Avis de la Commission nationale pour la protection des données relatif au projet de loi n° 7022 relative aux abus de marché et portant : 1. mise en œuvre du règlement (UE) n° 596/2014 du Parlement européen et du Conseil du 16 avril 2014 sur les abus de marché (règlement relatif aux abus de marché) et abrogeant la directive 2003/6/CE du Parlement européen et du Conseil et les directives 2003/124/CE, 2003/125/CE et 2004/72/CE de la Commission; 2. transposition de: a) la directive 2014/57/UE du Parlement européen et du Conseil du 16 avril 2014 relative aux sanctions pénales applicables aux abus de marché (directive relative aux abus de marché); b) la directive d'exécution (UE) 2015/2392 de la Commission du 17 décembre 2015 relative au règlement (UE) n° 596/2014 du Parlement européen et du Conseil en ce qui concerne le signalement aux autorités compétentes des violations potentielles ou réelles dudit règlement; 3. modification de la loi modifiée du 11 janvier 2008 relative aux obligations de transparence des émetteurs; et 4. abrogation de la loi modifiée du 9 mai 2006 relative aux abus de marché

Délibération n° 1003/2016 du 2 décembre 2016

Conformément à l'article 32, paragraphe (3), lettre (e) de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel (ci-après désignée « la loi modifiée du 2 août 2002 » ou « la loi »), la Commission nationale pour la protection des données (ci-après désignée « la Commission nationale » ou « la CNPD ») a notamment pour mission d'*« être demandée en son avis sur tous les projets ou propositions de loi portant création d'un traitement de même que sur toutes les mesures réglementaires ou administratives émises sur base de la présente loi »*.

Par courrier en date du 7 octobre 2016, Monsieur le Ministre des Finances a invité la Commission nationale à se prononcer sur le projet de loi n° 7022 relative aux abus de marché (ci-après « le projet de loi »). La Commission nationale regrette qu'elle n'ait pas été saisie plus tôt dans la procédure législative, alors que le Conseil d'Etat a été saisi pour avis déjà à la date du 2 août 2016.

Le projet de loi a pour objectif d'adapter la législation luxembourgeoise en matière d'abus de marché afin de garantir l'application intégrale et cohérente des nouvelles règles découlant du règlement (UE) n° 596/2014 du Parlement européen et du Conseil du 16 avril 2014 sur les abus de marché (ci-après « le règlement n° 596/2014 » ou « le règlement européen »), de la directive 2014/57/UE du Parlement européen et du Conseil du 16 avril 2014 relative aux sanctions pénales applicables aux abus de marché et de la directive d'exécution (UE) 2015/2392 de la Commission du 17 décembre 2015 relative au règlement (UE) n° 596/2014 du Parlement européen et du Conseil en ce qui concerne le signalement aux autorités compétentes des violations potentielles ou réelles dudit règlement (ci-après « la directive d'exécution 2015/2392 »). Plusieurs des dispositions des mesures touchent au domaine de la protection des données à caractère personnel et la CNPD note que le législateur européen a intégré la législation applicable dans ce domaine dans le paquet législatif, notamment par le biais de l'article 26 du règlement n° 596/2014, qui énonce explicitement qu'*« [e]n ce qui*

concerne le traitement de données à caractère personnel dans le cadre du présent règlement, les autorités compétentes exécutent leurs tâches aux fins du présent règlement conformément aux dispositions législatives, réglementaires et administratives nationales transposant la directive 95/46/CE ».

Pour sa part, la Commission nationale entend limiter ses observations aux questions soulevées par les dispositions du projet de loi sous examen traitant des aspects liés au respect de la vie privée et à la protection des données à caractère personnel.

I. Quant à la qualité des données traitées par la CSSF et échangées entre la CSSF et le Procureur d'Etat

Le projet de loi fait état d'une coopération entre la Commission de Surveillance du Secteur Financier (ci-après désignée « la CSSF ») et le Procureur d'Etat. La CNPD prend acte de la précision dans le commentaire des articles qu'une disposition similaire figure déjà dans la loi modifiée du 9 mai 2006 relative aux abus de marché (ci-après désignée « la loi modifiée du 9 mai 2006 »)[1].

En effet, conformément à l'article 7 du projet de loi, la CSSF pourrait échanger avec le Procureur d'Etat et le Service de Police Judicaire « *toute information qu'ils jugent utile ou nécessaire* ». L'article détaille ensuite la procédure de coopération entre la CSSF et le Procureur d'Etat dans le cadre de la répression administrative ou pénale des violations ou infractions en matière d'abus de marché. D'après cet article, un dossier d'enquête tenu par le Procureur d'Etat pourrait, sous certaines conditions, être transmis à la CSSF afin que cette dernière puisse poursuivre la procédure.

La Commission nationale rappelle que le traitement de données à caractère personnel par le Procureur d'Etat tombe dans le champ d'application de l'article 8 de la loi modifiée du 2 août 2002, d'après lequel « *[l]e traitement des données dans le cadre d'enquêtes pénales et de procédures judiciaires est opéré dans le respect des dispositions du Code d'instruction criminelle, du Code de procédure civile, de la loi portant règlement de procédure devant les juridictions administratives ou d'autres lois* ». Il y a lieu de noter que ces Codes-loi ne contiennent pas de dispositions spécifiques relatives à la protection des données et à la vie privée.

Vu la possibilité pour le Procureur d'Etat de transmettre un dossier à la CSSF, la Commission nationale estime nécessaire de préciser si l'article 8 précité continuerait à s'appliquer aux données traitées par la CSSF lors de la poursuite de la procédure, dans la mesure où des données à caractère personnel judiciaires issues de l'enquête du Procureur d'Etat auront été transmises à la CSSF.

La même question se pose dans le cadre des autorisations judiciaires prévues par les paragraphes (4) et (7) de l'article 4 ainsi que par l'article 5 du projet de loi. En effet, les données à caractère personnel traitées par la CSSF, qui est une autorité administrative, lors de sa procédure administrative, tombent dans le champ d'application du régime dit « ordinaire » de la loi modifiée du 2 août 2002, alors que les données à caractère personnel sont à qualifier comme données judiciaires tombant dans le champ d'application de l'article 8 de la loi, du moment que le juge d'instruction émet l'autorisation judiciaire demandée par la CSSF.

[1] Voir le commentaire des articles, p. 25.

Nonobstant ses commentaires relatifs à l'article 4, paragraphe (1), point (7) du projet de loi[2], la Commission nationale estime nécessaire de préciser en détail dans le projet de loi les règles applicables à ces genres d'enquêtes mixtes.

II. Quant aux pouvoirs de la CSSF d'exiger la communication des enregistrements téléphoniques, des communications électroniques ou des enregistrements de données relatives au trafic

A. Les données traitées par les entités surveillées, les émetteurs, les réviseurs d'entreprises agréés et les cabinets de révision agréés

L'article 4, paragraphe (1), point (6) du projet de loi, qui met en œuvre l'article 23, paragraphe (2), lettre (g) du règlement n° 596/2014, confère à la CSSF le pouvoir d'obtenir la communication des enregistrements téléphoniques, des communications électroniques ou des enregistrements de données relatives au trafic détenues par les entités soumises à sa surveillance prudentielle, les émetteurs, les réviseurs d'entreprises agréés et les cabinets de révision agréés. Le commentaire des articles précise que la CSSF n'aurait accès qu'aux données existantes et que la disposition n'obligerait de toute façon pas les entités visées d'enregistrer ou de conserver les communications[3]. Il est également expliqué que l'article 29, paragraphe (1) de la loi modifiée du 9 mai 2006 donne actuellement à la CSSF le pouvoir « *d'exiger la communication des enregistrements téléphoniques et des données échangées existants* »[4].

A ce titre, la Commission nationale note qu'à l'époque de l'élaboration de la loi modifiée du 9 mai 2006, le Conseil d'Etat s'était interrogé sur la base légale de cette communication[5]. Par l'adoption du règlement n° 596/2014, cette base légale est dès lors en principe créée.

Cependant, alors que le règlement européen oblige les Etats membres de doter l'autorité compétente du pouvoir de « *se faire remettre les enregistrements des conversations téléphoniques, des communications électroniques ou des enregistrements de données relatives au trafic détenus par des entreprises d'investissement, des établissements de crédit ou des institutions financières* »[6], le projet de loi inclut également les émetteurs, les réviseurs d'entreprises agréés et les cabinets de révision agréés dans le champ d'application de cette disposition.

---

[2] Voir le point II.B. du présent avis.
[3] Voir le commentaire des articles, p. 23.
[4] Ibid, p. 22.
[5] « *[L]e Conseil d'Etat se demande tout d'abord quelle est la base légale pour cette communication? Est-ce la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel? Dans l'affirmative, quelle disposition précise est à appliquer? Quant à la loi organique de la CSSF (loi du 23 décembre 1998), elle ne fournit probablement pas de base juridique satisfaisante. A supposer que ces deux textes ne fournissent pas de base juridique suffisante, il faudrait, selon le Conseil d'Etat, en créer une dans le cadre du projet sous avis. En effet, la solution alternative consistant à soumettre tout transfert à une procédure d'autorisation ou de notification ne serait guère praticable* ». Avis du Conseil d'Etat du 15 novembre 2005, doc. parl. n° 5415/2, p. 7.
[6] Les notions d' « *entreprise d'investissement* » et d' « *établissement de crédit* » sont définies à l'article 4, paragraphe (1), point (2) et (3) du règlement n° 596/2014. Une définition du terme « *institution financière* » ne figure pas dans cet article. En revanche, tant l'article 23 de la version allemande que l'article 23 de la version anglaise utilise un terme défini à l'article 4, paragraphe (1), point (4) du règlement, à savoir « Finanzinstitut » et « financial institution ». Sur cette base, la Commission nationale part du postulat que le terme « *établissement financier* », tel que défini à l'article 4, paragraphe (1), point (4) de la version française dudit règlement, devrait figurer à la place d'« institution financière » dans l'article 23, paragraphe (2), lettre (g).

A l'instar de l'avis du 15 novembre 2005 du Conseil d'Etat et vu le fait que les émetteurs, les réviseurs d'entreprises agréés et les cabinets de révision agréés ne figurent pas parmi les entités listées à l'article 23 du règlement européen, la Commission nationale estime que le projet de loi va au-delà du champ d'application défini par le règlement européen en ajoutant ces trois dernières catégories d'organismes.

B. Les données traitées par les fournisseurs de services de communications électroniques et les opérateurs de réseaux de communications publics

L'article 4, paragraphe (1), point (7) du projet de loi complèterait, selon le commentaire des articles[7], l'article 4, paragraphe (1), point (6) en prévoyant que la CSSF, sous réserve de l'autorisation judiciaire du juge d'instruction prévue à l'article 5 du projet de loi, pourrait « *exiger la communication des enregistrements de données relatives au trafic détenus par les fournisseurs de services de communications électroniques et les opérateurs de réseaux de communications publics lorsqu'il existe des raisons de suspecter une violation et que de tels enregistrements peuvent se révéler utiles à la manifestation de la vérité dans le cadre d'une enquête relative à la violation de l'article 14 ou 15, du règlement (UE) n° 596/2014* ». Cet article met en œuvre l'article 23, paragraphe (2), lettre (h) du règlement n° 596/2014, qui dispose qu'« *[a]fin de mener à bien leurs missions au titre du présent règlement, les autorités compétentes sont dotées,* ***conformément au droit national****, au moins des pouvoirs de surveillance et d'enquête suivants : ... se faire remettre,* ***dans la mesure où le droit national l'autorise****, les enregistrements existants de données relatives au trafic détenus par un opérateur de télécommunications, lorsqu'il existe des raisons de suspecter une violation et que de tels enregistrements peuvent se révéler pertinents pour l'enquête relative à la violation de l'article 14, point a) ou b), ou de l'article 15* ».

Or, en l'état actuel du droit luxembourgeois, la CNPD estime que ce pouvoir est prohibé par l'article 5 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 (ci-après « la loi modifiée du 30 mai 2005 »).

En premier lieu, bien que le règlement européen ne fournisse pas de définition du terme « opérateur de télécommunication », les auteurs du projet de loi ont opté pour l'inclusion des opérateurs figurant dans la loi modifiée du 30 mai 2005, à savoir les fournisseurs de services de communications électroniques et les opérateurs de réseaux de communications publics.

Ainsi, en ce qui concerne les données relatives au trafic détenues par les entités visées, l'article 3, paragraphe (1), point 27 du règlement n° 596/2014 précise que la notion d'« *enregistrements de données relatives au trafic* » doit être interprétée comme étant les enregistrements de données relatives au trafic tels qu'ils sont définis à l'article 2, deuxième alinéa, point b), de la directive 2002/58/CE du Parlement européen et du Conseil concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques[8]. Bien que l'article de la directive, ainsi que l'article 2, lettre

---

[7] Voir le commentaire des articles, p. 22-23.

[8] Telle que modifiée par la Directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009 modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques, la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques et le règlement (CE) n° 2006/2004 relatif à la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs.

(e) de la loi modifiée du 30 mai 2005 qui le transpose, ne définissent pas la notion « d'enregistrements de données relatives au trafic », les « données relatives au trafic » y sont définies comme « *toutes les données traitées en vue de l'acheminement d'une communication par un réseau de communications électroniques ou de sa facturation* ».

Le projet de loi ne contient pas de précisions additionnelles quant aux données auxquelles la CSSF aurait accès avec l'autorisation judiciaire, indiquant seulement qu'il s'agit des données « *détenues* » par les fournisseurs de services de communications électroniques et les opérateurs de réseaux de communications publics.

Pourtant, en droit luxembourgeois, l'utilisation de ces données n'est possible que dans des conditions très restrictives, notamment à des fins de facturation ou à des fins de recherche, de constatation et de poursuite d'infractions pénales. En vertu du paragraphe (3) de l'article 5 de la loi modifiée du 30 mai 2005, « *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* ». Pour ce qui est du traitement à des fins autres que la facturation, le paragraphe 1er de l'article 5 prévoit un régime restrictif qui limite la conservation des données relatives au trafic « *[p]our 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 ...* ».

A cet égard, la Commission nationale soulève que le législateur luxembourgeois n'a pas encore précisé quelles données doivent être conservées par les fournisseurs de services de communications électroniques et les opérateurs de réseaux de communications publics à des fins de facturation. En revanche, pour ce qui est de la conservation des données relatives au trafic dans le cadre de la répression pénale, le règlement grand-ducal du 24 juillet 2010 déterminant les catégories de données à caractère personnel générées ou traitées dans le cadre de la fourniture de services de communications électroniques ou de réseaux de communications publics énonce les données qui doivent être conservées.

Il s'avère dès lors que les données qui sont actuellement détenues par les fournisseurs de services de communications électroniques et les opérateurs de réseaux de communications publics sont celles qui sont énumérées dans ce règlement grand-ducal et conservées afin de les mettre à disposition aux autorités judiciaires pour la recherche, la constatation et 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.

Les auteurs du projet de loi soulignent dans le commentaire de l'article 4, que les données relatives au trafic ont un caractère particulièrement sensible[9]. Un point qu'a également soulevé le Contrôleur européen de la protection des données dans son avis du 10 février 2012 sur le projet de règlement européen dans lequel il avait remarqué que « *[l]es données relatives à l'utilisation de moyens de communications électroniques peuvent contenir un vaste ensemble d'informations personnelles, telles que l'identité des personnes émettant et recevant l'appel, l'heure et la durée de l'appel, le réseau utilisé, la localisation géographique de l'utilisateur en cas de téléphone portable, etc. Certaines données relatives au trafic concernant l'utilisation de l'internet et du courrier électronique (par exemple la liste des sites internet visités) peuvent en*

[9] Voir le commentaire des articles, p. 23.

outre révéler d'importants détails sur le contenu de la communication. Par ailleurs, le traitement de données relatives au trafic est contraire au secret de la correspondance »[10].

Compte tenu du caractère sensible des données, l'accès par la CSSF aux données relatives au trafic détenues par les fournisseurs de services de communications électroniques et les opérateurs de réseaux de communications publics prévu par le projet de loi constituerait un changement fondamental du régime de l'utilisation des données relatives au trafic.

Ce pouvoir constitue une ingérence dans le droit au respect de la vie privée et dans le droit à la protection des données et doit être conforme à l'article 8 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales. La base légale doit également être suffisamment accessible et prévoir, avec une précision suffisante, dans quelles circonstances et sous quelles conditions la mesure peut être mise en œuvre.

La Commission nationale souligne que le règlement n° 596/2014 a été adopté le 16 avril 2014, soit huit jours après que la Cour de justice de l'Union européenne (ci-après « la CJUE ») ne rende un arrêt dans les affaires jointes C-293/12 et C-594/12 *Digital Rights Ireland et autres* (ci-après « l'arrêt *Digital Rights* ») le 8 avril 2014[11]. Cet arrêt traite précisément de la question de l'accès aux données relatives au trafic détenues par les fournisseurs de services de communications électroniques et les opérateurs de réseaux de communications publics. Dans cet arrêt, la CJUE a invalidé la Directive 2006/24/CE du Parlement européen et du conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE (ci-après « la Directive 2006/24/CE »), en jugeant qu'elle ne respectait pas le principe de proportionnalité et, plus précisément, que la mesure n'était pas limitée à ce qui était strictement nécessaire afin d'atteindre l'objectif légitime de la directive, tel que requis par la Charte des droits fondamentaux de l'Union européenne (ci-après désignée « la Charte »).

Alors que l'annulation de la Directive 2006/24/CE n'entrainait pas la caducité automatique de la législation nationale luxembourgeoise la transposant, à savoir l'article 5 de la loi modifiée du 30 mai 2005, le gouvernement luxembourgeois a pris l'initiative de proposer une modification de la législation nationale afin de la rendre conforme à l'arrêt *Digital Rights*, en déposant le projet de loi n° 6763. La Commission nationale a eu l'occasion de se prononcer tant sur la conformité de la législation luxembourgeoise avec l'arrêt *Digital Rights* avant le dépôt du projet

[10] Avis du Contrôleur européen de la protection des données du 10 février 2012 sur les propositions de la Commission de règlement du Parlement européen et du Conseil sur les opérations d'initiés et les manipulations de marché, et de directive du Parlement européen et du Conseil relative aux sanctions pénales applicables aux opérations d'initiés et aux manipulations de marché, JO C 177 du 20.6.2012, p. 1–11, paragraphe 24.
[11] Arrêt du 8 avril 2014, *Digital Rights Ireland et autres*, C-293/12 and C-594/12, EU:C:2014:238.

de loi n° 6763 que sur le contenu dudit projet de loi dans ses avis du 13 mai 2014[12] et du 19 juin 2015[13].

Sans vouloir reprendre le contenu de ses avis, la Commission nationale relève que la CJUE dans l'affaire *Digital Rights* critiquait plus particulièrement l'absence d'un « *critère objectif permettant de délimiter l'accès des autorités nationales compétentes aux données et leur utilisation ultérieure à des fins de prévention, de détection ou de poursuites pénales concernant des infractions pouvant, au regard de l'ampleur et de la gravité de l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte, être considérées comme suffisamment graves pour justifier une telle ingérence* »[14].

En ce qui concerne la détermination claire des infractions permettant le recours aux données relatives au trafic, le projet de loi n° 6763 prévoit de remplacer la condition actuelle prévue à l'article 5 de la loi modifiée du 30 mai 2005 par le critère que l'infraction pénale doit figurer sur une liste exhaustive d'infractions considérées comme étant suffisamment graves. A cet égard, la CNPD note que les sanctions pénales prévues à l'article 32 de la loi du 9 mai 2006 figurent sur la liste proposée par le projet de loi n° 6763, tout comme elles sont par ailleurs implicitement visées par l'article 5 de la loi modifiée du 30 mai 2005 actuellement applicable. N'y figurent pas, les sanctions administratives que peut infliger la CSSF en fonction de l'article 33 de la loi du 9 mai 2006.

En implémentant la nouvelle législation européenne en matière d'abus de marché, le projet de loi sous examen prévoit, comme la loi du 9 mai 2006, tant des sanctions administratives que pourrait infliger la CSSF que des infractions pénales pour les comportements considérés comme étant graves. Sans aborder la question de la problématique du principe *non bis in idem*, la Commission nationale note que le commentaire des articles précise qu'afin de ne pas violer ce principe, les auteurs du projet de loi ont décidé de « *reprendre le mécanisme prévu par la loi modifiée du 9 mai 2006, mécanisme qui repose sur deux volets, à savoir, d'une part, l'exigence d'un dol spécial pour les infractions pénales et, d'autre part, l'attribution d'une compétence exclusive et alternative soit aux juridictions judiciaires, soit à la CSSF pour sanctionner les abus de marché* » afin de délimiter « *le champ des comportements considérées comme graves et justifiant une répression pénale, par opposition aux manquements administratifs* »[15]. Il s'ensuit donc que les auteurs du projet de loi n'estiment pas qu'une infraction sanctionnée par une « répression administrative » par la CSSF aux termes de l'article 33 de la loi du 9 mai 2006 doit s'entendre comme un manquement grave. En d'autres mots, les comportements et infractions « graves » relèvent de la compétence des juridictions judiciaires.

---

[12] Avis de la Commission nationale pour la protection des données du 13 mai 2014 quant à la conformité de la loi modifiée du 30 mai 2005 relative aux dispositions spécifiques de protection des personnes à l'égard du traitement des données dans le secteur des communications électroniques et des articles 67-1, 88-2 et 88-4 du Code d'instruction criminelle avec les exigences posées par l'arrêt du 8 avril 2014 dans les affaires jointes C-293/12 et C-594/12 pour la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communication (http://www.cnpd.public.lu/fr/decisions-avis/2014/Vorratsdatenspeicherung/214_2014_Deliberation_Ministere-Justice_avis-loi-modifiee-30-mai-2005-arret-CJUE-8-avril-2014-affaires-jointes-C-293-12-et-C-594-12-conservation-donnees.pdf).

[13] Avis de la Commission nationale pour la protection des données du 19 juin 2015 relatif au projet de loi n° 6763 portant modification du Code d'instruction criminelle et de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques, doc. parl. n° 6763/2.

[14] Arrêt du 8 avril 2014, *Digital Rights Ireland et autres*, C-293/12 and C-594/12, EU:C:2014:238, point 60.

[15] Voir le commentaire des articles, p. 31.

Il y a lieu de constater que le projet de loi contourne les sauvegardes et restrictions imposées par la loi, qui sont nécessaires afin de rendre l'utilisation des données relatives au trafic légitime. En effet, pour le cas où les comportements sur lesquels portent l'enquête de la CSSF seraient suffisamment graves, il incomberait au Procureur d'Etat, et non à la CSSF, de poursuivre l'enquête.

En revanche, si les manquements n'étaient pas considérés comme étant suffisamment graves pour justifier l'intervention du Procureur d'Etat, la CSSF pourrait enquêter et pourrait, en vertu de l'article sous examen et à condition d'avoir obtenu l'autorisation judiciaire du juge d'instruction, se faire communiquer les données relatives au trafic détenues par les fournisseurs de services de communications électroniques et les opérateurs de réseaux de communications publics.

Il s'ensuit que les données en question pourraient être accédées dans le cadre de la répression administrative des manquements administratifs, un seuil nettement inférieur aux conditions posées par l'article 5 de la loi modifiée du 30 mai 2005, par l'arrêt *Digital Rights* et par le projet de loi n° 6763, que les autorités judiciaires doivent remplir pour pouvoir se faire communiquer les données.

La CNPD souligne d'ailleurs que la Suède, l'Allemagne et l'Autriche ont, lors de l'annonce de l'adoption du règlement n° 596/2014 par le Conseil de l'Union européenne, déclaré qu'ils présumaient que l'accès par les autorités administratives compétentes ne concerne pas les données conservées en vertu de la Directive 2006/24/CE (la directive sur la conservation des données), car « *cela enfreindrait l'exigence prévue par cette directive de ne conserver des données qu'à des fins de recherche, de détection et de poursuite d'infractions graves. Toute extension de l'accès aux données relatives au trafic en dehors de procédures judiciaires créerait un dangereux précédent pour d'autres dossiers de l'UE* »[16].

Il est à noter que la CJUE reprochait également à la directive de ne pas avoir prévu une durée de conservation précise des données, une différenciation dans la durée de conservation en fonction de la catégorie des données conservées ou encore des exceptions pour les personnes dont les communications sont soumises au secret professionnel. Ces critiques se trouvent également applicables dans le cas d'espèce étant donné que de telles précisions font défauts dans le projet de loi sous examen.

Au vu de ce qui précède, la CNPD estime que l'article 4, paragraphe (1), point 7 du projet de loi n'est ni compatible avec la jurisprudence européenne, à savoir l'arrêt *Digital Rights,* ni avec le projet de loi n° 6763, de sorte qu'elle est d'avis qu'il convient de supprimer cette disposition du projet de loi sous avis.

III. Quant à la tenue de registres des signalements reçus

L'article 8, paragraphe 1er et l'annexe du projet de loi mettent en œuvre l'article 32 du règlement n° 596/2014 et transposent la directive d'exécution 2015/2392. Ces dispositions imposent aux autorités de contrôle l'obligation de mettre en place des mécanismes efficaces pour permettre le signalement des violations par des « informateurs », à savoir des mécanismes de

[16] Conseil de l'Union européenne, Projet de Procès-verbal du 3309e session du Conseil de l'Union européenne (AFFAIRES ÉTRANGÈRES), tenue à Luxembourg les 14 et 15 avril 2014, doc. n° 8947/14, p. 8.

« *whistleblowing* », ainsi que les procédures à suivre par la CSSF lors de la réception et le suivi des signalements.

S'il est vrai que les principes de la protection des données à caractère personnel ont été intégrés dans la directive d'exécution 2015/2392 et que l'annexe constitue une transposition fidèle de cette directive, la Commission souhaite néanmoins apporter quelques précisions quant au texte de l'annexe.

A. Les données traitées

Il ressort du 1er paragraphe de la section VII de l'annexe du projet de loi que *« [l]a CSSF tient un registre de tous les signalements de violations reçus conformément au règlement (UE) n° 596/2014 et à la présente loi »*.

A cet égard, la CNPD s'interroge sur les données qui figureraient dans cette base de données. S'agit-il seulement des données relatives aux signalements, ou également des données issues des investigations. Est-ce que les informations reçues d'autres autorités seraient également conservées dans cette base de données ?

Conformément à l'article 4, paragraphe (1) de la loi du 2 août 2002, l'utilisation des données traitées doit se limiter aux finalités pour lesquelles elles ont été collectées et les données doivent être adéquates, pertinents et non excessives au regard des finalités pour lesquelles elles ont été collectées. La Commission nationale recommande dès lors de préciser dans le projet de la loi quelles données seront traitées dans ce registre.

B. L'enregistrement des appels effectués par les informateurs

En vertu des sections VI et VII de l'annexe, la CSSF aurait l'option d'enregistrer les appels des informateurs. La CNPD s'interroge sur la mise en œuvre pratique de ces enregistrements, notamment si l'informateur laisserait un message sur un répondeur ou si un des membres du personnel spécialisés entretiendrait une conversation téléphonique avec l'informateur.

La Commission nationale rappelle que l'article 4 de la loi modifiée du 30 mai 2005 énonce le principe de la confidentialité des communications effectuées au moyen d'un réseau de communications public et de services de communications électroniques accessibles au public ainsi que l'interdiction de stocker les communications. Un tel stockage ou enregistrement ne peut se faire qu'avec le consentement de l'utilisateur concerné ou si une des exceptions du paragraphe (3) de l'article 4 s'applique.

Pour le cas où les communications tant des informateurs, que des membres du personnel de la CSSF spécialisés seraient enregistrées, les informateurs pourraient consentir à l'enregistrement de leurs appels. En revanche, pour ce qui est des membres du personnel spécialisés de la CSSF, qui se trouvent dans une situation de subordination par rapport à leur employeur, le consentement ne serait pas considéré comme étant légitime et est d'ailleurs exclu par l'article L. 261-1 du Code du Travail. Par ailleurs, la CNPD estime qu'aucune des exceptions actuellement prévues au paragraphe (3) de l'article 4 ne pourraient permettre à la CSSF d'enregistrer les communications de ses salariés dans le cadre du présent projet de loi.

Dès lors, si les communications des salariés de la CSSF serait enregistrées, une modification du paragraphe (3) de l'article 4 de la loi modifiée du 30 mai 2005 serait nécessaire afin d'y prévoir une exception supplémentaire.

C. L'anonymat des appelants

Il ressort du texte de l'annexe que les informateurs auraient la possibilité de faire des signalements de manière anonyme. A ce sujet, la Commission nationale se rallie cependant à l'avis n° 1/2006 du Groupe de travail « Article 29 » relatif à l'application des règles de l'UE en matière de protection des données aux mécanismes internes de dénonciation des dysfonctionnements dans les domaines de la comptabilité, des contrôles comptables internes, de l'audit, de la lutte contre la corruption et la criminalité bancaire et financière[17], qui estime qu'il ne convient pas d'encourager les signalement anonymes, mais au contraire de promouvoir l'identification des informateurs. En effet, l'identification de l'informateur permet de limiter les risques engendrés par des signalements anonymes, comme p.ex. les dénonciations calomnieuses.

D. L'information et les droits des personnes

A l'instar de l'avis n° 1/2006 du Groupe de travail « Article 29 » précité[18], la CNPD rappelle que non seulement les droits des personnes effectuant des signalements doivent être garantis, mais également ceux des personnes faisant l'objet d'un signalement, le cas échéant.

(i). Le droit à l'information

L'article 26 de la loi modifiée du 2 août 2002 donne à chaque personne concernée le droit d'obtenir certaines informations relatives au traitement mis en œuvre par le responsable du traitement.

En fonction de la section IV de l'annexe, la CSSF fournit les informations contenues dans les sections IV et V de l'annexe par le biais de son site Internet. De plus, il est prévu dans la section VI que l'*informateur* reçoit les informations contenues dans les sections IV et V « *avant réception du signalement de violation, ou au plus tard au moment de la réception* »[19].

Comme soulevé par le Groupe de travail « Article 29 » dans son avis n° 1/2006, les personnes concernées ont le droit d'obtenir les informations énoncées à l'article 26, paragraphe (2) de la loi modifiée du 2 août 2002 lorsque leurs données personnelles sont collectées auprès d'un tiers et non directement auprès d'elles[20]. Cette disposition s'applique lorsqu'un informateur effectue un signalement concernant une tierce personne et fournit des données à caractère personnel relatives à cette dernière. La personne faisant l'objet d'un signalement devrait dès lors être informée dans les plus brefs délais après l'enregistrement des données la concernant. Vu les exceptions établies à l'article 27 de la loi modifiée du 2 août 2002, la CNPD se rallie à la recommandation du Groupe de travail « Article 29 », selon laquelle cette notification peut

---

[17] Groupe de travail « Article 29 », Avis n° 1/2006 du 1er février 2006 relatif à l'application des règles de l'UE en matière de protection des données aux mécanismes internes de dénonciation des dysfonctionnements dans les domaines de la comptabilité, des contrôles comptables internes, de l'audit, de la lutte contre la corruption et la criminalité bancaire et financière (WP 117), p. 11.

[18] Ibid, p. 14-15.

[19] Voir la section VI, para. (4) de l'annexe.

[20] Groupe de travail « Article 29 », Avis n° 1/2006 du 1er février 2006 relatif à l'application des règles de l'UE en matière de protection des données aux mécanismes internes de dénonciation des dysfonctionnements dans les domaines de la comptabilité, des contrôles comptables internes, de l'audit, de la lutte contre la corruption et la criminalité bancaire et financière (WP 117), p. 14.

être retardée s'il existe un risque sérieux qui compromettrait la capacité de l'organisme, dans le cas d'espèce la CSSF, d'enquêter efficacement sur les faits allégués[21].

En ce qui concerne les informations fournies aux personnes concernées par le biais du site Internet de la CSSF, le projet de loi indique dans les sections IV et V de l'annexe que seraient fournies notamment des informations relatives aux procédures applicables aux signalements, aux règles de confidentialité applicables aux signalements ainsi que les procédures de protection des salariés.

Or, l'article 26 précité de la loi précise que la personne concernée a le droit d'obtenir des informations relatives au responsable du traitement, les finalités du traitement, les destinataires auxquels les données sont susceptibles d'être communiquées, le fait de savoir si la réponse aux questions est obligatoire et les conséquences d'un défaut de réponse, ainsi que l'existence d'un droit d'accès. Il ne résulte pas clairement du projet de loi que ces informations seraient fournies à l'informateur et à la personne faisant l'objet d'un signalement.

A cet égard, la Commission nationale renvoie à l'arrêt « *Smaranda Bara* » de la CJUE du 1er octobre 2015[22], selon lequel « *les articles 10, 11 et 13 de la directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, doivent être interprétés en ce sens qu'ils s'opposent à des mesures nationales, telles que celles en cause au principal, qui permettent à une administration publique d'un État membre de transmettre des données personnelles à une autre administration publique et leur traitement subséquent, sans que les personnes concernées n'aient été informées de cette transmission ou de ce traitement* ». La Commission nationale souligne dès lors l'importance d'assurer que les personnes concernées, tant les informateurs que les personnes faisant l'objet d'un signalement, obtiennent toutes les informations requises en vertu de l'article 26 de la loi du 2 août 2002.

Sous réserve des observations sous le point III.B. du présent avis et en considération du fait que la CSSF pourrait enregistrer les communications avec les personnes effectuant des signalements, la CNPD souligne que l'information doit être suffisamment claire pour permettre à la personne concernée de savoir si les communications sur la ligne téléphonique sur laquelle elle appelle sont enregistrées, à l'instar de l'article 4 de la loi modifiée du 30 mai 2005.

(ii). Le droit d'accès

A défaut de précisions dans le projet de loi, la Commission rappelle que chaque personne concernée dispose d'un droit d'accès aux données la concernant, tel que défini à l'article 28 de la loi modifiée du 2 août 2002. Sous réserve des dérogations admises au titre de l'article 29 de la loi, les personnes concernées pourraient exercer leur droit d'accès auprès de la CSSF pendant la procédure administrative dans les conditions établies par l'article 28 de la loi.

En ce qui concerne les données traitées par le Procureur d'Etat et le Service de Police Judiciaire, la Commission nationale réitère ses remarques ci-dessus selon lesquelles de tels traitements tomberaient dans le champ d'application de l'article 8 de la loi modifiée du 2 août 2002 et que l'article 28 ne s'appliquerait pas à ces données.

[21] Ibid.
[22] Arrêt du 1er octobre 2015, *Smaranda Bara et autres*, C-201/14, EU:C:2015:638, point 46.

Afin de permettre aux personnes concernées de savoir quelle disposition s'applique au traitement de leurs données, il conviendrait de préciser quel régime est applicable aux données échangées entre la CSSF, le Procureur d'Etat et, le cas échéant, le juge d'instruction[23], échanges mélangeant des données administratives avec des données judiciaires.

E. La sécurité des données

La section IX (« Procédures de protection des données à caractère personnel ») de l'annexe entend transposer l'article 9 de la directive d'exécution 2015/2392 et dispose que *« (1) La CSSF conserve les registres visés à la section VII au sein d'un système sécurisé et confidentiel. (2) L'accès au système visé au paragraphe 1er est soumis à des restrictions afin de garantir que les données qui y sont conservées soient uniquement accessibles aux membres du personnel de la CSSF qui ont besoin de ces données dans l'exercice de leurs fonctions. »*

En application des articles 22 et 23 de la loi modifiée du 2 août 2002, la CSSF est obligée d'adopter les mesures techniques et organisationnelles nécessaires afin d'assurer la sécurité des données, notamment par un système de traçage des accès aux données. La Commission nationale estime dès lors qu'il conviendrait de modifier l'article afin de l'aligner sur les dispositions contenues dans d'autres lois ou règlements grand-ducaux, et qu'il pourrait avoir la teneur suivante : *« Le système informatique par lequel l'accès au registre est opéré doit être aménagé de sorte que l'accès aux fichiers soit sécurisé moyennant une authentification forte, que les informations relatives à la personne ayant procédé à la consultation, les informations consultées, la date, l'heure et la référence du dossier dans le cadre duquel la consultation a été effectuée, ainsi que le motif précis de la consultation puissent être retracés. Les données de journalisation doivent être conservées pendant un délai de cinq ans à partir de leur enregistrement, délai après lequel elles sont effacées, sauf lorsqu'elles font l'objet d'une procédure de contrôle.»*

F. La durée de conservation des données

En application de l'article 4, paragraphe (1), lettre (d) de la loi modifiée du 2 août 2002, les données à caractère personnel traitées par la CSSF devraient en principe être conservées, sous une forme permettant l'identification des personnes concernées, pendant une période n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles les données ont été collectées.

A ce titre, l'article 28 du règlement n° 596/2014 prévoit que « *les données à caractère personnel doivent être conservées pendant une durée maximale de cinq ans* ».

A défaut de précision ultérieure dans le règlement n° 596/2014, la Commission nationale recommande de spécifier que la date de départ serait la date de la réception du signalement. Dans l'hypothèse d'une constatation par la CSSF d'une violation de la loi, les données pourraient toutefois être conservées au-delà du délai susmentionné dans le cadre de la procédure administrative ou de la transmission des données aux autorités judiciaires compétentes.

[23] Voir ci-avant point I du présent avis.

IV. Quant aux destinataires

Le cadre législatif sous examen impose à la CSSF une obligation de coopération avec d'autres autorités, notamment le Procureur d'Etat et le Service de Police Judiciaire, l'Inspection du Travail et des Mines, ainsi que les autorités compétentes d'autres Etats membres et des pays tiers.

Pour ce qui est de la transmission de données à caractère personnel au sein et en dehors de la CSSF, la section X de l'annexe prévoit que « *[l]a CSSF dispose de procédures adéquates pour la transmission, en son sein et à des tiers, des données à caractère personnel de l'informateur et de la personne faisant l'objet d'un signalement.* ». Or, comme l'a déjà soulevé le Conseil d'Etat à plusieurs reprises « *...l'accès à des fichiers externes et la communication de données informatiques à des tiers constituent une ingérence dans la vie privée et partant, en vertu de l'article 11, paragraphe 3, de la Constitution, est une matière réservée à la loi formelle. Dans ce cas, l'essentiel du cadrage normatif doit figurer dans la loi.*

La loi doit indiquer les bases de données auxquelles une autorité publique peut avoir accès ou dont une autorité publique peut se faire communiquer des données, tout comme les finalités de cet accès ou de cette communication. En cas d'accès direct et, le cas échéant, d'interconnexion, la loi doit encore préciser que le système informatique par lequel l'accès est opéré doit être aménagé de sorte que l'accès est sécurisé moyennant une authentification forte (...) »[24].

La Commission nationale estime dès lors que la disposition en question devrait être précisée afin d'assurer que les modalités de transmission soient prévues et que les données à caractère personnel soient protégées pendant toute les étapes du traitement.

A. Le Procureur d'Etat et le Service de Police Judiciaire

En ce qui concerne la coopération entre la CSSF, le Procureur d'Etat et le Service de Police Judiciaire, la CNPD réitère ses commentaires faits au point I du présent avis concernant l'incertitude du régime applicable aux données échangées entre la CSSF et le Procureur d'Etat et y ajoute que la transmission de données entre tous les intervenants doit être ménagée de façon à assurer pendant toutes les étapes du traitement la confidentialité et la sécurité des données.

B. l'Inspection du Travail et des Mines

En application de la section VIII de l'annexe, une coopération entre la CSSF et l'ITM est prévue afin de protéger les salariées qui signalent des violations du règlement n° 596/2014. Il ressort de ces dispositions, que la CSSF et l'ITM « *se dotent de procédures communes précisant l'échange d'informations et la coopération visés...* ».

Or, s'agissant d'une matière dont l'essentiel du cadrage normatif doit figurer dans la loi[25], les modalités d'accès et de transmission de données à caractère personnel devraient figurer dans la loi.

---

[24] Avis du Conseil d'Etat du 7 juin 2016 concernant le projet de loi portant modification de la loi du 24 juillet 2014 concernant l'aide financière de l'Etat pour études supérieures, doc. parl. n° 6975/5, p. 4. Voir aussi l'avis du Conseil d'Etat du 9 décembre 2014 à l'égard du projet de loi 6588 portant organisation du secteur des services de taxis et modification du code de la consommation, doc. parl. n° 6588/8, p. 7.

[25] Voir le point IV du présent avis.

Dès lors, la Commission nationale estime nécessaire d'adapter le texte du projet de loi sous examen afin d'y prévoir les modalités et conditions précises des transmissions et échanges de données entre la CSSF et l'ITM.

C. Les destinataires dans les autres Etats membres de l'Union européenne et dans les pays tiers

Les articles 25 et 26 du règlement n° 596/2014 obligent, sous certaines conditions, la CSSF de coopérer avec les autorités compétentes d'autres Etats membres, avec l'Autorité européenne des marchés financiers ainsi qu'avec des autorités de surveillance des pays tiers. Pour ce faire, les articles 10 et 11 du projet de loi établissent les conditions de l'échange d'informations entre la CSSF et les autres autorités.

Les transferts des données à caractère personnel éventuels pouvant avoir lieu dans le cadre de cette coopération sont entourés de garanties, non seulement en vertu du règlement n° 596/2014[26], mais également en vertu de la directive d'exécution 2015/2392 et du projet de loi. La Commission nationale se limite dès lors à formuler quelques observations ponctuelles.

La CNPD constate que le projet de loi prévoit la possibilité pour la CSSF d'utiliser les données qui lui sont transmises tant par des autorités compétentes d'autres Etats membres que par des autorités de surveillance des pays tiers à des fins autres que « *l'exercice de ses fonctions telles que définies dans la présente loi et dans le cadre de procédures administratives ou judiciaires spécifiquement liées à cet exercice* » ou de les transmettre à une autorité compétente étrangère, si l'autorité communiquant les données y a consenti[27]. La Commission nationale rappelle que les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes et ne peuvent pas être traitées ultérieurement de manière incompatible avec ces finalités[28]. La CSSF doit dès lors s'assurer du respect de ce principe lors de chaque traitement effectué, y compris lors d'une éventuelle transmission de données à des autorités compétentes européennes, à l'Autorité européenne des marchés financiers ou à des autorités de surveillance des pays tiers.

En vertu de l'article 25, paragraphe (1), alinéa (4) du règlement n° 596/2014, la CSSF pourra transmettre « *des informations spécifiques liées aux enquêtes ou aux procédures pénales engagées concernant d'éventuelles violations du présent règlement* » à d'autres autorités compétentes des Etats membres et à l'Autorité européenne des marchés financiers « *afin de satisfaire à leur obligation de coopérer entre elles et avec l'AEMF aux fins du présent règlement* ». Pour le cas où un tel échange nécessiterait un traitement de données judiciaires, la Commission nationale rappelle que ceci doit se faire dans le respect de l'article 8 de la loi modifiée du 2 août 2002.

V. Quant à la publication des décisions de la CSSF

Selon l'article 34 du règlement n° 596/2014, la CSSF publie sur son site Internet « *toute décision infligeant une sanction administrative ou toute autre mesure administrative pour cause*

[26] Notamment les articles 27-29.
[27] Voir les articles 10, paragraphe (3) et 11, paragraphe (4) du projet de loi.
[28] Voir l'article 4, paragraphe (1), lettre (a) de la loi modifiée du 2 août 2002 et l'article 5, paragraphe (1), lettre (b) du règlement (UE) n° 2016/640.

de violation du présent règlement sur leur site internet immédiatement après que la personne faisant l'objet de cette décision a été informée de cette décision ». Aux termes du règlement européen, la publication doit mentionner, au minimum, le type et la nature de la violation et l'identité de la personne faisant l'objet de la décision.

L'article 14 du projet de loi met cette disposition en œuvre en précisant que les décisions publiées par la CSSF figureront sur son site Internet pendant une durée de cinq ans et que les données à caractère personnel figurant dans les décisions ne seront maintenues sur son site que pendant une période maximale de 12 mois.

Comme l'a soulevé le Contrôleur européen de la protection des données dans son avis du 10 février 2012 cité ci-haut[29], une telle publication constitue une ingérence dans la vie privée et les droits fondamentaux de la personne faisant objet de la décision. Elle doit dès lors, même en se conformant au règlement n° 596/2014, être limitée à ce qui est strictement nécessaire.

Ainsi, la CNPD souhaite préciser que, par l'indication de l'identité de la personne faisant l'objet de la décision, elle comprend que sont visés exclusivement le nom et le prénom de la personne concernée et estime qu'aucune autre donnée à caractère personnel ne devrait figurer dans la décision publiée sur le site de la CSSF.

Pour le surplus, la Commission nationale n'a pas d'autres observations à formuler.

Ainsi décidé à Esch-sur-Alzette en date du 2 décembre 2016.

La Commission nationale pour la protection des données

Tine A. Larsen Présidente	Thierry Lallemang Membre effectif	François Thill Membre suppléant

[29] Contrôleur européen de la protection des données, op. cit. section 2.6.