Autorité de protection des données
Gegevensbeschermingsautoriteit

**Autorisation (délivrée) n° 001/2024 du 6 novembre 2024**

**Objet: demande d'autorisation visée à *l'article 15, § 2, al. 2, de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges*** (AH-2024-0010)

Le Service d'Autorisation et d'Avis de l'Autorité de protection des données (ci-après « l'Autorité »),

Présent.e.s : Mesdames Juline Deschuyteneer, Nathalie Ragheno et Griet Verhenneman et Messieurs Bart Preneel et Gert Vermeulen ;

Vu la loi du 3 décembre 2017 *portant création de l'Autorité de protection des données,* (ci-après « LCA ») ;

Vu l'article 15 de la loi du 17 janvier 2003 *relative au statut du régulateur des secteurs des postes et des télécommunications belges* (ci-après « LIBPT ») ;

Vu la loi du 13 juin 2005 *relative aux communications électroniques* (ci-après « LCE ») ;

Vu l'article 25, alinéa 3, de la LCA selon lequel les décisions du Centre de Connaissances sont adoptées à la majorité des voix ;

Vu le règlement (UE) 2016/679 *du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE* (ci-après « RGPD »);

Vu la loi du 30 juillet 2018 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel* (ci-après « LTD »);

Vu les articles 43, 54 et 55 du Règlement d'Ordre Intérieur de l'Autorité de Protection des Données ;

Vu la demande d'autorisation des Président et Membre du Conseil de l'Institut belge des services postaux et des télécommunications, Messieurs Michel Van Bellighen et Axel Desmedt (ci-après « le demandeur »), reçue le 17 janvier 2024 ;

Vu les demandes d'informations complémentaires adressées à l'Institut belge des services postaux et des télécommunications, le 19/04/2024, le 26/04/2024 et le 17/05/2024 ;

Vu les réponses communiquées par celui-ci, le 23/04/2024, le 06/05/2025 et le 08/05/2024 ;

Vu la décision prise lors de la séance du Centres de Connaissances du 6 juin 2024 de traiter le dossier au terme d'une procédure écrite, après prise en compte des dernières réponses que doit communiquer l'Institut belge des services postaux et des télécommunications ;

Vu les réponses communiquées par ce dernier le 20/09/2024 ;

Vu la demande d'informations complémentaires adressées à l'Institut belge des services postaux et de télécommunications le 30/09/2024 ;

Vu les réponses communiquées par celui-ci le 3/10/2024, et la demande d'informations complémentaires adressées à celui-ci le 11/10/2024 ;

Vu la réponse communiquée par l'Institut belge des services postaux et de télécommunications le 16/10/2024 ;

Prend, le 6 novembre 2024, la décision suivante :

## I. Objet et contexte de la demande d'autorisation

1. Le demandeur a introduit auprès de l'Autorité une demande d'autorisation visée à l'article 15, § 2, al. 2, de la LIBPT (ci-après, « **la Demande** »). Cette disposition prévoit une compétence spécifique dans le cadre de laquelle l'Autorité est amenée à autoriser (ou pas) l'accès de l'Institut belge des services postaux et des télécommunications (ci-après, « **l'Institut** ») à des métadonnées de communications électroniques traitées par les opérateurs. Elle prévoit ce qui suit :

> « […] *§ 2. Lorsque c'est nécessaire pour permettre à l'Institut d'accomplir l'une de ses missions d'application et de contrôle des dispositions énumérées à l'article 14, § 1er, 3°, a) et g) à i), l'Institut peut exiger, par demande écrite et motivée, d'un opérateur de répondre à une demande de métadonnées. L'Institut fixe le délai de communication des données*

*demandées.*

*Sauf en cas d'urgence dûment justifiée et sauf lorsque des métadonnées anonymes sont demandées à l'opérateur, l'Institut ne peut adresser la demande à l'opérateur qu'après avoir soumis une demande écrite et motivée à l'Autorité de protection des données et après avoir obtenu l'autorisation écrite de cette dernière.*

*En cas d'urgence dûment justifiée, l'Institut communique à l'Autorité de protection des données, sans délai après l'envoi de la demande à l'opérateur, une copie de cette demande, la motivation de la demande ainsi que la justification de l'urgence. L'Autorité de protection des données effectue ultérieurement un contrôle.*

*Lorsqu'à la suite de ce contrôle ultérieur, l'Autorité de protection des données refuse de confirmer la validité de la demande envoyée par l'Institut à l'opérateur, l'Institut le notifie sans délai à l'opérateur concerné et supprime les métadonnées reçues.*

*Pour l'application du présent paragraphe, l'Institut demande à l'opérateur des métadonnées anonymisées ou pseudonymisées, sauf lorsqu'elles ne lui permettent pas de rencontrer l'objectif poursuivi.*

[…]

*§ 4. Pour l'application des paragraphes 1er à 3, la motivation de la demande adressée à l'opérateur ou à l'Autorité de protection des données doit être développée au regard des circonstances.*

*Pour l'application des paragraphes 1er et 2, l'Institut motive:*

*1° le lien entre les données demandées et la mission attribuée à l'Institut;*

*2° le caractère strictement nécessaire des données demandées dans le cadre de cette mission.*

*Pour l'application du paragraphe 2, l'Institut indique dans la demande adressée à l'Autorité de protection des données:*

*1° le motif pour lequel la communication par l'opérateur de métadonnées anonymisées ne permet pas de rencontrer l'objectif poursuivi;*

*2° le motif pour lequel la communication par l'opérateur de métadonnées pseudonymisées ne permet pas de rencontrer l'objectif poursuivi, sauf lorsque la demande précise que l'opérateur doit fournir de telles données.*

*Sont consignées dans un registre tenu auprès de l'Institut:*

*1° les demandes adressées aux opérateurs et à l'Autorité de protection des données;*

*2° la motivation de la demande et la justification de l'urgence communiquées à l'Autorité de protection des données conformément au paragraphe 2, alinéa 3;*

*3° les autorisations données par l'Autorité de protection des données* ».

2. La demande concerne un projet de recherche que mènerait l'Institut , relatif aux risques liés aux données de signalisation dites « SS7 » (ci-après, « **le Projet** »). Le demandeur a notamment joint à

sa demande un formulaire complété de consultation préalable de l'Autorité sur projet de traitement à haut risque individuel (ci-après, « **la Consultation Préalable** »), un projet de décision du Conseil de l'IBPT (ci-après, « **le Projet de Décision** ») ainsi qu'une analyse d'impact relative à la protection des données pour le projet DAP20/01 (ci-après, « **l'Analyse d'Impact** »).

3. L'Autorité a également demandé au demandeur de lui communiquer les avis des délégués à la protection des données (ci-après, « DPO ») évoqués dans les documents communiqués. Quant à ceux-ci toutefois, celui-ci a précisé que les DPO « *ont marqué leur accord de façon informelle et à titre préliminaire sur base des textes provisoires. Après obtention de la décision de votre Autorité, le projet de décision de l'IBPT, l'analyse d'impact et le projet de convention de sous-traitance avec l'ERM seront finalisés et un avis formel des deux DPO's sera demandé* ». L'Autorité en prend acte mais considère cependant que conformément aux articles 24, 1., et 38, 1., du RGPD, les DPO concernés doivent être consultés **et leurs avis doivent être documentés avant l'introduction d'une demande d'autorisation auprès de l'Autorité**.

4. En synthèse quant au traitement envisagé, l'Institut entend charger l'Ecole Royale Militaire (ci-après, « **ERM** ») de la réalisation d'une recherche sur la base de métadonnées de communications électroniques réelles, collectées auprès d'opérateurs belges, afin d'identifier des failles et vulnérabilités du protocole SS7 ainsi que de créer une méthode de détection de celles-ci.

5. A titre préliminaire, l'Autorité rappelle les **réserves sérieuses** qu'elle a déjà émises quant à l'attribution à celle-ci d'une compétence d'autorisation dans le domaine du traitement des données de communications électroniques[1]. En outre, le **contrôle non exhaustif** de l'Autorité est exclusivement fondé sur les documents précités ainsi que les réponses communiquées par le demandeur aux demandes qui lui ont été adressées. Il **ne consiste pas en une évaluation de la conformité du traitement de données envisagées au RGPD et aux dispositions de droit belge applicables au traitement de données à caractère personnel**. Autrement dit, la délivrance d'une autorisation ne peut être interprétée comme une garantie de conformité à l'ensemble de ces règles.

[1] Voir les considérants nos 68 et s. de l'avis n° 32/2022 du 16 février 2022 *concernant les articles 7, 25, 1° et 47 du projet de loi portant dispositions diverses en matière d'Economie (CO-A-2021-280, CO-A-2021-281 et CO-A-2021-283)*. Voir également les considérants nos 59 et s. de l'annexe à l'avis du Comité de direction de l'APD du 25 février 2022 *concernant un avant-projet de loi modifiant la loi du 3 décembre 2017 portant création de l'Autorité de protection des données (AH-2022-0020)*, disponible sur
https://www.autoriteprotectiondonnees.be/publications/avis-concernant-un-avant-projet-de-loi-modifiant-la-loi-du-3-decembre-2017-portant-creation-de-lautorite-de-protection-des-donnees.pdf, dernièrement consulté le 17/01/2024.

## II. Examen

La présente décision est structurée comme suit :

## II.1. Finalité et fondement juridique du traitement

### II.1.1. Fixation des éléments essentiels du traitement par la loi et standard d'évaluation

6. « *L'Autorité rappelle que toute ingérence dans le droit au respect de la protection des données à caractère personnel, en particulier lorsque l'ingérence s'avère importante comme c'est le cas en l'espèce, n'est admissible que* ***si elle encadrée par une norme suffisamment claire et précise et dont l'application est prévisible pour les personnes concernées.*** *Ainsi, toute norme encadrant des traitements de données à caractère personnel, en particulier lorsque ceux-ci constituent une ingérence importante dans les droits et libertés des personnes concernées, doit répondre* ***aux exigences de prévisibilité et de précision*** *de sorte qu'à sa lecture,* ***les personnes concernées, puissent entrevoir clairement les traitements qui sont faits de leurs données et les circonstances dans lesquelles un traitement de données est autorisé****. En exécution de l'article 6.3 du RGPD, lu en combinaison avec les articles 22 de la Constitution et 8 de la Convention européenne des droits de l'homme et des libertés fondamentales, les* ***éléments essentiels du traitement*** *doivent y être* ***décrits avec précision****. Il s'agit, en particulier, de la ou des* ***finalité(s)*** *précise(s) du traitement ; de* ***l'identité du (ou des) responsable(s) du traitement*** *; des* ***catégories de données traitées****, étant entendu que celles-ci doivent s'avérer – conformément à l'article 5.1. du RGPD, « adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées » ; des* ***catégories de personnes concernées*** *(personnes à propos desquelles des données seront traitées) ; de la* ***durée de conservation des données*** *; des destinataires ou* ***catégories de destinataires*** *auxquels leurs données sont communiquées et les* ***circonstances dans lesquelles et les raisons pour lesquelles elles seront communiquées*** *ainsi que* ***toutes mesures visant à assurer un traitement licite et loyal de ces données à caractère personnel*** » (mise en gras dans le texte original)[2].

7. A cet égard, l'article 54, § 3, du Règlement d'Ordre Intérieur de l'Autorité rappelle ce qui suit :

> « *Conformément aux principes de prévisibilité et de légalité notamment consacrés dans l'article 22 de la Constitution, l'Autorité ne peut se substituer au législateur et déterminer les éléments essentiels des traitements de données à caractère personnel dont l'autorisation est sollicitée.*

[2] Avis de l'Autorité n° 108/2021 du 28 juin 2021, *concernant un avant-projet de loi relatif à la collecte et à la conservation des données d'identification, de trafic et de localisation dans le secteur des communications électroniques et à leur accès par les autorités et un projet d'arrêté royal modifiant l'arrêté royal du 19 septembre 2013 portant exécution de l'article 126 de la loi du 13 juin 2005 relative aux communications électroniques (CO-A-2021-099)*, considérant n° 27.

Voir également les considérants nos 58 et s. de l'avis n° 32/2022 du 16 février 2022 *concernant les articles 7, 25, 1° et 47 du projet de loi portant dispositions diverses en matière d'Economie (CO-A-2021-280, CO-A-2021-281 et CO-A-2021-283)*.

*Dans le cadre de sa compétence d'autorisation visée aux paragraphes 1er et 2, et sur base des informations communiquées par le demandeur, le cas échéant, à la suite d'une demande d'informations complémentaires du Service, le Service vérifie que les éléments du traitement de données sollicité reposent sur et sont conformes à la (ou aux) disposition(s) normatives de rang législatif qui les identifie(nt).*

*Le Service vérifie également, dans la mesure du possible et sur la même base, si les modalités du projet de traitement soumis à autorisation sont conformes aux principes de nécessité et de proportionnalité en matière de protection du droit au respect la vie privée et du droit à la protection des données à caractère personnel* ».

### II.1.2. Finalité du traitement

8. Dans la Consultation Préalable, l'Institut précise que le traitement de données envisagé est un traitement ultérieur de données consistant en une « *réutilisation à des fins de* ***recherche scientifique*** » (mis en gras par l'Autorité). La Demande se réfère à « …***een onderzoek uit te voeren*** *om de* ***risico's*** *die verbonden zijn aan de signalisatiegegevens (de zogenaamde 'SS7') van de openbare elektronische-communicatienetwerken te kunnen opsporen, observeren en analyseren* » (mis en gras par l'Autorité). L'objectif poursuivi renseigné dans celle-ci est d'identifier les « ***echte anomalieën en echte kwetsbaarheden*** » (mis en gras par l'Autorité). La Consultation Préalable se réfère à « *détecter, observer et analyser les* ***risques et vulnérabilités*** *liés à ces données* » (soit les « *données de signalisation (dites 'SS7')* ») (mis en gras par l'Autorité) ; il s'agit de lancer des « *programmes de détection d'anomalie* ».

9. L'Analyse d'Impact précise que le Projet « *a pour objectif de trouver des* ***méthodes de détection d'anomalies sur les réseaux SS7 et d'étudier leur vulnérabilité*** » (mis en gras par l'Autorité). Elle explique ce qui suit : « *Il n'y a pas de type de message MAP qui peut être considéré en tant que tel comme* ***suspect****. En revanche, le cumul d'un ensemble de paramètres de message peut révéler une* ***anomalie****. Il sera donc nécessaire d'établir les liens entre les messages (par exemple grâce aux valeurs IMSI, MSISDN ou GT) pour reconstituer des séquences dont il faudra rechercher le* ***caractère suspect*** » (mis en gras par l'Autorité). Concrètement, l'Analyse d'Impact évoque l'hypothèse de la « *fraude à la signalisation* ». Et elle se réfère même à des « *anomalies* ***encore inconnues*** », ainsi qu'au développement de solutions visant à détecter « *des* ***événements suspects*** » (mis en gras par l'Autorité). Indirectement, elle mentionne, dans le cadre de l'analyse des menaces liées au Projet, les hypothèses d' « ***écoute d'appel,*** [de] ***fraude à la facturation*** *et* **[d]** ***'interception de SMS*** » (mis en gras par l'Autorité).

10. **Globalement au titre de la finalité, l'Analyse d'Impact énonce ce qui suit** :

> « *Le but du traitement est de détecter des* ***anomalies*** *et les* ***vulnérabilités*** *des réseaux belges mobiles SS7. Ceci requiert des données réelles qui ne peuvent être obtenues que par les opérateurs télécom belges. Les finalités du traitement sont donc déterminées et explicites.*
>
> ***La recherche*** *a pour finalité une meilleure connaissance des* ***failles*** *des réseaux, ce qui est* ***profitable aux opérateurs, aux utilisateurs et aux services de renseignement et de sécurité****. Il s'agit donc de finalités légitimes tant pour les opérateurs que pour l'IBPT et pour le centre de recherche de l'ERM* » (souligné par l'Autorité).

11. Bien que le Projet ne définisse pas précisément et exhaustivement le type de vulnérabilités qu'il entend détecter via la recherche envisagée (ainsi, des vulnérabilités existantes pourront être recherchées tout comme de nouvelles vulnérabilités), **l'Autorité considère que la finalité poursuivie est suffisamment déterminée et explicite**[3]. En effet, compte-tenu de la diversité de la fraude dans le contexte des communications électroniques, l'Autorité concède qu'une certaine souplesse soit nécessaire en la matière afin de garantir l'efficacité de la recherche envisagée.

12. La finalité poursuivie est par ailleurs **légitime** et l'Autorité souligne au passage qu'il est utile et nécessaire de voir si les faiblesses connues du SS7 sont exploitées et s'il y a de nouvelles faiblesses ou attaques qui ne sont pas encore connues. **Même s'il serait évidemment préférable de remplacer complètement le SS7 (un système datant des années 1970 et intrinsèquement très peu sûr)**, dès lors que les faiblesses du SS7 peuvent permettre de lire les messages SMS, d'écouter les messages vocaux et d'intercepter les appels téléphoniques.

13. S'agissant de l'objectif de **recherche scientifique**, dans la **Consultation Préalable**[4], l'Institut précise cependant que l'opérateur utilise un sel qui lui est propre « *pour permettre à chaque opérateur individuellement* ***d'identifier un identifiant pseudonymisé relevé par la recherche, et nécessitant une intervention par un opérateur*** » (mis en gras par l'Autorité). Cette approche contredit celle présentée dans l'Analyse d'Impact. En effet, telle que présentée dans la Consultation Préalable, l'étude envisagée apparaît pouvoir conduire à des **interventions opérationnelles** concrètes au niveau des opérateurs, au-delà de la simple recherche scientifique.

14. Interrogé à ce sujet, le demandeur a répondu ce qui suit :

> « *Comme indiqué à titre préliminaire,* ***il convient de prendre en compte la dernière version de l'analyse d'impact****, telle que fournie en annexe de notre courrier du 30*

[3] Voir néanmoins la note de bas de page n° 15.

[4] Qui sur ce point, n'apparaît pas cohérente avec l'Analyse d'Impact.

*novembre 2023. Après concertation avec les opérateurs, l'IBPT a décidé de supprimer cette faculté pour les opérateurs. Il n'y aura donc* ***pas de retour d'information immédiate, ni d'impact opérationnel concret auprès des opérateurs sur la base des cas concrets d'anomalies détectés dans le cadre de la recherche*** » (mis en gras par l'Autorité).

15. L'Autorité prend acte de cette réponse : **l'étude n'aura pas d'impact sur des cas concrets impliquant des personnes concernées**. Cela étant précisé, il va de soi que l'étude pourra avoir un impact opérationnel et stratégique **général** au niveau des opérateurs, l'objectif global étant d'améliorer la sécurité dans le contexte du protocole SS7.

### II.1.3. Mission d'intérêt public de l'Institut fondant le traitement

16. Dans sa Demande, le demandeur se réfère de manière générale aux articles 107/2 à 107/4 de la LCE. Sur « *le lien entre les données demandées et la mission attribuée à l'Institut* »[5], l'Institut précise ce qui suit : « *In dit geval, en zoals hierboven aangegeven, zullen de gevraagde gegevens het BIPT in staat stellen de kennis en het begrip van de risico's in verband met de signalisatiegegevens te verbeteren door de geplande studie samen met de KMS tot een goed einde te brengen* ». L'Analyse d'Impact se rattache de manière générale à la « *mission générale de surveillance et de contrôle du respect des obligations des opérateurs en matière de sécurité des réseaux* », et renvoie aux articles 107/2, 107/3 et 107/4, de la LCE, comme le Projet de Décision.

17. C'est **dans sa Consultation Préalable que l'Institut se réfère explicitement à la mission d'intérêt public** (article 6, 1., e), du RGPD) **consacrée dans l'article 107/4, § 4, de la LCE**, rédigé comme suit :

> « *L'Institut* ***coordonne*** *les initiatives relatives à la sécurité des réseaux publics de communications électroniques et des services de communications électroniques accessibles au public.*
>
> ***Il supervise*** *la détection, l'observation et l'analyse des problèmes de sécurité, et peut fournir aux utilisateurs des informations en la matière* » (mis en gras par l'Autorité).

18. D'après son exposé des motifs dans sa dernière version[6], cette disposition reprend l'ancien article 114/2 de la LCE et constitue la transposition de l'article 41 du Code des communications électroniques européen[7]. Le § 4 invoqué provient toutefois de l'ancien article 113/1 de la LCE, inséré par l'article 77

---

[5] Article 15, § 4, al. 1er, 1°, de la LIBPT.

[6] *Doc. Parl.*, Chambre des Représentants, n° 55-2256/001, commentaire des articles, p. 78.

[7] Directive (UE) n° 2018/1972 du Parlement européen et du Conseil *du 11 décembre 2018 établissant le code des communications électroniques européen (refonte)*. Cette disposition vise la mise en œuvre et l'exécution du Code en prévoyant notamment certains pouvoirs au profit des autorités nationales compétentes.

d'une loi du 10 juillet 2012 *portant des dispositions diverses en matière de communications électroniques*. Disposition qui elle-même, constitue une reprise d'un plus ancien article 113 de la LCE. Le commentaire de cet article 77 ne précise rien à son sujet[8]. Dans sa substance, cette disposition apparaît remonter au texte originel de la LCE (2005) et plus précisément, à un amendement n° 129 de M. De Coene et consorts[9], motivé sur ce point comme suit « *L'ajout relatif au rôle de coordination de l'Institut doit permettre de renforcer l'aspect proactif du traitement des problèmes de sécurité rencontrés sur internet* »[10].

19. Bien que l'Autorité perçoive que la mise en œuvre de dispositions normatives et compétences d'autorités publiques visant à garantir la sécurité de l'information dans le secteur des communications électroniques puissent requérir une certaine souplesse de mise en œuvre[11], elle considère que **l'article 107/4, § 4, de la LCE** ne répond pas aux exigences découlant des principes de prévisibilité et de légalité rappelés précédemment et **ne peut fonder le traitement de données envisagé par l'Institut[12]**. Cette disposition à la formulation trop générale, ne permet pas d'identifier les éléments essentiels des traitements de données à caractère personnel qu'elle serait susceptible de fonder, y compris à l'aune de la consécration dans la loi, du pouvoir de l'Institut de requérir des opérateurs la communication de métadonnées de communications électroniques lorsque celles-ci sont nécessaires à l'exécution de ses missions.

20. Interrogé au sujet du fondement juridique du traitement de données envisagé, **le demandeur a rappelé que l'article 15, § 2, de la LIBT renvoyait à la LEC et a précisé en particulier ce qui suit** :

> « *Les fondements juridiques du traitement sont à trouver non seulement à l'article 107/4, § 4,* ***mais avant tout également à l'article 107/4, § 1er de la loi du 13 juin 2005*** *relative aux communications électroniques (ci-après la « loi télécom »), qui prévoit que :*
>
> *« 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.*

[8] *Doc. Parl.*, Chambre des Représentants, n° 53-2143/001, p. 70.

[9] *Doc. Parl.*, Chambre des Représentants, n° 51-1425/008, P. 16.

[10] Le rapport des discussions indique en outre ce qui suit : « *M. Philippe De Coene (sp.a-spirit) entend conférer à l'IBPT un rôle de coordination visant à permettre de renforcer l'aspect proactif du traitement des problèmes de sécurité rencontrés sur internet* », *Doc. Parl.*, Chambre des Représentants, n° 51-1425/018, p. 51.

[11] Ainsi par exemple, les données qu'il conviendra de traiter dans un cas concret lié à un incident de sécurité dépendront de la nature de cet incident de sécurité de telle sorte que celles-ci ne peuvent être listées dans une norme du rang de loi à la manière dont les données contenues dans une banque de données créée en vue de la réalisation d'une mission d'intérêt public, le sont.

[12]

*A la demande de l'Institut, un opérateur participe à un exercice relatif à la sécurité des réseaux ou services ou organise un tel exercice* » (mis en gras par l'Autorité).

21. Cela étant précisé, l'article 107/4, § 1er, al. 1er, de la LEC se réfère soit à l'hypothèse où il convient de « *remédier à un incident de sécurité* », soit à celle où il convient d'empêcher un tel incident « *lorsqu'une menace importante a été identifiée* ». L'article 107/2 de la LCE vise en substance, des obligations de l'opérateur dans le domaine de la sécurité, et l'article 107/3 vise d'une part, une obligation de notification de l'opérateur en cas de « *menace particulière et importante d'incident de sécurité* », et d'autre part, des obligations en matière de « *violation de données à caractère personnel* ».

22. Réinterrogé à ce sujet, le demandeur a plus directement évoqué l'hypothèse d'un « ***exercice*** » **relatif à la sécurité**, soit l'application de **l'article 107/4, § 1er, al. 2**, de la LCE, selon lequel « *A la demande de l'institut, un opérateur participe à un exercice relatif à la sécurité des réseaux ou services ou organise un tel exercice* ». Plus exactement, le demandeur a répondu ce qui suit aux interrogations additionnelles posées par l'Autorité :

« *À la lecture de votre commentaire, il nous semble utile de clarifier la portée de l'article 107/4.*

*Cet article, qui transpose l'article 41*[13] *du Code des communications électroniques européen (ci-après « le Code »), prévoit qu'en application des articles 107/2 à 107/4,*

---

[13] **Cette disposition** est rédigée comme suit :

« *Mise en œuvre et exécution*

*1. Les États membres veillent à ce que, pour mettre en œuvre l'article 40, les autorités compétentes aient le pouvoir de donner des instructions contraignantes, y compris concernant 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 et les dates limites de mise en œuvre, aux fournisseurs de réseaux de communications électroniques publics ou de services de communications électroniques accessibles au public.*

*2. Les États membres veillent à ce que les autorités compétentes aient le pouvoir d'imposer aux fournisseurs de réseaux de communications électroniques publics ou de services de communications électroniques accessibles au public de:*

*a) fournir les informations nécessaires pour évaluer la sécurité de leurs réseaux et services, y compris les documents relatifs à leurs politiques de sécurité; et*

*b) se soumettre à un audit de sécurité effectué par un organisme qualifié indépendant ou une autorité compétente et d'en communiquer les résultats à l'autorité compétente; le coût de l'audit est à la charge du fournisseur.*

*3. Les États membres veillent à ce que les autorités compétentes disposent de tous les pouvoirs nécessaires pour enquêter sur les cas de non-conformité ainsi que sur leurs effets sur la sécurité des réseaux et services.*

*4. Les États membres veillent à ce que, pour mettre en œuvre l'article 40, les autorités compétentes aient le pouvoir d'obtenir l'assistance d'un centre de réponse aux incidents de sécurité informatique (CSIRT) désigné en vertu de l'article 9 de la directive (UE) 2016/1148 en ce qui concerne les questions relevant des tâches des CSIRT en vertu de l'annexe I, point 2, de ladite directive.*

*5. En fonction des besoins et conformément au droit national, les autorités compétentes consultent les services répressifs nationaux compétents, les autorités compétentes au sens de l'article 8, paragraphe 1, de la directive (UE) 2016/1148 et les autorités nationales chargées de la protection des données et coopèrent avec eux* ».

**L'article 40** est rédigé comme suit :

« *Sécurité des réseaux et services*

*« 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 » (soulignement ajouté).*

*Il ne s'agit donc pas uniquement d'imposer des mesures visant à remédier à une menace ponctuelle qui se réalise (par exemple, une attaque informatique), mais bien également à **intervenir en amont de la survenance d'incidents** et à éviter que des menaces ne se réalisent et engendrent des incidents de sécurité (cf. partie soulignée).*

*Dans cet objectif, les opérateurs doivent prendre les **mesures techniques et organisationnelles** visées à l'article 107/2, en ce compris procéder aux **analyses de risques nécessaires de façon globale** et non au cas par cas (angle de vue*

---

*1. Les États membres veillent à ce que les fournisseurs de réseaux de communications électroniques publics ou de services de communications électroniques accessibles au public prennent des mesures techniques et organisationnelles adéquates et proportionnées pour gérer les risques en matière de sécurité des réseaux et des services de manière appropriée. Compte tenu des possibilités techniques les plus récentes, ces mesures garantissent un niveau de sécurité adapté au risque existant. En particulier, des mesures sont prises, y compris le chiffrement le cas échéant, pour prévenir et limiter l'impact des incidents de sécurité pour les utilisateurs et pour d'autres réseaux et services.*

*L'Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information (ENISA) facilite, conformément au règlement (UE) no 526/2013 du Parlement européen et du Conseil ( 3 ), la coordination entre les États membres afin d'éviter des exigences nationales divergentes susceptibles de créer des risques en matière de sécurité et des obstacles au marché intérieur.*

*2. Les États membres veillent à ce que les fournisseurs de réseaux de communications électroniques publics ou de services de communications électroniques accessibles au public notifient sans retard indu à l'autorité compétente tout incident de sécurité ayant eu un impact significatif sur le fonctionnement des réseaux ou des services.*

*Afin de déterminer l'ampleur de l'impact d'un incident de sécurité, il est tenu compte en particulier des paramètres suivants, lorsqu'ils sont disponibles:*

*a) le nombre d'utilisateurs touchés par l'incident de sécurité;*

*b) la durée de l'incident de sécurité;*

*c) l'étendue géographique de la zone touchée par l'incident de sécurité;*

*d) la mesure dans laquelle le fonctionnement du réseau ou du service est affecté;*

*e) l'ampleur de l'impact sur les activités économiques et sociétales.*

*Le cas échéant, l'autorité compétente concernée informe les autorités compétentes des autres États membres et l'ENISA. L'autorité compétente concernée peut informer le public ou exiger des fournisseurs qu'ils le fassent, dès lors qu'elle constate qu'il est dans l'intérêt public de divulguer l'incident de sécurité.*

*Une fois par an, l'autorité compétente concernée soumet à la Commission et à l'ENISA un rapport succinct sur les notifications reçues et l'action engagée conformément au présent paragraphe.*

*3. Les États membres veillent à ce qu'en cas de menace particulière et importante d'incident de sécurité dans des réseaux de communications électroniques publics ou des services de communications électroniques accessibles au public, les fournisseurs de ces réseaux ou services informent leurs utilisateurs potentiellement touchés par une telle menace de toute mesure de protection ou correctrice que ces derniers peuvent prendre. Le cas échéant, les fournisseurs informent également leurs utilisateurs de la menace elle-même.*

*4. Le présent article est sans préjudice du règlement (UE) 2016/679 et de la directive 2002/58/CE.*

*5. La Commission peut, en tenant le plus grand compte de l'avis de l'ENISA, adopter des actes d'exécution détaillant les mesures techniques et organisationnelles visées au paragraphe 1, ainsi que les circonstances, le format et les procédures applicables aux exigences de notification prévues au paragraphe 2. Ils s'appuient, dans toute la mesure du possible, sur des normes européennes et internationales et n'empêchent pas les États membres d'adopter des exigences supplémentaires aux fins des objectifs énoncés au paragraphe 1.*

*Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 118, paragraphe 4* ».

*« **macro** » au niveau de l'opérateur et son organisation dans son ensemble et non uniquement au niveau « micro » de chaque incident individuel ou risque d'incident imminent et ponctuel).*

*En application de l'article 107/4, l'IBPT peut imposer aux opérateurs de **participer à un exercice visant à analyser ces risques « globaux », afin d'identifier les menaces et de prévenir la survenance d'incidents**. Tel est précisément l'objet du projet de recherche SS7 auquel il est demandé aux opérateurs de participer en tant qu'exercice relatif à la sécurité des réseaux. Cette mesure a pour objectif de faire progresser les connaissances concernant les failles de sécurité du protocole de signalisation « SS7 » (analyser les risques et identifier les menaces au niveau global) afin de leur permettre d'acquérir les outils nécessaires afin de prévenir les incidents de sécurité potentiels*[14].

*La compétence confiée à l'IBPT en cette matière est donc volontairement formulée de façon large, dès lors que de multiples mesures peuvent s'avérer nécessaires afin d'atteindre cet objectif d'analyse des risques et de mise en œuvre des mesures techniques et organisationnelles adéquates et proportionnées, compte tenu des possibilités techniques les plus récentes, afin de garantir un niveau de sécurité adapté au risque existant.*

*Par analogie, votre Autorité est également chargée d'examiner les mesures techniques et organisationnelles prises en matière de protection des données à caractère personnel. La liste de ces mesures n'est pas davantage exhaustive et votre Autorité dispose également d'une marge d'appréciation quant au caractère adéquat de ces mesures (cf. votre point 8).*

*À titre d'illustration, quelques cas concrets dans lesquels le protocole SS7 peut constituer une faille de sécurité :*

- *Signaling Interception: Het monitoren van SS7-metadata kan ongeautoriseerde toegang of onderscheppingspogingen detecteren. Wanneer eindgebruikers contact opnemen met elkaar via SMS of een oproep via het 2G-netwerk, dan worden de eindgebruikers verbonden via het SS7-protocol. Kwaadwillige organisaties kunnen via kwetsbaarheden in dit protocol toegang krijgen tot de uitgewisselde gegevens tussen deze eindgebruikers, zoals onder andere de*

[14] Voir la note de bas de page n° 15.

*locatiegegevens die worden uitgewisseld, identifiers van de gebruikte toestellen, tot zelfs de inhoud van de uitgewisselde communicatie.*

- *Specifieke smishing-aanvallen: aangezien uitgewisselde gegevens tussen eindgebruikers onderschept kunnen worden, kunnen aanvallers op basis van deze informatie geloofwaardigere smishing-aanvallen uitvoeren, met als doel fraude te plegen.*
- *SIM-swapping: wanneer kwaadwillige actoren toegang kunnen krijgen tot de SS7-gegevens van een eindgebruiker, en daarmee bijvoorbeeld de tweefactor-authenticatie van de gebruiker onderscheppen of de nodige oproepen/SMS'en door te sturen naar hun eigen telefoon, kunnen ze op basis daarvan fraude plegen omdat ze in het bezit zijn van de nodige authenticatiecodes.*

*ENISA heeft over de veiligheid in en van signalisatie in 2018 een assessment gepubliceerd, waaraan het BIPT heeft meegewerkt: Signalling Security in Telecom SS7/Diameter/5G — ENISA (europa.eu)* [15]

***En conclusion :***

1) *L'article 107/4 ne vise pas uniquement à remédier à des incidents de sécurité ponctuels, mais a une portée bien plus large ;*
2) *La finalité spécifique visée par le projet de recherche SS7, à savoir rechercher des failles de sécurité et créer des mécanismes de détection à partir de métadonnées entre dans le cadre plus large des compétences de l'IBPT en application des articles 107/2 à 107/4 de la loi télécom ;*
3) *L'article 15, § 2, de la loi statut IBPT autorise l'IBPT à demander aux opérateurs des métadonnées pour les besoins du contrôle et de l'application de la loi télécom ; raison pour laquelle la présente demande de contrôle préalable vous est soumise* » (soulignement et mise en gras **dans le texte original**).

23. L'Autorité prend acte de ces explications. Elle relève premièrement que la LCE **ne définit pas le niveau de participation des opérateurs à l' « exercice » envisagé qui sera réalisé par l'ERM**. Dans ce cadre, l'Autorité considère **que leur participation peut se limiter à devoir collecter et communiquer les métadonnées de communication électroniques concernées**.

[15] L'Autorité observe qu'à la p. 18 de cette étude, il est indiqué ce qui suit :

« *SS7 related vulnerabilities have been analysed extensively by the industry. In recent years, many pages were written and many talks have taken place regarding the issue. As a result, at this point, we have a good coverage of the topic, public and industry awareness levels are high, as strong industry associations (e.g. GSMA) have tackled the problem. Solutions are available along with the necessary guidelines and documentations. The only issue remaining is the adoption/implementation of the proper measures at a larger scale* ».

24. Deuxièmement **quant à la nature du Projet**, l'Autorité observe que l'hypothèse d'un « exercice » relatif à la sécurité est susceptible de s'écarter du scénario des menaces concrètes. Dès le départ, la Consultation Préalable se référait explicitement à la réalisation d'une « ***recherche scientifique*** »[16] et l'Analyse d'Impact se réfère toujours à une « ***recherche*** »[17] et à un « ***projet de recherche*** »[18]. Plus explicitement, l'Analyse d'Impact précise encore que « *Les résultats de cette recherche seront communiqués aux opérateurs télécom, de manière à leur permettre d'améliorer la connaissance et la protection de leurs réseaux. Elle bénéficiera donc aussi aux utilisateurs de ces réseaux. En accord avec les opérateurs, les conclusions de la recherche seront également partagées avec la communauté scientifique, afin de permettre le « peer-review » et contribuer à la recherche de manière plus générale en la matière* »[19]. Elle revendique d'ailleurs en outre l'application de **l'article 89 du RGPD**, consacrant les garanties et dérogations applicables au traitement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques, et se réfère à plusieurs reprises au titre des « *Mesures protectrices des droits* », à la « ***réutilisation à des fins de recherche*** ». Le Projet de Décision lui-même, intègre explicitement et également, ces considérations. **L'Autorité considère que la recherche scientifique envisagée par l'IBPT et l'ERM peut être considérée comme un « exercice » relatif à la sécurité.**

25. Dans ces conditions en conclusion, l'Autorité est d'avis **que la recherche relative aux vulnérabilités du protocole SS7 et à leur mode de détection peut être fondée sur l'article 107/4, § 1er, al. 2**, de la LCE.

## II.2. Responsable(s) du traitement et sous-traitant(s)

### II.2.1. Rappel des principes

26. S'agissant de la **répartition des responsabilités** au regard du traitement des données à caractère personnel, l'Autorité réitère sa pratique d'avis constante selon laquelle une autorité publique (ou une entité privée) est en principe responsable du traitement de données nécessaire à la mise en œuvre de la mission d'intérêt public qui lui incombe (ou qui relève de l'autorité publique dont elle est investie)[20],

[16] Voir le considérant n° 8.

[17] Voir le considérant n° 10.

[18] Analyse d'Impact, p. 1.

[19] *Ibidem*.

[20] Article 6, 1., e), du RGPD.

ou nécessaire à l'obligation légale qui la lie[21], en vertu de la norme concernée[22, 23]. Cette approche est au demeurant conforme au récent arrêt de la Cour de justice (3e Ch.), du 11 janvier 2024, *Etat belge c/ Autorité de Protection des Données*, aff. C-231/22, concernant la responsabilité du Moniteur Belge.

27. Pour autant, « *l'Autorité n'exclut pas, sur le plan théorique, que le législateur puisse attribuer une* ***mission de sous-traitant*** *au sens du RGPD, à une autorité publique, à l'égard d'un traitement de données à caractère personnel. Pour autant dans ce cadre, que le législateur* ***le prévoie de manière claire et cohérente,*** *et* ***garantisse que*** *dans le cadre du traitement concerné,* ***le sous-traitant soit tenu d'agir conformément aux instructions*****[…]** *des autorités publiques recourant à ses services*[…]*. L'Autorité rappelle que selon le RGPD, le sous-traitant agit pour le compte du responsable du traitement, ne traite les données que sur instruction documentée du responsable du traitement et ne peut pas déterminer les finalités et les moyens du traitement*[…]*.* ***Les faits et le cadre normatif doivent refléter cette réalité****.* ***Et encore conviendra-t-il en fait, que le responsable du traitement ait le choix*** *de recourir ou pas au sous-traitant concerné* »[24] (mise en gras et soulignement dans le texte initial).

### II.2.2. Responsabilités de l'IBPT et des opérateurs

[21] Article 6, 1., c), du RGPD.

[22] Pour une application récente, mettant notamment en évidence la motivation de l'approche suivie par l'Autorité, voir l'avis n° 163/2023 du 18 décembre 2023 *concernant un avant-projet de loi portant statut social du magistrat (CO-A-2023-465)*, considérants nos 56-67.

Voir par ailleurs notamment : avis n° 143/2023 du 29 septembre 2023 *concernant un avant-projet de décret portant assentiment à l'accord de coopération entre la Région wallonne et la Communauté française désignant l'intégrateur de services de la Région wallonne et de la Communauté française et un projet d'accord de coopération relatif à la création du service commun aux Gouvernements Wallon et de la Communauté française, dénommé Banque Carrefour d'échange de données (non soumis à assentiment) (CO-A-2023-375), et concernant un avant-projet de décret portant assentiment à l'accord de coopération entre la Région wallonne et la Communauté française désignant l'intégrateur de services de la Région wallonne et de la Communauté française et un projet d'accord de coopération relatif à la création du service commun aux Gouvernements Wallon et de la Communauté française, dénommé Banque Carrefour d'échange de données (non soumis à assentiment) (CO-A-2023-376)* considérants nos 7 et s. ; avis de l'Autorité n° 83/2023 du 27 avril 2023 *concernant un avant-projet d'ordonnance modifiant l'ordonnance du 4 avril 2019 portant sur la plate-forme d'échange électronique des données de santé (CO-A-2023-147)*, considérant n° 11 ; avis n° 129/2022 du 1er juillet 2022 *concernant les articles 2 et 7 à 47 d'un projet de loi portant des dispositions diverses en matière d'Economie*, considérants nos 42 et s. ; l'avis n° 227/2022 du 29 septembre 2022 *concernant un avant-projet de décret relatif aux données ouvertes et à la réutilisation des informations du secteur public (CO-A-2022-209)*, considérants nos 17-23 ; avis n° 131/2022 du 1er juillet 2022 *concernant un projet de loi portant création de la Commission du travail des arts et améliorant la protection sociale des travailleurs des arts*, considérants nos 55 et s. ; l'avis n° 112/2022 du 3 juin 2022 *concernant un projet de loi modifiant le Code pénal social en vue de la mise en place de la plateforme eDossier*, considérants nos 3-41 et 87-88 ; avis n° 231/2021 du 3 décembre 2021 *concernant un avant-projet d'ordonnance concernant l'interopérabilité des systèmes de télépéage routier*, considérants nos 35-37 ; l'avis n° 37/2022 du 16 février 2022 *concernant un avant-projet de décret instituant la plateforme informatisée centralisée d'échange de données 'E-Paysage'*, considérant n° 22 ; l'avis n° 13/2022 du 21 janvier 2022 *concernant un projet d'arrêté du Gouvernement de la Région de Bruxelles-Capitale relatif à l'octroi de primes à l'amélioration de l'habitat et un projet d'arrêté du Gouvernement de la Région de Bruxelles-Capitale modifiant l'arrêté du Gouvernement de la Région de Bruxelles-Capitale du 9 février 2012 relatif à l'octroi d'aides financières en matière d'énergie*, considérants nos 9-17.

[23] Avis n° 154/2023 du 20 octobre 2023 *concernant un avant-projet de décret et ordonnance conjoints portant le code bruxellois de la gouvernance et de la donnée (CO-A-2023-407)*, considérant n° 167. Plus récemment, voir également l'avis n° 24/2024 du 18 mars 2024 *concernant un avant-projet de loi modifiant la loi relative à la création et à l'organisation d'un intégrateur de services fédéral* (CO-A-2023-554).

[24] Avis n° 163/2023 du 18 décembre 2023 *concernant un avant-projet de loi portant statut social du magistrat (CO-A-2023-465)*, considérants nos 62 et 67.

28. L'Autorité considère par conséquent qu'en principe et à tout le moins, **l'Institut est responsable** des traitements de données nécessaires à la réalisation de ses missions d'intérêt public.

29. Les **opérateurs** quant à eux, tenus de communiquer les informations à l'Institut **en exécution de l'article 15, § 2, de la LIBPT**, sont **responsables des traitements de collecte** des métadonnées de leurs réseaux ainsi que de **communication de celles-ci à l'Institut**, s'agissant d'une obligation légale leur incombant.

30. Pour le reste, et notamment concernant la responsabilité au regard de l'anonymisation ou de la pseudonymisation des données, des développements additionnels s'imposent.

### II.2.3. <u>Responsabilité de l'ERM</u>

31. A titre préliminaire, l'Autorité rappelle que l'ERM est un établissement **militaire** d'enseignement universitaire dont les élèves **sont des militaires en service actif**[25]. S'agissant du rôle joué par l'ERM, l'Analyse d'Impact indique que « *L'Ecole Royale Militaire (ERM)* ***est également chargée par la Défense*** *du projet de recherche « Security issues related to SS7 (and Diameter) 1* [(1. *Le volet 'Diameter' n'est pas concerné par le traitement de données SS7 des opérateurs*)] » *(DAP20/01)*[26]*, ci-après 'le projet', qui a pour objectif de trouver des méthodes de détection d'anomalies sur les réseaux SS7 et d'étudier leur vulnérabilité* » (mis en gras par l'Autorité). En outre, personne au sein de l'Institut n'est supposé avoir accès aux données traitées qui ne sont en principe accessibles que par les deux personnes qui ont accès aux données, à savoir le **chercheur en charge de l'étude et son directeur**, de l'unité de recherche Cylab de l'ERM[27].

32. Dans l'Analyse d'Impact et le Projet de Décision, l'Institut se considère responsable du traitement au motif qui suit : « *L'IBPT est responsable du traitement au sens du* [RGPD], ***puisqu'il détermine les finalités et les moyens du traitement de données à caractère personnel (données de signalisation SS7 provenant des opérateurs)*** » (mis en gras par l'Autorité). Sur le rôle de l'ERM, l'Analyse d'Impact poursuit « *En sa qualité de sous-traitant au sens du RGPD,* ***l'ERM réalise le traitement*** *de données* ***pour le compte de l'IBPT et lui prête assistance notamment quant aux mesures de sécurité à appliquer*** *à ces données, conformément au contrat de sous-traitance conclu entre l'IBPT et l'ERM* » (mis en gras par l'Autorité).

---

[25] Voir notamment https://www.rma.ac.be/fr/a-propos-de-lerm, dernièrement consulté le 28/05/2024 ; article 2, al. 1er, de la loi du 18 mars 1838 *organique de l'école militaire*.

[26] Référence utilisée également par l'Institut, « *Analyse d'impact relative à la protection des données pour le projet DAP20/01* ».

[27] L'Analyse d'Impact précise ce qui suit quant à l'Institut : « *Aucun membre du personnel de l'IBPT n'aura accès aux données, puisque celles-ci seront directement transmises des opérateurs vers l'ERM, sans transiter (même brièvement) par l'IBPT* ».

33. Dans ces conditions, l'Autorité s'est interrogée quant à la question de savoir si l'ERM ne jouerait pas un rôle de responsable conjoint du traitement, et a **consulté l'Institut notamment quant à la genèse du Projet**. Entre autres, la recherche est-elle initiée par l'Institut dans le cadre de sa mission d'intérêt public ou celle-ci l'est-elle par la Défense dans le cadre de ses propres missions d'intérêt public ?

34. Interrogé quant à sa position en la matière, le demandeur a répondu ce qui suit :

> « *Le présent projet « Projet SS7 »* ***résulte d'un constat commun de l'IBPT et de la Défense*** *selon lequel le protocole de signalisation dénommé « SS7 », qui est utilisé à grande échelle par les opérateurs télécom, présente certaines faiblesses fondamentales rendant très difficile et coûteuse la prévention des abus.*
>
> *Comme indiqué dans l'analyse d'impact que vous citez, le projet de recherche* ***dont a également été chargé l'ERM par la Défense*** *a pour objectif de trouver des méthodes de détection d'anomalies sur les réseaux SS7 et d'étudier leur vulnérabilité. Il s'agit donc d'un* ***objectif commun avec celui poursuivi par l'IBPT****.* ***Pour mener à bien une telle recherche, il s'avère cependant nécessaire de pouvoir disposer de données de trafic réelles*** *(bien que pseudonymisées, voire anonymisées).*
>
> *Puisqu'il* ***relève des missions de l'IBPT de demander la participation des opérateurs à des exercices*** *relatifs à la sécurité des réseaux ou services de communications électroniques, il a été prévu que l'IBPT prenne la responsabilité de définir les finalités et les moyens des traitements à réaliser sur ces données de trafic issues des opérateurs. Tel est notamment l'objet du projet de décision destiné aux opérateurs et du projet de convention de sous-traitance à conclure entre l'IBPT et l'ERM.*
>
> *Nous attirons en particulier votre attention quant aux limitations suivantes prévues par le projet de convention de sous-traitance IBPT-ERM :*
>
> - *L'ERM « ne traite les données à caractère personnel que sur instruction documentée du responsable du traitement, à moins qu'il ne soit tenu d'y procéder en vertu du droit de l'Union ou du droit belge auquel il est soumis » (art. 5.1 du projet de convention en annexe ; soulignement ajouté) ;*
>
> - *L'ERM traite les données à caractère personnel uniquement pour la finalité visée à l'article 4.1., à savoir « trouver des méthodes de détection d'attaques et*

*d'anomalies sur les réseaux SS7 et étudier leur vulnérabilité » (art. 5.2 du projet de convention en annexe) ;*

- *Le traitement par l'ERM n'a lieu que pendant la durée précisée à l'article 4.1., à savoir pendant la durée du Projet SS7, lequel prend fin de 31 décembre 2024 (art. 5.3 du projet de convention en annexe).*

*En outre, les demandes seront adressées aux opérateurs par l'IBPT, qui fixera les périodes exactes sur lesquelles devront porter les données (art. 4.3 du projet de convention en annexe).*

*Enfin, à la lecture des Guidelines 07/2020 on the concepts of controller and processor in the GDPR (pp. 3-4), il nous semble que les qualifications de « responsable du traitement » et de « sous-traitant » conférés respectivement à l'IBPT d'une part, et à l'ERM d'autre part, correspondent effectivement aux responsabilités et tâches revenant in concreto à chacune de ces autorités.*

*Nous attirons en particulier votre attention quant au passage suivant : "The controller's instructions may still leave a certain degree of discretion about how to best serve the controller's interests, allowing the processor to choose the most suitable technical and organisational means." Pour le surplus, s'il est vrai que le projet de recherche de l'ERM ne peut se poursuivre sans l'intervention de l'IBPT, l'inverse n'est pas exact ; en effet,* ***l'IBPT pourrait se tourner vers un autre expert technique afin de réaliser les recherches envisagées.*** *La participation conjointe des deux autorités n'est donc pas « inextricable », comme le conçoit l'EDPB pour retenir la qualification de « responsables conjoints » au sens de l'article 26 du RGPD. Le fait que les résultats de la recherche bénéficient à chacune des autorités ne nous parait pas un élément essentiel à prendre compte, dès lors que ces résultats bénéficieront également aux opérateurs et aux utilisateurs finaux des services de téléphonie mobile* » (mise en gras et soulignement **modifiés par l'Autorité**).

35. Interrogé à deux reprises complémentaires à ce sujet ainsi que plus particulièrement, sur le **cadre normatif** (notamment, Justel ne communique pas en ligne de version intégrale et consolidée de la loi du 18 mars 1838 *organique de l'école militaire*)[28] **régissant les activités de l'ERM ainsi que sur la décision par laquelle l'ERM est également chargée de mener la recherche concernée**, le demandeur a notamment répondu ce qui suit : « […] *Nous nous permettons de rappeler que l'IBPT est une autorité indépendante et ne reçoit d'instruction ni de l'ERM, ni de la Défense. En revanche, il est prévu - sur base du projet de convention de sous-traitance qui vous a été communiqué - que l'ERM*

[28] Voir https://www.ejustice.just.fgov.be/eli/loi/1838/03/18/1838031850/justel#list-link-1, dernièrement consulté le 15/05/2024.

*puisse agir, dans le cadre de ce projet de recherche,* ***comme expert technique désigné par l'IBPT*** *(cf. article 16, alinéa 4 de la loi statut IBPT : « Le Conseil peut faire appel à une expertise extérieure dans le cadre de l'accomplissement des missions de l'Institut. Ces experts doivent être indépendants de toute personne physique ou morale soumise au contrôle de l'Institut* » […] (mis en gras par l'Autorité).

36. Il a encore notamment précisé que « *Le programme de recherche de la Défense pour l'année 2020, incluant le projet de recherche en cause en l'espèce, a été validé par une* ***décision du Ministre de la Défense*** *du* ***07/02/2020*** » (mise en gras modifiée par l'Autorité). Et que « *D'un point de vue concret, la réalisation du projet de recherche a été affectée à l'Ecole Royale Militaire (ERM) qui constitue – au même titre que l'IRSD – l'une des entités habilitées à* ***entreprendre de la recherche scientifique pour le compte de la Défense*** » (mis en gras par l'Autorité). L'Institut a encore précisé que « *En matière de recherche,* ***la Défense finance*** *un certain nombre de projets de recherche de l'ERM, tel que celui-ci, mais n'est pas le seul partenaire de l'ERM en matière de recherche scientifique* » (mis en gras par l'Autorité). Il se dégage par ailleurs clairement des éléments communiqués par l'Institut que la recherche envisagée **entre dans le cadre des missions d'intérêt public de l'ERM[29], qui agit à la demande de La Défense[30], dans le domaine de la recherche scientifique**. A ce sujet, le « *Wetenschappelijk en Technologisch onderzoeksprogramma 2020* » précise ce qui suit : « *(2) Bij Defensie* ***beoogt het wetenschappelijk onderzoek drie strategische doelstellingen****: - de ondersteuning van het academisch onderwijs in de Koninklijke Militaire School als federale universiteit; - de steun aan de operaties; - de ondersteuning aan de besluitvorming* » (mis en gras par l'Autorité).

37. Dans ces conditions, l'Autorité considère que l'ERM **peut être considéré comme un sous-traitant de l'IBPT aux conditions suivantes.**

38. **Premièrement**, l'activité de recherche qui sera menée par l'ERM dans le cadre du Projet doit s'inscrire **exclusivement dans la recherche scientifique** poursuivie par celle-ci **dans le cadre de sa mission en tant qu' institution d'enseignement universitaire**. Pour que l'ERM puisse être considérée comme sous-traitant de l'Institut, l'activité menée par celle-ci devrait nécessairement

---

[29] L'article 1er *bis*, § 1er, de la loi du 18 mars 1838 *organique de l'Ecole Royale Militaire* énonce ce qui suit : « *L'Ecole est un établissement militaire d'enseignement universitaire, chargé de la formation académique, militaire et sportive des élèves.* ***Le Roi peut charger l'Ecole de missions complémentaires qui ont un lien avec*** *la formation ou* ***la recherche scientifique*** » (mis en gras par l'Autorité). L'article 6, al. 1er, 7°, de l'arrêté royal du 26 septembre 2002 *relatif à l'organisation de l'Ecole royale militaire*, prévoit que l'ERM est chargée de « *développer des activités de recherche scientifique dans le cadre de la mission d'enseignement de l'école, notamment dans le cadre d'un programme de recherche scientifique* ».

[30] Le « *Wetenschappelijk en Technologisch onderzoeksprogramma 2020* » communiqué par l'Institut apparaît quant à lui être proposé par l'Institut royal supérieur de Défense (ci-après, « **IRSD** »), voir l'arrêté royal du 10 août 2006 *relatif à l'organisation de l'Institut royal supérieur de Défense*. Selon cet arrêté, l'IRSD dépend directement du ministre de la Défense et est dirigé par un conseil d'administration. C'est ce dernier qui approuve les programmes dans le domaine de la recherche scientifique et technologique de la Défense et les soumet au ministre pour approbation. Le conseil d'administration propose annuellement au ministre une note de politique générale, les priorités du programme de recherche de la Défense et le programme de recherche de la Défense de l'année suivante. Sur les objectifs de la recherche scientifique au sein de la défense,

s'inscrire dans les seules activités poursuivies par l'Institut dans le cadre du Projet et du droit applicable à ceux-ci (LEC et LIBPT), et non pas dans celles, distinctes, de La Défense, que ces autres missions relèvent du soutien à la décision de La Défense ou d'un appui opérationnel pour cette dernière (ces autres missions poursuivent des finalités distinctes et de surcroît incompatibles avec la finalité du Projet, déterminée par l'IBPT conformément à la LEC et à la LIBPT). Cela ne ressort *a priori* pas de l'état de fait ou de droit de la situation telle que décrite par l'Institut au travers des réponses communiquées sur ce point à l'Autorité, notamment au travers des documents transférés par l'Institut concernant la genèse de la recherche à propos du protocole SS7 au sein de La Défense. En particulier, ces documents ne permettent pas de le vérifier. Or, il **appartient à l'Institut, en tant que responsable du traitement, de vérifier, de documenter et de garantir ces différents points, conformément aux articles 5, 2., et 24, 1., du RGPD**.

39. Deuxièmement, s'il est clair que l'Institut est libre dans son choix de l'ERM comme sous-traitant, le cadre normatif applicable à l'ERM **doit permettre le plein effet de la convention de sous-traitance qui sera conclue avec l'Institut, garantissant notamment que l'ERM agira exclusivement selon les instructions de l'Institut, sans que La Défense** (par l'intermédiaire de l'un ou l'autre de ses services ou composantes) **ne puisse interférer** dans l'activité de recherche qui sera menée ou avec les métadonnées de communications électroniques qui seront traitées à cette fin (instructions, accès aux données, etc.). **Ce qu'il appartient à l'Institut, en tant que responsable du traitement, de vérifier, de documenter et de garantir, conformément aux articles 5, 2., et 24, 1., du RGPD.**

40. L'Autorité souligne enfin **qu'à défaut de pouvoir être qualifiable de sous-traitant, l'ERM ne disposerait d'aucun fondement légal** pour traiter les métadonnées de communications électroniques en question dans le cadre du Projet.

### II.2.4. Responsabilité quant à la pseudonymisation/anonymisation

41. **La responsabilité quant à la pseudonymisation/anonymisation des données ne ressort pas clairement du cadre normatif applicable qui n'est pas explicite sur ce point.** Ni la LCE ni la LIBPT ne tranchent ce point alors qu'en principe, identifier le responsable du traitement revient à fixer un élément essentiel du traitement.

42. Sur le plan des principes, comme cela a été rappelé, l'opérateur est responsable de la communication des données à l'Institut *conformément à la LIBPT* (obligation légale s'appliquant à lui). Cela étant précisé, l'Analyse d'Impact précise que « *les données seront pseudonymisées par les opérateurs participant **selon les instructions reçues de l'IBPT et de l'ERM**, avant leur communication à l'ERM* » (souligné par l'Autorité). Elle précise encore « ***l'ERM et l'IBPT seront responsables de la***

***méthode*** *de pseudonymisation choisie conformément aux règles de l'art* » ; « *Les Données SS7 traitées par les opérateurs sur une durée d'1mois seront pseudonymisées par les opérateurs au moyen de la technique de pseudonymisation* ***fournie par l'ERM*** » (souligné par l'Autorité).

43. Il se dégage clairement de ces éléments que les opérateurs n'auront par conséquent aucune marge de manœuvre dans la détermination de la méthode de pseudonymisation/anonymisation des données : cette méthode leur sera imposée **par l'Institut**. Dans ces conditions, **la responsabilité des opérateurs** au regard du traitement de pseudonymisation/anonymisation des données sera **limitée à la correcte mise en œuvre des instructions** communiquées par l'Institut. A l'aune des développements précédents et des éléments justes évoqués, **la responsabilité** au regard du traitement **liée à la méthode de pseudonymisation/anonymisation incombe quant à elle à l'Institut** (il convient de se référer sur ce point, aux développements des considérants nos 22-36, concernant la responsabilité de ces deux instances).

44. L'Autorité considère en conclusion que **les opérateurs et l'Institut sont responsables conjoints du traitement de pseudonymisation/anonymisation des données, dans les limites juste précisées** et **la documentation tenue par l'IBPT (dont le Projet de Décision) doit être adaptée en conséquence**.

## II.3. Données traitées et pseudonymisation ou anonymisation

### II.3.1. Métadonnées de communications électroniques collectées au niveau des opérateurs

45. La Consultation Préalable de l'Autorité se réfère aux *« données de signalisation (dites 'SS7')* » et précise que « *Des données MAP, SCCP, SCTP sur une durée d'1mois sont pseudonymisées chez les opérateurs* »[31] (SCCP signifie « Signalling Connection Control Part », TCAP, « Transaction Capabilities Application Part », et MAP, « Mobile Application Part »). Le point n° 5.1 du Projet de Décision se réfère également aux catégories de données traitées notamment en renvoyant à la documentation officielle de l'International Telecommunication Union (ITU)[32] et de l'European Telecommunications Standards Institute (ETSI)[33, 34].

---

[31] Sur la pseudonymisation, voir les considérants nos 51 et s.

[32] Voir ITU-T, "Series Q : Switching and Signalling, Specifications of Signalling System No. 7 – Signalling connection control part (SCCP)", disponible sur file:///C:/Users/moinjean/Downloads/T-REC-Q.711-200103-I!!PDF-E.pdf, dernièrement consulté le 27/05/2024.

[33] ETSI TS 129 002 V17.4.0 (2023-09), Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 5G; Mobile Application Part (MAP) specification (3GPP TS 29.002 version 17.4.0 Release 17), disponible sur

https://www.etsi.org/deliver/etsi_ts/129000_129099/129002/17.04.00_60/ts_129002v170400p.pdf, dernièrement consulté le 27/05/2024.

[34] « *Tot de te verstrekken SS7-Gegevens behoren de verkeersgegevens die zijn opgenomen in de parameters van de volgende protocollen van de stapel van SS7-protocollen*[…] *inclusief de tijdgebonden parameters:* [SCCP, TCAP, MAP, MTP 2 en MTP3] ».

46. L'Analyse d'Impact précise que les données seront transférées via **deux échantillons**, à partir des données **traitées par l'opérateur <u>dans le cadre de la fourniture de ses services</u>**[35]. Il s'agit d'un premier échantillon portant sur une durée d'une semaine (des données de test pour vérifier la procédure de transfert et le caractère utilisable des données), et d'un second portant sur une durée **d'un mois** (les données qui alimenteront la recherche proprement dite). L'Analyse d'Impact précise qu'une « *période de 1 mois semble raisonnable pour pouvoir disposer d'anomalies en nombre et en variété* ». La Consultation Préalable précise encore que « *Les **données de réseaux réels** sont indispensables pour offrir de vraies anomalies et de vraies vulnérabilités, permettant de tirer des conclusions de recherche correctes* » (mis en gras par l'Autorité).

47. Sur ce point, l'Autorité considère comme **qu'il est proportionné d'envisager la recherche à mener sur la base de métadonnées réelles de communications électroniques**.

48. L'Autorité **considère également qu'un échantillon d'une durée d'un mois est raisonnable**.

49. L'Analyse d'Impact explique que « *SS7 est le protocole utilisé pour la signalisation GSM (2G et 3G) et intervient par exemple dans l'identification de l'appelant, l'échange de SMS et le routage d'appels* ». La Consultation Préalable spécifie que « *Des paramètres pertinents (e.g. IMSI, GT, SSN, MAP label, temps, localisation) seront extraits des messages et stockés comme données dérivées* ». Elle précise encore, au sujet des données traitées, qu'il « *s'agit de données de trafic, qui ne relèvent pas de l'art 9 du RGPD* ». Et l'Analyse d'Impact détaille ce qui suit : « *Les données considérées concernent le trafic de signalisation SS7 et **principalement** les protocoles MAP, SCCP ou SCTP. Ces données contiennent **entre autres** le type de message MAP, les abonnés intervenant dans une requête (IMSI ou MSISDN), les équipements mobiles (numéro hardware IMEI) et les adresses d'équipement sur le réseau source et sur le réseau de destination (Global TItle GT ou Point Code PC et SubSystemNumber SSN). Le temps et **parfois** la localisation (identifiant de l'antenne courante ou coordonnées GPS) se retrouvent dans les messages MAP et sont utiles pour la recherche d'incohérences souvent révélatrices d'attaque* » (mis en gras par l'Autorité).

50. Dans une certaine mesure, l'Autorité observe que le Projet donnera également lieu à la **production de données additionnelles issues des recherches menées**. Ainsi, l'Analyse d'Impact explique ce qui suit : « *Il n'y a pas de type de message MAP qui peut être considéré en tant que tel comme suspect. En revanche, le cumul d'un ensemble de paramètres de message peut révéler une anomalie Il sera donc nécessaire **d'établir les liens entre les messages** (par exemple grâce aux valeurs IMSI,*

[35] Ce point est important dès lors qu'il n'est en conséquence **pas question de prévoir la collecte de données conservées en vertu des obligations de conservation de données consacrées dans la LCE**.

*MSISDN ou GT)* ***pour reconstituer des séquences*** *dont il faudra rechercher le caractère suspect* » (mis en gras par l'Autorité).

51. L'Analyse d'Impact précise par ailleurs que « *le LAI (Location Area Identifier – indiquant un groupe d'antennes) sera inclus dans les données transmises à l'ERM, mais pas le Cell ID (identifiant de la cellule antenne courante), qui sera quant à lui masqué* ».

52. L'Autorité a interrogé le demandeur quant aux données à caractère personnel traitées en demandant la **communication d'une liste exhaustive des données à caractère personnel traitées**. Le demandeur a répondu ce qui suit :

> « *L'énumération de données visées à l'article 5.1 est en principe exhaustive, mais il ne peut être tout à fait exclu que la nécessité apparaisse en cours de recherche de* ***pouvoir demander des données accessoires liées*** »[36] (mis en gras par l'Autorité).

53. La convention de sous-traitance communiquée par l'IBPT dans sa réponse indique encore que « *Les Données relatives au temps (date et heure) et à la localisation (« Location Area Identifier », identifiant du groupe d'antennes) traitées dans le cadre du présent projet* ***sont insuffisamment précises que pour permettre à elles seules d'en déduire des données à caractère personnel*** » (mis en gras par l'Autorité).

54. Réinterrogé à ce propos, le demandeur a communiqué les informations suivantes :

> « *Notre réponse faisait référence au point 5.1 (« Gegevens in kwestie ») du projet de décision. L'article 4.2 du projet de convention de sous-traitance entre l'IBPT et l'ERM reprend également ces mêmes données.*

---

[36] L'article 4, 2., de la convention de sous-traitance communiquée est rédigé comme suit :

« *Catégories de données à traiter (ci-après les « Données ») : il s'agit des « données de signalisation SS7 » traitées par les opérateurs dans le cadre du roaming et communiquées par les opérateurs à l'ERM à la demande de l'IBPT, à savoir les données concernant principalement les protocoles MAP, SCCP ou SCTP.*

*Ces Données contiennent en particulier le type de message MAP, les abonnés intervenant dans une requête (IMSI ou MSISDN), les équipements mobiles (numéro hardware IMEI) et les adresses d'équipement sur le réseau source et sur le réseau destination (Global Title GT ou Point Code PC et SubSystemNumber SSN).*

*Avant leur transmission à l'ERM, l'opérateur aura préalablement pseudonymisé les champs permettant d'identifier un abonné, un utilisateur ou un équipement terminal et effacé le contenu des communications, conformément à l'article 5.*

*Les Données relatives au temps (date et heure) et à la localisation (« Location Area Identifier », identifiant du groupe d'antennes) traitées dans le cadre du présent projet sont insuffisamment précises que pour permettre à elles seules d'en déduire des données à caractère personnel.*

*- Catégories de personnes concernées : les utilisateurs finaux du réseau ou du service de téléphonie mobile de l'un des opérateurs participants, qui se trouvent en situation de roaming ou apparaissent comme tels, pendant les périodes sur lesquelles portent les échantillons de Données visés à l'article 5.1.*

*- Destinataire des données :* […] ».

*Dans le passage que vous citez (n° 34 du projet de décision, sous le point 5.1 et 2ème alinéa sous « Catégorie de données » au point 4.2 du projet de convention de sous-traitance), le terme « en particulier » s'explique par le fait que ces types de données* ***peuvent être constitués de plusieurs paramètres.*** *La liste exhaustive de ces paramètres est jointe en annexe*[37].

*Par ailleurs, le n° 37 du point 5.1 du projet de décision prévoit ce qui suit : « 37.* ***Naast deze verplichte « SS7-Gegevens » kan het BIPT extra gegevens die betrekking hebben op de oefening van het KMS opvragen.***"

*L'objectif de cette disposition est de* ***réserver le droit pour l'IBPT de demander à l'opérateur concerné certaines informations complémentaires en lien avec l'exercice réalisé afin de s'assurer de l'interprétation correcte des données transmises*** *(par exemple des détails concernant le format des données ou une spécificité du réseau télécom). Il ne s'agira* ***en principe pas de*** *données à caractère personnel. Le cas échéant, si votre Autorité devait l'estimer nécessaire, une restriction à cet égard peut être insérée dans le projet de décision.*

*Pour terminer, concernant votre question relative à la localisation (« Location Area Identifier », identifiant du groupe d'antennes), il a en effet été* ***choisi de ne pas traiter de données de « Cell-ID », soit d'identifiant de la cellule de l'antenne individuelle concernée) afin de supprimer tout risque de réidentification****.*

*La donnée « Cell-ID » permet d'indiquer, avec une précision variable*[38] *en fonction de la région concernée et de la densité des antennes*[39]*, le périmètre dans lequel se trouve l'équipement terminal connecté à l'antenne. En tant que telle, cette seule donnée ne permet pas d'identifier une personne physique, mais dans certaines circonstances (par exemple, zone très peu densément peuplée avec une habitation unique isolée de tout autre lieu de présence humaine à plusieurs kms à la ronde) et recoupée avec un ensemble d'autres données (par exemple, adresse du domicile de l'utilisateur de l'équipement habitant seul à cet endroit), cette donnée pourrait attribuée à une personne physique déterminée et donc constituer une donnée à caractère personnel.*

---

[37] Cette liste a été communiquée ultérieurement.

[38] « *L'ordre de grandeur du nombre de cellules pour un opérateur national est de 30.000 cellules. La superficie de la Belgique est de +/- 30.000 km². Une cellule représente donc théoriquement 1 km². En ville, où la densité des cellules sera plus grande, cette superficie sera réduite, dans les zones moins peuplées, elle augmentera fortement* ».

[39] « *La donnée « Cell-ID » est une donnée qui est liée à l'antenne avec laquelle l'utilisateur est connecté. Dans des zones denses, la « Cell-ID » peut être spécifique jusqu'à 100 mètres. Dans des zones peu peuplées, cette donnée peut couvrir une distance de 5 kms ou plus* ».

*Encore faudrait-il, à notre sens, que :*

1) *Soit cette personne soit la seule connectée à ce même cell-ID (ce qui n'arrive en pratique jamais) ;*
2) *Soit que la personne qui tente d'effectuer cette réidentification dispose de multiples autres données permettant de distinguer cette personne des autres utilisateurs finaux connectés sur ce même Cell-ID.*

*Ce cas d'école représente néanmoins un risque qui ne nous semble pas suffisamment insignifiant que pour pouvoir être écarté.*

*À l'inverse, le degré de précision de la donnée de « Location Area Identifier » (identifiant du groupe d'antennes) équivaut en Belgique à une précision de l'ordre de la province.*

*Dans un pays aussi densément peuplé que la Belgique, cette échelle ne nous semble pas présenter le même risque que celui susvisé concernant le Cell-ID, sauf à considérer que toute donnée de localisation, aussi générale soit-elle (niveau du pays ou même du continent) doive être considérée comme une donnée à caractère personnel* » (mis en gras par l'Autorité).

55. L'Autorité prend acte de ces éléments. L'annexe de paramètres est reprise en annexe du présent avis. Sur la base de celle-ci, l'Autorité a invité l'Institut à lui communiquer l'analyse justifiant pourquoi les utilisateurs ne sont effectivement pas réidentifiables, compte-tenu des données et des techniques de pseudonymisation utilisées dans le cadre de la recherche envisagée (l'Autorité attendant sur ce point une analyse comportant une explication pour chaque paramètre, indiquant pourquoi une réidentification n'est pas réalisable sur la base des données non pseudonymisées).

56. Le demandeur a communiqué des informations complémentaires (notamment les standards pertinents de l'ITU) ainsi qu'une analyse complémentaire. L'Autorité considère néanmoins que celle-ci n'est pas entièrement satisfaisante et ce, pour les raisons suivantes.

57. Tout d'abord **premièrement**, l'analyse menée prend généralement en compte séparément les paramètres concernés, pour conclure notamment que chaque paramètre ne peut permettre la réidentification d'une personne concernée. Or une telle analyse doit prendre en considération également **les combinaisons de ces paramètres**. Additionnellement, celle-ci ne tient pas particulièrement compte du fait que les personnes concernées sont **en situation de *roaming***.

58. S'agissant par exemple, d'abonnés d'un opérateur belge se trouvant à l'étranger (ou inversement, d'abonnés d'un opérateur étranger se trouvant en *roaming* en Belgique), cela diminue automatiquement la masse des utilisateurs et communications concernés. Si pour un pays tiers, il y a

peu d'abonnés à un opérateur belge qui y effectuent (ou y reçoivent) des appels[40] pendant la période couverte, les paramètres SeizureTime et StopTime deviennent potentiellement pertinents pour isoler certaines communications téléphoniques ou via SMS[41]. MTP3 est par ailleurs présenté comme responsable du routage et comme pointant des messages vers de bons nœuds dans le réseau, ce qui laisse entendre que ces données sont également liées à une localisation[42] (même si ce lien est probablement réalisé au niveau des opérateurs). Il ne serait pas exclu en théorie, de retrouver dans ce contexte des données à caractère personnel non pseudonymisées (des données brutes). Sans pour autant bien entendu, que l'ERM ne puisse réidentifier les personnes concernées.

59. **Deuxièmement**, à ce dernier égard, l'Institut précise notamment que « *KMS beschikt immers niet over (wettige) middelen waarvan mag worden aangenomen dat zij redelijkerwijs kunnen worden ingezet om de betrokken personen met behulp van derden te heridentificeren. Met andere woorden, de verwerking is zodanig georganiseerd dat re-identificatie uitdrukkelijk is uitgesloten en ter voorkoming daarvan zijn passende technische maatregelen genomen* ». **Il limite par conséquent principalement[43] le risque d'identification au niveau de l'ERM**[44]. **Or le demandeur n'exclut ni dans ses analyses, ni dans la convention de sous-traitance qu'un traitement ultérieur des données communiquées à l'ERM pourrait être autorisé si la loi le prévoit** (voir les considérants **nos 76-80** à ce sujet). Dans ces conditions, l'Autorité considère que le demandeur **ne peut pas se limiter à analyser le risque de réidentification des personnes concernées au niveau de l'ERM**, et ne peut exclure[45] l'hypothèse dans laquelle une personne concernée pourrait être réidentifiée par une autre autorité publique qui accèderait légalement aux données traitées dans le cadre de la recherche.

60. Par conséquent, l'Institut doit d'une part, **adapter l'analyse qu'il a réalisée à l'aune des développements précédents** (prise en considération des combinaisons de paramètres et des risques de réidentification par un autre responsable du traitement que l'ERM qui pourrait accéder légalement aux données). **Et d'autre part, il doit prévoir la mise en œuvre au niveau des**

---

[40] D'après les informations complémentaires communiquées par le demandeur, le paramètre CalledNoA est un « *paramètre identique pour chaque utilisateur d'un pays donné* ».

[41] On ne se retrouverait alors pas dans la situation de risque indiquée dans l'analyse communiquées par le demandeur, à savoir que « *Vu le grand nombre de sessions qui sont initiées toutes les secondes, il n'est pas suffisant pour retrouver un utilisateur particulier* ».

[42] Voir notamment les paramètres « opc » (« *originating point code* ») et « dpc » (« *destination point code* »).

[43] L'hypothèse d'une fuite de données suite à un contournement des mesures de sécurité qui seront mises en place également à l'ERM est pour le surplus effectivement improbable.

Notamment, le demandeur précise ceci : « *De meest risicovolle handeling binnen dit onderzoek vormt de overhandiging van de gegevens van de operatoren aan de KMS en de verdere transfer van die gegevens tot de kantoren van de KMS. Hierbij is de fysieke veiligheid van de gegevens primordiaal. Wij benadrukken dat deze fysieke veiligheid wordt verzekerd door de KMS volgens de regels van de kunst* ».

[44] Ce raisonnement reflète la jurisprudence *Breyer* de la Cour de justice. Voir notamment C..J.U.E. (6e Ch.), arrêt du 7 mars 2024, *OC*, aff. C-479/22 ; C.J.U.E. (4e Ch.), arrêt du 7 mars 2024, *IAB Europe*, aff. C-604/22 ; C.J.U.E. (2e Ch.), arrêt du 19 octobre 2016, *Breyer*, aff. C-582/14.

[45] Sans préjudice des développements du considérant n° 76.

**opérateurs**, **si** cela s'avère n'nécessaire à l'aune des métadonnées de communications électroniques collectées *in concreto*, **de mesures techniques de *differential privacy*** afin d'éviter la possible réidentification des personnes concernées. **La documentation pertinente de l'Institut (dont le Projet de Décision et l'Analyse d'impact et la convention) doit être modifiée en ce sens.**

61. En outre et enfin, l'Autorité ne peut se satisfaire de l'explication selon laquelle les données complémentaires qui pourraient être demandées aux opérateurs par l'Institut ne seront « *en principe pas des données à caractère personnel* ». L'Institut doit être en mesure **d'identifier clairement précisément l'ensemble des métadonnées de communications électroniques pour lesquelles une demande d'autorisation est introduite**. Autrement dit, l'Autorité considère que la documentation pertinente soumise par l'Institut (dont le Projet de Décision et la convention de sous-traitance) **doivent être adaptés afin de détailler exhaustivement ces données et de manière telle qu'en outre, aucune autre métadonnée de communication électronique ne puisse être demandée aux opérateurs par l'Institut (ou l'ERM) durant la réalisation de la recherche envisagée**.

62. Cela étant précisé, s'il apparaissait au cours du Projet que des métadonnées supplémentaires seraient nécessaires, il appartiendrait alors à l'Institut de **soumettre une nouvelle demande d'accès à ces métadonnées à l'Autorité**.

### II.3.2. Anonymisation ou pseudonymisation des métadonnées

63. Comme cela vient d'être souligné[46], le Projet repose sur des métadonnées de communications électroniques réelles. En application du principe de proportionnalité, l'Institut envisage de recourir à des données **pseudonymisées**. L'Analyse d'Impact précise que « *les opérateurs auront préalablement pseudonymisé les champs identifiants (IMSI, MSISDN, IMEI) et effacé les contenus des communications* »[47]. L'Institut précise que les données seront pseudonymisées par les opérateurs avant d'être communiquées à l'ERM, son sous-traitant. La Demande précise que « *De gebruikte pseudonimiseringsmethode is de 'random mapping table with salt' (zout) ["(Dit is een conversietable voor getallen die is gemaakt uit een willekeurige reeks getallen. Het zout is de parameter (een getal) die bepaalt welke sequentie zal worden gekozen uit de reeks mogelijkheden)"]* ». L'Analyse d'Impact

[46] Considérants nos 46-47.

[47] **Sur les données auxquelles sera appliqué un traitement de pseudonymisation**, l'Analyse d'Impact précise qu'elle « *portera sur les numéros de téléphone (MSISDN), les numéros IMSI et IMEI.* […] *Celle-ci garantit la cohérence (l'unicité) entre identifiants permettant d'établir les liens entre messages SS7 indispensables à la détection d'anomalies.* […] *Pour l'IMSI, constitué des champs MCC, MNC et MSIN, seule la partie MSIN sera pseudonymisée en transformant les 5 derniers digits par la mapping table. Les parties pays (MCC) et réseau (MNC) ne seront pas modifiées car elles sont utiles à la recherche et ne constituent pas un risque d'identification des abonnés. Un traitement similaire sera appliqué aux MSISDN et IMEI.* […] *la random mapping table et le sel utilisés seront immédiatement supprimés par les opérateurs, de manière à réduire au maximum le risque de dé-pseudonymisation* ».

et le Projet de Décisions précisent qu'une fois les données pseudonymisées, la *random mapping table* et le sel utilisés seront immédiatement supprimés.

64. **Dans sa Demande**, **l'Institut considère néanmoins que les données sont anonymisées** : « *In dit geval zouden de gegevens, rekening houdende met de gebruikte pseudonimiseringsmethode, naar onze mening* ***als geanonimiseerde*** *gegevens kunnen worden bestempeld* » (mis en gras par l'Autorité). Il en est **de même dans les réponses communiquées par l'Institut** à l'Autorité[48].

65. L'Autorité rappelle que les catégories suivantes de données, se recouvrant pour partie, sont pertinentes dans le cadre de la présente analyse : les données **à caractère personnel**[49] ; les données qui au terme d'un traitement spécifique peuvent être considérées comme **anonymes**[50] ; les données **pseudonymisées**[51], qui demeurent des données à caractère personnel ; et les données que le responsable du traitement a **tenté d'anonymiser via une méthode qui ne répond toutefois pas au standard élevé de l'anonymisation**, et demeurent par conséquent des données à caractère personnel (pour lesquelles il n'existe le cas échéant, qu'un risque faible de réidentification de personnes concernées).

66. En l'occurrence, s'il est positif que l'on ne conserve que des informations de localisation au niveau de la province, on ne peut pas exclure la possibilité d'identifier des utilisateurs d'un pays spécifique (par exemple, des utilisateurs des Philippines ou du Liechtenstein), ou des personnes dont les données

---

[48] Voir les considérants nos 34, 54 et 79.

[49] Soit, selon l'article 4, 1), du RGPD :

« *toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée»); est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale* ».

Cette définition doit être lue avec le considérant n° 26 du RGPD.

[50] Le dispositif du RGPD ne définit pas en tant que telle la donnée anonymisée, qui se définit *a contrario* de la définition de donnée à caractère personnel (article 4, 1), dans le considérant n° 26 du RGPD (ainsi les règles de protection des données ne s'appliquent pas « *aux informations anonymes, à savoir les informations ne concernant pas une personne physique identifiée ou identifiable, ni aux données à caractère personnel rendues anonymes de telle manière que la personne concernée ne soit pas ou plus identifiable. Le présent règlement ne s'applique, par conséquent, pas au traitement de telles informations anonymes, y compris à des fins statistiques ou de recherche* »).

Cela étant précisé, il n'est pas exclu que le dispositif d'autres texte définisse l'anonymisation. Voir par exemple l'article 2, 7), de la Directive (UE) 2019/1024 du Parlement européen et du Conseil du 20 juin 2019 concernant les données ouvertes et la réutilisation des informations du secteur public (refonte), selon lequel l'anonymisation est « *le processus de transformation des documents en documents anonymes ne permettant pas de remonter à une personne physique identifiée ou identifiable, ou le processus consistant à rendre anonymes des données à caractère personnel de telle sorte que la personne concernée ne soit pas ou plus identifiable* ».

Se référer également WP29, Opinion 05/2014 on Anonymisation Techniques, WP216, 10 avril 2014, disponible sur https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf,

dernièrement consulté le 27/05/2024, sujet en cours de révision au niveau de l'EDPB).

[51] L'article 4, 5), du RGPD, définit la pseudonymisation comme suit : « *le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable* ».

téléphoniques ont été obtenues par d'autres moyens. En conclusion, **l'Autorité considère que les données ne peuvent pas être considérées comme anonymes et qu'il convenait bien d'introduire une demande d'autorisation.**

### II.3.3. Catégories de personnes concernées

67. En ce qui concerne les **catégories de personnes concernées**, les documents communiqués par l'Institut précisent que seront concernés les utilisateurs finaux du réseau ou du service de téléphonie mobile de l'un des opérateurs participants, qui se trouvent **en situation de *roaming* ou apparaissent comme tels** (« *eindgebruikers van het netwerk of de dienst van [de operator], die zich in een situatie van roaming bevinden* ***op Belgisch grondgebied (« inkomende roaming »)*** *of* ***buiten Belgisch grondgebied (« uitgaande roaming »)****, of als zodanig verschijnen gedurende de perioden waarop de steekproeven van gegevens betrekking hebben* » (mis en gras par l'Autorité)), pendant la période d'un mois sur laquelle porte l'échantillon de données traitées dans le cadre du projet.

68. **Aucun de ces documents en revanche, n'estime le nombre de personnes concernées** impliquées par le Projet.

69. Interrogé à ce propos et quant à la limitation des personnes concernées à celles se trouvant en situation de *roaming*, le demandeur a répondu ce qui suit :

> « *L'IBPT ne dispose pas de données chiffrées à cet égard. Chaque opérateur concerné devrait être interrogé* » ;
>
> « *Dans la mesure techniquement possible pour les opérateurs, il s'agira à la fois :*
>
> - *des données relatives aux utilisateurs finaux des services de téléphonie souscrits auprès d'opérateurs en dehors de la Belgique et se trouvant en situation de roaming sur les réseaux des opérateurs belges (« roaming in ») ;*
> - *des données relatives aux utilisateurs finaux des services de téléphonie souscrits auprès des opérateurs belges et se trouvant en situation de roaming en dehors du territoire belge (« roaming out »)* ».
>
> « *Les périodes précises seront fixées en fonction de la date à laquelle sera obtenue la décision de l'APD. Il s'agira de données qui seront générées dans une période ultérieure* ».

70. L'Autorité a ensuite invité le demandeur à interroger les opérateurs afin d'avoir un **ordre de grandeur du nombre de personnes concernées**, et l'a interrogé sur la raison pour laquelle l'étude était limitée aux personnes en situation de *roaming*. Il a répondu ce qui suit :

> « *Proximus werd bevraagd hieromtrent. Op basis van **één dag** heeft Proximus na analyse **2.167.560 verschillende IMSI-gebruikers gedetecteerd** die hetzij roamen op het Belgisch grondgebied, hetzij roamen buiten Belgisch grondgebied. Hierbij wordt geen rekening gehouden met de roamende gebruikers van Orange Belgium en Telenet. Lineaire extrapolatie naar de volledige steekproef van één maand is niet mogelijk, maar deze waarde geeft een goed beeld van de grootte-orde* » (mise en gras et soulignement modifié par l'Autorité).
>
> « *Le choix pour le trafic international a été fait d'une part pour **réduire le volume du trafic** concerné (sans doute 10x moindre) et d'autre part pour pouvoir **analyser les éventuelles activités internationales suspectes*** » (mis en gras par l'Autorité).

71. L'Autorité prend acte de ces éléments et déplore ne disposer que d'une estimation partielle du nombre de personnes concernées.

### II.4. Autres mesures techniques et organisationnelles

#### II.4.1. Sort des données au terme de la recherche

72. Dans sa Consultation Préalable, l'institut précise qu' « *après la fin du projet, les données sur disque seront **effacées et écrasées (par disk wiping, write 0)*** » (mise en gras par l'Autorité). Et que de même, l'archive sera « *effacée **ou** détruite* » (l'Analyse d'Impact précise qu'elle sera détruite) (mise en gras par l'Autorité). L'Analyse d'Impact précise qu'il en sera de même du disque utilisé pour le transfert des données des opérateurs à l'ERM (effacement par *disk wiping (write 0)*).

73. L'Autorité a publié une recommandation au sujet de la suppression des données et invite le demandeur à s'y référer[52]. En tout état de cause, l'Autorité considère que l'effacement et l'écrasement des données par l'écriture de 0 constitue **une mesure insuffisante**, notamment l'écrasement ne se produisant pas vraiment lorsqu'il est recouru à un disque SSD.

74. L'Autorité considère qu'il convient d'établir une distinction selon le type de support des données. Si les données se trouvent sur des **« disques » SSD**, **ces supports doivent être détruits**. Il est en effet

[52] Recommendation on data sanitisation and data medium destruction techniques, v. 1.01, 23 mars 2021, disponible sur https://www.autoriteprotectiondonnees.be/publications/recommendation-n-03-2020-of-11-december-2020.pdf, dernièrement consulté le 16/01/24.

difficile de garantir que des données ont été supprimées de tels supports. Par contre, si des données se trouvent sur des **disques durs traditionnels**, les données doivent être **chiffrées** et leur **clé de chiffrement doit être supprimée**, étant entendu que cette clé ne peut avoir été conservée que dans les registres du CPU (elle ne peut pas être conservée dans la RAM des disques durs eux-mêmes). La documentation pertinente de l'Institut (dont le Projet de Décision) doit être modifiée en ce sens.

### II.4.2. Journalisation

75. Concernant la journalisation, l'Analyse d'Impact indique notamment que « *La traçabilité par logfile **pourrait** permettre de vérifier si le compte du serveur a été usurpé* » (mis en gras par l'Autorité). L'Autorité considère que le Projet de Décision et la convention de sous-traitance **doivent prévoir clairement d'une part, une journalisation détaillée** (date et heure, raison pour laquelle il est accédé aux données, personne accédant aux données, seul ou accompagnée, etc.) **des accès aux données**, et d'autre part, que les données de journalisation générées sont **conservées pour une durée de 10 ans**, pour des fins d'audit et contrôle en matière de protection des données.

### II.4.3. Mesures contre le traitement ultérieur de données

76. Les dispositions dont l'application est sollicitée par l'Institut ne consacrent pas une interdiction de la réutilisation des données collectées à d'autres fins que la recherche entreprise. Néanmoins, l'Autorité considère que **les règles régissant l'accès aux métadonnées de communications électroniques traitées par les opérateurs constituent à la fois une *lex posterior*** et surtout, une ***lex specialis*** par rapport aux autres règles de droit régissant le traitement de données par les autorités publiques autorisées à accéder aux métadonnées. Permettre le traitement ultérieur à d'autres fins que la finalité de leur collecte initiale auprès des opérateurs conformément à la LCE, de métadonnées de communications électroniques par l'autorité publique concernée (ou d'autres autorités publiques), reviendrait à permettre le contournement du système d'accès aux métadonnées spécifiquement (et exhaustivement) mis en place dans le cadre de la LCE. De telle sorte que **tout traitement ultérieur de ce type serait illicite**.

77. Cela étant rappelé, en pratique, l'Institut étant une **autorité publique**, il ne peut être exclu qu'il soit soumis à des obligations légales particulières qui ont un impact sur le traitement ultérieur des données à caractère personnel qu'il traite, tels que par exemple l'article 29, § 1er, du Code d'instruction

criminelle[53] et l'article 14, al. 2, de la loi du 30 novembre 1998 *organique des services de renseignement et de sécurité*[54]. *Mutatis mutandis,* la même situation se présente dans le cas de l'ERM.

78. L'Autorité a interrogé le demandeur à ce sujet (obligations applicables à l'Institut ainsi qu'à l'ERM) et celui-ci a répondu ce qui suit :

> « *Nous **n'avons pas connaissance d'obligations légales autres** que celles mentionnées auxquelles serait soumis l'IBPT et qui serait susceptible d'impliquer un traitement ultérieur de ces données par une autorité tierce.*
>
> *Nous nous permettons de rappeler qu'à aucun moment l'IBPT ne disposera lui-même des données des opérateurs : ces données sont pseudonymisées (voire anonymisées) par les opérateurs eux-mêmes et transmises directement à l'ERM, qui les traitera conformément aux instructions données par l'IBPT.*
>
> *Nous précisons encore que l'article 5.1 du projet de convention de sous-traitance IBPT-ERM prévoit ce qui suit :*
> *« Le sous-traitant ne traite les données à caractère personnel que sur instruction documentée du responsable du traitement, **à moins qu'il ne soit tenu d'y procéder en vertu du droit de l'Union ou du droit belge auquel il est soumis.** Dans ce cas, le sous-traitant **informe le responsable du traitement de cette obligation juridique avant le traitement, sauf si la loi le lui interdit pour des motifs importants d'intérêt public**. »*
> *Enfin, **compte tenu du niveau de sécurité élevé du mécanisme de pseudonymisation (voire d'anonymisation)** prévu, il ne nous semble pas qu'en la forme dans laquelle elles*

---

[53] « *Toute autorité constituée, tout fonctionnaire ou officier public et, pour le secteur des prestations familiales, toute institution coopérante au sens de la loi du 11 avril 1995 visant à instituer "la charte" de l'assuré social qui, dans l'exercice de ses fonctions acquerra la connaissance d'un crime ou d'un délit, sera tenu de donner avis sur-le-champ au procureur du Roi près le tribunal dans le ressort duquel ce crime ou ce délit aura été commis ou dans lequel l'inculpé pourrait être trouvé, et de transmettre à ce magistrat tous les renseignements, procès-verbaux et actes qui y sont relatifs.*

*Les fonctionnaires qui, sur la base de la loi du 20 décembre 2022 relative aux canaux de signalement et à la protection des auteurs de signalement d'atteintes à l'intégrité dans les organismes du secteur public fédéral et au sein de la police intégrée, ont recours au système de signalement, sont dispensés de l'obligation visée à l'alinéa 1er* ».

[54] « *Les autorités judiciaires les fonctionnaires et les agents des services publics, y compris des services de police, peuvent communiquer d'initiative au Service de Renseignement et de Sécurité concerné les informations utiles à l'exécution de ses missions.*

*A la requête d'un service de renseignement et de sécurité, les autorités judiciaires, les fonctionnaires et les agents des services publics, y compris des services de police, communiquent au service de renseignement et de sécurité concerné, les informations utiles à l'exécution de ses missions.*

*Lorsque les autorités judiciaires, les fonctionnaires et les agents des services publics, y compris les services de police, estiment que la communication des informations visées à l'alinéa 2 est de nature à porter atteinte à une information ou à une instruction judiciaire en cours ou à la récolte d'informations visée par la loi du 18 septembre 2017 relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l'utilisation des espèces, ou qu'elle est susceptible de nuire à l'intégrité physique d'une personne, ils peuvent refuser cette communication dans les cinq jours ouvrables de la demande, en exposant leurs raisons par écrit.*

*Dans le respect de la législation en vigueur, les services de renseignement et de sécurité peuvent selon les modalités générales fixées par le Roi, avoir accès aux banques de données du secteur public utiles à l'exécution de leurs missions* ».

*seront communiquées à l'ERM, ces données présenteront un intérêt quelconque autre qu'à des fins de recherche (ou éventuellement de statistiques). Le risque à cet égard nous semble donc très limité* » (mis en gras par l'Autorité).

79. Interrogé de nouveau à ce sujet, le demandeur a précisé ce qui suit :

« *Pour ce qui concerne tant l'IBPT que l'ERM, nous ne rejoignons pas votre conclusion concernant l'absence de garanties. En effet, il nous semble que les mesures prises pour protéger les données concernées contre les abus sont au contraire très élevées. Il ne nous a pas paru d'emblée utile de les énumérer dans le corps de notre email dès lors qu'elles sont décrites très précisément dans l'analyse d'impact au* ***point 3.2 de l'analyse d'impact*** *indiqué en réponse à votre point 8 (mesures techniques et organisationnelles), auquel nous nous permettons à nouveau de vous renvoyer.*

*Compte tenu de votre remarque, nous nous permettons également de rappeler que :*

- *Les données à caractère personnel concernées sont soumises aux standards les plus élevés en matière de techniques d'anonymisation,* ***de sorte que celles-ci peuvent à notre sens être considérées comme des données anonymes (auquel cas l'IBPT n'est pas tenue de soumettre une demande de contrôle préalable à votre Autorité)*** *;*
- *Ce n'est* ***qu'à titre de précaution, compte tenu de l'avis du Groupe 29 en la matière, que les données concernées par le présent projet ont été qualifiées de données « pseudonymes », dès lors que l'anonymisation complète semble être un concept de nature presque purement théorique*** *;*
- *Les garanties les plus strictes sont prises tant au niveau des limitations d'accès à ces données, qu'au niveau de la finalité des traitements envisagés qui est précisément circonscrite et de leur durée de conservation qui est strictement limitée à la durée du projet.*

*En outre, l'ERM ayant obtenu ces données en sa qualité de* ***sous-traitant de l'IBPT****, il nous semble que les possibilités de réutilisation ultérieure de ces données* ***sont limitées par la convention de sous-traitance (soumise en projet)****.*

*Le cas échéant,* ***nous pourrions ajouter une disposition visant à exclure toute réutilisation ultérieure de ces données sans l'accord préalable de l'IBPT****. Cela étant, nous nous interrogeons sur la raison pour laquelle nous devrions appliquer des mesures plus strictes que celles qui découleraient de l'application des règles en matière de réutilisation des*

*données prévues par le RGPD et de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel. Nous attirons également votre attention quant au fait que le projet de convention de sous-traitance est basé sur les clauses contractuelles types validées par la Décision d'exécution de la Commission du 4 juin 2021 relative aux clauses contractuelles types entre les responsables du traitement et les sous-traitants au titre de l'article 28, paragraphe 7, du RGDP.*

*Par ailleurs, nous n'avons* ***pas connaissance d'obligations légales autres*** *que celles prévues par la loi organique des services de renseignement et de sécurité et par le Code d'instruction criminelle qui seraient* ***susceptibles d'obliger l'ERM*** *à communiquer ces données à un tiers. Nous notons par ailleurs que les obligations légales que vous citez ne sont pas spécifiques au présent projet* » (mise en gras et soulignement modifié par l'Autorité).

80. L'Autorité prend acte de ces explications et considère, **sans préjudice des considérants nos 38-39 et 76**, **que la convention de sous-traitance doit être adaptée de la manière suggérée par l'Institut**, en prévoyant **que toute réutilisation ultérieure des données est exclue sans l'accord préalable de l'IBPT**.

### II.4.4. <u>Autres mesures techniques et organisationnelles</u>

81. Les autres mesures techniques et organisationnelles évoquées dans les documents communiqués par le demandeur n'appellent pas de commentaire particulier sous réserve de ce qui suit.

82. Le Projet de Décision et la convention de sous-traitance doivent prévoir des mesures techniques et organisationnelles suffisantes garantissant que seuls les chercheurs concernés ont accès aux données, **à l'exclusion notamment des gestionnaires de systèmes ou bases de données**. Interrogé sur ce point précis, le demandeur s'est limité à renvoyer aux documents communiqués (« *cf. l'article 5.4 du projet de convention de sous-traitance en annexe et point 3.2 de l'analyse d'impact* »).

83. De manière générale, l'Autorité considère en outre que les deux personnes qui traiteront les données, à savoir le chercheur en charge de l'étude et son directeur, doivent être **expressément soumises aux obligations suivantes, sur une base contractuelle** :

- **Séparation des autres traitements** : les chercheurs doivent maintenir le traitement des données concernées pour les finalités concernées séparés des autres traitements de données à caractère personnel qu'ils réalisent par ailleurs ;

- **Interdiction de « dé-pseudonymisation » des données** : les chercheurs doivent s'engager contractuellement à mettre en œuvre tous les moyens pour éviter que l'identité de personnes concernées par les données ne soit recherchée. Ils ne peuvent entreprendre aucune action dont le but serait de convertir des données pseudonymisées en données « dé-pseudonymisées » décodées ;

- **Interdiction de couplage** : les chercheurs ne peuvent entreprendre aucune tentative de coupler les données à caractère personnel obtenues à des données à caractère personnel qui leur aurait déjà été transmises dans le cadre d'autres autorisations ou par ailleurs ;

- **Confidentialité** : les chercheurs doivent s'engager au maintien de la confidentialité des données d'études et à veiller à ce que ces données soient exclusivement utilisées par eux, aux seules fins de la réalisation du Projet ;

- **Personnes qui traitent les données et liste de ces personnes** : les personnes compétentes qui traitent les données d'étude sont renseignées nominativement dans une liste.

84. L'Autorité rappelle que la présente autorisation n'est **pas** la suite d'**une évaluation approfondie et exhaustive de l'ensemble des mesures** techniques et organisationnelles à mettre en place, notamment compte-tenu de l'état de l'art, et souligne que **la responsabilité d'une telle analyse incombe au responsable du traitement**.

### II.5. Droits des personnes concernées

85. Dans sa Consultation Préalable, l'Institut invoque l'article 14, 5., b), du RGPD (fourniture de l'information exigeant des efforts disproportionnés) pour justifier qu'il est dispensé de l'obligation d'informer les personnes concernées. Il précise encore que le responsable du traitement et le sous-traitant prennent les mesures appropriées pour protéger les droits et libertés et les intérêts légitimes des personnes concernées, y compris « *en communiquant publiquement et de façon concertée quant au Projet* ».

86. La Consultation Préalable précise encore que « *Une communication publique sera effectuée concernant le projet. Les personnes concernées pourront donc s'adresser à l'IBPT ou à l'ERM pour recevoir plus d'informations sur le projet. Cependant, l'IBPT et l'ERM disposeront uniquement de données pseudonymes, de sorte qu'il ne sera pas possible de répondre à des demandes d'accès, de rectification, d'effacement ni de portabilité, puisque l'IBPT et l'ERM ne seront pas en mesure d'établir le lien entre les données pseudonymes et la personne concernée* » (souligné par l'Autorité).

87. Comme cela a déjà été indiqué, l'Institut **revendique l'application de l'article 89 du RGPD.** S'agissant de l'information de la personne concernée, **il invoque également celle de l'article 14, 5., b) du RGPD** (information impossible ou impliquant des efforts disproportionnés, en particulier dans l'hypothèse de la recherche scientifique). L'article 89 du RGPD (plus exactement, ses paragraphes .2 et .3) est (sont) exécuté(s) en droit belge dans les **articles 186 et s. de la LTD**. Conformément à l'article 89, 2., du RGPD, les dérogations aux droits visés aux articles 15, 16, 18 et 21 (sous réserve des garanties visées au 1.) s'appliquent « *dans la mesure où ces droits risqueraient de rendre impossible ou d'entraver sérieusement la réalisation des finalités spécifiques et où de telles dérogations sont nécessaires pour atteindre ces finalités* ».

88. L'Autorité considère **qu'il incombe tout d'abord à l'Institut d'informer le public quant à la réalisation de l'étude envisagée via son site internet. Une telle information doit être spécifiquement dédiée au Projet, et doit être complète** (finalité, parties prenantes, périodes concernées, opérateurs concernés, etc.) **et effective**. A cette fin, l'Autorité considère qu'elle doit être réalisée à la fois via la page d'accueil du site internet de l'Institut ainsi que via la page dédiée à la politique de protection des données de ce site. Cette information doit également être réalisée **au moment opportun**, soit dans un délai raisonnable avant la collecte des métadonnées, et **pendant la durée nécessaire**, c'est-à-dire à tout le moins jusqu'au terme de la conservation des données concernées par l'ERM pour l'Institut, étant entendu que dans un délai raisonnable après la publication de l'étude, une information via la page d'accueil du site internet de l'Institut n'apparaîtrait plus nécessaire. **La documentation pertinente de l'Institut (dont le Projet de Décision) doit être modifiée en ce sens**.

89. En outre, l'Autorité souligne que le niveau de prévisibilité des dispositions normatives invoquées par l'Institut dans sa demande ne peut suffire à autoriser l'application de l'article 14, 5., c), du RGPD. Autrement dit, **les opérateurs concernés** eux-mêmes devront également informer les personnes concernées à propos de la communication des métadonnées dans le cadre du Projet, de manière spécifique et complète. A cet égard, l'Autorité considère qu'une notification individuelle des personnes concernées (par exemple, en notifiant via sms celles qui arrivent sur un réseau en *roaming* pendant la période de l'étude, en notifiant les abonnés des opérateurs concernés par e-mail ou via la communication de leurs factures, etc.) serait en l'occurrence disproportionnée et **qu'une information du même type que celle que réalisera l'Institut via son site Internet apparaît suffisante (voir le considérant n° 88)**.

90. Enfin, l'Autorité relève que le Projet recevra également une certaine **publicité à partir du site Internet de l'Autorité elle-même**, dès lors notamment, que la présente décision doit être publiée.

## II.6. Durée de conservation des données

91. S'agissant de la durée de conservation des données, l'Analyse d'Impact précise ce qui suit :

> « *La durée de conservation des données correspondra à la durée du Projet (fin actuellement prévue le 30 juin 2024) + 6 mois pour couvrir une éventuelle publication et le rapport final.* ***Une demande de prolongation du Projet d'une durée d'un an supplémentaire est en cours****. Par ailleurs,* ***dans le cas où le Projet aurait une suite, il pourrait être utile de conserver les données plus longtemps****, par exemple pour comparaison ou pour éviter une période sans donnée* » (mis en gras par l'Autorité).

92. Avant tout, l'Autorité observe que l'Institut **n'invoque pas de disposition du rang de loi fixant la durée de conservation (de traitement) des métadonnées pseudonymisées** concernées par le Projet. Or il s'agit d'un élément essentiel du traitement qui devrait être déterminé (fût-ce via la fixation d'un délai maximal de conservation des données) dans une norme du rang de loi. Il lui appartient **d'identifier la disposition du rang de loi fixant la durée de traitement des données dans sa documentation**, conformément aux articles 5, 2., et 24, 1., du RGPD .

93. Ensuite, **le Projet de Décision et l'Analyse d'Impact doivent clairement indiquer un terme <u>déterminé et fixe</u> de conservation/traitement des données.** A défaut de prévoir une date explicite[55], il convient à tout le moins de **fixer une date qui peut être calculée précisément** à compter de la date de collecte des métadonnées auprès des opérateurs, et **endéans laquelle le traitement réalisé aux fins de la recherche doit cesser**. L'Institut **ne peut pas** se réserver la possibilité de « *conserver les données plus longtemps* », « *dans le cas où le Projet aurait une suite* ». L'Autorité considère que le Projet peut fixer une durée de conservation des données de **2 ans après la réalisation** des expérimentations (à exécuter dans le délai fixé pour la réalisation du Projet juste évoqué), **<u>à la seule fin</u>** de permettre aux relecteurs de la revue scientifique dans laquelle est envisagée la publication à paraître, de demander des expérimentations supplémentaires.

## <u>II.7. Décision</u>

**Par ces motifs,**

**L'Autorité décide d'autoriser l'accès de l'Institut à des métadonnées de communications électroniques pseudonymisées par les opérateurs concernés afin de faire réaliser par l'ERM, une recherche relative aux vulnérabilités du protocole SS7 et à leur mode de détection, en application de l'article 107/4, § 1er, al. 2, de la LCE, dans les limites des développements précédents (considérants nos 1-93), et en particulier, pour autant que les conditions suivantes soient rencontrées :**

---

[55] Dans l'Analyse d'Impact indique une fin prévue **le 30 juin 2024**. Il va de soi que cette échéance pourra être adaptée compte-tenu de la durée du processus d'autorisation par l'Autorité.

**1.** La recherche réalisée par l'ERM ne peut pas avoir d'impact sur des cas concrets impliquant des personnes concernées (**considérants nos 13-15**) ;

**2.** L'activité de recherche qui sera menée par l'ERM dans le cadre du Projet doit s'inscrire exclusivement dans la recherche scientifique poursuivie par celle-ci dans le cadre de sa mission en tant qu'institution d'enseignement universitaire. Ce qu'il appartient à l'IBPT, en tant que responsable du traitement, de vérifier, de documenter et de garantir conformément aux articles 5, 2., et 24, 1., du RGPD (**considérants nos 31-40**) ;

**3.** Le cadre normatif applicable à l'ERM doit permettre le plein effet de la convention de sous-traitance qui sera conclue avec l'Institut, garantissant notamment que l'ERM agira exclusivement selon les instructions de l'Institut, sans que La Défense (par l'intermédiaire de l'un ou l'autre de ses services ou composantes) ne puisse interférer dans l'activité de recherche qui sera menée ou avec les métadonnées de communications électroniques qui seront traitées à cette fin (instructions, accès aux données, etc.). Ce qu'il appartient à l'Institut, en tant que responsable du traitement, de vérifier, de documenter et de garantir, conformément aux articles 5, 2., et 24, 1., du RGPD (**considérants nos 31-40**) ;

**4.** L'Institut et les opérateurs sont responsables conjoints du traitement de pseudonymisation/anonymisation des données, dans les limites précisées dans la présente autorisation, et la documentation tenue par l'IBPT (dont le Projet de Décision) doit être adaptée en conséquence (**considérants nos 41-44**) ;

**5.** L'Institut doit adapter l'analyse qu'il a réalisée à propos des données traitées afin de prendre en considération les combinaisons de paramètres et les risques de réidentification par un autre responsable du traitement que l'ERM qui pourrait accéder légalement aux données). Il doit également prévoir la mise en œuvre au niveau des opérateurs, si cela s'avère n'nécessaire à l'aune des métadonnées de communications électroniques collectées *in concreto*, de mesures techniques de *differential privacy* afin d'éviter la possible réidentification des personnes concernées. La documentation pertinente de l'Institut (dont le Projet de Décision et l'Analyse d'impact et la convention) doit être modifiée en ce sens (**considérants nos 45-60**) ;

**6.** La documentation pertinente soumise par l'Institut (dont le Projet de Décision et la convention de sous-traitance) doit être adaptée afin de détailler exhaustivement l'ensemble des métadonnées de communications électroniques concernée, de manière telle qu'en outre, aucune autre métadonnée de communication électronique ne puisse être demandée aux opérateurs par l'Institut (ou l'ERM) durant la réalisation de la recherche envisagée. Cela étant précisé, s'il apparaissait au cours du Projet que des métadonnées supplémentaires seraient

nécessaires, il appartiendrait alors à l'Institut de soumettre une nouvelle demande d'accès à ces métadonnées à l'Autorité (**considérants nos 61-62**) ;

**7.** Au terme de leur durée de conservation, si les données se trouvent sur des « disques » SSD, ces supports doivent être détruits. Par contre, si des données se trouvent sur des disques durs traditionnels, les données doivent être chiffrées et leur clé de chiffrement doit être supprimée, étant entendu que cette clé ne peut avoir été conservée que dans les registres du CPU (elle ne peut pas être conservée dans la RAM des disques durs eux-mêmes). La documentation pertinente de l'IBPT (dont le Projet de Décision et la convention de sous-traitance) doit être adaptée en conséquence (**considérants nos 72-74**) ;

**8.** La documentation pertinente de l'IBPT (dont le Projet de Décision et la convention de sous-traitance) doit prévoir clairement d'une part, une journalisation détaillée (date et heure, raison pour laquelle il est accédé aux données, personne accédant aux données, seul ou accompagnée, etc.) des accès aux données, et d'autre part, que les données de journalisation générées sont conservées pour une durée de 10 ans, pour des fins d'audit et contrôle en matière de protection des données (**considérant n° 75**) ;

**9.** Sans préjudice des considérants nos 38-39 et 76, la convention de sous-traitance doit être adaptée de la manière suggérée par l'Institut, en prévoyant que toute réutilisation ultérieure des données est exclue sans l'accord préalable de l'IBPT (**considérants nos 76-80**) ;

**10.** Le Projet de Décision et la convention de sous-traitance doivent prévoir des mesures techniques et organisationnelles supplémentaires, telles que décrites dans la présente autorisation étant entendu que cette dernière n'est pas la suite d'une évaluation approfondie et exhaustive de l'ensemble des mesures techniques et organisationnelles à mettre en place, notamment compte-tenu de l'état de l'art, cette responsabilité incombant au responsable du traitement (**considérants nos 81-84**) ;

**11.** L'Institut d'informer le public quant à la réalisation de l'étude envisagée via son site internet. Une telle information doit être spécifiquement dédiée au Projet, et doit être complète (finalité, parties prenantes, périodes concernées, opérateurs concernés, etc.) et effective. A cette fin, l'Autorité considère qu'elle doit être réalisée à la fois via la page d'accueil du site internet de l'Institut ainsi que via la page dédiée à la politique de protection des données de ce site. Cette information doit également être réalisée au moment opportun, soit dans un délai raisonnable avant la collecte des métadonnées, et pendant la durée nécessaire, c'est-à-dire à tout le moins jusqu'au terme de la conservation des données concernées par l'ERM pour l'Institut, étant entendu que dans un délai raisonnable après la publication de l'étude, une

information via la page d'accueil du site internet de l'Institut n'apparaîtrait plus nécessaire. La documentation pertinente de l'Institut (dont le Projet de Décision) doit être modifiée en ce sens (**considérants nos 80-83**) ;

**12.** Les opérateurs eux-mêmes, devront également informer les personnes concernées, de manière spécifique et complète, à propos de la communication des métadonnées dans le cadre du Projet. A cette fin, une information du même type que celle que réalisera l'Institut via son site Internet, conformément à la présente autorisation, apparaît suffisante (**voir le considérant n° 89**) ;

**13.** L'Institut doit indiquer dans sa documentation la disposition du rang de loi fixant la durée de traitement des données. Cette documentation (dont le Projet de Décision et l'Analyse d'Impact) doit être en outre adaptée et indiquer un terme déterminé et fixe de conservation/traitement des données (**considérants nos 91-93**).

Pour le Service d'Autorisation et d'Avis,
(sé.) Bart Preneel - Membre externe du Service d'Autorisation et d'Avis, en remplacement de Cédrine Morlière, Directrice du Service d'Autorisation et d'Avis récusée de sa propre initiative

**Annexe – Liste de paramètres**

List of parameters
PSE: to be pseudonymised
NO: not needed
---

processSeqNr
seizureTime
stopTime
octetsSent
octetsReceived
msusSent
msusReceived
status
-mtp3Data
opc
dpc
ni
slc
-sccpData
PSE origGlobalTitle
PSE termGlobalTitle
calledNoA
callingNoA
calledNP
callingNP
calledSSN
callingSSN
callingAddrInd
calledAddrInd
callingTransType
calledTransType
PSE firstTermGlobalTitle
firstCalledNoA
firstCalledNP
firstCalledTransType
PSE lastTermGlobalTitle

```
  lastCalledNoA
  lastCalledNP
  lastCalledTransType
-mapData:
  -tcapData:
    otid
    dtid
    errorcode
    firstTcapMessageType
    lastTcapMessageType
    firstMessageComponentType
    lastMessageComponentType
    - abortCause
      abortCauseType   NO
      abortCauseValue  NO
    -opCodeList
      opcode: ?first + last? OR ?list like "2 7 7 7 7 2"?
      time  NO
  PSE imsi   (addressString only: I suppose NatureOfAddr always 1 and numberPlan=1)
  PSE msisdn (addressString ... idem)
  PSE vlr    (idem)
  PSE forwardedToNumber (idem)
  PSE msc    (idem)
  PSE hlr    (idem)
  subscriberCategory
  mapVersion
  cancellationType
  -ssData
    -sSactive    NO
    -sSinactive  NO
    voiceEnabled
    smsEnabled
    faxEnabled
    dataEnabled
  supportedCamelPhases        NO
  supportedLCSCapabilitySets  NO
  -gsmSCF
  PSE imei
```

serviceKey

-locationInformationType NO

-linkStatistics: NO

-linkDataList: NO