N° 7184[13]

CHAMBRE DES DEPUTES

Session ordinaire 2017-2018

P R O J E T D E L O I

portant création de la Commission nationale pour la protection des données et 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, portant modification du Code du travail et de la loi modifiée du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'Etat et abrogeant la loi du 2 août 2002 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel

* * *

AVIS DU CONSEIL DE L'ORDRE DES AVOCATS DU BARREAU DE LUXEMBOURG

(30.3.2018)

Le Projet de loi fait suite au 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 95/45/CE (ci-après le « **RGPD** »).

Suite à la demande lui adressée par Monsieur le Ministre des Communications et des Médias en date du 22 août 2017, le Conseil de l'ordre exprime ci-après son avis sur le Projet de loi ayant pour objet la mise en œuvre du RGPD dans le contexte législatif luxembourgeois.

Le Conseil de l'ordre a pris connaissance des différents avis émis, y compris l'avis de la Commission Nationale pour la Protection des Données (ci-après la « **CNPD** ») du 28 décembre 2017 et les derniers amendements gouvernementaux intervenus.

Fruit de l'évolution rapide des technologies et de la mondialisation ayant entrainé une collecte massive de données personnelles au cours des dernières années, le RGPD impose aux Etats membres un nouveau cadre juridique impliquant une plus grande responsabilisation des acteurs privés et publics que celle édictée par la directive 95/45/CE.

Le présent avis traitera des commentaires sur les pouvoirs de la CNPD tels qu'énoncés dans le Chapitre I du Projet de loi (I). Le Conseil de l'ordre émettra ensuite son avis quant au Chapitre II du Projet de loi, ayant trait aux dispositions spécifiques ouvertes à la latitude et à la discrétion des Etats Membres (II). Enfin, il prendra position sur d'autres dispositions du RGPD et du Projet de loi (III).

*

I. QUANT AUX POUVOIRS DE LA CNPD (Chapitre I du Projet de loi)

La modification des pouvoirs de la CNPD (enquête et sanction), ainsi que de toutes les autorités nationales pour la protection des données, constitue l'un des changements majeurs du RGPD dont l'encadrement strict constitue une garantie fondamentale d'un Etat de droit[1].

Les pouvoirs de la CNPD sont définis par deux articles distincts du Projet de loi selon que la CNPD agit (i) en tant qu'autorité de contrôle dans le cadre de la loi à intervenir pour transposer la directive (UE) 2016/680 du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données (la « **Directive Police et Justice** »), (article 12 du Projet de loi), ou (ii) dans le contexte du RGPD (article 11 du Projet de loi).

Ainsi, alors que les pouvoirs de la CNPD lorsqu'elle agit dans le contexte de la loi à intervenir transposant la Directive Police et Justice sont repris *in extenso* (article 18 du Projet de loi), les pouvoirs de la CNPD dans le contexte du RGPD ne sont pas repris ; le Projet de loi (article 16) se contente d'un simple renvoi à l'article 58 du RGPD. Le Conseil de l'ordre s'inquiète quant au manque de clarté découlant de cette technique législative.

Conformément à l'article 58 du RGPD, la CNPD se voit notamment dotée du pouvoir (i) de mener des enquêtes sous la forme d'audits sur la protection des données, (ii) d'obtenir du responsable du traitement et du sous-traitant l'accès à toutes les données à caractère personnel et à toutes les informations nécessaires à l'accomplissement de ses missions et (iii) d'obtenir l'accès à tous les locaux du responsable du traitement et du sous-traitant, notamment à toute installation et à tout moyen de traitement.

Des prérogatives similaires, mais pas identiques, sont accordées à la CNPD dans le cadre de la loi à intervenir relative aux traitements de données personnelles en matières pénale et de sécurité sociale (article 18 du Projet de loi). Ces pouvoirs résultent d'une reprise à l'identique des dispositions correspondantes de la Directive Police et Justice.

A ces pouvoirs d'investigation importants, sont associés de très forts pouvoirs de sanctions administratives (mesures d'interdiction ou de limitation, le cas échéant, sous astreintes, sanctions financières jusqu'à 20 millions d'euro ou 4% du chiffre d'affaires annuel mondial total de l'exercice précédent), toute entrave aux missions de la CNPD étant de surcroît passible de sanctions pénales (article 55 du Projet de loi).

Tout en prenant acte de la volonté des rédacteurs du Projet de loi de doter la CNPD de plus amples pouvoirs et de répondre ainsi aux exigences du RGPD, le Conseil de l'ordre s'inquiète plus que fortement quant à la technique législative retenue par les rédacteurs du Projet de loi pour ce faire.

Plus encore, le Conseil de l'ordre est d'avis que les dispositions du Projet de loi relatives aux pouvoirs de la CNPD et à l'encadrement de ces pouvoirs sont insuffisantes pour permettre d'assurer la sécurité juridique nécessaire au fonctionnement de cette autorité de contrôle.

L'organisation de la CNPD et son fonctionnement sont en effet en très grande partie laissés à l'appréciation de la CNPD, laquelle devra elle-même se doter de règles de fonctionnement.

Certes, le Projet de loi accorde à la CNPD, nouvelle mouture, le statut d'autorité de contrôle indépendante et prévoit qu'elle conserve la forme d'un établissement public. En tant qu'autorité administrative, la CNPD est soumise au respect des règles régissant la procédure administrative non contentieuse (PANC). Mais cette procédure est bien insuffisante lorsqu'il s'agit d'allouer à une administration des pouvoirs d'investigation normalement dévolus à la justice pénale (mener des enquêtes, obtenir la communication d'informations, accèder à tous les locaux du responsable du traitement, accéder à des bureaux de professionnels soumis au secret professionnel comme ceux des avocats). Etant pourvue du statut d'établissement public, la CNPD dispose d'un pouvoir réglementaire limité, conformément à l'article 108bis de la Constitution. Toutefois, les pouvoirs d'enquête et de sanction de la CNPD touchant directement aux droits fondamentaux des administrés, le Conseil de l'ordre estime qu'il serait plus que recommandé de fixer, dans la loi organique de l'autorité, les règles de fonctionnement de celle-ci.

---

1 *Cf* art. 58 RGPD et art. 14 et s. du Projet de loi.

Or, le Projet de loi reste silencieux quant aux conditions dans lesquelles la CNPD pourra être amenée à conduire ses enquêtes (a) ou encore à adopter ses décisions (**b**).

a) Pouvoir d'enquête de la CNPD

D'une manière générale, il est regrettable voire inquiétant que le Projet de loi ne détaille pas de façon exhaustive les pouvoirs d'enquête de la CNPD (points e) et f) de l'article 58 RGPD) tels que l'accès aux bâtiments et aux bases de données des responsables de traitement ou des sous-traitants, les saisies et perquisitions, l'audition des personnes concernées, etc.) ainsi que l'encadrement de ces pouvoirs et missions d'enquête.

Au-delà de considérations liées au respect des droits de l'homme, le Conseil de l'ordre considère que le défaut de précision et d'encadrement des pouvoirs d'enquête de la CNPD crée une insécurité juridique préjudiciable tant pour la CNPD que pour les justiciables.

Le législateur luxembourgeois pourrait, de l'avis du Conseil de l'ordre, utilement s'inspirer du projet de loi déposé par le Gouvernement belge (document 2648/001 – projet de loi du 23 août 2017), lequel est beaucoup plus précis. Celui-ci développe par exemple point par point les pouvoirs des inspecteurs s'agissant de l'identification des personnes, des auditions ou de la collecte ou recherche d'informations. Il distingue également les pouvoirs dont dispose l'autorité belge dans le cadre d'une enquête en prenant soin de détailler les mesures qui peuvent être prises du propre chef de cette autorité et en les distinguant de celles pour lesquelles une autorisation judiciaire sera nécessaire, telles que les mesures de perquisition et de saisie.

S'agissant plus précisément des perquisitions et saisies, lesquelles sont spécifiquement visées à l'article 58.1 (f) du RGPD, le Conseil de l'ordre note à cet égard que le Projet de loi, tel qu'actuellement rédigé, ne donne pas expressément à la CNPD la possibilité d'effectuer ces perquisitions et saisies. En l'absence de dispositions spécifiques à cet égard et donc de pouvoir de cœrcition, les pouvoirs d'enquête de la CNPD sont dès lors limités et dépendants du bon vouloir des responsables de traitement et des sous-traitants.

Certes, les responsables de traitement et sous-traitant ont l'obligation de collaborer avec la CNPD (article 58.1 (e) RGPD) sous peine de sanctions pénales (possiblement moins dissuasives que les sanctions administratives que la CNPD est habilitée à prononcer) puisque l'article 55 du Projet de loi incrimine pénalement toute entrave généralement quelconque à l'accomplissement des missions incombant à la CNPD. Le Conseil de l'ordre émet d'ailleurs d'importantes réserves quant à la conformité de cet article 55 avec le principe de légalité des peines.

Il n'en reste pas moins qu'en l'état, cette obligation de collaboration, assortie de sanctions pénales, entre en contradiction avec le droit fondamental de ne pas contribuer à sa propre incrimination (implicitement consacrée par l'article 6.1 de la Convention Européenne des droits de l'Homme) selon lequel une personne ne peut être contrainte à fournir elle-même la preuve d'infractions qu'elle aurait commise. La rédaction actuelle du Projet de loi a dès lors pour effet qu'exercer son droit à ne pas contribuer à sa propre incrimination en gardant le silence pourrait être passible de sanctions pénales[2]. Le Projet de loi ne prend pas en considération cette problématique. Les dispositions relatives aux astreintes pouvant être prononcées par la CNPD introduites sous l'article 52 du Projet de loi sont loin de remédier aux problématiques soulevées ci-dessus.

Au demeurant, à supposer que l'intention des rédacteurs du Projet de loi soit d'accorder à la CNPD de véritables pouvoirs de perquisition et de saisie (et répondre ainsi aux exigences de l'article 58.1 (f) du RGPD), il est impensable que de tels pouvoirs exorbitants et aussi intrusifs dans la vie privée ne soient pas strictement encadrés ni soumis à une autorisation judiciaire préalable (comme l'autorisation du juge d'instruction ou l'autorisation du Président du Tribunal d'arrondissement, comme c'est le cas pour les perquisitions et saisies diligentées par le Conseil de la concurrence) par le Projet de loi. Le Projet de loi devrait également alors prévoir les modalités de recours contre une telle autorisation judiciaire, garantie essentielle dans un Etat de droit contre l'arbitraire.

Dans ce contexte, le Conseil de l'ordre propose de créer un cadre similaire à celui prévu par les articles 5 et 6 de la loi du 23 décembre 2016 relative aux abus de marché. A cet égard, le Conseil de

---

2 Voir les critiques similaires formulées à l'encontre de la procédure d'enquête de la CSSF (A. Lutgen et M. Marty, « La pratique des sanctions administratives en matière financière », *J.T.L.*, 50/2017).

l'ordre fait remarquer que le Contrôleur Européen pour la Protection des données (CEPD) a déjà, dans un avis du 10 février 2012 relatif aux sanctions en matière d'abus de marchés, souligné la nécessité de soumettre l'accès par des institutions administratives à des locaux privés à une autorisation judiciaire préalable et plus généralement de réglementer de manière précise les inspections, perquisitions ou saisies par de telles institutions afin de limiter les risques d'atteintes disproportionnées à la protection de la vie privée et au domicile y compris des personnes morales[3].

Le Conseil de l'ordre constate encore que, selon les termes du Projet de loi, les agents de la CNPD ne disposeront pas de la qualité d'officier de police judiciaire. Le Conseil de l'ordre relève également à la lecture de l'avis rendu par la CNPD du 28 décembre 2017 sur le Projet de loi que la question de savoir si la CNPD devait se doter d'officiers de police judiciaire a été longuement débattue et finalement écartée. Dans ce contexte, le Conseil de l'ordre s'interroge dès lors sur la valeur légale des constatations effectuées par les agents de la CNPD lors de la phase d'enquête[4].

Afin d'éviter toute insécurité juridique tant pour la CNPD que pour les justiciables, il est primordial que les pouvoirs de la CNPD en matière d'enquête ainsi que leurs modalités d'exercice et limites, notamment quant au déroulement des saisies et perquisitions, soient encadrés par des dispositions spécifiques et précises de la loi.

Le Conseil de l'ordre estime enfin essentiel que le Projet de loi encadre les pouvoirs de la CNPD lorsque les mesures d'investigations sont effectuées auprès de responsables de traitement ou de sous-traitants soumis à un secret professionnel pénalement sanctionné (tels que les avocats et les médecins). Le Conseil de l'ordre rappelle que l'article 90 du RGPD prévoit expressément la possibilité pour les Etats membres d'adopter des règles spécifiques afin de définir les pouvoirs des autorités de contrôles à l'égard des responsables du traitement qui sont soumis au secret professionnel.

S'agissant des avocats en particulier, il est impératif que la présence du Bâtonnier ou de son représentant soit rendue obligatoire pour toutes démarches effectuées par la CNPD dans une étude d'avocats et ce afin de permettre d'assurer le strict respect du secret des communications de l'avocat avec ses clients et ses confrères. Le Conseil de l'ordre fait remarquer à cet égard que cet encadrement est déjà prévu dans le cadre des perquisitions policières[5].

b) Décisions de la CNPD

S'agissant des décisions de la CNPD ensuite, le Conseil de l'ordre note que la CNPD cumule en son sein les pouvoirs d'enquête, d'accusation et de poursuite.

Le Conseil de l'ordre est d'avis qu'afin de garantir l'indépendance de l'organe qui doit rendre la sanction et ainsi le droit fondamental à un tribunal impartial (article 6, §I Convention EDH), l'organe ayant le pouvoir de sanction devrait être distinct de celui qui doit se saisir de la plainte ou ordonner et mener l'enquête. Deux organes distincts avec des missions indépendantes bien définies devraient être créés.

A tout le moins, conformément à la jurisprudence de la Cour EDH, le cumul des fonctions d'enquête et de sanction instauré au sein d'une même autorité devrait être strictement encadré par le Projet de loi pour éviter toute suspicion de partialité. Comme le rappelle de manière constante la Cour EDH, l'impartialité s'apprécie non seulement de manière subjective (en essayant de déterminer la conviction personnelle de tel juge en telle occasion) mais également de manière objective, afin de s'assurer que le juge offre des garanties suffisantes pour exclure à cet égard tout doute légitime[6]. Le Conseil de l'ordre rappelle à ce propos l'opposition formelle du Conseil d'Etat formulée dans le cadre de l'adoption de la loi du 23 octobre 2011 relative à la concurrence, organisant le Conseil de la concurrence, nouvelle mouture, au sein duquel les fonctions d'enquête et de décision ont été réunies.

Le Conseil de l'ordre estime que les garanties posées par le Projet de loi sont insuffisantes afin de prémunir efficacement les justiciables contre les risques de partialité liés au cumul des fonctions d'enquête, d'accusation et de poursuite dans le chef d'une même autorité (indépendance « fonction-

---

3 CEPD, avis du 10 fév. 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* 177/01, 20 juin 2012, p.1.

4 Le Projet de loi ne prévoit pas la possibilité pour les agents de la CNPD de dresser des procès-verbaux.

5 Sur ce point il est renvoyé à la section II. du présent avis.

6 CEDH, Dubus c. France, n°5242/04, 11 juin 2009, §53 et les références y citées.

nelle »)[7]. Le Conseil de l'ordre relève qu'à cet égard le Projet de loi se contente de prévoir que le chef d'enquête ne participe pas aux décisions prises par le collège à la suite de l'enquête. C'est insuffisant.

La ségrégation entre les fonctions (enquêteur et juge) devrait s'appliquer à tous les agents de la CNPD (et non pas aux seuls commissaires). Les garde-fous devraient par ailleurs être d'autant plus importants que la CNPD constitue une autorité de taille relativement modeste en termes d'effectifs, à la différence de certains de ses homologues européens, notamment en France ou en Allemagne. Dans ces juridictions, la ségrégation des fonctions d'enquête et de jugement peut plus facilement être mise en œuvre de par l'existence de départements aux missions spécifiques dont les rôles sont alors clairement identifiables et, travaillant généralement à des étages distincts d'un même bâtiment, ce qui est de nature à limiter en pratique les interactions entre les différentes fonctions. Dans de petites autorités, en pratique, les agents sont amenés à se côtoyer plus fréquemment et à endosser successivement les fonctions d'enquêteur et celle de juge au gré des besoins des dossiers. La mise en œuvre d'une ségrégation effective des pouvoirs est partant certainement moins aisée. Les garanties à cet égard doivent donc être d'autant plus renforcées alors qu'ainsi que le relève la Cour EDH, « *en la matière, même les apparences peuvent revêtir de l'importance* » et *« il y va de la confiance que les tribunaux d'une société démocratique se doivent d'inspirer aux justiciables* »[8].

Enfin, le Conseil de l'ordre observe que, de manière très inquiétante, le Projet de loi n'accorde aucune place au respect du contradictoire.

Ainsi ne sont notamment pas prévus : l'accès au dossier par le responsable de traitement ou le sous-traitant, la présomption d'innocence, la communication préalable des griefs, le droit de présenter des observations écrites et/ou orales préalablement à la sanction administrative, etc. Dans le même ordre d'idée, rien n'est prévu dans le Projet de loi sur la procédure décisionnelle de la CNPD.

Certes, la CNPD, autorité administrative, est soumise au respect des règles régissant la procédure administrative non contentieuse. Toutefois, le Conseil de l'ordre estime qu'il serait plus qu'opportun de prévoir un régime plus restrictif que le droit commun, afin de garantir pleinement le respect des droits de la défense, déjà au stade de la prise de la décision administrative.

Afin d'offrir les garanties nécessaires dans le cadre du processus décisionnel de la CNPD, le Conseil de l'ordre estime que l'encadrement du processus décisionnel doit être introduit dans le Projet de loi. A nouveau, le Conseil de l'ordre est d'avis que le législateur luxembourgeois pourrait utilement s'inspirer du projet de loi déposé par le Gouvernement Belge (document 2648/001 – projet de loi du 23 août 2017), lequel détaille le processus décisionnel devant la chambre contentieuse de leur autorité de contrôle.

Le Conseil de l'ordre déplore enfin l'absence de magistrat professionnel au sein du collège de la CNPD[9].

*

---

7 Voir avis du Conseil d'Etat du 16 juillet 2010 n°5816/06 portant sur le projet de loi relative à la concurrence et abrogeant la loi modifiée du 17 mai 2004 relative à la concurrence, avis du Conseil d'Etat du 16 mars 2004 n°5229/05 portant sur le projet de loi relative à la concurrence ; CEDH, Dubus c. France, n°5242/04, 11 juin 2009, §53 : « *La Cour rappelle qu'aux fins de l'article 6 § 1, l'impartialité doit s'apprécier selon une démarche subjective, essayant de déterminer la conviction personnelle de tel juge en telle occasion, et aussi selon une démarche objective amenant à s'assurer qu'il offrait des garanties suffisantes pour exclure à cet égard tout doute légitime (voir, entre autres, Hauschildt c. Danemark, 24 mai 1989, § 46, série A no 154 et De Cubber c. Belgique, 26 octobre 1984, § 24, série A no 86). (...). En la matière, même les apparences peuvent revêtir de l'importance. Il y va de la confiance que les tribunaux d'une société démocratique se doivent d'inspirer aux justiciables, à commencer, au pénal, par les prévenus (Didier, précité)* », et §60 : « *En résumé, la Cour n'est pas convaincue par l'affirmation du Gouvernement sur l'existence d'une séparation organique au sein de la Commission bancaire. Elle estime que la requérante pouvait nourrir des doutes objectivement fondés quant à l'indépendance et l'impartialité de la Commission du fait de l'absence de distinction claire entre ses différentes fonctions* ».

8 CEDH, Dubus c. France, n°5242/04, 11 juin 2009, §53.

9 Une telle garantie a été introduite en matière de droit de la concurrence (article 7 (2) de la loi du 23 octobre 2011 relative à la concurrence).

II. QUANT AUX DISPOSITIONS SPECIFIQUES DU RGPD (Chapitre II du Projet de loi)

Le RGPD comprend en son Chapitre IX[10] des dispositions relatives à des situations particulières de traitement de données personnelles pour lesquelles les Etats membres sont libres d'adopter une législation complémentaire. Y figurent notamment le traitement de données dans le cadre des relations de travail (a), le traitement de données à des fins archivistiques dans l'intérêt public, de recherche scientifique, historique ou à des fins statistiques (b), et l'obligation de secret (c).

Dans ces domaines, les Etats membres sont libres d'adopter des dispositions particulières, y compris des dérogations aux droits visés par le RGPD. Celui-ci étant d'application directe, les points qui n'ont pas été abordés par la loi luxembourgeoise seront, le cas échéant, régis par le RGPD.

S'il est vrai que le Projet de loi semble vouloir limiter les dispositions spécifiques nationales au minimum, le Conseil de l'ordre ne peut que s'étonner du fait que de nombreux points du RGPD, pour lesquels des précisions sont laissées à la discrétion des Etats membres, n'ont pas été abordés, ou que sommairement, par le législateur dans le Projet de loi.

Il s'agit en particulier des points suivants :

a. Le traitement de données dans le cadre des relations de travail (article 88 du RGPD) et la surveillance sur le lieu de travail

Le RGPD modifie le cadre législatif en la matière.

Les Etats membres peuvent prévoir des dispositions pour assurer la protection des droits et libertés dans le traitement des données des salariés, aux fins, entre autres, de l'exécution du contrat de travail, du respect des obligations fixées par la loi, de la gestion et de l'organisation du travail, de la santé et sécurité au travail, de la protection des biens appartenant à l'employeur ou au client[11].

Ces règles doivent alors comprendre des mesures spécifiques pour protéger la dignité humaine, les intérêts légitimes et les droits fondamentaux des personnes concernées, en accordant une attention particulière à la transparence du traitement, au transfert de données au sein d'un groupe d'entreprises et aux systèmes de contrôle sur le lieu de travail[12].

Le fait que les dispositions du RGPD s'appliquent au contrôle et à la surveillance des travailleurs en termes d'utilisation de courrier électronique, d'accès à Internet, de caméras vidéo ou de données de localisation ne fait pas de doute.

Or, la protection des données ne peut pas être dissociée du droit du travail car il existe nécessairement une interaction entre les deux, ce qui a pu justifier l'existence du cadre juridique actuel relatif à la surveillance des employés sur le lieu de travail (1).

Tout en saluant les apports du nouvel article L. 261-1 du Code du travail proposé par le Projet de loi, le Conseil de l'ordre estime que ceux-ci ne sont pas pleinements satisfaisants et que certaines modifications sont essentielles (2).

1. *Le cadre juridique actuel*

Le régime du traitement de données à des fins de surveillance des salariés sur le lieu de travail est actuellement fixé conjointement par les articles 10, 11 et 14 de la loi modifiée du 2 août 2002 relative

---

10 Articles 85 à 91.

11 Article 88 RGPD Traitement de données dans le cadre des relations de travail : (1) Les États membres peuvent prévoir, par la loi ou au moyen de conventions collectives, des règles plus spécifiques pour assurer la protection des droits et libertés en ce qui concerne le traitement des données à caractère personnel des employés dans le cadre des relations de travail, aux fins, notamment, du recrutement, de l'exécution du contrat de travail, y compris le respect des obligations fixées par la loi ou par des conventions collectives, de la gestion, de la planification et de l'organisation du travail, de l'égalité et de la diversité sur le lieu de travail, de la santé et de la sécurité au travail, de la protection des biens appartenant à l'employeur ou au client, aux fins de l'exercice et de la jouissance des droits et des avantages liés à l'emploi, individuellement ou collectivement, ainsi qu'aux fins de la résiliation de la relation de travail.

12 Article 88 (2) RGPD : Ces règles comprennent des mesures appropriées et spécifiques pour protéger la dignité humaine, les intérêts légitimes et les droits fondamentaux des personnes concernées, en accordant une attention particulière à la transparence du traitement, au transfert de données à caractère personnel au sein d'un groupe d'entreprises, ou d'un groupe d'entreprises engagées dans une activité économique conjointe et aux systèmes de contrôle sur le lieu de travail.

à la protection des données à l'égard du traitement des données à caractère personnel (la « **Loi de 2002** »), et par l'article L. 261-1 du Code du travail.

Si l'article 10 de la Loi de 2002 prévoit les critères généraux du traitement à des fins de surveillance, l'article 11 vise plus précisément la surveillance sur le lieu de travail, en opérant un renvoi aux conditions spécifiques stipulées à l'article L. 261-1 du Code du travail.

Le régime actuel de la mise en œuvre d'une surveillance sur le lieu de travail est basé sur de deux principes, à savoir la mise en place d'une surveillance uniquement dans cinq hypothèses restrictivement prévues et la nécessité d'une autorisation préalable de la CNPD.

a. *L'autorisation préalable de la CNPD*

L'autorisation préalable est actuellement prévue à l'article 14 de la Loi de 2002, bientôt abrogée, et n'est pas reprise par le Projet de loi.

Cette nécessité de l'autorisation préalable de la CNPD en matière de surveillance présente en pratique de nombreux problèmes pour les responsables de traitement luxembourgeois par rapport à leurs homologues européens, eu égard notamment à la définition très technique et spécifique au droit luxembourgeois et à l'engorgement créé auprès de la CNPD dont le délai d'octroi d'une autorisation peut être supérieur à 12 mois dans certains cas.

b. *Les critères restrictifs posés par l'article L. 261-1 du Code de travail*

En sus du régime de l'autorisation préalable, l'article L. 261-1 du Code du travail limite les hypothèses dans lesquelles une surveillance sur le lieu de travail peut être mise en œuvre. Or tant les hypothèses en elles-mêmes posent problème que l'interprétation qui en est donnée par la CNPD[13] de sorte que les responsables de traitement luxembourgeois ne bénéficient pas des mêmes droits que leurs homologues européens, notamment français et belges.

Actuellement, à travers les autorisations accordées par la CNPD, il est possible de déterminer ce que l'autorité de contrôle accepte ou refuse, notamment de déterminer quels sont les éléments qui sont considérés comme des biens au sens de la notion « protection des biens ».

On y trouve à titre d'exemple :

– les biens meubles et immeubles clairement identifiables ;
– la sécurité et/ou le bon fonctionnement technique des systèmes informatiques, la protection physique des installations de l'entreprise et le contrôle des coûts afférents ;
– les biens incorporels (droit de propriété intellectuelle, secrets d'affaires et de fabrication, informations confidentielles ou soumises au secret bancaire).

La protection des biens recouvre la sécurité et le bon fonctionnement du réseau informatique.

En revanche, les demandes d'autorisation concernant la surveillance des communications électroniques sur les fondements suivants ont été refusées par la CNPD :

– la protection des intérêts économiques autres que ceux liés à des meubles ou immeubles clairement identifiables ;

---

13 Art. L. 261-1 du Code du travail : (1) Le traitement des données à caractère personnel à des fins de surveillance sur le lieu de travail peut être mis en œuvre, conformément à l'article 14 de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel, par l'employeur s'il en est le responsable. Un tel traitement n'est possible que s'il est nécessaire :

1. ***pour les besoins de sécurité et de santé des salariés***, ou
2. ***pour les besoins de protection des biens de l'entreprise***, ou
3. ***pour le contrôle du processus de production portant uniquement sur les machines***, ou
4. ***pour le contrôle temporaire de production ou des prestations du salarié***, lorsqu'une telle mesure est le seul moyen pour déterminer le salaire exact, ou
5. ***dans le cadre d'une organisation de travail selon l'horaire mobile*** conformément au présent code.

Dans les cas visés aux points 1, 4 et 5, le comité mixte d'entreprise, le cas échéant institué, a un pouvoir de décision tel que dé ni à l'article L.423-1, points 1 et 2. Dans les entreprises occupant au moins 150 salariés la délégation du personnel a un pouvoir de codécision dans les cas visés aux points 1, 4 et 5 conformément à l'article L.414-9, points 1 et 2.

Le consentement de la personne concernée ne rend pas légitime le traitement mis en œuvre par l'employeur.

– le contrôle du respect du code éthique de l'entreprise ;
– le contrôle du respect de la charte informatique ;
– la prévention de comportements illicites (ex. consultation de sites pornographiques, racistes, pédophiles, téléchargement illégal etc.) ;
– la prévention de téléchargements illicites d'œuvres protégées ;
– la protection de l'image de marque ou de la réputation de l'entreprise.

En effet la CNPD considère que les termes protection des biens » ne justifient pas le contrôle de l'usage des outils informatiques visant la prévention, la recherche et la détection d'actes susceptibles d'engager la responsabilité de l'employeur et qui constituent une violation du règlement interne de l'entreprise et/ou des obligations contractuelles du salarié.

Or, le Groupe de travail « Article 29 » fait quant à lui référence au droit de l'employeur de se protéger de la responsabilité ou du préjudice des actions des salariés. Le Groupe 29 estime que ce droit de l'employeur est un motif légitime « pouvant justifier des mesures appropriées visant à limiter le droit à la vie privée des salariés ».

La CNPD affirmait cependant que « *la prévention d'actes susceptibles d'engager la responsabilité de l'employeur n'est pas prévue à titre de critère de légitimation* »[14]. Par une telle prise de position elle ne fait que suivre le cadre juridique actuel imposé par la loi, ce qui ne peut pas lui être reproché. Force est de constater que ce régime trop restrictif crée des difficultés de part et d'autre et est bientôt désuet de sorte que sa modification s'impose.

On peut également citer d'autres cas précis dans lesquels des demandes de transfert de données de surveillance de salariés vers des Etats tiers, notamment par des maison-mères américaines pour des besoins de lutte contre la corruption, ont été refusées si les autorités judiciaires n'étaient pas impliquées dans le cadre de l'aide judiciaire internationale.

Les refus fréquents d'une surveillance pour des cas légitimes tels que la prévention d'abus manifestes des salariés, des violations des chartes informatiques et des codes éthiques, entre autres, place le Luxembourg dans une situation peu favorable par rapport à des pays comme la France[15], la Belgique ou l'Allemagne, qui admettent plus aisément une telle surveillance.

2. *Le cadre juridique tel que projeté par le nouvel art. L. 261-1 du Code du travail*

Il résulte du point précédent qu'une modification du cadre juridique actuel s'imposait.

Le Conseil de l'ordre salue la proposition du Gouvernement sur l'adoption d'un nouveau régime, tout en formulant de très importantes réserves sur certaines des dispositions du nouvel article L. 261-1 du Code du travail[16].

a. *Apports du nouvel article L. 261-1 du Code du travail*

Le Conseil de l'ordre salue le nouveau régime de surveillance sur le lieu de travail pour diverses raisons.

Tout d'abord, le système d'autorisation préalable a été supprimé, ce qui correspond parfaitement à l'esprit du RGPD. En effet, contrairement à la directive 95/46/CE, le RGPD ne prévoit plus le système d'autorisation préalable devant être sollicitée auprès de l'autorité de contrôle.

De fait, l'un des principaux changements apportés par le RGPD est justement celui de mettre un terme au contrôle *ex ante* effectué par les autorités nationales, qui consistait en un système d'autorisa-

---

14 H. BOCK et L. BERNS, « Du contrôle de la correspondance électronique du salarié : la délicate antinomie des droits sur le lieu de travail », in *Droit bancaire et financier au Luxembourg*, 2014-Volume 3, 38. p. 1819.

15 La législation française est plus claire et laisse assez de latitude à l'application de la surveillance sur le lieu de travail, tout en affirmant sans équivoque l'importance du respect du respect du droit des personnes et des libertés individuelles et collectives. Ainsi, **L'ART. L1121-1 DU CODE DU TRAVAIL** dispose que : « *Nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives de restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché*. ». Cet article est à conjuguer avec **L'ART. 9 DU CODE CIVIL** qui dispose que « *chacun a droit au respect de sa vie privée* (…) ».

16 Tel que proposé dans le projet 7184[10].

tions en amont, au bénéfice d'un contrôle *ex post*, effectué *a posteriori*. Ceci implique que tous les acteurs concernés par le RGPD doivent être conformes à tout instant, en application du principe d'*accountability*[17]

Il est important de préciser que la nouvelle réglementation européenne a pour ambition d'instaurer une responsabilisation accrue des acteurs. Ils devront être en mesure de prouver à tout moment, avant même la mise en place d'un traitement de données, leur conformité aux dispositions du RGPD. Désormais les employeurs, en tant que responsables du traitement des données de leurs salariés, devront se mettre en conformité en interne et *ab initio*, indépendamment d'une autorisation ou notification préalable à l'autorité de contrôle.

Le RGPD s'inscrit dans un effort de simplification administrative, de réduction des coûts et des différences entre les Etats membres, en mettant l'accent sur le rôle consultatif des autorités de contrôle en facilitant la prise de contacts et les consultations, en particulier pour les PME.

Ensuite, du fait de l'abrogation de la Loi de 2002, le Conseil de l'ordre salue la suppression de la définition très technique et spécifique au droit luxembourgeois de la notion de « surveillance », interprétée de façon particulièrement restrictive par la CNPD. Les responsables de traitement luxembourgeois pourront donc se référer à une définition davantage en ligne avec celle retenue notamment par la Cour EDH.

Enfin, le Conseil de l'ordre salue également vivement la suppression des hypothèses limitatives (en ce compris, *de facto*, l'interprétation particulière de la notion de protection de biens de l'entreprise de la CNPD) dans lesquelles une surveillance pouvait être mise en œuvre. Désormais, pour autant que les principes RGPD soient respectés, un traitement sur le lieu de travail pourra être mis en œuvre dans des hypothèses comme la protection de l'image de marque ou de la réputation de l'entreprise, la prévention de l'usage abusif des ressources de l'entreprise (tel que le téléphone) ou le respect d'une obligation légale ou réglementaire du responsable de traitement.

Le RGPD, d'application directe, pose les principes fondamentaux s'appliquant au traitement des données personnelles des salariés sur le lieu de travail, y compris à la surveillance par moyens techniques, et prévoit des garanties nécessaires pour les personnes concernées.

A cet égard, le Conseil de l'ordre souhaite rappeler que le RGPD et les principes protecteurs qui s'y trouvent s'appliqueront nécessairement aussi aux traitements de surveillance des salariés sur leur lieu de travail, en particulier aux principes de finalité, transparence et proportionnalité du traitement des données personnelles[18].

---

17 **Article 5 RGPD Principes relatifs au traitement des données à caractère personnel :**

1. Les données à caractère personnel doivent être :
   a) traitées de manière licite, loyale et transparente au regard de la personne concernée (licéité, loyauté, transparence) ;
   b) collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités ; le traitement ultérieur à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques n'est pas considéré, conformément à l'article 89, paragraphe 1, comme incompatible avec les finalités initiales (limitation des finalités) ;
   c) adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données) ;
   d) exactes et, si nécessaire, tenues à jour ; toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder (exactitude)
   e) conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées; les données à caractère personnel peuvent être conservées pour des durées plus longues dans la mesure où elles seront traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89, paragraphe 1, pour autant que soient mises en œuvre les mesures techniques et organisationnelles appropriées requises par le présent règlement afin de garantir les droits et libertés de la personne concernée (limitation de la conservation);
   f) traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (intégrité et confidentialité) ;
2. Le responsable du traitement est responsable du respect du paragraphe 1 et est en mesure de démontrer que celui- ci est respecté (responsabilité).

18 Voir notre bas de page n° 6 page 3.

Le **principe de transparence** nécessite que toutes informations et communications relatives au traitement des données à caractère personnel soient aisément accessibles, faciles à comprendre, et formulées en des termes clairs et simples. L'employeur est donc tenu d'informer le travailleur sur le traitement des données à caractère personnel effectué à des fins de surveillance et la manière dont celui-ci est mené. Une telle mention peut être faite dans la réglementation interne à l'entreprise.

Même si les critères existants sont abrogés, tout dépendra des **finalités du traitement** des données du salarié par l'employeur, le principe étant que ces données ne peuvent être collectées par l'employeur que pour des finalités précisément déterminées, explicites et légitimes et qu'elles ne peuvent pas être traitées ultérieurement de manière incompatible avec ces finalités.

L'employeur est tenu de poursuivre un but légitime lorsqu'il effectue un contrôle des salariés. À titre d'exemple, le contrôle des communications électroniques au sein de l'entreprise poursuit un but précis et légitime lorsque l'employeur le justifie par le besoin de suivre la correspondance professionnelle.

C'est également le principe de finalité qui impose aux employeurs une disposition relative au traitement ultérieur des données collectées. Les finalités d'un tel traitement ultérieur doivent être compatibles avec celles pour lesquelles les données ont été collectées initialement.

S'agissant du **principe de proportionnalité**, il requiert que le traitement des données à caractère personnel sur le lieu de travail soit limité au strict nécessaire pour atteindre ses objectifs, autrement dit au regard de ses finalités.

À cela s'ajoute que le RGPD impose une analyse d'impact relative à la protection des données (l'« **AIPD** ») de la part du responsable de traitement dès lors que le traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques.

Le Groupe de travail « Article 29 » sur la protection des données précise d'ailleurs dans ses Lignes directrices concernant l'AIPD et la manière de déterminer si le traitement est « susceptible d'engendrer un risque élevé » que pour la surveillance systématique par une entreprise des activités de ses employés (y compris leur poste de travail, leur activité sur Internet etc.), une AIPD est potentiellement requise. Cela dans la mesure où il s'agit d'une surveillance systématique et de données concernant des personnes vulnérables[19].

L'AIPD en cas de surveillance systématique par une entreprise de ses employés devra très certainement être la règle pour les traitements le plus intrusifs, notamment en ce qui la surveillance par voie de camera. Une AIPD en vertu de l'article 35 du RGPD pourrait donc être requise pour les traitements de surveillance des salariés plus intrusifs engendrant un risque élevé pour les salariés concernés. Il ne faut cependant pas en conclure que l'AIPD sera systématique en matière de surveillance des salariés.

Enfin, même en l'absence d'un système d'autorisation préalable, une marge de manœuvre sera accordée à la CNPD laquelle conserve son rôle de conseillère en la matière. Les employeurs responsables de traitement, auront toujours la possibilité de la consulter afin de mettre en place un traitement pour lequel une AIPD est requise (y compris donc la surveillance), conforme au RGPD (article 36 du RGPD).

Par ailleurs, la CNPD aura un pouvoir de sanction en cas de non-respect de l'une quelconque des dispositions du RGPD par un responsable de traitement.

b. *Réserves et modifications à apporter au texte du nouvel L. 261-1 du Code du Travail*

Si le Conseil de l'ordre reconnait l'apport du nouveau texte de l'article L. 261-1 du Code du travail, rendu nécessaire par l'abrogation de la Loi de 2002, celui-ci souhaite formuler quelques réserves quant à ce texte, dont certaines sont à ses yeux particulièrement importantes.

Premièrement, afin de clarifier quelque peu le texte et ôter tout risque de discussion quant à la portée du 3ème alinéa de l'article, le Conseil de l'ordre estime qu'il y aurait lieu de numéroter de manière un peu différente les alinéas de cet article. En effet, dans sa version actuelle, la portée du 3ème alinéa pourrait être mal comprise et étendue au-delà des cas de surveillance listés au second alinéa. Par

19 Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est « susceptible d'engendrer un risque élevé » aux fins du règlement (UE) 2016/679 adoptées le 4 avril 2017, telles que modifiées et adoptées en dernier lieu le 4 octobre 2017.

conséquent, le Conseil de l'ordre propose de numéroter les alinéas de cet article comme suit (nouvelle numérotation en gras) :

« (1) Le traitement de données à caractère personnel à des fins de surveillance des salariés sur le lieu de travail peut être mis en œuvre, conformément au règlement (UE) 2016/679 par l'employeur s'il en est le responsable.

(2) Lorsque le traitement des données à caractère personnel est mis en œuvre :

[…],

les dispositions prévues aux articles L. 211-8, respectivement L. 414-9 respectivement L.423-1 s'appliquent.

En cas de désaccord, la partie la plus diligente peut soumettre […].

Le consentement de la personne concernée […].

(3) Sans préjudice du droit à l'information de la personne concernée, […].

Deuxièmement, le Conseil de l'ordre constate que dans les trois cas listés dans le nouvel article L.261-1 du Code du Travail, les représentants des salariés auront la possibilité en cas de désaccord sur le régime de surveillance proposé de solliciter l'avis préalable de la CNPD.

Or, le Conseil de l'ordre ne pense pas qu'il soit nécessaire de prévoir une procédure de consultation spécifique autre que celle déjà prévue dans le RGPD (*cf.* ci-dessus). De plus, comme le Conseil de l'ordre l'a rappelé, les salariés ou leurs représentants peuvent toujours saisir la CNPD s'ils estiment qu'un traitement n'est pas conforme aux dispositions de RGPD, CNPD qui dispose désormais d'un pouvoir de sanction important.

Par ailleurs le Conseil de l'ordre craint que cette disposition ne soit contre-productive et n'engorge inutilement la CNPD avec une multitude de demandes d'avis préalables, parfois dans des hypothèses où les risques pour les droits des personnes concernées sont relativement limités. Dans certains cas, l'introduction de cette disposition pourrait même constituer un recul par rapport à la situation actuelle. Le Conseil de l'ordre pense notamment aux systèmes techniques relativement standards de badges permettant le contrôle des accès ou les horaires mobiles.

En effet, dans la mesure où la très grande majorité des systèmes de badges installés à ces fins sont standards et afin de simplifier l'obtention des autorisations à ces fins, la CNPD a mis en place sous le régime de la Loi de 2002 et l'actuel article L. 261-1 du Code du Travail un système d'autorisation simplifiée dont peuvent bénéficier les responsables de traitement qui s'engagent à respecter une série de conditions préétablies par la CNPD. En pratique, la CNPD a autorisé dans deux décisions uniques, des systèmes de surveillance pour les horaires mobiles et le contrôle des accès. Tout employeur peut bénéficier de ces autorisations uniques en adressant simplement à la CNPD un engagement formel de conformité.

Or, sous le nouveau régime de l'article L. 261-1 du Code du Travail, la CNPD devra répondre au cas par cas à chaque demande d'avis portant sur une surveillance instaurée en vue de la gestion des horaires mobiles (comme certains systèmes de badges) ou en vue de la sécurité des salariés (dont peut faire partie un système de badges en vue du contrôle des accès), alors que ces situations rentrent dans les hypothèses listées dans ledit article. Toutefois, le Conseil de l'ordre ne voit pas comment un système d'avis simplifié, à l'instar du mécanisme d'autorisations uniques décrit ci-dessus, pourrait être mis en place, chaque demande d'avis individuelle étant par définition spécifique.

En pratique, la CNPD pourrait fort bien se retrouver rapidement submergée par des demandes d'avis relatifs à des systèmes de surveillance relativement standardisés, proportionnés et peu intrusifs, l'empêchant ainsi de consacrer un temps et des ressources précieux à des missions comportant une plus-value plus importante pour les personnes concernées, tel que le RGPD l'a souhaité.

Troisièmement, le Conseil de l'ordre estime qu'il y aurait lieu de préciser dans l'alinéa relatif au consentement que le consentement du salarié ne peut constituer une base de légitimité s'agissant de la surveillance. Or, dans sa formule actuelle, la disposition est très générale.

Sur ce point, il y a lieu de se référer à l'avis du Groupe de travail « Article 29 » qui souligne que pour la plupart des traitements de données au travail il est improbable que le consentement légitimise le traitement de telles données (à moins que l'employé puisse refuser sans en subir des conséquences

indésirables)[20]. Le Conseil de l'ordre souhaite rappeler que, certes s'il s'agit de cas relativement limités, il est possible que le consentement d'un salarié soit donné librement à son employeur et que *de facto* il n'y a pas lieu de l'exclure de manière absolue. À ce titre, il convient de souligner que le Groupe de travail « Article 29 » dans ses dernières lignes directrices du 28 novembre 2017 sur le consentement affirme bien que le consentement du salarié peut être pris en considération dans certains cas particuliers[21]. L'exclusion pure et simple du consentement du salarié comme une base de légitimité de la surveillance des salariés est par conséquent en contraction avec la position claire du Groupe de travail « Article 29 ».

Quatrièmement, le Conseil de l'ordre émet les plus grandes réserves quant à l'actuel alinéa (3) de la nouvelle version de l'article L.261-1 du Code du Travail. Selon le Conseil de l'ordre, ce paragraphe est inutile et dangereux.

L'objet de cet alinéa est de permettre aux représentants des salariés de saisir la CNPD d'une demande d'avis préalable. Certes si cet objectif est parfaitement louable, le Conseil de l'ordre considère que cet alinéa doit être supprimé.

En effet, d'une part, comme il a été développé plus haut, le RGPD prévoit déjà des garde-fous importants et des mécanismes efficaces permettant aux salariés de faire valoir leurs droits.

D'autre part, la portée de cet alinéa est générale puisqu'il s'applique à toutes les hypothèses de surveillance, et pas uniquement à celles listées sous les points 1 à 3 du (1) (dans sa numérotation telle que prévue par le projet de loi), ce qui n'est pas sans poser problème. L'avis doit être préalable et la demande a un effet suspensif, ce qui implique en fait que, premièrement, le responsable du traitement ne pourra pas exposer les investissements nécessaires et mettre en place le système de surveillance projeté tant qu'il ne connaît pas les intentions de la délégation du personnel et de tous les salariés quant à une éventuelle demande d'avis préalable à la CNPD et, deuxièmement, la délégation du personnel et les salariés peuvent ainsi seuls faire échec à une mesure de surveillance projetée, y compris dans le cas où celle-ci est imposée par la loi notamment dans le secteur financier. En pratique, cela signifie également que pour tout type de surveillance sur le lieu de travail (et pas seulement les cas listés 1 à 3 du (1) (dans sa numérotation telle que prévue par le projet de loi), la CNPD pourrait être amenée à devoir rendre un avis duquel le responsable de traitement ne pourra que très difficilement se départir.

La frontière avec le régime de l'autorisation préalable, que le projet de loi entend justement supprimer, est particulièrement ténue. Le Conseil de l'ordre ne peut s'empêcher de penser qu'en pratique le régime de l'autorisation préalable est indirectement réintroduit par cet alinéa.

Le Conseil de l'ordre réitère ensuite ses craintes quant au risque d'engorgement créé auprès de la CNPD.

Par conséquent, le Conseil de l'ordre recommande avec une insistance toute particulière que cet alinéa soit supprimé.

Enfin, le Conseil de l'ordre souhaite encore formuler une remarque s'agissant de l'amendement n° 30 proposé dans le projet 7184/10 et l'article 72 nouvellement formulé.

Par cet article, la loi a vocation à abroger l'ensemble des décisions de la CNPD prises sous la Loi de 2002.

Si le Conseil de l'ordre estime que l'objectif de sécurité juridique visé par cet article est parfaitement louable, il estime qu'il serait opportun de vérifier la compatibilité de cette disposition notamment avec

---

20 Article 29 Data Protection Working Party, 17/EN WP249, Opinion 2/2017 on data processing at work adopted of 8 June 2017.

21 Article 29 Data Protection Working Party, 17/EN WP259, Guidelines on Consent under Regulation 2016/679 « *However this does not mean that employers can never rely on consent as a lawful basis for processing. There may be situations when it is possible for the employer to demonstrate that consent actually is freely given. Given the imbalance of power between an employer and its staff members, employees can only give free consent in exceptional circumstances, when it will have no adverse consequences at all whether or not they give consent*" [Example 5]: A film crew is going to be filming in a certain part of an office. The employer asks all the employees who sit in that area for their consent to be filmed, as they may appear in the background of the video. Those who do not want to be filmed are not penalised in any way but instead are given equivalent desks elsewhere in the building for the duration of the filming. Imbalances of power are not limited to public authorities and employers, they may also occur in other situations. As highlighted by WP29 in several Opinions, consent can only be valid if the data subject is able to exercise a real choice, and there is no risk of deception, intimidation, cœrcion or significant negative consequences (e.g. substantial extra costs) if he/she does not consent. Consent will not be free in cases where there is any element of compulsion, pressure or inability, to exercise free will.

les lignes directrices précitées du Groupe de travail « Article 29 » sur les AIPD qui précisent notamment qu'une étude d'impact ne sera pas nécessaire lorsque un traitement avait été autorisé par une autorité nationale sous le régime de la directive que les conditions et modalités de celui-ci n'ont pas été modifiées.

b. Dérogations applicables à des fins archivistiques (article 89 du RGPD)

L'article 89 du RGPD laisse la possibilité aux Etats membres de prévoir des mesures particulières, notamment des dérogations à certains droits visés par le RGPD[22] lorsque le traitement de données à caractère personnel est effectué à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique, historique ou à des fins statistiques.

Le Conseil de l'ordre constate que le Projet de loi reprend en ses articles 57 et 58 tous ces traitements, en limitant donc les droits des personnes concernées dans ces domaines, sauf en ce qui concerne le traitement de données à des fins archivistiques dans l'intérêt public.

Sur ce point, le Conseil de l'ordre rejoint l'avis de la CNPD du 28 décembre 2017 et considère que, le cas échéant, le RGPD s'appliquera entièrement aux traitements de données à des fins archivistiques dans l'intérêt public, avec toutes les conséquences que cela implique, notamment dans le domaine culturel.

Il importe cependant de préciser que les lignes directrices du Groupe de travail « Article 29 » sur la protection des données du 4 avril 2017, telles que modifiées, sur l'AIPD requise quand le traitement est « susceptible d'engendrer un risque élevé », citent des exemples d'opérations de traitement pour lesquels une AIPD est potentiellement requise. Y figure notamment le stockage à des fins d'archivage de données à caractère personnel sensibles, pseudonymisées, concernant des personnes vulnérables participant à des projets de recherche ou à des essais cliniques.

Il serait donc avisé d'inclure à l'article 57 du Projet de loi également les traitements de données à des fins archivistiques effectuées dans l'intérêt public, tout en y apportant des précisions et des garanties complémentaires appropriées lorsqu'il s'agit d'archivage de données sensibles.

c. Obligation de secret (article 90 RGPD) et la protection du secret professionnel de l'avocat

Le Conseil de l'ordre souligne que l'article 90 du RGPD intitulé « *Obligation de secret* », prévoit expressément la possibilité pour les Etats membres d'adopter, via leurs législations nationales, des règles spécifiques afin de définir les pouvoirs des autorités de contrôle, telles que la CNPD, à l'égard des responsables de traitements ou des sous-traitants qui sont soumis au secret professionnel. L'article 90 donne ainsi la possibilité aux Etats membres d'adopter des règles spécifiques lorsqu'il s'agit d'obtenir l'accès aux données à caractère personnel et l'accès aux locaux du responsable du traitement ou du sous-traitant qui sont soumis, en vertu du droit interne, à une obligation de secret professionnel.

En son considérant 164, le RGPD précise par ailleurs que sont visés tant l'accès aux données à caractère personnel, que l'accès aux locaux du responsable de traitement ou du sous-traitant.

Le Conseil de l'ordre ne peut que constater que le Projet de loi ne répond pas à cette question fondamentale de préservation du secret professionnel en ne prévoyant aucune disposition ou exception à la collecte des données auprès des personnes soumises au secret professionnel.

Or, le secret professionnel de l'avocat repose sur de nombreuses normes impératives, qu'il s'agisse de prescriptions légales pénalement sanctionnées ou de règles déontologiques. Il est protégé par la Cour Européenne des Droits de l'Homme qui le définit comme « *la base de la relation de confiance qui existe entre l'avocat et son client* [23] [24]» et érigé comme norme communautaire par la CJUE[25]. Le secret professionnel de l'avocat est d'ordre public. Il est général, absolu et illimité dans le temps[26] et il participe à l'Etat de droit. Il couvre toutes les confidences que l'avocat a pu recevoir à raison de son état

22 Il s'agit des droits prévus aux articles 15, 16, 18 et 21 du RGPD.

23 CEDH, 5e Sect. 24 juillet 2008, André et autres c. France, Req. n° 18603/03, point 41.

24 Article 7.1.2 du Règlement intérieur de l'Ordre des Avocats du Barreau de Luxembourg.

25 CJCE, 18 mai 1982, A.M.&S. c/ Commission des Communautés européenne, Aff. 155/79, Rec, p. 1575.

26 Article 7.1.1 du Règlement intérieur de l'Ordre des Avocats du Barreau de Luxembourg.

ou de sa profession. Sont ainsi couverts par le secret les informations reçues du client, celles reçues de tiers dans le cadre du dossier concernant ce client, mais également le nom du client ainsi que l'agenda de l'avocat[27].

Le Conseil de l'ordre est donc d'avis que le Projet de loi devrait prévoir une base juridique explicite encadrant les pouvoirs de contrôle de la CNPD dans le contexte de ses missions afin de concilier le droit à la protection des données à caractère personnel et l'obligation de secret qui s'impose à certains professionnels, dont les avocats.

Une disposition particulière devrait être insérée en ce sens afin de couvrir les situations dans lesquelles sont concernées les données à caractère personnel que le responsable du traitement ou le sous-traitant a reçues dans le cadre d'une activité couverte par l'obligation de secret. En ce sens le Conseil de l'ordre recommande l'insertion dans le Projet de loi d'une disposition *ad hoc*, telle que préconisée par le RGPD, en prévoyant des restrictions aux pouvoirs de la CNPD en sa qualité d'autorité de contrôle, notamment dans le cadre des mesures d'investigation en ce qui concerne les personnes soumises au secret professionnel.

Ainsi, le Conseil des barreaux européens (CCBE) préconise dans ses recommandations du 0.12.22016 pour la mise en œuvre du RGPD que cette disposition soit libellée comme suit:

> « *Lorsque le responsable de traitement ou le sous-traitant est un avocat et que l'autorité de contrôle cherche à utiliser les pouvoirs qui lui sont conférés par l'article 58 (1), points e) et f), pour obtenir l'accès aux données à caractère personnel et à d'autres informations nécessaires à l'accomplissement de ses tâches, ou pour accéder à des locaux détenus ou sous le contrôle du responsable de traitement ou du sous-traitant, y compris à tout matériel ou moyen de traitement des données, l'autorité de contrôle est tenue d'obtenir le consentement du barreau de l'avocat. Lorsqu'elle demande le consentement, l'autorité de contrôle doit exposer les motifs de sa demande, y compris les mesures qu'elle prendra pour concilier le droit à la protection des données à caractère personnel et le secret professionnel. Sans le consentement du barreau, l'autorité de contrôle ne peut exercer les pouvoirs qui lui sont conférés en vertu de l'article 58 (1) (e) et (f) du RGPD* ».

Le Conseil de l'ordre souhaite aller plus loin et propose que la présence du Bâtonnier ou de son représentant soit rendue obligatoire par le législateur pour toutes mesures effectuées par la CNPD dans une étude d'avocats, et ce afin que soit scrupuleusement respecté le lieu de travail de l'avocat et le secret des communications de l'avocat, comme c'est le cas actuellement dans le cadre des perquisitions policières, mais également dans le cadre des inspections prévues par l'article L. 311-8 du Code de la consommation

Enfin, le Conseil de l'ordre tient à préciser que le projet de loi français prévoit notamment que le secret ne peut être opposé aux membres et agents de la Commission, « *sauf concernant les informations couvertes par le secret professionnel applicable aux relations entre un avocat et son client (...).* ». L'autorité de contrôle française, la CNIL, a dans son avis relatif au projet de loi français, favorablement accueilli la clarification apportée aux conditions d'opposabilité à la Commission des différents secrets protégés par la loi.

Au regard de tous ces éléments, le Conseil de l'ordre estime que la protection des informations couvertes par le secret professionnel doit également être expressément garantie dans le Projet de loi.

*

27 Article 7.1.3. du Règlement intérieur de l'Ordre des Avocats du Barreau de Luxembourg.

III. QUANT A D'AUTRES DISPOSITIONS PARTICULIERES DU RGPD

a. Organismes et mécanismes de certification

Le RGPD, en son article 43, met en avant les mécanismes de certification, labels et marques en matière de protection des données comme outils de conformité permettant aux acteurs de démontrer qu'ils respectent leurs obligations. L'article 43 du RGPD prévoit à ce titre que la certification est délivrée et renouvelée par un organisme de certification disposant d'un niveau d'expertise approprié, après en avoir informé l'autorité de contrôle afin que cette dernière puisse exercer les pouvoirs que lui confère l'article 58, § 2, h).

Ceci constitue une réelle nouveauté, étant donné que ni la directive de 1995, ni la législation nationale luxembourgeoise, pas plus que les législations des pays voisins tels que la France et la Belgique, n'avaient organisé de mécanismes de certification.

Le RGPD laisse le choix aux Etats membres de déterminer qui de l'autorité nationale de contrôle ou de l'organisme national d'accréditation sera compétent pour agréer les organismes de certification. Faisant usage de cette latitude, l'article 17 du Projet de loi fait le choix de la CNPD, estimée plus apte que l'INLAS au regard de sa spécialité en la matière.

En application de l'article 43 (3) du RGPD, les critères et exigences requises pour l'agrément devront faire l'objet d'une publication par l'autorité de contrôle sous une forme aisément accessible et être transmis au comité européen de la protection des données.

Le Conseil de l'ordre regrette que l'article 17 du Projet de loi se borne à désigner la CNPD comme autorité compétente, sans préciser quels seront les critères et exigences à prendre en considération lors de l'élaboration des mécanismes de certification, ni même déterminer les contours d'une procédure d'agrément. De l'avis du Conseil de l'ordre, il aurait été opportun que le Projet de loi renvoie à un règlement grand-ducal, auquel il appartiendrait de régler ces questions ou d'opérer un renvoi vers des normes européennes à venir.

b. Les limitations des droits des personnes pour certains traitements particuliers, notamment pour la question du traitement des données KYC

Le RGPD prévoit que le traitement des données à caractère personnel n'est autorisé que si la personne concernée a donné son consentement au traitement, ou si le traitement peut reposer sur une autre base juridique énumérée à l'article 6 (1) lettres (a) à (f) du RGPD.

Conformément aux dispositions de l'article 6 (1) du RGPD, le traitement n'est licite que s'il est nécessaire (i) au respect d'une obligation légale à laquelle le responsable du traitement est soumis (point c)) ou (ii) à l'exécution d'une mission d'intérêt public (point e)).

Suivant l'article 6 (2) du RGPD, les Etats membres peuvent maintenir ou introduire des dispositions plus spécifiques pour adapter l'application des dispositions du RGPD pour ce qui est du traitement dans le but de respecter le point (1) (c) et (e) « *en déterminant plus précisément les exigences spécifiques applicables au traitement ainsi que d'autres mesures visant à garantir un traitement licite et loyal* ».

L'article 23 du RGPD donne la possibilité aux Etats membres de limiter par des mesures nationales la portée des droits des personnes concernées et des obligations des responsables de traitement prévus par le RGPD. Le législateur national peut prévoir des limitations si elles respectent les libertés et droits fondamentaux et constituent une mesure nécessaire et proportionnée pour garantir certains intérêts publics limitativement listés. Il s'agit entre autres de la sécurité nationale, défense nationale, sécurité publique, prévention et détection d'infractions pénales, ainsi que les enquêtes et poursuites en la matière ou l'exécution de sanctions pénales, d'autres objectifs importants d'intérêt public général, notamment un intérêt économique ou financier important y compris dans les domaines monétaire, budgétaire et fiscal, de la santé publique et de la sécurité sociale, la protection de l'indépendance de la justice et des procédures judiciaires.

Suivant le RGPD, certains traitements peuvent donc être effectués de manière licite s'ils sont nécessaires au respect d'une obligation légale, ou pour garantir certains intérêts publics, en limitant de ce fait les droits de la personne concernée par le traitement. Ceci cependant à conditions que ces limitations

soient expressément prévues et précisées par des mesures législatives nationales. Or le Projet de loi reste silencieux à ce propos, aucun encadrement ni général ni précis n'est prévu en sa version actuelle quant aux limitations possibles. Même si une possibilité est de prévoir de telles limitations dans les législations spécifiques concernées, il aurait été préférable de regrouper toutes les limitations aux droits des personnes concernées et les modifications aux législations spécifiques dans le Projet de loi.

Nombreux sont les domaines dans lesquels le traitement doit être exercé afin de garantir certains intérêts publics, ou lorsque le traitement est effectué pour se conformer au respect d'une obligation légale.

Le cadre juridique de collecte, analyse, conservation et partage de données à caractère personnel dans le contexte la loi modifiée du 12 novembre 2004 relative à la lutte contre le blanchiment et contre le financement du terrorisme (la « **Loi AML** ») est en large partie couvert par la Loi AML elle-même ainsi que par la Directive Police et Justice. À ce titre le Conseil de l'ordre salue l'effort de la CNPD par sa prise de position complète dans son avis relatif au projet de loi n° 7128[28] portant transposition de la directive (UE) 2015/849 du 20 mai 2015 (eine directive) même si cette position devra être complétée car elle ne fait que prendre position sur la dernière réforme européenne en la matière.

Le Conseil de l'ordre entend cependant souligner que l'existence de possibilités de limitations du RGPD ne suffit pas, par elle-même, à fonder un droit général et automatique des autorités nationales à refuser à la personne concernée dont les données sont collectées à des fins de KYC l'exercice de ses droits conférés par le RGPD.

Le Projet de loi devrait définir clairement et explicitement, les exceptions possibles aux droits des personnes concernées.

Le Conseil de l'ordre est d'avis que le Projet de loi sous examen, en son état actuel de rédaction, ne comporte pas de garanties légales suffisantes de nature à assurer un juste équilibre entre les droits énoncés au RGPD et les intérêts publics ou obligations légales qui sont susceptibles de les limiter. Le Projet de loi ne permet pas d'appréhender l'étendue des limitations dont pourraient bénéficier les traitements concernés, la nature exacte de ceux-ci et, par conséquent le caractère proportionné des limitations faites aux droits du RGPD.

Il faudra à l'avenir modifier les lois spéciales (Loi AML, MiFID, fiscales etc.) pour que soit respecté à minima la législation sur la protection des données. Comme indiqué ci-dessus, il aurait été préférable de prévoir toutes ces modifications des lois spéciales dans le Projet de loi.

Par conséquent, lorsque l'accès aux données par la personne concernée est limité ou différé dans certains cas précis, ceux-ci devraient être mentionnés dans le Projet de loi, du moins par un renvoi aux dispositions législatives applicables en la matière. Il est vrai que certains projets de lois spécifiques semblent déjà introduire une telle limitation ou une possibilité de suspension de l'exercice de certains droits des personnes concernées mais ces dispositions ne sont pas conformes aux exigences de l'article 23 RGPD. En effet, cette disposition requiert dans son al. (2) que les dispositions spécifiques en question contiennent des précisions quant :

a) aux finalités du traitement ou des catégories de traitement;

b) aux catégories de données à caractère personnel;

c) à l'étendue des limitations introduites;

d) aux garanties destinées à prévenir les abus ou l'accès ou le transfert illicites;

e) à la détermination du responsable du traitement ou des catégories de responsables du traitement;

f) aux durées de conservation et aux garanties applicables, en tenant compte de la nature, de la portée et des finalités du traitement ou des catégories de traitement;

g) aux risques pour les droits et libertés des personnes concernées; et

h) au droit des personnes concernées d'être informées de la limitation, à moins que cela risque de nuire à la finalité de la limitation.

Or, prenons l'exemple de la limitation ou la possibilité de suspension du droit d'accès, telles que prévues au nouvel article 3, paragraphe (6bis) de ce que le projet de loi n° 7128 portant transposition de la 4ème directive entend introduire dans la loi modifiée du 12 novembre 2004 relative à la lutte contre le blanchiment et contre le financement du terrorisme. En vertu de cette nouvelle disposition,

---

28 Délibération n° 21/2018 du 18 janvier 2018

« *le responsable de traitement limite ou diffère l'exercice du droit d'accès de la personne concernée aux données à caractère personnel la concernant lorsqu'une telle mesure est nécessaire pour:*

a) permettre au professionnel, à la cellule de renseignement financier, à une autorité de contrôle ou à un organisme d'autorégulation d'accomplir ses tâches comme il convient aux fins de la présente loi ou des mesures prises pour son exécution; ou

b) éviter de faire obstacle aux demandes de renseignements, analyses, enquêtes ou procédures à caractère officiel ou judiciaire, menées aux fins de la présente loi, des mesures prises pour son exécution ou de la directive (UE) 2015/849 et pour ne pas compromettre la prévention et la détection des cas de blanchiment ou de financement du terrorisme ni les enquêtes en la matière. »

Cette disposition limitative des droits des personnes concernées nous semble être trop vague et contraire à l'article 23 RGPD, entre autres, parce ce qu'elle ne précise pas quelles catégories de données à caractère personnel sont visées. Ainsi, plusieurs entreprises sujettes à la loi modifiée du 12 novembre 2004 relative à la lutte contre le blanchiment et contre le financement du terrorisme, se posent la question de savoir si elles pourront limiter l'accès des personnes concernées à des données de *scoring* qu'elles tiennent par rapport à celles-ci.

Alors que la Loi de 2002, prévoit expressément en son article 27 une exception au droit à l'information de la personne concernée lorsque « *le traitement est nécessaire pour sauvegarder la prévention, la recherche, la constatation et la poursuite d'infractions pénales y compris celles à la lutte contre le blanchiment, ou le déroulement d'autres procédures judiciaires* », le Conseil de l'ordre constate que le Projet de loi ne comporte aucune référence aux traitements de données collectées à des fins de lutte AML ou financement du terrorisme.

Il serait avisé que le Projet de loi prenne également position sur l'analyse de risque imposée par le RGPD aux responsables de traitement soumis à des obligations de vigilance simples ou renforcées. La même considération vaut pour la législation MiFID II qui implique l'adoption de dispositions spécifiques ou lois spéciales s'articulant avec les obligations du RGPD.

c. Les traitements des données de santé

Le RGPD en son article 9 (1), énonce que le traitement de certaines « catégories particulières de données à caractère personnel », dont les données concernant la santé ou concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique est interdit.

L'article 9 (2) dispose cependant que cette interdiction ne s'applique pas lorsque la personne concernée a donné son « consentement explicite au traitement de ces données à caractère personnel pour une ou plusieurs finalités spécifiques », ou lorsque certaines autres conditions citées au même article sont remplies.

• Caractère superfétatoire de l'article 68 du Projet de loi

L'article 68 du Projet de loi amendé est une copie quasi-servile de l'article 7 de la Loi de 2002. Cependant, alors que l'article 7 de la Loi de 2002 ne couvrait que les traitements de données relatives à la santé et à la vie sexuelle par les services de santé, l'article 68 du Projet de loi concerne dorénavant toutes les « catégories particulières de données à caractère personnel » de l'article 9 du RGPD.

Le Conseil de l'ordre ne parvient ainsi pas à saisir l'utilité de cet article 68 par rapport à l'article 9 du RGPD, qui est d'application directe au Luxembourg.

• La notion large de catégories particulières de données à caractère personnel

Le Conseil de l'ordre constate également qu'en l'état actuel du Projet de loi, les services de santé, notion qui comme le souligne la CNPD dans son avis du 28 décembre 2017 n'est d'ailleurs pas définie, se voient autorisés à traiter des « catégories particulières de données à caractère personnel » autres que des données de santé, comme l'origine raciale ou ethnique, les opinions politiques ou l'appartenance syndicale et ne comprend pas ce qui pourrait justifier une telle autorisation. Le Conseil de l'ordre renvoie à l'avis de la CNPD sur ce point.

• L'assimilation des entreprises d'assurances et autres aux services de santé

Plus particulièrement, l'article 68 (3) du Projet de loi semble, quant à lui, avoir substantiellement repris l'article 7 (3) de la Loi de 2002, en disposant que le traitement de telles catégories particulières de données à caractère personnel « *nécessaire aux fins de la gestion de services de santé* » peut notamment être mis en œuvre, « *lorsque le responsable de traitement est soumis au secret professionnel […] par les entreprises d'assurance, les sociétés gérant les fonds de pension, la Caisse médico-chirurgicale mutualiste* (…) ».

Le Conseil de l'ordre remarque qu'une telle dérogation pourrait ne pas être conforme au RGPD, qui limite le bénéfice d'une telle dérogation pour le traitement des données de santé aux professionnels de la santé et à certaines administrations de l'Etat membre concerné.

En effet, l'article 9 (2) (h) du RGPD dispose que le traitement de données de santé peut être effectué sans consentement explicite de la personne concernée uniquement lorsqu'il est « *nécessaire aux fins de la médecine préventive ou de la médecine du travail, de l'appréciation de la capacité de travail du travailleur, de diagnostics médicaux, de la prise en charge sanitaire ou sociale, ou de la gestion des systèmes et des services de soins de santé ou de protection sociale sur la base du droit de l'Union, du droit d'un Etat membre ou en vertu d'un contrat conclu avec un professionnel de la santé et soumis aux conditions et garanties visées au paragraphe 3* [ces conditions et garanties consistant en ce que les données soient traitées par un professionnel de la santé soumis à une obligation de secret professionnel ou par une autre personne également soumise à une obligation de secret] ».

L'article 9 (2) h) RGPD constitue la base juridique de légitimation du traitement de données sensibles et il y a partant lieu de souligner qu'en tout état de cause les dispositions de l'article 68 (1), (3) et (4) du Projet de loi ne peuvent en aucun cas permettre l'ouverture de nouveaux cas de légitimité d'utilisation des données sans le consentement de la personne concernée.

Le fait pour ces professionnels d'être assimilés à des services de santé, traitant des données de santé ne doit en aucun cas être constitutif d'une base juridique leur permettant de traiter des données sensibles, notamment génétiques, sans le consentement de leurs clients.

À cet égard le Conseil de l'ordre se rallie à la position de la CNPD formulé dans son avis du 28 décembre 2018 qui ne voit pas en quoi les entreprises d'assurances, les sociétés gérant les fonds de pension et la CMCM sont assimilés à des professionnels de santé.

Le Conseil de l'ordre est partant d'avis que le Projet de loi devrait être clairement précisé afin d'éviter que l'interprétation de l'article 68 (1), (3) et (4) soit contraire au RGPD.

À ce titre, il y a lieu de souligner que déjà lors des débats précédant l'adoption de la Loi de 2002 s'agissant du traitement de catégories particulières de données par les services de santé, le Conseil d'Etat faisait part dans son avis du 29.1.2002 de ses craintes d'abus en la matière.

Le Conseil de l'ordre renvoie également à la recommandation CM/Rec (2016) 8 du Comité des Ministres du Conseil de l'Europe[29] qui souligne la nécessité de fournir un cadre normatif ou conventionnel pour le traitement à des fins d'assurance de données à caractère personnel relatives à la santé, en particulier les données prédictives, de nature génétique ou non et interdit l'utilisation des tests génétiques prédictifs à des fins d'assurance.

Notamment le Conseil de l'Europe estime (Principe 1) que les assureurs devraient justifier le traitement de données à caractère personnel relatives à la santé, que (Principe 2) les assureurs ne devraient pas procéder au traitement de données à caractère personnel relatives à la santé sans le consentement libre, exprès et éclairé de l'assuré(e), consigné par écrit, et enfin (Principe 3) que les assureurs devraient prévoir les garanties suffisantes pour la conservation des données à caractère personnel relatives à la santé.

• Précision nécessaire de l'article 68 (3) du Projet de loi

L'article 68 (3) mériterait donc à tout le moins d'être complété, afin de préciser dans quelle mesure (à savoir, pour quelles finalités et moyennant quelles garanties) les entreprises d'assurance et les socié-

---

29 Recommandation CM/Rec(2016)8 du Comité des Ministres aux Etats membres sur le traitement des données à caractère personnel relatives à la santé à des fins d'assurance, y compris les données résultant de tests génétiques (adoptée par le Comité des Ministres le 26 octobre 2016).

tés gérant les fonds de pension et la CMCM pourraient être autorisées à traiter des données de santé sans consentement explicite de la personne concernée.

Sur ce point, le Conseil de l'ordre ne partage pas l'avis de l'Association des Compagnies d'Assurances et de Réassurances du Grand-Duché de Luxembourg (« **ACA** »), qui indiquait que le fait pour les entreprises d'assurances de ne pas être assimilées à des services de santé les empêcherait d'exercer leurs activités, dès lors qu'il suffira à ces entreprises de recueillir le consentement de leurs clients afin d'être en mesure de traiter leurs données de santé.

L'article 68 (4) du Projet de loi dispose quant à lui que les données visées à l'article 9 du RGPD « *peuvent être communiquées à des tiers ou utilisées à des fins de recherche, d'après les modalités et suivant les conditions à déterminer par règlement grand-ducal* ».

Le Conseil de l'ordre s'interroge quant à la pertinence du renvoi à un règlement grand-ducal, alors que le Projet de loi gagnerait en clarté à indiquer directement les modalités et conditions dans lesquelles de telles communications ou utilisations pourraient être effectuées. Comme le souligne à bon escient la CNPD, ce règlement grand-ducal n'a pas été pris dans l'ancienne législation. Le Conseil de l'ordre estime que ce n'est pas un règlement grand-ducal qui doit régler un tel point sensible mais bien la loi.

• Les données génétiques

Enfin, l'article 9 (4) du RGPD permet aux Etats Membres de maintenir ou introduire des conditions supplémentaires, y compris des limitations, en ce qui concerne le traitement des « *données génétiques, des données biométriques ou des données concernant la santé* ».

Le Conseil de l'ordre s'interroge quant à la raison ayant conduit le législateur à ne pas faire usage de cette possibilité, alors que le Luxembourg aurait pu se montrer innovant en la matière. Il se rallie à la position de la CNPD en ce qui concerne le fait que le Projet de loi ne prévoit pas de règles spécifiques relatives au traitement des données génétiques. Or, comme l'avait souligné le Conseil d'Etat dans son avis du 29.1.2002 dans le contexte de la Loi de 2002, les données génétiques en général font partie des données relatives à la santé.

La Loi de 2002 prévoit d'ailleurs un encadrement strict pour la collecte et l'utilisation des données génétiques et il ne faut en aucun cas baisser le niveau de protection actuel.

Force est de constater que la formulation actuelle de l'article 68 du Projet de loi est trop vague et imprécise. Elle ne peut demeurer en l'état s'agissant d'un domaine si important.

Le Projet de loi doit impérativement être précisé en ce qui concerne les données génétiques et plus particulièrement en ce qui concerne le traitement des données génétiques prédictives.

d. Représentation des personnes concernées

L'article 80 du RGPD offre la possibilité aux Etats membres d'investir les associations chargées de la protection des droits et des libertés dans le cadre de traitement de données à caractère personnel d'importants pouvoirs d'action.

Ces associations pourraient d'initiative, c'est-à-dire indépendamment de tout mandat d'une personne concernée, introduire une réclamation auprès de l'autorité de contrôle sur le territoire de l'État membre où elles ont été constituées (art. 77) ou diligenter un recours juridictionnel contre une décision de l'autorité de contrôle (art. 78) ou contre un responsable de traitement ou un sous-traitant (art. 79), si elles considèrent que les droits d'une personne concernée n'ont pas été respectés du fait que le traitement des données à caractère personnel n'a pas eu lieu en conformité avec le RGPD.

Les ASBL luxembourgeoises étant, conformément à l'article 3 de la loi du 21 avril 1928 sur les associations et les fondations sans but lucratif, dotées de la personnalité morale à compter du jour où leurs statuts sont publiés au Recueil électronique des sociétés et associations, ces dernières se voient *de facto* reconnaître la capacité (reconnue aux personnes juridiques, sauf exception) d'agir en justice afin de défendre leurs intérêts propres.

Quant à la possibilité pour une ASBL d'agir en justice dans l'intérêt de ses membres, l'article 7(2), al. 2 de la loi modifiée du 7 novembre 1996 portant organisation des juridictions de l'ordre administratif ouvre aux ASBL d'importance nationale, la possibilité d'exercer un recours contre un acte administratif lui ayant porté préjudice. Elle doit pour se faire rapporter la preuve d'une lésion d'un droit à caractère individuel ou corporatif dérivant directement de l'acte litigieux. Le législateur se refuse toutefois de

reconnaitre aux associations un droit d'action généralisé pour la défense de l'intérêt général, c'est-à-dire le droit d'agir contre les décisions individuelles pour la défense de l'intérêt général.

Il s'en suit que l'état actuel de la législation luxembourgeoise ne permet pas aux associations d'introduire une procédure indépendamment d'un mandat de la personne concernée. Le législateur ne peut donc se saisir de l'opportunité offerte par l'article 80 (2) du RGPD sans modifier les dispositions législatives précitées.

e. Recouvrement des amendes administratives et astreintes

Pour ce qui est du recouvrement des amendes et astreintes prononcées à l'égard des personnes physiques et morales de droit privé, l'article 53 du Projet de loi donne compétence à l'Administration de l'Enregistrement et des Domaines.

Le Conseil de l'ordre relève que ledit article reste silencieux quant à la procédure applicable au recouvrement des amendes administratives et astreintes prononcées à l'égard des personnes morales de droit public. Or, il appartient à la loi de déterminer l'administration en charge de recouvrement et selon quelle procédure.

Il conviendrait dès lors de compléter l'article 53 du Projet de loi en ce sens.

f. L'abolition des autorisations délivrées sur base des art. 14 et 19 de la Loi de 2002

Le Conseil de l'ordre questionne également le nouvel article 72 du Projet de loi en vertu duquel toutes les autorisations délivrées sur base des articles 14 et 19 de la Loi de 2002 sont abolies.

Il s'agit notamment des autorisations pour la surveillance sur le lieu de travail. On peut alors se poser la question de savoir si de tels traitements qui ont été autorisés par le passé, pourront faire l'objet d'une demande d'avis par la délégation du personnel ou, à défaut, par les salariés concernés (cf. supra).

Sont également concernées les autorisations sur base de l'article 19 de la Loi de 2002 et, plus particulièrement, les autorisations pour le transfert de données vers des pays en dehors de l'UE/EEE n'assurant pas un niveau de protection adéquat, au sens de l'article 18, paragraphe (2), pour autant que des garanties suffisantes au regard de la protection de la vie privée sont offertes, par exemple, sur la base des modèles de clauses contractuelles adoptés par la Commission européenne ou sur la base des règles d'entreprise contraignantes (« *Binding Corporate Rules* » ou « *BCR* » en anglais). L'abolition de ces autorisations n'est pas appropriée d'autant plus que l'article 46 (5) RGPD précise justement que les autorisations accordées par un État membre ou une autorité de contrôle sur cette base demeurent valables jusqu'à leur modification, leur remplacement ou leur abrogation par ladite autorité de contrôle.

Retenons également que le Groupe de travail « Article 29 » a précisé clairement qu'aucune AIPD n'est nécessaire pour les opérations de traitement qui ont fait l'objet d'un examen par une autorité de contrôle ou par le détaché à la protection des données, conformément à l'article 20 de la directive 95/46/CE, et dont la mise en œuvre n'a pas changé depuis le contrôle préalable. En effet, «*les décisions de la Commission qui ont été adoptées et les autorisations qui ont été accordées par les autorités de contrôle sur le fondement de la directive 95/46/CE demeurent en vigueur jusqu'à ce qu'elles soient modifiées, remplacées ou abrogées» (considérant 171)*[30]

L'abrogation des autorisations accordées par la CNPD sous l'ancienne législation semble dès lors également contreproductive par rapport à l'absence de nécessité de diligenter des AIPD lorsque de telles autorisations obtenues en vertu du regime antérieur existent.

g. La problématique du délégué à la protection des données et les contrats globaux

L'article 37 (2) du RGPD prévoit la possibilité pour un groupe d'entreprises de désigner un seul délégué à la protection des données (« **DPO** ») à condition qu'il soit facilement joignable à partir de chaque lieu d'établissement.

---

30 Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est « susceptible d'engendrer un risque élevé » aux fins du règlement (UE) 2016/679 adoptées le 4 avril 2017, telles que modifiées et adoptées en dernier lieu le 4 octobre 2017.

À cet égard il convient de souligner que le Centre commun de la sécurité sociale (CCSS) a dans une communication du 14 janvier 2016, émis des doutes sur la légalité des contrats globaux[31].

En effet, le CCSS, confronté à une augmentation de demandes de validation de tels contrats d'emploi globaux, a décidé de ne plus valider expressément le recours à un tel contrat à l'avenir en raison de l'absence de règles de droit en matière de sécurité sociale et du travail relatives aux contrats d'emploi globaux et à défaut d'une interprétation juridique convaincante permettant de conclure que ce genre de contrats ne se heurte pas aux dispositions légales existantes.

Le Conseil de l'ordre entend donc attirer l'attention sur le fait que l'article 37 (2) du RGPD permettant de désigner un seul DPO pour l'ensemble des sociétés d'un groupe peut se confronter à l'absence d'une reconnaissance légale des contrats globaux au Luxembourg, et ceci plus particulièrement dans l'hypothèse où le DPO mis à dispostion d'un groupe de sociétés n'a pas le statut d'un indépendant et que le recours à un contrat global serait la solution la plus adaptée. Le Conseil de l'ordre est dès lors d'avis qu'une réglementation des contrats globaux serait nécessaire au Luxembourg et plus particulièrement pour couvrir des cas de figures tels que visés par le RGPD. Ce point n'est pas à négliger si l'on considère le nombre important de DPO qui seront employés par des groupes de sociétés au Luxembourg.

Luxembourg, le 30 mars 2018

François PRUM
Bâtonnier

---

31 Communication du Centre commun de la sécurité sociale du 14.6.2016
http://www.ccss.lu/archives/detail/?tx_ttnews%5Btt_news%5D=796&cHash=f4223bde13304e207e3e0bcb2e83ff40

Impression: CTIE – Division Imprimés et Fournitures de bureau