Nº 7526

CHAMBRE DES DEPUTES

Session ordinaire 2019-2020

P R O J E T D E L O I

portant modification de la loi modifiée du 30 mai 2005

- **relative aux dispositions spécifiques de protection de la personne à l'égard du traitement des données à caractère personnel dans le secteur des communications électroniques et**
- **portant modification des articles 88-2 et 88-4 du Code d'instruction criminelle**

* * *

(Dépôt: le 20.2.2020)

SOMMAIRE:

*

ARRETE GRAND-DUCAL DE DEPOT

Nous HENRI, Grand-Duc de Luxembourg, Duc de Nassau,

Sur le rapport de Notre Ministre des Communications et des Médias et après délibération du Gouvernement en Conseil;

Arrêtons:

Article unique.– Notre Ministre des Communications et des Médias est autorisé à déposer en Notre nom à la Chambre des Députés le projet de loi portant modification de la loi modifiée du 30 mai 2005

- relative aux dispositions spécifiques de protection de la personne à l'égard du traitement des données à caractère personnel dans le secteur des communications électroniques et
- portant modification des articles 88-2 et 88-4 du Code d'instruction criminelle.

Palais de Luxembourg, le 11 février 2020

Le Ministre des Communications et des Médias,
Xavier BETTEL

HENRI

*

TEXTE DU PROJET DE LOI

Article unique. À l'article 7 de la loi modifiée du 30 mai 2005 – relative aux dispositions spécifiques de protection de la personne à l'égard du traitement des données à caractère personnel dans le secteur des communications électroniques et – portant modification des articles 88-2 et 88-4 du Code d'instruction criminelle sont apportées les modifications suivantes :

1° Le paragraphe 5, lettre (b) est complété comme suit :

« et au paragraphe (5*bis*). »

2° Il est inséré entre les paragraphes 5 et 6 le paragraphe libellé comme suit :

« (5*bis*) En outre, en cas d'appel au numéro d'urgence unique européen 112 ainsi qu'aux numéros d'urgence déterminés par l'Institut luxembourgeois de régulation, les informations relatives à la localisation de l'appelant obtenues à partir de l'appareil mobile, si elles sont disponibles, sont mises à disposition sans tarder après l'établissement de la communication d'urgence au centre de réception des appels d'urgence le plus approprié, même lorsque l'appelant a désactivé la fonction de localisation. Ces informations sont à effacer après un délai de 24 heures au plus. »

*

EXPOSE DES MOTIFS

Des informations précises, fiables et promptes sur la localisation des personnes appelant un numéro d'urgence sont cruciales pour l'efficacité des services d'urgence, et, en définitive, elles permettent de sauver des vies. Elles améliorent le niveau de protection et la sécurité des personnes en situation d'urgence et aident les services d'urgence à exécuter leurs fonctions.

Les centres de réception des appels d'urgence peuvent recevoir, sur base de l'article 7, paragraphe 5, lettre (a), de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques, de la part des fournisseurs ou opérateurs de services de téléphonie fixe ou mobile, les données traitées dans un réseau de communications électroniques accessible au public indiquant la position géographique de l'équipement terminal d'un appelant au numéro d'appel d'urgence unique européen 112 ainsi qu'aux numéros d'urgence déterminés par l'Institut luxembourgeoise de régulation (ILR).

Lorsque l'appel est effectué à partir d'une ligne de téléphonie fixe, la localisation géographique des appelants mise à disposition des centres de réception des appels d'urgence est précise. Dans le cas des appels d'urgence émis à partir d'un téléphone mobile, la localisation géographique des appels est actuellement déterminée par la borne du réseau de téléphonie mobile traitant l'appel (« Cell ID »). Le rayon de ces bornes peut se révéler très large dans certaines configurations, en particulier dans les zones rurales[1]. Or la grande majorité de ces appels sont émis, à l'heure actuelle, au moyen d'un téléphone portable[2].

L'évolution des technologies de localisation permet d'améliorer les informations de localisation de ces appels dans le cadre des services d'urgence. En particulier, il s'agit de mettre à profit les fonctionnalités de localisation géographique des appareils de téléphonie mobile connectés via le système mondial de navigation par satellite (GNSS) ou via un réseau Wifi. En effet, ces deux méthodes de positionnement se révèlent bien plus précises que celle basée sur la localisation de la cellule du réseau de téléphonie mobile traitant cet appel[3].

L'article 7, paragraphe 5, lettre (a), de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques transpose notamment l'article 26, paragraphe 5, de la Directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communication électroniques (directive « service universel »), telle

---

1 Un rayon de 1,75 km en moyenne au Royaume-Uni, selon le rapport technique « Emergency Communications ; Advanced Mobile Location for emergency calls » de l'Institut européen des normes de télécommunications (European Telecommunications Standards Institute « ETSI », référence DTR/EMTEL-00035, 2016).

2 Sur 285 millions d'appels d'urgence dans l'Union européenne en 2015, 79% ont été émis au moyen d'un téléphone portable, d'après les données compilées par le projet pilote HELP112 de la Commission européenne sur l'élaboration, la mise en œuvre et l'exécution du transfert de données GNSS lors d'un appel au numéro européen unique d'urgence 112 aux centres de réception des appels d'urgence.

3 Un rayon de 5 mètres à l'extérieur et d'environ 25 mètres à l'intérieur, selon le rapport technique de l'ETSI précité.

que modifiée par la Directive 2009/136/CE. La Cour de Justice de l'Union européenne (« CJUE ») avait jugé que la version originale de cet article (article 26, paragraphe 3, de la Directive 2002/22/CE) :

> « impose aux États membres, sous la condition de faisabilité technique, une obligation de résultat, laquelle ne se limite pas à la mise en place d'un cadre réglementaire approprié, mais exige que les informations sur la localisation de tous les appelants au 112 soient effectivement transmises aux services d'urgence »[4].

La CJUE a rappelé récemment ce caractère et a aussi indiqué que l'article 26, paragraphe 5, de la Directive modifiée « service universel » confère aux États membres :

> « une marge d'appréciation dans la définition des critères relatifs à la précision et à la fiabilité des informations de localisation de l'appelant au 112, étant toutefois précisé que les critères qu'ils définissent doivent assurer, dans les limites de faisabilité technique, une localisation de la position de l'appelant aussi fiable et précise que nécessaire pour permettre aux services d'urgence de venir utilement à son aide […] »[5].

Aussi, l'utilisation des fonctionnalités de localisation géographique des appareils de téléphonie mobile apporterait des moyens techniques complémentaires permettant aux services d'urgence d'apporter utilement de l'aide aux appelants du 112 ainsi qu'aux numéros d'urgence déterminés par l'ILR.

L'application mobile d'alerte des populations sur téléphone mobile « GouvAlert.lu » met déjà à la disposition du Central des secours d'urgence, l'organe national unique de réception et de régulation des demandes de secours en provenance du numéro d'appel d'urgence « 112 »[6], la localisation géographique des utilisateurs qui contactent le 112 à partir de l'application. Si cette application permet d'améliorer la précision de la localisation géographique des utilisateurs en situation d'urgence, elle requiert néanmoins de leur part deux interventions : l'installation de l'application (ainsi que la connexion internet qui permet cette installation) et son utilisation.

Les nouvelles fonctionnalités de localisation géographique des appareils de téléphonie mobile connectés via le système mondial de navigation par satellite (GNSS) ou via un réseau Wifi présentent donc l'avantage d'être intégrées dans les téléphones –une mise à jour des systèmes d'exploitation de ces appareils suffit–, d'être activées automatiquement –le SMS de localisation est transmis dès que l'utilisateur appelle le numéro d'urgence « 112 » ou un autre numéro d'urgence déterminé par l'ILR – et d'apporter une localisation précise de l'appelant dès que la communication d'urgence est établie, quand cette information est disponible.

Cette évolution est consacrée par la Directive (UE) 2018/1972 du 11 décembre 2018 établissant le code des communications électroniques européen (refonte, « CCEE »), qui va abroger au 21 décembre 2020 la Directive « service universel ». En effet, l'article 109, paragraphe 6, du CCEE, prend en compte les informations obtenues à partir des téléphones portables, quand il énonce :

> « Les États membres veillent à ce que les informations relatives à la localisation de l'appelant soient mises à la disposition du [centre de réception des appels d'urgence ou « PSAP »] le plus approprié sans tarder après l'établissement de la communication d'urgence. Ces informations comprennent les informations de localisation par réseau et, si elles sont disponibles, les informations relatives à la localisation de l'appelant obtenues à partir de l'appareil mobile. »

Le présent projet de loi réaliserait donc une transposition précoce de cette disposition, en vue de permettre la localisation géographique de l'appelant, si elle est disponible, par l'appareil mobile sans autre intervention qu'un appel au numéro d'appel d'urgence unique européen 112 ou à un autre numéro d'urgence déterminé par l'ILR. Le Central des secours d'urgence dispose dès à présent de la capacité technique pour recevoir les données de localisation via l'appareil mobile. Étant donné que sa prestation pourra être améliorée grâce à cette fonctionnalité, il est opportun de ne pas attendre la fin des travaux préparatoires relatifs à la transposition du Code européen des communications électroniques. Il s'agit ainsi de procéder sans tarder à la transposition de ce point précis de cet instrument juridique qui pourra se faire par une adaptation de la loi précitée du 30 mai 2005. Cette adaptation aura aussi pour effet de renforcer la sécurité juridique en autorisant explicitement la transmission des données personnelles relatives à la géolocalisation, en conformité avec le nouveau Code européen des communications électroniques et le récent arrêt de la Cour de Justice européenne.

---

4 Arrêt du 11 septembre 2008, Commission/ Lituanie, C-274/07, point 40.

5 Arrêt du 5 septembre 2019, AW e. a. (Appels au 112), C-417/18, points 22 et 34.

6 Cf. article 23 paragraphe 3 de la loi du 27 mars 2018 portant organisation de la sécurité civile.

COMMENTAIRE DE L'ARTICLE UNIQUE

L'article proposé complète le paragraphe 5, lettre (b), en vue de réserver la possibilité à l'ILR de fixer, en cas de besoin, le format et les modalités techniques de mise à disposition des informations relatives à la localisation de l'appelant obtenues à partir de l'appareil mobile dans le cadre d'un appel au numéro d'urgence 112.

L'article proposé insère un paragraphe 5*bis* à la suite de l'article 7, paragraphe 5. Ces deux paragraphes concernent les appels d'urgence. Il a néanmoins été choisi d'ajouter un nouveau paragraphe au lieu d'insérer une lettre supplémentaire à l'article 7 paragraphe 5. En effet, le nouveau paragraphe proposé concerne une source distincte d'informations relatives à la localisation : les informations de localisation de l'appelant sont actuellement fournies, sur base des informations obtenues à partir des réseaux de télécommunication, par les fournisseurs ou opérateurs de services de téléphonie fixe ou mobile. Il s'agit donc, dans le présent projet de loi, de compléter ce dispositif, en introduisant une disposition applicable aux informations relatives à la localisation de l'appelant obtenues à partir de l'appareil mobile dont les système d'exploitation a été mis à jour en vue d'activer une fonctionnalité permettant la localisation des appelants dès que la communication d'urgence est établie. L'article proposé reprend la terminologie de l'article 109, paragraphe 6, de la Directive (UE) 2018/1972 établissant le CCEE, en effet il correspond à une transposition anticipée de celui-ci.

Il convient d'apprécier le fait que la fonctionnalité de localisation des utilisateurs soit activée en cas d'appel au numéro d'urgence unique européen 112 ou à un autre numéro d'urgence déterminé par l'ILR, quand bien même ils auraient désactivé en général la fonction de localisation sur leur téléphone mobile, à la lumière de l'article 7, paragraphe 5 de la loi modifiée du 30 mai 2005. La lecture combinée des lettres (a) et (c) de ce paragraphe suit une logique similaire selon laquelle, quand bien même l'appelant aurait empêché l'identification de sa ligne en général, celle-ci est présentée, ainsi que les données de localisation, dans le cadre d'un appel d'urgence aux numéros dédiés. Le législateur s'est prononcé en faveur de cette dérogation au droit de l'appelant d'empêcher l'indication de l'identification de la ligne appelante dès la version initiale de la loi[7], ainsi que, ultérieurement, sur la pertinence de la présentation des données de localisation dans le cadre des appels d'urgence[8]. Cette caractéristique se fonde sur la nature urgente de l'appel, sur l'impératif de rapidité de la localisation pour aider les services d'urgence à exécuter leurs fonctions et sur celui de simplicité en faveur de l'appelant en situation d'urgence qui n'a qu'une seule action à faire, celle de composer un numéro d'urgence.

L'article 109, paragraphe 6, précité de la Directive (UE) 2018/1972 établissant le CCEE englobe à la fois le Central des secours d'urgence et les autres centres de réception des appels d'urgence[9]. Aussi, les termes « au numéro d'appel d'urgence unique européen 112 ainsi qu'aux numéros d'urgence déterminés par l'Institut luxembourgeois de régulation » sont repris par analogie à l'article 4, paragraphe 3, lettre (c) et à l'article 7, paragraphe 5, lettres (a) et (c) de la loi du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques[10]. Il appartiendra à l'ILR de spécifier, en concertation avec les services concernés, les numéros d'urgence autres que le 112 auquel l'article proposé s'appliquera.

Par ailleurs, l'article proposé détermine la durée maximale de conservation des données relatives à la localisation de l'appelant obtenues à partir de l'appareil mobile à 24 heures.

Enfin, il est utile de rappeler que la réception et l'utilisation des informations relatives à la localisation des appelants, qu'elle provienne des informations de localisation par réseau et, lorsqu'elles sont disponibles, les informations relatives à la localisation des appelants obtenues à partir de l'appareil mobile doivent respecter le droit applicable en matière de traitement de données à caractère personnel, que ce soit le cadre général ou celui spécifique applicable au secteur des communications électroniques. À ce titre, il convient de lire l'article 7, paragraphe 7 sur l'information du public par les opérateurs au

---

7 Rapport de la Commission de la fonction publique, de la réforme administrative, des médias et des communications du 12 avril 2005 sur projet de loi 5184[14], p.17.

8 Rapport de la Commission l'enseignement supérieur, de la recherche, des médias, des communications et de l'espace du 4 juillet 2011 sur le projet de loi 6243[8], p. 5.

9 Cf. Article 2, points 36 à 38, de la Directive (UE) 2018/1972 du 11 décembre 2018 établissant le code des communications électroniques européen (refonte).

10 Cf. Règlement 14/182/ILR de l'Institut Luxembourgeois de Régulation du 26 août 2014 relatif à la détermination de numéros d'urgence au sens de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques.

sujet des possibilités offertes aux paragraphes précédents de ce même article, en lien avec la nouvelle possibilité ouverte par le paragraphe 5*bis* proposé par le présent projet de loi.

*

FICHE D'EVALUATION D'IMPACT

Coordonnées du projet

Intitulé du projet :	**Projet de loi portant modification de la loi modifiée du 30 mai 2005 – relative aux dispositions spécifiques de protection de la personne à l'égard du traitement des données à caractère personnel dans le secteur des communications électroniques et – portant modification des articles 88-2 et 88-4 du Code d'instruction criminelle**
Ministère initiateur :	**Ministère d'Etat – Service des Médias et des Communications**
Auteur(s) :	**Tatiana Isnard**
Téléphone :	**247-82184**
Courriel :	**tatiana.isnard@smc.etat.lu**
Objectif(s) du projet :	**Transposition anticipée de l'article 109 point 6 de la Directive (UE) 2018/1972 établissant le code des communications électroniques européen (refonte) afin d'autoriser l'utilisation des données de localisation géographique générées par les téléphones mobiles, si elles sont disponibles, seulement pour la finalité de localisation des appelants au numéro d'appel d'urgence unique européen 112 et aux numéros d'urgence déterminés par l'ILR et de permettre à l'ILR de fixer, si besoin, le format et les modalités techniques de mise à dispositions de ces données.**
Autre(s) Ministère(s)/Organisme(s)/Commune(s)impliqué(e)(s) :	
Ministère de l'Intérieur, en particulier le Corps grand-ducal d'incendie et de secours (CGDIS) Commissariat du Gouvernement à la protection des données auprès de l'État	
Date :	**09/01/2020**

Mieux légiférer

1. Partie(s) prenante(s) (organismes divers, citoyens, …) consultée(s) : Oui ☐ Non ☒
   Si oui, laquelle/lesquelles :
   /
   Remarques/Observations :
   /

2. Destinataires du projet :
   – Entreprises/Professions libérales : Oui ☐ Non ☒
   – Citoyens : Oui ☐ Non ☒
   – Administrations : Oui ☒ Non ☐

3. Le principe « Think small first » est-il respecté ? Oui ☐ Non ☒ N.a.[1] ☐
   (c.-à-d. des exemptions ou dérogations sont-elles prévues suivant la taille de l'entreprise et/ou son secteur d'activité ?)
   Remarques/Observations :
   /

1 N.a. : non applicable.

4. Le projet est-il lisible et compréhensible pour le destinataire ? Oui ☒ Non ☐

   Existe-t-il un texte coordonné ou un guide pratique, mis à jour et publié d'une façon régulière ? Oui ☒ Non ☐

   Remarques/Observations :

   Le texte coordonné de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques est annexé à l'avant-projet de loi.

5. Le projet a-t-il saisi l'opportunité pour supprimer ou simplifier des régimes d'autorisation et de déclaration existants, ou pour améliorer la qualité des procédures ? Oui ☒ Non ☐

   Remarques/Observations :

   Il permet d'améliorer la qualité des procédures de gestion des appels au numéro d'urgence 112 aux numéros d'urgence déterminés par l'ILR grâce à l'utilisation des informations relatives à la localisation de l'appelant obtenues à partir de l'appareil mobile.

6. Le projet contient-il une charge administrative[2] pour le(s) destinataire(s) ? (un coût imposé pour satisfaire à une obligation d'information émanant du projet ?) Oui ☐ Non ☒

   Si oui, quel est le coût administratif[3] approximatif total ? (nombre de destinataires x coût administratif par destinataire)

   /

7. a) Le projet prend-il recours à un échange de données inter-administratif (national ou international) plutôt que de demander l'information au destinataire ? Oui ☐ Non ☒ N.a. ☐

      Si oui, de quelle(s) donnée(s) et/ou administration(s) s'agit-il ?

      /

   b) Le projet en question contient-il des dispositions spécifiques concernant la protection des personnes à l'égard du traitement des données à caractère personnel[4] ? Oui ☒ Non ☐ N.a. ☐

      Si oui, de quelle(s) donnée(s) et/ou administration(s) s'agit-il ?

      Les données de localisation des appelants au numéro d'urgence unique européen 112 et aux numéros d'urgence déterminés par l'ILR générées par les appareils mobiles, si elles sont disponibles, dans l'unique finalité de la gestion d'un appel d'urgence au 112 et aux numéros d'urgence déterminés par l'ILR. Ces données seront transmises au centre de réception des appels d'urgence le plus approprié et conservées 24 heures au plus.

8. Le projet prévoit-il :
   - une autorisation tacite en cas de non réponse de l'administration ? Oui ☐ Non ☐ N.a. ☒
   - des délais de réponse à respecter par l'administration ? Oui ☐ Non ☐ N.a. ☒

---

2 Il s'agit d'obligations et de formalités administratives imposées aux entreprises et aux citoyens, liées à l'exécution, l'application ou la mise en oeuvre d'une loi, d'un règlement grand-ducal, d'une application administrative, d'un règlement ministériel, d'une circulaire, d'une directive, d'un règlement UE ou d'un accord international prévoyant un droit, une interdiction ou une obligation.

3 Coût auquel un destinataire est confronté lorsqu'il répond à une obligation d'information inscrite dans une loi ou un texte d'application de celle-ci (exemple: taxe, coût de salaire, perte de temps ou de congé, coût de déplacement physique, achat de matériel, etc.).

4 Loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel (www.cnpd.lu)

– le principe que l'administration ne pourra demander des informations supplémentaires qu'une seule fois ? Oui ☐ Non ☐ N.a. ☒

9. Y a-t-il une possibilité de regroupement de formalités et/ou de procédures (p.ex. prévues le cas échéant par un autre texte) ? Oui ☐ Non ☐ N.a. ☒
   Si oui, laquelle :
   /

10. En cas de transposition de directives communautaires, le principe « la directive, rien que la directive » est-il respecté ? Oui ☒ Non ☐ N.a. ☐
    Sinon, pourquoi ?
    /

11. Le projet contribue-t-il en général à une :
    a) simplification administrative, et/ou à une Oui ☐ Non ☒
    b) amélioration de la qualité réglementaire ? Oui ☐ Non ☒
    Remarques/Observations :
    /

12. Des heures d'ouverture de guichet, favorables et adaptées aux besoins du/des destinataire(s), seront-elles introduites ? Oui ☐ Non ☐ N.a. ☒

13. Y a-t-il une nécessité d'adapter un système informatique auprès de l'Etat (e-Government ou application back-office) ? Oui ☐ Non ☒
    Si oui, quel est le délai pour disposer du nouveau système ?
    /

14. Y a-t-il un besoin en formation du personnel de l'administration concernée ? Oui ☐ Non ☐ N.a. ☒
    Si oui, lequel ?
    /
    Remarques/Observations :
    /

Egalité des chances

15. Le projet est-il :
    – principalement centré sur l'égalité des femmes et des hommes ? Oui ☐ Non ☒
    – positif en matière d'égalité des femmes et des hommes ? Oui ☐ Non ☒
      Si oui, expliquez de quelle manière :
      /
    – neutre en matière d'égalité des femmes et des hommes ? Oui ☒ Non ☐
      Si oui, expliquez pourquoi :
      /
    – négatif en matière d'égalité des femmes et des hommes ? Oui ☐ Non ☒
      Si oui, expliquez de quelle manière :
      /

16. Y a-t-il un impact financier différent sur les femmes et les hommes ? Oui ☐ Non ☐ N.a. ☒
    Si oui, expliquez de quelle manière :
    /

Directive « services »

17. Le projet introduit-il une exigence relative à la liberté d'établissement soumise à évaluation[5] ? Oui ☐ Non ☐ N.a. ☒

Si oui, veuillez annexer le formulaire A, disponible au site Internet du Ministère de l'Economie et du Commerce extérieur :

www.eco.public.lu/attributions/dg2/d_consommation/d_march_int_rieur/Services/index.html

18. Le projet introduit-il une exigence relative à la libre prestation de services transfrontaliers[6] ? Oui ☐ Non ☐ N.a. ☒

Si oui, veuillez annexer le formulaire B, disponible au site Internet du Ministère de l'Economie et du Commerce extérieur :

www.eco.public.lu/attributions/dg2/d_consommation/d_march_int_rieur/Services/index.html

*

FICHE FINANCIERE

Le projet de loi sous rubrique n'a pas d'incidence financière sur le budget de l'État.

*

5 Article 15, paragraphe 2 de la directive « services » (cf. Note explicative, p. 10-11)

6 Article 16, paragraphe 1, troisième alinéa et paragraphe 3, première phrase de la directive « services » (cf. Note explicative, p. 10-11)

TEXTE COORDONNE

LOI DU 30 MAI 2005

– relative aux dispositions spécifiques de protection de la personne à l'égard du traitement des données à caractère personnel dans le secteur des communications électroniques et

– portant modification des articles 88-2 et 88-4 du Code d'instruction criminelle.

Art. 1er. Champ d'application

Sous réserve des dispositions générales concernant la protection des personnes à l'égard du traitement des données à caractère personnel ou régissant les réseaux et services de communications électroniques, les dispositions suivantes s'appliquent spécifiquement au traitement de ces données à caractère personnel dans le cadre de la fourniture de services de communications électroniques accessibles au public sur les réseaux de communications publics *(Loi du 28 juillet 2011)* « y compris les réseaux de communications publics qui prennent en charge les dispositifs de collecte de données et d'identification ».

Art. 2. Définitions

Aux fins de la présente loi on entend par:

(a) «abonné»: une personne physique ou morale partie à un contrat avec une entreprise offrant des services de communications électroniques accessibles au public, pour la fourniture de tels services;

(b)[1] (…)

(b)[2] «consentement»: toute manifestation de volonté libre, spécifique et informée par laquelle la personne concernée ou son représentant légal, judiciaire ou statutaire accepte que les données à caractère personnel la concernant fassent l'objet d'un traitement;

(c)[2] «communication»: toute information échangée ou acheminée entre un nombre fini de parties au moyen d'un service de communications électroniques accessible au public à l'exception des informations qui sont acheminées dans le cadre d'un service de radiodiffusion au public par l'intermédiaire d'un réseau de communications électroniques sauf si et dans la mesure où un lien peut être établi entre l'information et l'abonné ou l'utilisateur identifiable qui la reçoit;

(d)[2] «courrier électronique»: tout message sous forme de texte, de voix, de son ou d'image envoyé par un réseau de communications public qui peut être stocké dans le réseau ou dans l'équipement terminal du destinataire jusqu'à ce que ce dernier le récupère;

(e)[2] «données relatives au trafic»: toutes les données traitées en vue de l'acheminement d'une communication par un réseau de communications électroniques ou de sa facturation;

(f)[2] «données de localisation»: toutes les données traitées dans un réseau de communications électroniques « ou par un service de communications électroniques »[3] indiquant la position géographique de l'équipement terminal d'un utilisateur d'un service de communications électroniques accessible au public;

(g)[2] «Institut»: l'Institut Luxembourgeois de Régulation;

(h)[2] «réseau de communications électroniques»: les systèmes de transmission et, le cas échéant, les équipements de commutation ou de routage et les autres ressources qui permettent l'acheminement de signaux par câble, par voie hertzienne, par moyen optique ou par d'autres moyens électromagnétiques comprenant les réseaux satellitaires, les réseaux terrestres fixes (avec commutation de circuits ou de paquets, y compris l'Internet) et mobiles, les systèmes utilisant le réseau électrique, pour autant qu'ils servent à la transmission de signaux, les réseaux utilisés pour

---

1 Supprimé par la loi du 28 juillet 2011.

2 Renuméroté par la loi du 28 juillet 2011.

3 Inséré par la loi du 28 juillet 2011.

la radiodiffusion sonore et télévisuelle et les réseaux câblés de télévision, quel que soit le type d'information transmise;

(i)[4] «réseau de communications public»: un réseau de communications électroniques utilisé entièrement ou principalement pour la fourniture de services de communications électroniques accessibles au public. Le fournisseur du réseau de communications public est dénommé ci-après «opérateur»;

(j)[4] «service de communications électroniques»: un service fourni normalement contre rémunération qui consiste entièrement ou principalement en la transmission de signaux sur les réseaux de communications électroniques, y compris les services de télécommunications et les services de transmission sur des réseaux utilisés pour la radiodiffusion, mais qui exclut les services consistant à fournir des contenus à l'aide de réseaux et de services de communications électroniques ou à exercer une responsabilité éditoriale sur ces contenus; il ne comprend pas les services de la société de l'information qui ne consistent pas entièrement ou principalement en la transmission de signaux sur des réseaux de communications électroniques. Le fournisseur de services de communications électroniques est dénommé ci-après «fournisseur de services»;

(k)[4] «service à valeur ajoutée»: tout service qui exige le traitement de données relatives au trafic ou à la localisation, à l'exclusion des données qui ne sont pas indispensables pour la transmission d'une communication ou sa facturation;

(l)[4] «utilisateur»: une personne physique ou morale qui utilise ou demande un service de communications électroniques accessible au public à des fins privées ou professionnelles sans être nécessairement abonnée à ce service.

(Loi du 28 juillet 2011)

(m)[5] « violation de données à caractère personnel»: une violation de la sécurité entraînant accidentellement ou de manière illicite la destruction, la perte, l'altération, la divulgation ou l'accès non autorisés de données à caractère personnel transmises, stockées ou traitées d'une autre manière en relation avec la fourniture de services de communications électroniques accessibles au public ».

Art. 3. Sécurité « du traitement »[5]

(1) Le fournisseur de services prend les mesures techniques et d'organisation appropriées afin de garantir la sécurité de ses services, le cas échéant conjointement avec l'opérateur en ce qui concerne la sécurité du réseau. En cas d'atteinte ou de risque d'atteinte grave à la sécurité du réseau ou des services, le fournisseur de services et le cas échéant l'opérateur prend les mesures appropriées pour y remédier, les frais étant à sa seule charge.

(Loi du 28 juillet 2011)

« Sous réserve des dispositions générales de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel, les mesures visées ci-dessus, pour le moins:

– garantissent que seules des personnes autorisées peuvent avoir accès aux données à caractère personnel à des fins légalement autorisées,
– protègent les données à caractère personnel stockées ou transmises contre la destruction accidentelle ou illicite, la perte ou l'altération accidentelles et le stockage, le traitement, l'accès et la divulgation non autorisés ou illicites, et
– assurent la mise en œuvre d'une politique de sécurité relative au traitement des données à caractère personnel.

La Commission nationale pour la protection des données est habilitée à vérifier les mesures prises par les fournisseurs de services de communications électroniques accessibles au public, ainsi qu'à émettre des recommandations sur les meilleures pratiques concernant le degré de sécurité que ces mesures devraient atteindre. »

(2) Sans préjudice de ce qui précède, le fournisseur de services et le cas échéant l'opérateur informe ses abonnés de tout risque imminent d'atteinte à la sécurité du réseau ou des services mettant en cause

4 Renuméroté par la loi du 28 juillet 2011.

5 Inséré par la loi du 28 juillet 2011.

la confidentialité des communications ainsi que du moyen éventuel pour y remédier, y compris en en indiquant le coût probable.

(Loi du 28 juillet 2011)

« (3) En cas de violation de données à caractère personnel, le fournisseur de services de communications électroniques accessibles au public avertit sans retard la Commission nationale pour la protection des données de la violation.

Lorsque la violation de données à caractère personnel est de nature à affecter négativement les données à caractère personnel ou la vie privée d'un abonné ou d'un particulier, le fournisseur avertit également sans retard indu l'abonné ou le particulier concerné de la violation.

La notification d'une violation des données à caractère personnel à l'abonné ou au particulier concerné n'est pas nécessaire si le fournisseur a prouvé, à la satisfaction de la Commission nationale pour la protection des données, qu'il a mis en œuvre les mesures de protection technologiques appropriées et que ces dernières ont été appliquées aux données concernées par ladite violation. De telles mesures de protection technologiques rendent les données incompréhensibles à toute personne qui n'est pas autorisée à y avoir accès.

Sans préjudice de l'obligation du fournisseur d'informer l'abonné et le particulier concerné, si le fournisseur n'a pas déjà averti l'abonné ou le particulier de la violation de données à caractère personnel, la Commission nationale pour la protection des données peut, après avoir examiné les effets éventuellement négatifs de cette violation, exiger du fournisseur qu'il s'exécute.

La notification faite à l'abonné ou au particulier décrit au minimum la nature de la violation de données à caractère personnel et les points de contact auprès desquels des informations supplémentaires peuvent être obtenues et recommande des mesures à prendre pour atténuer les conséquences négatives possibles de la violation de données à caractère personnel. La notification faite à la Commission nationale pour la protection des données décrit en outre les conséquences de la violation de données à caractère personnel, et les mesures proposées ou prises par le fournisseur pour y remédier.

La Commission nationale pour la protection des données peut adopter des lignes directrices et, le cas échéant, édicter des instructions précisant les circonstances dans lesquelles le fournisseur est tenu de notifier la violation de données à caractère personnel, le format applicable à cette notification et sa procédure de transmission.

Lors d'un premier manquement aux obligations de notification, le fournisseur est averti par la Commission nationale pour la protection des données. En cas de manquement répété la Commission nationale peut prononcer une amende d'ordre qui ne peut excéder 50.000 euros.

Un recours en réformation est ouvert devant le tribunal administratif contre les décisions prises par la Commission nationale pour la protection des données dans le cadre du présent article.

(4) Les fournisseurs tiennent à jour un inventaire des violations de données à caractère personnel, notamment de leur contexte, de leurs effets et des mesures prises pour y remédier, les données consignées devant être suffisantes pour permettre à la Commission nationale pour la protection des données de vérifier le respect des dispositions du paragraphe (3). Cet inventaire comporte uniquement les informations nécessaires à cette fin.

(5) Quiconque contrevient aux dispositions des paragraphes (1), (2) et (4) est puni d'un emprisonnement de huit jours à un an et d'une amende de 251 à 125.000 euros ou d'une de ces peines seulement. La juridiction saisie peut prononcer la cessation du traitement contraire aux dispositions du présent article sous peine d'astreinte dont le maximum est fixé par ladite juridiction. »

Art. 4. Confidentialité des communications

(1) Tout fournisseur de services ou opérateur garantit la confidentialité des communications effectuées au moyen d'un réseau de communications public et de services de communications électroniques accessibles au public, ainsi que la confidentialité des données relatives au trafic y afférentes.

(2) Il est interdit à toute autre personne que l'utilisateur concerné d'écouter, d'intercepter, de stocker les communications et les données relatives au trafic y afférentes, ou de les soumettre à tout autre moyen d'interception ou de surveillance sans le consentement de l'utilisateur concerné.

(3) Le paragraphe (2):

(a) n'empêche pas le stockage technique nécessaire à l'acheminement d'une communication, sans préjudice du principe de confidentialité;

(b) « ne s'applique pas aux autorités judiciaires agissant dans le cadre des compétences leur attribuées par la loi et celles compétentes en vertu des articles 88-1 à 88-4 du Code d'instruction criminelle pour sauvegarder la sûreté de l'Etat, la défense, la sécurité publique et pour la prévention, la recherche, la constatation et la poursuite des infractions pénales »[6] ;

(c) ne s'applique pas aux communications et aux données relatives au trafic y afférentes, effectuées à destination du numéro d'appel d'urgence unique européen 112 et des numéros d'urgence déterminés par l'Institut dans le seul but de permettre (a) la réécoute de messages lors de problèmes de compréhension ou d'ambiguïté entre l'appelant et l'appelé, (b) la documentation de fausses alertes, de menaces et d'appels abusifs et (c) la production de preuves lors de contestation sur le déroulement d'actions de secours.

Les données relatives au trafic afférentes aux communications visées ci-dessus, y compris les données de localisation, sont à effacer une fois le secours apporté. Le contenu des communications est à effacer après un délai de 6 mois au plus;

(d) n'affecte pas l'enregistrement de communications et des données relatives au trafic y afférentes, lorsqu'il est effectué dans le cadre des usages professionnels licites, afin de fournir la preuve d'une transaction commerciale *(loi du 27 juillet 2007 qui modifie la loi du 2 août 2002)* « ou de toute autre communication commerciale ».

Les parties aux transactions *(loi du 27 juillet 2007 qui modifie la loi du 2 août 2002)* « ou à toutes autres communications commerciales » sont informées au préalable de ce que des enregistrements sont susceptibles d'être effectués, de la ou des raisons pour lesquelles les communications sont enregistrées et de la durée de conservation maximale des enregistrements. Les communications enregistrées sont à effacer dès que la finalité est atteinte, et en tout état de cause, lors de l'expiration du délai légal de recours contre la transaction;

(Loi du 28 juillet 2011)

(e) « ne s'applique pas au stockage d'informations, ou l'obtention de l'accès à des informations déjà stockées, dans l'équipement terminal d'un abonné ou d'un utilisateur à condition que l'abonné ou l'utilisateur ait donné son accord, après avoir reçu une information claire et complète, entre autres sur les finalités du traitement. Les méthodes retenues pour fournir l'information et offrir le droit de refus devraient être les plus conviviales possibles. Lorsque cela est techniquement possible et effectif, l'accord de l'abonné ou de l'utilisateur peut être exprimé par l'utilisation des paramètres appropriés d'un navigateur ou d'une autre application.

Cette disposition ne fait pas obstacle à un stockage ou à un accès techniques visant exclusivement à effectuer la transmission d'une communication par la voie d'un réseau de communications électroniques, ou strictement nécessaires au fournisseur pour la fourniture d'un service de la société de l'information expressément demandé par l'abonné ou l'utilisateur ».

(4) Quiconque contrevient aux dispositions du présent article est puni d'un emprisonnement de huit jours à un an et d'une amende de 251 à 125.000 euros ou d'une de ces peines seulement. La juridiction saisie peut prononcer la cessation du traitement contraire aux dispositions du présent article sous peine d'astreinte dont le maximum est fixé par ladite juridiction.

Art. 5. Données relatives au trafic

(1) (a) *(Loi du 24 juillet 2010)* « Pour les besoins de la recherche, de la constatation et de la poursuite d'infractions pénales qui emportent une peine criminelle ou une peine correctionnelle dont le maximum est égal ou supérieur à un an d'emprisonnement, et dans le seul but de permettre, en tant que de besoin, la mise à disposition des autorités judiciaires d'informations, tout fournisseur de services ou opérateur qui traite ou génère dans le cadre de la fourniture de services des données relatives au trafic est tenu de conserver ces données pendant une période de six mois à compter de la date de la communication. L'obligation

6 Modifié une première fois par la loi du 28 juillet 2011 et une deuxième fois par la loi du 28 juillet 2014.

de conserver inclut la conservation des données relatives aux appels téléphoniques infructueux lorsque ces données sont générées ou traitées et stockées (en ce qui concerne les données de la téléphonie) ou journalisées (en ce qui concerne les données de l'internet) dans le cadre de la fourniture des services de communications concernés. Un règlement grand-ducal détermine les catégories de données relatives au trafic susceptibles de pouvoir servir à la recherche, à la constatation et à la poursuite d'infractions visées ci-dessus. Ce règlement peut également déterminer les formes et les modalités suivant lesquelles les données visées sont à mettre à la disposition des autorités judiciaires ».

(b) Après la période de conservation prévue sub (a), le fournisseur de services ou l'opérateur est obligé d'effacer les données relatives au trafic concernant les abonnés et les utilisateurs, ou de les rendre anonymes.

(2) « Tout fournisseur de services ou tout opérateur qui traite des données relatives au trafic concernant les abonnés et les utilisateurs, est tenu de prendre toutes les dispositions nécessaires pour que de telles données soient conservées pendant la période prévue sub (1) (a) de manière telle qu'il est impossible à quiconque d'accéder à ces données dès lors qu'elles ne sont plus nécessaires à la transmission d'une communication ou aux traitements prévus par les dispositions sub (3) et (4), à l'exception des accès qui sont:

– ordonnés par les autorités judiciaires agissant dans le cadre des compétences leur attribuées par la loi et celles compétentes en vertu des articles 88-1 à 88-4 du Code d'instruction criminelle pour sauvegarder la sûreté de l'Etat, la défense, la sécurité publique et pour la prévention, la recherche, la constatation et la poursuite des infractions pénales visées au paragraphe (1) (a), ou
– demandés par les organes compétents dans le but de régler des litiges notamment en matière d'interconnexion ou de facturation » [7].

(3) Les données relatives au trafic qui sont nécessaires en vue d'établir les factures des abonnés et aux fins des paiements d'interconnexion peuvent être traitées. Un tel traitement n'est possible que jusqu'à la fin de la période au cours de laquelle la facture peut être légalement contestée ou des poursuites engagées pour en obtenir le paiement et ne peut en tout état de cause dépasser 6 mois lorsque la facture a été payée et n'a pas fait l'objet de litige ou de contestation.

(4) Les données relatives au trafic peuvent être traitées en vue de commercialiser des services de communications électroniques ou de fournir des services à valeur ajoutée dans la mesure et pour la durée nécessaires à la fourniture ou à la commercialisation de ces services pour autant que le fournisseur d'un service de communications électroniques ou l'opérateur informe préalablement l'abonné ou l'utilisateur concerné des types de données relatives au trafic traitées, de la finalité et de la durée du traitement et que celui-ci ait donné son consentement, nonobstant son droit de s'opposer à tout moment à un tel traitement.

(5) Le traitement des données relatives au trafic effectué dans le cas des activités visées aux paragraphes (1) à (4) est restreint aux personnes agissant sous l'autorité du fournisseur de services ou de l'opérateur qui sont chargés d'assurer la facturation ou la gestion du trafic, répondre aux demandes de clientèle, détecter les fraudes, commercialiser les services de communications électroniques ou fournir un service à valeur ajoutée. Le traitement doit se limiter à ce qui est nécessaire à de telles activités.

(6) Quiconque contrevient aux dispositions des paragraphes (1) à (5) du présent article est puni d'un emprisonnement de huit jours à un an et d'une amende de 251 à 125.000 euros ou d'une de ces peines seulement. La juridiction saisie peut prononcer la cessation du traitement contraire aux dispositions du présent article sous peine d'astreinte dont le maximum est fixé par ladite juridiction.

(Loi du 24 juillet 2010)

« **Art. 5-1.** (1) Les données conservées au titre des articles 5 et 9 sont soumises aux exigences prévues aux articles 22 et 23 de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel.

---

7 Modifié une première fois par la loi du 24 juillet 2010 et une deuxième fois par la loi du 28 juillet 2014.

(2) Les données sont détruites lorsque la durée de conservation prend fin, à l'exception des données auxquelles on a pu légalement accéder et qui ont été préservées.

Art. 5-2. (1) La Commission nationale pour la protection des données transmet annuellement à la Commission de l'Union européenne des statistiques sur la conservation de données au titre des articles 5 et 9.

A cet effet les fournisseurs de services ou opérateurs conservent et continuent à la Commission nationale, sur demande de celle-ci, les informations comprenant notamment:

- les cas dans lesquels des informations ont été transmises aux autorités compétentes conformément à la législation nationale applicable,
- 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,
- les cas dans lesquels des demandes de données n'ont pu être satisfaites.

(2) Ces statistiques ne contiennent pas de données à caractère personnel. »

Art. 6. Facturation détaillée

(1) Tout abonné a le droit de recevoir une facture non détaillée gratuite.

(2) Les appels gratuits y compris ceux aux lignes d'assistance ne sont pas indiqués sur la facture détaillée indépendamment de son degré de détail. En outre la facture détaillée ne contient aucune indication permettant d'identifier l'appelé.

Art. 7. Identification de la ligne appelante et de la ligne connectée

(1) Dans les cas où la présentation de l'identification de la ligne appelante est offerte, le fournisseur du service permet à l'abonné et à l'utilisateur appelant d'empêcher, par un moyen simple et gratuit, la présentation de l'identification de la ligne appelante et ce, appel par appel. L'abonné appelant dispose de cette possibilité de manière permanente pour chaque ligne.

(2) Dans les cas où la présentation de l'identification de la ligne appelante est offerte, l'abonné appelé doit pouvoir empêcher, par un moyen simple et gratuit pour un usage raisonnable de cette fonction, la présentation de l'identification de la ligne pour les appels entrants.

(3) Dans les cas où la présentation de l'identification de la ligne appelante est offerte et où l'identification de la ligne appelante est présentée avant l'établissement de l'appel, l'abonné appelé doit pouvoir, par un moyen simple et gratuit, refuser les appels entrants lorsque l'utilisateur ou l'abonné appelant a empêché la présentation de l'identification de la ligne appelante.

(4) Dans le cas où la présentation de l'identification de la ligne connectée est offerte, l'abonné appelé doit pouvoir, par un moyen simple et gratuit, empêcher la présentation de l'identification de la ligne connectée à l'utilisateur appelant.

(5) *(Loi du 28 juillet 2011)*

« (a) Tout fournisseur ou opérateur de services de téléphonie fixe ou mobile qui fournit un accès au numéro d'appel d'urgence unique européen 112 ainsi qu'aux numéros d'urgence déterminés par l'Institut luxembourgeois de régulation transmet (« push ») pour chaque appel à destination d'un de ces numéros d'appel d'urgence les données disponibles concernant l'appelant y compris les données de localisation.

Aux termes du présent paragraphe on entend par « données disponibles »:

– les données relatives à l'identification: le numéro de téléphone, nom, prénom(s), domicile ou lieu de résidence habituel, dénomination ou raison sociale, lieu d'établissement de l'abonné et de l'utilisateur pour autant que ce dernier soit identifié ou identifiable; l'indication du caractère public ou non public des données, ainsi que

– toutes les données traitées dans un réseau de communications électroniques indiquant la position géographique de l'équipement terminal d'un utilisateur d'un service de communications électroniques accessible au public (données de localisation).

(b) « L'Institut luxembourgeois de régulation fixe, en cas de besoin, le format et les modalités techniques de mise à disposition des données visées au paragraphe (5) » « et au paragraphe (5*bis*) ».

(Loi du 28 juillet 2011)

(c) Pour les appels effectués à destination du numéro d'appel d'urgence unique européen 112 et des numéros d'urgence déterminés par l'Institut, l'identification de la ligne appelante « et les données de localisation de l'appelant » est toujours présentée même lorsque l'appelant l'a empêchée.

« (5*bis*) En outre, en cas d'appel au numéro d'urgence unique européen 112 ainsi qu'aux numéros d'urgence déterminés par l'Institut luxembourgeois de régulation, les informations relatives à la localisation de l'appelant obtenues à partir de l'appareil mobile, si elles sont disponibles, sont mises à disposition sans tarder après l'établissement de la communication d'urgence au centre de réception des appels d'urgence le plus approprié, même lorsque l'appelant a désactivé la fonction de localisation. Ces informations sont à effacer après un délai de 24 heures au plus. »

(6) Les dispositions du paragraphe (1) s'appliquent également aux appels provenant de l'Union européenne à destination de pays tiers. Les dispositions des paragraphes (2), (3) et (4) s'appliquent également aux appels entrants provenant de pays tiers.

(7) Le fournisseur du service informe le public, par des moyens appropriés et au plus tard lors de la conclusion d'un contrat des possibilités sus énoncées.

(8) L'abonné appelé prétendant être victime d'appels à contenu malveillant ou dérangeant peut demander l'identification de la ligne appelante ou connectée, des appels répétés ou intempestifs, déclarés comme étant malveillants ou dérangeants, lesquels ont été effectués ou repérés sur base d'un même numéro d'appel ou d'un même raccordement. Un règlement grand-ducal fixera les modalités à respecter par le fournisseur du service ou l'opérateur ainsi que par les abonnés prétendant être victime d'appels à contenu malveillant ou dérangeant. Il précisera également les caractéristiques d'un appel à contenu malveillant ou dérangeant et déterminera l'utilisation de l'identification de la ligne appelante même si sa présentation est empêchée.

(9) Quiconque contrevient aux dispositions du présent article est puni d'un emprisonnement de huit jours à un an et d'une amende de 251 à 125.000 euros ou d'une de ces peines seulement. La juridiction saisie peut prononcer la cessation du traitement contraire aux dispositions du présent article sous peine d'astreinte dont le maximum est fixé par ladite juridiction.

Art. 8. Renvoi automatique d'appels

Dans le cas où le renvoi automatique d'appels (ou déviation) est offert, le fournisseur du service confère à tout abonné la possibilité de mettre fin, par un moyen simple et gratuit, au renvoi automatique d'appels par un tiers vers son appareil terminal lorsque le fournisseur du service peut identifier l'origine des appels renvoyés. Le cas échéant, cette identification se fait en collaboration avec d'autres fournisseurs de services concernés.

Art. 9. Données de localisation autres que les données relatives au trafic

(1) (a) *(Loi du 24 juillet 2010)* « Pour les besoins de la recherche, de la constatation et de la poursuite d'infractions pénales qui emportent une peine criminelle ou une peine correctionnelle dont le maximum est égal ou supérieur à un an d'emprisonnement, et dans le seul but de permettre, en tant que de besoin, la mise à disposition des autorités judiciaires d'informations, tout fournisseur de services ou opérateur qui traite ou génère dans le cadre de la fourniture de services des données de localisation autres que des données relatives au trafic est tenu de conserver ces données pendant une période de six mois à compter de la date de la communication. L'obligation de conserver inclut la conservation des données relatives aux appels téléphoniques infructueux lorsque ces données sont générées ou traitées et stockées (en ce qui concerne les données de la téléphonie) ou journalisées (en ce qui concerne les données de l'internet) dans le cadre de la fourniture des services de communications

concernés. Pour l'application du présent paragraphe, une seule information de localisation est requise par communication ou appel. Un règlement grand-ducal détermine les catégories de données de localisation autres que les données relatives au trafic susceptibles de pouvoir servir à la recherche, à la constatation et à la poursuite d'infractions visées ci-dessus. Ce règlement peut également déterminer les formes et les modalités suivant lesquelles les données visées sont à mettre à la disposition des autorités judiciaires ».

(b) Après la période de conservation prévue sub (a), le fournisseur de services ou l'opérateur est obligé d'effacer les données de localisation autres que les données relatives au trafic concernant les abonnés et les utilisateurs, ou de les rendre anonymes.

(2) Tout fournisseur de services ou opérateur qui traite des données de localisation, autres que les données relatives au trafic, concernant les abonnés et les utilisateurs, est tenu de prendre toutes les dispositions nécessaires à ce que de telles données soient conservées pendant la période prévue au paragraphe (1), (a) de manière telle qu'il est impossible à quiconque d'accéder à ces données, à l'exception des accès qui sont ordonnés par les autorités judiciaires agissant dans le cadre des compétences leur attribuées par la loi et celles compétentes en vertu des articles 88-1 à 88-4 du Code d'instruction criminelle pour sauvegarder la sûreté de l'Etat, la défense, la sécurité publique et pour la prévention, la recherche, la constatation et la poursuite des infractions pénales visées au paragraphe (1), (a) »[8].

(3) Tout fournisseur de services ou opérateur ne peut traiter des données de localisation autres que les données relatives au trafic et concernant les abonnés ou les utilisateurs que si celles-ci ont été rendues anonymes ou moyennant le consentement de l'abonné ou de l'utilisateur, dans la mesure et pour la durée nécessaires à la fourniture d'un service à valeur ajoutée et sous réserve des dispositions des paragraphes (2), (4) et (5).

(4) Le fournisseur du service et le cas échéant l'opérateur informe préalablement l'abonné ou l'utilisateur sur les types de données de localisation traitées, autres que les données relatives au trafic, sur la ou les finalité(s) et la durée de ce traitement ainsi que sur la transmission de ces données à des tiers en vue de la fourniture du service à valeur ajoutée. L'abonné ou l'utilisateur a la possibilité de retirer à tout moment son consentement pour le traitement des données de localisation autres que les données relatives au trafic.

Lorsque l'abonné ou l'utilisateur a donné son consentement au traitement des données de localisation autres que les données relatives au trafic, il doit garder la possibilité d'interdire temporairement, par un moyen simple et gratuit, le traitement de ces données pour chaque connexion au réseau ou pour chaque transmission de communication.

(5) Le traitement effectué des données de localisation, autres que les données relatives au trafic, dans le cas des activités visées aux paragraphes (1) à (4) est restreint aux personnes agissant sous l'autorité du fournisseur de services ou de l'opérateur ou du tiers qui fournit le service à valeur ajoutée. Le traitement doit se limiter à ce qui est nécessaire à de telles activités.

(6) Quiconque contrevient aux dispositions du présent article est puni d'un emprisonnement de huit jours à un an et d'une amende de 251 à 125.000 euros ou d'une de ces peines seulement. La juridiction saisie peut prononcer la cessation du traitement contraire aux dispositions du présent article sous peine d'astreinte dont le maximum est fixé par ladite juridiction

Art. 10. Annuaires d'abonnés

(1) L'abonné doit être informé gratuitement et avant d'y être inscrit des fins auxquelles sont établis des annuaires d'abonnés imprimés ou électroniques accessibles au public (ci-après «les annuaires») ou consultables par l'intermédiaire de services de renseignements, dans lesquels les données le concernant peuvent figurer, ainsi que de toute autre possibilité d'utilisation reposant sur des fonctions de recherche intégrées dans les versions électroniques des annuaires.

(2) (a) L'abonné doit avoir la possibilité d'indiquer clairement, lors de la souscription de l'abonnement ou à tout autre moment lors de nouvelles éditions de mises à jour ou d'annuaires, si les données à caractère personnel le concernant, et lesquelles de ces données, doivent

8 Modifié une première fois par la loi du 24 juillet 2010 et une deuxième fois par la loi du 28 juillet 2014.

figurer dans un annuaire public, dans la mesure où ces données sont pertinentes par rapport à la fonction de l'annuaire en question telle qu'elle a été établie par le fournisseur de l'annuaire.

(b) L'abonné doit pouvoir vérifier, corriger ou supprimer ces données. La non-inscription dans un annuaire public d'abonnés, la vérification, la correction ou la suppression de données à caractère personnel dans un tel annuaire est gratuite.

(3) Quiconque contrevient aux dispositions du présent article est puni d'un emprisonnement de huit jours à un an et d'une amende de 251 à 125.000 euros ou d'une de ces peines seulement. La juridiction saisie peut prononcer la cessation du traitement contraire aux dispositions du présent article sous peine d'astreinte dont le maximum est fixé par ladite juridiction.

(Loi du 27 juin 2018)

« Art. 10*bis*. Fichier centralisé auprès de l'Institut

(1) Il est créé un fichier sous forme électronique auprès de l'Institut qui contient les données transmises conformément au paragraphe 2. Le fichier a pour finalité de mettre à la disposition des autorités et services énumérés au paragraphe 4 les données y figurant.

Le fichier est hébergé auprès du Centre des technologies de l'information de l'État qui en assure la gestion opérationnelle.

(2) Les entreprises notifiées auprès de l'Institut conformément à la loi du 27 février 2011 sur les réseaux et les services de communications électroniques qui fournissent un service de communications électroniques accessible au public en ayant recours à des ressources de numérotation luxembourgeois (ci-après : « les entreprises notifiées ») transmettent d'office et gratuitement à l'Institut par voie électronique et au moyen d'un interface sécurisé, les données suivantes :

1° pour les personnes physiques : le nom, le prénom, le lieu de résidence habituelle, la date et le lieu de naissance ainsi que le numéro de contact de l'abonné ;

pour les personnes morales : la dénomination ou raison sociale, l'adresse du lieu d'établissement ainsi que le numéro de contact ;

2° le nom de l'entreprise notifiée, la nature du service fourni par celle-ci, le numéro d'appel alloué pour lequel le service en question a été souscrit et, si disponible, la date de la fin de la relation contractuelle ou en cas de prépaiement la date de désactivation du numéro d'appel.

3° pour les personnes physiques, le type, le pays de délivrance et le numéro de la pièce d'identité ou de l'attestation de dépôt d'une demande de protection internationale de l'abonné en cas de service à prépaiement.

Ces données doivent être actualisées au moins une fois par jour, même en l'absence de changement.

Un rapport sur le transfert des données est généré automatiquement une fois par jour auprès du Centre des technologies de l'information de l'État.

Le protocole et l'interface sécurisés ainsi que le format d'échange à utiliser pour le transfert de ces données sont déterminés par règlement de l'Institut.

(3) Le non-respect du paragraphe 2 et du règlement de l'Institut pris en son exécution peut être sanctionné par l'Institut conformément à l'article 83 de la loi du 27 février 2011 sur les réseaux et les services de communications électroniques.

(4) Le procureur d'État, le juge d'instruction et les officiers de police judiciaire visés à l'article 10 du Code de procédure pénale agissant dans le cadre de l'article 48-27, paragraphe 1 er du Code de procédure pénale, ainsi que le Service de renseignement de l'État accèdent de plein droit au fichier visé au paragraphe 1 er. L'accès de plein droit se limite aux mesures prévues par l'article 48-27 du Code de procédure pénale et à celles prises dans le cadre de la loi du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État.

Les centres d'appels d'urgence de la police grand-ducale accèdent aux seules données visées au paragraphe 2, point 1°. Cet accès se limite aux mesures particulières de secours d'urgence prestées

dans le cadre des activités des centres d'appels d'urgence de la police grand-ducale et s'effectue uniquement sur les communications entrantes.

Le motif de chaque consultation doit être enregistré au moment de l'accès.

Le Service de renseignement de l'État et les centres d'appels d'urgence de la police grand-ducale désignent chacun en ce qui le concerne les agents qui bénéficient d'un accès individuel.

(5) L'accès à distance aux données du fichier centralisé se fera par voie de requête électronique et sera sécurisé par un mécanisme d'authentification forte.

(6) Les informations relatives à la personne ayant procédé à la consultation, les informations consultées, les critères de recherche, la date et l'heure de la consultation, ainsi que le motif de la consultation sont enregistrées. Ces données sont effacées irrémédiablement et sans délai, cinq ans à compter de la date d'accès.

(7) Les données à caractère personnel consultées doivent avoir un lien direct avec les faits ayant motivé la consultation.

Les données visées au paragraphe 2 doivent être effacées irrémédiablement et sans délai trois ans à compter de la fin de la relation contractuelle ou, en cas de service à prépaiement, à compter de la date de désactivation du numéro d'appel.

(8) L'institut fait procéder régulièrement à un audit sur le fonctionnement du fichier prévu au paragraphe 1er pour contrôler la mise en œuvre des mesures techniques et organisationnelles appropriées. »

Art. 11. Communications non sollicitées

(Loi du 28 juillet 2011)

(1) L'utilisation de systèmes automatisés d'appel et de communication sans intervention humaine (automates d'appel), de télécopieurs ou de courrier électronique à des fins de prospection directe n'est possible que si elle vise l'abonné ou l'utilisateur ayant donné son consentement préalable ».

(2) Nonobstant le paragraphe (1), le fournisseur qui, dans le cadre d'une vente d'un produit ou d'un service, a obtenu[9] de ses clients leurs coordonnées électroniques en vue d'un courrier électronique, peut exploiter ces coordonnées électroniques à des fins de prospection directe pour des produits ou services analogues que lui-même fournit pour autant que lesdits clients se voient donner clairement et expressément le droit de s'opposer, sans frais et de manière simple, à une telle exploitation des coordonnées électroniques lorsqu'elles sont recueillies et lors de chaque message, au cas où ils n'auraient pas refusé d'emblée une telle exploitation.

(3) L'envoi de communications non sollicitées à des fins de prospection directe par d'autres moyens que ceux visés aux paragraphes (1) et (2) n'est possible que si l'abonné *(Loi du 28 juillet 2011)* « ou l'utilisateur » concerné a donné son consentement préalable.

(4) Il est interdit d'émettre des messages électroniques à des fins de prospection directe en déguisant, dissimulant ou en dénaturant l'identité de l'émetteur au nom duquel la communication est faite, ou sans indication d'adresse valable à laquelle le destinataire peut transmettre une demande de faire cesser ces communications.

(5) Les paragraphes (1) et (3) s'appliquent à l'abonné qui est une personne physique.

(6) Quiconque contrevient aux dispositions du présent article est puni d'un emprisonnement de huit jours à un an et d'une amende de 251 à 125.000 euros ou d'une de ces peines seulement. La juridiction saisie peut prononcer la cessation du traitement contraire aux dispositions du présent article sous peine d'astreinte dont le maximum est fixé par ladite juridiction.

---

9 Supprimé par la loi du 28 juillet 2011.

Art. 12. Commission nationale pour la protection des données

La Commission nationale pour la protection des données instituée par l'article 32 de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel est chargée d'assurer l'application des dispositions de la présente loi et de ses règlements d'exécution *(loi du 27 juillet 2007 qui modifie la loi du 2 août 2002)* « sans préjudice de l'application de l'article 8 de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel ».

(Loi du 2 avril 2014)

« Art. 12*bis*. Action en cessation

(a) Le magistrat présidant la Chambre du tribunal d'arrondissement siégeant en matière commerciale, à la requête de la Commission nationale pour la protection des données, peut ordonner toute mesure destinée à suspendre provisoirement ou à faire cesser tout traitement contraire aux dispositions de la présente loi.

(b) L'ordonnance peut intervenir indépendamment de l'action publique. La mesure ordonnée par le magistrat présidant la Chambre du tribunal d'arrondissement siégeant en matière commerciale prend toutefois fin en cas de décision d'acquittement prononcée par le juge pénal et coulée en force de chose jugée.

(c) L'action en cessation est introduite selon la procédure applicable devant le tribunal des référés. Le magistrat présidant la Chambre du tribunal d'arrondissement siégeant en matière commerciale statue comme juge de fond. Le délai d'appel est de quinze jours.

(d) L'affichage de la décision peut être ordonné à l'intérieur ou à l'extérieur de l'établissement du contrevenant et aux frais de celui-ci. La décision précise la durée de l'affichage et elle peut également ordonner la publication, en totalité ou par extrait aux frais du contrevenant, par la voie des journaux ou de toute autre manière.

Il ne peut être procédé à l'affichage et à la publication qu'en vertu d'une décision judiciaire coulée en force de chose jugée.

(e) Tout manquement aux injonctions ou interdictions portées par une décision judiciaire prononcée en vertu du présent article et coulée en force de chose jugée est puni d'une amende de 251 à 50.000 euros. »

Art. 13. Disposition transitoire

Le fournisseur offrant un annuaire public au sens de l'article 10 avant l'entrée en vigueur de la présente loi informe l'abonné sans délai et conformément à l'article 10 paragraphe (1) de la finalité du traitement de ses données.

Art. 14. Dispositions modificatives

Les articles suivants du Code d'instruction criminelle sont modifiés comme suit:

(a) *Art. 88-2: Les alinéas 1, 2, 3 et 5 de l'article 88-2 du Code d'instruction criminelle sont modifiés comme suit:*

al 1: Les décisions par lesquelles le juge d'instruction ou le président de la chambre du conseil de la Cour d'appel auront ordonné la surveillance et le contrôle de télécommunications ainsi que de correspondances confiées à la poste seront notifiées aux opérateurs des postes ou télécommunications qui feront sans retard procéder à leur exécution.

al 2: Ces décisions et les suites qui leur auront été données seront inscrites sur un registre spécial tenu par chaque opérateur des postes ou télécommunications.

al 3: Les télécommunications enregistrées et les correspondances ainsi que les données ou renseignements obtenus par d'autres moyens techniques de surveillance et de contrôle sur la base de l'article 88-1 seront remis sous scellés et contre récépissé au juge d'instruction qui dressera procès-verbal de leur remise. Il fera copier les correspondances pouvant servir à conviction ou à décharge et versera ces copies, les enregistrements ainsi que tous autres données et renseignements

reçus au dossier. Il renverra les écrits qu'il ne juge pas nécessaire de saisir aux opérateurs des postes qui les remettront sans délai au destinataire.

al 5: Les communications avec des personnes liées par le secret professionnel au sens de l'article 458 du Code pénal et non suspectes d'avoir elles-mêmes commis l'infraction ou d'y avoir participé ne pourront être utilisées. Leur enregistrement et leur transcription seront immédiatement détruits par le juge d'instruction.

(b) Art 88-4: Les alinéas 1 et 4 de l'article 88-4 du Code d'instruction criminelle sont modifiés comme suit:

al 1: Les décisions par lesquelles le Président du Gouvernement aura ordonné la surveillance et le contrôle de télécommunications ainsi que de correspondances seront notifiées aux opérateurs des postes ou télécommunications qui feront procéder sans retard à leur exécution.

al 4: Les correspondances seront remises sous scellés et contre récépissé au service de renseignements. Le chef du service fera photocopier les correspondances pouvant servir à charge ou à décharge et renverra les écrits qu'il ne juge pas nécessaire de retenir aux opérateurs des postes qui les feront remettre au destinataire.

Art. 15. Disposition diverse

La référence à la présente loi se fait sous une forme abrégée en recourant à l'intitulé suivant: « Loi du…concernant la protection de la vie privée dans le secteur des communications électroniques ».

Art. 16. Entrée en vigueur

La présente loi entre en vigueur le premier jour du mois qui suit sa publication au Mémorial.

Mandons et ordonnons que la présente loi soit insérée au Mémorial pour être exécutée et observée par tous ceux que la chose concerne.

Impression: CTIE – Division Imprimés et Fournitures de bureau