N° 7024[4]

CHAMBRE DES DEPUTES

Session ordinaire 2016-2017

P R O J E T D E L O I

portant mise en oeuvre du règlement (UE) 2015/751 du Parlement européen et du Conseil du 29 avril 2015 relatif aux commissions d'interchange pour les opérations de paiement liées à une carte, et portant modification:

1. **de la loi modifiée du 5 avril 1993 relative au secteur financier;**
2. **de la loi modifiée du 23 décembre 1998 portant création d'une commission de surveillance du secteur financier;**
3. **de la loi modifiée du 5 août 2005 sur les contrats de garantie financière;**
4. **de la loi modifiée du 11 janvier 2008 relative aux obligations de transparence des émetteurs;**
5. **de la loi modifiée du 17 décembre 2010 concernant les organismes de placement collectif;**
6. **de la loi modifiée du 12 juillet 2013 relative aux gestionnaires de fonds d'investissement alternatifs;**

   et

7. **de la loi modifiée du 18 décembre 2015 relative à la défaillance des établissements de crédit et de certaines entreprises d'investissement**

* * *

AVIS DE LA COMMISSION NATIONALE POUR LA PROTECTION DES DONNEES

(16.3.2017)

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 de 2002"), 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"*.

Le 29 juillet 2016, Monsieur le Ministre des Finances a déposé à la Chambre des députés le projet de loi n° 7024 relative aux commissions d'interchange et modifiant différentes lois relatives aux services financiers secteur financier (ci-après désigné „le projet de loi"). Au vu des changements apportés par le projet de loi sur les traitements des données à caractère personnel mis en oeuvre par les entités tombant dans le champ d'application du projet de loi, la Commission nationale regrette de ne pas avoir été saisie formellement dudit projet de loi par Monsieur le Ministre des Finances, alors même que le Conseil d'Etat, dans son avis du 13 décembre 2016 a souligné *„que la Commission nationale pour la*

protection des données devrait être entendue en son avis, vu les enjeux, en l'occurrence, au niveau de la protection des données à caractère personnel"[1].

Dès lors et en application de l'article 32, paragraphe (3), lettre (f) de la loi modifiée du 2 août 2002, la Commission nationale a pris la décision de se saisir elle-même pour aviser le présent projet de loi.

Selon l'exposé des motifs, le projet de loi a un double objectif, à savoir la mise en oeuvre du règlement (UE) n° 2015/751 du Parlement européen et du Conseil du 29 avril 2015 relatif aux commissions d'interchange pour les opérations de paiement liées à une carte, ainsi que la modification de plusieurs lois applicables au secteur financier dont, notamment, la loi modifiée du 5 avril 1993 relative au secteur financier (ci-après „la loi modifiée du 5 avril 1993").

Plus particulièrement, le projet de loi vise à faciliter l'externalisation, autrement appelée la sous-traitance, des services par une personne physique ou morale soumise à la surveillance prudentielle de la Commission de Surveillance du Secteur Financier (ci-agrès désignée „la CSSF") en vertu de la loi modifiée du 5 avril 1993 ou établie au Luxembourg et soumise à la surveillance de la Banque centrale européenne (ci-après désignée „l'entité surveillée").

Pour atteindre cet objectif, le projet de loi remplace l'exception au secret professionnel relative à la sous-traitance actuellement prévue à l'article 41, paragraphe (5) de la loi modifiée du 5 avril 1993 par trois nouvelles exceptions, à savoir une exception pour la sous-traitance des activités à une entité établie au Luxembourg et surveillée par la CSSF, la Banque Centrale Européenne (ci-après la „BCE") ou le Commissariat aux assurances (ci-après le „CAA") (ci-après désignée „la sous-traitance surveillée"), une exception pour la sous-traitance à une entité du groupe auquel l'entité surveillée appartient (ci-après désignée „la sous-traitance intragroupe"), ainsi qu'une exception pour la sous-traitance *„dans tous les autres cas"* (ci-après désignée „la sous-traitance extragroupe").

L'externalisation des activités par une entité surveillée implique dans la plupart des cas des traitements de données à caractère personnel et, comme l'a souligné le Conseil d'Etat dans son avis du 13 décembre 2016[2], une augmentation du risque de divulgation des données. Il est dès lors primordial d'entourer la sous-traitance d'un niveau élevé de garanties pour assurer la protection et la confidentialité des données à caractère personnel du début à la fin de la sous-traitance.

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, à savoir l'article 41 de la loi modifiée du 5 avril 1993.

Elle rappelle que le règlement n° 2016/679 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 (règlement général sur la protection des données) (ci-après „le RGPD") sera applicable à partir du 25 mai 2018. Il convient ainsi d'analyser le projet de loi à la lumière de la loi modifiée du 2 août 2002 qui est la législation actuellement en vigueur, d'une part, et du nouveau Règlement européen d'autre part.

I. Quant à la terminologie

Alors que le RGPD consacre la notion de „groupe d'entreprises"[3], la CNPD s'interroge sur la précision que les services doivent être sous-traités *„intégralement"* à l'intérieur du groupe. *„[L]es auteurs du projet de loi ont-ils voulu dire que l'externalisation portera sur la totalité d'un service déterminé? Quel régime s'appliquera dans ce cas en présence d'une externalisation partielle d'un service? Le régime défini par la CSSF dans ses circulaires sera-t-il d'application? Ou est-ce que les auteurs du projet de loi ont visé l'hypothèse d'une externalisation exclusivement effectuée au sein du groupe auquel appartient l'établissement concerné?"*[4].

Le commentaire des articles précise uniquement que la sous-traitance en cascade à l'intérieur du groupe serait permise en vertu de l'alinéa en question[5].

---

1 Avis du Conseil d'Etat du 13 décembre 2016, doc. parl. n° 7024/02, p. 4.

2 Avis du Conseil d'Etat du 13 décembre 2016. doc. parl. n° 7024/02, p. 4.

3 Par exemple, voir l'article 4, paragraphe (19).

4 Avis du Conseil d'Etat du 13 décembre 2016, doc. parl. n° 7024/02, p. 7.

5 Commentaire des articles, p. 15.

Il pourrait en être déduit que la disposition relative à la sous-traitance intragroupe vise l'hypothèse où la totalité des services sous-traités sera fournie par une entité du groupe auquel appartient l'entité surveillée et qu'afin que ce dernier puisse bénéficier de l'exception au secret professionnel établie par la disposition, un sous-traitant n'appartenant pas au même groupe que l'entité surveillée ne pourra pas être recruté.

Pour autant, cette disposition en elle-même ne précise pas avec une clarté suffisante les conditions sous lesquelles les entités surveillées seront exemptées de l'obligation au secret professionnel. La Commission nationale estime dès lors nécessaire de modifier le projet de loi afin d'y définir davantage les conditions dans lesquelles la sous-traitance intragroupe pourrait avoir lieu et, notamment, la spécification qu'elle doit avoir lieu *„intégralement à l'intérieur du groupe"*.

II. Quant à la relation contractuelle entre le responsable du traitement et le sous-traitant

La loi modifiée du 2 août 2002 et le RGPD soumettent le recours par un responsable du traitement à un sous-traitant à la conclusion d'un contrat ou d'un autre acte juridique écrit, qui doit comporter au moins les clauses obligatoires figurant dans les deux textes législatifs[6]. Le pays d'établissement du sous-traitant n'a pas d'incidence sur la nécessité de conclure un tel contrat, la conclusion étant obligatoire dans tous les cas de sous-traitance.

S'agissant de la sous-traitance surveillée, l'alinéa 1er de l'article 41, paragraphe (2*bis*), tel qu'ajouté par le projet de loi sous examen, subordonne le recours par une entité surveillée à un sous-traitant à la conclusion d'un contrat de service entre les deux parties.

S'agissant de la sous-traitance intragroupe et extragroupe, cette exigence ne ressort pas clairement des alinéas 2 et 3 de l'article sous examen. En effet, ces dispositions ne soumettent pas la transmission des données confidentielles dans le cadre d'une sous-traitance à la conclusion d'un contrat de service. Le projet de loi fait uniquement mention d'un „accord de confidentialité" que les entités surveillées pourraient mettre en place avec les sous-traitants afin de leur transmettre des données confidentielles.

Ni le projet de loi, ni le commentaire des articles ne fournissent de définition ou d'explications quant à la forme ou au contenu dudit „accord de confidentialité". En l'absence de précisions à cet égard, la Commission nationale part du postulat que, contrairement à la sous-traitance surveillée, les auteurs du projet de loi n'entendent pas subordonner la sous-traitance intragroupe ou la sous-traitance extragroupe à la conclusion d'un contrat de service.

Alors que la Commission nationale constate que des circulaires de la CSSF prévoient que la sous-traitance doit faire l'objet d'un contrat[7], elle estime qu'afin d'écarter tout risque d'insécurité juridique et pour créer une base légale unique qui garantirait pour toutes les relations de sous-traitance la protection et la confidentialité des données, il est nécessaire de spécifier dans le projet de loi que la sous-traitance doit être encadrée par un contrat ce service, quelles que soient les modalités de la sous-traitance.

III. Quant à la sous-traitance en cascade

Comme soulevé au point I., le commentaire des articles relatif à la sous-traitance intragroupe précise que la sous-traitance en cascade serait permise en vertu du nouvel alinéa 2 du paragraphe (2*bis*) de l'article 41[8]. Alors que le projet de loi n'y fait aucune référence dans le cadre de la sous-traitance surveillée ou la sous-traitance extragroupe, il est envisageable que la sous-traitance en cascade puisse également être mise en oeuvre dans ces deux cas.

En l'absence d'obligation de conclure un contrat de service, l'article 14 du projet de ioi sous examen ne prévoit pas de base juridique contraignante en vertu de laquelle la sous-traitance en cascade par les

---

6 Les clauses obligatoires sont prévues à l'article 22, paragraphe (2) de la loi modifiée du 2 août 2002 et à l'article 28, paragraphes (2) et (3) du RGPD.

7 Circulaire CSSF 12/552, telle que modifiée, point 207 *„Tout accord de sous-traitance fait l'objet d'un contrat officiel et détaillé (cahier des charges inclus."*; la Circulaire CSSF 05/178, p. 3 *„Toute sous-traitance doit être formalisée par un contrat de services avec un cahier des charges qui tient compte des conditions énumérées ci-dessous."*

8 Commentaire des articles, p. 15.

entités surveillées doit faire l'objet d'un contrat et établissant des critères de contrôle que les entités surveillées devraient adopter dans le cadre de la sous-traitance en cascade.

S'il est vrai que la loi modifiée du 2 août 2002 ne comporte pas d'indications spécifiques concernant la sous-traitance en cascade, le RGPD subordonne, en revanche, expressément le recours à la sous-traitance en cascade à l'autorisation écrite préalable du responsable du traitement[9]. Le sous-traitant doit ainsi obtenir soit une autorisation préalable spécifique, soit une autorisation préalable générale pour pouvoir recruter d'autres sous-traitants. Dans le cas où le responsable du traitement accorderait une autorisation générale, le sous-traitant sera obligé d'informer le responsable de tout changement prévu concernant l'ajout ou le remplacement d'autres sous-traitants afin de donner la possibilité à ce dernier de s'opposer à de tels changements.

La Commission nationale relève d'ailleurs que l'importance de maîtriser la sons-traitance informatique en cascade a été soulevée dans des circulaires de la CSSF[10] .

Compte tenu de l'importance de maîtriser la sous-traitance en cascade et afin d'établir une base légale uniforme imposant un contrat de service pour la sous-traitance en cascade, la CNPD recommande de modifier l'article 14 du projet de loi pour imposer que l'obligation de conclure un contrat de service s'étend à la sous-traitance en cascade et que ce contrat doit indiquer les conditions dans lesquelles le sous-traitant peut avoir recours à d'autres sous-traitants.

IV. Quant aux transferts de données vers des pays tiers

En vertu de l'article 41, paragraphe (2*bis*), alinéas 2 et 3, tel qu'ajouté par le projet de loi, les entités régulées pourraient transmettre des données confidentielles, y compris l'historique des transactions des clients, à des sous-traitants établis hors du Luxembourg dans le cadre de la sous-traitance intragroupe et extragroupe. Par ailleurs, le texte actuel ne s'oppose, en principe, pas à ce qu'un sous-traitant recruté sur base de l'alinéa 1er sous-traite des services à un sous-traitant sur base de l'alinéa 2, donc faisant parti du même groupe que le sous-traitant, établi dans un pays tiers.

A. *Les règles en matière de protection des données*

Dans la législation applicable en matière de protection des données, les transferts de données vers des pays tiers sont strictement encadrés par la loi.

Conformément à la loi modifiée du 2 août 2002, les transferts vers des pays tiers ne sont possibles que si la Commission Européenne a désigné le pays tiers en question comme assurant un niveau de protection adéquat aux termes d'une „décision d'adéquation". A l'heure actuelle, l'Islande, le Liechtenstein, la Norvège, la Suisse, l'Andorre, les îles de Guernesey, Jersey, Man et Féroé, l'Argentine, l'Uruguay, la Nouvelle Zélande et l'Israël et les sociétés tombant dans le champ d'application de la *„Canadian Personal Information Protection and Electronic Documents Act"* au Canada font l'objet d'une décision d'adéquation. Aux Etats-Unis, seules les entreprises qui ont volontairement adhérés au *„EU-U.S. Privacy Shield Framework"* peuvent directement recevoir des données provenant de l'Union européenne.

Le RGPD reprend le régime des décisions d'adéquation et vise à maintenir les décisions rendues sur base de la Directive 95/46/CE 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 (ci-après „la Directive 95/46/CE"), qui a été transposée en droit luxembourgeois par la loi modifiée du 2 août 2002.

A défaut de décision d'adéquation, un responsable du traitement peut mettre en place des garanties appropriées pour pourvoir effectuer des transferts vers des pays tiers, conformément à l'article 19 de la loi de 2002. Ces garanties appropriées peuvent actuellement résulter des clauses contractuelles types adoptées par la Commission européenne en application de l'article 26, paragraphe (4) de la Directive 95/46/CE ou des règles contraignantes d'entreprise approuvées par les autorités de protection

9 RGPD, art. 28, paragraphe (2).

10 Circulaire CSSF 12/552, telle que modifiée, point 186; Circulaire CSSF 05/178, p. 3.

des données des Etats membres concernés. Le recours à ces types de transfert de données nécessite actuellement l'autorisation préalable de la CNPD[11].

La possibilité d'effectuer des transferts sur base de garanties appropriées a été maintenue dans les articles 46 et 47 du RGPD. Contrairement à la loi actuellement en vigueur, le RGPD liste les garanties appropriées qui ne nécessiteront, en principe, plus d'autorisation préalable de la part de la CNPD à l'avenir, tel que des règles d'entreprises contraignantes approuvées conformément à la procédure prévue par le RGPD.

En l'absence d'une décision d'adéquation ou des garanties appropriées, la loi de 2002 et le RGPD permettent aux responsables du traitement de fonder le transfert de données vers des pays tiers sur des dérogations pour des situations spécifiques limitativement prévues par ces textes, par exemples, avec le consentement de la personne concernée ou si le transfert est nécessaire à l'exécution d'un contrat auquel la personne concernée et le responsable du traitement sont parties ou à l'exécution des mesures précontractuelles prises à la demande de la personne concernée[12].

B. *La sous-traitance intragroupe et extragroupe*

Le projet de loi, quant à lui, pose une double condition que les entités régulées doivent remplir afin de recourir à la sous-traitance intragroupe et à la sous-traitance extragroupe. D'une part, les entités surveillées doivent s'assurer que la sous-traitance est entourée d'une obligation de confidentialité. Les personnes au service des sous-traitants doivent ainsi soit être soumises à une obligation de secret professionnel, soit être liées par un accord de confidentialité. D'autre part, les clients des entités régulées doivent être informés de la sous-traitance intragroupe et doivent donner leur accord préalable par écrit à la sous-traitance extragroupe.

Dans l'optique de la CNPD, la double condition prévue par le projet de loi ne suffit pas pour assurer que les données à caractère personnel soient protégées lors du transfert vers et le traitement par le sous-traitant dans un pays tiers.

En l'absence d'une obligation de secret professionnel, la seule garantie serait l'accord de confidentialité. Compte tenu de l'absence des précisions dans le projet de loi quant au format et au contenu de „l'accord de confidentialité", il n'y a aucune certitude qu'un tel accord mettrait en place des garanties suffisantes pour protéger les données.

En ce qui concerne la sous-traitance intragroupe, la CNPD note qu'en matière de protection des données, la simple information préalable de la personne concernée n'est pas une base légale pour effectuer un transfert de données vers un pays tiers.

Pour ce qui est de la sous-traitance extragroupe, le client doit, selon l'article 41, paragraphe (2*bis*), alinéa 3, tel qu'ajouté par le projet de loi, donner son accord préalable par écrit à *„la sous-traitance des services sous-traités, [au] type de renseignements transmis dans le cadre de la sous-traitance et [au] pays d'établissement des entités prestataires des services sous-traités"*. Dans l'optique de la CNPD, l'accord donné sur base de ces informations ne saurait pas être considéré comme étant éclairé. En effet, comme soulevé par le Conseil d'Etat dans son avis du 13 décembre 2016[13], les informations qui devraient être fournies en vertu du projet de loi ne sont pas aussi complètes que les informations devant être fournies au client en vertu du point 193 de la Circulaire CSSF 12/552 pour que ce dernier puisse donner son accord à la levée du secret professionnel.

De plus, en matière de protection des données à caractère personnel, l'article 19 de la loi modifiée du 2 août 2002 énonce les dérogations au principe d'interdiction des transferts vers des pays tiers, sur base desquelles un responsable du traitement peut transférer des données vers un pays tiers. Une de ces dérogations est le consentement de la personne concernée[14].

---

11 Cependant, le projet de loi n° 7049 portant modification de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel envisage d'abolir l'obligation pour le responsable du traitement d'obtenir une autorisation préalable, pour le cas où il aurait recours à ces mesures.

12 Loi modifiée du 2 août 2002, art. 19, paragraphe (1) et RGPD, art. 49.

13 Avis du Conseil d'Etat du 13 décembre 2016, doc. parl. n° 7024/02, p. 8.

14 Loi modifiée du 2 août 2002, art. 19, paragraphe (1), lettre (a).

Le consentement figure également à l'article correspondant dans le RGPD relatif aux „dérogations pour des situations particulières"[15], qui précise qu'afin de constituer une base légale pour le transfert de données, le consentement de la personne concernée doit être explicite et le responsable du traitement doit avoir informé la personne concernée *„des risques que ce transfert pouvait comporter pour elle en raison de l'absence de décision d'adéquation et de garanties appropriées"*[16].

Aux termes de l'article 2, lettre (c) de la loi de 2002, le consentement de la personne concernée doit être libre, spécifique et informé. Le RGPD reprend ces exigences dans son article 4, numéro (11) et ajoute qu'en plus d'être libre, spécifique et éclairé, il faut encore que le consentement soit univoque et qu'il résulte d'une déclaration ou d'un acte positif clair. Il en résulte que la transparence est un aspect fondamental du consentement[17]. La personne concernée doit recevoir toutes les informations nécessaires à la bonne compréhension des traitements mis en oeuvre par le responsable du traitement.

A cet égard, le Groupe de Travail „Article 29" a précisé qu'afin d'être informé ou éclairé, le consentement doit *„être fondé sur l'appréciation et la compréhension des faits et des conséquences d'une action"*[18]. Dans le cadre des transferts des données vers des pays tiers, cela implique que la personne concernée doit avoir été informée des circonstances particulières du transfert, afin de permettre à cette dernière de *„donner son consentement en pleine connaissance de cause"*[19].

Au vu ce qui précède et du fait que les entités surveillées ne seraient tenues, en vertu du projet de loi sous avis, de fournir que des informations très générales sur la sous-traitance, l'accord du client, dans le format prévu par le projet de loi, ne saurait pas remplir les exigences établies par la loi de 2002 et par le RGPD et ne saurait des lors pas être considéré comme étant suffisamment informé et éclairé.

En tout état de cause, comme soulevé ci-avant, le consentement de la personne concernée constitue une dérogation au principe érigé par la loi de 2002 selon lequel le transfert des données à caractère personnel ne peut avoir lieu que si le pays en question assure un niveau de protection adéquat. A cet égard, le Groupe de Travail „Article 29" a précisé que ces dérogations ne devraient pas être utilisées pour les transferts qui puissent être qualifiés de répétitifs, massifs ou structurels[20]. Il est évident que le recours à un sous-traitant entraînerait dans la plupart des cas des transferts répétitifs, massifs et/ou structurels. Dans le même ordre d'idée, le RGPD précise que le consentement fait partie des *„dérogations pour des situations particulières"*.

Vu les volumes substantiels des données à caractère personnel qui seraient transmises entre le responsable du traitement et le sous-traitant[21], il serait plus opportun de recourir à des garanties appropriées, telles que des règles d'entreprises contraignantes ou des clauses contractuelles types, prévues par l'article 19 de le loi de 2002 et les articles 46 et 47 du RGPD, si des données sont transférées vers un pays, qui ne fait pas l'objet d'une décision d'adéquation.

La CNPD relève qu'une dérogation à une règle doit être interprétée de façon stricte[22]. En prévoyant que le transfert des données pourrait avoir lieu avec le consentement de la personne concernée, le projet de loi créerait en effet une application généralisée de la dérogation relative au consentement, ce qui va à l'encontre de l'esprit de la loi de 2002 et du RGPD.

Dès lors en ce qui concerne la protection des données à caractère personnel, la CNPD estime que la dérogation généralisée relate m consentement prévue par le projet de loi ne correspond pas aux critères établis par la loi de 2002 et par le RGPD et ne peut pas à lui seul servir de base légale pour le transfert de données vers des pays tiers.

---

15 RGPD, art. 49.

16 RGPD, art. 49, paragraphe (1), lettre (a).

17 Avis 15/2011 du Groupe de Travail „Article 29" sur la définition du consentement (WP 187), p. 10.

18 Ibid, p. 21.

19 Document de travail du Groupe de Travail „Article 29" relatif à une interprétation commune des dispositions de l'article 26, paragraphe 1, de la directive 95/46/CE du 24 octobre 1995 (WP 114), p. 14.

20 Document de travail du Groupe de Travail „Article 29" relatif à une interprétation commune des dispositions de l'article 26, paragraphe 1, de la directive 95/46/CE du 24 octobre 1995 (WP 114), p. 11 et 13.

21 Avis du Conseil d'Etat du 13 décembre 2016, doc. parl. n° 7024/02, p. 10.

22 Arrêt de la Cour de Justice de l'Union européenne du 22 novembre 2012, Probst. C-119/12, EU:C:2012:748, point 23; Arrêt de la Cour de Justice de l'Union européenne du 21 décembre 2016, Tele2 Sverige AB, C-203/15 et C-698/15, ECLI:EC:C:2016:970, point 89.

C. *Conclusion*

Vu l'absence d'une définition d'„accord de confidentialité", la Commission nationale estime que le projet de loi dans son état actuel n'entoure pas le transfert de données vers des pays tiers des garanties suffisantes.

Par ailleurs, la CNPD tient à souligner que l'accord du client, tel que prévu par le projet de loi, ne saurait pas être considéré comme étant informé et éclairé au sens de la loi de 2002 et du RGPD. Finalement, en tout état de cause, dans le cadre de la sous-traitance intragroupe et la sous-traitance extragroupe, telles que prévues par le projet de loi, le consentement généralisé ne pourra pas servir de base légale pour les entités régulées pour effectuer des transferts des données vers des pays tiers.

La CNPD estime donc que le projet de loi n'offre pas dans son état actuel un cadre juridique suffisant pour assurer que les données à caractère personnel des clients des entités régulées soient protégées lors d'un transfert vers un pays tiers.

Elle suggère dès lors de modifier le projet de loi afin d'y indiquer les conditions dans lesquelles ces transferts pourront avoir lieu, notamment en ce qui concerne des garanties à mettre en place entre l'entité régulée et les sous-traitants pour assurer la protection des données lors des transferts vers des pays tiers.

V. Quant à l'information de la personne concernée

Le droit à l'information de la personne concernée, bien que lié étroitement, est distinct de l'obligation du responsable du traitement de s'assurer que le consentement est informé et éclairé[23], est prévu à l'article 26 de la loi modifiée du 2 août 2002. En vertu de cet article, 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.

La liste des informations qui devront être fournies à la personne concernée sera étendue par le RGPD. Cette dernière doit ainsi être informée non seulement des finalités des traitements, mais également de leur base juridique[24]. En sus des informations qui sont obligatoires à l'heure actuelle, les personnes concernées recevront, entre autres, communication des intérêts légitimes poursuivis par le responsable du traitement lorsque le traitement est fondé sur cette base légale, la durée de conservation des données, le fait que le responsable du traitement a l'intention de transférer des données vers un pays tiers et l'existence d'une décision d'adéquation ou, le cas échéant, les garanties appropriées sur base desquelles le transfert aurait lieu, y compris comment avoir accès à ces garanties appropriées[25].

L'article 14, 2°, du projet de loi précise que le client de l'entité régulée devrait être informé au préalable par écrit *„des services sous-traités, du type de renseignements transmis dans le cadre de la sous-traitance et du pays d'établissement des entités prestataires des services sous-traités"* dans le cadre de la sous-traitance intragroupe.

S'agissant de la sous-traitance extragroupe, l'article 14, 3° du projet de loi obligerait l'entité régulée d'informer ses clients de *„la sous-traitance des services sous-traités, [au] type de renseignements transmis dans le cadre de la sous-traitance et (au) pays d'établissement des entités prestataires des services sous-traités"*.

Conformément à ses remarques relatives au consentement de la personne concernée, la CNPD estime que le projet de loi dans son état actuel ne permet au client ni de clairement prendre connaissance des conditions sous lesquelles la sous-traitance aurait lieu, ni de maîtriser ses données.

En effet, en vertu des règles actuelles établis par la CSSF dans la Circulaire CSSF 12/552, les clients doivent être informés de *„l'intérêt de [la] sous-traitance, de la spécificité de la finalité recherchée, du contenu de l'information transmise, du destinataire et de la localisation, ainsi que de la durée dans le temps"*[26], avant de donner leur accord à la levée du secret professionnel.

---

23 Avis 15 2011 du Groupe de Travail „Article 29" sur la définition du consentement (WP 187). p. 21.

24 RGPD, art. 13, paragraphe (1).

25 Ibidem, art. 13, paragraphe (1), lettre (d) et paragraphe (2).

26 Circulaire CSSF 12/552, telle que modifiée, point 193.

Ces informations sont davantage appropriées pour assurer que les clients soient clairement informés de la sous-traitance et les risques y associés. La CNPD estime nécessaire de modifier le projet de loi afin d'y prévoir que les clients doivent recevoir au moins les informations indiquées au point 193 de la Circulaire CSSF 12/552, sinon celles énumérées à l'article 14 du RGPD.

VI. Quant aux mesures de sécurité

Les banques et professionnels du secteur financier collectent et traitent une pléthore de données à caractères personnel relatives à leurs clients, y compris des données sensibles telles que des copies des pièces d'identité ou l'historique des transactions. Le traitement de ces données implique des risques non-négligeables, dans la mesure où la divulgation des données pourrait causer un préjudice grave aux clients. Ces risques augmentent avec l'utilisation accrue de nouveaux systèmes informatiques et de structures de sous-traitance de plus en plus complexes. En effet, en confiant leurs données à des sous-traitants, les entités surveillées *„pourrait perdre le contrôle exclusif de ces données …"*[27].

En permettant aux entités surveillées de recourir à la sous-traitance „simple" et à la sous-traitance en cascade, les nouvelles exceptions créées par le projet de loi engendrent dès lors des risques supplémentaires non-négligeables pour les entités surveillées et pour les clients.

Par ailleurs, les modifications apportées par le projet de loi sous avis ne se limitent pas à des exceptions au secret professionnel dans le cadre de la sous-traitance. Les paragraphes (3) et de l'article 41 projeté reformulent les paragraphes (3) et (4) de l'article 41 actuellement en vigueur. Ils précisent que, dans certains cas, des renseignements pourraient être transmis à des autorités nationales, européennes et étrangères chargées de la surveillance prudentielle de secteur financier ou de résolution, ainsi qu'à des actionnaires ou associés. Ces transferts impliquent également des risques, dans la mesure où des données à caractère personnel pourraient être communiquées à des tiers.

Tenant compte de ces risques, la CNPD s'interroge sur l'absence dans l'article du projet de loi sous examen des indications relatives à des mesures de sécurité devant être mises en place par les entités régulées pour assurer la sécurité et la confidentialité des données.

En matière de la protection des données à caractère personnel, les articles 22 et 23 de la loi modifiée du 2 août 2002 obligent le responsable du traitement de mettre en place des mesures techniques et organisationnelles nécessaires afin d'assurer la protection des données à caractère personnel. Cette obligation est reprise à l'article 32 du RGPD, en application duquel le responsable du traitement doit mettre en oeuvre les mesures appropriées afin de garantir un niveau de sécurité adapté au risque.

Eu égard au caractère sensible des données traitées, la CNPD suggère de préciser le texte du projet de loi en prévoyant que des mesures de sécurité doivent être mises en place par les entités surveillées lors de la sous-traitance et pour assurer la protection des données lors de la communication des données aux autorités, aux actionnaires et aux associés.

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

Ainsi décidé à Esch-sur-Alzette en date du 16 mars 2017.

La Commission nationale pour la protection des données

Tine A. LARSEN	Thierry LALLEMANG	Christophe BUSCHMANN
Présidente	*Membre effectif*	*Membre effectif*

27 Avis 05/2012 du Groupe de Travail „Article 29" sur l'informatique en nuage (WP 196), p. 6.

Impression: CTIE – Division Imprimés et Fournitures de bureau