Avis n° 35/2012 du 21 novembre 2012

Objet: Avis d'initiative sur la proposition de Règlement du Parlement européen et du Conseil 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[1] (CO-A-2012-015)

La Commission de la protection de la vie privée ;

Vu la loi du 8 décembre 1992 *relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel* (ci-après LVP), en particulier l'article 29 ;

Vu le rapport de Monsieur Willem Debeuckelaere, Président et de Monsieur Verschuere, Vice-président ;

Émet, le 21 novembre 2012, l'avis suivant :

[1] COM (2012)11 final.

I. INTRODUCTION

1. Objet du présent avis

1. Le 25 janvier 2012, la Commission européenne (CE) a publié sa proposition de cadre juridique renouvelé pour la protection des données dans l'Union européenne (Data Protection Package)[2]. Ce nouveau régime de protection envisagé se compose de deux propositions législatives :

- une proposition de Règlement du Parlement européen et du Conseil 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[3] (ci-après "le projet de Règlement") et,

- une proposition de Directive du Parlement européen et du Conseil 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[4] (ci-après "la proposition de Directive").

2. La Commission de la protection de la vie privée (ci-après la "CPVP") a pris connaissance de ces propositions et en a débattu lors de ses séances des 8 février, 29 février, 14 mars, 21 mars, 11 avril, 18 avril, 25 avril, 23 mai, 17 octobre et 21 novembre 2012.

3. Le présent avis d'initiative porte toutefois exclusivement sur le projet de Règlement. Il s'agit d'une première analyse – principalement par article – et la CPVP se réserve le droit d'émettre ultérieurement un avis complémentaire.

4. La CPVP attire l'attention sur le fait que le présent avis se base sur le texte en langue française et en langue néerlandaise du projet de Règlement. Elle le mentionne car elle a pu constater que le texte du projet diffère en certains points selon la langue de rédaction[5].

---

[2] COM(2012) 9 final.

[3] COM(2012) 11 final.

[4] COM(2012) 10 final.

[5] À titre d'exemple : la dernière phrase de l'article 47.3 a une autre signification en français qu'en néerlandais :

- "*Les membres de l'autorité de contrôle (…), n'exercent aucune activité professionnelle incompatible, rémunérée ou non.*

- De leden van de toezichthoudende autoriteit (…) verrichten gedurende hun ambtstermijn geen andere al dan niet bezoldigde beroepswerkzaamheden.".

2. Rétroactes

A. La communication du 4 novembre 2010 de la Commission européenne

5. Dans une communication du 4 novembre 2010 intitulée "*Une approche globale de la protection des données à caractère personnel dans l'Union européenne*", la Commission européenne énonce ses objectifs de réforme[6] :

- Renforcer les droits des personnes : accroître la transparence, permettre d'exercer un meilleur contrôle sur les données les concernant, garantir un consentement éclairé et libre, protéger les données sensibles, renforcer l'efficacité des voies de recours et des sanctions, et intensifier les actions de sensibilisation des personnes concernées à leurs droits;
- Renforcer la dimension "marché intérieur", notamment en réduisant la charge administrative, en responsabilisant davantage les responsables de traitement, en encourageant les initiatives en matière d'autorégulation et en examinant la possibilité d'instaurer des régimes européens de certification ;
- Réviser les règles de protection des données dans les domaines de la coopération policière et judiciaire en matière pénale (proposition de Directive) ;
- Prendre en compte la dimension globale de la protection des données : clarifier et simplifier les règles relatives aux transferts internationaux de données et promouvoir des principes universels ;
- Renforcer le cadre institutionnel en vue d'un plus grand respect des règles de protection des données : renforcer l'indépendance, clarifier et harmoniser le statut et les pouvoirs des autorités nationales de protection des données, améliorer la coopération et la coordination entre elles.

6. L'exposé des motifs du projet de Règlement formule les motifs retenus de l'action et les objectifs poursuivis par la CE dans les termes suivants : "*S'il demeure satisfaisant en ce qui concerne ses objectifs et ses principes, le cadre juridique actuel n'a cependant pas permis d'éviter une fragmentation de la mise en œuvre de la protection des données à caractère personnel dans l'Union, une insécurité juridique et le sentiment, largement répandu dans le public, que des risques importants subsistent, notamment dans l'environnement en ligne. C'est pourquoi il est temps de doter l'Union d'un cadre juridique plus solide et plus cohérent en matière de protection des données, assorti d'une application rigoureuse des règles, afin de permettre à l'économie numérique de se*

[6] Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des Régions : "*Une approche globale de la protection des données à caractère personnel dans l'Union européenne*" COM(2010) 609 final.

développer sur tout le marché intérieur et aux personnes physiques de maîtriser l'utilisation qui est faite des données les concernant, et de renforcer la sécurité juridique et pratique pour les opérateurs économiques et les pouvoirs publics"[7].

B. Prises de position antérieures de la CPVP

a) Contribution de la CPVP à la consultation publique de la CE (novembre 2010-janvier 2011)

7. Dans un courrier du 14 janvier 2011 – qui constitue une contribution à la consultation publique suivant la communication précitée du 4 novembre 2010 –, la CPVP soumet 9 observations à la Commission européenne. La première tient au choix de la norme : directive ou règlement. La CPVP y rappelle le nécessaire respect des principes de subsidiarité et de proportionnalité[8] dans ce choix. Partant, elle isole les traitements de données "multinationaux ou transnationaux" - soit des traitements de données intervenant de manière similaire au-delà des frontières d'un État membre ou opérés par un seul et unique responsable de traitement (multinationale) dans différents États de l'Union - pour lesquels une réglementation européenne harmonisée au plus haut niveau lui semble adéquate.

8. Pour ces mêmes seuls traitements, la CPVP se déclare favorable à la création d'une autorité européenne de protection des données. Cette autorité traiterait, à l'échelon européen, des questions à dimension trans/inter-nationale[9] sans jamais s'immiscer dans l'organisation interne des pouvoirs publics d'un État membre. Pour ces entreprises européennes multinationales, la CPVP plaidait également pour un système de déclaration européenne unique. Cette considération n'a plus lieu d'être dès lors que le projet de Règlement supprime toute déclaration préalable de traitement auprès de l'autorité de protection des données.

9. Toujours aux termes de ce courrier du 14 janvier 2011, la CPVP indique à la Commission européenne que le nouveau cadre légal devrait promouvoir (1) la fonction de délégué à la protection

---

[7] COM(2012) 11 final.

[8] Explication minimale des principes : c'est le principe de subsidiarité qui autorise la mise en œuvre d'une compétence attribuée à l'Union : il conditionne le déclenchement de la compétence. Voir les articles 5.1., 5.2., 5.3. et 5.4. du Traité sur l'Union européenne (TUE) : "*1. Le principe d'attribution régit la délimitation des compétences de l'Union. Les principes de subsidiarité et de proportionnalité régissent l'exercice de ces compétences.*
2. En vertu du principe d'attribution, l'Union n'agit que dans les limites des compétences que les États membres lui ont attribuées dans les traités pour atteindre les objectifs que ces traités établissent. Toute compétence non attribuée à l'Union dans les traités appartient aux États membres.
3. En vertu du principe de subsidiarité, dans les domaines qui ne relèvent pas de sa compétence exclusive, l'Union intervient seulement si, et dans la mesure où, les objectifs de l'action envisagée ne peuvent pas être atteints de manière suffisante par les États membres, tant au niveau central qu'au niveau régional et local, mais peuvent l'être mieux, en raison des dimensions ou des effets de l'action envisagée, au niveau de l'Union. (…).
4. En vertu du principe de proportionnalité, le contenu et la forme de l'action de l'Union n'excèdent pas ce qui est nécessaire pour atteindre les objectifs des traités. (…)."

[9] Swift, Google, Facebook, …

des données ainsi que, (2) dans le contexte des flux transfrontières de données toujours plus nombreux, le mécanisme des règles d'entreprise contraignantes (Binding Corporate Rules - BCR) et celui de la reconnaissance mutuelle telle qu'organisée par un certain nombre d'autorités de protection des données de l'Union[10].

10. Quant aux données génétiques, la CPVP insiste sur leur extrême sensibilité. À ses yeux, leur traitement devrait être limité aux fins de soins de santé et de recherche scientifique ou de médecine légale. Tout traitement dans un contexte contractuel, politique, social ou commercial devrait être exclu.

11. La CPVP se déclare favorable à l'introduction d'une obligation d'analyse d'impact sur la vie privée étant entendu que toutes mesures de protection efficaces et proportionnées doivent être déterminées en fonction des risques induits par les traitements et permettre une maîtrise raisonnable des risques sans toutefois aller jusqu'à entraver un service efficace et effectif aux citoyens et aux entreprises, ni le bon fonctionnement de ces dernières et des services publics par exemple.

12. Forte des connaissances acquises lors de l'organisation de sa conférence "Privacy and research : from obstruction to construction", la CPVP adresse également à la Commission européenne quelques recommandations tirées de ses conclusions et destinées à rencontrer tant la nécessaire protection des données des sujets de recherche que les intérêts légitimes des chercheurs. Des précisions sur l'application de la réglementation aux personnes décédées et des précisions quant aux conditions dans lesquelles des recherches peuvent être menées en Europe et quant à l'invocation possible d'autres bases de légitimité que le consentement sont, entre autres suggestions, communiquées à la Commission européenne.

b) Audition de la présidence de la CPVP par la Commission "Justice" de la Chambre des représentants

13. Un an plus tard, début mars 2012, la présidence de la CPVP attire l'attention de la Commission "Justice" de la Chambre des représentants sur le choix opéré par la Commission européenne de réglementer l'ensemble des traitements de données par voie de Règlement (à l'exception des traitements "police et justice" couverts par la proposition de Directive).

[10] La reconnaissance mutuelle est un accord qui a été mis en place par plusieurs autorités afin d'accélérer la procédure européenne de coopération pour les BCR. Selon cet accord, une fois que l'autorité chef de file (lead authority) considère que le BCR rencontre les exigences établies dans les documents de travail du Groupe de l'Article 29 et que son analyse a été revue par deux autorités, les autres autorités ayant adhéré au principe de la reconnaissance mutuelle acceptent que cette analyse constitue une base suffisante pour émettre leur propre autorisation ou approbation nationale du BCR, ou pour donner un avis positif à l'organisme en charge d'émettre l'autorisation.

14. De manière générale, la CPVP alerte le législateur belge sur les modifications importantes qu'induirait le projet de Règlement une fois adopté. La CPVP s'inquiète tout particulièrement du sort qui sera réservé aux comités sectoriels existants (Comité sectoriel de la Sécurité Sociale et de la Santé (CSSS & S), Comité sectoriel pour l'Autorité Fédérale (CSAF), Comité de Surveillance statistique (CS Stat) et Comité sectoriel du Registre national (CSRN) par exemple) au regard de leur compétence d'autorisation préalable. Le projet de Règlement limite en effet les cas dans lesquels une autorisation préalable doit être demandée à l'autorité de protection des données (article 34). Le mécanisme des autorisations telles que délivrées par les comités sectoriels précités ne semble pas être couvert par les dispositions en projet. Dans le même sens, la CPVP s'interroge sur l'utilisation future (admise ou pas ?) du numéro de Registre national.

15. À l'appui de ces considérations, la CPVP invite la Chambre des représentants à exercer le contrôle politique *a priori* que lui confère, depuis le Traité de Lisbonne, l'article 6 du Protocole n° 2 *sur l'application des principes de subsidiarité et de proportionnalité* annexé au Traité[11].

16. Le 20 mars 2012, le président, le vice-président et le commissaire B. De Schutter ont été auditionnés par la Commission "Justice" de la Chambre des représentants[12].

17. Aux termes de son avis de subsidiarité, la Commission "Justice" de la Chambre des représentants adopte le point de vue suivant :

Quant à la subsidiarité

- La dimension transfrontalière de la protection des données à caractère personnel, combinée à l'internationalisation croissante et à la problématique de l'Internet désormais omniprésent, est de nature à justifier une intervention au niveau européen ;
- Les États membres de l'Union devraient toutefois avoir la possibilité de transposer comme ils l'entendent la réglementation européenne dans leur ordre juridique ;
- Le choix d'un Règlement se heurte à des objections en matière de subsidiarité, car en optant pour un Règlement directement applicable sans transposition dans l'ordre

[11] Article 6 du Protocole n° 2 : "*Tout parlement national ou toute chambre de l'un de ces parlements peut, dans un délai de huit semaines à compter de la date de transmission d'un projet d'acte législatif, dans les langues officielles de l'Union, adresser aux présidents du Parlement européen, du Conseil et de la Commission un avis motivé exposant les raisons pour lesquelles il estime que le projet en cause n'est pas conforme au principe de subsidiarité. (…)*."

[12] Proposition de règlement du Parlement européen et du Conseil *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* COM(2012) 0011 ; Proposition de directive du Parlement européen et du Conseil *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* COM(2012) 0010 ; Avis de subsidiarité, rapport du 6 avril 2012 fait au nom de la Commission de la Justice par R. Landuyt, Chambre des représentants, Doc. Parl. DOC 53 2145/001, pp. 13-16.

juridique interne, la Commission européenne ignore la pratique et les caractéristiques propres à l'organisation de la protection des données en Belgique ;

- Le choix d'une Directive s'impose ; un Règlement ne peut être utilisé que pour certains thèmes spécifiques dont les États s'accordent à considérer qu'ils doivent être réglés par voie de Règlement (échange de données avec des pays extérieurs à l'Union européenne);
- Le pouvoir dont disposerait la Commission européenne de suspendre des décisions d'autorités de protection des données est considéré comme excessif (dépassement de compétence) ; un renforcement du rôle du Comité européen de la protection des données (*European Data Protection Board* – EDPB) est préférable ;
- L'article 62 proposé par le projet de Règlement doterait la Commission européenne de compétences étendues en ce qui concerne la législation d'exécution. La réglementation elle-même devrait être la plus complète possible afin d'assurer la participation de tous les acteurs, du Parlement européen et du Conseil.

Quant à la proportionnalité

- Le projet de Règlement influencerait ou modifierait globalement les traitements, existants aujourd'hui, de données à caractère personnel du secteur public (mécanisme de contrôle des comités sectoriels) ;
- Les autorisations préalables à la mise en œuvre de certains traitements délivrées par les comités sectoriels ne seraient plus admises si le Règlement tel que proposé devait entrer en vigueur ;
- Les États membres doivent pouvoir prévoir dans la loi quels sont les traitements qui requièrent des autorisations préalables ;
- La question se pose de savoir si l'utilisation d'un identifiant unique comme le numéro de Registre national n'est pas susceptible de poser problème : les États membres doivent pouvoir déterminer par une loi nationale les conditions dans lesquelles un numéro national d'identification ou tout autre identifiant de portée générale peut faire l'objet d'un traitement ;
- Le Règlement devrait s'appliquer également aux instances européennes elles-mêmes.

II. ANALYSE PAR ARTICLE DU PROJET DE RÈGLEMENT

1. Champ d'application territorial (article 3)

18. En application de l'article 3.1., le projet de Règlement s'applique lorsque le traitement de données à caractère personnel est effectué dans le cadre des activités d'un établissement d'un responsable de traitement ou d'un sous-traitant sur le territoire de l'Union. Dans l'hypothèse où un responsable du traitement établi en dehors de l'UE a recours à un sous-traitant établi dans l'UE, la CPVP estime qu'il faudrait clarifier si seul le sous-traitant est soumis à l'application du projet de Règlement ou si, au contraire, le responsable du traitement est également soumis à l'ensemble des obligations du projet de Règlement.

19. L'article 3.2. vise l'application du projet de Règlement dans les cas où le responsable du traitement n'est pas établi dans l'Union. Le fait que le traitement soit lié à une offre de biens ou de services à des personnes concernées ayant leur résidence dans l'Union (ou à l'observation de leur comportement) constitue dans ce cas le critère du champ d'application territorial du projet de Règlement.

20. Le critère des "moyens" retenu par la Directive 95/46/CE (article 4.1.c)) a pu souvent créer des problèmes d'interprétation et le nouveau critère proposé a pour ambition de contourner ces difficultés tout en protégeant de manière plus ciblée les citoyens européens. Il serait toutefois utile de clarifier la notion d' "offre de biens ou de services" afin de la limiter aux situations où les biens ne sont pas simplement accessibles pour des citoyens européens mais bien où l'offre de biens ou de services leur est clairement adressée, ce qui ressort par exemple de l'utilisation de noms de domaine d'États membres de l'UE, du fait que des possibilités particulières de livraison sont prévues et/ou du fait que l'offre tient compte de la langue/de la culture/des traditions/des usages d'un État membre déterminé, etc. (ce qu'on appelle la "target approach" ou approche ciblée), et ce afin d'éviter que tout site de commerce électronique étranger ne tombe dans le champ d'application du projet de Règlement.

2. Définitions (article 4)

A. Remarque générale

21. La CPVP se demande pourquoi les définitions n'apparaissent qu'à l'article 4 du projet de Règlement. Les articles 1 à 3 inclus utilisent en effet déjà de nombreuses notions qui ne sont

définies qu'à l'article 4. Elle estime dès lors que la construction de l'instrument serait plus logique si le volet relatif aux définitions était repris au premier article.

B. Donnée à caractère personnel et personne concernée

22. La CPVP accueille favorablement l'adaptation des définitions de "données à caractère personnel" et de "personne concernée", et en particulier l'ajout précisant qu'il convient de considérer l'ensemble des moyens susceptibles d'être raisonnablement mis en œuvre, soit par le responsable du traitement, soit par une autre personne, pour identifier la personne concernée. Cette précision figurait au considérant 26 de la Directive 95/46/CE et est à présent insérée au sein même de la définition, ce qui apporte plus de clarté et de sécurité juridique.

C. Données concernant la santé

23. La définition prévue à l'article 4.12. doit être lue à la lumière du considérant 26[13] qui prévoit une interprétation très large de cette notion : il ne s'agit pas uniquement des informations relatives à la santé physique ou mentale mais également toute information relative à la prestation de services de santé (tels que l'enregistrement du patient pour la prestation, les informations relatives aux paiements).

24. La CPVP est d'avis que la définition proposée par le projet de Règlement est (beaucoup) trop large et ne tient pas suffisamment compte des contextes multiples dans lesquels les traitements de telles données peuvent intervenir, ni de la finalité poursuivie par le traitement. Cette définition risque d'avoir des conséquences extrêmes non souhaitées. À titre d'exemple :

a. Des images vidéo de caméras de surveillance montrent qu'une personne a une jambe cassée. Sur la base de la définition dans le projet de Règlement, il s'agit d'une donnée à caractère personnel concernant la santé ;
b. Un service public est habilité à octroyer une réduction fiscale ou un autre avantage social aux personnes souffrant d'un handicap. Le fait que ce service public enregistre dans ses banques

[13] Considérant 26 du projet de Règlement : "*Les données à caractère personnel concernant la santé devraient comprendre, en particulier, l'ensemble des données se rapportant à l'état de santé d'une personne concernée; les informations relatives à l'enregistrement du patient pour la prestation de services de santé; les informations relatives aux paiements ou à l'éligibilité du patient à des soins de santé; un numéro ou un symbole attribué à un patient, ou des informations détaillées le concernant, destinés à l'identifier de manière univoque à des fins médicales; toute information relative au patient recueillie dans le cadre de la prestation de services de santé audit patient; des informations obtenues lors d'un contrôle ou de l'examen d'un organe ou d'une substance corporelle, y compris des échantillons biologiques; l'identification d'une personne en tant que prestataire de soins de santé au patient; ou toute information concernant, par exemple, une maladie, un handicap, un risque de maladie, un dossier médical, un traitement clinique ou l'état physiologique ou biomédical de la personne concernée, indépendamment de sa source, qu'elle provienne par exemple d'un médecin ou d'un autre professionnel de la santé, d'un hôpital, d'un dispositif médical ou d'une épreuve diagnostique in vitro*.".

de données qu'une personne fait partie de cette catégorie (sans spécifier de quel handicap il s'agit précisément) suffit à affirmer que ce service traite des données à caractère personnel concernant la santé au sens du projet de Règlement.

25. Enfin, alors que l'article 4.12. (définitions) retient la terminologie de "données concernant la santé", on retrouve également régulièrement dans le projet de texte les termes "données relatives à la santé". Une terminologie/traduction uniforme devrait être proposée.

D. Établissement principal

26. Pour les cas où le traitement de données a lieu dans le cadre des activités d'un responsable de traitement ou d'un sous-traitant établi dans plusieurs États membres, le projet de Règlement prévoit que l'autorité compétente sera uniquement celle du lieu où se situe l'établissement principal du responsable du traitement (voir infra).

27. Le projet de Règlement prévoit également un critère d'établissement principal pour les sous-traitants et il s'agit ici du lieu de l'administration centrale dans l'Union (article 4.13. *in fine*).

28. La CPVP a quelques réserves sur ce point dès lors qu'il n'y a aucune certitude qu'une administration centrale, par exemple la maison mère ou "headquarter" d'un groupe d'entreprises agissant en tant que sous-traitant, soit concrètement impliquée dans le traitement de données ou dans le contrat qui lie l'entreprise sous-traitante au responsable du traitement. L'autorité désignée compétente devrait être, pour les sous-traitants, au plus près des informations disponibles (lieu du traitement ou des décisions techniques ou organisationnelles relatives au traitement) et de la responsabilité juridique (personne liée juridiquement au contrat de sous-traitance) comme c'est le cas dans le projet de Règlement pour les responsables de traitement. Dans l'hypothèse où l'administration centrale (ou siège principal) n'a aucunement connaissance du contrat de sous-traitance et n'est en rien impliquée dans l'exécution de ce contrat, l'autorité compétente devrait en effet quand même faire appel à ses collègues pour obtenir des informations à ce sujet.

E. Règles d'entreprise contraignantes

29. La CPVP apprécie la reconnaissance explicite des règles d'entreprise contraignantes. Il faudrait toutefois veiller à ce que cette solution puisse également être offerte à des sociétés qui ne sont pas établies au sein de l'Union européenne mais qui ont malgré tout une obligation en vertu du

projet de Règlement de prévoir une protection adéquate dans le cadre de transferts de données depuis l'Union européenne (voir l'article 4.17.)[14].

F. L'enfant

30. Le considérant 29 du projet de Règlement précise que "*Afin de déterminer jusqu'à quel âge une personne est un enfant, le règlement devrait reprendre la définition retenue par la convention des Nations unies relative aux droits de l'enfant*". La plupart des États de l'Union européenne ayant ratifié la Convention des droits de l'enfant[15], le choix de cette définition de référence apparaît "démocratiquement" pertinent. Aux termes de l'article 4.18. du projet de Règlement, l'enfant est défini comme "*toute personne âgée de moins de dix-huit ans*". Le texte complet de la convention onusienne précise toutefois "*sauf si la majorité est atteinte plus tôt, en vertu de la législation qui lui est applicable*". Partant, une meilleure cohérence devrait être assurée entre le considérant 29 et la définition de l'enfant retenue à l'article 4.18.

31. Une définition basée sur l'âge a certes l'avantage de la sécurité juridique. La CPVP est cependant d'avis que la fixation arbitraire d'un âge (de majorité) en matière de protection des données à caractère personnel s'accommode mal avec la réalité des pratiques, internautes notamment, des (parfois très) jeunes. À l'instar de ce qui est prévu dans la *Recommandation R(2002)9 du Conseil de l'Europe sur la protection des données à caractère personnel collectées et traitées à des fins d'assurance*, la CPVP recommande d'informer l'enfant, de le consulter et de tenir compte de ses souhaits à partir d'un certain âge, soit de l'associer progressivement, en fonction de sa capacité de discernement, aux décisions à prendre par exemple quant à l'exercice de ses droits. Cette approche traduit l'attachement de la CPVP à mener le jeune à adopter un comportement informé, responsable et respectueux de soi et d'autrui dans l'utilisation des technologies de l'information et de la communication[16].

3. Principes relatifs au traitement des données à caractère personnel (article 5)

32. Bien que la CPVP soutienne entièrement le principe selon lequel les données doivent être adéquates et non excessives au regard de la finalité poursuivie (le principe de proportionnalité existant), elle estime que le principe de minimisation dans sa formulation (prévue) à l'article 5 c) va trop loin. Ce principe implique en effet que les données doivent être limitées au minimum nécessaire

[14] Par exemple, les clauses contractuelles types 2010/87/CE offrent une solution juridique pour les transferts de données vers des sociétés établies dans des pays tiers et agissant en tant que sous-traitant. Il conviendrait d'éviter que les règles d'entreprise contraignantes pour sous-traitants ne puissent être offertes qu'aux sociétés établies au sein de l'Union alors que la possibilité d'utiliser les clauses contractuelles types leur est offerte.

[15] La Belgique a ratifié la Convention internationale des Droits de l'Enfant en 1991.

[16] Voir en ce sens l'avis 2/2009 du 11 février 2009 du Groupe 29 *sur la protection des données à caractère personnel de l'enfant (Principes généraux et cas particulier des écoles)*.

et qu'il faut vérifier si les finalités ne peuvent être atteintes sans traitement de données à caractère personnel. Un tel principe est trop restrictif aux yeux de la CPVP car il pourrait, dans certains cas, empêcher la réalisation de la finalité du traitement en interdisant des traitements de données qui, bien que n'apparaissant pas strictement nécessaires au départ, s'avèrent finalement *a posteriori* indispensables au traitement (par exemple, en matière de recherche scientifique).

4. Licéité du traitement (article 6)

33. La CPVP attire tout d'abord l'attention sur le fait que le terme "licéité" dans ce contexte peut semer la confusion. On pourrait en effet en déduire que des traitements de données à caractère personnel qui peuvent se baser sur un des fondements repris à l'article 6.1. sont automatiquement conformes, en tous points, au projet de Règlement, alors que ce n'est évidemment pas le cas. Dès lors, la CPVP plaide pour que le terme "admissibilité" soit utilisé. Cette dernière notion a en effet une portée plus limitée que "licéité" et traduit donc mieux le fait que l'article 6 ne constitue qu'une première étape dans l'évaluation visant à savoir si un traitement de données à caractère personnel répond aux obligations définies dans le projet de Règlement.

34. En outre, la CPVP émet des réserves concernant l'article 6.1. f) du projet de Règlement qui interdit aux autorités publiques de rendre légitimes leurs traitements lorsqu'elles agissent sur la base de leur intérêt légitime prévalant sur les droits et intérêts des personnes concernées. Elle estime que cette base d'admissibilité du traitement ne peut pas être supprimée. En effet, on peut imaginer que des situations se produisent où une autorité publique n'a pas d'autre choix que de fonder certains traitements sur son intérêt légitime (par exemple dans le cadre de sa gestion du personnel).

35. De manière plus générale, la Commission a d'ailleurs également rédigé une note dans laquelle elle a réuni des éléments de réponse concernant la question de savoir si un cadre légal réglementaire distinct est nécessaire pour le secteur public et le secteur privé. Cette note est jointe en annexe du présent avis.

36. Enfin, la CPVP formule plusieurs remarques concernant l'article 6.4. du projet de Règlement, qui stipule ce qui suit : "*Lorsque la finalité du traitement ultérieur n'est pas compatible avec celle pour laquelle les données à caractère personnel ont été collectées, le traitement doit trouver sa base juridique au moins dans l'un des motifs mentionnés au paragraphe 1, points a) à e). (…).*". Soit le traitement est compatible, soit il ne l'est pas et dans ce cas, s'agissant d'un nouveau traitement, il doit satisfaire à l'ensemble des conditions légales et doit également trouver une base de légitimité. Toutes les hypothèses prévues à l'article 6 a) à f) devraient, dans ce cas, pouvoir s'appliquer et la CPVP ne comprend dès lors pas pourquoi le projet de Règlement ne mentionne que les hypothèses visées aux points a) à e). La CPVP estime également que le point b) de l'article 5 du projet de

Règlement devrait reprendre un renvoi clair à l'article 6.4. Ces deux dispositions sont en effet étroitement liées.

5. Consentement de la personne concernée (article 7)

37. Lorsque le responsable du traitement justifie son traitement sur la base du consentement, le projet de Règlement prévoit que celui-ci doit être explicite (article 4.8.) et que la charge de la preuve du consentement incombe clairement au responsable du traitement (article 7.1.). Le considérant 25 précise que le consentement peut être donné selon toute modalité appropriée, soit sous la forme d'une déclaration, soit par un acte non équivoque de la personne concernée ou une indication claire qui révèle que dans le contexte donné, elle accepte le traitement de données à caractère personnel proposé. Ces adaptations ont pour objectif de renforcer les droits des personnes concernées et de responsabiliser les responsables de traitement quant à la conservation des éléments de preuve.

38. Désormais, le projet de Règlement prévoit également que le consentement donné pourra être retiré à tout moment, sans justification ou motif. Cette disposition est présentée comme un renforcement des droits de la personne concernée et de la maîtrise qu'elle doit pouvoir exercer sur l'utilisation de ses données. La CPVP attire toutefois l'attention sur le fait que la possibilité d'un retrait unilatéral et non justifié d'un consentement légalement consacré qui touche aux intérêts de tiers peut hypothéquer les activités des responsables de traitement et que cette règle risque de remettre en cause l'équilibre consacré par la Directive 95/46/CE entre les droits de la personne concernée et les intérêts des responsables de traitement. Cette possibilité de retrait unilatéral doit par ailleurs s'apprécier au regard du droit d'opposition au traitement et aux conditions d'exercice de ce droit (voir infra).

39. La CPVP estime d'une manière générale qu'il faut éviter une survalorisation du consentement. Le consentement est admis comme base de légitimité mais il convient d'être attentif à sa fragilité et de ne pas vouloir fonder tous les traitements sur le consentement. De nombreuses dispositions du projet de Règlement se fondent sur le consentement comme base de légitimité, comme l'article 8.1. relatif au consentement des mineurs dans le contexte des services de la société d'information (voir supra). Or, dans ce contexte, il est le plus souvent fait usage de contrats d'adhésion à propos desquels on ne peut véritablement parler de consentement.

40. Par ailleurs, le projet de Règlement exclut l'usage du consentement comme fondement juridique valable pour le traitement lorsqu'il existe un déséquilibre significatif entre la personne concernée et le responsable du traitement (article 7.4.). Le considérant 34 précise qu'il s'agit du cas où la personne concernée se trouve dans une situation de dépendance par rapport au responsable du traitement, par exemple lorsque ses données à caractère personnel sont traitées par son

employeur dans le cadre de leur relation de travail. Il y a donc la volonté de formellement reconnaître que le caractère libre du consentement peut poser problème dans le contexte professionnel du fait de l'existence d'un lien de subordination[17].

41. Selon la CPVP, le fait d'exclure, en toute hypothèse, l'usage du consentement dans le contexte professionnel peut toutefois créer une plus grande insécurité juridique pour le responsable du traitement, et ce pour les traitements qui ne sont pas strictement nécessaires à l'exécution du contrat de travail. Pour que les traitements de données soient admissibles dans ces cas, le responsable du traitement doit effectuer lui-même *a priori* la mise en balance des intérêts (article 6.1. f) du projet de Règlement), avec le risque d'être *a posteriori* rappelé à l'ordre par le juge.

42. Aux yeux de la CPVP, le consentement d'un travailleur devrait dès lors quand même pouvoir constituer dans certains cas un fondement admissible. À cet effet, on peut s'inspirer du cadre réglementaire national existant. L'article 27 de l'arrêté royal du 13 février 2001, pris en exécution de la LVP, prévoit notamment l'interdiction pour l'employeur de baser le traitement de données **sensibles** exclusivement sur le consentement, **sauf dans l'hypothèse où le traitement vise l'octroi d'un avantage à la personne concernée**. La CPVP plaide pour que cette exception soit reprise dans le projet de Règlement.

6. Traitement de données à caractère personnel relatives aux enfants (article 8)

43. Le projet de Règlement introduit le principe d'une protection spécifique pour les mineurs (enfants) "*parce que ceux-ci peuvent être moins conscients des risques, des conséquences, des garanties et de leurs droits en matière de traitement des données*" (considérant 29).

44. La CPVP est favorable à cette initiative qui est d'ailleurs particulièrement indiquée dans le contexte des activités en ligne, des réseaux sociaux et des activités de marketing spécialement dirigées vers les jeunes. La CPVP rappelle l'initiative qu'elle a prise à cet égard avec son site Internet spécialement conçu pour les mineurs (jeunes et adolescents), et leurs parents et professeurs[18], anticipant ainsi l'invitation du projet de Règlement à mener des actions de sensibilisation pour cette catégorie de personnes concernées (article 52).

45. Quant aux garanties mises en place par le projet de Règlement, la CPVP accueille favorablement la précision apportée à l'article 6 f). Cette disposition prescrit que le fait qu'une

---

[17] Voir également à ce sujet la recommandation n° 01/2002 de la CPVP et les documents de travail WP48 et WP168 (point 66) du Groupe de l'Article 29.

[18] Site Internet "Je décide" : http://www.jedecide.be/.

personne soit mineure doit être pris en considération au moment d'évaluer l'éventuelle prévalence des intérêts, libertés ou droits fondamentaux de la personne concernée sur l'intérêt légitime du responsable du traitement. Dans le même sens, elle partage la volonté de la Commission européenne de soumettre les larges banques de données relatives aux mineurs à une analyse d'impact préalable relative à la protection des données (article 33), d'encourager les actions de sensibilisation par les autorités de protection des données (article 52), d'établir des codes de conduite spécifiques (article 38) et d'inviter les responsables de traitement à s'efforcer d'obtenir un consentement vérifiable lors de l'offre de services de la société de l'information (article 8).

46. Aux fins du présent règlement, s'agissant de l'offre directe de services de la société de l'information aux enfants, l'article 8 stipule que "*le traitement de données à caractère personnel relatives à un enfant de moins de 13 ans n'est licite que si et dans la mesure où le consentement est donné ou autorisé par un parent de l'enfant ou par une personne qui en a la garde*" (article 8.1.). L'article 8.2. stipule également ce qui suit : "*Le paragraphe 1 n'affecte pas la législation générale des États membres en matière contractuelle, telle que les dispositions régissant la validité, la formation ou les effets d'un contrat à l'égard d'un enfant*".

47. La CPVP comprend cette disposition comme une invitation à distinguer la légitimité (fondée sur le consentement) du traitement de données du mineur âgé de moins de 13 ans de la légalité de son engagement contractuel au regard du droit (civil) national. Une confirmation de cette lecture et une illustration, explicitant ce qu'il convient d'entendre par "offre directe de services de la société de l'information", seraient les bienvenues dans les considérants.

48. En outre, la CPVP se demande comment les exigences strictes requises pour qu'un consentement soit valable aux termes de l'article 7 du projet de Règlement peuvent être conciliées avec le consentement d'un mineur de plus de 13 ans.

49. La CPVP rappelle enfin qu'indépendamment de tout régime spécifique de protection, la situation particulière dans laquelle se trouvent les enfants peut et doit être prise en compte dans l'application des dispositions du projet de Règlement (exemple : l'information doit être compréhensible, ce qui implique que le responsable du traitement adapte son langage lorsqu'il s'adresse spécifiquement à des enfants). Il en est de même pour d'autres catégories de personnes. La CPVP pense ainsi aux personnes peu familiarisées avec l'outil informatique et les technologies de l'information et de la communication (personnes âgées, fracture numérique)[19].

[19] De manière générale, si la réglementation en matière de "protection des données" s'est progressivement complexifiée et si les *traitements* et les *données* sont aujourd'hui au centre de toutes les attentions (économiques et juridiques), il convient en effet de ne pas perdre de vue que l'objectif de la réglementation de ce droit fondamental est avant tout la protection de la *personne* (à l'égard du traitement de ses données).

50. À cet égard, la CPVP fait également remarquer que le projet de Règlement pourrait prévoir une disposition générale relative à la représentation des incapables. Cette disposition pourrait mettre l'accent sur le fait que lorsque ces représentants donnent leur consentement, ils ne doivent pas perdre de vue qu'ils donnent leur consentement pour un tiers et pas pour eux-mêmes et que la protection de la personne qu'ils représentent doit constituer leur fil conducteur dans cette décision.

7. Traitements portant sur des catégories particulières de données à caractère personnel (article 9)

51. L'article 9.1. qui définit les catégories particulières de données à caractère personnel (données sensibles) mentionne également les données génétiques. Ce n'était pas le cas de l'article 8.1. de la Directive 95/46/CE. La CPVP accueille favorablement cet ajout.

52. La CPVP a plus de réticences quant à la modification de la définition des données judiciaires prévue à l'article 8.5. de la Directive 95/46/CE et en particulier à la suppression du terme "infractions" ("offences" en anglais). Cette dernière notion permettait néanmoins de qualifier également de données judiciaires des infractions administratives ou des condamnations civiles (voir l'article 8, § 1 de la LVP).

53. En outre, la CPVP constate que le nombre de cas où le traitement de données judiciaires est jugé admissible a considérablement été étendu en comparaison avec ce qui est prévu à l'article 8.5. de la Directive 95/46/CE. Ainsi, en vertu de l'article 9.2. points a) et e) du projet de Règlement, le consentement de la personne concernée ou la publication des données par la personne concernée constituent des fondements d'exception à l'interdiction de traitement, alors que ces fondements ne sont pas prévus dans la Directive. La CPVP se demande quelle est la motivation d'un tel assouplissement.

54. En ce qui concerne le traitement de données relatives à la santé, le point de vue de la CPVP est exposé ci-dessus.

8. Traitement ne permettant pas l'identification (article 10)

55. L'article 10 du projet de Règlement prévoit que lorsque les données traitées ne permettent pas d'identifier une personne physique, le responsable du traitement n'est pas tenu d'obtenir des informations supplémentaires pour identifier la personne concernée afin de respecter ainsi les dispositions du présent règlement. La CPVP estime qu'il convient de clarifier les intentions poursuivies par cette disposition et, en toute hypothèse, d'éviter de déduire de celle-ci que le responsable du traitement n'est plus tenu à aucune obligation.

9. Transparence (articles 11 et 14)

56. La CPVP salue l'obligation générale de disposer de privacy policies qui soient transparentes, facilement accessibles, plus complètes et elle apprécie le fait que toute information ou communication du responsable du traitement utilise un langage clair et adapté à la personne concernée (article 11).

57. Le projet de Règlement prévoit en outre un contenu plus large des informations à communiquer par le responsable du traitement (les articles 14.1. à 14.3. du projet comparés aux articles 10 et 11 de la Directive 95/46/CE).

58. La CPVP apprécie l'information additionnelle relative à l'origine des données (article 14.3.) qui permettrait d'octroyer *de facto* davantage de contrôle aux personnes concernées sur leurs propres données.

59. Pour ce qui concerne les informations relatives aux droits des personnes concernées (article 14.1., point d)), la CPVP estime qu'il faudrait également mentionner les nouveaux droits créés au sein du projet de Règlement (droit à l'oubli, droit à la portabilité, mesures de profilage). Les informations relatives aux flux internationaux (article 14.1., point g)) devraient également inclure les garanties appropriées qui ont été mises en œuvre par le responsable du traitement dès lors que fréquemment, ces garanties mettent en place des droits pour les personnes concernées.

60. La CPVP fait également remarquer que le projet de Règlement (article 14, point 1, c)) définit le principe selon lequel, lors de l'information à la personne concernée, il faut également mentionner d'emblée le délai de conservation envisagé des données traitées. La CPVP partage l'idée que ce principe conférerait un niveau supérieur de transparence au traitement de données à caractère personnel dans les cas où le responsable du traitement a au préalable une idée claire de la durée de conservation (par ex. parce que celle-ci est ancrée dans la réglementation), mais parallèlement, elle attire l'attention sur le fait que pour le responsable du traitement, il est souvent impossible dans la pratique de définir au préalable un délai de conservation exact. De très nombreuses délibérations du Comité sectoriel pour l'Autorité Fédérale l'illustrent.
La CPVP craint dès lors que cette nouvelle règle ne conduise dans la pratique à ce que le responsable du traitement fasse tout au plus une estimation approximative du délai de conservation au moment de l'information de la personne concernée. Le responsable sollicitera même peut-être "par sécurité" un délai plus long que ce qui est strictement nécessaire.

61. Enfin, la CPVP attire l'attention sur le fait que – en vertu de l'article 14.5. point c) du projet de Règlement – l'obligation d'information ne s'applique pas *lorsque (les données ne sont pas collectées auprès de la personne concernée et que) l'enregistrement ou la communication des données sont expressément prévus par la législation*.

62. La CPVP estime que cette disposition semble d'une part impliquer un durcissement par rapport à la Directive 95/46/CE car le terme "expressément" a été ajouté (à comparer avec l'article 11.2. *in fine* de la Directive 95/46/CE). D'autre part, cette disposition semble également viser un assouplissement, étant donné que l'obligation pour les États membres – reprise à l'article 11.2. *in fine* de la Directive 95/46/CE – de prévoir *des garanties appropriées* dans les cas où la présente exception à l'obligation d'information peut être invoquée n'est pas réitérée dans le projet de Règlement.

63. La CPVP se demande dès lors si, lors de la rédaction de l'article 14.5., point c) du projet de Règlement, la Commission européenne avait l'intention d'apporter une modification par rapport à la situation actuelle. En d'autres termes, envisageait-elle un renforcement, un assouplissement ou un *statu quo* ?

64. Quoi qu'il en soit, la CPVP estime qu'un renforcement de cette exception à l'obligation d'information pourrait impliquer que de nombreux flux de données dans le secteur public belge seront soumis à l'obligation d'information, alors que jusqu'à présent, l'exception pouvait souvent être invoquée dès qu'un fondement au traitement pouvait être trouvé dans la réglementation. Le projet de Règlement pourrait ainsi avoir d'importantes implications pratiques pour les traitements de données dans le secteur public. Un exercice de grande envergure risque notamment de s'imposer afin de vérifier si le cadre réglementaire de chaque domaine suffit à justifier l'exception à l'obligation d'information ou si des interventions législatives sont requises, ou si l'obligation d'information doit le cas échéant quand même être remplie.

65. La CPVP émet de sérieux doutes quant à l'opportunité d'un tel exercice et elle plaide dès lors pour que l'on opte clairement, à l'article 14.5., point c) du projet de Règlement, pour le maintien de la situation existante telle que prévue à l'article 11.2., *in fine* de la Directive 95/46/CE.

10. Procédure et mécanismes prévus pour l'exercice des droits de la personne concernée (article 12)

66. La CPVP apprécie l'obligation du responsable d'un traitement automatisé de fournir à la personne concernée les moyens d'exercer ses droits et demandes par voie électronique

(article 12.1.), l'introduction d'un délai de réponse (article 12.2.) et le principe de gratuité (hormis en cas d'abus) (article 12.4.).

11. Droit d'accès (articles 15 et 20)

67. La CPVP estime que le droit d'accès (article 15) devrait également s'appliquer aux garanties appropriées mises en place dans le cadre des flux internationaux de données. Les garanties existantes, telles que les règles d'entreprise contraignantes et les clauses-types de la Commission européenne, comportent souvent en leur sein une possibilité d'accès à leur contenu par les personnes concernées. En effet, ces garanties prévoient souvent des droits pour les personnes concernées (en tant que tiers bénéficiaires).

68. Dès lors que le projet de Règlement instaure la possibilité pour les sous-traitants d'offrir eux-mêmes des garanties appropriées (article 42) et que ceux-ci ne sont pas nécessairement en contact avec les personnes concernées, une plus grande transparence et une possibilité d'accès par les personnes concernées aux garanties appropriées apportées par les sous-traitants devraient, selon la CPVP, également être insérées au sein même du projet de Règlement[20].

69. Par ailleurs, la Directive 95/46/CE prévoit en son article 12 l'obligation de communiquer à la personne concernée la logique qui sous-tend tout traitement automatisé de ses données, au minimum dans le cas des décisions automatisées visées à l'article 15, paragraphe 1. Les "mesures automatisées" pour lesquelles des règles spécifiques ont été définies à l'article 15 de la Directive 95/46/CE ont été combinées avec des "mesures de profilage" à l'article 20 du projet de Règlement. La CPVP estime toutefois qu'on peut également concevoir des traitements automatisés qui ne sont pas effectués dans le contexte du profilage (voir infra). Elle déplore que le projet de Règlement ne définisse pour ces cas aucune règle spécifique qui oblige le responsable du traitement à informer les personnes concernées concernant la logique qui sous-tend le traitement automatisé de leurs données.

12. Droit de rectification (article 16)

70. La CPVP estime que lorsque les données sont objectivement inexactes, elles devraient être simplement rectifiées. Par contre, la possibilité d'ajouter une déclaration rectificative prévue à l'article 16 ne pourrait s'appliquer que lorsque les données concernent des informations subjectives (par exemple, une appréciation) et que la personne concernée estime qu'elles sont inexactes alors

[20] Ce qui garantirait que le responsable du traitement soit tenu à la mise à disposition des garanties appropriées offertes par ses sous-traitants.

que le responsable du traitement n'est pas d'accord (cela permet, en pratique, de conserver les deux versions des données).

13. Droit à l'oubli numérique et à l'effacement (article 17)

71. Le droit à l'oubli et le droit à l'effacement (article 17) devraient être clairement distingués car il s'agit de deux concepts différents.

72. En outre, la CPVP constate que l'article 17 prévoit le droit pour la personne concernée d'obtenir l'effacement des données qui ne sont plus nécessaires à la réalisation des finalités pour lesquelles elles ont été collectées ou lorsque le délai de conservation autorisé a expiré et qu'il n'existe pas d'autre motif légal au traitement. Selon la CPVP, la personne concernée ne devrait pas avoir besoin de demander l'effacement dans ces hypothèses car ces données devraient être en tout état de cause effacées automatiquement. Elle estime dès lors que l'absence d'automaticité constitue un certain affaiblissement de la protection par rapport à la situation actuelle.

73. Enfin, la CPVP partage le point de vue selon lequel il convient de veiller tout particulièrement à l'exactitude et à la mise à jour des données de mineurs d'âge et partant, à leur effacement dès que leur conservation n'est plus justifiée. Aucune conséquence juridique n'est cependant attachée à l'incise "*en particulier en ce qui concerne les données à caractère personnel que la personne concernée avait rendues disponibles quand elle était enfant*" (article 17.1.). Cette absence de conséquences juridiques est de nature à semer la confusion et génère une certaine insécurité juridique.

14. Droit à la portabilité des données (article 18)

74. La CPVP accueille favorablement ce principe – qui a pour objectif de renforcer la position des personnes concernées en leur octroyant davantage de contrôle sur leurs données – mais estime qu'une vigilance sera nécessaire lors de l'établissement des mesures d'exécution de ce principe. Toutefois, selon la CPVP, les modalités actuellement prévues dans le projet de Règlement ne sont pas suffisamment élaborées pour pouvoir appliquer cet article dans la pratique.

15. Droit d'opposition (article 19)

75. Avec l'entrée en vigueur du projet de Règlement, le droit d'opposition prévu par la LVP disparaîtra dans les cas où le consentement de la personne concernée constitue la base légale d'un

traitement de données[21]. Cette position est inacceptable car elle impliquerait un affaiblissement des droits des personnes concernées. Le droit d'opposition est essentiel en ce qu'il ne permet plus au responsable du traitement de traiter les données au regard desquelles la personne concernée a exercé son droit d'opposition.

76. Le droit d'opposition offre aujourd'hui des garanties supérieures à la possibilité de retrait du consentement prévue par le projet de Règlement. Celle-ci précise en effet que "*Le retrait du consentement ne compromet pas la licéité du traitement fondé sur le consentement préalablement donné*." (article 7.3. du projet de Règlement). En tout état de cause, il faut considérer que le retrait d'un consentement ne peut avoir d'effet concret que pour l'avenir. Une telle disposition affaiblit considérablement la protection offerte dans l'actuelle réglementation par l'exercice du droit d'opposition.

77. Enfin, lors de la mise en œuvre du droit d'opposition, le projet de Règlement donne au responsable du traitement la faculté d'établir l'existence de raisons impérieuses et légitimes justifiant le traitement, qui priment les intérêts ou libertés et droits fondamentaux de la personne concernée (article 19.1.). À première vue, il s'agit de renforcer les droits des personnes concernées qui n'auront plus besoin de prouver des raisons prépondérantes et légitimes tenant à leur situation particulière (voir l'article 14. a) de la Directive 95/46/CE) dans le cadre de l'exercice de leur droit d'opposition. Au lieu de cela, le projet de Règlement entend désormais donner au responsable du traitement la possibilité de refuser l'exercice de ce droit. Selon la CPVP, cette nouvelle règle crée le risque de voir les responsables de traitement continuellement invoquer leur intérêt légitime pour s'opposer au droit d'opposition exercé par la personne concernée[22].

---

[21] En vertu de l'article 14 de la Directive 95/46/CE, les États membres étaient obligés de prévoir, au moins dans un certain nombre de cas (notamment dans les cas visés à l'article 7, points e) et f) et en cas de marketing direct), un droit d'opposition, mais ils étaient en outre également libres d'ancrer ce droit dans d'autres cas (tous les traitements, quelle que soit leur base de légitimité).

Dans la LVP, on avait effectivement choisi d'étendre ce droit à d'autres cas. Concrètement, l'article 12 de ladite loi stipule ce qui suit :

"*(…)*

Toute personne a en outre le droit de s'opposer, pour des raisons sérieuses et légitimes tenant à une situation particulière, à ce que des données la concernant fassent l'objet d'un traitement, sauf lorsque la licéité du traitement est basée sur les motifs visés à l'article 5, b) (traitement nécessaire à l'exécution d'un contrat) *et c)* (traitement nécessaire au respect d'une obligation à laquelle le responsable du traitement est soumis). *(…)*".

En bref, la LVP prévoit deux hypothèses complémentaires au minimum requis par la Directive 95/46/CE, soit lorsque le traitement est légitimé par la sauvegarde de l'intérêt vital de la personne concernée (article 5, d) de la LVP) et lorsque le traitement est légitimé par le consentement de la personne concernée (article 5, a) de la LVP).

Le projet de Règlement stipule pour sa part ce qui suit : (article 19) "*La personne concernée a le droit de s'opposer à tout moment, pour des raisons tenant à sa situation particulière, à ce que des données à caractère personnel fassent l'objet d'un traitement fondé sur l'article 6, paragraphe 1, points d), e) et f), à moins que le responsable du traitement n'établisse l'existence de raisons impérieuses et légitimes justifiant le traitement, qui priment les intérêts ou les libertés et droits fondamentaux de la personne concernée.*"

Le droit d'opposition est ainsi exclus dans le cas de traitements fondés sur le consentement (article 6.1., a) du projet de Règlement), le contrat (6.1., b) et la loi en général (6.1., c) – obligation légale du responsable du traitement.

[22] L'article 19.3. du projet de Règlement n'est pas d'un grand secours en ce qu'il prévoit : "*Lorsqu'il est fait droit à une opposition (…), le responsable du traitement n'utilise ni ne traite plus les données à caractère personnel concernées.*"

78. La CPVP s'inquiète également du fait que l'article 19.3. du projet de Règlement semble à nouveau remettre en question le caractère inconditionnel du droit d'opposition en matière de marketing direct, prévu à l'article 12, 3ème alinéa de la LVP ("*sans aucune justification*"), dès lors que cet article stipule : "*Lorsqu'il est fait droit à une opposition conformément aux paragraphes 1 et 2* (marketing direct)*, (…)*."

16. Profilage (article 20)

79. La CPVP estime que les garanties des personnes concernées devraient toujours inclure le droit d'obtenir une intervention humaine (ce qui n'est actuellement prévu dans le projet de Règlement qu'à l'article 20.2.a)). En outre, le droit de faire valoir son point de vue (article 15.2.a) de la Directive 95/46/CE) devrait également toujours s'appliquer. Ces deux garanties devraient donc clairement s'appliquer dans chacune des hypothèses de l'article 20.2. du projet de Règlement (en cas de contrat, d'application d'une loi ou de consentement).

80. Par ailleurs, à la lecture de l'article 20 du projet de Règlement, il n'est pas évident d'établir si le profilage réalisé à des fins de marketing direct, qui se traduit sous la forme de messages publicitaires spécifiques, entre dans le champ d'application de cet article dès lors qu'il n'a pas d'effets juridiques à l'égard de la personne concernée (hormis s'il est accompagné d'une réduction et donc d'une offre de prix) et qu'il ne l'affecte pas nécessairement de manière significative. La CPVP estime toutefois que ce type de profilage devrait être soumis aux conditions particulières de l'article 20.

81. La CPVP regrette en outre que le projet de Règlement se limite à mentionner dans un considérant que le profilage ne devrait pas concerner les enfants (considérant 58). La CPVP plaide pour que l'article 20 même (*mesures fondées sur le profilage*) traduise ce souhait et exclue de pouvoir se fonder sur le consentement d'un enfant dès lors que, dans le contexte du profilage, elle est d'avis que la condition de l'absence d'un déséquilibre entre les intérêts de la personne concernée (l'enfant) et le responsable du traitement n'est jamais satisfaite (article 7.4. du projet de Règlement : *conditions de consentement*).

82. Enfin, l'article 20.3. du projet de Règlement vise à exclure les traitement de données automatisés destinés à évaluer certains aspects personnels propres à une personne physique lorsqu'ils sont exclusivement fondés sur des catégories particulières de données (données sensibles). La CPVP se demande dans quelle mesure cette disposition ne limiterait pas les administrations publiques dans leurs politiques publiques en matière de soins de santé. Une solution à cet égard pourrait, aux yeux de la CPVP, être trouvée dans le cadre de la mise en œuvre de l'article 21 du

projet de Règlement. En outre, la CPVP se demande dans quelle mesure il est possible qu'un tel traitement puisse être exclusivement fondé sur des données sensibles.

17. Responsabilisation du responsable du traitement (article 22)

83. La CPVP apprécie l'ancrage du principe de responsabilisation des responsables de traitement imposant à ceux-ci la mise en place de mesures préventives qui ont pour objectif d'éviter toute atteinte éventuelle à la protection des données. Il vaut mieux en effet s'y prendre en amont, en employant des mécanismes préventifs permettant d'éviter les atteintes, plutôt que d'être lié à des principes et soumis à d'éventuelles sanctions en cas de non-respect. Ce principe est déjà mis en œuvre aujourd'hui au sein des règles d'entreprise contraignantes.

84. Cependant, la CPVP note une certaine incohérence, du fait que le principe vise les seuls responsables de traitement (article 22.1.) alors que les mécanismes listés de mise en œuvre de ce principe de responsabilisation concernent également directement le sous-traitant (article 22.2.).

85. La CPVP estime en outre que les obligations visées à l'article 22.3. devraient être clarifiées. Cet article traite d'une obligation d'audit et il n'est pas évident de savoir si l'élément de "proportionnalité" mentionné dans la dernière phrase de cet article 22.3. s'applique à l'obligation même (l'audit ne serait en d'autres termes obligatoire que dans la mesure où la situation le justifie) ou seulement au fait qu'il sera réalisé par des auditeurs externes ou internes (c.-à-d. : selon la situation, l'obligation impliquera ou pas des auditeurs externes). Les différences entre les traductions du projet de Règlement n'apportent qu'une confusion supplémentaire.

86. La CPVP estime quoi qu'il en soit que le responsable du traitement est le mieux placé pour juger lui-même – tout en tenant compte de la nature des données traitées, des risques, de l'existence éventuelle d'autres mécanismes de protection, etc. – si la réalisation d'un audit externe dans son organisation est une mesure utile ou si un audit interne suffit.

18. Protection des données dès la conception et protection des données par défaut (privacy by design and by default) (article 23)

87. La CPVP soutient l'insertion de ces principes mais souligne le fait que la conception des systèmes de traitement est parfois dans les mains, non pas des responsables de traitement, mais plutôt des concepteurs de produits ou de logiciels.

19. Le représentant (article 25)

88. En cas d'application de l'article 3.2. du projet de Règlement[23], l'article 25 du projet de Règlement prévoit la désignation d'un représentant dans l'Union.

89. Le rôle du représentant devrait être clarifié. Est-t-il uniquement un point de contact au sein de l'Union pour les autorités de protection de données ou a-t-il également un rôle en termes de responsabilité juridique ? L'article 4.14. du projet de Règlement précise qu'il peut être contacté par les autorités de contrôle (dans la version anglaise "may be addressed by **any** supervisory authority"). Ce rôle de point de contact est confirmé par l'article 53.1. c) sur les pouvoirs des autorités de protection des données (en application de cette disposition, elles peuvent lui ordonner de leur communiquer toute information utile), ainsi que par les articles 28.3. et 29. En termes de responsabilité juridique, il est assez surprenant que l'article 78 concernant la possibilité, pour les États membres, de prévoir des sanctions pénales, est également applicable au représentant, alors qu'aucune référence n'est prévue à son égard sous l'article 79 (*sanctions administratives*) ou sous l'article 77 (responsabilité civile). Par ailleurs, en ne stipulant pas clairement le fait que les obligations juridiques du responsable du traitement incombent également au représentant, la mise en place d'une responsabilité pénale directe peut poser problème du fait que l'on ne peut être normalement pénalement responsable pour les fautes d'autrui[24].

90. En outre, le projet de Règlement prévoit plusieurs exceptions à l'obligation de désigner un représentant (article 25.2.) et la CPVP a quelques remarques à ce sujet.

91. Tout d'abord, elle estime que l'utilité de désigner un représentant subsiste, même dans l'hypothèse où le responsable du traitement est établi dans un pays tiers assurant un niveau de protection adéquat (article 25.2. a)). Sur ce point, la CPVP souscrit à l'avis de l'ICO[25] qui stipule qu'un responsable du traitement établi dans un pays tiers assurant un niveau de protection adéquat pourrait enfreindre le Règlement sans toutefois enfreindre la loi de ce pays tiers.

92. Par ailleurs, le projet de Règlement prévoit également une exception pour les entreprises employant moins de 250 employés (article 25.2. b)), alors que le nombre de collaborateurs ne peut pas constituer, aux yeux de la CPVP, un critère pertinent pour évaluer les risques (voir infra).

---

[23] "*Le présent règlement s'applique au traitement des données à caractère personnel appartenant à des personnes concernées ayant leur résidence sur le territoire de l'Union, par un responsable du traitement qui n'est pas établi dans l'Union, lorsque les activités de traitement sont liées :*

a) à l'offre de biens ou de services à ces personnes concernées dans l'Union ; ou

b) à l'observation de leur comportement."

[24] Hormis le cas de la responsabilité pénale pour les personnes morales, mais il s'agit ici d'une spécificité.

[25] Information Commissioner's Office : initial analysis of the European Commission's proposals for a revised data protection legislative framework, 27 février 2012, p. 17.

93. En outre, en ce qui concerne l'exception relative au responsable du traitement n'offrant qu'occasionnellement des biens ou des services à des personnes concernées résidant dans l'Union (article 25.2. d)), le critère "caractère occasionnel de l'offre de biens et de services" peut créer des problèmes d'application (une seule collecte de données sensibles concernant 1.000.000 de personnes pourrait-elle être occasionnelle ?).

94. Enfin, la CPVP plaide pour une suppression complète de toute exception à l'obligation de désigner un représentant en cas de traitement de données sensibles.

20. Documentation (article 28)

95. La CPVP peut adhérer à la suppression de la déclaration obligatoire afin de la remplacer par une documentation interne obligatoire des traitements. Les éléments essentiels des traitements de données à caractère personnel devraient être facilement accessibles pour les personnes concernées et devraient être tenus à la disposition des DPA, par exemple via le délégué à la protection des données ou via un site Internet.

96. La CPVP a pu constater que l'intérêt particulier de la déclaration ne réside pas tant dans la transparence créée (vu que peu de citoyens consultent le registre public) mais bien dans le fait qu'elle oblige chaque responsable à se poser des questions pertinentes concernant la protection des données qui est visée. Il importe dès lors de veiller à ce que cet exercice soit toujours pratiqué lors de la conception et lors du déploiement d'un traitement. La constitution, la mise à jour et la conservation d'une documentation interne permet par conséquent de conserver les avantages de la déclaration (conscientiser à la nécessité de respecter les lois). Les inconvénients de la déclaration obligatoire (bureaucratie inutile, coûts de maintenance d'un registre public peu consulté) peuvent être évités.

97. La CPVP constate que les exceptions prévues à l'obligation de documentation (alinéa 4) sont trop larges étant donné que tout responsable devrait en tout cas toujours conserver une documentation de base reprenant les éléments essentiels du traitement de données : données de contact du responsable du traitement ainsi que de la personne qui peut concrètement être immédiatement contactée par la personne concernée pour l'exercice de ses droits (mais aussi l'identité des sous-traitants, du représentant éventuel, du délégué à la protection des données, une description succincte des traitements (reprenant les finalités, les catégories de données et les destinataires)).

98. Les exceptions susmentionnées ne peuvent pas non plus s'appliquer aux "données à caractère personnel sensibles".

99. En tout cas, il convient de veiller à ce que la DPA puisse être informée rapidement et complètement en cas de demande de documentation et d'informations (à développer de manière uniforme par la Commission comme prévu à juste titre aux alinéas 5 et 6 (après avis des DPA)).

100. Enfin, il faut remarquer que la liste des informations énumérées à l'article 28, alinéa 2 est énorme, et pour certains traitements, il est difficile voire impossible de l'appliquer. La CPVP estime donc qu'il n'est pas possible pour le responsable du traitement de toujours déterminer au préalable la durée de conservation des données qu'il appliquera. L'obligation devra dès lors être écrite, élaborée et maintenue de manière suffisamment souple pour permettre une application concrète au cas par cas. Il faut donc laisser de la marge pour permettre au responsable du traitement ou au sous-traitant de ne pas livrer certaines informations dans la mesure où on peut motiver, sur la base d'un fondement raisonnable, la raison pour laquelle c'est difficile ou impossible. Cela n'exclut pas que des éléments de base devront toujours être documentés. Il importe que le règlement fasse cette distinction.

21. Coopération avec l'autorité de contrôle (article 29)

101. La CPVP apprécie l'ajout de ce principe (article 29) mais la communication obligatoire d'informations ne peut pas être limitée aux hypothèses d'investigation (53.2a) : elle doit être plus large et porter notamment sur l'article 53.1c.

102. La DPA doit avoir la possibilité, pour l'ensemble de ses tâches de contrôle et de surveillance, de réclamer impérativement toute information pertinente au responsable ou, le cas échéant, au sous-traitant.

103. En outre, il conviendra de prévoir qui doit répondre et comment dans le cadre du système de guichet unique (application de l'article 51.2) et quelle est l'investiture pour les autres DPA. Afin d'éviter tout hiatus, il y a lieu de prévoir la possibilité pour chaque DPA de recourir à cette obligation de coopération, sans qu'aucune exception de compétence ne puisse être invoquée.

22. Sécurité des traitements (article 30)

104. La CPVP apprécie que le projet de Règlement impose les obligations en matière de sécurité également directement au sous-traitant (article 30.1). Dans la pratique, cela correspond à nos dispositions nationales (article 16, § 4 de la LVP).

105. La CPVP souligne également l'utilité d'exiger explicitement que les instructions données au sous-traitant soient consignées par écrit (article 26.3) et considère que cela devrait également être le cas pour le niveau de service ou de garantie relatif aux mesures de sécurité imposées par le responsable du traitement.

106. L'article 26.4 prévoit d'ailleurs que si un sous-traitant traite des données à caractère personnel d'une manière autre que celle définie dans les instructions, il devient le responsable du traitement et il est soumis aux dispositions applicables aux responsables conjoints du traitement. L'article 24, qui définit les règles applicables aux responsables conjoints du traitement, prévoit que ceux-ci définissent, par voie d'accord, leurs obligations respectives et que le non-respect de cette obligation peut être sanctionné d'une amende pouvant s'élever à 500.000 euros ou, dans le cas d'une entreprise, à 1% de son chiffre d'affaires annuel mondial (article 79.5.e). La CPVP fait toutefois remarquer que lorsqu'un sous-traitant utilise des données pour la réalisation d'une finalité propre, il n'avertit pas nécessairement le responsable initial du traitement de ces activités. Par conséquent (et bien que la CPVP soutienne l'idée que dans la situation en question, le sous-traitant doit être considéré comme le responsable du traitement), il faudrait veiller à ce que le responsable initial du traitement – qui, comme précisé, n'a pas connaissance de ces nouveaux traitements – ne puisse pas être sanctionné pour ne pas avoir conclu un contrat au sens de l'article 24 du projet de Règlement.

107. En ce qui concerne les conditions qui permettent au sous-traitant de recourir à un autre sous-traitant (article 26.2.d), la CPVP souhaite souligner le fait qu'outre l'autorisation préalable du responsable, cette sous-traitance ultérieure doit également faire l'objet d'un accord qui soumet le sous-traitant ultérieur aux mêmes obligations que le sous-traitant initial. Ce principe est repris dans les clauses contractuelles types 2010/87/UE qui ont été approuvées par la Commission européenne, et plus particulièrement dans la clause 11. Cette clause stipule également qu'en cas de manquement, par le sous-traitant ultérieur, aux obligations en matière de protection des données qui lui incombent conformément audit accord, le premier sous-traitant reste pleinement responsable envers le responsable du traitement.

23. Notification des violations aux DPA et à la personne concernée (articles 31 et 32)

108. Le projet de Règlement ne précise pas si chaque violation de la sécurité (violation de données) doit être notifiée à la DPA. Le texte délègue à la Commission européenne la tâche de déterminer, via un acte délégué, les circonstances dans lesquelles les responsables du traitement sont tenus de notifier la violation (article 31.5). On pourrait donc penser à juste titre qu'en l'absence d'approbation des actes délégués, toute violation de la sécurité devrait être notifiée à la DPA, ce qui constituerait peut-être une obligation trop vaste et impossible à mettre en œuvre. Il appartient également à la Commission européenne de déterminer les circonstances dans lesquelles des violations peuvent potentiellement porter atteinte aux données ou à la vie privée des personnes concernées. Ces critères permettraient de déterminer les violations qui doivent également être notifiées aux personnes concernées.

109. La CPVP estime que des critères clairs devraient être intégrés dans le texte même et non être déterminés a posteriori via des actes délégués. Il faut avant tout éviter une notification excessive de petites violations aux DPA de sorte que seules les violations ayant de graves conséquences ou concernant un grand nombre de personnes doivent être notifiées. Par ailleurs, les risques de pertes financières devraient également faire partie des critères nécessitant une notification aux personnes concernées.

110. Le projet de Règlement prévoit d'ailleurs une exception à la notification d'une violation à la personne concernée lorsque le responsable du traitement prouve, à la satisfaction de DPA, qu'il a mis en œuvre les mesures de protection technologiques appropriées de sorte que les données soient rendues incompréhensibles à toute personne ne disposant pas d'une autorisation d'accès (mesures de cryptage). La CPVP souligne que techniquement, rendre la lecture des données totalement incompréhensible[26] à quiconque ne doit pas constituer la conséquence des mesures de cryptage, mais bien leur finalité. L'exigence devrait plutôt viser cette finalité avec un caractère technique requis, associé à la nature des données, l'état de la technique et les coûts.

111. Enfin, la CPVP estime qu'il serait nécessaire de préciser dans le contrat entre le responsable du traitement et le sous-traitant qu'en cas d'incident de sécurité, le responsable du traitement et le sous-traitant collaborent pour déterminer les causes de l'incident et prendre des mesures palliatives ou correctives.

---

[26] La CPVP suggère de remplacer le terme "incompréhensible" (unintelligible) par le terme "inaccessible" (unaccessible).

112. La CPVP considère que le présent texte soulève encore tellement de questions que son adoption engendrera des situations impossibles, tant pour la DPA que pour le responsable ou, le cas échéant, pour le sous-traitant ou encore pour la personne concernée. La "data breach notification" (notification des violations de données) est assez récente et doit encore faire l'objet de nombreuses analyses et expérimentations. La CPVP estime dès lors que le déploiement nécessite d'établir un plan par étapes réaliste afin de pouvoir introduire cette obligation progressivement. Il faudra également prévoir un suivi attentif des avantages et inconvénients du mécanisme, des conséquences administratives et financières et du solde pour les droits de la personne concernée. Les rares expériences de la CPVP à cet égard ne sont pas d'emblée positives. La CPVP formule par conséquent de grandes réserves et espère que des analyses préalables suffisantes seront encore menées quant à la faisabilité et à l'efficacité de ce mécanisme, avec une question centrale : cela profite-t-il au citoyen ?

24. Analyse d'impact relative à la protection des données (article 33)

113. Outre les circonstances prévues à l'article 33.1., il est recommandé de donner à la DPA le pouvoir d'imposer un PIA par décision motivée. Cela doit permettra à la DPA d'agir de manière modulée et adéquate.

114. La CPVP ne comprend pas ce que représentent les "risques particuliers" à l'article 33.2.c : les zones accessibles au public sont actuellement les lieux par excellence où l'on effectue une surveillance par des dispositifs opto-électroniques. Sauf circonstances exceptionnelles où la DPA peut intervenir et imposer un PIA, on ne comprend pas pourquoi la vidéosurveillance (à grande échelle) de zones accessibles au public (portée de la notion ?) présente des risques particuliers (sauf lorsque des applications spéciales sont mises en œuvre comme par exemple la reconnaissance faciale ou lorsque les caméras et/ou les images ne sont pas utilisées d'une manière conforme aux prévisions raisonnables du grand public). Cela ne correspond en tout cas pas avec les expériences de la CPVP en matière de surveillance par caméras.

115. L'article 33.4. n'est pas clair et peut être interprété de nombreuses manières ou être ignoré. Cette disposition doit être supprimée ou précisée.

116. La CPVP se demande pourquoi l'article 33.5 renvoie à des traitements effectués dans le cadre de la législation européenne et non aussi de celle des États membres. L'adoption d'une législation nationale devrait toujours s'accompagner d'une analyse d'impact relative à la protection des données

(voir le considérant 73). La CPVP ne comprend dès lors pas pourquoi seule la législation européenne fait l'objet d'une dispense et non les autres instruments législatifs (adoptés par une assemblée parlementaire). Cette exception doit s'appliquer à toute législation mais doit toutefois être compensée par un avis obligatoire par la DPA concernée (article 52.1.f. : dans le cadre de cette consultation, la DPA compétente déterminera si un PIA est nécessaire et utile ainsi que la manière dont il doit être réalisé).

117. La CPVP est favorable à l'instrument "analyse d'impact relative à la protection des données". Elle peut donc entièrement souscrire au principe.

118. La CPVP sait toutefois d'expérience qu'un bon PIA ne peut pas être trop lourd et ne peut pas non plus se réduire à un exercice de style stérile où des consultants chèrement payés produisent de grandes quantités de texte. Il faut au contraire tout mettre en œuvre pour faire du PIA un instrument précis et concret qui indique de la manière la plus impartiale et la plus claire possible les objectifs et la finalité du traitement envisagé, quels sont les risques, ce qu'impliquent les options et comment sont respectées les obligations du responsable ou, le cas échéant, du sous-traitant. La question fondamentale à cet égard doit toujours être de savoir si le citoyen, la personne concernée, peut y trouver avantage ou en subir un préjudice et ce qui est fait pour renforcer les droits et les libertés de ce citoyen.

119. La manière dont cette obligation sera concrétisée, comme prévu aux articles 33.6. et 33.7., est dès lors importante. À cet égard, la CPVP demande également une introduction réfléchie et un contrôle régulier. Voir *mutatis mutandis* ci-dessus.

25. Autorisation et consultation préalables des DPA (article 34)

120. Le projet de Règlement entend limiter les pouvoirs d'autorisation préalable des autorités de protection des données au seul domaine relatif aux transferts internationaux de données (article 34.1). La réglementation belge actuelle en matière de protection des données prévoit toutefois un système d'autorisations préalables pour certains transferts de données bien déterminés émanant de services publics belges. L'article 34 risque donc de remettre ce système en question.

121. Les mécanismes de protection et les procédures qui ont été développés en Belgique prévoient en effet notamment la mise en place de Comités sectoriels (Sécurité Sociale et Santé, Registre national, Autorité fédérale, Statistique, Phenix (Justice), Banque-Carrefour des entreprises) ayant une compétence d'autorisation préalable. Ces Comités sont établis au sein de notre DPA mais sont mixtes, car composés pour partie de membres de la CPVP et pour une autre partie d'experts ou de

membres d'autorités publiques. Ces Comités ont en charge le contrôle de traitements de données effectués par des administrations publiques, principalement par la voie d'autorisations préalables. Ainsi, avant que ces autorités publiques puissent mettre certaines données à caractère personnel à disposition d'autres autorités publiques ou de tiers, une autorisation préalable doit être obtenue auprès d'un de ces Comités. C'est par exemple le cas pour l'accès à et l'utilisation du numéro de Registre national et l'accès au Registre de la population.

122. La procédure d'autorisation préalable par ces Comités permet d'accompagner utilement le secteur public lors de la mise en place d'un flux de données personnelles. Ces Comités jouent le rôle de guide auprès des responsables de traitement. Ils peuvent non seulement autoriser ou refuser entièrement un accès mais ils peuvent aussi accorder des autorisations auxquelles des conditions (suspensives) sont assorties.

123. La mise en place de consultations préalables, telle que prévue dans le projet de Règlement, aboutira par contre systématiquement soit à une absence de réaction de la DPA (engendrant une insécurité juridique dans le chef du responsable du traitement), soit à une interdiction[27] des traitements si ceux-ci ne sont pas conformes à la législation (art. 34.3). De plus, cette interdiction pourrait être applicable alors même que le traitement est fondé sur une loi, ce qui est excessif.

124. Accessoirement, la CPVP remarque également que dans l'article 34.4 du projet de Règlement, on propose aux autorités de protection des données d'établir une liste des traitements devant faire l'objet d'une consultation préalable. La CPVP estime qu'il s'agit d'une compétence excessive car ces choix doivent être démocratiquement décidés (c'est-à-dire par le législateur).

125. **En résumé, la CPVP estime que le système belge de Comités sectoriels, mis en place pour la protection des données à caractère personnel dans le cadre du secteur public, devrait pouvoir être intégralement maintenu** et que le projet de Règlement ne devrait pas porter atteinte aux systèmes purement nationaux qui ne mettent pas à mal le principe de la libre circulation des données. Le texte actuel de l'avant-projet ne prévoit toutefois pas cette possibilité (ni à l'article 34, ni au Chapitre IX). Apparemment, le représentant de la Commission européenne aurait pourtant déclaré – dans le cadre des réunions DAPIX – que l'on comprenait ce point de vue belge. La CPVP demande dès lors de modifier effectivement le projet de Règlement dans ce sens.

---

[27] L'article 34, point 3 prévoit toutefois l'obligation pour la DPA, en cas d'interdiction, de formuler "des propositions appropriées" "afin de remédier à cette non-conformité". Actuellement, les Comités sectoriels belges peuvent – dans les cas où des points d'amélioration de la protection de la vie privée sont encore détectés – accorder immédiatement une autorisation qu'ils assortissent d'une condition (suspensive). Dans le système du projet de Règlement, l'autorité de protection des données devra toujours, dans de telles situations, refuser et faire des "propositions appropriées", ce qui implique de facto que le demandeur devra ensuite introduire une nouvelle demande, ce qui est peu flexible et inefficace.

26. Le délégué à la protection des données (articles 35 à 37 inclus)

126. Le projet de Règlement consacre une section entière du chapitre relatif aux obligations du responsable de traitement et du sous-traitant à la fonction de délégué à la protection des données (articles 35-37).

127. La CPVP accueille favorablement cette reconnaissance formelle du délégué à la protection des données et de son rôle d'assistance[28] au responsable de traitement et au sous-traitant dans la mise en œuvre effective des différentes obligations qui leur incombent en vertu du Règlement. La désignation d'un délégué à la protection des données participe de la mise en œuvre du principe "d'accountability" et de l'approche "internal privacy management" du Règlement tout en conservant un lien étroit avec l'autorité de protection des données et les personnes concernées.

128. Si le projet de Règlement devait un jour entrer en vigueur, le rôle et le statut du "préposé à la protection des données" au sens de l'article 17*bis* de la LVP seraient enfin précisés ; précision à laquelle la CPVP invite l'exécutif belge depuis de nombreuses années[29].

129. La CPVP relève avec satisfaction que le délégué à la protection des données puisse être une personne employée par le responsable de traitement ou une personne externe (article 35.8) et qu'il se voit également confier le rôle de "point de contact" pour l'exercice de leurs droits par les personnes concernées. L'information à fournir par le responsable de traitement ou le sous-traitant est à cet égard essentielle (article 14.1 a)).

130. Quant à la coopération avec l'autorité de protection des données, la CPVP partage la vision du projet de Règlement (article 37, § 1, h)). Une relation, notamment d'échanges d'informations, apparaît essentielle.

131. De manière générale, la CPVP est également satisfaite des garanties d'indépendance exigées par le projet de Règlement, de même qu'elle approuve les obligations mises à charge des responsables de traitement et sous-traitants afin de permettre au délégué à la protection des données d'exercer pleinement sa fonction (article 35, §§ 5, 6, 7 et article 36). Ces garanties rejoignent celles qu'elle a, à plusieurs reprises, appelées de ses vœux dans l'exercice de sa

---

[28] Remarque de traduction : la CPVP relève que le terme "monitor the implementation and application of the policies.." utilisé à l'article 37 § 1 b) est traduit, dans la version française, par le terme "contrôler la mise en œuvre..". Elle est d'avis que cette traduction n'est pas adéquate. Les termes "veiller à (surveiller) et assister" (dans le sens d'un monitoring cardiaque par exemple), doivent lui être préférés.

[29] Voy. par exemple CPVP, Avis 15/2002 du 2 mai 2002 relatif au projet d'arrêté royal portant exécution de l'article 3 § 6 de la loi du 8 décembre 1992 *relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel* (§ 17).

compétence d'avis[30]. Elle constate toutefois l'absence totale de mécanisme/procédure/garanties contre le licenciement en raison de l'exercice par le délégué de ses fonctions. Elle aurait trouvé utile qu'à tout le moins les autorités de protection des données soient informées et/ou qu'une faculté de saisine de l'autorité de protection des données soit offerte au délégué à la protection des données en cas de licenciement (envisagé)[31].

132. Fidèle à sa jurisprudence, la CPVP est en outre d'avis que la fonction de délégué à la protection des données peut être exercée conjointement à une autre fonction pour autant que le délégué à la protection des données bénéficie en cette qualité de toute la liberté et de l'indépendance nécessaires pour mener à bien l'ensemble de ses missions[32]. La CPVP souligne à cet égard que l'indépendance du délégué à la protection des données ne peut raisonnablement s'envisager comme absolue, ne fut-ce que parce que le délégué à la protection des données est, dans certains cas à tout le moins, engagé dans un contrat de travail avec le responsable de traitement.

133. **Nonobstant l'appréciation favorable qui précède, la CPVP n'est pas favorable au choix opéré de rendre obligatoire la désignation d'un délégué à la protection des données dans certaines hypothèses.** À ses yeux, désigner un délégué à la protection des données doit rester optionnel. La désignation d'un délégué à la protection des données est une mesure - parmi toutes celles qui participent de l'accountability - que le responsable de traitement doit rester libre de mettre en œuvre compte tenu des traitements opérés, de la nature des données traitées, des risques, de l'existence d'autres mécanismes de protection en vigueur et du bénéfice réel pour la protection des données qu'apporterait la désignation du délégué à la protection des données dans le cas d'espèce.

134. Accessoirement, la CPVP a également des remarques à formuler concernant les critères utilisés dans le projet de Règlement pour déterminer si un délégué à la protection des données est obligatoire ou non :

a. Un des critères concerne la situation où le traitement est effectué par une entreprise employant au moins 250 travailleurs. La Commission estime que le nombre de travailleurs ne constitue pas un bon critère pour déterminer la

[30] Voy. les avis n° 01/2007, 16/2007 et 39/2008.

[31] Voy. par exemple la loi française 78-17 du 6 janvier 1978 *relative à l'informatique, aux fichiers et aux libertés* (Chapitre IV) et le décret d'application 2005-1309 du 20 octobre 2005.

[32] CPVP, Avis 33/2002 du 22 août 2002 portant sur le projet de loi relatif à la création du Centre fédéral d'expertise des soins de santé (point 21). Dans le même sens, CPVP, Avis 19/2002 du 10 juin 2002 relatif aux (1) projet de loi modifiant la loi du 8 août 1983 *organisant un Registre national des personnes physiques* et la loi du 19 juillet 1991 *relative aux registres de la population* et modifiant la loi du 8 août 1983 *organisant un Registre national des personnes physiques*, (2) projet d'arrêté royal relatif aux cartes d'identité et (3) projet d'arrêté royal portant mesures transitoires en ce qui concerne la carte d'identité électronique ; CPVP, Avis 23/2006 du 12 juillet 2006 portant sur l'avant-projet de loi relatif à l'encadrement des listes négatives (points 42 à 44).

nécessité d'un délégué à la protection des données. Une entreprise peut en effet employer 1000 travailleurs mais n'effectuer quasiment aucun traitement (sensible) de données à caractère personnel, tandis qu'une petite entreprise de 10 travailleurs peut par contre effectuer un très grand nombre de traitements sensibles.

b. La CPVP s'interroge sur la manière dont il convient d'interpréter le segment suivant de l'article 35, point 1, c) : *"(…) des traitements qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique des personnes concernées"*. La CPVP demande que dans le texte même de l'article 35, ou du moins dans un considérant, on clarifie ce qu'il y a lieu d'entendre pas là. Étant donné qu'il s'agit d'une hypothèse où un délégué à la protection des données doit obligatoirement être désigné, cette clarification ne peut pas attendre les actes délégués dont la Commission se réserve l'adoption à l'article 35.11.

27. Codes de conduite

135. La CPVP estime qu'il ne devrait pas être de la compétence de la Commission européenne mais bien du Comité européen de la protection des données de constater qu'un code de conduite est d'applicabilité générale sur le territoire de l'Union (article 38.4).

28. Transferts de données à caractère personnel vers des pays tiers ou à des organisations internationales

136. La CPVP estime que le projet de Règlement clarifie les règles en matière de flux transfrontières, notamment en ce qui concerne la définition des critères d'évaluation de l'adéquation des pays tiers ou la reconnaissance explicite des règles d'entreprises contraignantes.

137. La CPVP soutient également la volonté de simplifier les obligations des entreprises en supprimant les exigences d'autorisations nationales lorsque des clauses types ou des règles d'entreprises contraignantes sont utilisées.

138. Pour ce qui concerne en particulier l'article 42.5, la CPVP estime qu'il manque de clarté. Cet article semble concerner le secteur public et devrait explicitement s'y limiter. Il est essentiel que des solutions soient offertes en matière de flux internationaux pour le secteur public. Les clauses types ou règles d'entreprises contraignantes n'ont pas pour ambition de s'adresser au secteur public. Les accords de coopération ou les engagements unilatéraux qui sont utilisés par le secteur public devraient pouvoir subsister et même bénéficier d'une reconnaissance explicite dans le texte.

139. En ce qui concerne les règles d'entreprise contraignantes, le projet de Règlement entend lister les conditions devant être remplies en se fondant sur les exigences actuellement définies dans les documents du groupe de l'article 29[33]. Le projet de Règlement ne reprend cependant pas l'exigence actuelle relative à la nécessité de mettre en place au sein du groupe d'entreprises un système interne de traitement des plaintes des personnes concernées ni celle de la mise en place d'un programme de formation adéquat[34]. Ces obligations ne sont pas clairement stipulées et ne se retrouvent qu'au niveau de la description des missions du délégué à la protection des données. Cependant, si ce dernier doit être informé des plaintes relatives aux données à caractère personnel, ce n'est pas nécessairement lui qui doit prendre en charge ces missions (traitement de plaintes[35], formation des employés) et, de surcroit, la référence explicite à l'article 35 au sein de l'article 43.2.h ne garantit pas toujours son existence (la désignation d'un délégué à la protection des données n'étant obligatoire que dans certaines hypothèses). Par ailleurs, les documents du groupe de l'article 29 requièrent un engagement selon lequel, en cas de conflit entre une législation étrangère et les règles d'entreprises contraignantes, les membres du groupe d'entreprise acceptent de se soumettre à une nécessité de transparence interne (au sein du groupe) mais également, en cas de doute, à l'égard des autorités européennes de protection des données[36]. Cette condition n'est pas reprise au sein de l'article 43 du projet de Règlement. Enfin, comme souligné plus haut, la définition des règles d'entreprises contraignantes ne devrait pas limiter son application aux seules sociétés multinationales ayant un établissement au sein de l'Union.

140. Enfin, la dérogation prévue à l'article 44.1.h. relative à la possibilité pour le responsable de traitement d'évaluer lui-même les circonstances relatives à un transfert et d'offrir les garanties appropriées nécessaires est en contradiction et met en péril le régime des clauses contractuelles "ad hoc" et des BCR qui impliquent nécessairement l'intervention de l'autorité.

29. Les autorités de protection des données (articles 46 à 54 inclus)

141. Le Chapitre VI du projet de Règlement est entièrement consacré aux autorités de contrôle (autorités de protection des données). Leur statut, les règles relatives à leur établissement, leurs compétences, fonctions et pouvoirs sont plus nombreux et bien davantage précisés que dans la Directive 95/46/CE.

---

[33] Principalement le WP153, mais également le WP74 et WP108.

[34] Points 2.1 et 2.2 du WP153.

[35] La gestion de plainte doit néanmoins être confiée à une personne ou un département disposant d'un degré approprié d'indépendance dans l'exercice de ses fonctions (voir le WP 153 du Groupe de l'article 29 mais également la recommandation 01/2006 de la CPVP en matière de whistleblowing).

[36] Point 6.3 du WP153.

142. Le projet de Règlement entend renforcer l'indépendance des autorités de protection des données en tenant notamment compte de l'arrêt du 9 mars 2010 de la Cour de Justice de l'Union européenne à l'encontre de la république d'Allemagne[37].

143. La CPVP accueille favorablement les exigences prévues à l'article 47 du projet de Règlement au regard de l'indépendance des autorités de protection des données, tout particulièrement l'appréhension *globale* de cette indépendance : indépendance de ses membres (commissaires CPVP), ressources humaines suffisantes et personnel propre (secrétariat CPVP), ressources techniques, ressources financières appropriées soumises à un contrôle financier qui ne menace pas son indépendance ainsi que mise à disposition de locaux et de l'infrastructure nécessaires à l'exécution effective de ses fonctions et pouvoirs. À ces égards, la CPVP attire l'attention des autorités belges compétentes sur les nouvelles fonctions qui seront les siennes et sur les implications en termes de personnel et de moyens financiers qu'elles induisent. Citons ici par exemple l'appréciation des conclusions d'analyses d'impact préalables (article 33), le traitement des notifications de violations de données et l'examen de la question de savoir si le responsable de traitement a apporté les mesures adéquates destinées à limiter les effets préjudiciables de ces violations (articles 31-32), l'assistance à ses homologues européens, la coopération avec ces derniers et sa participation au comité européen de la protection des données (chapitre VII), ainsi que sa nouvelle compétence d'imposition de sanctions administratives (article 53.4 et articles 79.4, 5 et 6).

144. Quant aux conditions générales applicables aux membres de l'autorité de contrôle (article 48), la CPVP formule deux remarques :

a. Premièrement, elle est d'avis que les conséquences liées au fait qu'un membre ne remplit plus les conditions nécessaires à l'exercice de sa fonction ou a commis une faute grave devraient être laissées à l'appréciation du législateur national. La CPVP estime que la Commission européenne outrepasse ses compétences en prévoyant que, dans ces hypothèses, un membre peut être déclaré démissionnaire ou déchu du droit à la pension et à d'autres avantages.
b. Deuxièmement, elle estime que les membres des autorités de contrôle devraient toujours être désignés par le parlement et non pas par le Gouvernement (l'article 48, point 1 laisse ce choix en la matière aux États membres). Au parlement siègent en effet des représentants de toutes les tendances politiques, ce qui garantit un contrôle démocratique plus étendu. Selon la CPVP,

[37] Cour de justice européenne (Grande chambre), 9 mars 2010, affaire C-518/07.

une nomination des membres par le parlement rejoint davantage les conditions d'indépendance fixées dans l'arrêt de la Cour de Justice du 9 mars 2010.

145. Lorsque le traitement de données a lieu dans le cadre des activités d'un responsable de traitement ou d'un sous-traitant établi dans plusieurs États membres, le projet de Règlement prévoit que l'autorité compétente sera uniquement celle du lieu où se situe l'établissement principal du responsable de traitement (article 51.2). Les autorités européennes de protection des données ont qualifié ceci de "**one-stop-shop"** pour les responsables de traitement, soit le principe d'un guichet unique pour ces derniers.

146. Bien que de prime abord, ce principe soit attrayant[38], la CPVP émet toutefois de sérieuses réserves concernant sa faisabilité.

147. Ainsi, la notion d' "établissement principal" constitue l'un des éléments cruciaux de l'article 52 et la définition donnée à cette notion (article 4, point 13) est tout sauf claire, surtout en ce qui concerne ce segment : *"si aucune décision de ce type* (quant aux finalités, aux conditions et aux moyens du traitement de données à caractère personnel) *n'est prise dans l'Union, l'établissement principal est le lieu où sont exercées les principales activités de traitement dans le cadre des activités d'un établissement d'un responsable du traitement dans l'Union. (…)"*. La Commission se demande également comment les conflits de compétence entre autorités de protection des données – qui surgiront inévitablement sur la base de cet article 52 imprécis – seront résolus.

148. En outre, la CPVP s'inquiète des conséquences juridiques et pratiques de la désignation d'une seule autorité compétente dans une affaire déterminée. Elle pense pouvoir exprimer au mieux cette préoccupation à l'aide de quelques exemples :

a. Un travailleur belge employé en Belgique par une entreprise dont l' "établissement principal" se situe en Irlande introduit auprès de la DPA belge une plainte contre son employeur parce que son téléphone est mis sur écoute. La DPA belge transmet l'affaire à la DPA irlandaise qui, dans ce cas, serait l'autorité compétente. Supposons que la DPA irlandaise trouve un arrangement entre l'employeur et le travailleur. La DPA irlandaise doit-elle alors – outre le projet de Règlement – également tenir compte par exemple du droit social et pénal belge ?
Dans l'affirmative, cela implique que la DPA irlandaise doit donc appliquer

[38] De manière générale, la CPVP comprend l'objectif de l'introduction d'un guichet unique ("one stop shop") consistant à ce que, pour un même traitement réalisé dans plusieurs États membres, plusieurs autorités seraient compétentes parallèlement et différentes décisions pourraient dès lors être prises.

la législation belge. Une application cohérente d'une telle approche impliquerait également que toute DPA doit potentiellement pouvoir appliquer la réglementation des 26 autres États membres de l'UE lorsqu'elle est désignée conformément à l'article 51 en tant que DPA compétente et lorsque l'affaire concernée n'a pas seulement une influence sur le Règlement en matière de vie privée mais aussi sur d'autres règles de droit national (ce qui est souvent le cas). La CPVP s'interroge sérieusement sur la faisabilité d'un tel système.
Dans la négative, le risque est réel que dans l'exemple donné, l'arrangement de la DPA irlandaise aille à l'encontre de dispositions juridiques belges contraignantes en droit social et en droit pénal. Dans cette dernière hypothèse, un juge belge ne pourra pas respecter l'arrangement de la DPA irlandaise[39].

b. Une société chinoise a un établissement en Belgique qui vend des produits téléphoniques à des citoyens belges. La société a plusieurs établissements au sein de l'UE dont le polonais constitue le "principal". La société propose d'enregistrer toutes les conversations téléphoniques entre ses travailleurs et ses clients en expliquant que le but est uniquement d'améliorer la formation des travailleurs. Les syndicats craignent toutefois que les conversations enregistrées servent de toutes autres finalités (à savoir le contrôle des travailleurs) et demandent une médiation à la DPA belge. La DPA belge – bien qu'elle connaisse le mieux les rapports et les problèmes sociaux ainsi que la langue de toutes les personnes concernées – devra toutefois demander aux syndicats de s'adresser à la DPA polonaise …

c. Une société ICT américaine possédant plusieurs établissements dans l'UE, dont l' "établissement principal" se situe à Paris, installe une application cloud avec une société belge et dans ce cadre, une violation de la sécurité survient, rendant publiques des données de citoyens belges. Quelle DPA est compétente ? Peut-être la française. Dans ce cas, la DPA belge doit-elle orienter tous les citoyens lésés vers la CNIL ?

[39] Cet exemple attire par ailleurs également l'attention sur un autre problème, à savoir le fait que les règles de compétence applicables à l'égard des DPA ne sont pas cohérentes avec celles du pouvoir judiciaire, et ce alors qu'il est plutôt rare que les faits d'une infraction au Règlement concernent exclusivement la protection des données : les faits punissables comportent généralement plusieurs infractions dont un seul aspect concerne la "protection des données" et dont les autres aspects peuvent uniquement être appréciés par le pouvoir judiciaire. Dans la pratique, un litige concret doit toutefois souvent être appréhendé dans sa totalité (peu importe le nombre de disciplines juridiques auxquelles touche l'affaire et peu importe quel(le) DPA/tribunal est compétent(e)) afin de parvenir à une bonne solution.

149. En résumé, la CPVP craint donc que l'article 52, point 2 ne soit à l'origine d'interminables discussions et conflits de compétence entre autorités de protection des données et estime également que cette règle de compétence engendrera des situations illogiques et ingérables. **La CPVP rejette dès lors le critère "établissement principal".**

150. Parallèlement, elle a bien conscience que la discussion relative à la désignation de la DPA compétente est un exercice difficile qui requerra encore de nombreuses réflexions. Afin de fournir une première contribution à cette discussion, elle souligne que selon elle, un des critères alternatifs possibles pourrait être : une DPA est compétente dans les cas où le responsable du traitement s'adresse, via ses activités, à une clientèle/un marché déterminé(e) sur le territoire de l'État membre où opère cette DPA.

30. Coopération et cohérence (articles 55 à 72 inclus)

151. Du fait de la globalisation des traitements de données à caractère personnel, la CPVP estime certainement utile que les systèmes de coopération existants entre autorités européennes soient renforcés par des mécanismes d'assistance mutuelle (article 55), d'opérations conjointes (article 56) et de cohérence (articles 57 à 63).

152. La CPVP est par contre d'avis que la possibilité, dans le chef de la Commission européenne, de demander la suspension d'une mesure d'une DPA, qui risque donc de mener cette Commission à une application incorrecte ou incohérente du Règlement (article 60), va trop loin. En effet, comment une autorité de protection des données peut-elle prendre des décisions en toute indépendance si celles-ci peuvent ensuite être remises en question par le pouvoir exécutif ? D'après la CPVP, une telle approche va à l'encontre de l'article 8, 3e alinéa de la Charte des Droits fondamentaux de l'Union européenne.

153. La mise en place d'un secrétariat permanent pour le groupe de l'article 29 (futur comité européen de la protection des données - CEPD) (article 71) est également jugée utile par la CPVP, compte tenu du nombre toujours croissant de sujets traités au sein de ce groupe. La CPVP exprime cependant des doutes quant aux délais qui sont prévus pour l'adoption d'avis au sein du CEPD (1 mois) (article 58.7).

31. Sanctions (articles 78 et 79)

154. Tout d'abord, la CPVP émet de sérieux doutes quant à l'utilité d'un régime de sanctions administratives uniformes que les autorités de protection des données doivent mettre en œuvre. La CPVP se demande pourquoi on propose aujourd'hui d'y recourir, étant donné qu'elle ne voit pas de problème à ce niveau dans la situation existante. À titre d'exemple, elle se réfère au dossier Google Street View et à la collecte illégale de données de connexions Internet (Wi-Fi), dans lequel les autorités de protection des données concernées ont appliqué, chacune selon sa propre politique et sa propre législation, le régime de contrôle et le cas échéant le régime de sanction à sa disposition sans que cela ne pose de difficulté : le Nederlandse College Beschermingspersoonsgegevens aux Pays-Bas a sanctionné Google par une astreinte, la CNIL en France a infligé une amende et la CPVP a transmis le dossier au ministère public qui a proposé à Google une transaction à hauteur de 150.000 euros.

155. En outre, la CPVP s'oppose au fait qu'elle serait elle-même compétente pour infliger des sanctions, notamment en raison de son attachement au principe de la séparation des pouvoirs. En corollaire, la CPVP souhaite savoir si la réunion de toutes les compétences qui seraient les siennes en vertu du projet de Règlement est compatible avec l'exigence d'impartialité que requiert l'exercice d'à tout le moins certaines de ces compétences. Cette question devrait être analysée de manière approfondie, notamment à la lumière de la jurisprudence de la Cour européenne des Droits de l'homme[40]. Une réorganisation approfondie de la CPVP serait nécessaire (au niveau organisationnel, par exemple via des chambres distinctes, à l'instar du système mis en place par la CNIL en France).

156. À cet égard, la Commission fait également remarquer :

a. que d'un point de vue constitutionnel, seul le pouvoir judiciaire est compétent pour contrôler l'application de la loi et pour en sanctionner le non-respect. Cette compétence est ainsi confiée à des magistrats indépendants.

b. qu'il est plutôt rare que des faits soient exclusivement constitutifs d'un manquement en matière de protection des données : les faits délictueux comportent généralement plusieurs infractions dont un seul aspect a trait à la "protection des données". Dans ces cas, la compétence de l'autorité de protection des données empêchera cette dernière d'appréhender les faits de manière globale. Elle devra se

[40] Arrêt Dubus c. France du 11 juin 2009.

limiter à l'aspect "protection des données" car à son niveau, elle ne peut pas recourir à la technique du concours d'infractions, selon laquelle la peine la plus élevée est appliquée aux faits incriminés. Seuls les cours et tribunaux peuvent s'appuyer sur cette technique et appréhender globalement les faits délictueux.

157. La Commission se demande ensuite si on vise, à l'article 78, des sanctions administratives ou pénales. Cet article dispose ce qui suit : "*Les États membres prévoient les sanctions pénales applicables aux violations des dispositions du présent Règlement et prennent toutes les mesures nécessaires pour garantir leur application (…). Les sanctions pénales ainsi prévues doivent être effectives, proportionnées et dissuasives*".

158. Vu le choix d'un Règlement (en lieu et place d'une Directive) et à la lumière de la lecture conjointe de l'article 78 et de la base juridique indiquée dans le préambule pour le projet de Règlement, la CPVP conclut que la mission des États membres consiste ici à prévoir des sanctions administratives. En effet, lorsque l'UE veut demander aux États membres d'inscrire des sanctions pénales dans le droit national, elle doit utiliser à cet effet l'article 83.2 du Traité sur le fonctionnement de l'Union européenne[41] comme base juridique. Cet article exige clairement que l'adoption de normes minimales relatives à des sanctions pénales se fasse par une *Directive* (et non par un *Règlement*).

159. La CPVP émet également de sérieuses réserves quant à la qualification des sanctions établies à l'article 79. Bien que ces sanctions soient explicitement définies comme étant des "sanctions administratives", la CPVP estime qu'il s'agit ici plutôt de sanctions pénales, ce vu la jurisprudence permanente de la Cour européenne des Droits de l'homme[42] et vu la politique de l'Union européenne[43]. L'intérêt essentiel du constat qu'il s'agit ici de sanctions pénales réside dans le fait que l'article 6 de la Convention européenne des Droits de l'homme et l'article 6 du Traité sur l'Union européenne prescrivent que dans un tel contexte, il faut prévoir suffisamment de garanties juridiques (comme par exemple une possibilité de recours devant un juge indépendant). Le texte du projet de Règlement n'en fait aucune mention.

160. Qu'il s'agisse de sanctions administratives ou pénales, il est clair que le projet de Règlement introduit deux systèmes (articles 78 et 79) et d'après la CPVP, la conjonction des deux posera des

---

[41] "(…) *Lorsque le rapprochement des dispositions législatives et réglementaires des États membres en matière pénale s'avère indispensable pour assurer la mise en œuvre efficace d'une politique de l'Union dans un domaine ayant fait l'objet de mesures d'harmonisation, des directives peuvent établir des règles minimales relatives à la définition des infractions pénales et des sanctions dans le domaine concerné.* (…)"

[42] Cf. arrêt Engel du 8 juin 1976.

[43] Cf. l'article 6.3. du Traité sur l'Union européenne, sur la base duquel on peut conclure que l'UE adhère aux critères utilisés par la Cour européenne des Droits de l'homme pour distinguer des affaires pénales d'autres affaires. La Cour de Justice européenne l'a expressément confirmé notamment dans l'arrêt Spector du 23 décembre 2009 (§ 42, C-45/08).

problèmes. La CPVP pense notamment que l'application cumulative des deux régimes de sanctions peut conduire à une violation du principe général de droit selon lequel nul ne peut être poursuivi ou puni à raison des mêmes faits (non bis in idem).

161. La CPVP cite à l'appui de son analyse l'arrêt du 10 février 2009 de la Grande Chambre de la Cour Européenne des Droits de l'Homme (Zolotoukhine c. Russie) qui constate, alors qu'il y avait cumul d'une sanction administrative et d'une sanction pénale, la violation de l'article 4 du protocole n°7 selon lequel "*nul ne peut être poursuivi ou puni pénalement par les juridictions du même État en raison d'une infraction pour laquelle il a déjà été acquitté ou condamné par un jugement définitif conformément à la loi et à la procédure pénale de cet État*". En l'espèce, la Cour considère en effet que la procédure engagée contre le requérant, bien que qualifiée d'administrative en droit interne, doit s'analyser en une procédure pénale en raison notamment de la nature de l'infraction et de la sévérité de la peine.

162. La Commission attire également l'attention sur le fait que dans un État de droit, seules des infractions suffisamment précises peuvent être sanctionnées, que ce soit par voie de sanctions pénales ou de sanctions administratives. La CPVP constate à cet égard que nombre d'infractions prévues aux paragraphes 4 à 6 de l'article 79 auxquelles le législateur national associera le cas échéant des sanctions en application de l'article 78, font écho des obligations formulées en termes généraux, voire parfois vagues ou qui laissent à tout le moins une marge d'appréciation considérable aux responsables de traitement. Quelle prévisibilité dans ce cas ? La CPVP relève ainsi les articles 5a) (traitement licite, loyal et transparent), 5 e) (durée de conservation non excessive au regard de la réalisation des finalités), 5f) (traitement sous la responsabilité du responsable de traitement qui veille à la conformité de chaque opération), 6 e) (traitement nécessaire à la réalisation d'une mission effectuée dans l'intérêt public) et 6i) (intérêt légitime du responsable de traitement qui ne prévaut pas les intérêts ou libertés et droits fondamentaux des personnes concernées).

163. Enfin, la CPVP fait remarquer que l'article 79 du projet de Règlement laisse très peu de marge d'appréciation aux DPA. Elles ne peuvent notamment pas tenir compte des circonstances spécifiques dans lesquelles les infractions ont été commises. Ce n'est que dans un nombre limité de cas, où un responsable commet une première infraction non intentionnelle, qu'une sanction peut être remplacée par un avertissement. La CPVP estime recommandé de faire preuve ici de plus de flexibilité.

32. Dispositions relatives à des situations particulières de traitement de données (articles 80 à 85 inclus)

A. Les règles nationales existantes pour le secteur public

164. Le chapitre IX concerne les différents secteurs qui font l'objet de divergences nationales et dont on admet que ces divergences sont justifiées par les différentes cultures et traditions juridiques, tel qu'en matière de liberté d'expression, de traitement de données de santé, de sécurité sociale et d'emploi. Pour cette raison, les États sont invités pour ces aspects à élaborer leurs propres législations nationales.

165. Depuis l'introduction et le développement des droits fondamentaux, plus précisément du droit au respect de la vie privée en général et à la protection des données à caractère personnel en particulier, divers pays européens ont cherché à insérer ces droits de manière spécifique dans leur tissu administratif et institutionnel. Ces règles relatives à la protection de la vie privée dans le cadre des traitements de données réalisés par les autorités publiques font l'objet de telles divergences nationales que la CPVP estime que les systèmes existants dans chaque État membre devraient pouvoir être conservés.

166. Par exemple, si en matière de traitements de données de santé, un cadre d'action est laissé aux États membres pour les finalités médicales, de santé publique ou de sécurité sociale, aucune marge de manœuvre n'est laissée sous ce chapitre pour le traitement d'autres données à caractère personnel (que celles de relatives à la santé) dans le cadre de la sécurité sociale (et les traitements de données dans ce secteur ne concernent bien évidemment pas uniquement le simple remboursement des soins de santé ; ils peuvent par exemple aussi concerner les prestations versées dans le cadre du chômage ou des pensions).

167. Un deuxième exemple concerne l'actuel système belge des comités sectoriels, mis en place pour la protection des données à caractère personnel dans le secteur public, et dont la CPVP estime qu'il devrait pouvoir être intégralement maintenu (cf. supra).

168. La CPVP estime dès lors qu'il faut prévoir la possibilité de déclarer certaines dispositions du projet de Règlement non applicables aux traitements de données à caractère personnel dans le secteur public, de sorte que des systèmes nationaux existants – comportant des garanties propres de protection de la vie privée (par exemple un système d'autorisations préalables), ancrées au fil du

temps dans le cadre juridique – ne soient pas mis en péril et puissent encore être régis au niveau des États membres.

B. Utilisation du numéro d'identification du Registre national

169. La CPVP regrette la suppression de l'article 8.7 de la Directive 95/46/CE, lequel permet aux états de définir les conditions dans lesquelles un numéro national d'identification ou tout autre identifiant de portée générale peut faire l'objet d'un traitement. Cette disposition est supprimée sans aucune explication et n'est remplacée par aucune règle spécifique dédiée à cette donnée particulière.

170. On craint dès lors que le numéro d'identification du Registre national ne puisse plus être utilisé en Belgique. Il constitue toutefois une des pierres d'angle des actuels projets majeurs en matière d'eGovernment et une interdiction de son utilisation saborde *de facto* tous ces projets, alors que cela ne se justifie par aucun motif sérieux du point de vue de la protection de la vie privée. La législation belge prévoit en effet un système de protection particulier en termes de contrôle et d'autorisation pour l'utilisation du numéro d'identification du Registre national. Comme indiqué plus haut, la CPVP souhaite que ce système d'autorisations préalables soit maintenu.

171. Apparemment, le représentant de la Commission européenne aurait déclaré lors de la réunion DAPIX que l'ancien règlement prévu à l'article 8.7. de la Directive 95/46/CE devrait effectivement retrouver une place et que l'intention n'était pas d'empêcher la création et l'utilisation de numéros d'identification. La CPVP se réjouit d'ores et déjà de ce point de vue et tient à ce que le texte du projet de Règlement soit adapté en ce sens.

C. Les traitements de données relatives à la santé

172. L'article 81 du projet de Règlement comporte des dispositions spécifiques pour le traitement de données à caractère personnel relatives à la santé.

173. Ces règles doivent être lues conjointement avec la définition de la notion de "données à caractère personnel relatives à la santé", mentionnée à l'article 4.12. Ladite disposition doit à son tour être lue à la lumière du considérant 26[44]. Cette lecture révèle qu'une très large interprétation

[44] Les données à caractère personnel concernant la santé devraient comprendre, en particulier, l'ensemble des données se rapportant à l'état de santé d'une personne concernée; les informations relatives à l'enregistrement du patient pour la prestation de services de santé; les informations relatives aux paiements ou à l'éligibilité du patient à des soins de santé; un numéro ou un symbole attribué à un patient, ou des informations détaillées le concernant, destinés à l'identifier de manière univoque à des fins médicales; toute information relative au patient recueillie dans le cadre de la prestation de services de

est donnée à cette notion : il ne s'agit pas uniquement de données relatives à la santé physique ou mentale mais également de toute information relative à la prestation d'un service de santé au profit d'une personne (comme l'enregistrement du patient pour les soins, des informations relatives aux paiements ou à l'éligibilité du patient à des soins de santé).

174. La CPVP estime avant tout que cette définition proposée par le projet de Règlement est (bien) trop large et ne tient pas assez compte des nombreux contextes dans lesquels les traitements de telles données peuvent être réalisés.

175. En outre, elle constate que l'article 81 impose encore des conditions spécifiques (obligation de l'existence d'une base légale spécifique, obligation de secret professionnel ou d'une obligation de confidentialité équivalente) pour traiter de telles données. Ces modalités soulèvent des questions :

a. La CPVP estime que l'exigence selon laquelle par exemple des traitements de données à des fins de facturation de services hospitaliers devraient nécessairement être régis par une loi spécifique a peu de sens/est peu réaliste.

b. Il est également important pour la CPVP que la notion "d'obligation de confidentialité équivalente" (article 81, point 1, a)) ne soit pas interprétée comme étant limitée au secret professionnel car cela impliquerait la nécessité de garantir la supervision d'un professionnel des soins de santé pour tous ces traitements (également pour le traitement de données dans le cadre de la sécurité sociale et du remboursement des soins de santé).

c. La relation entre l'article 81 et l'article 9 du projet de Règlement est tout à fait imprécise, aux yeux de la CPVP. Cet article 9 prévoit une liste de motifs d'exception où le traitement de données relatives à la santé est permis. Un de ces motifs est mentionné à l'article 81 (à savoir l'article 9, point 2, h) et l'article 81 semble ne concerner que cette situation spécifique. Néanmoins, des données médicales peuvent également être traitées sur la base d'autres motifs énumérés à l'article 9, point 2, et pour ces traitements, aucun lien n'est établi avec l'article 81.

---

santé audit patient; des informations obtenues lors d'un contrôle ou de l'examen d'un organe ou d'une substance corporelle, y compris des échantillons biologiques; l'identification d'une personne en tant que prestataire de soins de santé au patient; ou toute information concernant, par exemple, une maladie, un handicap, un risque de maladie, un dossier médical, un traitement clinique ou l'état physiologique ou biomédical de la personne concernée, indépendamment de sa source, qu'elle provienne par exemple d'un médecin ou d'un autre professionnel de la santé, d'un hôpital, d'un dispositif médical ou d'une épreuve diagnostique in vitro.

En outre, certains autres motifs d'exception repris à l'article 9, point 2 recouvrent en partie les trois motifs énumérés à l'article 81, point 1, sans justification spécifique.
La CPVP demande dès lors de réexaminer en profondeur le lien entre les articles 9 et 81.

D. Les traitements de données à des fins de recherche historique, statistique et scientifique

176. Le projet de Règlement consacre un article complet à la recherche historique, statistique ou scientifique (l'article 83), ce qui facilite certainement la lecture des conditions légales relatives au traitement de données dans le cadre de la recherche scientifique[45]. Les conditions établies au sein de l'article 83.1, qui visent à promouvoir l'usage de données anonymes ou codées en matière de recherche scientifique, sont parfaitement en ligne avec notre législation nationale et d'autres standards internationaux[46]. Néanmoins, la CPVP estime que le texte de l'article 83, point 1, devrait formuler encore plus précisément le principe qui veut que des traitements de données doivent être réalisés, dans la mesure du possible, sur la base de données anonymes et si cela est impossible, que le traitement doit se faire sur la base de données codées et que, seulement si c'est également impossible, un traitement de données identifiables peut être admis.

177. La CPVP estime ensuite utile d'avoir reconnu la recherche historique, statistique ou scientifique comme fondement de légitimité pour le traitement des données sensibles (article 9.2.i)[47]. La Directive 95/46/CE permettait aux États membres de reconnaître la recherche scientifique comme motif d'intérêt public important (considérant 40) et des divergences d'implémentation nationales existaient en la matière.

178. La CPVP a plus de réserves à propos de l'article 6.2 qui semble permettre que des traitements de données "non-sensibles" puissent avoir lieu à des fins de recherche scientifique sans que le premier paragraphe de l'article 6 soit respecté. Il est pourtant essentiel, aux yeux de la CPVP, que tout projet de recherche passe par l'obligation de ce test de légitimité et cela afin d'éviter, par exemple, le développement de projets de recherche qui ne seraient pas éthiques.

---

[45] Aujourd'hui, les informations utiles sont dispersées au sein de la Directive 95/46/CE, notamment aux considérants 29, 34, 40 ; ainsi qu'aux articles 6.1.b, 6.1.e, 11.2, 13.2.

[46] Chapitre II de l'arrêté royal du 13/02/2001; mais également voir l'Art.40 de la loi fédérale allemande, l'article 46 de la loi fédérale autrichienne (DSG 2000), l'article 16 de la loi estonienne et l'article 3 de la Recommandation Rec(2006)4 du Conseil de l'Europe sur la recherche utilisant du matériel biologique d'origine humaine.

[47] Le congrès international sur la recherche scientifique que la CPVP a organisé en novembre 2010 conduisait également à ce constat.

179. L'article 5.e prévoit la possibilité explicite de conserver plus longuement les données à des fins de recherches historiques, statistiques ou scientifiques, rend légitime les archives publiques et fait écho à l'article 6.1.e de la Directive 95/46/CE. Selon cet article, des garanties appropriées devaient être prévues par les États membres et ces garanties sont proposées directement dans le texte du projet dès lors qu'il a pour but d'être directement applicable. La condition est de procéder à un examen périodique de la nécessité de poursuivre la conservation. La CPVP estimerait utile d'ajouter d'autres garanties, telles que la nécessité de respecter strictement la finalité prévue de la recherche et la mise en place de mesures de sécurité pour ne permettre l'accès que dans le cadre de recherches historiques, statistiques ou scientifiques.

180. La CPVP s'étonne du fait que les exceptions qui avaient été introduites dans la Directive 95/46/CE en ce qui concerne l'exercice des droits des personnes concernées (articles 11.2, 13.2) ne se retrouvent plus dans le projet de Règlement, hormis sous la forme d'une éventuelle adoption d'actes délégués (article 83.3). Les exceptions devraient figurer au sein même du texte afin de garantir leur existence dès son entrée en vigueur et devraient contenir en leur sein les garanties appropriées qui sont actuellement prévues par les États membres. La CPVP, sur la base de son expérience notamment acquise dans le cadre de la conférence internationale "Privacy and research : from obstruction to construction" de novembre 2010[48] qu'elle a organisée, a une proposition concrète de texte :

- *In addition to the circumstances referred to in Article 14(5), paragraphs 1 to 4 of Article 14 shall not apply where the data are directly[49] or indirectly obtained from the data subject, under condition that the information or part of the information referred to in Article 14 (1 to 3) is likely to render impossible or seriously impair the achievement of the objectives of the scientific research[50]. From the moment that the information is not any more likely to render impossible or seriously impair the achievement of the objectives of the scientific research, the data subject shall be informed without delay.*
- *Article 15 shall not apply under condition that the information or part of the information referred to in Article 14 (1 to 3) is likely to render impossible or seriously impair the achievement of the objectives of the scientific research, unless the interests of the research are overridden by the interests or the fundamental rights and freedoms of the data subject. From the moment that the information is not any more likely to render*

[48] http://www.privacyandresearch.be/

[49] Une exemption en cas de collecte directe est déjà prévue dans différentes législations nationales, telles que la loi fédérale allemande (Art.33), la loi portugaise (Art. 10) ainsi que la loi luxembourgeoise (art. 27).

[50] Informer clairement des finalités précises de la recherche peut évidemment influencer et dès lors compromettre ses résultats. Une exception similaire se retrouve dans la loi polonaise (Art. 25 de la loi du 29 août 1997) pour les collectes indirectes de données.

impossible or seriously impair the achievement of the objectives of the scientific research, the controller or processor shall grant the data subject access to the data without delay.

E. Règles de protection des données des églises et associations religieuses

181. La CPVP se demande quelle est la portée de l'article 85 du projet de Règlement.

33. Actes délégués et actes d'exécution

182. Le projet de Règlement est caractérisé par un grand nombre d'actes délégués et d'actes d'exécution (articles 86 et 87).

183. La CPVP est d'avis que dans quasiment tous les cas, les délégations prévues ne respectent pas les conditions dans lesquelles le recours aux actes délégués est autorisé (article 291 § 1, al. 1 TFUE). L'objet d'un acte délégué est normalement de compléter l'acte législatif, en précisant certains éléments techniques ou de modifier des éléments *non essentiels* de l'acte législatif lui-même. Nonobstant l'interprétation restrictive donnée à la notion d'éléments essentiels et partant, la largesse des délégations autorisées[51], la CPVP estime qu'en l'espèce, la Commission européenne outrepasse ses compétences compte tenu du nombre de délégations accordées (article 86.2), des objets de celles-ci et du fait qu'à défaut de certaines d'entre-elles, les dispositions prévues dans le projet de Règlement ne pourraient (utilement) sortir leurs effets.

184. Aucune information n'est d'ailleurs fournie par le projet de Règlement quant à l'intention ou non de la Commission européenne d'adopter ces multiples actes délégués ni à propos du délai dans lequel ceux-ci seraient possiblement adoptés. Quid dès lors dans l'attente de ces actes délégués ? Le but ne peut quand même pas être de remplacer un système existant qui fonctionne bien par de nouvelles règles juridiques qui nécessitent encore sur de très nombreux points cruciaux des actes délégués ou des actes d'exécution (leur contenu et le calendrier dans lequel ils seront pris étant plus qu'imprécis) avant d'être applicables dans la pratique.

[51] N. De Sadeleer, I. Hachez, "Hiérarchie et typologie des actes juridiques de l'Union européenne", in *Les innovations du Traité de Lisbonne : incidences pour le praticien*, Bruylant, Bruxelles, 2011.

185. La CPVP insiste dès lors formellement pour limiter strictement les actes délégués et les actes d'exécution aux éléments non essentiels. Cela implique dès lors que quasiment tous les articles du projet de Règlement permettant de prendre de tels actes soient révisés.

L'Administrateur f.f., Le Président,

(sé) Patrick Van Wouwe (sé) Willem Debeuckelaere

Pour copie certifiée conforme :

Patrick Van Wouwe,
Chef de section OMR 12.12.2012

Annexe : Réflexions sur la distinction public-privé dans le cadre de la proposition de règlement protection des données COM(2012)11 du 25/01/2012

1.1. La question centrale est de savoir si un cadre légal, réglementaire distinct est nécessaire pour le secteur public et pour le secteur privé. On fait ici abstraction des besoins spécifiques pour la police et la justice étant donné qu'un autre instrument est de facto déjà proposé à cet effet[52].

1.2. Une telle approche doit être évitée autant que possible. Dans la mesure du possible, tous les règlements, tant les principes de base que l'élaboration concrète, doivent être harmonisés au maximum. C'est certainement valable pour les principes de base (les fondements du traitement, les principes de base, les droits de la personne concernée, le respect des règles de droit, l'échange international de données). Mais il faut également utiliser au maximum le même instrument et le même cadre juridique pour l'élaboration concrète, les procédures, le contrôleur indépendant, les exceptions, etc.

À ce jour, les principaux textes réglementaires internationaux en matière de protection de la vie privée et des données à caractère personnel ne font pas cette distinction et ont vocation à s'appliquer "tous secteurs confondus", public et privé.

Citons à cet égard la Convention 108 du Conseil de l'Europe (1981) dont l'article 3, § 1 (champ d'application) mentionne explicitement que "Les Parties s'engagent à appliquer la présente Convention aux fichiers et aux traitements automatisés de données à caractère personnel dans les secteurs public et privé". Cette application aux secteurs public et privé n'est en aucune façon remise en cause dans le cadre du processus de modernisation/révision de la Convention 108 actuellement en cours.

Le rapport explicatif de la Convention 108 explicite ce large champ d'application (points 33 et s.) :

"*Conformément au paragraphe 1, la Convention s'applique aux secteurs public et privé. Bien que la plus grande partie de la circulation internationale des données concerne le secteur privé, la Convention revêt une grande importance pour le secteur public et ceci pour deux raisons : tout d'abord l'article 3 impose aux États membres d'appliquer les principes de la protection des données même s'ils traitent des fichiers publics - comme c'est généralement le cas – entièrement à l'intérieur de leurs frontières nationales. Ensuite, la Convention offre assistance aux personnes*

[52] Ce qui va d'emblée engendrer de nombreux problèmes étant donné qu'aucune délimitation claire n'a été établie entre le monde de la police et de la justice et les acteurs privés qui y interviennent (avocats, notaires, huissiers de justice, sanctions administratives communales, surveillance privée, détectives privés, etc.). Un instrument légal sera quoi qu'il en soit nécessaire pour encadrer cela.

concernées qui souhaitent exercer leur droit d'être informées sur leur dossier détenu par une autorité publique dans un pays étranger.

La distinction secteur public/secteur privé ne se retrouve pas dans les autres dispositions de la Convention, notamment parce que ces notions peuvent avoir une signification différente d'un pays à l'autre. ***Mais elle peut jouer un rôle dans les déclarations que les Parties ont la faculté de faire pour ce qui est du champ d'application de la Convention (paragraphe 2)***".

Certains États ont fait usage de la faculté de dérogation au champ d'application de la Convention offerte par l'article 3 § 2 (voy. aussi le rapport explicatif ci-dessus), notamment pour certains fichiers relevant du secteur public[53]. Au vu des déclarations mentionnées en note, l'on constate que cette exclusion du champ d'application a eu lieu lorsque la loi nationale organisait un encadrement de ce type de fichiers (flexibilité pour le secteur public – rôle de la loi nationale).

Il est intéressant de relever que l'État belge n'en a pas faite en ce sens. Notons que la protection des données à caractère personnel n'en était à l'époque qu'à ses débuts (premier instrument juridique contraignant) et qu'il s'agissait d'une Convention internationale à "traduire" en droit interne".
Voy. déclaration de la Belgique du 28/05/1993
http://conventions.coe.int/Treaty/Commun/ListeDeclarations.asp?NT=108&CM=&DF=&CL=FRE&VL=0.

De la même manière, la directive européenne 95/46/CE couvre les secteurs public et privé (avec la nuance formulée ci-dessus au point 1.1. quant aux secteurs "police et justice" et aux domaines ne relevant pas de la compétence du législateur européen mais bien de la souveraineté nationale). Ceci ne figure pas littéralement et aussi explicitement que dans la Convention 108 mais se déduit de l'ensemble des dispositions de la directive. Voy. par exemple la définition du responsable de traitement qui inclut " l'autorité publique". Cette option n'est pas remise en cause dans la proposition de règlement de la Commission européenne. Elle n'a pas non plus été relevée comme posant difficulté dans les rapports d'évaluation de la même Commission.

---

[53] Pour des exemples de réserves concernant le "secteur public" : voy. La déclaration formulée par Andorre : pas d'application de la Convention "aux registres publics expressément régulés par la loi en Andorre". Le Liechtenstein a pour sa part exclu du champ d'application de la Convention les traitements opérés par l'Administration des Finances et ceux des Assemblées parlementaires et commissions (idem Suisse pour cette dernière dérogation). Voy. également la déclaration du Luxembourg qui exclut l'application de la Convention aux banques de données qui, en vertu d'une loi ou d'un règlement, sont accessibles au public. Les Pays-Bas ont pour leur part formulé la même réserve quant à de nombreux fichiers : archives désignées par la loi, fichiers destinés à l'application de la loi électorale, registre d'état civil, fichier central des étudiants de l'enseignement supérieur établi dans le cadre de la loi relative à l'enseignement universitaire [De nombreux États ont bien sûr, par ailleurs, plus classiquement, exclu les fichiers de données liés à la sûreté nationale, sécurité publique, infractions pénales]

Le choix de l'instrument par la Commission européenne, soit un règlement directement applicable, et non plus une directive à transposer en droit interne, intervient dans l'analyse également. Si la transposition que requiert une directive laissait, par nature, une certaine marge de manœuvre pour le législateur national, notamment pour d'éventuels traitements de données du secteur public, le caractère directement applicable d'un règlement ne permet pas ces nuances à moins pour le règlement de prévoir lui-même, en son sein, des dispositions spécifiques, nuancées ou suffisamment flexibles pour tenir compte des spécificités de ce secteur. La lecture de la proposition de règlement et les explications fournies par la Commissaire européenne V. Reding à son sujet indiquent que le texte a d'abord été pensé pour les entreprises, multinationales, dans un souci de simplification, de sécurité juridique, et de libre circulation des données dans un contexte de mondialisation. Reprenant le constat fait par le Conseil de l'Europe en 1981 déjà, selon lequel la plus grande partie de la circulation (internationale) des données concerne le secteur privé, les ambitions de l'UE font sens. Il n'en demeure pas moins qu'une certaine flexibilité au regard des traitements de données du secteur public – traitements très clairement identifiés et délimités - ne compromettrait pas la réalisation de ces objectifs pour le secteur privé. La protection des données à caractère personnel dans/par le secteur public, s'inscrirait dans le respect du règlement moyennant aménagements spécifiques et meilleure prise en compte de la règlementation nationale (plus traditionnellement applicable à ce secteur, à tout le moins davantage que le secteur privé).

1.3. Une des difficultés à laquelle on est systématiquement confronté lorsque l'on fait une telle distinction est la question du critère qui doit être appliqué. Travaillera-t-on de manière organique, ou préfère-t-on une approche matérielle ? Et qu'en est-il des institutions et missions intermédiaires (p&p). La jurisprudence du Conseil d'État et de la Cour de cassation (conflits d'attribution) concernant par exemple la question de savoir si des établissements d'enseignement libre sont ou non des autorités administratives est un bel exemple de discussion qui n'est pourtant jamais réellement tranchée : never ending story. Mais il y a bien entendu de nombreux autres exemples : sécurité sociale, soins de santé, …

2.1. Cela ne signifie pas que des institutions publiques, organes de gestion, administrations ou autres relèvent au sens strict de l'autorité publique ou, au sens large, qu'ils n'ont pas besoin de règlements propres. Le secteur public dispose de caractéristiques spécifiques propres à l'État : privilège du préalable, pouvoir d'exécution direct, droit de monopole, contrôle démocratique du législateur et du pouvoir exécutif, etc. Il faut en tenir compte lors de l'élaboration concrète des principes de base et il faut surtout tenir compte des procédures et des formes de contrôle et du respect des règles de droit.

2.2. Un autre aspect est la surveillance et la conservation de l'acquis : de nombreuses institutions publiques disposent d'un instrument affiné pour traiter des données à caractère personnel. Dans de

nombreux cas, ce traitement est également réalisé en vertu de règlements en matière de vie privée et de sécurité. Souvent, ces mécanismes sont satisfaisants, pour ne pas dire qu'ils fonctionnent très bien. Par exemple, on peut se référer à l'ensemble du fonctionnement de la Banque-carrefour de la Sécurité sociale. Remettre à présent ce système en question en faisant prévaloir tout simplement les fondements théoriques de la proposition de règlement UE sur le traitement de données à caractère personnel risque de donner lieu à de gigantesques problèmes administratifs et à la suppression d'un instrument affiné et opérationnel de protection des données à caractère personnel. De la même manière, voy. la Loi sur le Registre national et le Comité sectoriel d'autorisation, mécanisme de surcroît en conformité avec les exigences de la Directive 95/46/CE relatives à l'encadrement des traitements d'identifiants uniques (voy. infra).

2.3. On ne peut pas non plus ignorer les mérites de la Directive 95/46/CE : mettre purement et simplement de côté les qualités de cette directive n'a pas de sens. Par exemple : l'article 8, point 7[54] qui a constitué en Belgique la base de l'utilisation ultérieure du numéro de Registre national et de l'élaboration du Registre national lui-même. Bien entendu de manière légale et réglementée, notamment via le Comité sectoriel du Registre national. Il s'agit en la matière d'un instrument important dans le droit administratif et l'e-government, qui est avant tout destiné au secteur public[55].

Il ne s'agit que d'un exemple de la qualité de l'ancienne directive qui n'a à ce jour malheureusement pas été reprise dans la proposition européenne. Dans le cadre de règlements spécifiques pour des applications tant privées que publiques, il vaut la peine de pouvoir développer les acquis de la Directive 95/46/CE.

2.4. Respect des acquis et du contrôle démocratique. À cet égard, on peut se référer aux conventions collectives de travail belges rendues obligatoires qui, à partir de la concertation sociale, ont fourni d'importantes contributions à la protection de la vie privée et à son acceptation par les secteurs. Mais il en va de même par exemple pour la sécurité sociale : celle-ci est gérée par une représentation paritaire et sous le contrôle du Comité sectoriel de la Sécurité Sociale. La sphère de la protection de la vie privée regorge d'exemple de mécanismes de protection de la vie privée élaborés non pas par l'autorité au sens strict, mais par la société civile, des partenaires sociaux et l'ensemble des acteurs dans un secteur donné : voir en la matière le secteur de la santé. Remplacer ces acquis par des "delegated acts" constitue une destruction manifeste des acquis démocratiques. Voir à ce propos les articles 81 et 82 de la proposition UE.

---

[54] "*Les États membres déterminent les conditions dans lesquelles un numéro national d'identification ou tout autre identifiant de portée générale peut faire l'objet d'un traitement.*"

[55] Des autorisations sont accordées aux organismes publics et privés de droit belge pour les informations nécessaires à l'accomplissement de tâches d'intérêt général qui leur sont confiées par ou en vertu d'une loi, (…) ou de tâches reconnues explicitement comme telles par le comité sectoriel précité (article 5, premier alinéa, 2° de la loi du 8 août 1983 Registre national).

3. Problèmes concrets p&p dans l'actuelle proposition de règlement.

3.1. Article 6, 1, f (intérêt pondéré) : on ne comprend pas pourquoi actuellement l'article 6 relatif à la licéité du traitement exclut les "autorités publiques" pour ce motif de traitement. Le considérant 38 précise que "étant donné qu'il appartient au législateur de fournir la base juridique autorisant les autorités publiques à traiter des données, ce motif ne devrait pas valoir pour les traitements effectués par ces autorités dans l'accomplissement de leur mission". La motivation ne convainc pas la CPVP. Voir le raisonnement tenu dans le projet d'avis sur la proposition de règlement.

3.2. Quid de l'article 21 de la proposition.

3.3. L'article de la proposition qui suscite le plus d'inquiétude est l'article 34 : consentement et consultation préalables. Une application soutenue de l'esprit de cette disposition doit aboutir à l'interdiction de l'ensemble des autorisations préalables sur lesquelles repose le système des comités sectoriels et des contrôleurs régionaux. Le mécanisme de base est en effet une autorisation préalable après une demande du responsable du traitement, la constitution d'un dossier, le respect d'obligations de base (dont la sécurité), l'avis d'organismes de référence et l'appréciation par un organe de gestion à composition paritaire.

La "solution" qui consisterait pour la Commission belge de la protection de la vie privée à utiliser la faculté prévue à l'article 34 § 4 (mécanisme de consultation) ne peut, aux yeux des commissaires, apporter avec certitude en l'état du texte actuel, la même protection que le mécanisme des comités sectoriels existants.

L'article 34 § 4 prévoit que "L'autorité de contrôle établit et publie une liste de traitements devant faire l'objet d'une consultation préalable au titre du paragraphe 2 b). L'autorité de contrôle communique cette liste au Comité européen de la protection des données".

L'article 34 § 2 b) mentionne pour sa part que le responsable de traitement consulte l'autorité de protection des données "lorsque l'autorité de contrôle estime nécessaire de procéder à une consultation préalable au sujet de traitements susceptibles de présenter des risques particuliers au regard des droits et libertés des personnes concernées, du fait de leur nature, de leur portée et/ou de leurs finalités, ces traitements étant précisés conformément au paragraphe 4".

MAIS ….

- le système belge des autorisations des comités sectoriels n'est pas exclusivement fondé sur le risque (parfois même absence de risque ex. : CS Banque Carrefour des entreprises) mais également / surtout sur une approche sectorielle ;
- quant à la composition reflétant pour moitié le secteur concerné, l'on peut s'interroger sur la compatibilité de celle-ci avec l'article 47, § 3 (Indépendance) de la proposition de règlement qui mentionne que "les membres de l'autorité de contrôle (…) et, pendant la durée de leur mandat, n'exercent aucune activité professionnelle incompatible, rémunérée ou non" ;
- et SURTOUT, la liste de traitements que la CPVP adopterait (reflétant les compétences actuelles des Comités sectoriels) est, en application de l'article 58, § 2 c) soumis à l'avis du Comité européen de la protection des données et partant, à l'avis et une éventuelle mesure de suspension de la Commission européenne (articles 59 et s. chapitre relatif à la Coopération et au mécanisme de cohérence).

3.4. Article 51.2, compétence : le principe du guichet unique : cela pose des problèmes particuliers aux autorités, plus particulièrement dans le cadre de relations, de contrats, de collaborations au niveau d'entreprises et d'organisations internationales (p.ex. en matière d'ICT, notamment de cloud, de pharmaceutique, de finances, …). Étant donné que la DPA compétente ne sera généralement pas le contrôleur national, le problème se pose toutefois de savoir comment une commission vie privée étrangère pourra gérer la structure administrative et constitutionnelle propre à tous ces autres pays …

3.5. Chapitre IX, dispositions relatives à des situations particulières de traitement des données ; les articles 81, 82, dans une certaine mesure 83 et 85, notamment, posent des questions et des problèmes spécifiques pour le secteur public. À première vue, ils ouvrent des possibilités pour les autorités publiques d'intervenir dans certains domaines dans le cadre de leur mission de service public. Ces possibilités sont toutefois prévues comme un règlement d'exception ce qui, dans l'ensemble du concept du règlement, ne laisse aucune place pour d'autres domaines d'activité des autorités. En outre, la formulation de ces exceptions est tellement pointue et restrictive que celles-ci deviennent plutôt un carcan qu'une réelle possibilité d'intervention par les propres autorités publiques.

4. Un problème de base, qui dépasse de loin l'objectif de la présente note p&p, découle des prétentions totalitaires de la proposition de l'UE.

4.1. Le traitement de données à caractère personnel n'est pas une activité en soi. La protection des données à caractère personnel est un droit fondamental transversal et relatif par excellence.

Transversal car ce droit influe et doit être appliqué à la quasi-totalité des activités humaines. Relatif car ce droit n'est presque jamais isolé mais doit toujours être mis en équilibre avec d'autres droits et libertés.

4.2. La formulation d'un système absolu de protection des données à caractère personnel qui ne laisse (plus) aucune place à d'autres droits et libertés, ancrés dans la structure constitutionnelle, administrative et organisationnelle d'un état et d'une société risque dès lors de se heurter à ces autres fondements et droits fondamentaux.