Autorité de protection des données
Gegevensbeschermingsautoriteit

Avis n° 32/2022 du 16 février 2022

Objet : Demandes d'avis 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)

Le Centre de Connaissances de l'Autorité de protection des données (ci-après « l'Autorité »),
Présents : Messieurs Yves-Alexandre de Montjoye et Bart Preneel ;

Vu la loi du 3 décembre 2017 *portant création de l'Autorité de protection des données*, en particulier les articles 23 et 26 (ci-après « LCA ») ;

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 demandes d'avis du Vice-Premier ministre et ministre de l'Economie et du Travail, Pierre-Yves Dermagne, reçue le 23 décembre 2021 ;

Vu les informations complémentaires reçues les 21 et 24 janvier 2022 ;

Vu la connexité de ces trois demandes d'avis ;

émet, le 16 février 2022, l'avis suivant :

I. OBJET ET CONTEXTE DE LA DEMANDE D'AVIS

1. Le Vice-Premier ministre et ministre de l'Economie et du Travail a sollicité l'avis de l'Autorité concernant les articles 7, 25,1° et 47 du projet de loi portant dispositions diverses en matière d'Economie (ci-après « le projet » ou « le projet de loi »).

2. Les dispositions en projet **trouvent leur origine dans le nouvel article 127/1 de la loi du 13 juin 2005 relative aux communications électroniques** (ci-après « la loi télécom »), tel qu'il sera inséré par le projet de loi révisé 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 (ci-après « le projet de loi révisé relatif à la collecte et à la conservation des données télécom »). Le nouvel article 127/1 de la loi télécom détermine, en effet, les catégories d'autorités[1] qui peuvent obtenir d'un opérateur des données conservées en vertu des nouveaux articles 122, 123, 126 et 127 de la loi télécom, tout en exigeant qu'une autre norme législative formelle prévoit cet accès et détermine les conditions dans lesquels il peut avoir lieu.

3. Les **trois dispositions en projet** visent ainsi à **organiser les conditions dans lesquelles l'Autorité belge de la concurrence** (ci-après « l'ABC »), les **agents de l'inspection économique** (ci-après « l'IE ») et **l'Institut national de statistiques** (ci-après l' « INS ») pourront avoir accès aux données de trafic, de localisation ou encore d'identification qui sont conservées par les opérateurs télécom en exécution des nouveaux articles 122 et suivants de la loi télécom, tels qu'ils seront modifiés à la suite de l'adoption du projet de loi relatif à la collecte et à la conservation des données télécom.

II. EXAMEN DE LA DEMANDE D'AVIS

A. Remarques préalables

4. La communication des données de trafic et de localisation à certaines autorités est une question qui est régie, entre autre, par la 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 (ci-après « la directive ePrivacy »), qui précise et

[1] Les autorités sont identifiées par le biais des finalités qu'elles poursuivent.

complète le RGPD en ce qui concerne le traitement des données à caractère personnel dans le secteur des communications électroniques[2].

5. Pour rappel, **cette directive interdit**, en principe[3], **la conservation, et *a fortiori*, la communication des données de trafic et de localisation**[4]. Aux termes de l'article 15.1 de la directive ePrivacy, **les Etats membres peuvent toutefois adopter des mesures législatives** qui **imposent aux opérateurs télécom de conserver** des données de trafic et de localisation **et de les communiquer aux autorités**, si cela s'avère **nécessaire, approprié et proportionné**, dans une société démocratique, **pour poursuivre l'un des objectifs légitimes** énoncés à l'article 15.1 de la directive ePrivacy[5]. La Cour de justice de l'Union européenne (ci-après « la CJUE ») a clarifié, à travers plusieurs arrêts[6], les exigences auxquelles de telles mesures législatives doivent répondre pour être admissibles au regard du droit européen.

6. Tout d'abord, la CJUE a indiqué, à plusieurs reprises, que **l'accès des autorités publiques aux données de trafic et de localisation conservées par les opérateurs télécom était subordonné à la condition que la conservation de ces données ait été effectuée d'une manière conforme à la directive ePrivacy**, telle que celle-ci a été interprétée par la CJUE[7]. En d'autres termes, c'est uniquement si la conservation des données de trafic et de localisation a eu lieu conformément à la directive ePrivacy qu'il possible de prévoir qu'un accès à ces données puisse être octroyé à des autorités publiques.

7. **Il appartient donc à l'auteur du projet de s'assurer que les nouvelles dispositions de la loi télécom**, qui déterminent les conditions dans lesquelles les opérateurs doivent (ou peuvent) conserver les données de trafic et de localisation, **respectent les exigences imposées par le droit européen**. À ce propos, l'Autorité **renvoie à son avis n° 108/2021** du 28 juin 2021 dans lequel elle a émis de nombreuses remarques, certaines étant tout à fait fondamentales, concernant l'avant-projet de loi relatif à la collecte et à la conservation des données télécom. **Elle insiste sur le fait que**

[2] Pour rappel, cette directive entend protéger les utilisateurs des services de communications électroniques contre les dangers pour leurs données à caractère personnel et leur vie privée résultant des nouvelles technologies.
[3] Les articles 6 et 9 précisent que les fournisseurs de réseaux publics de communications et de services de communications électroniques accessibles au public peuvent, dans certaines circonstances, et moyennant le consentement des utilisateurs ou des abonnées, traiter et conserver les données de trafic et de localisation.
[4] Voyez les articles 5 et 9 de la directive ePrivacy.
[5] Il s'agit des motifs suivants : « *pour sauvegarder la sécurité nationale — c'est-à-dire la sûreté de l'État — la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques, comme le prévoit l'article 13, paragraphe 1, de la directive 95/46/CE* ». L'Autorité relève qu'aux termes d'une jurisprudence bien établie de la CJUE que le renvoi à l'article 13 de la directive 95/46 doit se lire comme autorisant les Etats membres à prendre des mesures limitant l'obligation de confidentialité des données personnelles lorsque cette limitation est nécessaire pour atteindre l'un des objectifs énoncés à l'article 13 de la directive 95/46 (voir, par exemple, CJUE, 29 janvier 2008, Promiscuae, § 53-54). Depuis l'entrée en vigueur du RGPD, cette référence à l'article 13 de la directive 95/46 doit se lire comme une référence à l'article 23 du RGPD (voir l'article 94 du RGPD).
[6] Voyez, en particulier, CJUE, 8 avril 2014, *affaires jointes C-293/12 et C-594/12 « Digital Rights Irland et al »*; CJUE, 21 décembre 2016, *affaires jointes C-203/15 et C-698/15 « Tele2 Sverige et al »* ; CJUE, 2 octobre 2018, *affaire C-207/16 Ministerio Fiscal* ; CJUE, 2 octobre 2020, *affaires jointes C-511/18, C-512/18 et C-520/18 « Quadrature du Net et al »* ; CJUE, 2 mars 2021, *affaire C-746/18 « Prokuratuur »*.
[7] CJUE, 2 octobre 2020, *affaires jointes C-511/18, C-512/18 et C-520/18 « Quadrature du Net et al »*, § 167 ; CJUE, 2 mars 2021 ; CJUE, 2 mars 2021, *affaire C-746/18 « Prokuratuur »*, § 29.

le projet de loi doit réellement opérer le changement de perspective exigé par la jurisprudence de la CJUE et de la Cour constitutionnelle et qu'il ne peut donc pas imposer de nouvelles mesures de conservation des données de trafic et de localisation qui aboutiraient à réintroduire, *de facto*, des obligations de conservation généralisée et indifférenciée des données. À défaut, tant la conservation des données de trafic et de localisation par les opérateurs que leur communication aux autorités porteraient atteinte à la directive ePrivacy, interprétée à la lumière des articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne.

8. À ce propos, bien que l'Autorité n'ait pas procédé à une analyse approfondie de la version révisée du projet de loi relatif à la collecte et à la conservation des données télécom, qui a été annexée aux trois demandes d'avis portant sur les dispositions du projet de loi qui entendent autoriser certaines autorités à avoir accès aux données de trafic et de localisation conservées par les opérateurs, **une première lecture non-exhaustive de cette version révisée laisse entrevoir que des problèmes subsistent**[8]. Pour que les autorités publiques puissent avoir accès aux données conservées par les opérateurs télécom, tout en respectant la directive ePrivacy, **il convient, avant tout, de s'assurer que la règlementation qui encadre la conservation des données respecte les exigences imposées par la directive ePrivacy**, telle qu'elle a été interprétée par la CJUE.

9. Ensuite, conformément à l'exigence de prévisibilité, la CJUE rappelle que **la communication aux autorités nationales** des données conservées par les opérateurs **doit être encadrée par des règles claires et précises** indiquant les **circonstances et sous quelles conditions cette communication a lieu**. Cette règlementation doit prévoir des conditions matérielles et procédurales afin de garantir que l'accès aux données conservées soit limité au strict nécessaire[9] :

   - La **règlementation doit déterminer la finalité pour laquelle les autorités peuvent obtenir un accès aux données conservées** par les fournisseurs de services de communication. À cet égard, la Cour indique que **l'accès aux données ne peut, en principe, être justifiée que par l'objectif d'intérêt général pour lequel leur conservation a été imposée**[10]. Ainsi, un accès à des fins de poursuite et de sanction d'une infraction pénale ordinaire ne saurait en aucun cas être accordé lorsque leur conservation a été justifiée par l'objectif de lutte contre la criminalité grave ou, *a fortiori*, de sauvegarde de la sécurité nationale. En revanche, conformément au principe de proportionnalité, un accès à des données conservées en vue de la lutte contre la criminalité grave peut, pour autant que soient respectées les conditions matérielles et procédurales

[8] L'Autorité a, notamment, constaté que le projet de loi révisé maintenait des obligations de conservation systématique des données de trafic de l'ensemble des utilisateurs de moyens de communications électroniques de permettre d'établir la fraude ou l'utilisation malveillante du réseau ou du service ou d'identifier son auteur et son origine (nouvel article 122 § 4 de la loi télécom) et pour assurer la sécurité et le bon fonctionnement des réseaux et des services de communications électroniques, et en particulier pour détecter et analyser une atteinte potentielle ou réelle à cette sécurité, en ce compris identifier l'origine de cette atteinte (nouvel article 122 § 4/1 de la loi télécom).
[9] CJUE, arrêt du 21 décembre 2016, §§ 118-121.
[10] CJUE, arrêt du 2 mars 2021, § 31.

entourant un tel accès, être justifié par l'objectif de sauvegarde de la sécurité nationale. En outre, la Cour admet que les Etats peuvent prévoir que des données conservées d'une manière conforme aux articles 5, 6, 9 ou 15 de la Directive ePrivacy peuvent être communiquées aux autorités, dans le respect de conditions matérielles et procédurales, à des fins de lutte contre la criminalité grave ou de sauvegarde de la sécurité nationale[11]. Le législateur peut donc prévoir que les autorités peuvent accéder aux données conservées en application des nouveaux articles 122 et 123 de la loi télécom pour d'autres finalités que celles qui étaient poursuivies par leur conservation initiale, mais uniquement si ces finalités de traitement ultérieur relèvent de la sauvegarde de la sécurité nationale ou de la lutte contre la criminalité grave ou d'un autre objectif listé à l'article 15 de la directive ePrivacy qui présente un degré d'importance similaire.

- La **réglementation doit se fonder sur des critères objectifs pour définir les circonstances et les conditions dans lesquelles l'accès aux données doit être accordé**[12]. À cet égard, un accès ne saurait, en principe, être accordé, en relation avec l'objectif de lutte contre la criminalité, qu'aux données de personnes soupçonnées de projeter, de commettre ou d'avoir commis une infraction ou encore d'être impliquées d'une manière ou d'une autre dans une telle infraction. Toutefois, dans des situations particulières, telles que celles dans lesquelles des intérêts vitaux de la sécurité nationale, de la défense ou de la sécurité publique sont menacés par des activités de terrorisme, l'accès aux données d'autres personnes pourrait également être accordé lorsqu'il existe des éléments objectifs permettant de considérer que ces données pourraient, dans un cas concret, apporter une contribution effective à la lutte contre de telles activités.

- **L'accès des autorités nationales compétentes aux données conservées doit, en principe, sauf cas d'urgence dûment justifiés, être subordonné à un contrôle préalable effectué soit par une juridiction soit par une entité administrative indépendante[13]**. La décision de cette juridiction ou de cette entité doit intervenir à la suite d'une demande motivée de ces autorités[14]. Par ailleurs, la Cour a souligné que l'autorité chargée d'exercer le contrôle préalable, qu'il s'agisse d'une juridiction ou d'une entité administrative indépendante, doit avoir la qualité de tiers par rapport à celle qui demande l'accès aux données, afin que la première puisse exercer ce contrôle de manière impartiale, à l'abri de toute influence extérieure[15]. Toutefois, **la Cour constitutionnelle belge**, s'appuyant sur la jurisprudence de la Cour européenne des droits

[11] CJUE, arrêt du 6 octobre 2020, § 164-165.
[12] CJUE, arrêt du 2 mars 2021, § 50.
[13] Dans son arrêt du 2 mars 2021, la CJUE indique que la raison d'être de ce contrôle préalable (par une juridiction ou une autorité administrative indépendante) vise à assurer une conciliation *in concreto* des différents intérêts en présence, en veillant notamment à ce que les seules données qui sont communiquées sont les données qui s'avèrent strictement nécessaire pour atteindre l'objectif d'intérêt général pour lequel cet accès est accordé (voir les § 50-51).
[14] CJUE, arrêt du 21 décembre 2018, § 120 ; CJUE, arrêt du 2 mars 2021, § 51.
[15] CJUE, arrêt du 2 mars 2021, § 52.

de l'homme (ci-après « CEDH »)[16], considère que qu'il n'est **pas requis de prévoir un contrôle préalable pour accéder à de simples données d'identification**. Pour l'accès à ces données, un contrôle *a posteriori* par une instance judiciaire ou administrative indépendante suffit[17].

- **Les autorités qui ont eu accès aux données doivent en informer les personnes concernées dès le moment où cette communication n'est pas susceptible de compromettre les enquêtes menées par ces autorités**. En effet, cette information est, de fait, nécessaire pour permettre aux personnes concernées d'exercer, notamment, le droit de recours, explicitement prévu à l'article 15 § 2 de la directive ePrivacy, lu en combinaison avec le RGPD, en cas de violation de leurs droits[18]. La **Cour constitutionnelle** estime toutefois, en s'appuyant sur la jurisprudence de la CEDH, qu'il n'est **pas nécessaire que la personne concernée soit informée de l'accès à ses données d'identification**[19].

10. Afin de garantir l'effectivité du droit à la protection des données à caractère personnel et des droits conférés par la directive ePrivacy, l'Autorité estime qu'il y a lieu doit prévoir que **les métadonnées** de communications électroniques **qui auraient été obtenues de manière illégale ne peuvent être utilisés à l'encontre de la personne concernée** dans le cadre d'une procédure qui implique la prise d'une décision coercitive à son égard.

11. Dans la suite de l'avis, l'Autorité va examiner dans quelle mesure les dispositions en projet répondent à ces exigences.

12. Mais préalablement à cet examen, l'Autorité entend souligner **l'importance d'assurer une certaine transparence quant à la pratique des autorités publiques en matière d'accès et d'utilisation des métadonnées** de communications électroniques. En effet, une telle transparence est nécessaire pour permettre **un contrôle de cette pratique** par le Parlement et la société civile. Certes, le nouvel article 127/1 § 7 de la loi télécom, qui y sera inséré par le projet de loi révisé relatif à la collecte et à la conservation des données télécom, prévoit déjà que l'IBPT doit transmettre « *annuellement au ministre et au ministre de la Justice des statistiques sur la fourniture aux autorités de données conservées en vertu des articles 122, 123, 126, 126/1 et 127. Ces ministres les transmettent annuellement à la Chambre des représentants* ». Aux termes de cette nouvelle disposition de la loi télécom, « *Ces statistiques comprennent notamment : 1° les cas dans lesquels des données conservées ont été transmises aux autorités compétentes conformément aux dispositions légales applicables ; 2° le laps de temps écoulé entre la date à partir de laquelle les données ont été conservées et la date à laquelle les autorités compétentes ont demandé leur transmission ; 3° les cas dans lesquels*

[16] Voyez l'arrêt de la CEDH, Breyer c. Allemagne, 30 janvier 2020.
[17] C.C, arrêt n° 158/2021 du 18 novembre 2021, § B.14.3
[18] CJUE, arrêt du 21 décembre 2018, § 121.
[19] C.C., arrêt n° 158/2021 du 18 novembre 2021, § B.14.3

des demandes de données conservées n'ont pu être satisfaites ». L'Autorité souligne que **les informations qui doivent être communiquées en exécution de l'article 127/1 § 1 de la loi télécom ne sont pas suffisantes pour permettre au Parlement et à la société civile de contrôler le caractère strictement nécessaire et proportionné** des dispositions prévoyant les obligations de conservation et de communications de métadonnées. Il convient, dès lors, de modifier l'article 127/1 § 7 (nouveau) de la loi télécom afin d'imposer que les statistiques que l'IBPT doit transmettre annuellement au Ministre des Télécommunication et au Ministre de la Justice portent également sur (1) le nombres d'accès accordés aux différentes autorités publiques, (2) le nombre de métadonnées transmises, (3) le nombre de personnes concernées par ces accès et (4) la mesure dans laquelle ces accès se sont avérés effectivement nécessaires pour permettre aux autorité de réaliser les missions pour lesquelles ils ont été autorisés. Il convient, en outre, **d'imposer aux différentes autorités publiques habilitées à accéder aux métadonnées** de communications électroniques de **publier annuellement des statistiques** sur (1) le nombre d'accès qui leur a été accordé, (2) le nombre de métadonnées auxquelles elles ont eu accès, (3) le nombre de personnes concernées par ces accès, (4) l'impact de ces accès sur l'exercice de leurs missions (e.g. dans quelle mesure l'accès aux métadonnées a effectivement permis à l'enquête d'aboutir). **Le projet de loi sera adapté afin d'y insérer une telle obligation de publication de statistiques à charge de l'ABC, du SPF Economie et de l'INS**.

B. Accès aux données par l'Autorité belge de la concurrence (CO-A-2021-280)

13. L'**article 7 du projet de loi** insère un nouveau **paragraphe 1/1 dans l'article IV.40** du Code de droit économique (ci-après « le CDE »). Cette nouvelle disposition entend permettre à **l'auditeur de l'ABC** de demander aux opérateurs télécom **des données de trafic, des données de localisation, des données ou documents d'identification et des adresses IP** qui sont visées par le nouvel article 127/1, §§ 2 et 3, de la loi télécom[20], si cela s'avère nécessaire pour poursuivre les infractions aux articles 101 et 102 TFUE et aux articles IV.1, IV.2 et IV.2/1 et pour contrôler les concentrations. La disposition en projet précise que la poursuite de ces infractions et le contrôle des concentrations « *visent à préserver un intérêt économique important de l'Union européenne ou de la Belgique* ».

[20] Les données visées par le nouvel article 127/1 §§ 2 et 3 sont les données conservées par les opérateurs en exécution des nouveaux articles 122, 123, 126 et 127. Il s'agit, en particulier, des données de trafic nécessaires à l'établissement des factures des abonnés ou celles qui sont nécessaires aux paiements d'interconnexion, des données de trafic, y compris les données de localisation (article 122 § 2), des données de trafic nécessaires pour assurer le marketing des services de communications électroniques propres et établir le profil d'utilisation de l'abonné ou de l'utilisateur final (article 122 § 3), des données de localisation et d'autres des données de trafic nécessaires afin de détecter et d'analyser une fraude présumée ou une utilisation malveillante présumée du réseau (article 122 § 4), des données de trafic nécessaires pour assurer la sécurité et le bon fonctionnement du réseau et des services de communications électroniques (article 122 § 4/1), des données de localisation autres que les données de trafic (article 123), des données de souscription de l'abonné au service et des données nécessaires pour identifier l'utilisateur final, l'équipement terminal ou le service de communication employé (article 126) et les données et documents d'identification de l'utilisateur final (article 127).

14. L'Autorité constate que la **disposition en projet**, qui vise à encadrer les conditions dans lesquelles l'ABC peut avoir accès aux données, **répond aux exigences fondamentales identifiées par la CJUE.**

15. Tout d'abord, **la disposition en projet détermine les finalités** pour lesquelles l'ABC peut obtenir un accès aux données conservées, à savoir la poursuite des infractions aux articles 101 et 102 TFUE et aux articles IV.1, IV.2 et IV.2/1 et le contrôle des concentrations ; ce qui vise « *à préserver un intérêt économique important de l'Union européenne ou de la Belgique* ».

16. L'Autorité constate également que **la règlementation prévoit**, conformément à la jurisprudence de la CJUE, **des critères objectifs pour définir les circonstances et les conditions dans lesquelles l'accès aux données doit être accordé**. En effet, aux termes de l'article IV.40 § 1 du CDE, l'auditeur peut recueillir *« tous les renseignements nécessaires* » en vue de la réalisation de ses missions, en l'occurrence la poursuite des infractions aux articles 101 et 102 TFUE et aux articles IV.1, IV.2 et IV.2/1 et le contrôle des concentrations. En outre, cet article prévoit que la demande de renseignements doit mentionner la base juridique et le « *but* » de la demande. Selon les informations fournies par la déléguée du Ministre, **la notion de « renseignements nécessaires » doit être interprétée comme les renseignements susceptibles de permettre à l'auditeur de vérifier les présomptions d'infraction qui justifient la conduite de l'enquête**. En d'autres termes, il est prévu que l'ABC ne puissent obtenir un accès aux données de trafic, aux données de localisation, aux données d'identification et aux adresses IP que dans la mesure où ces données lui permettent de vérifier les présomptions d'infraction. **L'Autorité en prend note**.

17. En outre, la disposition en projet prévoit que « *La mise à disposition de ces données peut uniquement être réclamée sur demande motivée et avec l'autorisation préalable d'un juge d'instruction du tribunal de première instance néerlandophone de Bruxelles ou d'un juge d'instruction du tribunal de première instance francophone de Bruxelles, qui pour l'application du présent alinéa est également compétent en dehors de son arrondissement* ». **Tout accès aux données est donc subordonné à un contrôle préalable par le juge d'instruction** qui, selon les explications complémentaires fournies par la déléguée du Ministre, examinera si la demande d'accès de l'ABC est justifiée, notamment en veillant à ce que l'ABC dispose effectivement d'indices suffisamment concordants et sérieux permettant de suspecter une infraction aux articles 101 et 102 TFUE et aux articles IV.1, IV.2 et IV.2/1 et le contrôle des concentrations. **L'Autorité en prend note**.

18. Enfin, la déléguée du Ministre a indiqué à l'Autorité, à la suite d'une demande d'informations complémentaires, que le livre IV du CDE **garantit que les personnes concernées** par la communication des données **de trafic, des données de localisation, des données ou documents d'identification et des adresses IP seront informées de cette communication** dès que cette

information n'est plus susceptible de compromettre les enquêtes menées par ces autorités, c'est-à-dire au moment les parties peuvent avoir accès au dossier d'instruction. **L'Autorité en prend note**.

19. L'Autorité rappelle que pour garantir l'effectivité du droit à la protection des données à caractère personnel et les droits que les personnes concernées tirent de la directive ePrivacy, il convient de prévoir, dans le CDE, que **les métadonnées** de communications électroniques qui auraient été **obtenues de manière illégale** par l'ABC **ne peuvent être utilisés à l'encontre de la personne concernée** dans le cadre d'une procédure qui implique la prise d'une décision coercitive à son égard.

C. Accès aux données par les agents de l'inspection économique (CO-A-2021-281)

20. L'article 25, 1° du projet de loi entend compléter l'article XV.3, 5/1° du CDE afin de permettre aux **agents de l'IE d'avoir accès**, **sous certaines conditions**,

(1) À des **documents et données d'identification** conservés par les opérateurs télécom **afin de pouvoir procéder à l'identificatio**n de personnes physiques ou morales **à l'aide du numéro de téléphone de l'intéressé ou de l'adresse IP**,

(2) Aux **données de trafic, aux données de localisation et aux adresses IP**, telles que visées par l'article 127/1 de la loi du 13 juin 2005 relative aux communications électroniques et conformément à celui-ci **dans le cadre de la recherche et de la constatation d'infractions de niveau 5 ou 6**.

i) Concernant la possibilité pour les agents de l'IE d'avoir accès aux documents et données d'identifications conservés par les opérateurs télécom afin de pouvoir procéder à l'identification de personnes physiques ou morales à l'aide du numéro de téléphone de l'intéressé ou de l'adresse IP

21. La **disposition en projet** entend permettre aux agents de l'IE, chargés de rechercher et de constater les infractions au CDE, d'avoir **accès aux documents et données d'identification** conservés par les opérateurs télécom **afin de pouvoir identifier des personnes** physiques ou morales **à l'aide d'un numéro de téléphone** ou **d'une adresse IP**. Il s'agit, donc, d'imposer aux opérateurs de communiquer aux agents de l'IE les données d'identification :
- De la personne titulaire du numéro de téléphone au moyen duquel une infraction au CDE aurait été commise,
- De la personne titulaire d'un contrat de service d'accès à internet à qui était attribuée l'adresse IP qui a été identifiée comme étant celle attribuée à l'appareil connecté à internet au moyen duquel une infraction au CDE aurait été commise.

22. Tout d'abord, l'Autorité relève qu'aux termes de la jurisprudence de la CJUE, le **fait pour une autorité publique d'accéder aux documents et données d'identification** conservés par un opérateur télécom **à la seule fin de l'identification** de l'utilisateur concerné constitue **une ingérence** dans le droit à la vie privée **qui ne saurait être qualifiée de « grave »**. Dès lors, la CJUE admet qu'une telle **ingérence est susceptible d'être justifiée par un objectif de prévention, de recherche, de détection et de poursuite d'infractions en général**, sans qu'il soit nécessaire que ces infractions soient qualifiées de « graves »[21]. La CJUE a ainsi, notamment, jugé que l'accès d'autorités publiques aux données visant à l'identification des titulaires de cartes SIM activées avec un téléphone mobile volé, telles que les nom, prénom et, le cas échéant, l'adresse de ces titulaires peut être avoir lieu afin de rechercher, de détecter et de poursuivre des infractions, sans que celles-ci doivent être qualifiées de « graves »[22], à condition toutefois que l'accès à ces données soit soumis au strict respect des conditions matérielles et procédurales devant régir l'utilisation de ces données. L'Autorité y reviendra.

23. Il ressort très clairement de la jurisprudence européenne qu'une mesure législative, qui vise à permettre aux agents de l'IE d'obtenir des documents et données d'identification conservés par un opérateur télécom afin de pouvoir identifier l'utilisateur concerné **à partir d'un numéro de téléphone** qu'ils fournissent à l'opérateur, constitue une mesure appropriée, nécessaire et proportionnée, **à condition toutefois que cet accès respecte les autres conditions matérielles et procédurales devant régir l'utilisation de ces données** (*cf. infra*).

24. La question peut sembler, à première vue, **plus délicate** concernant **la possibilité d'obtenir des documents et données d'identification conservés par un opérateur à partir d'une adresse IP** communiquée par les agents de l'IE. En effet, pour que les opérateurs puissent identifier la personne à laquelle cette adresse était attribuée à un certain moment, et transmettre ensuite les documents et données d'identifications aux agents de l'IE, il est nécessaire que les adresses IP soient conservées au-delà de leur durée d'attribution. Or, dans son arrêt du 6 octobre 2020, la CJUE a jugé qu'une mesure législative ne peut imposer une obligation de conservation généralisée et indifférenciée des adresses IP attribuées à la source d'une connexion que dans le cadre de la lutte contre la criminalité grave (ou afin d'atteindre l'un des objectifs énoncés à l'article 15 de la directive ePrivacy présentant un degré d'importance similaire), étant donné la gravité de l'ingérence dans le droit à la vie privée causé par une conservation généralisée et indifférenciée des adresses IP attribuées à la source d'une connexion[23]. Toutefois, comme la CJUE le reconnait elle-même, dans le cas d'une infraction commise en ligne, l'adresse IP attribuée à la source d'une connexion peut constituer le seul moyen d'investigation

[21] Voyez, notamment, CJUE, 6 novembre 2020, § 157 et 158.
[22] CJUE, 2 octobre 2018, §§ 48-63.
[23] La gravité de l'ingérence est justifiée en raison du fait que « *les adresses IP [peuvent] être utilisées pour effectuer notamment le traçage exhaustif du parcours de navigation d'un internaute et, par suite, de son activité en ligne, ces données permettent d'établir le profil détaillé de ce dernier* » (§ 153).

permettant l'identification de la personne à laquelle cette adresse était attribuée au moment de la commission de cette infraction[24]. Dans ces circonstances, l'**Autorité estime que la communication des documents et des données d'identification** de l'abonné que l'opérateur a identifié **à partir d'une adresse IP** qui lui a été attribuée à un moment donné, peut constituer une **mesure nécessaire, appropriée et proportionnée**, **à condition** toutefois que cette **communication soit** soumise au strict respect **des conditions matérielles et procédurales** devant régir l'utilisation de ces données (*cf. infra*).

25. À ce propos, l'Autorité remarque tout d'abord que, conformément à la jurisprudence de la CJUE, **la réglementation définit les circonstances et les conditions dans lesquelles l'accès aux données d'identification peut être accordé**[25]. En effet, l'article XV.3, 5/1°, alinéa 1er, du CDE dispose que les agents de l'IE peuvent « *se faire produire par toute personne, gratuitement et sur première réquisition, tous les renseignements permettant l'identification des personnes faisant l'objet d'une enquête et des personnes impliquées dans des flux financiers et de données nécessaires dans le cadre de l'enquête* ». La disposition en projet s'insère, à la suite de cet alinéa, indiquant que « *Pour ce qui concerne l'identification de personnes physiques ou morales à l'aide du numéro de téléphone de l'intéressé ou de l'adresse IP, ils peuvent […] demander la mise à disposition de documents et de données d'identification à l'opérateur […]* ».

26. Ensuite, l'Autorité constate que la disposition en projet prévoit un contrôle préalable interne à l'administration puisque toute demande d'accès aux données et documents d'identification doit (1) être validée par le fonctionnaire dirigeant ou son représentant et (2) être autorisée par d'autres agents de l'IE que ceux qui ont formulés la demande à qui il est demandé de contrôler la nécessité et la proportionnalité de la mesure. Aucun contrôle préalable par une juridiction ou une autorité administrative indépendante n'est donc prévu en l'espèce. Bien qu'il ne soit pas évident à la lecture de la jurisprudence de la CJUE que l'absence d'un tel contrôle préalable soit admissible au regard du droit européen, l'Autorité note que la Cour constitutionnelle, qui s'appuie sur la jurisprudence de la CEDH, juge qu'il n'est pas requis d'organiser une supervision a priori pour accéder à de simples données d'identification. Dans ces conditions, **l'Autorité prend note de la décision** de l'auteur du projet **de ne pas prévoir de contrôle préalable à la communication des documents et des données d'identification** de l'abonné que l'opérateur a identifié à partir d'une adresse IP ou d'un numéro de téléphone.

27. Toutefois, l'Autorité insiste sur le fait qu'il est essentiel que les mesures de contrôle interne permettent de veiller à ce que les agents de l'IE n'accèdent aux données et documents d'identification de personnes qui ont été identifiées à l'aide d'un numéro de téléphone ou d'une adresse IP que si, à la

[24] CJUE, 6 octobre 2020, § 154.
[25] CJUE, arrêt du 2 mars 2021, § 50.

lumière des faits, ils disposent d'un faisceau d'indices concordants et sérieux que ces données d'identifications rendraient possibles ou accélèreraient la recherche et le constat des infractions au CDE. En outre, l'Autorité souligne que **l'identification d'une personne à partir d'un numéro de téléphone ou d'une adresse IP permet d'identifier la personne qui est abonnée au service de communications électroniques en question**, **laquelle ne correspondra pas nécessairement à la personne ayant commis l'infraction ou étant impliquée dans celle-ci**. Il est essentiel que les agents de l'IE aient conscience qu'il peut être impossible pour la personne identifiée qui ne serait pas impliqué dans l'infraction d'en rapporter la preuve (négative). L'Autorité indique dès lors qu'en fonction des circonstances de la cause, des actes d'investigations complémentaires à l'identification de la personne titulaire du numéro de compte ou du contrat d'accès à internet, pourront s'avérer nécessaire pour corroborer les suspicions d'infractions réalisées à l'aide d'un moyen de communications électroniques.

ii) Concernant la possibilité pour les agents de l'IE d'avoir accès aux données de trafic, aux données de localisation et aux adresses IP dans le cadre de la recherche et de la constatation d'infractions de niveau 5 ou 6

28. Le nouvel article XV.3, 5/1°, dernier alinéa, du CDE, inséré par l'article 25, 1° du projet de loi, entend permettre aux agents de l'IE, chargés de rechercher et constater des infractions au CDE, d'avoir accès, sous certaines conditions, aux données de trafic, données de localisation et adresses IP conservées par les opérateurs en exécution des (nouveaux) articles 122, 123, 126, 126/1 et 127 de la loi télécom. La disposition en projet précise que « *Les données de trafic et de localisation peuvent uniquement être demandées pour la recherche et la constatation d'infractions de niveau 5 ou 6* », c'est-à-dire les infractions sanctionnées des peines les plus sévères.

29. L'Autorité constate que la **disposition en projet**, qui vise à encadrer les conditions dans lesquelles les agents de l'IE peuvent avoir accès aux données de trafic, aux données de localisation et aux adresses IP, telles que visées par l'article 127/1 de la loi télécom, **répond essentiellement aux exigences fondamentales identifiées par la CJUE.**

30. Tout d'abord, la **disposition en projet** – lue en combinaison avec l'article XV.2 du CDE – détermine les finalités pour lesquelles les agents de l'IE peuvent obtenir un accès aux données conservées, à savoir la recherche et la constatation d'infractions au CDE de niveau 5 ou 6 (à l'exception de celles reprises dans le Livre IV et dans ses arrêtés d'exécution). La possibilité de ne pouvoir accéder aux données de trafic et de localisation uniquement pour la recherche et la constatation d'infractions de niveau 5 ou 6, c'est-à-dire les infractions considérées comme étant les plus graves, est conforme à la jurisprudence de la CJUE. **Toutefois, il convient de lever tout ambiguïté dans la disposition en projet quant au fait que les adresses IP ne pourront également être communiquées aux**

agents de l'IE qu'en vue de rechercher et de constater des infractions au CDE de niveau 5 ou 6.

31. L'Autorité constate que la disposition en projet vise les « *les adresses IP, telles que visées par l'article 127/1 de la loi du 13 juin 2005 relatives aux communications électroniques* ». Cette disposition de la loi télécom renvoie aux données conservées en exécution des articles (nouveaux) 126 et 127. Le nouvel article 126 porte sur la conservation des données de souscription et des données nécessaires pour identifier l'utilisateur final, l'équipement terminal ou le service de communications électroniques employé. Il délègue au Roi le pouvoir d'énumérer les données précises qui doivent être conservées par les opérateurs, mais il précise que ces données ne peuvent pas porter *« sur le contenu des communications électroniques, ni sur des métadonnées de communications électroniques qui donnent des informations sur le destinataire de la communication, comme l'adresse IP du destinataire de la communication ou sur la localisation de l'équipement terminal* »[26]. Aux termes du nouvel article 126 de la loi télécom, le Roi ne peut imposer que la conservation des adresses IP attribuées à la source de la connexion. **Les agents de l'IE ne peuvent donc avoir accès, en exécution du nouvel article XV.3, 5/1°, dernier alinéa, du CDE, qu'aux adresses IP attribuées à la source de la connexion, à l'exclusion des adresses IP du destinataire de la communication**. Il convient, en outre, de souligner que le nouvel article 127/1 § 3, alinéa 4, de la loi télécom précise que « *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* »[27]. Cette limitation quant au type d'adresse IP qui peuvent être communiquées aux autorités (à savoir uniquement les adresses IP attribuées à la source de la connexion et uniquement dans la mesure où l'autorité qui sollicite l'accès ne dispose pas, par ailleurs, d'information qui lui permettrait de tracer le parcours de navigation d'un utilisateur final sur Internet) est tout à fait essentielle pour assurer la proportionnalité de l'ingérence causé dans le droit au respect de la vie privée par la conservation et l'accès aux métadonnées.

32. Conformément à la jurisprudence de la CJUE, **la réglementation définit les circonstances et les conditions dans lesquelles l'accès aux données d'identification doit être accordé**[28]. En effet, l'article XV.3, 5/1°, alinéa 1er, du CDE dispose que les agents de l'IE peuvent « *se faire produire par toute personne, gratuitement et sur première réquisition, tous les renseignements permettant*

[26] C'est l'Autorité qui souligne

[27] C'est l'Autorité qui souligne

[28] CJUE, arrêt du 2 mars 2021, § 50.

l'identification des personnes faisant l'objet d'une enquête et des personnes impliquées dans des flux financiers et de données nécessaires dans le cadre de l'enquête ». C'est donc dans, sous la stricte condition, que les données s'avèrent nécessaires dans le cadre de l'enquête que les agents de l'IE pourront y avoir accès.

33. En outre, la disposition en projet prévoit que *« Les données de trafic, les données de localisation et les adresses IP, telles que visées par l'article 127/1 de la loi du 13 juin 2005 relative aux communications électroniques et conformément à celui-ci, peuvent uniquement être réclamées sur demande motivée et avec l'autorisation préalable d'un juge d'instruction du tribunal de première instance néerlandophone de Bruxelles ou d'un juge d'instruction du tribunal de première instance francophone de Bruxelles* ». Tout accès aux données est donc subordonné, conformément à la jurisprudence de la CJUE, à un contrôle préalable par le juge d'instruction. **L'Autorité en prend note**. Elle **rappelle que le juge d'instruction est tenu de n'accorder l'accès** aux données de trafic et de localisation **que si, à la lumière des faits, il existe un faisceau d'indices concordants et sérieux** que les données à caractère personnel recherchées rendraient possible ou accéléraient la recherche et le constat des infractions au CDE.

34. Enfin, **il appartient à l'auteur du projet de loi de s'assurer que le cadre règlementaire garantit que les personnes concernées** par la communication de leurs données d'identification **seront informées de cette communication** dès que cette information n'est plus susceptible de compromettre les enquêtes menées par ces autorités. Si cela n'est pas déjà prévu en droit positif, le cadre règlementaire sera adapté afin que les personnes concernées disposent des informations requises.

35. L'Autorité rappelle que, pour garantir l'effectivité du droit à la protection des données à caractère personnel et les droits que les personnes concernées tirent de la directive ePrivacy, il convient de prévoir que les **métadonnées** de communications électroniques qui auraient été **obtenues de manière illégale** par les agents de l'IE **ne peuvent être utilisés à l'encontre de la personne concernée** dans le cadre d'une procédure qui implique la prise d'une décision coercitive à son égard.

D. Accès aux données par l'Institut national de statistiques (CO-A-2021-283)

36. L'article 47 du projet de loi entend insérer un nouvel article 24*sexies* dans la loi du 4 juillet 1962 relative à la statistique publique (ci-après « la loi du 4 juillet 1962 »). Cette **nouvelle disposition** entend **autoriser l'INS**, « ***à des fins statistiques, à procéder, au traitement et à l'étude de données***

***conservées par les opérateur**s, conformément à l'article 127/1, § 2, 10° de la loi du 13 juin 2005 relative aux communications électroniques* ».

37. Le nouvel article 127/1 § 2, 10°, de la loi télécom, qui entrera en vigueur après l'adoption du projet de loi relatif à la collecte et à la conservation des données télécom, entend autoriser « *les autorités qui sont légalement habiliter à réutiliser des données à des fins de recherche scientifique ou historique ou à des fins statistiques* » à obtenir « *des données conservées en vertu des articles 122 et 123 […] pour autant que prévu et par et aux conditions fixées par une norme législative formelle* ».

38. Les **données conservées en vertu des (nouveaux) articles 122 et 123 de la loi télécom sont nombreuses**. Il s'agit, en particulier, des données de trafic nécessaires à l'établissement des factures des abonnés ou celles qui sont nécessaires aux paiements d'interconnexion, des données de trafic, y compris les données de localisation (article 122 § 2), des données de trafic nécessaires pour assurer le marketing des services de communications électroniques propres et établir le profil d'utilisation de l'abonné ou de l'utilisateur final (article 122 § 3), des données de localisation et d'autres des données de trafic nécessaires afin de détecter et d'analyser une fraude présumée ou une utilisation malveillante présumée du réseau (article 122 § 4), des données de trafic nécessaires pour assurer la sécurité et le bon fonctionnement du réseau et des services de communications électroniques (article 122 § 4/1) et des données de localisation autres que les données de trafic (article 123).

39. Comme le relève, à juste titre, l'Exposé des motifs, l'article 5.1.b) du RGPD impose que les données à caractère personnel soient « *collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités* », tout en reconnaissant que « *le traitement ultérieur […] à des fins statistiques n'est pas considéré, conformément à l'article 89, paragraphe 1, comme incompatible avec les finalités initiales* ». Aux termes de l'article 89.1 du RGPD, le traitement à des fins statistiques doit être soumis à des garanties appropriées pour les droits et libertés des personnes concernées.

40. Le **traitement, par l'INS, à des fins statistiques, des données conservées** par les opérateurs conformément à l'article 127/1 § 2, 10° de la loi télécom doit donc **être considéré** comme étant, en principe, **compatible avec les finalités pour lesquelles ces données ont été initialement conservées**[29].

[29] Rappelons que la CJUE a jugé, dans plusieurs arrêts, que la règlementation doit déterminer la finalité pour laquelle les autorités peuvent obtenir un accès aux données conservées par les fournisseurs de services de communication, étant entendu que cet accès ne peut, en principe, être justifiée que par l'objectif d'intérêt général pour lequel leur conservation a été imposé. Bien que la CJUE ne se soit pas encore prononcé sur une règlementation qui accorde un accès aux données conservées par les opérateurs à des fins statistiques, l'Autorité relève qu'il n'apparait, en principe pas contraire au RGPD ou à la directive ePrivacy d'autoriser, à des fins statistiques, la communication des données de trafic conservées par les fournisseurs de services de communication, quand bien même la conservation des données n'a pas été initialement imposée pour des finalités statistiques. En effet, le RGPD met en place un « régime de faveur » pour les traitements ultérieurs à des fins statistiques.

41. L'Autorité relève, en outre, que la loi du 4 juillet 1962 prévoit, conformément à l'article 89.1 du RGPD, plusieurs garanties appropriées pour les droits et libertés des personnes concernées[30].

42. L'Autorité rappelle que **le traitement des données de trafic et de localisation** doit, non seulement **respecter** les exigences imposées par **le RGPD**, mais également celles qui découlent de la **directive ePrivacy** qui, rappelons-le, précise et complète le RGPD en ce qui concerne le traitement des données à caractère personnel dans le secteur des communications électroniques[31].

43. Cette **directive** impose, entre autres, de **garantir la confidentialité** des données relatives au trafic afférentes aux communications effectuées au moyen d'un réseau public de communications et de services de communications électroniques accessibles et des données de localisation autres que les données de trafic.

44. **Le nouvel article 24*sexies*** de loi du 4 juillet 1962, introduit par l'article 47 du projet de loi, **entend déroger au principe de la confidentialité** des données de trafic et de localisation. De telles dérogations ne sont admissibles **que dans les limites prévues à l'article 15.1 de la directive ePrivacy**. Pour rappel, l'article 15.1 de la Directive ePrivacy prévoit que : « *les États membres peuvent adopter des mesures législatives visant à limiter la portée des droits et des obligations prévus aux articles 5 et 6, […] et à l'article 9 de la présente directive lorsqu'une telle limitation constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale — c'est-à-dire la sûreté de l'État — la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques, comme le prévoit l'article 13, paragraphe 1, de la directive 95/46/CE […]* ». Aux termes d'une jurisprudence bien établie de la CJUE, il convient de lire le renvoi à l'article 13 de la directive 95/46 comme autorisant les Etats membres à prendre des mesures limitant l'obligation de confidentialité des communications électroniques et des données de trafic et de localisation y afférentes lorsque cette limitation est nécessaire pour atteindre l'un des objectifs énoncés à l'article 13 de la directive 95/46[32]. Depuis l'entrée en vigueur du RGPD, cette référence à l'article 13 de la directive 95/46 doit se lire comme une référence à l'article 23 du RGPD[33].

45. Il ressort de l'Exposé des motifs du projet de loi et des informations complémentaires reçues par le délégué du Ministre que **l'objectif poursuivi** par l'article 47 du projet de loi est de permettre à l'INS

[30] Cette loi du 4 juillet 1962, prévoient des garanties pour les personnes concernées, comme l'obligation de respecter les principes de licéité et de loyauté, de finalité, de proportionnalité et d'impartialité, d'objectivité et d'indépendance professionnelle ou encore l'obligation de garantir un secret statistique. Par ailleurs, l'Autorité rappelle qu'elle a examiné, dans son avis n° 127/2021 du 28 juillet 2021, un avant-projet de loi modifiant la loi du 4 juillet 1962. Dans cet avis, l'Autorité formulé plusieurs remarques et recommandation de modifications afin que la loi relative à la statistique publique prévoie des garanties appropriées adéquates pour les personnes concernées.
[31] Article 1.2 de la directive ePrivacy. L'Autorité relève encore que, contrairement au RGPD, la directive ePrivacy entend également protéger les intérêts légitimes des abonnés qui sont des personnes morales (article 1er de la directive ePrivacy).
[32] Voir, par exemple, CJUE, 29 janvier 2008, Promiscuae, § 53-54
[33] Voir l'article 94 du RGPD

d'avoir accès aux données conservées par les opérateurs télécom pour **établir des statistiques relatives à l'utilisation des technologies de l'information et de la communication par les ménages et les entreprises**, comme le requièrent les deux règlements européens suivants : le règlement 2019/1700 du Parlement européen et du Conseil du 10 octobre 2019 établissant un cadre commun pour des statistiques européennes relatives aux personnes et aux ménages fondées sur des données au niveau individuel collectées à partir d'échantillons (ci-après « le règlement 2019/1700 ») et le règlement 2019/2152 du Parlement européen et du Conseil du 27 novembre 2019 relatif aux statistiques européennes d'entreprises (ci-après « le règlement 2019/1952 »).

46. Le délégué du Ministre a indiqué, à la suite d'une demande d'informations complémentaires, **que la production de statistiques de qualité** concernant l'utilisation des technologies de l'information et de la communication par les ménages et les entreprises **nécessitait de collecter des informations tant auprès des personnes concernées** (par le biais d'enquêtes) **qu'auprès des opérateurs télécom**. En effet, d'une part, certaines informations ne peuvent être fournies que par les personnes concernées par le biais d'enquête (par exemple, les données concernant l'usage d'internet, le recours à l'*e-commerce* ou aux services d'e-*government*). Les règlements d'exécution du règlement 2019/1700, à l'instar du règlement d'exécution 2021/1223 de la Commission du 27 juillet 2021, imposent d'ailleurs que les données pertinentes soient collectées par le biais d'une enquête. D'autre part, l'exactitude données récoltées par le biais d'enquêtes peut s'avérer problématique, en particulier, concernant les éléments suivants :

> « De *antwoorden van de gezinnen/ondernemingen zijn fout of de gezinnen zijn het antwoord schuldig omdat de informatie te technisch is: De gezinnen/ondernemingen hebben het door de WIFI-technologie moeilijk om een onderscheid te maken tussen vast internet en mobiel internet. Ze denken ten onrechte dat WIFI (draadloos) gelijk staat met mobiele internet waardoor we het aandeel gezinnen met vast internet onderschatten. Door de informatie van de telecomoperatoren te koppelen aan de gegevens van de enquête kunnen we dit corrigeren op het niveau van een case (microniveau). Verder is het voor de gezinnen ook moeilijk om correcte informatie te geven over bijvoorbeeld de snelheid van de internetverbinding of de technologie die er mee samenhangt (vb. klassieke internetconnectie of ADSL).*
>
> *De resultaten geven geen correct beeld van de volledige bevolking: Bij de enquête werkt ongeveer de helft van de gezinnen die via een steekproef getrokken worden mee. Het al dan niet deelnemen aan een enquête hangt samen met de leeftijd, het geslacht en de socio-economische status. Mensen die tot een lagere sociale klasse behoren, doen minder mee aan enquêtes en de kans is groot dat deze*

> *profielen ook minder dan de andere toegang hebben tot internet. Ook taalbarrières, technische barrières (deelnemers begrijpen niet altijd wat wordt bedoeld met "vast", "breedband", enz.) kunnen een vertekening van de resultaten veroorzaken. Om daarvoor te kunnen corrigeren, dienen we voor de totale bevolking (minstens op gezinsniveau) informatie te hebben over de toegang tot internet en het profiel. Dit laat toe om de resultaten te herwegen (kalibreren) en zo op macro niveau te corrigeren ».*

47. L'Autorité **prend note** du fait que les données conservées par les opérateurs peuvent participer à assurer la qualité des données à partir desquelles les statistiques concernant l'utilisation des technologies de l'information et de la communication sont établies.

48. L'Autorité estime que l'établissement de telles statistiques, conformément aux règlements n° 2019/1700 et n° 2019/1952, peut être qualifié d'« *objectif important d'intérêt public général de l'Union ou d'un Etat membre* »[34], qui est un des objectifs permettant, aux termes de l'article 15.1 de la directive ePrivacy lu à la lumière de l'article 23.1.e) du RGPD, de limiter l'obligation de confidentialité des données de trafic et de localisation afférentes aux communications électroniques, à condition que cette limitation apparaissent, en outre, comme étant nécessaire, appropriée et proportionnée.

49. Afin d'assurer une **prévisibilité suffisante** à la règlementation, **il convient d'inscrire**, dans le nouvel article 24*sexies*, introduit par l'article 47 du projet, **la finalité statistique concrète** pour laquelle l'INS peut solliciter un accès aux données conservées par les opérateurs télécom visées par le nouvel article 127/1 § 2 de la loi télécom. Le **projet sera adapté** en conséquence.

50. Par ailleurs, l'Autorité constate, à ce propos, que **la disposition en projet permet actuellement à l'INS d'avoir accès à toutes les données** conservées en exécution des articles 122 et 123 de la loi télécom, **et pas uniquement aux données nécessaires** afin de lui permettre de réaliser des statistiques portant sur l'utilisation des technologies de l'information et de la communication. Or, comme l'Autorité l'a déjà relevé plus haut dans son avis, les données conservées en exécution des articles 122 et 123 de la loi télécom sont très nombreuses et variées et elles sont dès lors, comme la CJUE l'a souligné à plusieurs reprises, « *susceptibles de révéler des informations sur un nombre*

[34] Plusieurs considérants des règlements n° 2019/1700 et n° 2019/1952 soulignent l'importance de disposer de statistiques fiables pour permettre aux autorités de mettre en place des politiques responsables. Voyez, par exemple, le premier considérant du règlement 2019/1700 : « Les données et les indicateurs statistiques constituent l'épine dorsale de politiques responsables fondées sur des données probantes. Dans le contexte de la stratégie Europe 2020 et du renforcement de la gouvernance économique, les indicateurs sociaux jouent un rôle essentiel pour éclairer et soutenir les principales priorités de l'Union. Ces priorités concernent en particulier la croissance inclusive et durable et la création d'emplois ; la cohésion sociale ; la réduction de la pauvreté, des inégalités et de l'exclusion sociale ; l'inclusion des personnes handicapées et l'égalité de traitement ; et les compétences, la mobilité et l'économie numérique. En particulier, les indicateurs sociaux sont nécessaires pour fournir une base statistique solide pour l'élaboration et le suivi des politiques menées par l'Union et les États membres en vue de s'atteler à ces priorités. Des statistiques de qualité sont nécessaires pour améliorer la résilience et les objectifs de cohésion de l'Union, et préserver ses niveaux de bien-être. Des données fiables sont également d'une grande importance pour faire rempart aux fausses informations »

important d'aspects de la vie privée des personnes concernées, y compris des informations sensibles, telles que l'orientation sexuelle, les opinions politiques, les convictions religieuses, philosophiques, sociétales ou autres ainsi que l'état de santé […]. Prises dans leur ensemble, lesdites données peuvent permettre de tirer des conclusions très précises concernant la vie privée des personnes dont les données ont été conservées, telles que les habitudes de la vie quotidienne, les lieux de séjour permanents ou temporaires, les déplacements journaliers ou autres, les activités exercées, les relations sociales de ces personnes et les milieux sociaux fréquentés par celles-ci. En particulier, ces données fournissent les moyens d'établir le profil des personnes concernées, information tout aussi sensible, au regard du droit au respect de la vie privée, que le contenu même des communications »[35].

51. **Autoriser l'INS à avoir accès à toutes les données** de trafic et de localisation conservées par les opérateurs en exécution des nouveaux articles 122 et 123 de la loi télécom **va au-delà de ce qui est nécessaire pour permettre à l'INS d'atteindre la finalité statistique visée**. Conformément au principe de proportionnalité et de minimisation des données[36], **il convient de d'autoriser l'INS à avoir accès aux seules données nécessaires au regard de la finalité statistique poursuivie**, à savoir la production de statistiques, conformément aux règlements européens précités, concernant l'utilisation des technologies de l'information et de la communication par les ménages et les entreprises.

52. À la suite d'une demande d'informations complémentaires, le délégué du Ministre **a identifié les catégories de données** qui sont nécessaires pour que l'INS puisse atteindre la finalité statistique poursuivie :

> « *• Vast internet: het adres van een aansluiting -> De gegevens zijn nodig om de koppeling te kunnen maken met een huishouden en zo te bepalen of de leden van een huishouden toegang hebben tot vast internet.*
> *• Vast internet: de identiteit van de persoon (naam, voornaam en adres of het rijksregisternummer) of onderneming (naam en adres of KBO-nummer of BTW-nummer) die het contract heeft afgesloten -> De gegevens zijn nodig om de koppeling te kunnen maken met een huishouden en zo te bepalen of de leden van een huishouden toegang hebben tot vast internet.*
> *• Vast internet: Informatie over het type verbinding op het vlak van de potentiële snelheid (vb. Viber, …) -> De gegevens zijn nodig om bij nieuwe technologieën na te gaan welke profiele toegang hebben tot de nieuwe technologie en welke profielen uitgesloten zijn.*
> *• Mobiel internet: de identiteit van de persoon (naam- adres of het rijksregisternummer) of onderneming (naam- adres of KBO-nummer of BTW-nummer) die het contract heeft*

[35] Voyez, par exemple, CJUE, 8 avril 2014, *affaires jointes C-293/12 et C-594/12 « Digital Rights Irland* et *al »*, § 27 ; CJUE, 21 décembre 2016, *affaires jointes C-203/15 et C-698/15 « Tele2 Sverige et al »*, § 99 ; CJUE, 2 octobre 2020, *affaires jointes C-511/18, C-512/18 et C-520/18 « Quadrature du Net et al »*, § 117.
[36] Ce principe est consacré par la Charte des droits fondamentaux de l'Union européenne, le RGPD, la directive ePrivacy ainsi que par la loi du 4 juillet 1962.

afgesloten. -> De gegevens zijn nodig om de koppeling te kunnen maken met een persoon en nadien huishouden en zo te bepalen of iemand van het gezin toegang heeft tot mobiel internet.

• Informatie over de facturatie aan klanten: de identiteit van de persoon of de onderneming aan wie de factuur gericht is -> De gegevens zijn nodig om de koppeling te kunnen maken met de gezinnen die deelnamen aan het Huishoudbudgetonderzoek.

• Informatie over de facturatie aan klanten: Bedrag van de factuur, periode, de opdeling van de kostprijs per dienst (vast internet, mobiel internet, vaste telefoon, mobiele telefoon en digitale TV) -> De gegevens zijn nodig om de informatie van het Huishoudbudgetonderzoek te verrijken en zo ene beter beeld te krijgen van de uitgaven van gezinnen voor Telekomdiensten ».

53. Le **nouvel article 24*sexies*** de la loi du 4 juillet 1962, introduit par l'article 47 du projet de loi, **sera donc modifié afin d'y inscrire les catégories de données auxquelles l'INS** peut avoir accès parmi toutes les données conservées par les opérateurs en exécution des nouveaux articles 122 et 123 de la loi télécom, étant donné que celles-ci doivent être pertinentes, adéquates et limitées à ce qui est nécessaire au regard de la finalité poursuivie.

54. En outre, l'Autorité relève que la réalisation des statistiques concernant l'utilisation des technologies de l'information et de la communication par les ménages et les entreprises **ne nécessite pas de collecter les données de l'ensemble de la population**. Afin de respecter les principes de nécessité et de proportionnalité, le projet doit préciser que **la collecte doit être limitée à un échantillon représentatif de la population**. Le **projet sera adapté** en conséquence.

55. Par ailleurs, le nouvel article 24*sexies* de la loi du 4 juillet 1962, introduit par l'article 47 du projet de loi, autorise l'INS à avoir un accès permanent aux données conservées par les opérateurs télécom. À la suite d'une demande de justification concernant la nécessité d'un tel accès permanent aux données de trafic et de localisation, le délégué du Ministre a indiqué que « *Het volstaat dat Statbel 2 keer per jaar de gegevens ontvangt. Deze frequentie is noodzakelijk omdat de ICT-enquête een jaarlijkse enquête is. De veldwerkperiode van de enquête loopt van januari van het jaar tot en met augustus. De resultaten dienen eind september aan Eurostat geleverd te worden. Om dit voor te bereiden wordt er in juni al een tussentijds bestand aangemaakt met de gegevens voor de periode januari tot en met april* ».

56. À partir du moment où il suffit que l'INS puisse avoir accès aux données de trafic pertinentes deux fois par an pour pouvoir atteindre la finalité statistique poursuivie, il convient, en **application des principes de nécessité et de proportionnalité,** de prévoir que **l'INS ne peut avoir accès** aux données détenues par les opérateurs télécom **qu'à des période déterminée de l'année** (et non

tout au long de l'année). Au vu des informations fournies par le délégué du Ministre, la disposition en projet pourrait prévoir un accès aux données deux fois par an. La disposition en projet **sera adaptée en ce sens**.

57. Pour conclure, l'Autorité souligne que, si le nouvel article 24*sexies* de la loi du 4 juillet 1962, introduit par l'article 47 du projet de loi, était modifié conformément aux recommandations émises ci-dessus, la disposition en projet assurerait un juste équilibre entre les différents intérêts en présence tout en encadrant de manière suffisamment précise et prévisible les circonstances et les conditions dans lesquelles l'INS pourra avoir accès aux données télécom.

E. Remarque finale concernant l'attribution de nouvelles compétences à l'Autorité de protection des données par le projet de loi révisé relatif à la collecte et à la conservation des données télécom

58. **D'initiative**, et à titre tout à fait non-exhaustif, l'Autorité a relevé que **les articles 19 et 34 du projet de loi révisé relatif à la collecte et à la conservation des données télécom attribuait une nouvelle compétence à l'Autorité**.

59. Le nouvel article 28/1 § 2 de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges, inséré par l'article 19 du projet de loi révisé relatif à la collecte et à la conservation des données télécom, prévoit que :

> « *Lorsque c'est nécessaire pour permettre à l'Institut d'accomplir l'une de ses missions énumérées à l'article 14, paragraphe 1er, 3°, a) et g) à i), les membres du personnel de l'Institut, qui n'agissent pas dans un cadre pénal, peuvent exiger d'un opérateur de leur fournir des métadonnées de communications électroniques conservées par l'opérateur, autres que les données relatives à l'utilisateur final ou à l'abonné.*
>
> *Il soumet préalablement sa demande motivée à l'approbation de l'Autorité de protection des données, sauf cas d'urgence dûment justifié. En cas d'urgence dûment justifiée, il communique à l'Autorité de protection des données, la demande envoyée à l'opérateur*

dans délai après cet envoi. Un contrôle ultérieur est effectué par l'Autorité de protection des données »

60. Les missions *énumérées à l'article 14, paragraphe 1er, 3°, a) et g) à i),* de la loi du 17 janvier 2003 sont les suivantes : « *le contrôle du respect des normes suivantes et de leurs arrêtés d'exécution :*
a) la loi du 13 juin 2005 relative aux communications électroniques ;
[…]
g) la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques, pour ce qui concerne les secteurs des communications électroniques et des infrastructures numériques ;
h) 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, en ce qui concerne le secteur des infrastructures numériques ;
i) le Règlement (UE) 611/2013 de la Commission du 24 juin 2013 concernant les mesures relatives à la notification des violations de données à caractère personnel en vertu de la Directive 2002/58/CE du Parlement européen et du Conseil sur la vie privée et les communications électroniques »

61. Le nouvel article 62 § 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, modifié par l'article 34 du 19 du projet de loi révisé relatif à la collecte et à la conservation des données télécom, prévoit que :

« *Lorsque cela s'avère strictement nécessaire à la réalisation de ses tâches énumérées à l'article 60, a) à e), de la présente loi, le CSIRT national peut obtenir d'un opérateur, au sens de l'article 2, 11°, de la loi du 13 juin 2005 relative aux communications électroniques, des données relatives à l'utilisateur ou à l'abonné visées à l'article 2, 5° de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges ou des métadonnées de communications électroniques au sens de l'article 2, 91° de la loi du 13 juin 2005 relative aux communications électroniques conservées par celui-ci.*
Les finalités poursuivies par les tâches précitées sont :
- la prévention de menaces graves contre la sécurité publique ;
- l'examen de défaillances de la sécurité des réseaux ou de services de communications électroniques ou des systèmes d'information ;
- la prévention, la recherche et la détection des infractions commises en ligne ou par le biais d'un réseau ou service de communications électroniques, en ce compris des faits qui relèvent de la criminalité grave.
Lorsque le CSIRT national adresse à un opérateur une demande de données relatives à l'utilisateur ou à l'abonné visées à l'article 2, 5° de la loi du 17 janvier 2003 relative au

statut du régulateur des secteurs des postes et des télécommunications belges, cette demande est autorisée par le supérieur hiérarchique.

Lorsque le CSIRT national adresse à un opérateur une demande de métadonnées de communications électroniques au sens de l'article 2 de la loi du 13 juin 2005 relative aux communications électroniques autres que celles visées à l'alinéa précédent, cette demande doit faire l'objet d'un contrôle préalable par l'Autorité de protection des données créé par la loi du 3 décembre 2017.

En cas de situation urgente dûment justifiée, le CSIRT national peut se passer du contrôle préalable visée à l'alinéa précédent et solliciter directement les données. Cette demande est envoyée sans délai à l'autorité visée à l'alinéa précédent pour permettre un contrôle ultérieur.

Le directeur du CSIRT national désigne expressément les personnes habilitées à traiter ces données de communications électroniques.

Le CSIRT national informe, dans la mesure du possible, les personnes physiques concernées de l'accès à leurs données de communications électroniques lorsque cela n'est plus susceptible de compromettre le bon déroulement de ses tâches ou d'une enquête en cours et lorsque ces personnes peuvent être identifiées […] »

62. Les missions pour lesquelles le *CSIRT national,* à savoir le CCB, peut obtenir des métadonnées de communications électroniques sont les suivantes :

« a) le suivi des incidents au niveau national et international, en ce compris le traitement de données à caractère personnel lié au suivi de ces incidents ;

b) l'activation du mécanisme d'alerte précoce, la diffusion de messages d'alerte, les annonces et la diffusion d'informations sur les risques et incidents auprès des parties intéressées ;

c) l'intervention en cas d'incident ;

d) l'analyse dynamique des risques et incidents et conscience situationnelle ;

e) la détection, l'observation et l'analyse des problèmes de sécurité informatique ».

63. Tout d'abord, l'Autorité constate que l'Exposé des motifs du projet de loi révisé relatif à la collecte et à la conservation des données télécom ne donne pas d'explications ou d'informations permettant de comprendre concrètement pourquoi il peut être nécessaire que l'IBPT et le CCB aient accès à des métadonnées brutes de communications électroniques. **Il appartient au législateur de s'assurer qu'il est effectivement nécessaire que ces institutions aient accès aux métadonnées brutes de communications en vérifiant, notamment, que ces institutions ne seront pas en mesure**

de remplir leurs missions si elles n'ont pas accès aux métadonnées de communications. L'Autorité souligne, en particulier, que s'il est possible que l'IBPT et/ou le CCB remplissent leurs missions à l'aide de données anonymisées ou pseudonymisées, le projet doit prévoir que seules des données anonymisées ou pseudonymisées pourront leur être transmises[37]. Toutefois, **si et dans la mesure où l'IBPT et/ou le CCB ont pour mission de service publique de détecter, en temps réel, des cyberattaques et d'y mettre fin** (ce qui peut impliquer de devoir bloquer certains services ou certaines adresses IP afin de mettre fin, par exemple, à des attaques DDOS, de désactiver des botnets ou encore de mettre fin à des tentatives de phishing), **l'Autorité comprend que l'IBPT et/ou le CCB doivent pouvoir accéder à des métadonnées brutes de communications électronique**.

64. Toutefois, au vu de la gravité de l'ingérence qu'un tel accès cause dans le droit au respect de la vie privée, l'Autorité considère **qu'il est essentiel de tenir un débat parlementaire approfondi afin de définir les contours exacts des pouvoirs et des missions** des services de police, des **services judiciaires**, des services de renseignements, des services militaires ou encore des autorités administratives chargées de détecter et de lutter contre les cyberattaques. L'Autorité insiste pour que ce débat porte aussi sur les nécessaires limites à mettre en place concernant les traitements ultérieurs des métadonnées (par exemple par les services de renseignements ou les services de police) qui auront été collectées dans le cadre de la lutte contre cybercriminalité.

65. Ensuite, l'Autorité relève que l'exigence de prévisibilité, couplée au principe de minimisation des données consacré par l'article 5.1. c) du RGPD, requiert que les dispositions en projet **délimitent précisément quelles sont les catégories de données auxquelles l'IBPT ou le CCB peut avoir accès pour remplir quelles missions**. En d'autres termes, les dispositions en projet doivent identifier, pour chaque mission de l'IBPT et du CCB, les catégories de données auxquelles lesdites institutions doivent avoir accès pour remplir les missions de service public qui leur sont confiées, étant donné que ces catégories de données doivent être « *adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées* ».

66. En outre, au vu de la gravité des risques d'abus, l'Autorité estime, conformément à la jurisprudence européenne, que les **accès aux métadonnées** de communication qui ont lieu dans le cadre de missions **qui impliquent la prise de décisions coercitives** à l'égard des personnes concernées ou **qui impliquent une collecte massive** de métadonnées de communications électroniques, **doivent**

[37] L'Autorité souligne toutefois qu'il peut être particulièrement difficile de réellement anonymiser ou même pseudonymiser des métadonnées de communications électroniques. Il apparait, en effet, qu'il est tout à fait possible voire assez facile, de réidentifier des personnes à partir d'un set de métadonnées de communications électroniques anonymisées. Voir Ana-Maria Creţu, Federico Monti, Stefano Marrone, Xiaowen Dong, Michael Bronstein, Yves-Alexandre de Montjoye, "Interaction data are identifiable even across longperiods of time", Nature Communications, 25 janvier 2022

faire l'objet d'un contrôle indépendant par un organe qui dispose **d'une expertise technique suffisante**.

67. Par contre, pour les missions de l'IBPT et du CCB **qui n'impliquent pas la prise de décision coercitive** à l'égard des personnes concernées et **qui n'impliquent pas de collecte massive** de métadonnées de communications électroniques, en lieu et place de prévoir un système d'autorisation préalable, c'**est au législateur qu'il revient d'encadrer adéquatement cet accès** en le limitant à des données anonymisées, voire pseudonymisées tout en sécurisant l'utilisation de la clef de pseudonymisation et en prévoyant toute autre mesure adéquate[38].

68. Le projet de loi révisé relatif à la collecte et à la conservation des données télécom attribue à l'Autorité la compétence de contrôler préalablement toute communication de métadonnées de communication à l'IBPT et au CCB dans le cadre de leurs missions qui impliquent la prise de décisions coercitives à l'égard des personnes concernées. L'Autorité **a plusieurs remarques** à formuler à cet égard :

69. Tout d'abord, l'Autorité remarque que le nouvel article 62 de la loi du 7 avril 2019, introduit par le projet de loi révisé relatif à la collecte et à la conservation des données télécom prévoit que l'accès du CCB aux données de trafic et de localisation poursuit, notamment, la finalité suivante : « *la prévention, la recherche et la détection des infractions commises en ligne ou par le biais d'un réseau ou service de communications électroniques, en ce compris des faits qui relèvent de la criminalité grave* ». Dans ce contexte, **l'Autorité s'interroge sur la cohérence de lui confier la mission de contrôle préalable** visant à garantir la pertinence, la nécessité et la proportionnalité des communications de données de trafic et de localisation au CCB alors que, pour les communications de données de trafic et de localisation à toutes les autres catégories d'autorités publiques chargées d'une mission qui implique la prise de décision coercitive à l'encontre d'une personne, le contrôle préalable à la communication des métadonnées télécom est exercé par le juge d'instruction.

70. Ensuite, l'Autorité attire l'attention sur le fait **qu'elle ne dispose actuellement ni de l'expertise technique nécessaire ni des ressources nécessaires pour pouvoir effectuer cette nouvelle mission de manière effective**. Or le contrôle indépendant ne constitue une garantie appropriée pour les personnes concernées qu'à la condition qu'il soit réalisé par une autorité qui dispose de l'expertise technique suffisante. À défaut, le contrôle préalable ne sert à rien. Dans l'hypothèse où l'auteur du projet de loi révisé relatif à la collecte et à la conservation des données télécom persiste dans son intention de confier une mission de contrôle préalable à l'Autorité, il lui revient de s'assurer qu'elle disposera des moyens supplémentaires nécessaires à l'exercice de cette mission qui impliquera de devoir recruter de nouveaux profils qui disposent d'une expertise technique et juridique très

[38] Toutefois, l'Autorité est consciente de la difficulté entourant l'anonymisation des métadonnées (cf. supra)

particulière qui ne se retrouve pas parmi les membres du personnel de l'Autorité. **Dans ces conditions, l'Autorité se demande s'il n'existe pas un organe qui serait mieux équipé et mieux qualifié pour faire un tel contrôle**, voire s'il ne convient pas **de créer une nouvelle institution spécialisée pour l'exercice d'un tel contrôle.**

71. Cette question **se pose avec d'autant plus d'acuité** que le fait de confier à l'Autorité une mission de contrôle préalable à l'issue de laquelle elle est amenée à autoriser ou à refuser la communication des métadonnées de télécommunication **risque de porter atteinte à l'exigence d'impartialité qui s'impose à l'Autorité**, comme le rappelle, notamment le considérant n° 129 du RGPD[39]. Pour rappel, le principe de l'impartialité impose, non seulement que l'Autorité agisse de manière impartiale, c'est-à-dire sans « parti pris » (impartialité « subjective »), mais également qu'elle apparaisse comme agissant de manière impartiale (impartialité « objective »)[40]. **L'impartialité objective exige que le contexte dans lequel l'Autorité exerce sa compétence ne puisse susciter aucune une crainte légitime de partialité**. En confiant à l'Autorité la tâche de contrôler préalablement – et d'autoriser préalablement – les communications de métadonnées télécom à l'IBPT et au CCB, le législateur risque de mettre à mal l'impartialité de l'Autorité dans sa dimension objective. En effet, les personnes concernées par une communication de métadonnées télécom au CCB ou à l'IBPT doivent disposer, en vertu de l'article 77 du RGPD, du droit d'introduire une réclamation auprès d'une autorité de contrôle « *si elle considère que le traitement de données à caractère personnel la concernant constitue une violation du [RGPD]* ». Or, à partir du moment où l'Autorité a autorisé la communication de données préalablement à sa mise en œuvre, la personne concernée peut légitimement douter de l'impartialité de l'Autorité si celle-ci était amenée à devoir contrôler, a posteriori, ladite communication, par le biais de son service d'inspection ou de sa chambre contentieuse[41]. Ce doute quant à la capacité de l'Autorité d'exercer ses compétences coercitives de manière impartiale alors qu'elle aurait autorisé préalablement la communication de données sera d'autant plus fort à la suite de la réforme de l'Autorité puisque l'avant-projet de loi modifiant la loi du 3 décembre 2017 portant création de l'Autorité de protection des données entend renforcer le fonctionnement collégial de l'Autorité et de ses différents organes.

72. En tout état de cause, si l'auteur du projet de loi du projet de loi révisé relatif à la collecte et à la conservation des données télécom persiste à vouloir confier la mission de contrôle préalable à l'Autorité malgré les considérations et les réserves qui viennent d'être émises, **l'Autorité souligne qu'il devra s'assurer que l'Autorité sera en mesure d'exercer toute nouvelle mission qui lui est confiée**

[39] [39] « *Les pouvoirs des autorités de contrôle devraient être exercés conformément aux garanties procédurales appropriées prévues par le droit de l'Union et le droit des État membres, d'une manière impartiale et équitable et dans un délai raisonnable* ».
[40] Ceci est une application de la règle « *Justice must not only be done, it must also be seen to be done* ».

[41] Dans le même ordre d'idée, il serait tout aussi malaisé de confier à la section de législation du Conseil d'Etat un pouvoir d'autorisation préalable des décisions administratives contraignantes alors que sa section du contentieux administratif peut être amenée à évaluer, ultérieurement, à un stade contentieux, la validité de tels actes.

avec toute l'effectivité requise, à défaut de quoi la règlementation belge ne respecterait pas la directive ePrivacy, telle qu'elle a été interprété par la CJUE.

73. Enfin, l'Autorité attire l'attention sur le fait que les dispositions en projet doivent faire l'objet d'une notification auprès de la Commission européenne en exécution de l'article 51.4 du RGPD.

PAR CES MOTIFS,

L'Autorité estime que les modifications suivantes doivent être apportés au projet de loi

- Prévoir que les métadonnées de communications électroniques qui auraient été obtenues de manière illégale ne peuvent être utilisés à l'encontre de la personne concernée dans le cadre d'une procédure qui implique la prise d'une décision coercitive à son égard (cons. 10, 19, 35)

- Insérer une obligation, à charge de l'ABC, du SPF Economie et de l'INS, de publier annuellement des statistiques concernant sur (1) le nombre d'accès qui leur a été accordé, (2) le nombre de métadonnées auxquelles elles ont eu accès, (3) le nombre de personnes concernées par ces accès, (4) l'impact de ces accès sur l'exercice de leurs missions (cons. 12).

- Lever tout ambiguïté quant au fait que les adresses IP ne pourront être communiquées aux agents de l'IE qu'en vue de rechercher et de constater des infractions au CDE de niveau 5 ou 6 (cons. 30)

- Inscrire la finalité statistique concrète pour laquelle l'INS peut solliciter un accès aux données conservées par les opérateurs télécom visées par le nouvel article 127/1 § 2 de la loi télécom (cons. 44)

- Inscrire les catégories de données auxquelles l'INS peut avoir accès, étant donné que ces catégories de données doivent être pertinentes, adéquates et limitées à ce qui est nécessaire au regard de la finalité statistique concrète poursuivie (cons. 50-53).

- Préciser que, pour réaliser les statistiques relatives à l'usage des technologies de l'information et de la communication par les ménages et les entreprises, l'INS ne peut avoir accès qu'aux métadonnées pertinentes d'un échantillon représentatif de la population (et non de l'ensemble de la population) (cons. 54)

- Prévoir que l'INS ne peut avoir accès aux données détenues par les opérateurs télécom qu'à des période déterminée de l'année (et non tout au long de l'année) (cons. 55-56)

En outre, l'Autorité attire l'attention sur les éléments suivants :

- La version révisée du projet de loi relatif à la collecte et à la conservation des données télécom, qui déterminent les conditions dans lesquelles les opérateurs doivent (ou peuvent) conserver les données de trafic et de localisation, doit respecter la directive ePrivacy, à défaut de quoi l'accès à ces données ne saurait être jugé conforme à ladite directive (cons. 6-8)

- L'identification d'une personne à partir d'un numéro de téléphone ou d'une adresse IP permet d'identifier la personne qui est abonnée au service de communications électroniques en question, mais cette personne ne correspondra pas nécessairement à la personne ayant commis l'infraction ou étant impliquée dans celle-ci (cons. 26)

- Lorsqu'un juge d'instruction est saisi d'une demande d'accès aux données conservées par les opérateurs télécom, il est tenu de n'accorder l'accès à ces données que si, à la lumière des faits, il existe un faisceau d'indices concordants et sérieux que les données à caractère personnel recherchées rendraient possible ou accéléraient la recherche et le constat des infractions (cons. 33)

- L'auteur du projet de loi doit s'assurer que le cadre règlementaire garantit que les personnes concernées par la communication de leurs données seront correctement informées de cette communication dès que cette information n'est plus susceptible de compromettre les enquêtes menées par ces autorités (cons. 34)

- L'auteur du projet de loi révisé relatif à la collecte et à la conservation des données télécom doit vérifier qu'il est bien nécessaire que l'IBPT et le CCB aient accès aux données de trafic et de localisation conservées par les opérateurs télécom, en vérifiant, notamment, que ces institutions ne seront pas en mesure de remplir leurs missions si elles n'ont pas accès à ces données (cons. 63)

- Plus fondamentalement, il convient de tenir un débat parlementaire approfondi afin de définir les contours exacts des pouvoirs et des missions des différentes institutions (police, services de renseignement, défense, pouvoir judiciaire, autorités administratives) qui sont impliquées dans la lutte contre la cybercriminalité, notamment en raison du fait que les mesures qui peuvent être prises dans le cadre de la lutte contre la cybercriminalité interfèrent de manière très importante

avec le droit à la vie privée et le droit à la protection des données à caractère personnel des citoyens et citoyennes (cons. 64)

- Le cas échéant, l'auteur du projet de loi révisé relatif à la collecte et à la conservation des données télécom doit inscrire, pour chaque mission de l'IBPT et du CCB, les catégories de données auxquelles lesdites institutions doivent avoir accès pour remplir les missions de service public qui leur sont confiées, étant donné que ces catégories de données doivent être « *adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées* » (cons. 65)

- L'Autorité estime que pour les missions de l'IBPT et du CCB qui n'impliquent ni de collecter les métadonnées de communications électroniques « en masse » ni la prise de décision coercitive à l'égard des personnes concernées, en lieu et place de prévoir un système d'autorisation préalable, c'est au législateur qu'il revient d'encadrer adéquatement cet accès en le limitant à des données anonymisées, voire pseudonymisées tout en sécurisant l'utilisation de la clef de pseudonymisation et en prévoyant toute autre mesure adéquate (cons. 67).

- L'Autorité s'interroge sur la cohérence de lui confier la mission de contrôle préalable visant à garantir la pertinence, la nécessité et la proportionnalité des communications de données de trafic et de localisation au CCB alors que, pour les communications de données de trafic et de localisation à toutes les autres catégories d'autorités publiques chargées d'une mission qui implique la prise de décision coercitive à l'encontre d'une personne, le contrôle préalable à la communication des métadonnées télécom est exercé par le juge d'instruction (cons. 69).

- L'Autorité attire l'attention sur le fait qu'elle ne dispose actuellement ni de l'expertise technique nécessaire ni des ressources nécessaires pour contrôler de manière effective la pertinence, la nécessité et la proportionnalité des communications de données de trafic et de localisation vers des institutions chargées de veiller à la sécurité des réseaux (cons. 70) Elle souligne, en outre, que l'exercice d'une telle mission d'autorisation préalable risque de porter atteinte à l'exigence d'impartialité qui s'impose à elle (cons. 71). Dans ces conditions, l'Autorité se demande s'il n'existe pas un organe qui serait mieux équipé et mieux qualifié pour faire un tel contrôle, voire s'il ne convient pas de créer une institution dédiée à l'exercice d'un tel contrôle (cons. 70)

- Si l'auteur du projet de loi du projet de loi révisé relatif à la collecte et à la conservation des données télécom persiste à vouloir confier la mission de contrôle préalable à l'Autorité malgré les considérations et les réserves qui viennent d'être émises, il convient qu'il s'assure, avant de confier

cette nouvelle mission à l'Autorité, que celle-ci disposera des moyens supplémentaires nécessaires à l'exercice de cette mission supplémentaire (cons. 72).

- Les articles 19 et 34 du projet de loi révisé relatif à la collecte et à la conservation des données télécom doivent faire l'objet d'une notification auprès de la Commission européenne en exécution de l'article 51.4 du RGPD (cons. 73)

Pour le Centre de Connaissances,
(sé) Rita Van Nuffelen – Responsable a.i. du Centre de Connaissances