Comité de sécurité de l'information
chambre autorité fédérale

DELIBERATION N° 20/023 DU 6 OCTOBRE 2020 RELATIVE A LA COMMUNICATION DES DONNEES A CARACTERE PERSONNEL PAR LE SPF FINANCES A LA CELLULE DE TRAITEMENT DES INFORMATIONS FINANCIERES (CTIF), AU MOYEN DE L'APPLICATION WEB DOLSIS

Vu la loi du 15 août 2012 *relative à la création et à l'organisation d'un intégrateur de services fédéral*, en particulier l'article 35/1, §1, premier alinéa;

Vu la loi du 3 décembre 2017 *portant création de l'Autorité de protection des données*, en particulier les articles 111 et 114 ;

Vu la loi 5 septembre 2018 *instituant le comité de sécurité de l'information et modifiant diverses lois concernant la mise en œuvre du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE*, en particulier l'article 98 ;

Vu la demande de la Cellule de Traitement des Informations Financières (CTIF);

Vu le rapport du service publique fédéral Stratégie et Appui;

Vu le rapport de la présidente.

A. OBJET

1. La Cellule de Traitement des Informations financières (CTIF) est une autorité administrative indépendante, ayant la personnalité juridique, qui dépend du Service Public Fédéral des Finances. Elle a pour mission, en application de la loi du 18 septembre 2017 *relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l'utilisation des espèces*, de recevoir et d'analyser les déclarations de soupçon émanant des personnes et organismes visés par la loi[1]. Lorsque l'analyse révèle des indices suffisamment sérieux de blanchiment provenant d'une série d'infractions sous-jacentes ou de financement du terrorisme, la CTIF transmet le dossier aux autorités judiciaires.

[1] Voir les articles 47 et 76, § 3, de la loi du 18 septembre 2017 relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l'utilisation des espèces.

2. Les compétences de la CTIF lui permettent d'identifier des indices sérieux de blanchiment d'argent ou de financement du terrorisme par le biais d'une série d'infractions sous-jacentes, telles que le trafic de main d'œuvre clandestine, la criminalité organisée, l'abus de biens sociaux, l'abus de confiance ou les infractions liées à l'état de faillite. La collaboration avec certains services publiques fédéraux ainsi que des services de sécurité sociale est donc de nature à permettre à la CTIF de mieux pouvoir détecter certains des phénomènes criminels cités car elle serait alors en mesure de comparer les informations qu'elle possède (opérations financières, documents fournis par une personne intervenant dans un dossier) à tout élément permettant de se faire une idée précise de la situation socio-économique de la personne sur laquelle porte l'analyse.

3. L'article 81, § 1, alinéa 1, 4°, de la loi du 18 septembre 2017 permet à la Cellule de Traitement des Informations financières de s'adresser aux services administratifs de l'Etat afin de se faire communiquer les renseignements qu'elle juge utile à l'accomplissement de sa mission.

4. Vu ce qui précède, les chambres réunies du Comité de sécurité de l'information ont autorisé la communication des données à caractère personnel par des institutions de sécurité sociale à la Cellule de Traitement des Informations financières, en particulier des données des registres Banque-carrefour, de la banque de données DIMONA, du fichier du personnel, de la banque de données DmfA, du répertoire des employeurs, du fichier des déclarations de travaux, du cadastre LIMOSA, du fichier GOTOT, du répertoire des CPAS (LivingWages), du répertoire de l'ONEm (UnemploymentData), du répertoire de l'ONSS (Activités complémentaires) et du cadastre des pensions (délibération n° 14/058 du 2 septembre 2014, modifiée le 7 juillet 2020 et le 1ier septembre 2020).

5. L'ancien Comité sectoriel pour l'Autorité Fédérale a également autorisé par délibération n°18/2018 du 3 mai 2018 la communication de certaines données à caractère personnel par le SPF Finances à la CTIF dans le cadre de l'exercice de ses missions de lutte contre le blanchiment et le financement du terrorisme et ce aux mêmes conditions que celles visées dan la délibération AF n° 30/2015 du 10 décembre 2015 qui autorise le demandeur à avoir accès à des données du SPF Finances pour la même finalité, à savoir vérifier si les soupçons de blanchiment et de financement du terrorisme des déclarants sont confirmés et s'il existe des indices sérieux que des capitaux blanchis proviennent d'une des formes graves de criminalités sous-jacentes visées par la loi du 18 septembre 2017 précitée.

6. La CTIF a été autorisé de recevoir l'information suivante des personnes faisant l'objet d'une déclaration de soupçon de blanchiment de capitaux et/ou de financement du terrorisme :

- numéro de référence cadastrale du bien immobilier ;

- nature du bien immobilier selon le code de construction du Cadastre (maison, terrain, appartement, …) ;

- superficie de la parcelle cadastrale ;

- année de construction ;droits réels liés à la parcelle cadastrale (usufruit, nue-propriété, …), identité des détenteurs de droits réels sur le bien immobilier (numéro registre national des personnes physiques, nom, prénom, date de naissance et adresse connue de l'Administration générale de la Documentation patrimoniale) ;

- mutations au niveau des droits réels limitées à 10 ans précédant la date de consultation(modifications/ changements des éléments substantiels des droits réels afférents à une parcelle cadastrale et de leur(s) titulaire(s)) ;

- revenu cadastral de la parcelle.

7. Le CTIF demande actuellement l'autorisation formelle de recevoir les données à caractère personnel susmentionnées du SPF Finances *via l'application web Dolsis de la Banque carrefour de la sécurité sociale*.

8. L'application web Dolsis a été spécialement conçue pour déverrouiller des sources authentiques pour les services de contrôle et d'inspection des communautés, des régions et du gouvernement fédéral. Les modalités d'application de Dolsis ont été fixées par la recommandation n° 12/01 du 8 mai 2012 de l'ancien comité sectoriel de la sécurité sociale et de la santé.

II. TRAITEMENT DE LA DEMANDE

A. RECEVABILITE ET COMPETENCE DU COMITE

9. En vertu de l'article 35/1, §1, premier alinéa, de la loi du 15 août 2012 *à la création et à l'organisation d'un intégrateur de services fédéral* la communication de données à caractère personnel par des services publics et des institutions publiques de l'autorité fédérale à des tiers autres que les institutions de sécurité sociale visées à l'article 2, alinéa 1er, 2°, de la loi du 15 janvier 1990 *relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale* doit faire l'objet une délibération préalable de la chambre autorité fédérale du comité de sécurité de l'information, dans la mesure où les responsables du traitement de l'instance qui communique et des instances destinatrices ne parviennent pas, en exécution de l'article 20 de la loi du 30 juillet 2018 *relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel*, à un accord concernant la communication ou au moins un de ces responsables du traitement demande une délibération.

10. Le Comité de sécurité de l'information note que la communication des données à caractère personnel prévues a déjà été autorisée par l'ancien Comité sectoriel de l'Autorité Fédérale lors de la délibération n° 18/2018 du 3 mai 2018, et que l'application vise spécifiquement l'utilisation de l'application Web Dolsis de la Banque carrefour de la sécurité sociale. Conformément à l'article 111 de la loi précitée du 30 juillet 2018, les autorisations accordées par les comités sectoriels de la Commission pour la protection de la vie privée restent valables pour l'entrée en vigueur de la loi en question, sans préjudice des pouvoirs de contrôle de l'Autorité de protection des données.

B. QUANT AU FOND

B.1. RESPONSABILITE

11. Conformément à l'article 5.2 du règlement général sur la protection des données (ci-après dénommé «RGPD»), le SPF Finances (instance qui transfert les données) et le CTIF (instance destinataire) en tant que responsables du traitement sont responsables du respect des principes du RGPD et devraient être en mesure de le démontrer.

12. Le Comité de sécurité de l'information rappelle que le responsable du traitement doit tenir un registre des activités de traitement effectuées sous sa responsabilité dans les conditions prévues à l'article 30 du RGPD.

B.2. LICEITE

13. Conformément à l'article 5.1 a) RGPD, les données à caractère personnel doivent être traitées d'une manière licite à l'égard de la personne concernée. Cela signifie que le traitement envisagé doit être fondé sur l'un des motifs juridiques énoncés à l'article 6 RGPD.

14. Le Comité note que le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement (article 6.1 e) RGPD. En vertu de la loi du 18 septembre 2017 *relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l'utilisation des espèces*, la CTIF a pour mission d'analyser les informations faisant état de soupçons émanant de personnes et d'institutions visées par la loi. Si l'analyse révèle des preuves sérieuses de blanchiment d'argent fondées sur une série d'infractions sous-jacentes ou d'indications de financement du terrorisme, la CTIF transmettra le dossier aux autorités judiciaires.

15. Compte tenu de ce qui précède, le Comité de sécurité de l'information considère que le traitement prévu des données à caractère personnel est licite.

B.3. LIMITATION DES FINALITES

16. Article 5.1 b) RGPD ne permet le traitement de données à caractère personnel que pour des fins déterminées, explicites et légitimes (principe de finalité). En outre, les données ne peuvent pas faire l'objet d'un traitement ultérieur d'une manière incompatible avec ces objectifs.

17. La communication de données à caractère personnel a pour objet d'identifier des preuves sérieuses de blanchiment d'argent ou de financement du terrorisme sur la base d'un certain nombre d'infractions sous-jacentes, telles que le trafic de travailleurs clandestins, la criminalité organisée, l'abus de biens de l'entreprise, l'abus de confiance ou une infraction liée à l'état de faillite. Grâce à sa coopération avec un certain nombre d'institutions publiques, tant fédérales que sociales, le CTIF sera en mesure de mieux détecter les faits criminels susmentionnés en comparant les informations qu'il détient (opérations financières, documents fournis par une personne intervenant dans un dossier) avec des éléments permettant de décrire la situation socio-économique de la personne concernée.

18. Compte tenu de ce qui précède, le Comité de sécurité de l'information considère que les finalités de la communication envisagée de données à caractère personnel sont déterminées, explicites et légitimes.

19. L'article 5, paragraphe 1, point b), du RGPD dispose également que les données à caractère personnel ne peuvent être traitées d'une manière incompatible avec leurs objectifs initiaux. Afin d'établir si les finalités d'un traitement ultérieur sont compatibles avec celles pour lesquelles les données à caractère personnel ont été collectées initialement, le responsable du traitement, après avoir respecté toutes les exigences liées à la licéité du traitement initial, devrait tenir compte, entre autres: de tout lien entre ces finalités et les finalités du traitement

ultérieur prévu; du contexte dans lequel les données à caractère personnel ont été collectées, en particulier les attentes raisonnables des personnes concernées, en fonction de leur relation avec le responsable du traitement, quant à l'utilisation ultérieure desdites données; la nature des données à caractère personnel; les conséquences pour les personnes concernées du traitement ultérieur prévu; et l'existence de garanties appropriées à la fois dans le cadre du traitement initial et du traitement ultérieur prévu.[2]

20. Les données à caractère personnel ont été recueillies à l'origine dans le cadre des missions statutaires du Service de documentation patrimoniale du SPF concernant 1) l'établissement de la documentation cadastrale, 2) la réalisation de l'objectif fiscal du cadastre, 3) l'objectif documentaire du cadastre, en particulier la conservation et la mise à jour de la documentation, d'une part, et la communication des données cadastrales et la fourniture de copies des documents cadastraux, d'autre part, et 4) le service de sécurité juridique. La communication des données à des tiers et à d'autres institutions est limitée aux cas prévus par le législateur, conformément à l'article 337 du code de l'impôt sur le revenu.

« Les fonctionnaires de l'administration des contributions directes et de l'administration du cadastre restent dans l'exercice de leurs fonctions, lorsqu'ils communiquent aux autres services administratifs de l'Etat, y compris les parquets et les greffes des cours et de toutes les juridictions aux Communautés, aux Régions et aux établissements ou organismes publics visés à l'article 329 , les renseignements qui sont nécessaires à ces services, établissements ou organismes pour assurer l'exécution des dispositions légales ou réglementaires dont ils sont chargés. »

21. Compte tenu de l'article 337 du Code de l'impôt sur le revenu et de la loi du 18 septembre 2017 *relative à la prévention du blanchiment d'argent et du financement du terrorisme et à la limitation de l'utilisation des espèces*, le Comité de sécurité de l'information établit un lien suffisant entre les objectifs de la collecte initiale et les objectifs du traitement ultérieur envisagé. Le Comité de sécurité de l'information considère donc que l'objet du traitement ultérieur est compatible avec l'objectif pour lequel les données à caractère personnel ont été initialement collectées.

B.4. PROPORTIONALITE

B.4.1. Minimisation des données

22. L'article 5.1 b) du RGPD dispose que les données à caractère personnel doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées («minimisation des données»).

23. L'ancien Comité sectoriel pour l'Autorité Fédérale a estimé que les informations demandées semblaient nécessaires à l'exécution des missions légales de la CTIF. Ces informations permettent de confirmer ou de réfuter les indications sérieuses de blanchiment d'argent provenant de la traite des êtres humains, de confirmer ou de réfuter la déclaration d'un suspect selon laquelle ses revenus proviennent de la vente de bâtiments, de procéder à la

[2] Considération 50 du RGDP.

saisie des bâtiments ou de procéder à des vérifications parce qu'il y a des indices de fraude concernant ces bâtiments.

24. Compte tenu de ce qui précède, le Comité de sécurité de l'information considère que les données à caractère personnel sont adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées.

B.4.2. Limitation de la conservation

25. En ce qui concerne le délai de conservation, le Comité rappelle que les données à caractère personnel ne doivent plus être conservées sous une forme permettant d'identifier les personnes concernées au-delà des finalités pour lesquelles les données à caractère personnel sont traitées.

26. Les données consultées seront conservées pendant 10 ans, compte tenu de la durée légale de conservation des données relatives à l'identification des clients et aux transactions, qui est imposée aux personnes et institutions tenues de signaler les transactions financières suspectes (art. 60 de la loi du 18 septembre 2017).

27. Cette période semble être conforme à l'article 5.1 e) du RGDP. Le Comité note également qu'il convient, dans la pratique, d'établir une distinction entre les différentes méthodes de conservation dans le temps. Le traitement d'un dossier permanent nécessite la conservation des données de manière à ce que celles-ci soient disponibles et accessibles aux fonctionnaires responsables de la gestion du dossier. Une fois qu'un fichier peut être archivé, l'accès et la disponibilité des données sont limités pour la méthode de conservation choisie. Dès que la conservation n'est plus utile, les données ne doivent plus être conservées sous une forme permettant l'identification des personnes concernées.

B.5. TRANSPARANCE

28. Conformément à l'article 14 du RGDP, le responsable du traitement doit fournir à la personne concernée certaines informations concernant le traitement de données à caractère personnel non obtenues de la personne concernée. Cette information n'est pas nécessaire l'obtention ou la communication des informations sont expressément prévues par le droit de l'Union ou le droit de l'État membre auquel le responsable du traitement est soumis et qui prévoit des mesures appropriées visant à protéger les intérêts légitimes de la personne concernée (article 14.5 RGPD), en particulier l'article 337 du Code de l'impôt sur le revenu, en ce qui concerne la communication des données du cadastre par l'administration publique fédérale.

29. Le Comité de sécurité de l'information constate que les règles applicables prévoient effectivement des mesures appropriées pour protéger les intérêts légitimes de la personne concernée.

B.6. SECURITE

30. Les données à caractère personnel doivent être traitées en prenant des mesures techniques ou organisationnelles appropriées de manière à assurer une sécurité adéquate, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle («intégrité et confidentialité»).

31. La communication des données à caractère personnel prévues par le SPF Finances à la CTIF sera effectuée par l'intermédiaire de l'application web DOLSIS de la Banque carrefour de la sécurité sociale, qui est déjà utilisée pour la communication de données à caractère personnel par les institutions de sécurité sociale. L'accès aux banques de données à caractère personnel en question n'est autorisé que pour autant que les mesures de sécurité contenues dans la recommandation n° 12/01 du 8 mai 2012 de l'ancien Comité sectoriel de la sécurité sociale et de la santé liées à l'application DOLSIS soient effectivement respectées par la CTIF.

32. Le but de l'application Web DOLSIS est de visualiser certaines données personnelles du réseau de sécurité sociale et des bases de données des institutions fédérales dans le cadre de la réalisation des tâches de l'utilisateur. L'application Web DOLSIS ne fournit pas la fonctionnalité nécessaire pour stocker ces données dans ses propres bases de données. Dans la mesure où une autorité souhaite stocker des données à caractère personnel à partir du réseau de sécurité sociale, il est souhaitable de ne pas utiliser l'application web DOLSIS, mais (après délibération du Comité de sécurité de l'information) les services Web de la Banque carrefour de la sécurité sociale.

33. Le Comité rappelle que, dans certains cas, l'article 35 du RGPD impose au responsable du traitement de procéder à une évaluation de l'impact des activités de traitement envisagées sur la protection des données à caractère personnel avant le traitement. À cet égard, le Comité se référerait aux "lignes directrices pour les évaluations d'impact sur la protection des données et déterminerait si le traitement présente un "risque probablement élevé" au sens du règlement (CE) no 2016/679 du groupe de travail article 29 et de la recommandation de la Commission no 01/2018 du 28 février 2018 relative à la protection de la vie privée en ce qui concerne l'évaluation d'impact sur la protection des données et la consultation préalable'.

34. Si cette évaluation montre qu'il y a lieu de prendre des mesures supplémentaires, les parties concernées présentent, de leur propre initiative, une demande de modification du présent débat. Le cas échéant, la communication de données à caractère personnel n'a lieu que lorsque l'autorisation requise du comité a été obtenue. Si l'analyse d'impact sur la protection des données montre qu'il existe un risque résiduel élevé, le demandeur doit soumettre le traitement des données prévu à l'Autorité de la protection des données, conformément à l'article 36.1 du RGPD.

Par ces motifs,

la chambre autorité fédérale du Comité de sécurité de l'information

conclut que la communication des données à caractère personnel par le SPF Finances à la Cellule de Traitement des Informations financières (CITF) via l'application web Dolsis, en vue de réaliser ses missions, est autorisée moyennant le respect des mesures de protection des données définies, en particulier les mesures en matière de limitation de la finalité, de minimisation des données, de limitation de la durée de conservation des données et de sécurité de l'information.

Le comité de sécurité de l'information indique que les responsables du traitement sont tenus de procéder, le cas échéant, à une évaluation d'impact sur la protection des données. Si cette évaluation montre qu'il y a lieu de prendre des mesures supplémentaires pour protéger les droits et libertés des personnes concernées, les parties sont tenues de soumettre les dispositions relatives au traitement des données modifiées au Comité de sécurité de l'information.

M. SALMON
Présidente