Avis n° 10/2014 du 5 février 2014

Objet: Avis d'initiative portant 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, tel que voté par la Commission LIBE du Parlement européen le 17 octobre 2013 (CO-A-2014-001)

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 Monsieur Stefan Verschuere, Vice-président;

Émet, le 5 février 2014, l'avis suivant :

Résumé

Le 21 novembre 2012, la CPVP rendait d'initiative un avis critique 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* (ci-après « le projet de Règlement ») déposé par la Commission européenne.

Dans la lignée des objections et commentaires exprimés aux termes de cet avis 35/2012, la CPVP formule ci-dessous son point de vue au regard du projet de texte voté par la Commission chef de file « Libertés civiles, justice et affaires intérieures » (LIBE) du Parlement européen le 17 octobre 2013.

La CPVP souhaite attirer l'attention tant des parlementaires européens que des responsables politiques (belges) compétents - aujourd'hui et au lendemain des élections à venir – sur les implications des orientations prises par la Commission chef de file. Une attention toute particulière est apportée à certains concepts qui ne figurent pas dans le projet déposé par la Commission européenne (les données pseudonymes), qui revêtent une autre dimension aux yeux des parlementaires de la Commission LIBE (certification, BCR sous-traitants) ou qui font très largement débat au(x) niveau(x) du Conseil européen (profilage, principe du guichet unique « one-stop-shop » et voies de recours, traitements à des fins de recherche historique, statistique et scientifique).

Une protection renforcée des droits des personnes concernées ? Un des objectifs déclarés de la réforme de la protection des données est le renforcement des droits des personnes concernées, plus particulièrement à l'ère du numérique omniprésent et face aux géants (européens et non européens) de l'Internet. Dans son avis 35/2012, la CPVP a d'emblée émis des doutes sur le renforcement réel qui serait apporté par le projet de Règlement, en particulier par rapport à l'acquis de la directive 95/46/CE.

Une protection réelle passe bien sûr par le contenu du droit mais aussi par sa mise en œuvre effective (notamment praticable pour les responsables de traitement) et, *in fine*, par les moyens accessibles mis à la disposition de la personne concernée pour les faire valoir tant auprès du responsable de traitement qu'auprès de l'autorité de contrôle et des instances judiciaires. A l'appui de ce postulat, la CPVP formule les commentaires ci-après.

I. Un champ d'application adéquat

1. Les traitements de données réalisés dans le cadre de l'utilisation des réseaux sociaux ne peuvent totalement échapper à l'application du projet de Règlement. *Son champ d'application matériel* doit les inclure et la portée de l'exception pour les activités purement personnelles et domestiques définie de manière à les couvrir (points 6 et s.)

2. La CPVP s'oppose à l'insertion de la notion de *« données pseudonymes »*, qu'elles soient le résultat d'un codage ou un moyen d'identification dans l'environnement numérique. L'insertion d'une

sous-catégorie de données personnelles dans le projet de Règlement complique davantage l'interprétation des notions actuelles de « données à caractère personnel » et « données anonymes », sur lesquelles repose le régime en vigueur. En prévoyant par ailleurs un régime de protection indistinctement « allégé » pour cette catégorie de données à caractère personnel, la réforme envisagée aboutirait à un inacceptable affaiblissement du niveau de protection garanti (points 9 et s.).

II. Des définitions adéquates

3. 3. La CPVP plaide pour une définition des données relatives à la santé qui tienne compte du contexte dans lequel intervient le traitement de telles données (points 15 et s.). S'agissant de leur traitement à des fins thérapeutiques, elle s'oppose à l'obligation imposée aux Etats membres d'adopter une législation spécifique permettant le traitement (points 129 et s.).

III. Un régime dérogatoire adéquat

4. La Commission LIBE réduit les possibilités d'exemptions à l'application du Règlement, que ce soit par la voie des articles auxquels il peut être dérogé ou par le biais des motifs pour lesquels l'Etat membre peut instaurer un régime dérogatoire. A cet égard, la CPVP alerte le lecteur sur la suppression du motif « intérêt général de l'Union ou d'un Etat membre » et sur son remplacement par les seules « taxation matters » (points 56 et s.).

IV. Des droits effectifs, renforcés (ou au minimum préservés par rapport à l'acquis de la directive 95/46/CE) pour les personnes concernées

5. La CPVP accueille favorablement les modifications apportées par la Commission LIBE quant au contenu de l'*information* des personnes concernées, tout particulièrement en ce qui concerne le délai de conservation des données, les mesures de sécurité mises en place, la logique qui préside aux traitements, les éléments relatifs au profilage et les garanties entourant les flux transfrontières. Elle n'est par contre pas convaincue de la valeur ajoutée des pictogrammes proposés. Elle s'oppose enfin à la suppression de l'exercice de certains droits des personnes concernées dans les cas où le responsable de traitement serait soumis au secret professionnel (points 18 et s.).

6. La CPVP regrette que la suppression des termes « droit à l'oubli » à l'intitulé de l'article 17 ne s'accompagne pas de davantage de *clarification quant à la portée exacte du droit à l'effacement* que cet article consacre. En particulier, la CPVP est d'avis que l'obligation pour les responsables de traitement de contacter tous les tiers qui auraient légalement rediffusé les données initialement traitées sera difficilement praticable (points 24 et s.)

7. La CPVP relève que la Commission LIBE n'apporte pas de correctif complet à l'affaiblissement du *droit d'opposition*. En effet, le droit d'opposition prévu par la Loi Vie privée (LVP) disparaît dans les cas où le consentement de la personne concernée constitue la base légale du

traitement de données. La balance des intérêts à opérer par le responsable de traitement lui-même - laquelle peut l'amener à refuser à la personne concernée l'exercice d'un droit – crée le risque inacceptable de voir les responsables de traitement continuellement invoquer leur intérêt légitime pour s'opposer à l'exercice du droit d'opposition (points 31 et s.).

8. Quant à l'encadrement proposé du *profilage*, la CPVP plaide pour un régime de protection qui encadre à la fois les traitements basés sur un profil constitué *et* les décisions individuelles automatisées actuellement visées par l'article 15 de la directive 95/46/CE. Quant au profilage à proprement parler, la création d'un profil d'une part et l'application de profils d'autre part devraient tous deux être règlementés, dans l'esprit de la Recommandation du Conseil de l'Europe relative au profilage, en ce compris dans le « droit à l'anonymat » qu'elle introduit (points 33 et s.).

9. La CPVP regrette la réduction de l'obligation de *documentation* à un strict minimum. L'obligation ainsi conçue n'amène plus le responsable de traitement à se poser les questions pertinentes au regard des traitements envisagés comme c'est le cas avec l'obligation actuelle de déclaration à laquelle elle entend se substituer. La CPVP est d'avis que la documentation devrait, au minimum, inclure, outre les données de contact des responsables de traitement, sous-traitants, représentant et délégué à la protection des données éventuels et destinataires des données, une description de la finalité des traitements et les catégories de données traitées (points 60 et s.).

10. La CPVP demande que le *système des comités sectoriels et leur compétence d'autorisation* de certains traitements spécifiques de données puisse être maintenu aux termes de la nouvelle règlementation européenne. Elle est en effet convaincue que le travail d'analyse de ces comités est essentiel et que les conditions posées dans leurs autorisations encadrent de manière adéquate les flux de données du secteur public (principalement). Elle plaide avec insistance pour le maintien de ce mécanisme bénéfique à la protection de la vie privée et des données à caractère personnel des citoyens (points 68 et s.).

11. En d'autres termes, la CPVP regrette qu'il n'ait pas été tenu compte de la pratique et de l'expérience positive de certaines autorités de protection des données dans l'application de leur règlementation nationale. Outre le mécanisme des autorisations délivrées par les comités sectoriels évoqué ci-dessus, la CPVP déplore la disparition de la disposition de la directive 95/46/CE actuellement en vigueur qui permet d'encadrer l'accès et l'utilisation du *numéro de registre national*. Elle plaide pour le possible maintien de cette règlementation (points 127 et s.).

12. Forte de son expérience en la matière, la CPVP propose également un certain nombre d'amendements à l'encadrement de la *recherche historique, statistique et scientifique* qui tendent à trouver le juste équilibre entre les intérêts des chercheurs d'une part et le nécessaire respect de la protection de la vie privée et des données à caractère personnel dans ce secteur d'autre part (points 131 et s.).

13. Quant aux *instances et voies de recours accessibles* à la personne concernée, la CPVP ne peut soutenir la traduction du principe du guichet unique en l'état (voy. infra). Ce principe s'accompagne d'une multiplicité de recours administratifs et judiciaires possibles pour la personne concernée, tant dans l'Etat membre dans lequel il réside habituellement qu'à l'étranger. Selon la CPVP, la complexité du système des voies de recours offertes par le projet de Règlement - notamment dans sa version votée par la Commission LIBE - n'offre pas de garanties suffisantes pour lui permettre de considérer que les articles 16 TFUE, 8 et 47 de la Charte des droits fondamentaux de l'Union et 6 (accès au tribunal) et 13 (recours effectifs) de la Convention européenne des droits de l'homme sont pleinement mis en œuvre (points 115 et s.).

14. La CPVP accueille favorablement la tentative de la Commission LIBE d'apporter une solution aux transferts de données vers des pays tiers non adéquats, du type notamment de ceux révélés par l'affaire SWIFT (et ses transferts de données vers l'UST (US Treasury des Etats-Unis)) ou encore plus récemment par les révélations d'E. Snowden relatives aux vastes programmes de surveillance des services secrets américains (NSA – National Security Agency). La CPVP s'oppose par contre au rôle qu'on voudrait y voir jouer les autorités de protection des données, notamment d'autoriser de tels transferts et émet de sérieux doutes sur l'opportunité et la praticabilité – tant d'un point de vue pratique que légal – de l'information individualisée à la personne concernée par de tels transferts (points 95 et s.)

V. Des obligations praticables pour les entreprises et bénéfiques à la protection des données des personnes concernées – risk based approach

15. Comme dans son avis 35/2012, la CPVP plaide pour un système d'obligations cohérentes et basées sur l'appréciation concrète du risque réel induit par les traitements réalisés.

16. La CPVP est d'avis que les *violations de données (data breach)* à notifier – que ce soit à l'autorité de protection des données ou à la personne concernée – ne sont pas (suffisamment) définies. Ce déficit de précision risque de rendre, dès leur conception, ineffectives cette obligation et l'information corrélative utile qu'elle se veut apporter à l'autorité de contrôle et à chacun (points 62 et s.).

17. La CPVP soutient le déploiement de la fonction de *délégué à la protection des données* pour autant que la désignation d'un tel délégué reste une faculté pour le responsable de traitement. Telle fonction doit être conçue comme une mesure d'accountability dont le responsable de traitement doit rester libre de faire le choix compte tenu des traitements opérés, des risques réels, de l'existence d'autres mécanismes de protection et du bénéfice réel pour la protection des données qu'elle apporterait. Partant, la CPVP ne peut souscrire à l'orientation de la Commission LIBE qui étend plus encore les cas dans lesquelles cette désignation d'un délégué est obligatoire, *a fortiori* dans des

hypothèses fondées sur des critères de risque qui ne lui apparaissent pas pertinents (points 76 et s.).

18. Dans la même optique de soutenir les incitants à la diffusion et la mise en place d'une véritable culture de la protection des données en entreprise, la CPVP regrette que la Commission LIBE omette *les BCR sous-traitants* (Binding Corporate Rules for processors). Ces règles apportent un haut niveau de protection des données dans les cas de transferts de données traitées à l'origine par un groupe multinational en tant que sous-traitant. S'opposer à celles-ci ne fait que créer de l'insécurité juridique et pousser les entreprises à opter pour des outils moins protecteurs qui n'offrent pas cet avantage qu'ont les BCR de promouvoir nos règles européennes à l'étranger (points 86 et s.).

19. La CPVP insiste pour que les critères et exigences applicables aux mécanismes de *certification*, y compris les conditions d'octroi, de révocation et les conditions de reconnaissance au sein de l'Union et dans les pays tiers ainsi que les critères d'accréditation des certificateurs soient déterminés par les autorités de protection des données. A ces conditions seules, elle pourrait admettre que la certification intègre la liste des garanties adéquates de protection autorisant un flux de données vers un pays tiers non-adéquat au même titre que les clauses contractuelles types ou les BCR. Elle est par contre opposée à un régime de sanction allégé pour les entreprises certifiées qui se rendraient coupables d'un manquement au projet de Règlement (points 75-81 et 85).

VI. Une autorité de protection des données accessible

20. Quant à son propre rôle, la CPVP est d'avis qu'il est très certainement amené à évoluer, quel que soit le sort réservé à la proposition de Règlement déposé par la Commission européenne. Plusieurs commentaires ci-dessus soulignent certaines préoccupations de la CPVP quant au rôle qu'on voudrait lui voir jouer, quant aux compétences qu'on voudrait lui confier (certification, autorisation de certains transferts de données en – dehors de l'Union européenne (article 43a)), suppression de la compétence d'autorisation de flux de données dans le secteur public). Son indépendance est à préserver de même que sa vocation à sensibiliser comme à guider et assister le grand public et les entreprises.

21. Quant aux *sanctions*, la CPVP est particulièrement soucieuse de préserver l'objectif premier de son travail, soit la mise en conformité de traitements réalisés avec les exigences de la règlementation en matière de protection des données. A l'appui de son expérience, elle privilégie la médiation à la sanction, tout particulièrement pour des raisons liées au nécessaire respect du principe de la séparation des pouvoirs. Les montants, fussent-il maximaux, excessivement élevés des amendes administratives prévues par la Commission LIBE la confortent dans cette prise de position (points 123 et s.).

22. Enfin, la CPVP est convaincue qu'une coopération régulière et structurée entre autorités de protection (européennes) des données est indispensable. Elle privilégie toutefois la création d'une *autorité européenne de protection des données* (bénéficiant de la personnalité juridique, établie au niveau de l'Union européenne et dont les décisions s'imposeraient à l'ensemble des Etats de l'Union) dans les cas de traitements « transfrontières » (soit des traitements communs à plusieurs Etats membres de l'Union). A cet égard, elle est favorable au renforcement du rôle du Comité européen de la protection des données (CEPD – points 109 et s.), en ce compris dans la préparation des actes délégués (points 141 et s.). Subsidiairement, le concept d'autorité chef de file associé à une procédure de co-décision lui semble davantage défendable que celui d'un guichet unique dont le rôle serait confié à la seule autorité du lieu de l'établissement principal du responsable de traitement et dont les décisions s'imposeraient à toutes les autorités de protection des données concernées. L'autorité de protection des données doit rester un interlocuteur de proximité, tout particulièrement pour les citoyens qui voudraient déposer plainte (points 104 et s.).

TABLES DES MATIERES

I. Introduction, rétroactes, portée et objectif du présent avis

1. Le 21 novembre 2012, la CPVP rendait d'initiative un avis critique 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* (règlement général sur la protection des données – ci-après « le projet de Règlement ») déposé par la Commission européenne le 25 janvier 2012.

2. Dans la lignée des objections et commentaires exprimés aux termes de cet avis 35/2012, la CPVP formule ci-dessous son point de vue au regard du projet de texte voté - dans le cadre de la procédure de co-décision -, le 17 octobre 2013 par la Commission chef de file « Libertés civiles, justice et affaires intérieures » du Parlement européen (ci-après la Commission LIBE).

3. La CPVP ne procède pas à un examen systématique de chacun des très nombreux amendements votés par la Commission LIBE. Son analyse ne prétend pas être exhaustive.

4. La CPVP n'en souhaite pas moins attirer l'attention tant des parlementaires européens que des responsables politiques (belges) compétents – aujourd'hui et au lendemain des élections à venir – sur les implications des orientations prises par la Commission chef de file. Une attention toute particulière est apportée à certains concepts qui ne figurent pas dans le projet déposé par la Commission européenne (les données pseudonymes), qui revêtent une autre dimension aux yeux des parlementaires européens (certification, BCR « sous-traitants ») ou qui font très largement débat au(x) niveau(x) du Conseil européen (profilage, principe du guichet unique « one-stop-shop » et voies de recours, recherche historique, scientifique et statistique). La CPVP suit en effet de très près les débats européens sur le document, assurant un soutien technique indépendant à la Ministre de la Justice et au SPF en particulier lors des réunions du groupe de travail DAPIX (Groupe de travail sur l'échange et la protection des données).

5. Comme déjà mentionné, les commentaires qui suivent s'inscrivent dans la continuité de ceux exprimés par la CPVP au regard du projet de Règlement déposé par la Commission européenne dans son avis 35/2012. Le cas échéant il y est ici explicitement renvoyé.

II. Analyse de certaines dispositions et concepts-clé

1. Chapitre I : Dispositions générales

1.1. Champ d'application matériel (article 2)

6. La Commission LIBE considère que l'exception concernant les activités purement personnelles et domestiques couvre également les publications de données dont on peut raisonnablement s'attendre à ce qu'elles ne soient accessibles qu'à un nombre limité (limited) de personnes.

7. Cette position rejoint la jurisprudence de l'arrêt Linqvist de la Cour de Justice de l'Union européenne[1] et permet de considérer, par exemple, que les traitements réalisés par les particuliers dans le cadre de leur utilisation des réseaux sociaux sont *inclus* dans le champ d'application du projet de Règlement, lorsque les informations sont rendues accessibles à un nombre indéterminé de personnes. Bien que la mise en œuvre concrète de l'ensemble des obligations du projet de Règlement par les particuliers puisse poser certains problèmes pratiques, la CPVP soutient néanmoins l'idée de principe selon laquelle ces traitements devraient rester dans le champ d'application du droit de la protection des données personnelles. Le cas échéant, un régime adapté à la spécificité des réseaux sociaux et tenant compte du respect dû à la liberté d'expression et d'information, pourrait être organisé.

8. Compte tenu des risques induits par l'utilisation des réseaux sociaux, de la perte de maîtrise informationnelle en particulier, et des conséquences dommageables de ces traitements de données (que corroborent le nombre et la nature des plaintes reçues par la CPVP dans ce domaine), il serait impensable pour la CPVP que ceux-ci sortent totalement du champ d'application de la règlementation en matière de protection des données personnelles et que les personnes concernées n'aient, partant, plus aucun recours à ce titre.

1.2. Données pseudonymes (article 4. 2a)

9. La Commission LIBE introduit la notion de « données pseudonymes » à l'article 2a) en les définissant comme *« personal data that cannot be attributed to a specific data subject without additional information, as long as such aditional information is kept separately and subject to technical and organisational measures to ensre non-attribution »*. La Commission

[1] Affaire C-101/01, CJUE, 6 novembre 2003.

LIBE prévoit également un certain nombre de conditions particulières du traitement de telles données (voy. ci-dessous), notamment des dérogations qui appellent de la part de la CPVP les réflexions et commentaires suivants.

Le concept de données pseudonymes : une réalité mutiple

10. L'identification d'une personne ne se limite pas à la simple possibilité de connaître son identité civile (nom, prénom, adresse,…) mais comprend également la **faculté de pouvoir la distinguer ou la singulariser parmi les autres** personnes (*the person is « singled out »*). En effet, dans le régime de protection des données personnelles, les individus doivent être protégés dès qu'ils peuvent être singularisés puisque dès ce moment, ils peuvent être traités de manière personnalisée/différenciée, avec un risque de discrimination. Selon la CPVP, **la notion de données pseudonymes recouvre en réalité des situations très différentes** :

11. *La pseudonymisation de données (par exemple les données codées) :* les données relatives à l'identité civile d'une personne sont remplacées par un alias ou un code. Ce processus de minimisation est fréquemment utilisé dans le cadre de la recherche scientifique dont l'**objectif particulier est, non pas de prendre des mesures individualisées** envers l'une ou l'autre personne en particulier mais bien d'accroître **les connaissances globale de la société. La poursuite de cet objectif légitime a justifié un régime distinct adapté** dans la réglementation actuelle (directive 95/46/CE et Loi Vie privée). L**a pseudonymisation**[2] **rencontre dans ce contexte les exigences de proportionnalité :** lorsqu'il n'est pas possible en pratique de réaliser l'objectif de recherche poursuivi au moyen de données anonymes[3], le recours à la pseudonymisation est admis .

12. *Les pseudonymes « numériques » comme forme alternative d'identification :* le développement de la société de l'information permet à des sociétés privées de singulariser des individus sans avoir pour autant besoin de connaître leur identité civile. Il est fait usage d'autres identifiants (un login, un code lié au téléphone, à l'ordinateur, à une carte à puce ou l'empreinte digitale). Ces identifiants permettent d'obtenir et de rassembler des informations précises sur les habitudes de consommation, les déplacements, l'emploi, le

[2] La pseudonymisation a été définie dans l'ISO 29100 : *"pseudonymization : process applied to personally identifiable information (PII) which replaces identifying information with an alias. Note 1 to entry: Pseudonymization can be performed either by PII principals themselves or by PII controllers. Pseudonymization can be used by PII principals to consistently use a resource or service without disclosing their identity to this resource or service (or between services), while still being held accountable for that use. Note 2 to entry: Pseudonymization does not rule out the possibility that there might be (a restricted set of) privacy stakeholders other than the PII controller of the pseudonymized data which are able to determine the PII principal's identity based on the alias and data linked to it"*.

[3] Voir le Chapitre II de l'Arrêté royal du 13/2/2001 exécutant la Loi Vie privée.

niveau de vie etc. … des personnes qui sont singularisées. **Ces traitements ont directement pour finalité de traiter les individus de manière individuelle**, en leur communicant une information personnalisée, en leur offrant un prix différencié, en leur permettant ou non l'accès à certains services.

Un régime de protection indistinctement allégé ? Rejet de la CPVP

13. Dans les deux cas de figure, les données pseudonymes sont des données personnelles. Cette qualification importante ressort de la définition donnée par la Commission LIBE et est, aux yeux de la CPVP, essentielle. **La CPVP rejette cependant l'idée d'inclure une définition de « donnée pseudonyme » dans la nouvelle règlementation et ce, pour deux raisons principales :**

- Inclure une nouvelle notion de donnée pseudonyme distincte de la définition des données à caractère personnel - alors même que la donnée pseudonyme est une donnée à caractère personnel - ne fera qu'ajouter de la confusion à l'interprétation des notions de données personnelles et anonymes ;

- Certains amendements (voy. ci-dessous) proposent de soumettre *de manière générale* les données pseudonymes à un régime de protection allégé (un « régime light »), ce qui, aux yeux de la CPVP, est tout simplement inacceptable. Si le contexte particulier de la recherche peut justifier un régime adapté, le cas échéant dérogatoire sur certains aspects, de telles dérogations ne se justifient pas, bien au contraire, pour l'ensemble des données pseudonymes. L'identité numérique doit, selon la CPVP, bénéficier de la même protection que l'identité civile ou traditionnelle. Il est essentiel que les traitements visés au point 12 ci-dessus soient pleinement soumis au droit de la protection des données, garantissant notamment la mise en balance des intérêts en présence et la transparence vis-à-vis des individus.

  Sur ce dernier point, la CPVP vise en particulier le considérant 38 tel que voté par la Commission LIBE qui prévoit que les traitements de données pseudonymes sont, *ipso facto*, considérés comme rencontrant les attentes raisonnables des personnes concernées, ce qui pourrait conduire à faire l'économie de la balance des intérêts en présence prévue à l'article 6.1.f du projet de Règlement. Le considérant 58a soulève le même problème en soulignant que les profilages réalisés exclusivement par le traitement de données pseudonymes devraient être présumés comme n'affectant pas de manière significative les droits ou libertés des personnes concernées. La pseudonymisation des données n'est en effet qu'une mesure d'ordre technique qui peut être prise en considération lors de la mise en balance des intérêts

en présence, mais qui ne peut en soi justifier l'économie de l'analyse des autres éléments contextuels du traitement (voy. également ci-dessous le point 54 au regard de l'article 20 consacré au profilage).

1.3. Notion de « Profilage » (article 4.3a)

14. Absente de la proposition originale de la Commission européenne, cette notion clé à l'ère du numérique et des entrepôts de données, est définie par la Commission LIBE. Il est renvoyé sur cet aspect à l'analyse de l'article 20 qui traite de l'encadrement du profilage (points 39-44).

1.4. Définition des données de santé (article 4.12)

15. Dans son avis de 2012, la CPVP attire l'attention sur le fait que, dans la proposition de la Commission européenne, la définition de "données relatives à la santé" est (beaucoup) trop large et ne tient pas suffisamment compte des contextes multiples dans lesquels les traitements de telles données peuvent intervenir[4]. La définition retenue par la Commission LIBE pose exactement le même problème. Pour ne prendre qu'un seul exemple : imaginons que des images vidéo de caméras de surveillance montrent qu'une personne a une jambe cassée ; sur la base de la définition du texte voté par la Commission LIBE, il s'agit là d'un traitement de données relatives à la santé et ce traitement doit faire l'objet d'un régime de protection particulier.

16. Afin d'éviter de telles situations absurdes, la CPVP plaide pour une règlementation aux termes de laquelle l'accent est mis sur le traitement ainsi que sur la finalité de ce traitement (et pas sur la nature des données traitées)[5]. De cette façon, beaucoup moins de traitements relèveront de l'interdiction de principe de traitement, ce qui permettra de limiter cette interdiction de traitement aux cas où les traitements impliquent un risque réel. Concrètement, la CPVP propose la formulation suivante :
"Article 4 (12) "données concernant la santé" : toute information relative à la santé physique ou mentale passée, actuelle ou future de la personne concernée ;"

---

[4] Points 23-25 de l'avis n° 35/2012.

[5] Cela permettrait de rejoindre la conception du traitement de données concernant la santé dans le cadre de la modernisation de la Convention n° 108. Une alternative consisterait, sans toucher au principe d'une définition « par nature », à tenir compte du contexte dans la détermination des *conditions* auxquelles ces traitements de données relatives à la santé pourraient avoir lieu.

"Article 9, point 1. Le traitement des données à caractère personnel visant à révéler (…) des données concernant la santé (…) sont interdits."[6]

2. Chapitre III :Droits de la personne concernée

17. Avec la réforme qu'elle propose, la Commission européenne affirme avoir pour ambition de renforcer les droits des personnes concernées à l'ère du numérique. Dans son avis 35/2012, la CPVP démontre toutefois que cet objectif n'est pas toujours rencontré ; ni par certaines nouvelles dispositions ni par certains amendements apportés aux droits existants. De manière générale, la CPVP est opposée à tout recul des droits consacrés par la directive 95/46/CE et tels que transposés en droit belge par la Loi Vie privée (LVP). C'est à l'aune de cette préoccupation qu'elle formule les remarques ci-dessous au regard des orientations prises par la Commission LIBE.

2.1. Droit à l'information (articles 13a et 14)

18. La CPVP soutient les modifications apportées par la Commission LIBE quant au contenu de l'information à donner aux personnes concernées en ce qui concerne plus spécifiquement : le délai de conservation des données (qui peut être désormais déterminé de manière souple par référence à certains paramètres et non plus uniquement en termes de durée quantifiée – article 14.1.c)), les mesures de sécurité mises en place (article 14.1.b)), la logique qui préside au traitement (article 14.1.gb)), les éléments d'information spécifiques en cas de profilage (article 14.1.ga) – voy. toutefois la demande de précision exprimée au point 45 ci-dessous), les garanties encadrant les flux transfrontières de données (article 14.1.g)) et l'information selon laquelle des données ont été communiquées au cours des 12 mois précédents à une autorité publique dans le cadre de l'article 43a) (voy. ci-dessous au point 100 pour cet élément particulier).

19. A l'inverse, la CPVP émet de sérieux doutes sur la valeur ajoutée en termes d'information réelle à la personne concernée, des 6 pictogrammes dont la communication est exigée du responsable de traitement en sus des éléments visés à l'article 14 (article 13a)). Outre le fait qu'ils représentent une charge administrative indéniable pour le responsable de traitement, les 3 premiers pictogrammes impliquent une auto-évaluation nécessairement positive par le responsable de traitement (à défaut ce dernier serait en contradiction avec les obligations auxquelles il est tenu par le projet de Règlement) alors que les 3 pictogrammes suivants

[6] Remarque : si cette approche devait être retenue, les considérants y afférents devraient également être revus (voir par exemple le considérant 26).

sont destinés à donner une information factuelle à la personne concernée. Cette double perspective est, selon la CPVP, de nature à prêter davantage à confusion qu'à éclairer utilement la personne concernée.

20. La CPVP a pu constater que les responsables de traitement tenus au secret professionnel avancent souvent leur obligation audit secret pour tenter de se dispenser de l'application de la Loi Vie privée, en particulier quant aux droits de la personne concernée et la compétence de contrôle de la CPVP. Si le secret professionnel, comme la règlementation relative à la protection des données protègent la confidentialité des données, la seconde va bien au-delà de la préservation de la confidentialité (notamment dans ses principes de finalité, de proportionnalité, de sécurisation des données etc.).

21. Partant, la CPVP accueille favorablement la tentative de la Commission LIBE de concilier les exigences du secret professionnel (qui peut cependant varier d'un Etat Membre à l'autre) avec celles la protection des données.

22. Toutefois, la manière dont la Commission LIBE tente de prendre en compte l'obligation de secret professionnel auquel serait tenu un responsable de traitement est également insatisfaisante et introduit, aux yeux de la CPVP, une exception très largement injustifiée au droit à l'information (article 14.5.da)). Supprimer le droit à l'information, fut-ce uniquement en cas de collecte indirecte, à la personne concernée au motif que le responsable de traitement est soumis au secret professionnel ou à toute autre obligation au secret paraît, sans autres nuances, indéfendable. En droit belge à tout le moins, l'opposabilité du secret professionnel vise *les tiers* et non la personne qui se confie elle-même. Que la collecte soit en ce cas directe ou indirecte est, a priori, sans incidence ; le secret professionnel interdit, sauf exceptions, la *communication* à des *tiers* des données couvertes par ledit secret. De manière générale, la CPVP plaide pour une disposition qui concilie « protection des données » et « secret professionnel » ; l'assujetti au secret professionnel ne pouvant être amené, au nom de la mise en oeuvre de la règlementation en matière de protection des données, à enfreindre son obligation au secret.

2.2. Droit d'accès et portabilité des données (article 15)

23. La CPVP salue la clarification apportée par la Commission LIBE quant au droit d'accès d'une part et la portabilité des données d'autre part.

2.3. Droit à l'effacement (article 17)

24. La CPVP constate avec satisfaction que l'intitulé de l'article 17 a été modifié : le texte de la Commission LIBE ne mentionne plus le titre « droit à l'oubli numérique et à l'effacement », mais uniquement « droit à l'effacement». Cette modification répond aux vœux exprimés par la CPVP dans son avis 35/2012. Elle y estime que le droit à l'oubli et le droit à l'effacement doivent être clairement distingués. En effet, alors que le droit à l'effacement des données quand leur traitement n'est pas conforme aux dispositions applicables va de soi, la question demeure de savoir quels seraient les droits et obligations supplémentaires qu'emporterait l'introduction d'un droit à l'oubli.

25. Cette dernière notion ne reçoit pas la même acception dans les différents ordres juridiques. De plus, elle est souvent d'ordre jurisprudentiel et non formellement consacrée par la loi ; elle concerne le plus souvent le secteur de la presse et les données judiciaires et son champ d'application est incertain[7].

26. La CPVP considère que le texte tel que modifié par la Commission LIBE ne résout pas les problèmes que le texte proposé par la Commission européenne soulève. En effet, la nouvelle disposition ne clarifie pas si l'article 17 instaure un nouveau droit, ou ne fait qu'aménager le droit à l'effacement de données illicitement traitées (et une obligation corollaire). De plus, la CPVP est d'avis qu'il sera difficile de mettre en pratique l'obligation pour les responsables de traitement de contacter tous les tiers qui auraient légalement rediffusé des données ayant elles-mêmes fait l'objet d'une première publication licite.

27. La compatibilité et l'effectivité de ce droit à l'effacement que la personne concernée peut exercer auprès de tiers doivent également être examinées au regard de la directive 2000/31 sur le commerce le électronique, laquelle prévoit notamment l'interdiction de prévoir des mesures générales de surveillance à l'égard des intermédiaires de la société de l'information, comme les moteurs de recherche par exemple[8].

---

[7] Cela ressort notamment de l'affaire pendante actuellement devant la CJUE (Affaire C-131/12, Google c. Agence Espagnole de Protection des Données), dans le cadre de laquelle l'avocat général a rendu un avis qui concluait non seulement que le régime actuel de la directive 95/46 ne consacre pas l'existence d'un droit à l'oubli, mais en outre s'interrogeait sur la qualité des moteurs de recherches, lesquelles ne pourraient être considérés comme des responsables de traitement au sens de la directive 95/46.

[8] Le considérant n°17 du projet de Règlement dispose que Le présent règlement devrait s'appliquer sans préjudice de la directive 2000/31/CE, et notamment de ses articles 12 et 15 relatifs à la responsabilité des prestataires intermédiaires. Toutefois, des difficultés d'application simultanée des deux textes ne sont pas à exclure. Voy. à ce sujet l'arrêt de la C.J.U.E. Sabam c. Tiscali, aff. C-70/10, 24 novembre 2011 qui confirme que le droit européen, et notamment la directive 2000/31 précitée s'oppose à une injonction faite à un fournisseur d'accès à Internet de mettre en place un système de filtrage de toutes les communications électroniques transitant par ses services, notamment par l'emploi de logiciels «peer-to-peer», qui s'applique indistinctement à l'égard de toute sa clientèle, à titre préventif, à ses frais exclusifs, et sans

28. Enfin, la différence entre les deux hypothèses visées par l'article 17.1 et 17.2 n'est pas évidente : en effet, la nouvelle version de l'article 17.1, tel que modifié par la Commission LIBE, ajoute les tiers comme destinataires de l'obligation d'effacement, en plus du responsable de traitement. Ces tiers étaient déjà visés par l'article 17.2, mais cette disposition prévoit que le responsable du traitement doit prendre toutes les mesures raisonnables pour procéder à l'effacement des données, y compris par les tiers. Il semble donc que les tiers n'ont, dans cette hypothèse, pas d'obligation *directe* de procéder à l'effacement des données.

29. Pourtant, le nouvel article 17.3 prévoit que le responsable du traitement, mais également les tiers, doivent procéder à l'effacement des données sans délai, sauf dans les cas mentionnés au même article. Il semble donc que l'obligation d'effacement s'adresse aux tiers que l'on soit dans l'hypothèse de l'article 17.1 (données initialement publiées sans justification légale) ou dans l'hypothèse de l'article 17.2 (données rendues publiques par le responsable du traitement sans aucune justification fondée sur l'article 6.1).

30. Pour ces raisons, la CPVP est d'avis que le régime instauré par l'article 17 n'est pas clair et manque de cohérence, ce qui rend son application encore moins aisée.

2.4. Droit d'opposition et marketing direct (article 19)

31. Dans son avis 35/2012 (points 75-78), la CPVP met en évidence qu'avec l'entrée en vigueur du projet de Règlement, le droit d'opposition prévu par la Loi Vie privée (LVP) disparaît dans les cas où le consentement de la personne concernée constitue la base légale du traitement de données. Le texte voté par la Commission LIBE n'apporte aucun correctif à cet affaiblissement des droits de la personne concernée.

32. Les hypothèses dans lesquelles le responsable de traitement a la faculté d'établir l'existence de raisons impérieuses et légitimes justifiant le traitement et qui priment les intérêts ou libertés et droits fondamentaux des personnes concernées sont certes réduites : lorsque le traitement est fondé sur l'article 6(1) f) tel que voté par la Commission LIBE (soit le traitement fondé sur l'intérêt légitime du responsable de traitement), le droit d'opposition est formulé de manière inconditionnelle. S'agissant du marketing direct qui serait reconnu comme un intérêt légitime au sens de l'article 6 (1) f), la possibilité pour le responsable de traitement de refuser l'exercice du droit d'opposition n'existe plus. Néanmoins, dans les cas

---

limitation dans le temps. L'efficacité dans le temps d'une demande d'effacement sera réduite si le tiers ne doit plus, après l'effacement des données, s'assurer que l'information litigieuse ne réapparaisse.

où elle subsiste, cette balance des intérêts à opérer par le responsable de traitement lui-même au regard de l'exercice d'un droit *de* la personne concernée crée, aux yeux de la CPVP, le risque inacceptable de voir les responsables de traitement continuellement invoquer leur intérêt légitime pour s'opposer au droit d'opposition exercé par la personne concernée.

2.5. Profilage

Rappel de la proposition initiale de la Commission européenne

33. Dans sa Communication du 25 janvier 2012[9], la Commission européenne considère que *« les données à caractère personnel sont devenues un atout pour de nombreuses entreprises. La collecte, la globalisation et l'analyse de données concernant des clients potentiels représentent souvent une part importante de leurs activités économiques. Dans ce nouvel environnement numérique, les personnes physiques ont le droit d'exercer une maîtrise effective sur leurs données. »*

34. L'article 20 du projet de Règlement déposé par la Commission européenne est intitulé « Mesures fondées sur le profilage » et consacre le droit de toute personne à ne pas être soumis à une mesure produisant des effets juridiques ou l'affectant de manière significative, prise sur le seul fondement d'un traitement automatisé destiné à évaluer certains aspects personnels propres à cette personne physique ou à analyser ou prévoir en particulier le rendement professionnel de celle-ci, sa situation économique, sa localisation, son état de santé, ses préférences personnelles, sa fiabilité ou son comportement.

35. Cet article 20 est inspiré de l'article 15, paragraphe 1, de la directive 95/46/CE relatif aux décisions individuelles automatisées, qu'il complète et assortit de garanties supplémentaires. Il tient également compte de la recommandation du Conseil de l'Europe concernant le profilage. La Commission européenne entend donc, semble-t-il, par cette nouvelle disposition étendre la protection déjà accordée par l'article 15 de la directive 95/46 à certains types de profilage.

36. La CPVP partage le constat fait par la Commission européenne (point .. ci-dessus). Dans le prolongement de son avis 35/2012, elle porte une attention toute particulière à cette notion de profilage. Elle aborde ci-dessous les aspects suivants :

---

[9] Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des Régions (COM(2012) 9 final).

- ✓ Le lien (et sa distinction d') avec le principe de l'interdiction des décisions individuelles automatisées
- ✓ La définition du profilage
- ✓ Les conditions du traitement des données personnelles dans le cadre du profilage
- ✓ Un aspect spécifique : profilage et (non-) discrimination
- ✓ Le droit à l'anonymat

Profilage et décisions individuelles automatisées : deux concepts à distinguer

37. La CPVP regrette que le terme « profilage » de l'article 20 ait englobé le régime actuel des décisions automatisées de l'article 15 de la Directive 95/46. En effet, il est envisageable que des décisions automatisées soient adoptées sans qu'un profil n'ait été constitué au préalable.[10] A l'inverse, il est possible de créer des profils ou de profiler des personnes sans prendre de mesures qui les affectent de manière significative ou produisent des effets juridiques à leur égard.[11]

38. Dès lors, la CPVP estime qu'il est plus protecteur pour les individus de diviser cet article 20 en deux parties, en conservant d'une part le régime encadrant les décisions automatisées, tel que consacré par la directive 95/46/CE, et en ajoutant d'autre part un régime spécifique qui règlementera le profilage. A défaut, il lui semble que le règlement propose un régime de protection en-deçà de celui offert par l'article 15 de la directive 95/46/CE. Cet affaiblissement du niveau de protection est inacceptable à ses yeux.

Définition du profilage (article 4.3a))

39. Le terme « profilage » n'est pas défini de manière autonome par le projet de Règlement déposé par la Commission européenne. L'article 4.3a nouveau du projet de la Commission LIBE le définit pour sa part comme *« toute forme de traitement automatisé de données à caractère personnel destiné à évaluer certains aspects personnels propres à une personne physique ou à analyser ou prévoir en particulier le rendement professionnel de celle-ci, sa situation économique, sa localisation, son état de santé, ses préférences personnelles, sa fiabilité ou son comportement ».*

[10] Ainsi par exemple, un Questionnaire à Choix Multiple (QCM) ou des critères d'attribution de prêts bancaires ne nécessitent pas obligatoirement la constitution d'un profil préalable.

[11] Un profil abstrait peut être nourri des informations de plusieurs catégories de personnes, dans le cadre du datamining. En outre, un profil individualisé des comportements d'une personne peut être créé sans prendre de mesures à son égard.

40. La CPVP estime qu'il existe une différence entre la collecte de données à des fins d'établissement de profils, la création de profils (abstraits ou individuels), et l'application de ces profils à un individu. Ces trois opérations nécessitent un traitement susceptible d'entrer dans la définition du profilage tel que défini par l'article 4.3a du projet de texte de la Commission LIBE.

41. Or, la définition du profilage est ambigüe et ne permet pas de savoir si elle entend englober à la fois la création d'un profil et son application à un individu. En outre, la CPVP constate que l'intitulé de l'article 20 n'est plus « Mesures basées sur le profilage », mais « Profilage », ce qui pourrait laisser entendre que le champ d'application de l'article 20 tel que proposé par le texte de la Commission LIBE est plus large.

42. A l'appui de ce qui précède, la CPVP est d'avis qu'il convient de clarifier cet aspect en précisant que *toutes* les opérations relatives au profilage (collecte des données, création de profils abstraits ou individuels, et application de ces profils pour en tirer des conclusions et/ou des démarches vis-à-vis de la personne profilée) doivent être réglementées.

43. A ce titre, la CPVP est d'avis que le projet de texte devrait se rapprocher de celui de la Recommandation du Conseil de l'Europe sur le profilage et inclure – sans s'y limiter - la définition de profil, défini comme « un ensemble de données qui caractérise une catégorie d'individus et qui est destiné à être appliqué à un individu »[12].

44. La CPVP estime par ailleurs qu'il est important de définir le profil comme un ensemble de données sans exiger que ces données soient des données à caractère personnel, dès lors qu'un profil peut aussi être constitué au départ de données anonymisées ou d'informations. Or, de tels profils peuvent également être appliqués à un individu.

Conditions de traitement des données personnelles dans le cadre du profilage

45. La CPVP estime que dans tous les cas, un individu devrait être informé que ses données seront utilisées pour établir des profils. Dans ce cas, il devrait ressortir clairement du projet de règlement que l'on est face à un nouveau traitement de données. L'article 14 (ga) proposé par la Commission LIBE devrait être adapté en ce sens dès lors qu'il ne semble viser que *l'application* d'un profil (« le profilage ») et non sa création.

[12] Le profil devrait en outre, selon la CPVP, également couvrir tout ensemble de données qui caractérise les comportements d'un individu particulier et les données qui le concernent.

46. L'article 20 tel qu'amendé par la Commission LIBE prévoit que tout individu peut s'opposer à toute forme de profilage. L'article 20.2 prévoit en outre un régime plus strict en ce qui concerne le profilage conduisant à des mesures produisant des effets juridiques pour la personne concernée ou affectant de manière significative ses intérêts, ses droits ou libertés.

47. La CPVP accueille favorablement le fait que l'article 20 s'applique à *tous les types* de profilages, et non uniquement à ceux conduisant à des mesures produisant des effets juridiques pour la personne concernée ou affectant de manière significative ses intérêts, ses droits ou libertés. Cette disposition ainsi rédigée permet d'englober le profilage à des fins de marketing (voy le point 80 de l'avis 35/2012).

48. Dans les cas visés à l'article 20.2, le profilage peut uniquement se baser sur un contrat, sur le consentement de la personne concernée ou sur la législation. Des garanties appropriées doivent également entourer le profilage. Ainsi que la CPVP le mentionne dans son précédent avis 35/2012, une intervention humaine devrait systématiquement être prévue dans chacune des hypothèses de l'article 20.2 du projet de Règlement (point 79 de l'avis 35/2012).

Un aspect spécifique : profilage et (non)-discrimination

49. La CPVP s'interroge également sur la portée de l'article 20.3, qui interdit le profilage qui aura l'effet de discriminer les individus sur la base de leur race, leur origine ethnique, leurs opinions politiques, leur religion ou leurs croyances, leur appartenance syndicale, leur orientation sexuelle ou leur identité de genre, ou qui résulte dans des mesures qui auraient un tel effet.

50. En effet, la notion de discrimination n'est pas définie dans le projet de Règlement. Plusieurs textes européens font référence à cette notion[13], mais le projet de Règlement n'y renvoie pas explicitement. En outre, il est clair que le profilage a précisément pour objet de traiter des individus de manière distincte selon leurs caractéristiques, lesquelles pourraient être des caractéristiques listées à l'article 20.3.

51. De plus, dans la mesure où les discriminations sont interdites en vertu d'autres textes légaux, la CPVP ne voit pas la valeur ajoutée de l'article 20.3 dès lors qu'il ne fait

[13] Par exemple, Directive 2000/78/CE du Conseil du 27 novembre 2000 portant création d'un cadre général en faveur de l'égalité de traitement en matière d'emploi et de travail ; la Directive 2000/43/CE du Conseil du 29 juin 2000 relative à la mise en œuvre du principe de l'égalité de traitement entre les personnes sans distinction de race ou d'origine ethnique.

qu'interdire ce qui est déjà interdit. Elle recommande donc de supprimer le texte en l'état ou de le préciser par un renvoi à des textes précis ou à une définition précise du terme de discrimination.

52. L'article 20.3 proposé par la Commission européenne prévoit que le profilage ne peut être uniquement basé sur les catégories particulières de données à caractère personnel mentionnées à l'article 9. La CPVP rappelle à cet égard qu'elle indique dans son avis précédent 35/2012 que cette disposition risque d'exclure les traitements effectués par certaines administrations publiques dans leurs politiques publiques en matière de soins de santé (point 82 de l'avis 35/2012).

53. Enfin, la CPVP rappelle que le considérant 58a institue une présomption selon laquelle le profilage basé uniquement sur le traitement de données pseudonymes ne sera pas considéré comme affectant significativement les intérêts, droits ou libertés des personnes concernées. La CPVP renvoie sur ce point au point 13 ci-dessus consacré plus spécifiquement aux données pseudonymes et ajoute que le seul fait que des données pseudonymes soient utilisées ne suffit pas à exclure les risques liés au profilage, notamment le risque de discrimination.

54. En outre, la dernière phrase du considérant 58a semble supposer que les données pseudonymes ne permettent pas d'être attribuées à une personne concernée particulière, ce qui n'est pas le cas. Ce considérant procède d'une mauvaise compréhension de la définition de donnée pseudonyme, qui reste en tout état de cause une donnée à caractère personnel. Par conséquent, la CPVP propose de supprimer le considérant 58a.

Droit à l'anonymat

55. La CPVP est d'avis que l'article 20 devrait introduire un principe consacrant le droit de bénéficier d'un produit ou d'un service sans devoir communiquer des données à caractère personnel, à moins que le service requis ne nécessite de connaître l'identité de la personne concernée. Un tel principe a été introduit par la Recommandation du Conseil de l'Europe sur le profilage. En outre, afin d'assurer un consentement libre, spécifique et éclairé au profilage, le texte devrait prévoir que les prestataires de services de la société de l'information devraient assurer, par défaut, un accès non profilé aux informations relatives à leurs services.

2.6. Restrictions (article 21)

56. La Commission LIBE réduit les articles auxquels il peut être dérogé au titre d'exception (article 21). Les principes de base énoncés à l'article 5 a)-e) demeurent applicables en toute circonstance de même que l'article 20 (profilage) ce qui n'était pas le cas dans le texte original de la Commission européenne. Dans le même esprit de protection renforcée, la Commission LIBE ajoute un certain nombre d'éléments devant figurer dans les législations nationales dérogatoires, s'appuyant pour se faire sur la jurisprudence constante de la Cour européenne des droits de l'homme. Les motifs pour lesquels l'Etat membre peut adopter un régime dérogatoire à ces dispositions du projet de Règlement se voient également limitées. Ainsi, la référence à l'intérêt public est réduite au seul motif des « taxation matters ».

57. A première lecture, toute restriction de la possibilité de déroger à un régime de protection paraît devoir être favorablement accueillie, *a fortiori* par une autorité de protection des données telle la CPVP. Toutefois, un régime inapplicable à défaut de dérogations adéquates entraîne, entre autres effets pervers, les risques de contournement systématique des dispositions et d'interprétation erronée ou volontairement biaisée. En d'autres termes, mieux vaut un régime de protection qui prévoit des exceptions appropriées qu'un régime indistinctement *théoriquement* applicable mais inapplicable en pratique, par exemple pour le secteur public. A cet égard, la CPVP alerte le lecteur sur la suppression de la notion d'*« intérêt général de l'Union ou d'un Etat membre »* (article 21.1 c)) et sa réduction aux seules *« taxation matters »*.[14] La CPVP privilégie le maintien des exceptions formulées par l'article 13 de la directive 95/46/CE dont la pertinence n'a, à sa connaissance, pas été remise en cause.

3. Chapitre IV : Obligations du responsable de traitement

58. Dans l'esprit de son avis 35/2012 et comme grille de lecture du Chapitre IV de la proposition de règlement de la Commission européenne, la CPVP se pose la question de la valeur ajoutée réelle et concrète pour la protection des personnes concernées à l'égard des traitements de données les concernant, des obligations mises à charge des responsables de traitement et des sous-traitants. Dans cette appréciation, la praticabilité des mesures d'accountability développées ainsi que leur coût entrent en ligne de compte. En d'autres

[14] La CPVP est par exemple d'avis que la sécurité sociale devrait pouvoir être reconnue comme un intérêt général d'un Etat membre de l'Union et justifier un régime dérogatoire pour certains aspects des traitements réalisés dans ce secteur souvent très spécifiquement encadré au niveau national. La CPVP a notamment à l'esprit la compétence en ce domaine du Comité sectoriel de la sécurité sociale et de la santé (voy. point .. ci-dessous).la sécurité sociale pourrait ainsi utilement être mentionnée dans un considérant relatif à l'article 21. Elle plaide en toute hypothèse pour une clarification du régime applicable aux traitements de données personnelles dans ce secteur dès lors que la lecture combinée des articles 21, 81.1c) et 82a tels que proposés par la Commission LIBE est source de confusion.

termes, la CPVP plaide pour un système d'obligations cohérentes et basées sur l'appréciation concrète du risque réel induit par les traitements réalisés. C'est à l'aune de ces critères que quelques – unes des obligations mises à charge du responsable de traitement et du sous-traitant ainsi que d'autres mesures visant à leur responsabilisation sont, dans la version qu'en propose la Commission LIBE, commentées ci-dessous.

3.1. Responsable de traitement et sous-traitant (article 26)

59. La question de la sous-traitance ultérieure et des conditions qui devraient l'encadrer est évoquée aux points 91-92 ci-dessous relatif aux BCR sous-traitants.

3.2. Documentation (article 28)

60. La Commission LIBE réduit l'obligation de documentation au strict minimum. Tout responsable de traitement et sous-traitant doivent conserver une documentation faisant état des seuls quelques éléments suivants : nom et données de contact du responsable de traitement, du/des co-responsables de traitement éventuels, du sous-traitant et du représentant le cas échéant ; identité et données de contact du délégué à la protection des données éventuel ainsi que celles des responsables de traitement auxquels les données sont communiquées.

61. Dans son avis 35/2012, la CPVP se déclare favorable à l'obligation de documentation interne en lieu et place de la déclaration préalable de traitements pour autant que l'intérêt particulier de cette déclaration - soit l'obligation pour le déclarant de se poser les questions pertinentes au regard des principes de protection des données concernant ses traitements - demeure. Cet exercice de réflexion disparaît dans l'obligation de documentation minimaliste que formule la Commission LIBE du Parlement européen. La CPVP est d'avis que cette documentation devrait en outre inclure : une description succincte des traitements reprenant les finalités poursuivies et les catégories de données traitées (point 97 de l'avis 35/2012).

3.3. Sécurité et notification des violations de données (articles 30, 31 et 32)

62. A l'article 30 (1a.), la CPVP salue les précisions apportées quant au contenu de la politique de sécurité.

63. Quant à la notification des violations de données (data breach), la Commission LIBE maintient la distinction proposée par la Commission européenne entre (1) notification aux

autorités de protection des données (article 31) et (2) notification aux personnes concernées (article 32). Si la Commission LIBE enjoint les responsables de traitement et sous-traitants à notifier ces violations non plus dans les 24h mais bien « sans retard » - ce qu'accueille favorablement la CPVP -, elle ne précise pas davantage que la Commission européenne (ou de manière insuffisante) quelles seront les violations à notifier. Comme dans son avis 35/2012, la CPVP est d'avis que le texte en l'état engendrera des situations « impossibles » tant pour l'autorité de protection des données que pour le responsable de traitement, le sous-traitant et la personne concernée elle-même. Ce déficit de précision risque de rendre, dès leur conception, ineffectives cette obligation et l'information corrélative utile qu'elle se veut apporter à l'autorité de contrôle et à chacun.

3.4. Respect to Risk (32a)), Data Protection Impact assessment (article 33), Data protection compliance review (article 33a))

64. Avec l'adoption de l'article 32a) intitule "Respect to risk", la Commission LIBE affiche son intention de justifier les obligations de désignation d'un représentant dans l'Union (article 25), de nomination d'un délégué à la protection des données (article 35) et d'une analyse d'impact sur la protection des données (article 33 - DPIA) au regard des risques spécifiques que créent certains traitements.

65. La CPVP n'est cependant pas convaincue par la manière dont la Commission LIBE justifie - de manière théorique, *a priori*, et se mettant à la place du responsable de traitement ou du sous-traitant - ses conclusions. Ainsi, alors que l'article 32a.1. parle de traitements *« likely to present specific risks »* et que l'article 32a.2. liste les mesures à prendre *« according to the result of the risk analysis »* (soit la désignation d'un représentant, d'un délégué à la protection des données ou la réalisation d'un DPIA), les articles qui détaillent les hypothèses dans lesquelles ces obligations doivent impérativement être mises en œuvre ne laissent aucune marge d'appréciation au responsable de traitement. L'article 32 a.1. semble être plus une construction textuelle qu'une véritable mise en œuvre de la « risk based approach » par le responsable de traitement pour laquelle plaide la CPVP.

66. De manière générale, la CPVP s'interroge sur la qualification de *« risqués »* ou de *« présentant des risques particuliers »* de certains traitements identifiés comme tels. Elle renvoie quant à ce à son avis 35/2012 (points 113 et s.).

67. Quant à l'instrument « Analyse d'impact relatif à la protection des données » à proprement dit, la CPVP y est favorable pour autant que celui-ci porte sur des traitements adéquatement identifiés comme particulièrement « risqués » (voy. ci-dessus), soit effectif, concret et

réalisé de la manière la plus impartiale possible. Avec les mêmes exigences, elle accueille favorablement le principe du « lifecycle data protection management » (intitulé de la section 3) et celui d'une évaluation périodique de l'analyse d'impact (article 33a.).

3.5. Autorisations et consultation préalable (article 34)

68. Dans son avis 35/2012, la CPVP constate que le projet de Règlement de la Commission européenne entend limiter les pouvoirs d'autorisation préalable des autorités de protection des données au seul domaine des transferts internationaux de données. Partant, la CPVP y plaide pour que le système belge des Comités sectoriels mis en place pour la protection des données à caractère personnel dans le cadre du secteur public, soit intégralement maintenu (Sécurité sociale et santé, Registre national, Autorité fédérale, Statistique, Banque-carrefour des entreprises). La procédure d'autorisation préalable de ces Comités permet d'accompagner utilement le secteur public lors de la mise en place de flux de données personnelles. Ces Comités jouent le rôle de guide auprès des responsables de traitement. Ils peuvent autoriser ou refuser un accès mais également assortir leurs autorisations de conditions suspensives ou résolutoires (points 120 et s. de l'avis 35/2012).

69. La CPVP constate que le texte voté par la Commission LIBE ne répond pas à ses préoccupations. Le régime de consultation préalable (parfois présenté comme un palliatif adéquat) ne permet pas – ni dans sa version « Commission européenne », ni dans celle amendée de la Commission LIBE – un tel maintien.

70. La CPVP suggère par conséquent l'insertion de l'amendement suivant :
« *Notwithstanding paragraph 2, Members States may require controllers to consult with, and obtain prior authorisation from, the supervisory authority in relation to the processing of personal data by a controller for the performance of a task carried out by the controller in the public interest, including the processing of such data in relation to social protection and public health».*

3.6. Délégué à la protection des données (articles 35 et suivants)

71. Comme c'est le cas dans la proposition initiale de la Commission européenne, la Commission LIBE fait de la désignation d'un délégué à la protection des données une *obligation* pour le responsable de traitement et le sous-traitant dans un certain nombre d'hypothèses. A celles déjà énoncées dans la proposition originale, la Commission LIBE ajoute une quatrième : lorsque les activités de base du responsable de traitement consistent en des traitements a)

de données sensibles, b) de données de localisation, c) de données relatives à des mineurs ou à des employés dans de larges bases de données.

72. La Commission LIBE modifie également l'une des hypothèses dans lesquelles un délégué devra être désigné. Le critère de *« toute entreprise employant 250 personnes »* est ainsi remplacé par celui du nombre de personnes concernées par les traitements annuellement réalisés par le responsable de traitement (5000 – article 35.1.b)). Dans son avis 35/2012, la CPVP souligne l'absence de pertinence du critère du seuil de personnes employées par le responsable de traitement, critère qui ne tient pas compte des risques induits par les traitements réalisés. Le nombre de personnes concernées – outre qu'il semble difficilement praticable – prête le flanc à la même critique.

73. De manière générale, la CPVP est d'avis qu'au vu des 4 hypothèses dans lesquelles la désignation d'un délégué à la protection des données est obligatoire, peu de traitements ne justifieront pas la désignation d'un délégué à la protection des données. Désigner un délégué à la protection des données doit, de l'avis de la CPVP, rester optionnel. La mise en œuvre d'une telle fonction est une mesure – parmi toutes celles qui participent de l'accountability – dont le responsable de traitement doit rester libre de faire le choix 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 cette nomination. C'est en ce sens que la CPVP privilégie la faculté laissée à cet égard aux responsables de traitement et aux sous-traitants aux termes du texte discuté au Conseil (DAPIX).

74. La CPVP relève enfin qu'à l'article 34.2., la Commission LIBE prévoit que lorsqu'il existe, la consultation préalable peut se faire auprès du délégué à la protection des données en lieu et place de l'autorité de contrôle. Selon la CPVP, ce type de mesure pourrait être introduite - même dans un régime de désignation non obligatoire du délégué à la protection des données - comme incitant précisément à sa désignation.

3.7. Certification (article 39)

75. La Commission LIBE propose un corpus plus abouti de règles relatives à la certification. Conçue par la Commission européenne comme un outil d'information destiné à *« permettre aux personnes concernées d'évaluer rapidement le niveau de protection des données offert par les responsables de traitement et les sous-traitants »* (article 39.1. de la proposition de la COM), la certification entraîne par contre un certain nombre de conséquences juridiques concrètes aux termes du texte voté par la Commission LIBE.

76. Ainsi, l'article 42.2 (aa) qualifie le « European Data Protection Seal » de garantie adéquate pour le transfert de données vers un responsable de traitement établi hors de l'Union européenne en l'absence de décision d'adéquation de la règlementation qui lui est applicable (voy. point 85).

77. L'article 79.2b) relatif aux sanctions administratives commenté ci-après (points 123-126) indique quant à lui que le bénéficiaire d'un tel label sera administrativement sanctionné dans un nombre réduit d'hypothèses. La CPVP souligne dès à présent qu'elle y est opposée.

78. La CPVP n'en est dès lors que plus convaincue encore de la nécessité de prévoir que les critères et exigences applicables aux mécanismes de certification, y compris les conditions d'octroi, de révocation et les conditions de reconnaissance au sein de l'Union et dans les pays tiers ainsi que les critères d'accréditation des certificateurs, sont déterminés par les autorités de protection des données, le cas échéant regroupées au sein du Comité européen de la protection des données (CEDP). La consultation du CEPD par la Commission européenne dans le cadre de l'élaboration de l'acte délégué sur ce sujet est un minimum.

79. Sur la base de ces critères et exigences, des certificateurs externes certifiés (par les autorités de protection des données et/ou le CEPD) accèderont ou non aux demandes de certification des responsables de traitement et sous-traitants. Cette répartition des rôles entre autorités de contrôle et certificateurs certifiés vise à préserver l'indépendance des autorités de protection des données et à garder entière leur compétence de contrôle, en ce compris sur les responsables de traitement et sous-traitants certifiés.

80. Comme pour le registre des violations de données (article 31.4.), la CPVP souscrit à l'idée d'un registre public des certificats délivrés et retirés (article 39.1h)).

81. Enfin, la CPVP relève que l'article 23 fait du *« data protection by design »* un critère de sélection des marchés publics. Il ne semble dès lors pas exclu que le label européen de protection des données joue ici un rôle important, dans la lignée des dispositions actuelles des directives 2004/17/CE et 2004/18/CE relatives aux procédures de passation de certains marchés publics. La CPVP y restera attentive.

4. Chapitre V : Flux transfrontières

4.1. Transferts de données au moyen de garanties appropriées (article 42)

Le sort des autorisations existantes

82. La CPVP regrette que la Commission LIBE propose que les décisions prises en vertu de l'article 26.2 de la Directive 95/46/CE (autorisations de transferts de données sur la base de contrats *ad hoc*, de contrats types ou de BCR) ne demeureront valides que deux années après l'entrée en vigueur du projet de Règlement européen.

83. Cette position impliquera une surcharge administrative importante et non nécessaire tant pour les autorités européennes de protection des données qui devront réévaluer l'ensemble des décisions déjà accordées (alors qu'elles auront certainement des tâches plus essentielles à mener) que pour les entreprises qui devront réintroduire de nouvelles demandes d'autorisation pour des transferts qui pourtant auront déjà été autorisés.

84. Elle induit par ailleurs une importante *insécurité juridique* et implique que les entreprises hésitent actuellement à investir dans des outils protecteurs en termes de protection des données mais qui n'auront qu'une durée de validité limitée. Cette mesure aura (et a déjà actuellement) un effet complètement contre-productif. Pour ces raisons, la CPVP s'y oppose vivement.

Une nouvelle garantie : la certification

85. La CPVP relève que la labellisation d'un responsable de traitement ou d'un sous-traitant - en ce compris au bénéfice de responsables de traitement et de sous-traitants établis en dehors de l'Union européenne - au moyen du « European Data protection Seal » est listée parmi les garanties adéquates autorisant un transfert de données vers un pays tiers non – adéquat (article 42.2. aa)). La CPVP renvoie à cet égard aux points 75-81 ci-dessus relatifs à la certification et est d'avis que ce n'est qu'aux conditions et uniquement aux conditions qu'elle expose dans ces paragraphes que telle certification pourrait avoir pour conséquence d'autoriser un transfert de données sans autre forme de garantie complémentaire.

4.2. Règles d'entreprises contraignantes ou Binding Corporate Rules (BCR) pour les sous-traitant (article 43)

86. Dans son avis 35/2012 sur la proposition de règlement européen[15], la CPVP accueille positivement la proposition de reconnaître explicitement les Règles d'entreprise contraignantes (Binding Corporate Rules - BCR). Elles sont utilisées depuis quelques années déjà[16] par les entreprises multinationales afin d'offrir des garanties suffisantes pour leurs transferts intra-groupes de données personnelles.

87. Cependant, si le vote de la Commission LIBE conserve la référence aux BCR, elle tend à supprimer la possibilité de faire usage des « BCR sous-traitants » (« BCR Processor »[17]). La CPVP s'oppose à cette position pour les raisons ci-dessous:

88. Cette suppression est vecteur d'insécurité juridique pour les entreprises qui recourent déjà à cette solution. Depuis janvier 2013, les « BCR sous-traitants » peuvent faire l'objet d'une procédure de coopération européenne[18] et, déjà, plusieurs dossiers sont en cours d'évaluation[19].

89. Par ailleurs, on supprimerait un outil offrant actuellement les garanties les plus protectrices en termes de protection des données pour les transferts internationaux de données vers des sous-traitants et la meilleure manière de promouvoir à l'étranger les principes européens de protection des données. Les sociétés n'auraient d'autre alternative que de signer des clause-types 2010/87/EU ou de se limiter à faire appel des sous-traitants établis dans l'Union européenne ou dans un pays considéré comme offrant une protection adéquate (par ex. les

---

[15] http://www.privacycommission.be/sites/privacycommission/files/documents/Opinion_35_2012.pdf

[16] Dans les faits, ils sont utilisés depuis 2003, date à laquelle le G29 a reconnu aux entreprises la possibilité de faire usage des BCR.

[17] Si les « BCR responsable de traitement » (BCR-Controller) sont des outils permettant un encadrement des transferts de données traitées à l'origine par les entreprises du groupe en tant que responsable de traitement (Par ex. données relatives aux employés ou aux clients du groupe), les « BCR sous-traitants » encadrent le transfert de données traitées à l'origine par le groupe en tant que sous-traitants (par exemple un groupe proposant de l'outsourcing à des sociétés tierces telle que la gestion des données des employés ou des clients de ces sociétés tierces).

[18] G29 a établi le cadre permettant l'usage des « BCR sous-traitants » depuis le mois de juin 2012 (WP195 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp195_en.pdf) et les entreprises peuvent introduire leur demande de procédure de coopération européenne depuis le mois de janvier 2013 (http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/20121221_pr_bcrs_en.pdf).

[19] A notre connaissance, il y a déjà 8 dossiers en cours de procédure de coopération européenne mais il faut ajouter les société qui font actuellement les investissements préalables nécessaires à l'introduction formelle de leur dossier.

sociétés établies aux USA et ayant souscrit aux principes du Safe Harbor[20]). Les BCR vont au-delà des simples engagements juridiques prévus dans la clause-type 2010/87/EU, car ils imposent en outre la mise en place de mesures assurant la mise en œuvre concrète des engagements juridiques (audit régulier, formation des employés, système interne de gestion des plaintes, etc.)[21].

90. Une critique parfois formulée à l'égard des « BCR sous-traitant »(et qui justifierait sa suppression par a Commission LIBE ?) serait le manque de garantie encadrant la sous-traitance ultérieure. Or, la CPVP estime que les garanties proposées sont suffisantes. Comme le prévoit déjà la clause-type 2010/87/EU, les sociétés sous-traitantes peuvent, sous conditions strictes[22], faire appel à des sous-traitants ultérieurs et apporter les garanties contractuelles nécessaires à ces activités. Les conditions visent notamment à garantir la transparence à l'égard des responsables de traitement (sociétés clientes du groupe) et le maintien de leur contrôle sur l'éventuelle intervention de sous-traitants ultérieurs[23]. Par ailleurs, les activités de sous-traitances ultérieures extra-groupes devront être encadrées par des contrats[24].

91. Par ailleurs, il serait totalement incohérent de s'opposer aux « BCR sous-traitants » en invoquant le manque de conditions strictes encadrant la sous-traitance ultérieure au vu des très faibles conditions[25] encadrant la sous-traitance ultérieure au sein de l'UE actuellement prévues par le texte de la Commission LIBE elle-même (article 26.2d)). Les conditions strictes des « BCR sous-traitants » encadrant la mise en place de sous-traitance ultérieure

---

[20] L'application du Safe Harbor à des sociétés sous-traitantes pose néanmoins certaines difficultés (voir la FAQ 10) et ce cadre juridique n'est pas exempt de critique, voir à ce sujet la communication de Commission européenne du 27 novembre 2012 « on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU ».

[21] Mesures d'accountability, soutenues également dans le projet de règlement européen de protection des données.

[22] Voir le point 6.1 du WP195.

[23] Cette intervention ne peut se faire qu'avec leur accord. Selon la sensibilité des activités concernées, les parties peuvent librement décider de prévoir un consentement spécifique pour chaque sous-traitant ultérieur ou si un consentement général suffit. Dans cette dernière hypothèse, le responsable doit toujours avoir la possibilité d'objecter avant l'intervention d'un sous-traitant ultérieur et dans ce cas de pouvoir mettre un terme au contrat.

[24] Les garanties que devront offrir les sous-traitants ultérieurs devront se calquer sur les garanties offertes par le sous-traitant principal à l'égard de la société cliente. En tout état de cause, le sous-traitant principal se porte garant à l'égard de son client des éventuelles déficiences des sous-traitants ultérieurs.

[25] L'article 26.2.d ne prévoit pas qu'un contrat soit nécessairement signé entre le sous-traitant et les sous-traitants ultérieurs et il prévoit que cette sous-traitance puisse avoir lieu sans l'autorisation préalable du responsable, ce qui risque certainement de l'empêcher de garder le contrôle nécessairement lié à son rôle de responsable de traitement. Par ailleurs, le sous-traitant principal ne se porte pas garant des fautes commises par les sous-traitants ultérieurs.

en dehors de l'UE[26] devraient plutôt servir de modèle d'inspiration au Parlement européen et au Conseil européen dans le cadre de l'adoption des règles encadrant la sous-traitance ultérieure au sein de l'Union[27].

92. Il est un fait aujourd'hui que les sociétés multinationales qui offrent des services de sous-traitance font appel à des sous-traitants ultérieurs. L'autonomie offerte aux sous-traitants d'encadrer juridiquement leur sous-traitance ultérieure a été reconnue juridiquement par les Etats membres, la Commission européenne et les autorités européennes de protection des données depuis l'approbation des clauses-types 2010/87/EU. Ce n'est pas en interdisant les « BCR sous-traitant » que l'on stoppera ce développement, notamment du cloud computing. L'objectif du droit n'est pas de limiter les développements technologiques mais de les encadrer du mieux possible.

93. Une autre raison parfois avancée et qui fonderait l'objection (de la Commission LIBE) aux « BCR sous-traitant » est le risque posé quant à l'accès aux données par les autorités étrangères. Les BCR visent à encadrer les activités commerciales et ne peuvent par nature restreindre les pouvoirs des autorités étrangères[28]. Cependant, en cas de conflit de droit, les « BCR sous-traitants » prévoient des obligations strictes de transparence à l'égard des responsables de traitement mais également à l'égard des autorités européennes de protection des données qui doivent intervenir[29]. Les garanties prévues pour les « BCR sous-traitants » vont par conséquent dans le même sens que l'article 43a proposé par le Comité LIBE et vont certainement au-delà de celles offertes actuellement dans les clause-types 2010/87/EU ou par ex. dans le Safe Harbor.

94. En conclusion, outre le fait que les arguments de fond justifiant la suppression des « BCR sous-traitants » ne sont, aux yeux de la CPVP, pas défendables, le fait de s'opposer à ceux-ci ne fait que créer de l'insécurité juridique et pousser les entreprises à opter pour des outils moins protecteurs qui n'offrent pas cet avantage qu'ont les BCR de promouvoir les règles européennes de protection des données à l'étranger.

---

[26] Voir notamment les points point 6.1.vi et vii des « BCR Processor » (WP195) mais également l'article 11 des clauses types 2010/87/EU.

[27] Article 26.2.d. relatif à la sous-traitance ultérieure au sein de l'UE.

[28] La meilleure voie à suivre serait encore de prévoir l'imposition d'autorisations d'autorités publiques européennes pour le transfert à de telles fins et la conclusion d'accords internationaux. Les solutions politiques et industrielles sont également à privilégier.

[29] Voir le point 6.3 du WP195.

4.3. Transferts et divulgations non autorisées par le droit de l'Union (article 43.a))

95. La CPVP considère qu'une surveillance générale, massive et systématique des citoyens belges et européens n'est pas acceptable dans une société démocratique. Partant, la CPVP accueille positivement l'initiative de la Commission LIBE à l'article 43a. ainsi qu'au considérant 82 consistant à tenter d'apporter des solutions aux pratiques - et conséquences en termes de protection de la vie privée et données à caractère personnel – notamment révélées dans la presse ces derniers mois.

96. En quelques mots, l'article 43.a) prévoit qu'il incombe à l'autorité de protection des données d'évaluer la compatibilité avec le Règlement de la demande de transmission de données vers un pays tiers (demande fondée sur une décision de justice de cet état par exemple (cas de l'affaire SWIFT, Snowden, les demandes eDiscovery ou de la SEC américaine (Security Exchange Commission) pour des exemples concrets)) et d'autoriser, le cas échéant, le dit transfert. C'est également l'autorité de protection des données qui préviendra « l'autorité nationale compétente ».

97. La CPVP estime néanmoins nécessaire que soient conclus des accords internationaux afin de réguler les actions des Etats tiers dans le cadre de la lutte contre les infractions graves et la sécurité nationale. A cet égard, la référence à l'article 43a. aux traités d'assistance mutuelle est certainement utile dans le cadre de la lutte contre ces infractions.

98. Si la CPVP est d'avis que les autorités de protection des données ne peuvent raisonnablement pas être totalement écartées ou laissées dans l'ignorance totale de ce type de transferts de données, elle n'estime cependant pas que celles-ci soient les mieux placées, ni même instituées pour décider qu'un jugement ou décision administrative étrangère peut ou non être accueilli.

99. Il est à cet égard surprenant que l'article 43a. proposé ne confie de pouvoirs qu'aux autorités de protection des données (qui informeront les autorités nationales compétentes) alors que le considérant 90 fait référence à l'intervention de la Commission européenne qui doit assurer que le droit européen aura toujours préséance, qui devra tenter de résoudre le conflit juridictionnel avec le pays tiers et qui fournira de l'information et de l'aide aux responsables de traitement et sous-traitants concernés. Il y a là une certaine confusion des rôles respectifs des autorités de protection des données et de la Commission européenne qui démontre, à n'en pas douter, que les autorités de protection des données ne sont ni outillées, ni instituées pour le rôle politique qu'on voudrait leur voir jouer aux termes de cet

article 43a. L'entité chargée d'évaluer les demandes pourrait être celle désignée dans l'accord international concerné.

100. Si la CPVP estime utile qu'une information générale soit offerte quant aux demandes réalisées dans les 12 derniers mois, elle a plus de doutes sur l'option de prévoir une information spécifiques aux personnes concernées. Le fait d'imposer cette transparence ne solutionne pas l'éventuel conflit de droit dans laquelle l'entreprise peut se trouver si cette transparence est interdite de la part des autorités étrangères.

101. Par ailleurs, la seule référence aux juridictions ou autorités administratives étrangères ne suffisent pas, dès lors que dans le cas de PRISM, elles ne sont pas systématiquement concernées. Il serait utile d'étendre le champ de l'article aux autorités publiques en général.

102. Enfin, la CPVP accueille favorablement le considérant 82 qui prévoit de manière explicite que le fait qu'une législation étrangère permette un accès extraterritorial à des données personnelles traitées dans l'Union sans l'autorisation données en vertu du droit d'un Etat membre ou du droit de l'Union, doit être considéré comme une indication de non-adéquation.

4.4. Exceptions (article 44)

103. Pour les raisons déjà développées dans son précédent avis sur la proposition de règlement (point 140 de l'avis 35/2012), la CPVP accueille favorablement la suppression du point h de l'article 44.1. Elle tient également à souligner que, de manière générale, les dérogations prévues à l'article 44 doivent être interprétées de manière restrictive et ne peuvent porter sur des transferts massifs ou répétitifs de données, ni servir de base à des transferts de données qui ont lieu d'une manière telle qu'elle ne peut être considérée comme étant nécessaire et proportionnée dans une société démocratique.

5. Chapitre VII : Coopération et cohérence

5.1. Principe du « one-stop shop » - guichet unique (article 51)

104. Le texte de la Commission LIBE remanie le mécanisme de « one-stop-shop » tel qu'imaginé par la proposition de la Commission européenne. Le premier paragraphe de l'article 51 reste presqu'inchangé, mais précise que chaque autorité de contrôle sera compétente pour exercer ses pouvoirs sur son propre territoire, sans préjudice des articles 73 et 74, lesquels concernent le droit de *porter plainte* devant l'autorités de contrôle de son domicile et le droit

de contester devant un juge les décisions de l'autorité de contrôle. En outre, l'article 51.1 précise que les traitements effectués par les autorités publiques seront uniquement de la compétence de l'autorité de contrôle de l'Etat Membre concerné. La CPVP accueille favorablement ces précisions.

5.2. La « lead authority » - l'autorité chef de file (article 54bis)

105. La désignation d'une « lead authority », en cas de traitement transfrontière, tel que l'article 51.2 le prévoit dans la proposition de la Commission européenne, est encadrée par un nouvel article 54 bis, intitulé « autorité chef de file ». Ce nouvel article se réfère à la notion d'établissement principal, tel que défini par l'article 4 (13), lui-même modifié.

106. L'établissement principal est en effet désormais défini comme *« le lieu de l'établissement de l'entreprise ou du groupe d'entreprises dans l'Union, qu'il s'agisse du responsable du traitement ou du sous-traitant, où sont prises les principales décisions quant aux finalités, aux conditions et aux moyens du traitement de données à caractère personnel »*. Différents critères objectifs complémentaires mentionnés dans cet article permettent de déterminer plus concrètement quel sera l'établissement principal d'un responsable du traitement.

107. Malgré les réserves déjà exprimées par la CPVP dans son précédent avis sur la notion d'établissement principal (points 18 et s. de l'avis 35/2012), les modifications apportées par la Commission LIBE vont dans un sens de simplification dès lors que, par exemple, l'établissement principal sera déterminé de la même manière pour les responsables du traitement et pour les sous-traitants, ce qui n'était pas le cas dans la proposition de la Commission européenne. En outre, les critères de détermination indicatifs et non exclusifs, sont plus flexibles.

108. C'est dans le cas de « traitements transfrontières » que la désignation d'une autorité chef de file sera nécessaire (article 54 bis voté par la Commission LIBE). Un tel traitement est défini comme ayant lieu dans le cadre des activités d'un responsable du traitement ou d'un sous-traitant établis dans l'Union, et dont le responsable du traitement ou le sous-traitant sont établis dans plusieurs États membres, *ou concernant des données à caractère personnel de résidents de différents États membres*. La CPVP accueille favorablement cet ajout de bout de phrase, dès lors qu'une autorité chef de file sera également désignée dans le cas où des données d'autres personnes concernées que celles résidant dans le pays de l'Etat Membre où est établi le responsable du traitement seront traitées. Il est en effet nécessaire que dans ces cas, toutes les autorités de contrôle des Etats Membres dont les habitants voient leurs données traitées, reçoivent un rôle dans le contrôle des traitements en cause.

5.3. Un renforcement du rôle du Comité européen de la protection des données

109. La CPVP constate avec satisfaction que le texte tel que modifié par la Commission LIBE permet de saisir le Comité européen de la protection des données (CEPD) concernant d'éventuels litiges sur la désignation de l'autorité chef de file. A cet égard, le paragraphe 3 de l'article 54 bis et le paragraphe 4 du même article semblent en contradiction dès lors que le paragraphe 3 mentionne un *avis* qui peut être adopté par le CEPD à cet égard, alors que le paragraphe 4 dispose que le CEPD peut *décider* d'identifier l'autorité chef de file. Le texte devrait être clarifié à cet égard.

110. Une fois l'autorité chef de file désignée, le texte spécifie qu'elle devra consulter toutes les autres autorités de contrôle compétentes en vertu de l'article 51.1, avant de prendre les mesures qui s'imposent aux fins de contrôler les activités du responsable du traitement. Dans le cas où l'autorité chef de file désire adopter une mesure qui produit des effets juridiques contraignants à l'égard du responsable du traitement, ces autres autorités compétentes peuvent s'opposer à une telle mesure. Dans ce cas, le CEPD sera saisi, et pourra en dernier ressort adopter une décision contraignante pour l'autorité de contrôle.

111. La CPVP rejette toutefois l'idée de permettre à une autorité chef de file d'adopter des décisions contraignantes à l'égard d'un traitement pour lequel d'autres autorités de contrôle sont compétentes. En effet, une procédure de codécision, impliquant l'ensemble des autorités de contrôles compétentes, est plus appropriée dans ce cas, dès lors que la décision adoptée par l'autorité chef de file sera partagée par toutes les autres autorités compétentes.

112. En tout état de cause, à la place d'un système d'autorité chef de file (que cela soit avec procédure de codécision ou non), la CPVP préfère qu'un organe spécifique, tel que le Comité européen de la protection des données (CEPD), soit investi du pouvoir de superviser les traitements transfrontières telles que définis à l'article 54 bis.

113. De manière plus générale, la CPVP est en faveur de la création d'un organe autonome européen, chargé *au minimum* de trancher des litiges de compétences entre autorités de contrôles (si le système d'autorité chef de file devait être retenu), ou encore d'adopter des décisions contraignantes dans certains cas (comme la prise de mesures contraignantes dans le cas de traitements transfrontières, dans l'hypothèse où le système d'autorité chef de file serait exclu). Un tel organe pourrait par exemple prendre la forme d'une agence, laquelle devrait en outre disposer de la personnalité juridique pour pouvoir adopter des décisions.

114. La CPVP remarque d'ailleurs que rien n'est dit dans le projet de règlement sur les possibilités de recours contre les décisions du CEPD, alors que toute décision d'une autorité de contrôle doit pouvoir faire l'objet d'une contestation devant un juge, conformément à l'article 74. Le texte devrait dès lors prévoir qu'un recours devant la Cour de Justice de l'Union Européenne est ouvert contre les décisions du CEPD.[30]

6. Chapitre VIII : Recours, responsabilité et sanctions

6.1. Complexité du système des voies de recours

115. Une personne concernée confrontée à une violation de son droit fondamental à la protection de ses données à caractère personnel risque de se retrouver devant plusieurs juridictions de plusieurs Etats Membres différents. En effet il peut s'agir de :

- L'autorité de contrôle locale, située dans l'Etat Membre où le plaignant a introduit sa plainte (article 73 du projet de Règlement),
- L'autorité de contrôle chef de file, dans l'Etat Membre où le responsable du traitement a son principal établissement (Article 54 bis du projet de Règlement),
- Les tribunaux de l'Etat Membre dans lequel de l'autorité chef de file[31] est établie (lieu du principal établissement du responsable du traitement) concernant le recours contre les décisions de l'autorité de contrôle chef de file (Articles 54 bis et 74 combinés),
- Les tribunaux de l'Etat Membre où la personne concernée a sa résidence habituelle, concernant une action judiciaire contre le responsable du traitement (article 75).[32]
- Les tribunaux de l'Etat Membre de l'Autorité ayant reçu la plainte pour les actions judiciaires contre les Autorités locales.

116. Contrairement à la directive 95/46/CE, qui repose sur le rapprochement des législations en vue de promouvoir le marché intérieur (article 114 du TFUE), le projet de règlement entend se baser sur l'article 16 TFUE qui consacre un droit fondamental, à savoir la protection des droits fondamentaux des citoyens. Il reproduit l'article 8 de la Charte des droits fondamentaux de l'Union Européenne. La CPVP est d'avis que l'article 16 TFUE a pour but de protéger les droits fondamentaux des citoyens, et n'est pas rédigé pour permettre aux responsables du traitement de traiter plus facilement leur données, notamment en ayant accès à un interlocuteur unique qui superviserait leurs activités (principe du one-stop shop).

---

[30] Comme le prévoit l'article 263 TFUE.

[31] A savoir les tribunaux de l'Etat Membre dans lequel le responsable du traitement a son principal établissement au sens de l'article 4 (13).

[32] Ces hypothèses ne sont pas limitatives, dès lors que, par exemple, l'article 74.2 permet à une personne concernée d'agir devant les tribunaux de l'Etat Membre où est établie l'autorité de contrôle pour l'obliger à agir suite à une plainte.

6.2. Absence de recours effectifs tels que garantis par la Charte des droits fondamentaux de l'UE

117. En permettant que l'autorité de contrôle chef de file soit différente de celle qui reçoit une plainte, la personne concernée qui a déposé cette plainte se verra confrontée à une autorité de contrôle étrangère parfois très éloignée géographiquement, parlant une langue autre que la sienne, et soumise à une procédure différente. Ces obstacles, ajoutés aux coûts que pourrait engendrer une telle procédure, sont susceptibles de contrevenir à l'article 16 TFUE en rendant cette procédure extrêmement difficile.

118. En outre, il convient de rappeler que l'article 47 de la Charte des Droits Fondamentaux de l'Union Européenne consacre le droit de bénéficier d'un recours effectif devant un tribunal. Cet article reprend les articles 13 et 6(1) de la CEDH. Cet accès effectif à une instance nationale est interprété *in concreto* par la Cour européenne des droit de l'homme.[33]

119. Or, dans le cas d'une application de l'article 74, un recours contre la décision prise par une autorité chef de file qui serait située à l'étranger devrait avoir lieu devant les tribunaux de cette autorité. Il en ressort que l'accès à un recours effectif contre une décision concernant un droit fondamental est rendue extrêmement difficile pour la personne concernée. Il existe certes l'article 74.4 selon lequel une personne, concernée par une décision adoptée par une autorité de contrôle dans un autre Etat Membre, peut demander à son autorité de contrôle de son pays de résidence d'introduire une action en son nom contre cette autorité de contrôle étrangère. Toutefois, cette disposition n'est pas des plus claires (qui supporte les frais, l'autorité peut-elle refuser d'intenter une telle action, quelle type d'action est visée ?), et sa mise en œuvre risque de ne pas suppléer aux difficultés auxquelles seront confrontées les personnes concernées qui désirent introduire une recours contre une décision d'une autorité étrangère.

120. Il en est de même en ce qui concerne l'article 75, qui prévoit le droit d'intenter une action judiciaire contre le responsable du traitement soit dans son pays d'établissement principal, soit dans l'Etat Membre de résidence de la personne concernée. En conséquence, il se peut qu'une multitude d'action judiciaires soient introduites dans différents Etats Membres et que toutes concernent la *même* violation des dispositions du règlement. Outre cette difficulté, il est possible qu'un autre tribunal soit saisi d'un recours contre la décision d'une autorité de contrôle. Dans ces hypothèses, un conflit de compétences ne manquera pas de se poser.

---

[33] Voir C.E.D.H., arrêt N°12964/87, 16 décembre 1992, *de Geouffre de la Pradelle v. France*.

121. Même si l'article 76, §§ 2 et 3, avance quelques principes pour tenter d'éviter des conflits de décisions judiciaires, la CPVP est d'avis il ressort clairement que la complexité du système empêche les personnes concernées de disposer d'un recours effectif pour faire valoir leurs droits, ceci en contradiction avec les articles 47 et 8 de la Charte des droits fondamentaux de l'Union Européenne, et 16 TFUE.

122. Pour ces raisons, la CPVP émet les plus grandes réserves quant au système de recours tel que proposé par le projet de règlement, tel que combiné avec le mécanisme de one-stop-shop. L'exercice du droit fondamental à la vie privée des citoyens s'en voit amoindri et la cohérence du système ne peut être assurée si les règles de compétences présentées restent inchangées.

6.3. Sanctions administratives (article 79)

123. La CPVP note que le texte voté par la Commission LIBE (article 79.2a)) prévoit qu'en cas de manquement au Règlement, l'autorité de protection des données imposera au minimum une des 3 sanctions suivantes : un avertissement (s'agissant d'une première violation non intentionnelle), des audits « protection des données » à réaliser à intervalles réguliers ou une amende administrative proportionnée d'un montant maximal de 100.000.000 d'euros ou, le cas échéant, d'un montant maximal équivalent à 5% du chiffre d'affaire mondial. Ces montants seront actualisés par voie d'acte délégué. Enfin, le responsable de traitement et le sous-traitant bénéficiant du label européen de la protection des données se verront imposer une amende administrative dans les seuls cas de violation intentionnelle ou par négligence (voy. point 77 ci-dessus).

124. La CPVP réitère ici les griefs qu'elle formule dans son avis 35/2012 au regard de la proposition initiale de la Commission européenne (points 154 – 163). La CPVP reste opposée à l'attribution d'une compétence de sanction administrative dans le chef des autorités de protection des données (quelle que soit la forme que prenne cette sanction administrative et fussent les différentes formes de sanctions présentées de manière graduelle).

125. La CPVP est particulièrement soucieuse de préserver l'objectif premier de son travail, soit la mise en conformité des traitements réalisés avec les exigences de la règlementation en matière de protection des données. A l'appui de son expérience, elle est en mesure d'affirmer que la médiation permet, dans la plupart des cas, d'obtenir cette mise en conformité mais aussi, une plus grande acceptation des règles applicables en la matière par les parties et partant, une prise de conscience réelle des enjeux de la protection de la vie privée et des données personnelles. Dans les rares cas d'échec de la médiation, la CPVP est

d'avis qu'il incombe aux autorités judiciaires de prendre le relais dans le respect des règles de la séparation des pouvoirs. La CPVP a donc clairement une préférence pour l'orientation prise par le Conseil (DAPIX) d'accorder aux autorités de protection des données la *faculté* (et non l'obligation) d'imposer des amendes administratives. Elle est par contre d'avis que des mesures telles les avertissements ou l'organisation d'audits réguliers peuvent s'avérer de précieux outils de contrôle et des vecteurs de mise en conformité. Quant aux montants de ces amendes, la CPVP les juge, fussent-ils maximaux, excessifs. Le pourcentage du chiffre mondial reste quant à lui incalculable à défaut de précisions complémentaires sur la notion de « chiffre d'affaire mondial ».

126. Enfin, la CPVP est opposée au régime de faveur accordé aux responsables de traitements et sous-traitants certifiés (article 39). Au contraire, il lui semble que l'octroi de ce label doit amener les bénéficiaires à un engagement strict sur le respect de la règlementation. La rupture de confiance doit, à ses yeux, *a fortiori* être plus sévèrement sanctionnée.

7. Chapitre IX : Dispositions particulières

7.1. Numéro de Registre national

127. Dans son avis 35/2012, la CPVP regrette la suppression de l'article 8.7. de la directive 95/46/CE qui permet aux Etats membres 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. Elle craint que le numéro d'identification du Registre national ne puisse plus être utilisé (points 169-171).

128. En conséquence, la CPVP plaide pour l'insertion d'un amendement autorisant le traitement du numéro de registre national tel que règlementé par la loi du 8 aout 1983 organisant un registre national des personnes physiques, en ce compris lorsque tel traitement est soumis à l'autorisation du Comité sectoriel compétent (voir supra points 68-70).

7.2. Traitements de données de santé à des fins thérapeutiques (article 81)

129. La CPVP attire l'attention sur la formulation inutilement sévère du fondement juridique pour le traitement de données concernant la santé dans le cadre de finalités thérapeutiques. Dans la législation actuelle, le traitement de données concernant la santé est toujours admissible dans ce contexte. L'article 81, point 1, a) du texte voté par la Commission LIBE prescrit toutefois que de tels traitements ne seront admissibles que s'ils sont encadrés par une législation européenne ou nationale spécifique. La CPVP ne comprend pas dans quelle

mesure une législation spécifique obligatoire dans tous ces cas pourrait contribuer à améliorer concrètement la protection de la vie privée du citoyen. Elle considère que dans de nombreuses situations, cela engendrera une bureaucratie superflue.

130. La CPVP estime par contre que la poursuite de la finalité thérapeutique combinée avce la garantie du secret professionnel (ou toute autre obligation de secret équivalente) suffit en principe pour justifier l'admissibilité[34] du traitement de données relatives à la santé à des fins thérapeutiques et propose dès lors de formuler l'article 81, point 1, a) comme suit :

"Dans les limites du présent règlement et conformément à l'article 9, paragraphe 2, point h), les traitements de données à caractère personnel relatives à la santé doivent être nécessaires :

(a) aux fins de la médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements ou de la gestion de services de santé et lorsque le traitement de ces données est effectué par un praticien de la santé soumis au secret professionnel, ou par une autre personne également soumise à une obligation de confidentialité équivalente, par le droit de l'Union ou d'un État membre ou par des réglementations arrêtées par les autorités nationales compétentes ; Le droit de l'Union ou d'un État membre peut apporter des mesures appropriées et spécifiques pour préserver les intérêts légitimes des personnes concernées ;

7.3. Les traitements de données à des fins de recherche historique, statistique et scientifique (article 83)

131. Les traitements réalisés à des fins de recherche historique, statistique et scientifique (HSS) bénéficient actuellement d'un régime favorable[35] et il est nécessaire que ce régime subsiste mais également que les règles et garanties soient davantage harmonisées afin de permettre leur application au niveau européen. En effet, de plus en plus de projets de recherche dépassent le cadre purement national et il est essentiel de faciliter le travail des scientifiques en évitant tant que possible les divergences des législations nationales.

Délai de conservation

132. Tout comme le projet initial de la Commission européenne, le projet voté par la Commission LIBE prévoit la possibilité de conserver les données plus longtemps à des fins de recherche

[34] En cas d'admissibilité d'un traitement, il convient évidemment de respecter également tous les autres principes qui seront repris dans le nouveau Règlement (finalité, proportionnalité, sécurité, etc.).

[35] 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.

HSS (article 5.e). La Commission LIBE ajoute comme finalité *l'archivage* et prévoit comme garantie additionnelle que des mesures de sécurité et d'organisation doivent être prises afin que les données ne soient accessibles que pour ces finalités. La CPVP accueille favorablement ces ajouts (la référence aux mesures de sécurité avait spécifiquement été suggérée par la CPVP dans son avis 35/2012[36]).

Compatibilité en cas de traitements ultérieurs

133. La CPVP estime toutefois qu'il serait utile de reprendre l'exception prévue actuellement à l'article 6 de la Directive 95/46/EC qui énonce que les traitements ultérieurs à des fins historiques, statistiques ou scientifiques (en ajoutant la finalité d'archivage) ne sont pas réputés incompatibles (dans le respect des garanties visées aux articles 83 et 83a).

Article 5.b : collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes (purpose limitation); Further processing of data for historical, statistical, scientific or archive purposes shall not be considered as incompatible subject to the conditions and safeguards referred to in article 83 and 83a;

134. La CPVP ne soutient pas la modification proposée au considérant 126 qui prévoit que les données traitées à des fins de recherche HSS pourraient être traitées à d'autres fins avec le consentement ou sur la base du droit de l'Union ou d'un Etat membre. Cela revient, à ses yeux à rétablir en partie l'article 6.4 dont la Commission LIBE propose cependant la suppression[37].

Recital 126. Scientific research for the purposes of this Regulation should include fundamental research, applied research, and privately funded research and in addition should take into account the Union's objective under Article 179(1) of the Treaty on the Functioning of the European Union of achieving a European Research Area. The processing of personal data for historical, statistical and scientific research purposes should not result in personal data being processed for other purposes, unless with the consent of the data subject or on the basis of Union or Member State law.

Bases de légitimité: le consentement

---

[36] Point 179.

[37] Point 36 avis 35/2012.

135. Concernant les bases de légitimité, la Commission LIBE prévoit la réintroduction de la nécessité du consentement dans le cadre du traitement des données médicales à des fins de recherche HSS. Comme le prévoit déjà la Directive 95/46/CE, les Etats membres peuvent prévoir une dérogation à la nécessité du consentement dans le cadre des recherches poursuivant un objectif d'intérêt public important[38]. Malgré la possibilité offerte à la Commission européenne d'adopter des actes délégués pour spécifier davantage cet objectif d'intérêt public important, la CPVP estime que le principe de réintroduction de la nécessité du consentement n'est pas une bonne chose et que cette proposition entrainera clairement une divergence entre les législations nationales.

Article 81

1a. When the purposes referred to in points (a) to (c) of paragraph 1 can be achieved without the use of personal data, such data shall not be used for those purposes, unless based on the consent of the data subject or Member State law.

1b. Where the data subject's consent is required for the processing of medical data exclusively for public health purposes of scientific research, the consent may be given for one or more specific and similar researches. However, the data subject may withdraw the consent at any time.

1c. For the purpose of consenting to the participation in scientific research activities in clinical trials, the relevant provisions of Directive 2001/20/EC shall apply.

2. Processing of personal data concerning health which is necessary for historical, statistical or scientific research purposes shall be permitted only with the consent of the data subject, and shall be subject to the conditions and safeguards referred to in Article 83.

~~***2a. Member States law may provide for exceptions to the requirement of consent for research, as referred to in paragraph 2, with regard to research that serves a high public interests, if that research cannot possibly be carried out otherwise. The data in question shall be anonymised, or if that is not possible for the research purposes, pseudonymised under the highest technical standards, and all necessary measures shall be taken to prevent unwarranted re-identification of the data subjects. However, the data subject shall have the right to object at any time in accordance with Article 19.***~~

136. Par ailleurs, la CPVP ne comprend pas la raison pour laquelle, à l'article 83a concernant les archives, il est prévu que le droit national doit porter notamment sur la question du

[38] Considérant 34 de la Directive.

consentement. La CPVP ne soutient absolument pas l'idée que les traitements par les services d'archive doivent faire l'objet d'un consentement.

Article 83a

1. Once the initial processing for which they were collected has been completed, personal data may be processed by archive services whose main or mandatory task is to collect, conserve, provide information about, exploit and disseminate archives in the public interest, in particular in order to substantiate individuals' rights or for historical, statistical or scientific research purposes. These tasks shall be carried out in accordance with the rules laid down by Member States concerning access to and the release and dissemination of administrative or archive documents and in accordance with the rules set out in this Regulation, specifically with regard to consent and the right to object

137. Si la nécessité du consentement devrait être évitée, il faudrait néanmoins que chaque projet de recherche fasse l'objet d'une mise en balance des intérêts en présence. C'est pourquoi, comme déjà expliqué dans son précédent avis 35/2012, « *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* ».

Article 6.2. Processing of personal data which is necessary for the purposes of historical, statistical or scientific research shall be lawful subject to the conditions and safeguards referred to in Article 83.

Conditions de traitement

138. Concernant les conditions à respecter dans le cadre des recherches HSS, l'article 83.1 promeut utilement l'usage de données anonymes ou de la pseudonymisation en matière de recherche scientifique, et cette finalité est parfaitement en ligne avec notre législation nationale et d'autres standards internationaux[39]. Néanmoins, la CPVP estime que le texte de l'article 83, point 1, devrait permettre l'utilisation de données directement identifiables lorsqu'il est impossible de faire usage de données anonymes ou de la pseudonymisation. En ne prévoyant pas cette possibilité, le projet de texte poussera les responsables à se tourner

[39] 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.

vers d'autres bases de légitimité que celles prévues aux articles 6.2 et 9.2.i et ia (ce qui reviendra à leur éviter également l'application des autres garanties - pourtant utiles - prévues aux articles 81 et 83). On ne peut sérieusement envisager que la recherche historique doivent nécessairement se limiter à des données anonymes ou opter pour la pseudonymisation alors que par nature, l'identité des personnes faisant l'objet de la recherche s'avère souvent nécessaire. Il conviendrait donc dès lors de rajouter les termes prévus initialement par la Commission européenne *« as long as these purpose can be fulfilled in this manner »*.

Article 83

In accordance with the rules set out in this Regulation, personal data may be processed for historical, statistical or scientific research purposes only if:

(a) these purposes cannot be otherwise fulfilled by processing data which does not permit or not any longer permit the identification of the data subject;

(b) data enabling the attribution of information to an identified or identifiable data subject is kept separately from the other information under the highest technical standards, and all necessary measures are taken to prevent unwarranted re-identification of the data subjects, as long as these purpose can be fulfilled in this manner .

Droits des personnes concernées

139. Concernant les exceptions à l'exercice des droits des personnes concernées, la CPVP accueille favorablement l'intention de les prévoir directement dans le règlement[40]. Elle regrette cependant l'absence d'exception au droit d'accès ainsi qu'au droit de rectification (pourtant actuellement prévu par l'article 13.2 de la Directive 95/46/CE).

Article 15 and 16 shall not apply under condition that the information or part of the information referred to in Article 15 or the rectification is likely to render impossible or seriously impair the achievement of the objectives of the scientific, statistical or historical 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 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.

[40] Voir le point 180 de l'avis 35/2012 qui critiquait l'intention de la Commission européenne de régler ce problème par acte délégué.

140. L'exception au droit d'information est prévue par la Commission LIBE (art. 14.5.b). La CPVP estime qu'elle pourrait s'étendre à la finalité statistique (art.81a)[41]. Par ailleurs, une exception au devoir d'information devrait également être prévue pour les collectes directes de données[42] lorsque celle-ci peut rendre impossible ou sérieusement compromettre les objectifs scientifiques poursuivis. Dès le moment où la transparence ne risque plus de compromettre la finalité, elle pourrait être réalisée. Il s'agit par exemple d'éviter d'être contraint de préciser préalablement à la collecte d'information qu'une étude psycho-sociologique porte sur les comportements éventuellement racistes des individus. Il est évident que la précision de cette finalité aura un impact sur les réponses fournies ce qui pourrait fausser les résultats[43]. La CPVP fait à cet égard une proposition de texte basé sur celui déjà proposé dans son avis 35/2012 :

Article 14

5. Paragraphs 1 to 4 shall not apply, where:

(b) the data are processed for historical, statistical or scientific research purposes or for archive services subject to the conditions and safeguards referred to in Articles 81 and 83, are not collected from the data subject and the provision of such information proves impossible or would involve a disproportionate effort and the controller has published the information for anyone to retrieve; or

14.5.ba: data are processed for historical, statistical or scientific research purposes subject to the conditions and safeguards referred to in Articles 81 and 83 and the provision of such 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, statistical or historical research. 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 17.3.ca

for archive services in accordance with Article 83a;

---

[41] Il en est de même pour l'exception au droit d'effacement (17.3.c).

[42] 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).

[43] Informer clairement des finalités précises de la recherche peut évidemment influencer et dès lors compromettre les 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.

8. Chapitre X : Actes délégués et actes d'exécution

8.1. Actes délégués (article 86)

141. Pour de multiples raisons auxquelles il est ici renvoyé à l'avis 35/2012 (points 182-185), la CPVP s'est d'emblée opposée aux très grand nombre d'actes délégués prévus par le projet de règlement déposé par la Commission européenne. La réflexion de la Commission LIBE à cet égard ne semble pas aboutie. La liste des actes délégués de l'article 86 reste ainsi ouverte. La CPVP accueille néanmoins favorablement le recours, dans plusieurs dispositions, à la compétence d'avis et de recommandation du Comité européen de la protection des données (CEPD) ainsi que la consultation préalable de ce dernier dans les cas où l'adoption d'un acte délégué est maintenue.

L'Administrateur f.f., Le Président,

(sé) Patrick Van Wouwe (sé) Willem Debeuckelaere