n'y aurait par conséquent plus de redondance complète pour le switching office de [confidentiel], ce qui aurait des conséquences importantes en cas de problèmes au sein du switching office de [confidentiel].

6.3.2. La gravité de l'infraction

88. La deuxième étape du calcul du montant de base consiste à multiplier le chiffre d'affaires pertinent avec un pourcentage reflétant la gravité de l'infraction, qui peut être faible, moyenne, grave ou très grave.

89. L'IBPT évalue le degré de gravité de l'infraction au cas par cas pour chaque type d'infraction, en tenant compte de la nature de l'infraction et de son impact réel et/ou possible sur les objectifs réglementaires[1].

90. En cas de violation limitée de l'un des objectifs en question ou de violation d'une obligation purement administrative, l'on peut parler d'infraction légère. En cas de violation de différents objectifs, cette violation peut être considérée comme une infraction moyenne à grave. Une violation considérable d'un objectif peut en revanche constituer une infraction très grave. L'infraction est d'autant plus grave si elle constitue une violation considérable de plusieurs objectifs. Lors de l'examen de l'impact réel et/ou possible de l'infraction sur ces objectifs, l'IBPT tient compte des circonstances pertinentes du cas en question. Le degré de gravité varie en principe entre 0 % et 5 % du chiffre d'affaires pertinent.

91. Il s'agit en l'occurrence d'une violation possible des intérêts des utilisateurs finaux (particuliers, entreprises et pouvoirs publics, qui sont des clients de Telenet). Une interruption du service en raison d'une défaillance du site de [confidentiel] porterait directement atteinte à leurs intérêts.

92. L'IBPT qualifie cette infraction de moyenne :

[1] Ces objectifs réglementaires consistent notamment en la promotion ou le maintien de la concurrence, la promotion des intérêts des consommateurs, la stimulation de l'économie, la protection de l'intérêt public, la promotion de la gestion efficace des ressources rares (spectre), etc.

92.1. vu l'impact potentiellement considérable d'une interruption du fonctionnement du site de [confidentiel];

92.2. vu qu'au final aucun incident de sécurité ne s'est produit et qu'il n'y a eu aucun impact dans la pratique.

93. L'IBPT applique donc un pourcentage de 0,5 % au chiffre d'affaires pris en compte de [confidentiel] €, de sorte que le montant de base équivaut à [confidentiel] € (montant arrondi).

6.4. Circonstances aggravantes et atténuantes

6.4.1. Introduction

94. L'IBPT estime en outre qu'il est approprié et proportionné d'adapter le montant de base en fonction du comportement concret du contrevenant, en tenant compte des circonstances aggravantes et/ou atténuantes qui peuvent respectivement augmenter et/ou faire baisser le montant de base de l'amende.

95. L'IBPT retient les trois circonstances aggravantes suivantes.

6.4.2. Manquement de Telenet malgré l'appel de l'IBPT

96. Telenet n'a pas sécurisé l'accès au site de [confidentiel] de manière suffisante, alors que l'IBPT lui avait demandé à maintes reprises (voir notamment les e-mails du 16 et 17 février 2022) de pouvoir visiter ce site afin de contrôler la sécurité physique de l'accès au site.

97. Par conséquent, Telenet savait que ce point nécessitait une attention particulière et a tout de même omis de faire le nécessaire, comme cela a été constaté.

6.4.3. Collaboration insuffisante avec l'IBPT pendant la tempête Eunice

98. En préparation de la tempête Eunice, l'IBPT a organisé une réunion le vendredi 18 février 2022 à 9h30 avec les principaux opérateurs actifs en Belgique.

99. Lors de cette réunion, l'IBPT a demandé aux opérateurs de fournir les informations suivantes lors de la tempête, afin de pouvoir régulièrement faire rapport au Centre de crise concernant l'état des réseaux :

99.1. Un rapport toutes les deux heures selon un modèle fourni par l'IBPT (période révisable en fonction de la situation) ;

99.2. Les coordonnées géographiques des antennes perturbées dans un tableau composé de deux colonnes (X et Y).

100. Il s'agit d'une forme simplifiée de rapportage afin de faciliter le travail de l'opérateur.

101. Telenet est le seul opérateur à ne pas avoir fourni ces informations ou à ne pas l'avoir fait en temps utile ou au format désiré, comme le montre le tableau ci-dessous :

Date et heure du rapportage demandé	Réception du rapport de Telenet
18 février 2022 – 13h00	13h59
18 février 2022 – 15h00	-
18 février 2022 – 17h00	17h26
18 février 2022 – 19h00	20h23
18 février 2022 – 21h00	-
19 février 2022 – 9h00	-

102. Il convient de remarquer que Telenet avait déjà signalé lors de la réunion précitée du 18 février 2022 qu'elle ne pouvait pas garantir un rapportage régulier de l'état du réseau. L'IBPT avait alors insisté sur l'importance et la nécessité de ce rapportage. Dans un e-mail envoyé à l'IBPT le 23 février 2022, Telenet indiquait à nouveau qu'elle n'avait pas pu satisfaire aux demandes de rapportage de l'IBPT. Toutefois, l'IBPT rappelle que Telenet est le seul opérateur qui n'a pas effectué le rapportage comme demandé.

103. Dans ses remarques écrites du 20 mai 2022, Telenet explique ce qui suit : elle « *a tenu l'IBPT au courant le jour de la tempête du statut du réseau via des mises à jour régulières sur le statut (à 13h59, 15h43, 16h02, 16h18, 17h26 et 20h23), mais certes pas au format spécifique demandé par l'IBPT. L'Institut était ainsi tout à fait au courant de l'état du réseau de Telenet.* »

104. L'IBPT reconnaît que Telenet lui a adressé le 18 février 2022 un e-mail à 15h43, à 16h02 et à 16h18. Mais ces e-mails ne donnent pas un « update du statut » du réseau de Telenet (donner la situation du réseau à un moment donné, en particulier la liste des antennes qui ne fonctionnaient plus correctement du fait de la tempête) mais visent à se coordonner avec l'IBPT dans le cadre du risque d'envol de la tente sur le site de [confidentiel].

105. De plus, comme expliqué dans la section 4.2, Telenet, en contactant l'IBPT le 18 février 2022 en raison du risque que la tente sur le site de [confidentiel] s'envole à cause de la tempête Eunice, n'a pas respecté la matrice d'escalade en appelant un membre du service Sécurité des réseaux de l'IBPT au lieu d'appeler le service de garde pour la sécurité des réseaux de l'IBPT (la permanence). Par le passé, l'IBPT a pourtant informé de manière répétée Telenet, ainsi que les autres opérateurs, de cette matrice d'escalade et de la procédure de communication (e-mails du 15 mars 2018 et du 17 septembre 2021). Il est important que Telenet en tienne compte :

105.1. afin de garantir que les membres du personnel de Telenet qui traitent un incident de sécurité la connaissent et aient l'automatisme de contacter la permanence ;

105.2. afin de garantir une diffusion correcte de l'information et une réponse effective aux questions. Seule la permanence est disponible 24h sur 24, 7 jours sur 7. De plus, contacter la permanence permet de garantir que les informations sont centralisées

auprès du membre du personnel de l'IBPT qui est responsable de la permanence au moment de la notification de l'incident. Le traitement de ces informations est crucial lors de la gestion d'incidents. En cas de non-respect des procédures, des situations qui sont déjà critiques peuvent devenir plus graves et entraîner des pertes économiques ou humaines qui auraient pu être évitées si les procédures avaient été suivies, notamment en cas de perturbation de l'accès aux services d'urgence.

106. Telenet reconnaît que le premier contact téléphonique avec l'IBPT n'est pas passé par le service de garde. Toutefois, selon Telenet, l'IBPT n'a indiqué à aucun moment – ni pendant la tempête ni pendant une discussion post mortem – que Telenet aurait dû appeler un autre numéro de l'IBPT. De plus, Telenet a envoyé presque immédiatement après la conversation téléphonique initiale un e-mail au service de garde de l'IBPT, comme prévu dans la matrice d'escalade de l'IBPT, demandant à l'IBPT d'intervenir.

107. Selon l'IBPT, Telenet n'est pas soudainement disculpée du non-respect de la procédure parce que l'IBPT aurait pu lui communiquer ce reproche plus tôt.

108. Par contre, l'IBPT estime que le fait que Telenet ait adressé ses e-mails à l'adresse e-mail de la permanence comme expliqué ci-dessus réduit l'importance des circonstances aggravantes.

6.4.4. Le non-respect régulier des procédures par Telenet lors des incidents souligne le manque de volonté d'appliquer les processus internes et l'expertise adéquats en matière de gestion de crise.

109. Lors du suivi de la gestion de l'incident (risque d'envol de la tente lors de la tempête), l'IBPT a été renvoyé vers divers points de contact de Telenet qui ne disposaient pas de toutes les informations et n'a pas reçu l'autorisation de contacter la personne responsable de la gestion de l'incident. Telenet n'a donc pas donné suite à la demande de l'IBPT de désigner un point de contact unique, étant donné que diverses personnes étaient impliquées, chacune ayant ses propres coordonnées, et aucune n'était d'ailleurs capable de fournir les informations nécessaires.

110. Dans ses remarques écrites du 20 mai 2022, Telenet explique ce qui suit : « *L'IBPT n'étaye pas les conclusions de ce paragraphe par des exemples concrets. Telenet n'est pas au courant de n'avoir « régulièrement » pas respecté les procédures en cas d'incidents. S'il existe des lacunes dans les processus internes, nous aimerions recevoir des exemples concrets afin de pouvoir prendre les mesures nécessaires. En cas de manquements avérés, Telenet est naturellement disposée à examiner des adaptations de ses processus et à optimiser ceux-ci en concertation avec l'IBPT.* »

111. Lors de l'audition, Telenet a admis qu'il y avait parfois un problème lors d'incidents véritablement critiques en raison de la subdivision entre d'une part le SOC et d'autre part le SPOC au sein de regulatory.

112. Lors de la tempête Eunice, le point de contact de Telenet auprès de l'IBPT n'était pas en mesure de lui fournir une vue globale sur le réseau, soit par manque d'informations à sa disposition, soit par manque de temps. Durant cette tempête, un employé de Telenet a redirigé les membres du service sécurité des réseaux de l'IBPT vers son collègue, qui a lui-même redirigé les membres de ce service vers le premier employé.

113. Lors d'incidents en 2021 (10/03/2021 et 23/03/2021), les numéros fournis par Telenet à la permanence de l'IBPT ne fonctionnaient pas ou personne ne répondait. Ces situations néfastes à la gestion d'incidents sont occasionnées par une sous-traitance par Telenet des activités de monitoring. Telenet semble avoir des difficultés à fournir des rapports simplifiés à cause de la multiplication d'acteurs. L'IBPT a toujours réagi par rapport à ces difficultés en rappelant à Telenet ou aux opérateurs les numéros de téléphone à utiliser et les règles à suivre.

114. Les critiques qui résultent des deux paragraphes précédents ne sont cependant pas prises en compte pour le calcul du pourcentage lié aux circonstances aggravantes, étaient donné qu'elles ne ressortent pas d'écrits.

6.4.5. Conclusions en ce qui concerne les circonstances aggravantes

115. Compte tenu des arguments de Telenet, l'IBPT limite l'augmentation du montant de base à 5 % au lieu de 10 % dans le projet de décision, de sorte que le montant de base de l'amende passe ainsi à [confidentiel] € (montant arrondi).

6.5. Calcul final du montant de l'amende

116. L'IBPT revoit finalement le montant de l'amende à la baisse à 190 000 € (montant arrondi) afin de parvenir à montant proportionné. Cette diminution est considérable (moins [confidentiel] %). Cette diminution est justifiée par le principe de proportionnalité appliqué par l'IBPT, conformément à ses « lignes directrices » :

« 24. Lors des différentes étapes susmentionnées, l'IBPT prend en compte la proportionnalité et la nécessité de donner à l'amende un effet dissuasif ce qui, peut, le cas échéant, mener à un ajustement du montant de l'amende à la hausse ou à la baisse. […]

27. Enfin, le montant de l'amende proposée doit être suffisamment élevé pour atteindre les objectifs poursuivis, mais en vertu du principe de proportionnalité, ledit montant ne devrait toutefois pas dépasser ce qui est nécessaire pour atteindre ces objectifs. Pour apprécier la proportionnalité du montant de l'amende, l'IBPT tiendra compte de la taille du contrevenant et de sa capacité financière. »

117. L'ampleur de la réduction est justifiée, étant donné qu'il s'agit de la première fois qu'une procédure d'infraction est initiée pour un tel incident. L'IBPT souhaite par ce biais envoyer un signal clair aux opérateurs tels que Telenet concernant de telles violations qui peuvent également faire l'objet d'une procédure d'infraction à l'avenir. D'autre part, l'IBPT estime que l'amende peut être réduite de manière significative car il est supposé que cela conduira en principe à une réaction appropriée au non-respect de cette obligation et aura également un effet suffisamment dissuasif concernant d'autres infractions. L'IBPT se réserve le droit de rendre la détermination de l'amende plus stricte si cela devait s'avérer nécessaire.

118. L'amende finalement imposée est donc très loin du maximum légal autorisé par l'article 21 de la loi sur le statut de l'IBPT. Les considérations qui précèdent permettent de conclure que l'amende infligée dans les circonstances actuelles est toutefois proportionnée par rapport à l'objectif déclaré de l'amende, à savoir susciter une réaction appropriée à l'infraction et avoir un effet dissuasif à l'avenir.

7. Décision

119. L'IBPT :

119.1. déclare que Telenet a enfreint l'article 107/2, § 1er, de la loi du 13 juin 2005 relative aux communications électroniques ;

119.2. somme Telenet de prendre des mesures adéquates et proportionnées de nature technique et organisationnelle telles que visées à l'article 107/2, § 1er, de la loi télécoms afin de sécuriser l'accès physique à son site de [confidentiel], notamment les mesures visées au point 64 ;

119.3. somme Telenet de lui communiquer dans les 15 jours suivant la présente décision le calendrier des travaux de reconstruction du site de [confidentiel], en incluant des détails sur les travaux et délais prévus ;

119.4. impose à cet égard à Telenet une amende administrative de 190 000 euros. Cette amende est reversée au Trésor public.

Voies de recours

Conformément à l'article 2, § 1er, 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 des marchés, Place Poelaert 1, B-1000 Bruxelles. Les recours sont formés, à peine d'irrecevabilité prononcée d'office, par requête signée, à laquelle est jointe la décision attaquée, 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.

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 des 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.

Axel Desmedt
Membre du Conseil

Bernardo Herman
Membre du Conseil

Luc Vanfleteren
Membre du Conseil

Michel Van Bellinghen
Président du Conseil