Table des matières

# 1. Résumé

1. La ministre des Télécommunications doit faire publier au Moniteur belge une circulaire qui « *comprend une liste des autorités belges qui sont habilitées à obtenir d'un opérateur des données conservées en vertu des articles 122, 123, 126, 126/1, 126/3 et 127* » de la loi du 13 juin 2005 relative aux communications électroniques. Cette liste se trouve en annexe. Les autorités qui se trouvent sur cette liste ont rédigé une fiche comprenant davantage d'informations. Ces fiches sont publiées sur le site Internet de l'IBPT. Le présent document comprend également des considérations générales concernant les requêtes des autorités et leur exécution par les opérateurs.

# 2. Objet

2. Le présent document constitue la circulaire que la ministre des Télécommunications[1] doit publier au Moniteur belge conformément à l'article 127/1, § 5, alinéa 2, de la loi du 13 juin 2005 relative aux communications électroniques (ci-après la loi relative aux communications électroniques). Cet article a été introduit dans cette loi par la loi du 20 juillet 2022 relative à la collecte et à la conservation des données d'identification et des métadonnées dans le secteur des communications électroniques et à la fourniture de ces données aux autorités (ci-après la loi sur la conservation des données de 2022).

3. L'article 127/1, § 5, alinéa 2, de la loi relative aux communications électroniques indique que la circulaire « *comprend une liste des autorités belges qui sont habilitées à obtenir d'un opérateur des données conservées en vertu des articles 122, 123, 126, 126/1, 126/3 et 127* » de cette même loi. Cette liste se trouve en annexe. Des informations plus détaillées se trouvent dans des fiches publiées sur le site Internet de l'IBPT[2]. Ces fiches ont été rédigées par les autorités listées en annexe du présent document.

4. La présente circulaire comprend également des considérations générales destinées à aider les opérateurs[3] et les autorités belges compétentes dans le cadre de demande de données conservées en vertu d'un des articles précités.

5. Un opérateur a demandé que la présente circulaire reprenne la liste des autorités qui peuvent adresser aux opérateurs une requête de gel de données existantes (quick freeze) ou futures (future freeze).

6. Cependant, cette forme de conservation de données (quick freeze et future freeze) n'est pas prévue par la loi relative aux communications électroniques mais par les législations des autorités demanderesses. Dès lors, la présente circulaire ne reprend ci-après et uniquement à titre d'information les autorités belges qui peuvent adresser aux opérateurs de telles requêtes, étant donné que davantage d'informations sont reprises dans les fiches publiées sur le site Internet de l'IBPT :

---

[1] Selon l'article 127/1, § 5, alinéa 2, de la loi du 13 juin 2005 relative aux communications électroniques, il revient au ministre de publier cette circulaire dans le Moniteur belge. L'article 2, 2°, de cette même loi définit la notion de « ministre » comme « *les ministres ou secrétaire d'Etat qui sont compétents pour les matières relatives aux communications électroniques telles que visées dans la présente loi* ».

[2] https://www.ibpt.be/operateurs/interception-legale.

[3] L'article 2, 11°, de la loi relative aux communications électroniques définit un opérateur comme « *une personne ou entreprise qui fournit un réseau public de communications électroniques ou un service de communications électroniques accessible au public.* »

6.1. Les autorités judiciaires sur base des articles 39ter à 39quinquies du Code d'instruction criminelle ;

6.2. Les services de renseignement et de sécurité sur base de l'article 13/6 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité ;

6.3. La FSMA sur base de l'article 81, § 1bis et de l'article 84, § 1bis/1 de la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers.

7. En plus d'être publiée au Moniteur belge, la présente circulaire est publiée sur le site Internet de l'IBPT[4]. Les modifications au présent document ou à son annexe seront publiées de la même manière.

8. La présente circulaire est interprétative et est destinée aux opérateurs et aux autorités belges qui peuvent obtenir d'un opérateur des données conservées en vertu des articles 122, 123, 126, 126/1, 126/3 ou 127 de la loi relative aux communications électroniques.

# 3. Notions

## Différents types de données

9. L'article 3, 9), du Règlement (UE) 2023/1543 du Parlement européen et du Conseil du 12 juillet 2023 relatif aux injonctions européennes de production et aux injonctions européennes de conservation concernant les preuves électroniques dans le cadre des procédures pénales et aux fins de l'exécution de peines privatives de liberté prononcées à l'issue d'une procédure pénale (ci-après le règlement relatif aux preuves électroniques en matière pénale)[5] définit les « **données relatives aux abonnés** » comme « *toutes données détenues par un fournisseur de services concernant l'abonnement à ses services, relatives à:*

*a) l'identité d'un abonné ou d'un client, telles que le nom, la date de naissance, l'adresse postale ou géographique, les données de facturation et de paiement, le numéro de téléphone ou l'adresse électronique fournis ;*

*b) le type de service et sa durée, y compris les données techniques et les données identifiant les mesures techniques connexes ou les interfaces utilisées ou fournies par l'abonné ou le client au moment du premier enregistrement ou de la première activation, et les données relatives à la validation de l'utilisation du service, à l'exclusion des mots de passe ou autres moyens d'authentification utilisés à la place d'un mot de passe qui sont fournis par un utilisateur ou créés à la demande d'un utilisateur.* »

10. Plusieurs législations européennes font référence à la notion de **données de trafic** :

10.1. L'article 2, alinéa 2, b), de la directive « vie privée et communications électroniques »[6] définit les « données relatives au trafic » comme « *b) toutes les données traitées en*

[4] https://www.ibpt.be/operateurs/interception-legale.
[5] J.O. L 191/118 du 28.07.2023.
[6] Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques).

*vue de l'acheminement d'une communication par un réseau de communications électroniques ou de sa facturation* » ;

10.2. L'article 3, 11), du règlement relatif aux preuves électroniques en matière pénale définit les « données relatives au trafic comme « *les données relatives à la fourniture d'un service proposé par un fournisseur de services qui servent à fournir des informations contextuelles ou supplémentaires sur ce service et qui sont générées ou traitées par un système d'information du fournisseur de services, tels que la source et la destination d'un message ou un autre type d'interaction, l'emplacement du dispositif, la date, l'heure, la durée, la taille, le routage, le format, le protocole utilisé et le type de compression, et d'autres métadonnées de communications électroniques et des données, autres que les données relatives aux abonnés, relatives au début et à la fin d'une session d'accès d'un utilisateur à un service, telles que la date et l'heure d'utilisation, la connexion et la déconnexion du service* ».

11. L'article 9 de la directive « vie privée et communications électroniques » (transposé dans l'article 123 de la loi relative aux communications électroniques) vise le traitement par les opérateurs de « **données de localisation autres que les données relatives au trafic** ». Il s'agit de données de localisation nécessaires pour le fonctionnement du réseau mais qui ne sont pas liées à une communication de contenu.

12. L'article 2, 93°, de la loi relative aux communications électroniques définit les « **métadonnées de communications électroniques** » comme suit « *les données traitées dans un réseau de communications électroniques aux fins de la transmission, la distribution ou l'échange de contenu de communications électroniques, y compris les données permettant de retracer une communication et d'en déterminer l'origine et la destination ainsi que les données relatives à la localisation de l'appareil produites dans le cadre de la fourniture de services de communications électroniques, et la date, l'heure, la durée et le type de communication.* » Cette définition a été reprise du projet de règlement « vie privée et communications électroniques », qui a été proposé par la Commission européenne pour remplacer la directive vie privée et communications électroniques[7].

13. Plusieurs législations définissent la notion de **contenu** :

13.1. L'article 3, 12), du règlement relatif aux preuves électroniques en matière pénale définit les « données relatives au contenu » comme « *toutes données dans un format numérique telles que du texte, de la voix, des vidéos, des images et du son, autres que les données relatives aux abonnés ou les données relatives au trafic* » ;

13.2. L'article 2, 92°, définit le « contenu de communications électroniques » comme « *le contenu échangé au moyen de services de communications électroniques, notamment sous forme de texte, de voix, de documents vidéo, d'images et de son* ».

14. L'article 3, 8), du règlement relatif aux preuves électroniques regroupe les différentes catégories de données sous la notion de « **preuves électroniques** »: « *les données relatives aux abonnés, les données relatives au trafic ou les données relatives au contenu stockées par un fournisseur de services ou pour le compte d'un fournisseur de services, sous une forme numérique, au moment de la réception d'un certificat d'injonction européenne de production (EPOC) ou d'un certificat d'injonction européenne de conservation (EPOC-PR)* ».

[7] Proposal of 10.1.2017 of the European Commission for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications).

15. Les relations entre les différents types de données sont les suivantes.

16. Les notions de données de trafic au sens de la directive « vie privée et communications électroniques » et de métadonnées au sens de la loi relative aux communications électroniques sont similaires. Il convient cependant de noter les différences suivantes :

16.1. La notion de métadonnées exclut les données de trafic qui sont nécessaires pour la facturation (par exemple le nom et l'adresse (électronique) de l'abonné pour envoyer la facture) et qui ne répondent pas à la définition de métadonnées ;

16.2. La notion de métadonnées inclut les données de localisation autres que les données relatives au trafic, étant donné que la notion de métadonnées inclut « *les données relatives à la localisation de l'appareil produites dans le cadre de la fourniture de services de communications électroniques* ».

17. Les données de trafic ou de métadonnées ne sont pas des données du contenu de la communications électroniques.

18. Les articles 126 et 127 de la loi relative aux communications électroniques obligent les opérateurs à conserver des données, dans le but ultime d'identifier l'utilisateur final. Cependant, cela n'exclut pas que l'article 126 puisse contenir des données de trafic (ou métadonnées). Ainsi, selon l'article 126, § 1er, 15°, les opérateurs doivent conserver l'adresse IP à la source de la connexion et selon la jurisprudence de la CJUE, les adresses IP font partie des données relatives au trafic[8].

19. Le fait que les adresses IP peuvent être utiles pour identifier l'utilisateur final est reflété dans la définition de « données demandées à la seule fin d'identifier l'utilisateur » de l'article 3, 10) du règlement relatif aux preuves électroniques en matière pénale : « *les adresses IP et, si nécessaire, les ports de provenance et l'horodatage pertinents, à savoir la date et l'heure, ou les équivalents techniques de ces identifiants et les informations connexes, lorsque les services répressifs ou les autorités judiciaires les demandent à la seule fin d'identifier l'utilisateur dans le cadre d'une enquête pénale spécifique* ».

20. Les données que les opérateurs doivent conserver en vertu des articles 126/1 à 126/3[9] de la loi relative aux communications électroniques (conservation de données ciblée sur base géographique) sont des données de trafic (ou métadonnées).

## Notion de requête

21. Le présent document utilise la notion de « requête » pour désigner la demande formelle d'une autorité envers un opérateur de lui fournir des données conservées sur base des articles 122, 123, 126, 126/1, 126/3 et 127 de la loi relative aux communications électroniques. En pratique, la requête d'une autorité peut porter une autre dénomination (par exemple le réquisitoire ou la réquisition).

[8] C.J.U.E, arrêt *La Quadrature du Net,* 6 octobre 2020, C-511/18, C-512/18 et C- 520/18, point 152.
[9] L'article 127/1, § 5, de la loi relative aux communications électroniques, qui constitue le fondement juridique de la présente circulaire, vise les articles 126/1 et 126/3. En réalité, ce sont les articles 126/1, 126/2 et 126/3 qui sont consacrés à la conservation ciblée sur base géographique et les données à conserver dans ce cadre sont listées à l'article 126/2, § 2.

# 4. La compétence matérielle de l'autorité qui requiert les données

## Aperçu des deux conditions reprises dans l'article 127/1 de la loi relative aux communications électroniques

22. Les paragraphes 2 à 4 de l'article 127/1 de la loi relative aux communications électroniques prévoient ce qui suit :

« *§ 2. Seules les autorités suivantes peuvent obtenir d'un opérateur des données conservées en vertu des articles 122 et 123, pour les finalités ci-dessous, pour autant que prévu par et aux conditions fixées dans une norme législative formelle :*

*1° les services de renseignement et de sécurité, afin d'accomplir les missions qui leur sont attribuées par la loi du 30 novembre 1998 organique des services de renseignement et de sécurité ;*

*2° les autorités compétentes aux fins de la prévention de menaces graves pour la sécurité publique ;*

*3° les autorités chargées de la sauvegarde des intérêts vitaux de personnes physiques ;*

*4° les autorités compétentes pour l'examen d'une défaillance de la sécurité du réseau ou du service de communications électroniques ou des systèmes d'information ;*

*5° les autorités administratives ou judiciaires compétentes pour la prévention, la recherche, la détection ou la poursuite d'une infraction commise en ligne ou par le biais d'un réseau ou service de communications électroniques ;*

*6° les autorités administratives ou judiciaires compétentes pour la prévention, la recherche, la détection ou la poursuite d'un fait qui relève de la criminalité grave ;*

*7° les autorités administratives chargées de préserver un intérêt économique ou financier important de l'Union européenne ou de la Belgique, y compris dans les domaines monétaire, budgétaire et fiscal, de la santé publique et de la sécurité sociale;*

*8° les autorités administratives ou judiciaires compétentes pour la prévention, la recherche, la détection ou la poursuite d'un fait qui constitue une infraction pénale mais qui ne relève pas de la criminalité grave;*

*9° l'Institut dans le cadre du contrôle de la présente loi et les autorités compétentes pour la protection des données dans le cadre de leurs missions de contrôle;*

*10° les autorités qui sont légalement habilitées à réutiliser des données à des fins de recherche scientifique ou historique ou à des fins statistiques.*

*§ 3. Les données conservées en vertu des articles 126 et 127 le sont pour les autorités et les finalités visées au paragraphe 2, 1° à 8°.*

*Seules les autorités visées au paragraphe 2 peuvent obtenir d'un opérateur des données conservées en vertu des articles 126 et 127, pour les finalités prévues dans ce même paragraphe, pour autant que prévu par et aux conditions fixées dans une norme législative formelle.*

*Par dérogation à l'alinéa 2, les autorités visées au paragraphe 2, 10°, ne peuvent pas obtenir d'un opérateur des adresses IP attribuées à la source de la connexion.*

*Par dérogation à l'alinéa 2, une demande d'une autorité d'obtenir d'un opérateur des adresses IP attribuées à la source d'une connexion n'est autorisée qu'aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave, de la prévention des menaces graves contre la sécurité publique et de la sauvegarde des intérêts vitaux d'une personne physique, lorsque cette autorité serait en mesure, à l'aide des informations en sa possession et des adresses IP attribuées à la source de la connexion obtenues de l'opérateur, de tracer le parcours de navigation d'un utilisateur final sur Internet.*

*§ 4. Les données conservées en vertu des articles 126/1 et 126/3 le sont pour les autorités*

*et finalités visées au paragraphe 2, 1° à 3° et 6°.*

*Seules les autorités visées au paragraphe 2, 1° à 3°, 6° et 9°, peuvent obtenir d'un opérateur, pour les finalités visées dans ce même paragraphe, des données conservées en vertu des articles 126/1 et 126/3, pour autant que prévu par et aux conditions fixées dans une norme législative formelle.* »

23. Ces paragraphes visent l'hypothèse selon laquelle une autorité belge exige d'un opérateur qu'il lui fournisse des données personnelles conservées en vertu des articles 122, 123, 126, 126/1, 126/3 ou 127 de la loi relative aux communications électroniques.

24. L'exposé des motifs de la loi sur la conservation des données de 2022 prévoit que l'article 127/1 de la loi relative aux communications électroniques ne s'applique pas « *aux situations dans lesquelles les données sont transmises à une autorité par l'une des parties à la communication ou demandées par une autorité à l'une des parties. Entre notamment dans cette dernière hypothèse, la situation ou une partie transmet à une autorité ses métadonnées à des fins de plainte, de règlement d'un litige ou d'une instruction d'office*[10]*.* » (page 96)

25. Cette situation est rencontrée à l'article 122, § 6, de la loi relative aux communications électroniques, qui prévoit ce qui suit : « *L'Institut, le Service de médiation pour les télécommunications, l'Autorité belge de la concurrence, les juridictions de l'ordre judiciaire et le Conseil d'Etat peuvent, dans le cadre de leurs compétences, être informés des données de trafic et de facture pertinentes en vue du règlement de litiges, parmi lesquels des litiges relatifs à l'interconnexion et la facturation.* »

26. Cette disposition ne constitue pas une base légale qui permet à ces différentes autorités d'exiger des données des opérateurs, conservées sur base des articles 122, 123, 126, 126/1, 126/3 et 127 de la loi relative aux communications électroniques, mais vise la situation dans laquelle une partie à la communication (qui, le cas échant, peut être l'opérateur lui-même) transmet des données à l'autorité.

27. Par ailleurs, l'exposé des motifs de la loi sur la conservation des données de 2022 prévoit que l'article 127/1 de la loi relative aux communications électroniques ne s'applique pas non plus :« *lorsqu'un operateur transmet des données anonymes à un tiers. Les données doivent être rendues anonymes conformément aux exigences du RGPD et doivent être rendues anonymes par rapport aux personnes physiques et morales auxquelles ces données se rapportent (et pas uniquement par rapport aux personnes physiques comme c'est le cas dans le RGPD). En effet, la directive « vie privée et communications électroniques » (directive 2002/58) protège la confidentialité des données liées tant aux personnes morales qu'aux personnes physiques.* » (page 96)

28. Il ressort de l'article 127/1 qu'un opérateur ne peut pas utiliser pour ses propres besoins des données conservées en vertu des articles 126, 126/1, 126/3 ou 127, qui sont des données conservées pour les autorités. Ce principe est sans préjudice de la possibilité pour un opérateur de conserver, dans les conditions fixées par la loi (voir en particulier les articles 122 et 123 de la loi relative aux communications électroniques), des données pour ses propres besoins ou dans l'intérêt de ses clients.

29. Conformément à l'article 127/1, §§ 2 à 4, de la loi relative aux communications électroniques, un opérateur ne peut pas communiquer à un tiers des données personnelles conservées en vertu des articles 122, 123, 126, 126/1, 126/3 ou 127 de la loi relative aux communications

[10] Projet de loi relatif à la collecte et à la conservation des données d'identification et des métadonnées dans le secteur des communications électroniques et à la fourniture de ces données aux autorités, Doc., Ch., 2021-2022, n°2572/001.

électroniques, sauf dans les hypothèses prévues dans cet article 127/1 et qui sont exposées ci-dessous.

30. Comme il ressort de l'article 127/1 de la loi relative aux communications électroniques et de l'exposé des motifs de la loi sur la conservation des données de 2022, une autorité belge qui exige d'un opérateur de lui fournir des données personnelles conservées en vertu des articles 122, 123, 126, 126/1, 126/3 ou 127 de la loi relative aux communications électroniques doit répondre aux deux conditions cumulatives suivantes :

30.1. elle doit remplir l'une des finalités d'accès aux données visées à l'article 127/1[11], et ;

30.2. une norme législative formelle doit l'habiliter à requérir ces données à l'opérateur.

31. Ces deux conditions sont examinées plus en détail ci-dessous.

## Première condition : remplir une finalité d'accès aux données reprise à l'article 127/1 de la loi relative aux communications électroniques

32. L'autorité qui exige d'un opérateur de lui fournir des données personnelles conservées en vertu des articles 122, 123, 126, 126/1, 126/3 ou 127 de la loi relative aux communications électroniques doit remplir l'une des finalités d'accès aux données visées à l'article 127/1 de cette même loi.

33. Les finalités d'accès admises sont différentes selon que les données auxquelles l'autorité accède sont conservées en vertu :

33.1. des articles 122 et 123 de la loi relative aux communications électroniques (données conservées par les opérateurs pour leurs propres besoins ou dans l'intérêt de leurs clients), ou ;

33.2. des articles 126 et 127 de la loi relative aux communications électroniques (données (techniques) en vue d'identifier l'utilisateur final), ou ;

33.3. des articles 126/1 à 126/3 de la loi relative aux communications électroniques (métadonnées conservées dans le cadre de la conservation ciblée sur base géographique).

34. Le tableau ci-dessous reprend la liste exhaustive des finalités d'accès admises selon le type de données conservées :

| Ensemble des finalités d'accès visées dans l'article 127/1, § 2 | Finalités d'accès admises selon les différents types de données conservées |
|---|---|

[11] La notion d'accès aux données se retrouve dans la jurisprudence de la CJUE et permet de simplifier le texte mais, en pratique, les opérateurs fournissent aux autorités les données demandées.

| | Données art. 122 et 123[12] | Données art. 126 et 127[13] | Données art. 126/1 à 126/3[14] |
|---|---|---|---|
| 1° les services de renseignement et de sécurité afin d'accomplir les missions en vertu de la loi des services de renseignement et de sécurité[15] | Oui | Oui | Oui |
| 2° la prévention de menaces graves pour la sécurité publique | Oui | Oui | Oui |
| 3° la sauvegarde des intérêts vitaux de personnes physiques | Oui | Oui | Oui |
| 4° l'examen d'une défaillance de la sécurité du réseau ou du service de communications électroniques ou des systèmes d'information | Oui | Oui | Non |
| 5° la prévention, la recherche, la détection ou la poursuite d'une infraction commise en ligne ou par le biais d'un réseau ou service de communications électroniques | Oui | Oui | Non |
| 6° la prévention, la recherche, la détection ou la poursuite d'un fait qui relève de la criminalité grave | Oui | Oui | Oui |
| 7° préserver un intérêt économique ou financier important de l'UE ou de la Belgique | Oui | Oui | Non |
| 8° la prévention, la recherche, la détection ou la poursuite d'un fait qui constitue une infraction pénale mais qui ne relève pas de la criminalité grave | Oui | Oui | Non |
| 9° l'IBPT dans le cadre du contrôle de la loi relative aux communications électroniques et les autorités compétentes pour la protection des données dans le cadre de leurs missions de contrôle | Oui | Oui | Oui |
| 10° la recherche scientifique ou historique ou fins statistiques | Oui | Oui (sauf adresse IP) | Non |

35. A titre d'exemple, « l'examen d'une défaillance de la sécurité du réseau ou du service de communications électroniques ou des systèmes d'information » (finalité d'accès reprise à l'article 127/1, § 2, 4°, de la loi relative aux communications électroniques) permet aux autorités compétentes en la matière de remplir la première condition de l'article 127/1 (finalité d'accès, cf. supra) pour ce qui concerne les données conservées par les opérateurs conformément aux articles 122, 123, 126 et 127 mais pas pour les données conservées par

[12] Voir article 127/1, § 2.
[13] Voir article 127/1, § 3. L'article 127/1, § 3, alinéa 3 précise que « *Par dérogation à l'alinéa 2, une demande d'une autorité d'obtenir d'un opérateur des adresses IP attribuées à la source d'une connexion n'est autorisée qu'aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave, de la prévention des menaces graves contre la sécurité publique et de la sauvegarde des intérêts vitaux d'une personne physique, lorsque cette autorité serait en mesure, à l'aide des informations en sa possession et des adresses IP attribuées à la source de la connexion obtenues de l'opérateur, de tracer le parcours de navigation d'un utilisateur final sur Internet.* »
[14] Voir article 127/1, § 4.
[15] Loi organique des services de renseignement et de sécurité du 30 novembre 1998.

ces mêmes opérateurs conformément aux articles 126/1 à 126/3 (données conservées sur base géographique).

36. L'article 127/1, § 1er, de la loi relative aux communications électroniques indique ce qui suit :

« [...], *la criminalité grave comprend notamment les faits pour lesquels il existe des indices sérieux :*

*1° qu'ils sont de nature à entraîner la peine minimale d'emprisonnement correctionnel principal visée à l'article 88bis, § 1er, alinéa 1er, du Code d'instruction criminelle ;*

*2° qu'ils sont de nature à entraîner une sanction de niveau 5 ou 6 visée à l'article XV.70 du Code de droit économique ;*

*3° qu'ils pourraient constituer une infraction aux articles 14 ou 15 du règlement (UE) n° 596/2014 du Parlement européen et du Conseil du 16 avril 2014 sur les abus de marché (règlement relatif aux abus de marché) et abrogeant la directive 2003/6/CE du Parlement européen et du Conseil et les directives 2003/124/CE, 2003/125/CE et 2004/72/CE de la Commission ou aux dispositions prises sur la base ou en exécution de ces articles.* »

# Deuxième condition : la norme législative formelle

37. L'autorité qui exige d'un opérateur qu'il lui fournisse des données personnelles conservées en vertu des articles 122, 123, 126, 126/1 à 126/3 ou 127 de la loi relative aux communications électroniques doit également disposer d'une norme législative formelle qui l'habilite à requérir ces données de l'opérateur. A titre d'exemple, les autorités qui sont compétentes pour « l'examen d'une défaillance de la sécurité du réseau ou du service de communications électroniques ou des systèmes d'information » (finalité d'accès reprise à l'article 127/1, § 2, 4°, de la loi relative aux communications électroniques) ne pourront en pratique accéder aux données conservées par les opérateurs conformément aux articles 122, 123, 126 et 127, que pour autant que la loi organique de ces autorités le prévoie expressément et selon les conditions fixées par cette loi.

38. Selon l'exposé des motifs de la loi sur la conservation des données de 2022, la norme législative formelle « *doit avoir au moins le niveau d'une loi : loi fédérale, décret, ordonnance, règlement européen, etc.* » (page 96)

39. Cette norme législative formelle doit préciser :

> « *— la ou les catégories d'entreprises auxquelles l'autorité peut demander des données ;*
> *— les catégories de données qui peuvent être demandées ;*
> *— les finalités poursuivies ;*
> *— les mécanismes de contrôle de la demande de données, qui est effectué en interne ou, le cas échéant, par une juridiction ou une autorité administrative indépendante.* »
> (art. 127/1, § 5, de la loi relative aux communications électroniques).

40. Cette disposition fait l'objet des explications suivantes dans l'exposé des motifs de la loi sur la conservation des données de 2022 (pages 115 et 116) :

« *Afin d'éviter toute interprétation de la législation organique ou sectorielle sur laquelle une autorité se base pour obtenir les données de l'opérateur, il est essentiel que cette législation*

*prévoie le pouvoir de l'autorité d'obtenir les données de l'opérateur (ou une expression équivalente, cette notion pouvant être plus large que la notion d'opérateur au sens de la loi télécom) et ne se contente pas de prévoir un pouvoir d'obtenir des données de toute personne. Il est aussi essentiel que cette législation prévoie que l'autorité peut obtenir des données d'identification ou des métadonnées (ou toute expression qui vise à préciser les données à obtenir de l'opérateur) et ne se contente pas de prévoir que l'autorité peut demander toute information utile […] Ne peuvent pas être reprises sur cette circulaire des autorités qui seraient simplement légalement habilitées à demander à des acteurs économiques toute donnée utile.* »

41. Par ailleurs, dans son arrêt La Quadrature du Net du 6 octobre 2020 (affaires jointes C-511/18, C-512/18 et C-520/18), la CJUE admet que les États membres imposent aux opérateurs certaines mesures de conservation de données « *dès lors que ces mesures assurent, par des règles claires et précises, que la conservation des données en cause est subordonnée au respect des conditions matérielles et procédurales y afférentes et que les personnes concernées disposent de garanties effectives contre les risques d'abus.* » (dispositif de l'arrêt)

42. C'est la norme législative formelle qui doit contenir ces conditions matérielles et procédurales et les garanties contre les abus.

## Liste des autorités qui déclarent répondre aux deux conditions

43. L'annexe à la présente circulaire comprend une liste d'autorités qui déclarent répondre aux deux conditions susmentionnées.

44. L'objectif poursuivi est que cette liste soit aussi exhaustive que possible. Cependant, il convient de noter que celle-ci a été établie sur la base des informations communiquées par les autorités concernées à l'IBPT et à la ministre des Télécommunications. Son caractère exhaustif ne peut donc être garanti.

45. Si une autorité demande des données à un opérateur, conservées sur base des articles 122, 123, 126, 126/1, 126/3 et 127 de la loi relative aux communications électroniques, sans être reprise sur cette liste, elle devra indiquer à l'opérateur qu'elle répond bien aux deux conditions susmentionnées : répondre à une des finalités d'accès prévues par l'article 127/1, §§ 2 à 4, de la loi relative aux communications électroniques et disposer d'une norme législative formelle qui répond aux exigences du paragraphe 5, alinéa 1er, de ce même article. Le simple fait qu'une autorité ne soit pas reprise dans cette liste ne justifie toutefois pas que l'opérateur refuse de donner suite à la demande qui lui est adressée par cette autorité.

46. Si l'une de ces conditions n'est pas remplie, l'opérateur devra refuser d'exécuter la requête. Si les deux conditions sont remplies, l'autorité devra être reprise sur la liste en annexe. Afin que cette liste puisse être mise à jour de manière à refléter au mieux la réalité, il est demandé ce qui suit :

46.1. toute autorité qui ne figure pas sur la liste mais qui estimerait disposer des habilitations légales lui permettant d'y être reprise est priée de le porter à la connaissance de l'IBPT et du cabinet du ou de la ministre des Télécommunications ;

46.2. de même, les autorités concernées sont également priées de leur notifier toute modification de leur législation qui nécessiterait une adaptation de cette liste.

47. Enfin, il convient de rappeler la nature purement interprétative de la présente circulaire, qui n'a pas force de loi, et est formulée sous réserve de l'interprétation des cours et tribunaux.

# 5. La compétence territoriale de l'autorité qui requiert les données

48. Il résulte de l'arrêt du 1er décembre 2015 (P. 13.2082.N/1, YAHOO! Inc.) de la Cour de cassation de Belgique qu'un opérateur est soumis à la législation belge du seul fait de sa participation active à la vie économique en Belgique et doit donc faire droit à une demande de données du procureur du Roi conformément à l'article 46bis du Code d'instruction criminelle :

« *2. L'article 46bis Code d'instruction criminelle dispose :*

*- au paragraphe 1er, alinea 1er, qu'en recherchant les crimes et les délits, le procureur du Roi peut, par une décision motivée et écrite, requérir le concours de l'opérateur d'un réseau de communication électronique ou d'un fournisseur d'un service de communication électronique afin d'obtenir les données prévues par cette disposition ;*

*- au paragraphe 2, alinéa 1er, que chaque opérateur d'un réseau de communication électronique et chaque fournisseur d'un service de communication électronique qui est requis de communiquer les données visées au paragraphe 1er, les fournisse au procureur du Roi.*

*3. Au paragraphe 2, alinéa 4, cette disposition énonce aussi que le refus de communiquer les données visées est puni d'une amende. Cette sanction pénale vise à imposer l'obligation de concours incombant aux opérateurs et fournisseurs visés et confère, dans cette mesure, à l'article 46bis, § 2, du Code d'instruction criminelle le caractère d'une mesure coercitive.*

*4. En règle générale, un État ne peut prendre des mesures coercitives que sur son propre territoire afin d'imposer le respect de ses lois et, s'il prend une telle mesure sur le territoire d'un autre État, il s'approprie un pouvoir extraterritorial qui méconnaît la souveraineté de cet État.*

*5. Un État prend une mesure coercitive sur son propre territoire lorsqu'il existe un lien territorial suffisant entre cette mesure et ce territoire. Le lien qui est, à tout le moins, requis, est notamment déterminé par la nature et la portée de la mesure coercitive.*

*6. La sanction pénale prévue à l'article 46bis, § 2, alinéa 4, du Code d'instruction criminelle vise uniquement à imposer aux opérateurs et fournisseurs actifs depuis la Belgique une mesure ayant pour objectif d'obtenir de simples éléments d'identification ensuite d'une infraction dont l'enquête relève de la compétence des juridictions répressives belges. Cette mesure ne requiert pas la présence à l'étranger des fonctionnaires de police ou magistrats belges, ni de personnes agissant pour leur compte. Cette mesure ne requiert pas davantage la commission d'un quelconque acte matériel à l'étranger. Elle concerne, par conséquent, une mesure coercitive dont la portée est limitée et dont l'exécution ne requiert aucune intervention en dehors du territoire belge.*

*7. L'article 3 du Code pénal dispose que l'infraction commise sur le territoire du royaume, par des Belges ou par des étrangers, est punie conformément aux dispositions des lois belges. L'infraction prévue à l'article 46bis, § 2, alinéa 4, du Code d'instruction criminelle est commise en un lieu où les données requises doivent être reçues. Par conséquent, l'opérateur ou le fournisseur qui refuse de communiquer ces données est passible d'une peine en Belgique, quel que soit le lieu où il est établi.*

*8. Il ressort de ce qui précède, d'une part, que la mesure consistant en l'obligation de fournir les données visées en l'espèce est prise sur le territoire belge à l'égard de chaque opérateur ou fournisseur qui oriente activement ses activités économiques vers des consommateurs en Belgique et, d'autre part, que la juridiction belge qui condamne un opérateur ou fournisseur établi à l'étranger en raison de l'inobservation de cette obligation et impose ainsi le respect d'une mesure prise en Belgique, n'exerce pas de pouvoir de juridiction extraterritorial. Dans la mesure où il est déduit d'une autre prémisse juridique, le moyen manque en droit.*

*9. Les juges d'appel, adoptant les motifs du jugement entrepris et par des motifs propres, ont considéré notamment que la demanderesse, en tant que fournisseur d'un service de messagerie électronique gratuit, est présente sur le territoire de la Belgique et se soumet volontairement à la loi belge parce qu'elle participe activement à la vie économique en Belgique notamment par l'usage du nom de domaine « www.yahoo.be », l'usage de la langue locale, par la publicité faite en fonction de la localisation des utilisateurs de ses services et par son accessibilité en Belgique pour ces utilisateurs via notamment une boîte de réclamations et une rubrique FAQ. En adoptant les motifs du jugement entrepris (points 4.2. et 4.4.), les juges d'appel ont aussi considéré que :*

*- le procureur du Roi ne demande rien, aux États-Unis, à un ressortissant de ce pays mais, substantiellement, demande quelque chose en Belgique à un ressortissant de ce pays prestataire de services en Belgique ; ».*

49. Ce même raisonnement a été répété dans l'arrêt du 19 février 2019 (P.17.1229.N/1, Skype communications) de la Cour de cassation de Belgique mais cette fois pour une demande de fournir le contenu d'une communication électronique à un juge d'instruction :

*« 8. L'article 88bis du Code d'instruction criminelle, tel qu'applicable en l'espèce, dispose :*
*« § 1er. Lorsque le juge d'instruction estime qu'il existe des circonstances qui rendent le repérage de télécommunications ou la localisation de l'origine ou de la destination de télécommunications nécessaire à la manifestation de la vérité, il peut faire procéder, en requérant au besoin le concours technique de l'opérateur d'un réseau de télécommunication ou du fournisseur d'un service de télécommunication directement ou par l'intermédiaire d'un service de police désigné par le Roi :*

*1° au repérage des données d'appel de moyens de télécommunication à partir desquels ou vers lesquels des appels sont adressés ou ont été adressés ;*
*2° à la localisation de l'origine ou de la destination de télécommunications.*

*Dans les cas visés à l'alinéa 1er, pour chaque moyen de télécommunication dont les données d'appel sont repérées ou dont l'origine ou la destination de la télécommunication est localisée, le jour, l'heure, la durée et, si nécessaire, le lieu de la télécommunication sont indiqués et consignés dans un procès-verbal.*

*Le juge d'instruction indique les circonstances de fait de la cause qui justifient la mesure dans une ordonnance motivée qu'il communique au procureur du Roi.*

*Il précise la durée durant laquelle elle pourra s'appliquer, cette durée ne pouvant excéder deux mois à dater de l'ordonnance, sans préjudice de renouvellement.*
*[...]*
*§ 2. Chaque opérateur d'un réseau de télécommunication et chaque fournisseur d'un service de télécommunication communique les informations qui ont été demandées dans un délai à fixer par le Roi, sur la proposition du Ministre de la Justice et du Ministre compétent pour les télécommunications.*

*Toute personne qui, du chef de sa fonction, a connaissance de la mesure ou y prête son concours, est tenue de garder le secret. Toute violation du secret est punie conformément à l'article 458 du Code pénal.*

*Toute personne qui refuse de prêter son concours technique aux réquisitions visées dans cet article, concours dont les modalités sont déterminées par le Roi, sur la proposition du Ministre de la Justice et du ministre compétent pour les télécommunications, est punie d'une amende de vingt-six euros à dix mille euros. »*

*L'article 90quater, § 2, du Code d'instruction criminelle, tel qu'applicable en l'espèce, dispose :*

*« Si la mesure comporte une opération sur un réseau de communication, l'opérateur de ce réseau, ou le fournisseur du service de télécommunication, est tenu de prêter son concours technique, quand le juge d'instruction le requiert directement ou par l'intermédiaire d'un service de police désigné par le Roi.*

*Toute personne qui, du chef de sa fonction, a connaissance de la mesure ou y prête son concours, est tenue de garder le secret. Toute violation du secret est punie conformément à l'article 458 du Code pénal.*

*Toute personne qui refuse de prêter son concours technique aux réquisitions visées dans cet article, concours dont les modalités sont déterminées par le Roi, sur la proposition du Ministre de la Justice et du Ministre compétent pour les télécommunications, est punie d'une amende de vingt-six euros à dix mille euros. »*

*Ces dispositions permettent au juge d'instruction belge, dans le cadre de son instruction, de demander à chaque opérateur d'un réseau de télécommunication et chaque fournisseur d'un service de messagerie électronique dont l'activité économique s'adresse activement aux consommateurs en Belgique, de communiquer les informations ou de fournir l'assistance technique visées en l'espèce, indépendamment du lieu où cet opérateur ou ce fournisseur est établi ou du lieu où se situe l'infrastructure requise pour donner suite à la demande du juge d'instruction.*

*En effet, d'une part un tel opérateur ou fournisseur est soumis à la législation belge du seul fait de sa participation active à la vie économique en Belgique.*

*D'autre part, l'obligation de coopérer ainsi visée ne requiert pas l'intervention des autorités judiciaires belges à l'étranger. Par conséquent, le juge d'instruction n'est pas tenu d'adresser sa demande d'entraide judiciaire à l'État où le siège ou l'infrastructure de cet opérateur ou de ce fournisseur se situent et n'est pas davantage lié par la législation de ce pays. »*

# 6. Les mentions minimales de la requête adressée à l'opérateur

50. L'article 127/1, § 6, de la loi relative aux communications électroniques prévoit ce qui suit :

« *Les demandes que les autorités adressent aux opérateurs afin d'obtenir certaines données conservées en vertu des articles 122, 123, 126, 126/1, 126/3 ou 127 comprennent les mentions minimales suivantes :*
*1° l'identité de l'autorité demanderesse, ou, lorsque la demande est envoyée à l'opérateur par un service central pour le compte de cette autorité, l'identité de ce service ;*

*2° la fonction de la personne de contact auprès de l'autorité demanderesse, ou, lorsque la demande est envoyée à l'opérateur par un service central pour le compte de l'autorité, la fonction de la personne de contact auprès de ce service central ;*
*3° la base juridique sur laquelle se fonde la demande, sauf lorsque la demande est envoyée à l'opérateur par le biais d'un service central pour le compte d'une autre autorité ;*
*4° le délai de réponse souhaité.* »

51. L'article 127/1, § 6, 3°, précité prévoit que la requête doit comprendre « *la base juridique sur laquelle se fonde la demande, sauf lorsque la demande est envoyée à l'opérateur par le biais d'un service central pour le compte d'une autre autorité* ». Ce service central est en pratique le « NTSU », à savoir le *National Technical & Tactical Support Unit* des unités spéciales de la police fédérale. En pratique, lorsque la demande de données est envoyée à l'opérateur par le biais du NTSU, l'autorité demanderesse introduit la demande de données dans la plateforme d'échange TANK du NTSU[16]. Dans ce cas, la requête (qui contient la base légale) doit aussi être introduite dans cette plateforme.

52. Un opérateur doit refuser une requête écrite qui n'est pas signée. Si la signature est électronique, elle doit répondre aux exigences légales en la matière. Une signature en dessous d'un email ne répond pas à ces exigences.

# 7. Le contrôle interne ou externe de la requête

53. L'article 4 du règlement relatif aux preuves électroniques en matière pénale fait la distinction entre :

- « *1. Une injonction européenne de production visant à obtenir des données relatives aux abonnés ou visant à obtenir des données demandées à la seule fin d'identifier l'utilisateur telles qu'elles sont définies à l'article 3, point 10)*[17] », et ;

- « *2. Une injonction européenne de production visant à obtenir des données relatives au trafic, à l'exception des données demandées à la seule fin d'identifier l'utilisateur telles qu'elles sont définies à l'article 3, point 10) [...]* ».

54. On retrouve une distinction similaire en droit belge. Ainsi, le Code d'instruction criminelle prévoit ce qui suit[18] :

« *46bis. § 1er. En recherchant les crimes et les délits, le procureur du Roi peut, par une décision motivée et écrite, procéder ou faire procéder sur la base de toutes données détenues*

[16] Il s'agit d'une plateforme gérée par le NTSU, qui permet d'envoyer aux opérateurs certaines demandes de données des autorités judiciaires et des services de renseignement et de sécurité et de recevoir la réponse des opérateurs.
[17] L'article 3, point 10), de ce règlement définit les « données demandées à la seule fin d'identifier l'utilisateur » comme suit : « les adresses IP et, si nécessaire, les ports de provenance et l'horodatage pertinents, à savoir la date et l'heure, ou les équivalents techniques de ces identifiants et les informations connexes, lorsque les services répressifs ou les autorités judiciaires les demandent à la seule fin d'identifier l'utilisateur dans le cadre d'une enquête pénale spécifique ».
[18] Il en va de même pour les articles 81, § 1er, alinéa 1er, et 84, § 1er, alinéa 1er, de la loi sur la surveillance financière (loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers), dont la terminologie utilisée est presque identique à celle respectivement des articles 46bis et 88 bis du Code d'instruction criminelle. Voir également, l'article 2, 5°, de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges.

*par lui, ou au moyen d'un accès aux fichiers des clients des acteurs visés à l'alinéa 2, premier et deuxième tirets, à :*

*1° l'identification de l'abonné ou de l'utilisateur habituel d'un service visé à l'alinéa 2, deuxième tiret, ou bien du moyen de communication électronique utilisé ;*

*2° l'identification des services visés à l'alinéa 2, deuxième tiret, auxquels une personne déterminée est abonnée ou qui sont habituellement utilisés par une personne déterminée. »*
(nous soulignons)

*« Art. 88bis. § 1er. S'il existe des indices sérieux que les infractions sont de nature à entraîner un emprisonnement correctionnel principal d'un an ou une peine plus lourde, et lorsque le juge d'instruction estime qu'il existe des circonstances qui rendent le repérage de communications électroniques ou la localisation de l'origine ou de la destination de communications électroniques nécessaire à la manifestation de la vérité, il peut faire procéder :*

*1° au repérage des données de trafic de moyens de communication électronique à partir desquels ou vers lesquels des communications électroniques sont adressées ou ont été adressées;*

*2° à la localisation de l'origine ou de la destination de communications électroniques. »*
(nous soulignons)

55. Cette distinction est aussi reflétée pour ce qui concerne le contrôle de la requête, comme expliqué ci-dessous.

56. Comme exigé par la jurisprudence de la CJUE[19], en cas de demande de trafic, à l'exception de données demandées à la seule fin d'identifier l'utilisateur et sauf cas d'urgence, la requête de l'autorité doit faire l'objet d'un contrôle préalable par une autorité administrative indépendante (par exemple l'Autorité de protection des données) ou une juridiction (par exemple un juge d'instruction). En cas d'urgence, le contrôle doit intervenir dans un bref délai. Ce contrôle (préalable ou a posteriori) est un contrôle externe, étant donné que le contrôle est effectué par une autorité distincte de la personne ou de l'autorité demanderesse.

57. En cas de demande de données relatives aux abonnés ou visant à obtenir des données à la seule fin d'identifier l'utilisateur, ce contrôle externe n'est pas requis mais un contrôle interne (contrôle au sein de l'autorité demanderesse) est nécessaire. Ce contrôle interne comprend par exemple une vérification du respect des formalités (par exemple la présence des signatures requises, la référence à la base légale), de la nécessité et de la proportionnalité de la demande. Il est effectué par exemple par le procureur du Roi, par le préposé à la protection des données à caractère personnel (DPO ou Data protection officer) de l'autorité demanderesse, le supérieur hiérarchique ou l'officier de police judiciaire désigné spécialement à cet effet pour ce qui concerne la loi sur le statut de l'IBPT[20].

58. C'est la législation organique de l'autorité demanderesse qui détermine quel contrôle doit être effectué (interne ou externe), par qui et en quoi il consiste. Les contrôles interne et externe font référence à un contrôle par une autorité et non au contrôle effectué par l'opérateur.

59. Cette distinction entre contrôle externe et contrôle interne découle de l'arrêt « loi carte prépayée » de la Cour constitutionnelle (arrêt n° 158/2021 du 18 novembre 2021) :

*« B.16.8.6. À cet égard, les parties requérantes renvoient à l'arrêt de la grande chambre de la Cour de justice du 2 mars 2021 en cause Prokuratuur (C-746/18, points 50 à 56), dans*

[19] Arrêt Digital Rights du 8 avril 2014 (C-293/12), arrêt Tele 2 du 21 décembre 2016 (C-203/15), arrêt La Quadrature du Net du 6 octobre 2020 (C-511/18) et arrêt Prokuratuur du 2 mars 2021 (C-746/18).

[20] Loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges.

*lequel la Cour de justice exige, selon elles, qu'une autorité administrative indépendante ou un juge contrôle au préalable chaque demande d'accès au regard des droits fondamentaux et règles nationales applicables et dans lequel elle précise, selon les parties requérantes, que le ministère public, qui dirige la procédure d'enquête et exerce le cas échéant l'action publique, ne dispose pas de l'indépendance requise pour pouvoir effectuer ce contrôle.*

*Toutefois, cet arrêt portait sur une demande du ministère public d'obtenir un accès à des données relatives au trafic et à des données de localisation. Comme il est dit en B.14.3, la Cour de justice et la Cour européenne des droits de l'homme n'exigent en revanche pas de contrôle judiciaire ou administratif préalable pour une demande d'accès à des données d'identification. En conséquence, le droit au respect de la vie privée ne s'oppose pas à une demande d'accès à de telles données qui émane du ministère public. »* (nous soulignons)

# 8. Demande adressée à la cellule de coordination de l'opérateur

60. Il résulte de l'article 127/3, § 1er, alinéa 3, de la loi relative aux communications électroniques qu'une autorité doit s'adresser à la Cellule de coordination de l'opérateur pour obtenir des données conservées sur base des articles 122, 123, 126, 126/1, 126/3 et 127 de la loi relative aux communications électroniques .

61. En vertu du même article, chaque opérateur doit disposer d'une telle cellule.

62. Une autorité belge qui ne disposerait pas encore des coordonnées de la permanence de la cellule de coordination des opérateurs peut s'adresser à l'IBPT pour obtenir l'accès à ces coordonnées.

63. Si une requête vise un opérateur bien précis (et non les opérateurs de manière générale) et qu'il apparait qu'elle aurait dû être adressée à un autre opérateur (par exemple car c'est cet autre opérateur qui dispose des informations concernant le numéro de téléphone visé dans la requête), l'autorité devra adresser une nouvelle requête à cet opérateur.

# 9. Qu'est-ce que l'opérateur peut/doit contrôler et dans quels cas peut-il/doit-il refuser une requête?

64. L'opérateur doit contrôler que la requête provient bien de l'autorité qui prétend s'adresser à elle (et non d'une personne qui se fait passer pour cette autorité), sauf si la requête a été introduite dans la plateforme d'échange « TANK » du NTSU. En effet, dans ce cas, ce contrôle est déjà effectué grâce à l'implémentation technique et aux règles fonctionnelles de cette plateforme. L'opérateur doit refuser d'exécuter la requête de l'autorité si la mention minimale (voir titre 4 ci-dessus) suivante n'est pas reprise sur cette requête : « *1° l'identité de l'autorité demanderesse, ou, lorsque la demande est envoyée à l'opérateur par un service central pour le compte de cette autorité, l'identité de ce service ».*

65. L'opérateur peut déterminer si la requête a fait l'objet d'un contrôle interne ou externe en examinant cette dernière.

66. Lorsqu'il ressort de la requête qu'elle a fait l'objet d'un contrôle externe (contrôle par une juridiction ou une autorité administrative indépendante), l'opérateur ne doit pas réaliser de contrôle complémentaire. Ceci vaut également lorsque ce contrôle est effectué après l'envoi de la requête à l'opérateur, en raison de l'urgence.

67. Lorsqu'il ressort de la requête qu'elle a fait l'objet d'un contrôle interne, il est attendu de l'opérateur qu'il procède à un contrôle de cette dernière. Lorsque c'est possible, ce contrôle est effectué avant de répondre à la requête. L'opérateur doit s'assurer que la base légale de la requête est suffisante pour requérir les données. Ainsi, l'exposé des motifs de la loi sur la conservation des données de 2022 (voir pages 116 et 117) indique ce qui suit : « *Avant de donner suite à une demande de données qui fait l'objet d'un contrôle interne, il revient à l'opérateur de vérifier l'existence de la base légale nécessaire pour requérir les données.* »

68. Un opérateur doit donc refuser de faire suite à une requête d'une autorité si elle ne repose pas sur une base légale suffisante (voir ci-dessus « 4. La compétence matérielle de l'autorité qui requiert les données » et les deux conditions à respecter). En pratique, l'opérateur pourra d'abord contrôler que la base légale de la requête est bien reprise dans l'annexe au présent document. Si c'est le cas, la base légale est en principe suffisante. Si cela n'est pas le cas, il devra examiner cette base légale plus en détail.

69. Un opérateur doit refuser d'exécuter la requête de l'autorité s'il n'apparaît pas que le contrôle interne ou externe de la requête a bien été effectué (contrôle préalable) ou sera effectué (contrôle a posteriori en cas d'urgence).

70. Ce contrôle ressort de la requête, par exemple, si elle indique qu'il a été effectué ou qu'il sera effectué (urgence). En d'autres termes, l'opérateur est autorisé à se fier à la déclaration dans la requête. Lorsque ce contrôle ne ressort pas de la requête et que l'opérateur le signale à l'autorité demanderesse, cette dernière peut informer l'opérateur que ce contrôle a bien été effectué (contrôle préalable) ou sera effectué (contrôle a posteriori en cas d'urgence).

71. En revanche, l'opérateur ne peut pas refuser d'exécuter la requête, au motif qu'il n'a pas pu prendre connaissance des documents échangés entre les différentes personnes ou autorités dans le cadre du contrôle interne ou externe.

72. Lorsqu'un opérateur refuse de faire suite à une requête, il doit en informer l'autorité demanderesse.

73. Comme expliqué dans l'exposé des motifs de la loi sur la conservation des données de 2022 (voir pages 116 et 117), *« que le contrôle soit interne ou externe, il ne revient pas à l'opérateur de juger de la proportionnalité des demandes de données de cette autorité ni de vérifier si la demande est suffisamment motivée.* »

74. Cependant, sans que cela ne constitue un argument pouvant être utilisé par l'opérateur pour refuser de se conformer à la requête, rien n'empêche l'opérateur de faire savoir à l'autorité demanderesse que cette requête lui semble disproportionnée, car elle nécessite une charge énorme de travail, afin de cette autorité puisse prendre conscience de l'ampleur de la requête et mieux évaluer la proportionnalité de cette dernière.

# 10. Les solutions en cas de différend entre l'opérateur et une autorité belge concernant une demande de données

75. L'IBPT n'est pas habilité à trancher un conflit entre un opérateur et une autorité. Le rôle de l'IBPT se limite :

75.1. à indiquer à un opérateur ou à une autorité, qui l'interroge sur ce sujet, la manière dont il entend appliquer la loi ;

75.2. à contrôler l'opérateur par rapport à certaines dispositions (par exemple la loi relative aux communications électroniques et ses arrêtés d'exécution mais pas les lois organiques d'autres autorités que l'IBPT ou le Service de médiation pour les télécommunications)[21].

76. En cas de conflit persistant, il reviendra aux cours et tribunaux de trancher le conflit.

77. Un opérateur ne peut être sanctionné pour ne pas fournir à une autorité une donnée dont il ne dispose pas (par exemple si l'opérateur ne dispose pas d'une donnée d'identification mais uniquement de données de souscription au service). Cependant, l'opérateur peut être sanctionné s'il ne respecte pas l'article 127 de la loi relative aux communications électroniques concernant l'identification de ses abonnés ou s'il ne conserve pas les données comme prévu aux articles 122, 123 et 126 à 126/3.

# 11. Annexe

78. Liste des autorités belges qui sont habilitées à obtenir d'un opérateur des données personnelles conservées en vertu des articles 122, 123, 126, 126/1, 126/3 et 127 de la loi relative aux communications électroniques.

Donné le

La Ministre des Télécommunications

P. DE SUTTER

[21] La liste des dispositions contrôlées par l'IBPT figure à l'article 14, § 1er, 3°, de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges.

Annexe à la circulaire : liste des autorités belges qui sont légalement habilitées à obtenir d'un opérateur des données conservées en vertu des articles 122, 123[22], 126, 127[23], 126/1 et 126/3[24] de la loi du 13 juin 2005 relative aux communications électroniques (LCE)

| Autorités | Données conservées sur base des art. 122 et 123 de la LCE | Données conservées sur base des art. 126 et 127 de la LCE | Données conservées sur base des art. 126/1 à 126/3 de la LCE | Base légale |
|---|---|---|---|---|
| Les autorités judiciaires (procureur du Roi, juge d'instruction, procureur européen et procureurs européens délégués) | Oui | Oui | Oui, mais uniquement pour les faits visés à l'article 127/1, § 1er, 1°, de LCE (criminalité grave)[25] | Art. 46bis, 88bis, 464/13 et 464/25 du Code d'instruction criminelle. Voir aussi art. 47quaterdecies du même Code en ce qui concerne les procureurs européens. |
| Cellule personnes disparues de la police fédérale | Oui | Oui | Oui | Art. 42, § 2, de la loi du 5 août 1992 sur la fonction de police |
| Les services de renseignement et de sécurité | Oui | Oui | Oui | Art. 16/2, 18/7, 18/8 et 18/17 de la loi organique des services de renseignement et de sécurité du 30 novembre 1998 |
| L'Autorité belge de la Concurrence (ABC) | Oui | Oui | Non | Art. IV.40, § 1er/1, du Code de droit économique |
| L'Autorité des services et marchés financiers (FSMA) | Oui | Oui | Oui, mais uniquement pour les faits visés à l'article 127/1, § 1er, de la LCE dont, entre autres, ceux visés à l'article | Art. 81, 82, 2° et 84 de la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers |

[22] Données conservées sur base des articles 122 et 123 : données de trafic et de localisation conservées par les opérateurs pour leurs propres besoins ou dans l'intérêt de leurs clients.

[23] Données conservées sur base des articles 126 et 127 : données (en ce compris les adresses IP) en vue de l'identification de l'utilisateur final.

[24] Données conservées sur base des articles 126/1 à 126/3 : métadonnées conservées dans le cadre de la conservation ciblée sur base géographique.

[25] Il s'agit des faits pour lesquels il existe des indices sérieux qu'ils sont de nature à entraîner la peine minimale d'emprisonnement correctionnel principal visée à l'article 88bis, § 1er, alinéa 1er, du Code d'instruction criminelle. Au 4/09/2023, cette peine minimale est un an d'emprisonnement.

| Autorités | Données conservées sur base des art. 122 et 123 de la LCE | Données conservées sur base des art. 126 et 127 de la LCE | Données conservées sur base des art. 126/1 à 126/3 de la LCE | Base légale |
|---|---|---|---|---|
| | | | 127/1, § 1er, 3°[26] (criminalité grave) | |
| Le service d'Inspection de la Direction-générale Animaux, Végétaux et Alimentation du Service public fédéral Santé publique, Sécurité de la Chaîne alimentaire et Environnement | Oui, uniquement à des fins d'identification | Oui | Non | Art. 11, § 1, de la loi du 24 janvier 1977 relative à la protection de la santé des consommateurs en ce qui concerne les denrées alimentaires et les autres produits |
| Le service de médiation pour les télécommunications | Oui, uniquement à des fins d'identification | Oui | Non | Art. 43bis, § 3, 7°, de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques |
| Les services d'inspection suivants du SPF Economie :<br>-DG de l'Energie (E2) ;<br>-DG de la Qualité et de la Sécurité (E6) ;<br>-DG de l'Inspection économique (E7) | Oui<br><br>Pour obtenir des données de trafic, de localisation et les adresses IP : uniquement pour les faits visés à l'article 127/1, § 1er, 2°, de la LCE (criminalité grave)[27] | Oui<br><br>Pour obtenir des adresses IP : uniquement pour les faits visés à l'article 127/1, § 1er, 2°, de la LCE (criminalité grave)[28] | Oui, mais uniquement pour les faits visés à l'art. 127/1, § 1er, 2°, de la LCE (criminalité grave)[29] | Art. XV.3, 5°/1, du Code de droit économique |
| Les officiers de police judiciaire (OPJ) de l'Institut belge des services postaux et | Oui | Oui | Oui, mais uniquement dans le cadre du contrôle du respect par l'opérateur de la LCE | Art. 25/1 de la loi du 17 janvier 2003 relative au statut du régulateur des |

[26] Il s'agit des faits qui pourraient constituer une infraction aux articles 14 ou 15 du règlement (UE) n° 596/2014 du Parlement européen et du Conseil du 16 avril 2014 sur les abus de marché (règlement relatif aux abus de marché) et abrogeant la directive 2003/6/CE du Parlement européen et du Conseil et les directives 2003/124/CE, 2003/125/CE et 2004/72/CE de la Commission ou aux dispositions prises sur la base ou en exécution de ces articles.

[27] Il s'agit des faits pour lesquels il existe des indices sérieux qu'ils sont de nature à entraîner une sanction de niveau 5 ou 6 visée à l'article XV.70 du Code de droit économique.

[28] Idem.

[29] Idem.

| Autorités | Données conservées sur base des art. 122 et 123 de la LCE | Données conservées sur base des art. 126 et 127 de la LCE | Données conservées sur base des art. 126/1 à 126/3 de la LCE | Base légale |
|---|---|---|---|---|
| des télécommunications (IBPT) | | | | secteurs des postes et des télécommunications belges |
| L'IBPT agissant dans le cadre d'une procédure administrative | Oui | Oui | Oui, mais uniquement dans le cadre du contrôle du respect par l'opérateur de la LCE | Art. 15 de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges |
| Le Centre pour la Cybersécurité Belgique (CCB)[30] | Oui | Oui | Oui | Art. 62 de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique |
| La Direction générale Statistique – Statistics Belgium du SPF Economie, PME, Classes moyennes et Energie | Données relatives à l'accès, l'utilisation et l'accessibilité financière des services de communications électroniques.<br><br>Données :<br>- Identité de la personne qui a conclu le contrat (nom et adresse ou numéro registre national) ;<br>- Identité de l'entreprise qui a conclu le contrat (nom et adresse ou numéro BCE ou numéro de TVA) ;<br>- Identité de la personne ou de l'entreprise à laquelle la facture est adressée ;<br>- Le montant de la facture ;<br>- La période à laquelle se rapportent les services facturés ;<br>- La ventilation du coût par service (internet fixe, internet mobile, téléphonie fixe, téléphonie mobile et télévision numérique) ; | | Non | Art. 24*sexies* de la loi du 4 juillet 1962 relative à la statistique publique |

[30] En tant que CSIRT national au sens de l'article 7, § 2, de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique.

| Autorités | Données conservées sur base des art. 122 et 123 de la LCE | Données conservées sur base des art. 126 et 127 de la LCE | Données conservées sur base des art. 126/1 à 126/3 de la LCE | Base légale |
|---|---|---|---|---|
| | - Informations sur le type de connexion en termes de vitesse potentielle (pour l'internet fixe uniquement).<br><br>A l'exclusion des adresses IP (voir article 127, § 3, alinéa 3, de la LCE). | | | |
| Les services d'urgence offrant de l'aide sur place[31] et les centrales de gestion du service médical d'urgence et des services de police offrant de l'aide à distance | Oui | Oui | Oui | Art. 107, §2 et 107, § 4, de la LCE[32] |

Des informations plus détaillées se trouvent dans des fiches publiées sur le site internet de l'IBPT[33] (une fiche a été établie pour chaque autorité à l'exception des services d'urgence offrant de l'aide sur place).

[31] Selon l'article 107, § 1er, de la LCE, il s'agit des services suivants :
1° le service médical d'urgence ;
2° les services d'incendie ;
3° les services de police ;
4° la protection civile.

[32] Cet article oblige l'opérateur qui achemine un appel vers un de ces services d'urgence à lui fournir, lors de l'appel, le numéro d'appel du terminal, le nom de l'utilisateur final et l'endroit où l'équipement terminal se situe au moment de l'appel. Lorsqu'en raison de problème technique, ces services d'urgence ne peuvent obtenir ces données, ils pourront obtenir de l'opérateur les données conservées les plus récentes qui correspondent à ces données.

[33] https://www.ibpt.be/operateurs/interception-legale.