CHAMBRE DES SALARIES
LUXEMBOURG

5 décembre 2017

AVIS II/55/2017

relatif au projet de loi 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 de la loi du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'État et abrogeant la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel.

relatif au projet de règlement grand-ducal portant fixation du siège de la Commission nationale pour la protection des données.

relatif au projet de règlement grand-ducal portant fixation des indemnités revenant au Président, aux membres et aux membres suppléants de la Commission nationale pour la protection des données.

relatif au projet de loi relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale […]

AVIS

18 rue Auguste Lumière L-1950 Luxembourg
B.P. 1263 L-1012 Luxembourg
T. +352 27 494 200 F. +352 27 494 250
csl@csl.lu www.csl.lu

Par lettres du 9 et du 22 août 2017, M. Xavier Bettel, Ministre d'État et M. Félix Braz, Ministre de la Justice ont soumis à l'avis de la Chambre des salariés (CSL) les projets de loi et de règlement grand-ducal sous rubrique.

1. Les deux projets de loi, ainsi que les deux projets de règlement grand-ducal ont trait à la protection des données à caractère personnel et viennent compléter, voir transposer le cadre légal européen.

- Le premier projet de loi porte création de la Commission nationale pour la protection des données et met en œuvre le 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. Il procède à l'abrogation de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel.

  Ce projet de loi est accompagné de deux projets de règlement grand-ducal.

  Le premier projet de règlement grand-ducal porte fixation du siège de la Commission nationale pour la protection des données et le second porte fixation des indemnités revenant au Président, aux membres et aux membres suppléants de la Commission nationale pour la protection des données.

- Le second projet de loi est relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale.

Pourquoi est-il nécessaire de protéger les données à caractère personnel ?

2. Dès que nous participons à la vie en société, il est fort probable que nos données personnelles se mettent à circuler.

Nous livrons en effet tous, consciemment ou inconsciemment, des données personnelles à une multitude d'organismes, tel par exemple :

- au magasin de vêtements lorsque nous acceptons de livrer des informations personnelles (nom et adresse, numéro de téléphone, adresse email, notre âge, date de naissance, etc) afin d'obtenir la carte de fidélité du magasin,
- à l'administration communale, lors de l'inscription de notre enfant dans une structure d'accueil communale (coordonnées de l'enfant, coordonnées des parents, numéro de téléphone privé et professionnel, lieu de travail des parents etc),
- à notre employeur qui aura besoin de disposer non seulement de notre nom et adresse, mais aussi de notre numéro de sécurité sociale et de notre numéro de compte bancaire,
- à l'administration fiscale lors de la remise de la déclaration d'impôt,
- à notre médecin traitant nous communiquerons même (et forcément) des informations relatives à notre état de santé,
- à notre banquier qui, lorsque nous lui demandons de nous accorder un prêt d'argent, nous demandera en sus des informations dont il dispose déjà, les coordonnées de notre employeur,
- etc.

3. Dans le cadre de la vie active/professionnelle, nombreuses sont ainsi les situations où des données personnelles de clients, patients, salariés, administrés etc, sont utilisées, traitées, enregistrées, stockées par des tiers et cela pour diverses raisons et finalités.

4. Que ce soit la collecte ou l'enregistrement des données, leur exploitation ou leur transmission à des tiers, il existe en permanence un risque d'atteinte à ses droits pour la personne concernée. Aussi peut-

être ne désire-t-elle simplement pas que ses données personnelles soient enregistrées ou encore continuées à des tiers.

5. En vertu de l'article 11(3) de notre Constitution *« L'Etat garantit la protection de la vie privée, sauf les exceptions fixées par la loi. »*

La notion de vie privée

Le droit à la vie privée se définit comme le droit pour une personne d'être libre de mener sa propre existence avec le minimum d'ingérences extérieures, ce droit comportant la ***protection contre toute atteinte portée au droit au nom, à l'image, à la voix, à l'intimité, à l'honneur et à la réputation, à l'oubli, ou à sa propre biographie****.*

La jurisprudence de la Cour européenne des droits de l'homme n'a pas limité le droit au respect de la vie privée au seul domicile privé : « le respect de la vie privée doit aussi englober dans une certaine mesure le droit de l'individu de nouer et de développer des relations avec ses semblables. Il n'y a ***aucune raison de principe d'en exclure les activités professionnelles ou commerciales****. » (Arrêt du 23 novembre 1992, Niemietz c/ Allemagne, A251/B)*

Chaque personne physique a donc le droit au respect de sa vie privée et l'Etat est le garant de ce principe, sauf les entorses que la loi autorise.

6. Les exemples cités ci-avant montrent que dans de nombreuses situations, il est indispensable que des données personnelles de personnes physiques circulent afin que la société puisse fonctionner.

7. Il s'agit donc de trouver un équilibre entre la nécessité de garantir le principe du respect à la vie privée et le besoin de faire circuler, d'utiliser et de gérer les données personnelles des citoyens.

8. Ceci est l'objectif poursuivi par la législation relative à la protection des données personnelles (ci-après législation PDP).

Elle a ainsi pour finalité de donner un certain nombre de garanties aux personnes physiques en insérant tout traitement de données dans des conditions légales précises.

La loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel

9. Le Luxembourg était assez précurseur en matière de protection des données alors que bien avant la première directive européenne en la matière, il avait voté déjà 1979 une loi réglementant l'utilisation de données nominatives dans les traitements informatiques.

10. L'arrivée des nouvelles technologies a fait que les échanges d'informations ne se sont plus arrêtés aux frontières et ceci a mené à la Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 traitant de l'harmonisation du niveau de protection au sein de l'Union Européenne et du principe de libre circulation des données.

11. C'est par la loi (modifiée) du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel que le Luxembourg a transposé cette directive en droit luxembourgeois, toujours en recherchant un équilibre entre d'une part, la protection des droits et libertés fondamentaux des personnes concernées (protection de la vie privée) et d'autre part, la libre circulation de ces données.

12. Depuis lors, toutes les personnes physiques ou morales telles des administrations, des entreprises, des associations et tous autres organismes, qui collectent, enregistrent, utilisent ou transmettent des données personnelles de personnes physiques, c. à d. des données qui permettent de les identifier, elles ne peuvent le faire que dans les conditions posées par la loi modifiée de 2002.

Ces entités doivent en avertir la personne concernée et lui communiquer le but poursuivi de ce que la loi appelle « le traitement des données à caractère personnel ».

Ce traitement doit être conforme à la loi et se limiter à ce qui est nécessaire et doit être proportionné aux buts initialement fixés.

Chaque utilisation des données doit donc se faire dans le respect de règles strictes, le contrôle en étant assuré par la Commission nationale pour la protection des données.

13. A l'origine, la loi de 2002 prévoit que tout fichier contenant des informations relatives à des personnes doit être ou bien déclaré à l'autorité de contrôle ou bien autorisé par elle (selon le type de données ou de traitement) avant de pouvoir être mis en place.

En 2007 la loi a été modifiée dans l'optique de simplifier substantiellement les formalités obligatoires, se traduisant par un allègement du régime d'autorisation préalable et par une simplification essentielle du régime de notification des traitements.

Précisons encore que la législation sur la protection des données personnelles s'applique aussi bien aux fichiers informatiques qu'aux fichiers papier, enregistrements audio et vidéo etc.

La loi réglemente aussi le traitement de données concernant la sécurité publique, la défense, la recherche, la santé et la poursuite d'infractions pénales ou la sûreté de l'Etat.

La nouvelle législation en matière de protection des données à laquelle tous les acteurs devront se conformer pour au plus tard le 25 mai 2018

14. Depuis la première directive européenne de 1995 (ayant donné lieu à la loi nationale de 2002 en matière de protection des données personnelles) la technologique a progressé et continue à évoluer de plus en plus vite.

De nombreux changements sont intervenus depuis et avec cela la nécessité d'adapter le cadre légal afin d'assurer une protection optimale des citoyens quant au traitement de leurs données à caractère personnel et avec cela leur droit au respect de leur vie privée.

15. Il a donc apparu nécessaire pour le législateur européen de poser d'une part, un cadre de protection des données garantissant une protection forte pour les citoyens tout en tenant compte des nouvelles évolutions technologiques, et, d'autre part, une harmonisation des règles en vigueur dans les différents Etats membres de l'Union européenne en permettant au marché économique de se développer dans l'ensemble du marché intérieur, dans le respect des droits fondamentaux des personnes physiques.

16. C'est dans cette optique que la Commission européenne a en 2012 initié une réforme du cadre légal existant, dans le but d'adapter les règles aux nouveaux défis, dans un souci de pérennité et de neutralité technologique, en tenant compte de l'évolution technologique et sociétale des deux dernières décennies.

17. Cette réforme a mené à un « paquet » de textes sur la protection des données qui contient :

1) le 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 (abrogeant la directive 95/46/CE), ci-après « le règlement (UE) 2016/679 », qui prévoit le régime général en matière de protection des données à caractère personnel,

et

2) la directive (UE) 2016/680 du Parlement européen et du Conseil 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 (abrogeant la décision-cadre 2008/977/JAI du Conseil) ci-après « la directive (UE) 2016/680 ».

18. Le règlement (UE) 2016/679 prévoit un délai de mise en application de deux ans. Il entrera définitivement en vigueur à partir du 25 mai 2018, date à laquelle il remplacera ainsi définitivement et directement les législations nationales actuellement existantes au sein des 28 Etats membres.

19. Les deux projets de loi sous avis représentent l'adaptation nationale du « paquet » de textes européens.

20. Le règlement (UE) 2016/679, tenant à harmoniser les règles nationales existantes et à moderniser le cadre légal, a pour but de renforcer la protection des données à caractère personnel dans une société de plus en plus digitale, en redonnant aux citoyens le contrôle des données personnelles qui les concernent, que celles-ci soient collectées et utilisées par les acteurs économiques privés ou par les acteurs du secteur public.

Etant donné qu'il s'agit d'un règlement européen, il est d'application directe dans tous les Etats membres, y compris au Luxembourg.

C'est par conséquent dès lors le règlement (UE) 2016/679 qui prévoit la majorité des dispositions de fond désormais applicables en matière de protection des données.

21. Le projet de loi 7184 portant création de la Commission nationale pour la protection des données et mise en œuvre du règlement (UE) 2016/679, soumis à l'avis de la CSL, vient compléter le règlement (UE) 2016/679 en se limitant à compléter le cadre européen par les dispositions nationales qui s'imposent, à savoir l'adaptation de la législation en ce qui concerne la Commission nationale pour la protection des données (CNPD) afin essentiellement d'octroyer à cette commission les nouveaux pouvoirs qui lui seront nécessaires pour qu'elle puisse exercer les missions qui lui reviennent de par le nouveau règlement (UE) 2016/679.

Le règlement (UE) 2016/679 prévoit en effet une responsabilisation accrue de tous les acteurs qui traitent des données personnelles et cela par le biais d'un autocontrôle des entreprises et des moyens de contrôles et de sanctions nettement plus conséquents et dissuasifs au profit des autorités nationales de contrôle en cas de violation constatée aux règles applicables, le but en étant protection plus efficace de la protection des données personnelles.

Le projet de loi no 7184 vise ainsi à doter la CNPD des moyens nécessaires tout en étendant son champ de compétences aux traitements de données à caractère personnel tombant dans le champ d'application de la future loi transposant la directive (UE) 2016/680 (projet de loi no 7168) concernant la protection des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité

nationale (mais à l'exception des traitements de données à caractère personnel effectués par les juridictions).

Les missions et les pouvoirs de la CNPD vont être nettement augmentés telle notamment la possibilité d'imposer des amendes administratives très dissuasives, pouvant aller jusqu'à 20 millions d'euros, ou dans le cas d'une entreprise jusqu'à 4% du chiffre d'affaires annuel mondial total de l'exercice précédent. Aussi la CNPD aura-t-elle des pouvoirs réglementaires très étendus en matière de protection des données.

Vu l'extension du champ de compétence de la CNPD, le projet de loi propose d'augmenter le nombre de commissaires du collège de la CNPD de 3 à 4 membres, en spécifiant qu'une expérience professionnelle dans le domaine de la prévention, la recherche, la constatation et la poursuite des infractions pénales doit être assurée au sein du collège.

Précisons encore que le projet de loi prévoit la suppression de la loi modifiée de 2002 étant donné que les règles en matière de protection des données personnelles résultent désormais essentiellement du règlement (UE) 2016/679.

22. Le second projet de loi sous avis est le projet de loi no 7168 relatif à la protection des données personnelles en matière pénale et de sécurité nationale.

Il complète la transposition du cadre légal européen en portant transposition en droit luxembourgeois de la directive (UE) n° 2016/680 du Parlement européen et du Conseil 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.

Ce projet, tout comme la directive européenne de base, tend à adapter les règles en matière pénale aux exigences posées par les évolutions technologiques des dernières décennies.

Il fixe les règles relatives à la protection des données applicables aux traitements de données à caractère personnel effectués par les autorités compétentes *(notamment la police, l'inspection générale de la police, le service de renseignement, l'administration pénitentiaire, l'armée, la cellule de renseignement financier, le parquet, le juge d'instruction,…)* à des fins de

- prévention et de détection des infractions pénales,
- enquêtes et de poursuites en matière d'infractions pénales,
- exécution de sanctions pénales,
- protection contre les menaces pour la sécurité publique et la prévention de telles menaces,
- protection contre les menaces pour la sécurité nationale et sa prévention.

Vue d'ensemble de la législation générale « protection des données »[1] telle qu'elle sera applicable au plus tard à partir du 25 mai 2018

Le champ d'application de la législation PDP

23. Dès que des données personnelles *(nom, prénom, âge, numéro de téléphone, adresse email, adresse, image de la personne, sa voix, etc.)* permettant d'identifier des personnes physiques, sont traitées *(c. à d. utilisées, stockées, gérées, etc.)* par une autre personne physique ou morale *(appelée le responsable du traitement)*, le cadre légal protecteur s'applique.

[1] Ci-après législation PDP

24. Mais attention :

Seules les personnes physiques sont protégées par la législation PDP à l'exclusion des personnes morales.

Sont aussi exclues du champ d'application, les traitements mis en œuvre dans le cadre des activités personnelles/domestiques d'une personne physique.

Précisons encore que la législation PDP s'applique à tout traitement de données effectué sur le territoire de l'Union européenne, peu importe où se situe le responsable du traitement.

Elle s'applique en outre à tout traitement de données relatives à des personnes physiques se trouvant sur le territoire de l'Union européenne et lié à une offre de biens/servies ou au suivi de leur comportement.

Quelques notions importantes en matière de protection des données à caractère personnel :

***25**. Donnée à caractère personnel :*

Il s'agit de toute information se rapportant à une personne physique et permettant de l'identifier.

Tels par exemple son nom, son adresse, son numéro de téléphone, son numéro d'identifiant ; sa donnée de localisation, sa capture d'image ; sa donnée physique, culturelle, sociale, économique, etc.

Traitement de données :

26. Il s'agit de toute opération effectuée ou non à l'aide de procédés automatisés, et appliqués à des données.

Tels par exemple la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, etc. peu importe le support utilisé.

Responsable du traitement :

27. C'est la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui détermine les finalités et les moyens du traitement des données.

Par exemple le médecin qui traite les données de ses patients, l'employeur qui traite les données de ses salariés, l'école qui traite les données de ses élèves, le propriétaire d'un magasin qui tient son fichier clients, etc….

Les conditions de licéité d'un traitement de données personnelles

28. Chaque responsable d'un traitement doit s'assurer de :

- Traiter les données de manière licite, loyale et transparente**,**
- Limiter les finalités : les données ne peuvent être traitées que pour une ou plusieurs finalités déterminées, explicites et légitimes,
- Utiliser des données adéquates, pertinentes et non excessives au regard des finalités déterminées,
- Garantir l'exactitude des données et, si nécessaire, les mettre à jour,
- Limiter la durée de conservation des données,
- Garantir une sécurité appropriée des données (contre le traitement non autorisé ou illicite, contre la perte, la destruction ou les dégâts d'origine accidentelle notamment).

Le responsable du traitement doit à tout moment pouvoir prouver que toutes ces obligations sont respectées.

29. Un traitement mis en œuvre n'est licite que s'il correspond à un des six cas d'ouverture posés par la législation PDP :

1. La personne concernée a donné son accord au traitement.

Par exemple : Monsieur X accepte de fournir ses coordonnées lors d'une inscription à une formation et accepte que celles-ci soient traitées par l'organisme formateur.

Notons que le responsable du traitement doit pouvoir prouver le consentement et si le consentement est donné dans une déclaration écrite qui comprend également d'autres questions, la demande de consentement doit être présentée sous une forme qui la distingue clairement des autres questions, et elle doit être formulée en des termes clairs et simples.
La personne concernée a en outre le droit de retirer son consentement à tout moment.

2. Le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci.

Par exemple : Si Madame Y ne donne pas son adresse privée au magasin de meubles où elle a acheté une armoire, celle-ci ne pourra pas lui être livrée et installée à son domicile. Il est donc nécessaire à l'exécution du contrat qu'elle livre cette information.

3. Le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis.

Par exemple : La loi impose au banquier de vérifier l'identité exacte de son client ; il est donc légitime pour lui de prendre une copie du document d'identité de son client.

4. Le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique.

Par exemple : Le médecin est tenu de prendre note des allergies de ses patients afin de ne pas leur prescrire des médicaments qu'ils ne supporteraient pas.

5. Le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement.

Par exemple : Il est légitime pour un Etat d'enregistrer le parcours criminel d'un citoyen.

6. Le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement.

Par exemple : Il est légitime pour une école supérieure de demander une copie du diplôme de fin d'études secondaires des candidats demandant leur admission au cycle d'études supérieures proposé par l'école.

Les données dont le traitement est interdit

30. La législation PDP interdit de traiter des données ayant trait:

- à l'origine raciale ou ethnique,
- aux opinions politiques,
- aux convictions religieuses ou philosophiques,
- à l'appartenance syndicale,

- aux données génétiques,
- aux données biométriques,
- aux données concernant la santé, la vie sexuelle ou l'orientation sexuelle.

Notons que la législation PDP fixe de nombreuses exceptions à ce principe, tel par exemple en matière de santé, la permission pour les professionnels de la santé de traiter les données liées à l'état de santé du patient.

Ou encore les cas dans lesquels le traitement d'une donnée sensible est nécessaire aux fins de l'exécution des obligations et de l'exercice des droits propres du responsable du traitement ou à la personne concernée en matière de droit du travail, de la sécurité sociale et de la protection sociale, dans la mesure où le traitement est autorisé en vertu d'une disposition légale européenne, nationale ou d'une convention collective de travail prévoyant des garanties appropriées pour les droits fondamentaux et les intérêts de la personne concernée.

Traitements spéciaux de données

31. Certains traitements de données sont spécialement réglementés, notamment les traitements effectués dans le cadre de la liberté d'expression, les traitements et accès du public aux documents officiels, les traitements de données particulières par les services de santé, les traitements à des fins de recherche scientifique ou historique ou statistiques et les traitements de données dans le cadre des relations de travail.

Traitement de données personnelles dans le cadre des relations de travail

32. Suivant l'article 88 du règlement EU 2016/679 « *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.*

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.

Chaque État membre notifie à la Commission les dispositions légales qu'il adopte en vertu du paragraphe 1 au plus tard le 25 mai 2018 et, sans tarder, toute modification ultérieure les concernant. »

33. Le texte européen permet ainsi au législateur national de réglementer particulièrement la question de la protection des données sur le lieu du travail.

34. Le législateur luxembourgeois a prévu dans son article L.261-1 du Code du travail national qu'un traitement de données à des fins de surveillance touchant des salariés ne peut être mis en œuvre par l'employeur que s'il est nécessaire :

1. Pour les besoins de sécurité et de santé des travailleurs.

Par exemple : Surveillance d'une station-service par caméra : protéger les salariés contre les agressions, risque d'explosion etc.

2. Pour les besoins de protection des biens de l'entreprise.

Par exemple : Protection de la salle des coffres-forts d'une banque par caméra

3. Pour le contrôle du processus de production portant uniquement sur les machines.

Par exemple : Surveillance d'une chaîne d'assemblage automatique de produits

4. Pour le contrôle temporaire de production ou des prestations du travailleur, lorsqu'une telle mesure est le seul moyen pour déterminer la rémunération exacte.

5. Dans le cadre d'une organisation de travail selon l'horaire mobile.

35. En ce qui concerne les points no 1, 4 et 5 le comité mixte d'entreprise lorsqu'il existe, et dès les prochaines élections sociales la délégation du personnel dans les entreprises d'au moins 150 salariés, a un pouvoir de décision quant à l'instauration d'un tel traitement aux fins de surveillance des salariés.

36. Notons aussi que le consentement de la personne concernée ne rend pas légitime un traitement mis en œuvre par l'employeur à des fins de surveillance et qui serait non conforme à la loi.

37. Avant de mettre en œuvre un traitement à des fins de surveillance, l'employeur doit au préalable informer aussi bien les salariés concernés, ainsi que le comité mixte d'entreprise ou, à défaut, la délégation du personnel[2] ou, à défaut encore, l'Inspection du travail et des mines.

38. Si le traitement est effectué en violation de l'article L.261-1 du Code du travail, alors l'employeur s'expose à une peine d'emprisonnement de 8 jours à 1 an et à une amende de 251 à 125.000 euros ou d'une de ces peines seulement.

Notons encore qu'une juridiction saisie d'une violation légale pourrait prononcer la cessation d'un traitement contraire à la loi sous peine d'astreinte.

39. La loi modifiée de 2002 fournit une définition de la notion de surveillance. Il s'agit de « toute activité qui, opérée au moyen d'instruments techniques, consiste en l'observation, la collecte ou l'enregistrement de manière non occasionnelle des données à caractère personnel d'une ou de plusieurs personnes, relatives à des comportements, des mouvements, des communications ou à l'utilisation d'appareils électroniques et informatisés ».

Cette définition disparaît avec le projet de loi 7184 qui abroge la loi de 2002. Ni le règlement (UE) 2016/679, ni le projet de loi no 7184 ne prévoient une définition de la notion de surveillance.

La CSL regrette ce manque et espère que la CNPD fera utilisation de son pouvoir réglementaire pour pallier à cette lacune.

[2] Dès les prochaines élections sociales : la délégation du personnel sera dans tous les cas informée, et à défaut ce sera l'ITM

40. La CSL revient en outre à ses critiques formulées dans le cadre du projet de loi 7049 portant modification de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard des données à caractère personnel.

41. Une des modifications qui étaient proposées par ce projet de loi résidait dans la suppression du système de l'autorisation préalable de la Commission nationale pour la protection des données (CNPD) d'un traitement à des fins de surveillance sur le lieu de travail.

42. Cette suppression devait être remplacée par un système de contrôle a posteriori qui ne faisait cependant pas l'objet de ce projet de loi.

43. C'est le projet de loi no 7184 sous avis qui, en investissant la CNPD de tous les moyens prévus par le règlement (UE) 2016/679, permettra ce contrôle par la CNPD.

44. Néanmoins la CSL s'exprime, comme dans son avis relatif au projet de loi no 7049, contre la suppression du mécanisme d'autorisation préalable en ce qui concerne un traitement de données à des fins de surveillance sur le lieu de travail et cela pour les raisons suivantes :

1. **Le règlement européen permet, comme nous l'avons précisé ci-avant, de consacrer des règles spécifiques dans les relations de travail. Rien ne s'oppose ainsi au maintien de notre mécanisme de contrôle préalable en ce qui concerne le domaine « relations de travail ».**

2. **Comment comptons-nous à échelle nationale assurer une protection suffisante des salariés sur le lieu de travail contre des abus de leur employeur à défaut de disposer de ce contrôle préalable ? Le contrôle a posteriori, sur base de plaintes effectuées par des salariés ou par la délégation du personnel de l'entreprise, sera-t-il aussi efficace que le système actuel obligeant l'employeur à attendre l'autorisation officielle de la CNPD avant de pouvoir mettre en place un dispositif de surveillance touchant ses salariés ? Probablement pas, cela d'autant que la CNPD ne sera élargie que d'un seul membre, ce qui semble insuffisant pour assurer un contrôle a posteriori efficace.**

3. **Les autorisations préalables actuelles de la CNPD sont toujours assorties de conditions précises d'exercice des modalités de surveillance.**

   Suivant les travaux parlementaires ayant donné naissance à la loi de 2002, l'exigence d'une autorisation préalable traduisait justement la volonté expresse du législateur luxembourgeois de protéger les personnes physiques contre certains traitements « susceptibles de présenter des risques particuliers au regard des droits et libertés des personnes concernées… ». Parmi ceux-ci figurent notamment les traitements en matière de surveillance sur le lieu de travail étant donné que ceux-ci présentent un risque particulier au regard de la vie privée des salariés sur leur lieu de travail.

   Ainsi par exemple un employeur voulant mettre en place un dispositif de vidéosurveillance doit-il à ce jour obtenir l'aval préalable de la CNPD. Ce qui implique que la CNPD vérifie si les finalités du traitement de données par vidéo caméra répondent à une ou plusieurs des conditions de légitimité admises (sécurité et santé des salariés, protection des biens de l'entreprise, contrôle du processus de production portant uniquement sur les machines). Ensuite elle analyse au cas par cas en détail la nécessité et la proportionnalité pour chaque « zone » surveillée.

   La jurisprudence a clairement établi que la CNPD dispose d'un pouvoir d'appréciation in concreto dans l'analyse qu'elle doit effectuer pour autoriser des traitements de données. Cette analyse suppose notamment un examen de moyens alternatifs permettant au responsable du traitement de réaliser les mêmes finalités, mais en utilisant des moyens

moins attentatoires à la vie privée des personnes concernées qu'une surveillance par vidéo camera.

Dans certaines zones où l'installation d'une caméra peut être légitime au sens de la loi, les droits des personnes concernées peuvent primer sur la nécessité de mettre en œuvre une vidéosurveillance.

Par exemple, l'installation d'une caméra de surveillance dans un bureau où travaille en permanence un salarié est considérée comme disproportionnée ou excessive, les droits et libertés fondamentaux des salariés prévalant sur les intérêts poursuivis par l'employeur.

De même, l'installation de caméras vidéo dans la cuisine d'un restaurant sera considérée comme disproportionnée et/ou excessive, considérant que tous les salariés employés à la cuisine se trouveront quasiment en permanence sous ces caméras.

C'est pourquoi la CNPD, dans ses décisions, exclut certaines zones et/ou assortit ses autorisations de conditions et exigences :

- **interdiction d'une surveillance permanente et continue, sauf exceptions rares ;**
- **interdiction d'enregistrer le son associé aux images ;**
- **interdiction de surveiller les prestations et les comportements des salariés ;**
- **interdiction de filmer les endroits réservés aux salariés pour un usage privé ;**
- **champ de vision limité des caméras filmant les accès intérieurs, extérieurs ou les alentours d'un bâtiment ou d'un site ;**
- **durée de conservation des images limitée etc.**

En supprimant l'exigence d'une autorisation, toute cette appréciation concrète des traitements de vidéosurveillance sur le lieu de travail ne se fera plus avant leur mise en œuvre, ce au détriment des salariés.

A défaut de les intégrer dans la future loi, ces restrictions ne seront donc plus clairement applicables et les employeurs auront l'impression d'en être libérés. La protection des salariés sera par conséquent gravement amoindrie.

4. **Le Code du travail prévoit certes des sanctions pénales contre le responsable d'un traitement illégal et permet même que la juridiction saisie prononce la cessation du traitement sous peine d'astreinte, mais encore faudrait-il qu'elles soient effectivement prononcées. Quel salarié osera dénoncer son employeur qui méconnait ces règles au risque de perdre son emploi ?**

45. Pour toutes ces raisons la CSL s'oppose à la suppression du mécanisme de l'autorisation préalable.

Même en admettant que la CNPD va user de son pouvoir règlementaire pour insérer les surveillances pratiquées sur le lieu de travail dans des conditions plus strictes, ceci sera certainement moins efficace que si elles sont stipulées noir sur blanc dans une autorisation préalable qui s'impose très clairement à un employeur et qui en plus est adaptée à la situation de l'entreprise en question.

46. A titre subsidiaire, la CSL espère néanmoins que la CNPD émettra sans tarder une réglementation stricte et précise pour toute sorte de traitement de données effectué à des fins de surveillance sur le lieu de travail.

46bis. La CSL est finalement d'avis que la délégation du personnel doit dans toutes les entreprises disposer d'un pouvoir de co-décision en ce qui concerne la mise en place (ainsi qu'un changement ultérieur) d'un traitement de données à des fins de surveillance sur le lieu de travail.

Cela est d'autant important si le mécanisme de l'autorisation préalable par la CNPD doit disparaître. Cela aidera à protéger les salariés contre une mise en place abusive de systèmes utilisés à des fins de surveillance sur le lieu de travail, les représentants du personnel pouvant au préalable vérifier et apprécier ensemble avec l'employeur si l'entreprise peut baser de manière légitime son mécanisme de surveillance sur un des cinq cas d'ouverture posés par le Code du travail.

En outre la future loi doit acter le principe que si la délégation du personnel a donné son accord au traitement de données à des fins de surveillance, cela ne peut en aucun cas avoir pour effet de rendre légitime un traitement mis en place par l'employeur en violation des règles légales.

Le projet de loi doit en outre fixer le droit pour la délégation du personnel d'être informée et consultée préalablement à la mise en œuvre de tout traitement de données par l'employeur qui concerne les salariés de l'entreprise, que le traitement soit mis en œuvre pour des besoins administratifs, pour des besoins de recrutement ou de gestion du personnel. Il doit en être de même de tout changement que l'employeur désire appliquer ultérieurement à un traitement de données.

La future loi doit aussi acter le principe que si la délégation du personnel a donné un avis favorable au traitement de données que l'employeur entend mettre en œuvre, cela ne peut en aucun cas avoir pour effet de rendre légitime un traitement mis en place par l'employeur en violation des règles légales.

Droits de la personne concernée par un traitement de données

47. Toute personne concernée par un traitement de données dispose d'un certain nombre de droits. Ces droits sont largement augmentés avec le règlement (UE) 2016/679.

Il s'agit du droit à l'information, du droit d'accès, du droit de rectification, du droit à l'effacement des données, du droit à la limitation du traitement, du droit à la portabilité des données, du droit d'opposition, du droit de s'opposer au profilage, du droit à la réclamation et du droit à réparation.

Droit à l'information

48. La personne concernée a le droit d'être informée au moment où les données la concernant sont collectées auprès d'elle-même sur les éléments suivants :

- l'identité et les coordonnées du responsable du traitement,
- le cas échéant, les coordonnées du délégué à la protection des données (voir explications sous les points no 64 et suivants),
- la finalité du traitement et sa base légale,
- si le traitement est basé sur l'intérêt légitime du responsable du traitement: son intérêt légitime est à spécifier,
- le ou les destinataires des données,
- la durée de conservation des données, sinon les critères employés pour la déterminer,
- l'existence du droit d'accès, à la rectification, à l'effacement, à la limitation des données, du droit de s'opposer au traitement et du droit à la portabilité des données, du droit de retirer son consentement et du droit d'introduire une réclamation,

- le caractère réglementaire, contractuel ou obligatoire ou non de la fourniture des données et les conséquences d'un éventuel refus,
- l'existence d'une prise de décision automatisée ou d'un profilage,
- le cas échéant l'utilisation des données à une autre fin.

49. Si les données ne sont pas recueillies directement auprès de la personne concernée :

- la source des données doit être indiquée avec la précision si la source est accessible au public ou pas ;
- le responsable du traitement fournit les informations énumérées au point 48 ci-avant :
    - dans un délai raisonnable après avoir obtenu les données à caractère personnel, mais ne dépassant pas un mois, ou
    - si les données à caractère personnel doivent être utilisées aux fins de la communication avec la personne concernée, au plus tard au moment de la première communication avec ladite personne; ou
    - s'il est envisagé de communiquer les informations à un autre destinataire, au plus tard lorsque les données à caractère personnel sont communiquées pour la première fois.

50. Notons en outre que toute personne a toujours le droit d'être informée sur demande dans un délai d'un mois, ainsi que d'être informée de toute violation de ses données.

Droit d'accès

51. La personne concernée a le droit d'accéder aux données traitées avec les informations relevant du droit à l'information et d'obtenir une copie gratuite des données. Précisons qu'en cas de demande de copies supplémentaires, le responsable du traitement pourra demander le paiement de frais raisonnables pour toute copie supplémentaire.

Droit de rectification

52. Il s'agit du droit de demander la rectification de données inexactes dans les meilleurs délais, ainsi que du droit d'obtenir que des données incomplètes soient complétées.

Droit à l'effacement des données dans les meilleurs délais

53. Ce droit joue dès que les données ne sont plus nécessaires pour la finalité visée, lorsque le traitement est basé sur le consentement et que le consentement est retiré, dans le cas de l'exercice justifié du droit d'opposition, lorsque le traitement de données est illicite, lorsque l'effacement est nécessaire pour garantir le respect d'une obligation légale, lorsque les données sont collectées dans le cadre de services proposés à des enfants/jeunes de moins de 16 ans.

Notons que des exceptions existent quant à l'exercice de ce droit et cela notamment dans les cas suivants :

- exercice du droit à la liberté d'expression/d'information,
- nécessité de garantir le respect d'une obligation légale,
- intérêt public dans le cadre de la santé publique,
- archivage dans l'intérêt public, recherche scientifique ou historique, statistiques,
- défense de droits en justice.

Droit d'opposition

54. Lorsque le traitement a lieu dans le cadre d'une mission publique et que le traitement est basé sur l'intérêt légitime du responsable du traitement, la personne concernée a le droit de s'opposer pour des raisons tenant à la situation particulière au traitement, sauf si l'intérêt public prime.

En outre, toute personne a le droit de s'opposer à un traitement de données à des fins de prospection.

Droit à la limitation du traitement

55. Ce droit peut être exercé pendant la vérification des données suite à une mise en doute de l'exactitude des données ou lorsque le traitement est illicite et la personne concernée s'oppose à l'effacement, mais demande la limitation ou encore lorsque le responsable du traitement n'a plus besoin des données, mais que la personne concernée en a besoin pour la défense de ses droits en justice ou encore lorsque la personne concernée s'oppose au traitement et le traitement est alors limité pendant le temps nécessaire pour vérifier si motifs légitimes du responsable du traitement prévalent.

Droit à la portabilité

56. Lorsque le traitement est fondé sur le consentement de la personne concernée ou lorsque le traitement est effectué à l'aide de procédés informatisés, la personne concernée a le droit de demander que les données soient d'office transférées par le responsable du traitement à un autre responsable du traitement.

Profilage et traitement automatisé de données

57. Toute personne a le droit de s'opposer à une décision basée sur un profilage ou un traitement automatisé de ses données lorsqu'il produit des effets juridiques ou affecte la personne significativement de manière similaire. Sauf si le traitement est nécessaire à la conclusion/exécution d'un contrat ou fondé sur le consentement explicite de la personne ou lorsque le traitement est autorisé par le droit européen ou national du responsable du traitement.

Attention aux données sensibles : elles ne peuvent faire l'objet d'un tel traitement que si la personne concernée a donné son consentement ou dans l'intérêt public et que des mesures appropriées de protection des droits et libertés ont été prises.

Droit à la réclamation

58. Chaque personne physique peut introduire une réclamation auprès de la CNPD pour violation de ses droits sur base de la législation PDP. La CNPD informe le plaignant de l'état d'avancement et de l'issue de la réclamation.

Droit à la réparation

58bis. Le responsable du traitement doit réparer le préjudice subi par la personne concernée, sauf à prouver qu'il n'est pas responsable.

Droit de recours

59. La loi prévoit aussi un droit de recours contre un responsable du traitement, voir même contre les décisions de la CNPD, ainsi que le droit de se faire représenter par un organisme/ASBL d'intérêt public

et actif dans le domaine de la protection des droits et libertés des personnes en matière de protection des données personnelles.

Les obligations du responsable du traitement

60. Nous l'avons déjà précisé en introduction, la législation PDP met un nombre important d'obligations à charge du responsable du traitement lesquelles peuvent être résumées comme suit :

- respecter toutes les règles légales posées par la législation PDP à tout moment,
- savoir démontrer et documenter à tout moment sa conformité à la législation PDP par des mesures techniques et organisationnelles appropriées,
- assurer la sécurité des données traitées,
- assurer au maximum la protection des données dès la conception et la protection des données par défaut,
- choisir (le cas échéant/s'il y a lieu) un sous-traitant qui présente des garanties suffisantes; baser cet accord sur un contrat écrit contenant des clauses de confidentialité,
- tenir un registre des activités de traitement,
- notifier à la CNPD toute violation des données traitées dans les meilleurs délais et au plus tard dans les 72 heures,
- informer la personne physique concernée de toute violation de données s'il y a un risque élevé d'atteinte aux droits et libertés,
- effectuer une analyse d'impact s'il y a un risque élevé pour les droits et libertés des personnes physiques,
- désigner le cas échéant un délégué à la protection des données.

61. Le non-respect de ces règles expose le responsable du traitement à une amende administrative jusqu'à 20 millions d'euros ou de 4% de son chiffre d'affaires annuel mondial.

Sécurité des traitements de données personnelles

62. Le responsable du traitement doit s'assurer de n'utiliser que des moyens garantissant la confidentialité, l'intégrité, la disponibilité et la résilience des systèmes de traitement.

Il doit disposer des moyens pour rétablir la disponibilité/accès aux données en cas d'incident.

Il doit aussi disposer d'une procédure pour tester, analyser et évaluer régulièrement l'efficacité des mesures de sécurité en fonction du degré de risques de chaque traitement.

Registre des traitements de données personnelles mis en œuvre

63. Le responsable du traitement doit disposer et tenir à jour un registre de tous ses traitements avec pour chaque traitement les précisions suivantes :

- nom, coordonnées du responsable du traitement, le cas échéant de son représentant et du délégué à la protection des données (voir ci-après sous les points 64 et suivants), et le cas échéant de son sous-traitant,
- la ou les finalités du traitement,
- la base légale du traitement,
- les catégories de personnes et de données concernées,
- les destinataires des données,

- les délais prévus pour l'effacement si possible, sinon les critères appliqués pour en décider,
- les personnes ayant accès en interne aux données,
- les mesures de sécurité techniques et organisationnelles prévues.

Le délégué à la protection des données

64. Dans certains cas le responsable du traitement sera tenu de nommer un délégué à la protection des données à savoir :

- lorsque le responsable du traitement est une autorité/organisme public, ou
- lorsqu'il traite des données nécessitant un suivi régulier et systématique à grande échelle, ou
- lorsqu'il traite à grande échelle des catégories particulières (celles qui sont en principe interdites d'être traitées) de données.

La CSL tient à relever qu'il ne sera pas aisé pour un responsable de traitement de déterminer s'il doit nommer un délégué à la protection des données, notamment s'il doit apprécier s'il est oui ou non dans la situation où il traite des données nécessitant un suivi régulier et systématique à grande échelle, ou s'il est oui ou non dans la situation où il traite à grande échelle des catégories particulières (celles qui sont en principe interdites d'être traitées) de données.

Le Gouvernement national devrait intervenir auprès des instances européennes afin qu'il soit remédié à cette incertitude et demander que des critères plus précis soient élaborés.

65. Le délégué à la protection des données a les missions suivantes :

- informer et conseiller le responsable du traitement et ses salariés,
- contrôler le respect de l'application de la législation PDP par le responsable du traitement et ses salariés, notamment en ce qui concerne les règles internes, la répartition des responsabilités, la sensibilisation et la formation du personnel,
- donner des conseils quant à l'analyse d'impact,
- coopérer avec l'autorité de contrôle nationale et être son point de contact.

66. Le délégué à la protection des données doit :

- être associé par le responsable du traitement à toute question liée à la protection des données,
- recevoir les ressources nécessaires, y compris les moyens d'entretenir ses compétences en matière de protection des données,
- recevoir l'accès aux données et aux traitements effectués,
- exercer sa mission en toute indépendance par rapport au responsable du traitement,
- rapporter au niveau hiérarchique le plus élevé de la direction du responsable du traitement.

67. Il peut être un salarié du responsable du traitement dont les tâches ne sont pas en conflit avec ses missions de délégué à la protection des données, ou un indépendant lié par contrat de service au responsable du traitement.

Il doit avoir de bonnes connaissances du droit et des techniques en matière de protection des données.

Analyse d'impact

67bis. Lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement doit

effectuer, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel.

Lorsqu'il effectue une analyse d'impact relative à la protection des données, le responsable du traitement doit demander conseil au délégué à la protection des données, si un tel délégué a été désigné.

L'analyse d'impact relative à la protection des données est, en particulier, requise dans les cas suivants :

a) l'évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques, qui est fondée sur un traitement automatisé, y compris le profilage, et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire ;

b) le traitement à grande échelle de catégories particulières de données ou de données à caractère personnel relatives à des condamnations pénales et à des infractions ; ou

c) la surveillance systématique à grande échelle d'une zone accessible au public.

La CNPD devrait établir et publier une liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise.

La CNPD, l'autorité nationale de contrôle indépendante

68. Rappelons que la CNPD est chargée de contrôler la conformité de tous les traitements de données par rapport à la législation PDP, y compris en matière pénale et de sécurité nationale sauf en ce qui concerne les traitements émis par les juridictions de l'ordre judiciaire, de l'ordre administratif et du ministère public en matière juridictionnelle (compétence de l'autorité de contrôle judiciaire).

69. Suite au règlement (UE) 2016/679 la CNPD se voit donc confier de larges pouvoirs que l'on peut résumer comme suit :

- elle dispose désormais d'un pouvoir réglementaire,
- elle reçoit les plaintes en matière de protection des données personnelles,
- elle vérifie la licéité des traitements mis en place,
- elle fournit sur demande à des personnes physiques des informations sur l'exercice de leurs droits,
- elle examine et retire le cas échéant les certifications en matière de protection des données,
- elle mène des investigations/enquêtes avec accès direct aux locaux où sont traités les données, ainsi qu'aux traitements,
- elle dénonce les infractions aux autorités judicaires,
- elle met en place des mécanismes pour permettre le signalement confidentiel de violations en matière pénale,
- elle enjoint au responsable du traitement de communiquer toute violation à la personne physique concernée s'il ne l'a pas fait,
- elle peut imposer une limitation/interdiction temporaire ou définitive de traitement,
- elle ordonne la rectification ou l'effacement de données,
- elle sanctionne par
    - des astreintes,
    - des avertissements,
    - des verrouillages,
    - l'effacement ou la destruction des données,

- l'interdiction de traitement,
- l'insertion de décisions d'interdiction dans les journaux.,
- une amende administrative jusqu'à 20 mio d'euros ou jusqu'à 4% du chiffre d'affaires annuel mondial du responsable du traitement,

- elle peut agir en justice.

70. Quiconque entrave la CNPD dans l'exercice de ses missions légales ou met en œuvre un traitement contraire à la loi s'expose à des sanctions pénales *(emprisonnement de 8 jours à 1 an et amende de 251 à 125000 euros)* .

71. La CSL est d'avis que la CNPD ne comprend pas suffisamment de membres pour faire face aux nombreuses nouvelles missions que la législation PDP lui accorde.

72. Sous réserve des remarques formulées, la CSL donne son accord au présent projet de loi.

Luxembourg, le 5 décembre 2017

Pour la Chambre des salariés,

Norbert TREMUTH
Directeur

Jean-Claude REDING
Président

L'avis a été adopté à l'unanimité.