Association des Banques et Banquiers, Luxembourg
The Luxembourg Bankers' Association
Luxemburger Bankenvereinigung

Luxembourg, 11 septembre 2012

Avis de l'ABBL sur la proposition de règlement 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

La protection des données et la protection de la vie privée sont des domaines fondamentaux dans lesquels il est d'importance primordiale qu'une législation cohérente et uniforme sur le plan européen soit adoptée. L'ABBL estime important, en 2012, de renforcer la protection du citoyen face aux abus de traitements de données personnelles qui ont lieu en particulier dans la sphère d'internet.

Parallèlement à la réglementation relative à la protection des données, un ensemble de règles de source européenne sont imposées aux établissements bancaires. La réglementation en matière de protection des données ne peut être déconnectée de l'environnement légal dans lequel vivent les entreprises européennes.

L'activité bancaire implique de la part des professionnels du monde de la finance la gestion des données personnelles relatives à leurs clients. Le banquier diligent est traditionnellement soucieux de respecter la sphère privée de son client, dont le principe de non-ingérence est une illustration. Ainsi, suivant une jurisprudence constante, le banquier ne doit pas s'immiscer dans les affaires de son client notamment en s'informant sur celui-ci au-delà de ce qui est nécessaire, ou en prenant une décision qui relève de la compétence de son client. De plus, du fait de l'application du secret bancaire, les banques veillent à la sécurité et la confidentialité des données dont elles sont les gardiens.

En même temps cependant, le banquier est nécessairement détenteur d'informations personnelles relatives aux personnes avec lesquelles il est en relation. Suivant la jurisprudence luxembourgeoise, « *par profession, le banquier est détenteur d'informations confidentielles sur ses clients et sur des tiers* »[1]. Liée à une évolution réglementaire inéluctable, le volume d'informations confidentielles détenues par le banquier ne cesse d'augmenter. C'est ainsi que la directive MIFID[2] impose aux professionnels de la finance de procéder à une évaluation de la situation de chaque client afin de pouvoir lui proposer les produits et services les plus adaptés à ses besoins. De même, en matière d'octroi de crédit à la consommation, le banquier doit s'enquérir de sa capacité de financement et ainsi évaluer « *la solvabilité du consommateur, à partir d'un nombre suffisant d'informations, fournies, le cas échéant,*

[1] Trib. Lux. 24 avril 1991, p 28, 173
[2] Directive 2004/39 concernant les marchés d'instruments financiers.

par ce dernier »[3]. La proposition de directive sur les contrats de crédit relatifs aux biens immobiliers à usage résidentiel prévoit également un certain nombre d'obligations à charge du banquier et en particulier qu'il « *procède à une évaluation rigoureuse de la solvabilité du consommateur, sur la base de critères incluant notamment les revenus, l'épargne, les dettes et les autres engagements financiers du consommateur* »[4].

Parallèlement aux informations relatives à ses clients, le banquier gère, par nécessité, des données relatives à des tiers, que ce soit afin de se prémunir contre d'éventuels fraudeurs, en vue de la prévention du blanchiment d'argent et du financement du terrorisme, ou encore en application de certaines dispositions légales, notamment relatives aux opérations d'initiés et aux manipulations de marché.

Dans le cadre de la lutte contre le blanchiment d'argent, les banques sont tenues d'identifier non seulement leurs clients mais également les personnes avec lesquelles elles effectuent des transactions à titre occasionnel (dès lors qu'il existe un soupçon de blanchiment ou que le montant de la transaction dépasse 15.000 euros). Les banques sont tenues de conserver les données relatives à ces personnes pendant une durée de cinq années à compter de l'exécution de la transaction. Quant bien même la banque se serait abstenu d'effectuer une transaction en raison de soupçons de blanchiment, il est plus qu'opportun qu'elle retienne les données relatives à ces personnes (en particulier afin d'éviter d'entrer à nouveau en relation avec de telles personnes) sans que celles-ci soient obligatoirement informées du traitement dont elles font l'objet.

Une logique similaire opère au regard de la lutte contre la corruption et le blanchiment d'argent lié à des actes de corruption, les banques étant tenues d'instaurer « *des procédures adéquates adaptées au risque afin de déterminer si le client est une personne politiquement exposée* »[5]. Il incombe ainsi aux établissements de crédit d'identifier « *les personnes physiques qui occupent ou se sont vu confier une fonction publique importante ainsi que les membres directs de leur famille ou des personnes connues pour leur être étroitement associées* ». Il est ainsi parfaitement légitime, sinon légalement requis, que les banques constituent, pour ce faire, des fichiers de personnes à risque, voire indésirables. Ces fichiers peuvent aussi bien contenir les noms de personnes avec lesquelles la banque a pu être en contact que ceux de personnes avec lesquelles elle ne souhaite pas ou n'est pas en droit d'établir de relations. Il peut également s'agir des personnes à l'encontre desquelles il existe des mesures restrictives, ou d'autres personnes faisant l'objet de sanctions au titre de la politique étrangère et de sécurité commune de l'Union européenne.

En application de la réglementation relative aux opérations d'initiés et aux manipulations de marché, les émetteurs d'instruments financiers sont tenus d'établir une liste des personnes travaillant pour eux et ayant accès à des informations

[3] Article 8 de la directive 2008/48/CE du 23 avril 2008.
[4] Article 14 de la proposition de directive sur les contrats de crédit relatifs aux biens immobiliers à usage résidentiel (COM 2011(142))
[5] Article 11.4 de la directive 2005/60/CE du 26 octobre 2005.

privilégiées[6]. Ces listes représentent un outil indispensable pour les entreprises en vue de prévenir les opérations d'initiés et manipulation de marché.

L'existence même de l'ensemble de ces fichiers et informations répertoriées par les établissements de crédit, indispensables à leur bon fonctionnement, ne doit pas être mise en péril par les règles relatives à la protection des données. Quelles sont dans ces hypothèses particulières les règles de conflit applicables ? Il importe que le législateur européen donne des solutions à cet égard et établisse l'ordre de primauté des règles issues des règlements et directives européennes. Une solution pourrait consister à introduire dans le règlement sur la protection des données la règle déjà applicable dans les ordres juridiques nationaux suivant laquelle la loi spéciale (directive relative à la lutte contre le blanchiment d'argent, directive relative aux abus de marché,…) déroge à la règle générale (règlement sur la protection des données).

Par ailleurs, les banques traitent des données relatives à des fraudes ou tentatives de fraude, dans l'intérêt des consommateurs et de toute personne utilisant les services de paiement. Il serait incompatible avec la logique de prévention des fraudes que soit imposé aux banques de recueillir le consentement des fraudeurs pour que les données les concernant soient répertoriées. L'article 79 de la directive sur les services de paiement (directive 2007/64/CE) prévoit ainsi que « l*es États membres autorisent le traitement des données à caractère personnel par les systèmes de paiement et les prestataires de services de paiement lorsque cela est nécessaire pour garantir la prévention, la recherche et la détection des fraudes en matière de paiements ».* S'il est compréhensible que ces traitements de données doivent être réalisés en conformité avec la directive 95/46/CE comme l'indique l'article 79 de la directive 2007/64/CE, il convient néanmoins de prévoir des exceptions aux règles relatives au consentement et à l'information des personnes concernées. En matière de prévention des fraudes comme en matière criminelle en général (lutte contre le blanchiment d'argent, procédures applicables à l'entraide judiciaire internationale en matière pénale), la règle du « no tipping off » (c'est-à-dire suivant laquelle il est interdit d'informer une personne qu'elle est visée par une enquête ou une procédure judiciaire) s'est en effet imposée afin de préserver l'efficacité des enquêtes en ces domaines.

Enfin, une législation assortie de sanctions à caractère pénal se doit d'être précise et d'utiliser une terminologie claire. Or de nombreuses dispositions de la proposition de règlement utilisent des termes flous aux contours incertains, que seuls des actes délégués viendront compléter ultérieurement. Une telle manière de légiférer introduit une trop grande insécurité juridique. Dans de nombreux articles du projet de règlement, la possibilité pour la Commission d'adopter des actes délégués devrait être remplacée par des clarifications introduites dans le dispositif du règlement. Si des actes devaient être adoptés ultérieurement, il serait utile que des lignes de conduite puissent être émises par les autorités de contrôle, donnant des indications aux entreprises sur la manière de procéder, en particulier pour les éléments nouveaux introduits par le texte, tel que l'analyse d'impact.

[6] Directive 2003/6/CE du 28 janvier 2003 sur les opérations d'initiés et les manipulations de marché

Chapitre I – Dispositions générales

Article 4 : Définitions

« Traitement de données » : la notion de traitement de données inclut la « *consultation* ». Si la simple « *consultation* » en tant que traitement de données ne posait pas de problème sous l'empire de la directive 95/46/CE, il en est différemment suivant la proposition de règlement. En effet, suivant la nouvelle définition du « *consentement* » de la proposition de règlement, le consentement ne peut être tacite ; il doit dans tous les cas être explicite et exprimer l'accord de la personne concernée à ce que ses données personnelles fassent l'objet d'un traitement. Si le seul critère de licéité du traitement est le consentement de la personne concernée, la seule possibilité pour « *consulter* » le nom d'une personne dans un fichier ou une base de données consiste à lui demander son accord avant de « *consulter* » ces données, ce qui risque fort de ne jamais être appliqué si les données se trouvent en libre accès pour la personne qui « *consulte* » (exemple : utilisation d'un annuaire, consultation des membres d'un réseau social, interrogation sur Internet,…). Or, en toute logique, si le nom d'une personne figure dans un fichier ou une base de données, c'est qu'il a déjà donné son consentement à ce premier traitement. Autrement dit, toute consultation d'une donnée suppose au préalable un traitement antérieur au cours duquel les données ont été collectées suivant des règles respectant la protection des données. L'un des buts du nouveau règlement étant notamment de simplifier et de réduire les formalités, le terme « *consultation* » devrait être supprimé de la liste des opérations considérées comme « *traitement de données* ».

« Consentement » : Suivant la proposition de règlement, le consentement de la personne concernée se définit comme *« toute manifestation de volonté, libre, spécifique, informée et explicite par laquelle la personne concernée accepte, par une déclaration ou par un acte positif univoque, que des données à caractère personnel la concernant fassent l'objet d'un traitement* ». Or, suivant la directive 95/46/CE, le consentement pouvait être tacite. Il ne peut en pratique en être autrement dans un grand nombre de situations, en particulier pour toute vidéosurveillance. Si une personne pénètre dans un lieu faisant l'objet d'une vidéosurveillance, en connaissance de cause puisque des panneaux informatifs figurent dans de tels lieux, elle consent tacitement à ce traitement. Un consentement exprès n'est pas envisageable dans ce cas précis.

De même, concernant la consultation d'une base de données (la simple consultation étant considérée comme un traitement de données), si une personne figure dans un annuaire public, le consentement à la consultation des données la concernant dans cet annuaire est obligatoirement tacite, l'opposition à cette consultation se traduisant nécessairement par le fait que les données ne figurent pas dans l'annuaire public.

La définition qui figure actuellement dans la directive 95/46/CE est plus souple et permet une meilleure adaptation aux différentes réalités entourant les traitements de données. Les termes « *explicite* » et « *par une déclaration ou par un acte positif univoque* » devraient être supprimés. Ils pourraient le cas échéant être remplacés par les termes « *ou par un acte non équivoque* », ce qui permettrait notamment de justifier la surveillance vidéo lorsque la personne pénètre dans un lieu surveillé en connaissance de cause.

Si la définition du consentement devait être maintenue, des exceptions devraient être prévues dans les hypothèses dans lesquelles seul un consentement tacite est possible.

« **Etablissement principal** » : cette notion ne tient pas compte de la situation des groupes d'entreprises. Pour ceux-ci, il est difficile de définir quel est « *l'établissement principal* » et quel est le « *sous-traitant* » au sens du projet de règlement. Une clarification est absolument nécessaire comte tenu non seulement des obligations qui en découlent pour les responsables de traitement, mais aussi et surtout au niveau de conséquences qui en découlent quant à la compétence des autorités de surveillance. Une imprécision plane à ce niveau du fait qu'il sera difficile de déterminer quel sera l'établissement principal. En effet, dans l'hypothèse des groupes d'entreprises, plusieurs entités juridiques dans différents pays peuvent avoir un rôle dans la détermination des finalités, des conditions et des modalités d'un traitement de données, indépendamment de la localisation de l'administration centrale. Le recours à la notion connue d' « *établissement stable* » serait plus adapté.

« Violation de données à caractère personnel » : Etant donné la lourdeur des obligations qui incombe au responsable du traitement, il serait largement souhaitable de limiter l'étendue de cette définition du concept de « *violation de données à caractère personnel* » aux seules violations qui ont eu un impact réel et ont porté préjudice à la personne concernée. C'est pourquoi l'ABBL suggère d'ajouter à la fin de la définition les termes suivants : « *lorsque cette violation est susceptible de porter préjudice à la personne concernée* ». Les obligations liées à de telles violations devraient être proportionnées à la gravité du problème et aux conséquences que celui-ci peut comporter. Ce n'est qu'en cas de conséquence sur la vie privée que les obligations prévues aux articles 31 et suivants devraient être applicables. Ainsi, seules les violations portant « *atteinte aux données à caractère personnel ou à la vie privée* » doivent faire l'objet d'une information des personnes concernées (voir en particulier les critères posés suivant le considérant 66). Ainsi, pour sauvegarder la cohérence de la réglementation européenne, les mêmes critères que ceux retenus dans la directive 2002/58/CE modifiée devraient être retenus : « *une violation devrait être considérée comme affectant les données à caractère personnel ou la vie privée d'un abonné ou d'un particulier lorsqu'elle est susceptible d'entraîner, par exemple, le vol ou l'usurpation d'identité, une atteinte à l'intégrité physique, une humiliation grave ou une réputation entachée* ». Cela pourrait, par exemple, être le piratage de bases de données contenant des adresses email. Le responsable du traitement devrait donc analyser les conséquences de la violation sur les personnes afin d'en déterminer la gravité. Il est enfin à noter qu'une destruction accidentelle de données ne comporte en général pas de dommage en termes de protection des données pour la personne concernée.

« Enfant » : d'un point de vue strictement juridique, un enfant est le descendant au premier degré d'une personne, l'âge n'ayant aucune incidence puisqu'une personne reste toute sa vie l'enfant d'une autre personne. Pour être correct, il conviendrait de remplacer la notion d' « *enfant* » par celle de « *mineur* », ce qui correspond effectivement à la définition d'une « *personne âgée de moins de dix-huit ans* ».

Chapitre II - Principes

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

L'article 5 de la proposition de règlement détaille des principes relatifs au traitement des données à caractère personnel. Suivant cette disposition, les données à caractère personnel doivent être « *traitées de manière licite, loyale et transparente au regard de la personne concernée* » (article 5a). Pour les raisons évoquées ci-dessus (voir introduction), le traitement ne peut pas être dans tous les cas *« transparent au regard de la personne concernée* ». Il en est ainsi en particulier dans tous les cas où il est dans l'intérêt d'une enquête et de l'établissement de crédit (cas des fraudes en matière de paiement notamment) que les personnes concernées ne soient pas informées du traitement les concernant. C'est pourquoi des exceptions pour certaines hypothèses limitées devraient être introduites dans le texte du règlement.

L'article 5 c) précise que les données doivent être « *adéquates, pertinentes et limitées au minimum nécessaire au regard des finalités pour lesquelles elle sont traitées* ». Cette exigence de traitement « minimaliste » ne doit pas venir contredire certains textes européens qui exigent au contraire qu'un maximum d'informations soit obtenu. Il en est ainsi en particulier en matière de lutte contre le blanchiment d'argent qui impose que le banquier (et l'ensemble des professionnels soumis à la législation contre le blanchiment d'argent) ait une connaissance aussi extensive que possible de son client afin de s'assurer qu'il ne sera pas utilisé pour blanchir les capitaux issus d'une infraction pénale. Par ailleurs, les obligations figurant dans la directive MIFID impliquent également une bonne connaissance par le banquier de son client. Il en est ainsi également dans la proposition de directive sur le crédit immobilier, suivant laquelle l'établissement de crédit qui accorde un crédit à un client doit être en mesure d'évaluer la capacité de crédit de son client sur la base de suffisamment d'informations avant la conclusion du crédit, suivant le principe d'un « *crédit responsable* ». C'est la raison pour laquelle, plutôt que de prévoir un principe absolu consistant à imposer un traitement minimaliste des données, il conviendrait plutôt de retenir l'idée d'un traitement « *proportionné* » des données, conforme à l'objectif dans lequel les données sont traitées.

L'article 5 e) impose que les données soient conservées « *pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées* ». Seules les exceptions relatives aux traitements à des fins de recherche historique, statistiques ou scientifiques peuvent déroger à ce principe. Il importe néanmoins de prendre en considération les délais de conservation imposés par certains textes légaux (à titre d'exemples : dix ans suivant l'article 16 du Code de commerce, cinq ans au titre de la législation anti blanchiment pour ce qui concerne la documentation relative au client ainsi qu'aux transactions) ainsi que les délais de prescription qui imposent de conserver pendant dix ans (en matière d'actes mixtes) tout élément de preuve concernant l'exécution des obligations qui incombent à une partie à un litige. Dans ces conditions, la plupart des documents à caractère contractuel doivent pouvoir être conservés pendant 10 ans après la fin de la relation contractuelle. Ainsi, les dispositions du règlement devraient préciser qu'elles sont applicables sans préjudice des dispositions légales relatives aux délais de

conservation imposés par des réglementations spécifiques et sans préjudice des dispositions relatives aux délais de prescription.

A l'article 5 f), il est requis des responsables du traitement qu'ils justifient, en « apportant la preuve » que le traitement est effectué conformément au règlement. Cette exigence de preuve risque d'être difficile à rapporter dans toutes les circonstances et nécessitera des charges administratives lourdes en termes de procédures afin de justifier chaque traitement et la manière dont ils sont conduits. En tout état de cause, cette obligation devrait consister en une obligation de moyen et non de résultat.

Article 6 : Licéité du traitement

L'article 6.1 c) précise que le traitement est licite s'il « *est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis* ». Cette disposition est très restrictive dans la mesure où elle ne vise que les obligations légales. Or, un grand nombre de textes réglementaires ainsi que des circulaires ou autres textes relevant plus de la « soft law » imposent des obligations auxquelles les professionnels sont tenus de se conformer. Il en est particulièrement ainsi des professionnels du secteur financier qui doivent se conformer aux règles édictées par les autorités de surveillance (tant luxembourgeoises qu'européennes), auxquelles sont attachées des sanctions administratives en cas de non conformité. Ces autorités émettent parfois des recommandations ou des « guidelines » qui, sans constituer des règles impératives sont néanmoins imposées aux établissements de crédit[7]. L'article 6.1 c) devrait se lire ainsi : « *le traitement est nécessaire au respect d'une obligation légale ou réglementaire à laquelle le responsable du traitement est soumis, ainsi qu'au respect des recommandations, injonctions ou autres exigences émises par des autorités de surveillance* ».

L'article 6.4 tend à restreindre les traitements ultérieurs de données lorsque la finalité est incompatible avec celle pour laquelle les données ont été collectées. La dernière phrase du paragraphe n'a pas sa place dans cette disposition dans la mesure où les modifications des clauses et conditions générales d'un contrat n'ont pas nécessairement pour effet de modifier la finalité du traitement. Il convient de supprimer cette phrase.

Article 7 : Conditions de consentement

L'article 7.1 impose au responsable de traitement de prouver que la personne concernée a consenti au traitement de ses données. Cette preuve risque en pratique d'être difficile à rapporter dans certains cas. Si la signature des conditions générales d'un contrat constitue effectivement une preuve du consentement d'un client, il est des cas dans lesquels le consentement n'est pas écrit. Il en est ainsi par exemple du cas de la surveillance par camera vidéo d'un distributeur automatique de billets, dans lequel le simple fait de se servir du distributeur implique un consentement, forcément tacite.

[7] Voir à titre d'exemple les « guidelines » émises par l'EBA (European Banking Authority).

Dans l'hypothèse d'un consentement écrit, il est également délicat de prouver que le consentement a été effectivement « informé ».

L'article 7.4 précise que « *le consentement ne constitue pas un fondement juridique valable pour le traitement lorsqu'il existe un déséquilibre significatif entre la personne concernée et le responsable du traitement* ». S'il est indéniable qu'un déséquilibre significatif existe dans le cadre d'une relation de travail entre un employé et son employeur, des situations similaires risquent de se produire dans de nombreuses hypothèses, y compris dans toute relation contractuelle dans laquelle le client est généralement considéré comme en position de faiblesse par rapport au professionnel. Le terme « *déséquilibre significatif* » est d'ailleurs utilisé dans la directive relative aux clauses abusives pour ce qui concerne les contrats d'adhésion. Ainsi, le consentement de la personne concernée risque de ne jamais pouvoir être considéré comme un fondement juridiquement valable pour le traitement de données dans le cadre d'un contrat puisque les conditions générales sont par définition des contrats d'adhésion. La notion de « *déséquilibre significatif* » devrait donc être clairement définie afin d'éviter d'aboutir à ce type de situation. Une solution consisterait par exemple à limiter le champ de cette disposition uniquement aux relations de travail.

Article 8 : Traitement de données à caractère personnel relatives aux enfants

Il transparaît de l'article 8.1 une certaine confusion dans la mesure où la protection envisagée à l'égard des enfants ne concerne que ceux âgés de moins de 13 ans. Quelle est l'utilité de la définition précisant « *moins de 18 ans* » si seuls ceux de moins de 13 ans sont visés ? Par ailleurs, la formulation « *qui en a la garde* » est appropriée pour des choses (cf article 1384 du code civil) mais non pour des personnes. Il conviendrait de remplacer cette notion par celle de « *personne exerçant l'autorité parentale* ».

Article 9 : Traitements portant sur des catégories particulières de données à caractère personnel

L'article 9.1 interdit le traitement de données concernant des condamnations pénales. Le paragraphe 2 j) de ce même article déroge au principe posé à l'article 9.1 dans la mesure où le traitement « *est nécessaire au respect d'une obligation légale ou réglementaire à laquelle le responsable du traitement est soumis* ». La question se pose de savoir si, dans ce cadre, les entreprises peuvent demander au personnel qu'elles recrutent de présenter un extrait de casier judiciaire. Cette exigence est souvent requise pour certaines activités, notamment en matière de gardiennage. Ainsi la loi du 12 novembre 2002 impose que la demande d'autorisation d'établissement soit accompagnée d'une liste du personnel engagé et contienne un extrait récent du casier judiciaire. En revanche, en l'absence d'exigence légale précise, il ne semble pas permis aux entreprises de requérir de telles données. Pourtant, pour des raisons légitimes de sécurité, les établissements bancaires exigent la production d'un extrait de casier judiciaire, en particulier lorsque la personne concernée est appelée à exercer certaines fonctions (sécurité, gestion de caisse, etc), mais aussi des fonctions de direction. Ainsi, l'EBA (European Banking Authority) a émis un document dans lequel il est requis que des informations concernant notamment d'éventuelles condamnations pénales soit renseignées concernant les personnes membres de la direction ou

détenant des fonctions clés dans un établissement de crédit[8]. En pratique, l'exigence consistant à fournir un extrait de casier judiciaire (vierge) existe pour de nombreuses professions (sécurité privée, transport de fonds, etc.)[9]. Ne faut-il pas considérer que le fait de demander un extrait de casier judiciaire, lorsqu'il est vierge, ne constitue pas un traitement de données judiciaires ?
Il conviendrait de s'assurer que de telles pratiques puissent perdurer même en l'absence de texte législatif ou réglementaire, dès lors que des exigences de sécurité imposent à l'employeur la vérification de l'absence de condamnation pénale dans le chef des personnes qu'il embauche. Proposition d'amendement : « *Le fait pour un employeur de requérir un extrait de casier judiciaire en vue de l'embauche d'un employé lorsque des exigences de sécurité l'imposent, ne constitue pas un traitement de données relatives aux condamnations pénales* ».
Une solution alternative consisterait également à étendre la rédaction du point j) de cet article : « *le traitement (…) est nécessaire au respect d'une obligation légale ou réglementaire à laquelle le responsable du traitement est soumis ainsi qu'au respect des recommandations, injonctions ou autres exigences émises par des autorités de surveillance*, ou à l'exécution… ».

Chapitre III - Droits des personnes concernées (articles 11 à 21)

Le chapitre III est révélateur de l'esprit du projet de règlement, lequel tend à renforcer la protection des données à caractère personnel et à permettre un exercice plus efficient des droits des personnes concernées.

1. Obligations du responsable de traitement

Article 11 : Transparence des informations et des communications

Le projet de règlement introduit un principe de transparence dans le traitement des données (article 11), lequel vient s'ajouter aux principes existants, et renforce encore, s'il en était besoin, la protection des droits des personnes concernées. Il prévoit notamment un libre accès aux règles internes du responsable de traitement (notion de « *règles internes facilement accessibles* »).
Le considérant 51 prévoit que le droit d'accès « *ne devrait pas porter atteinte aux droits et libertés d'autrui, notamment au secret des affaires […]* ». Néanmoins, il est ensuite indiqué que « *ces considérations ne sauraient aboutir au refus de toute information de la personne concernée* ». Cet ajout ne devrait pas avoir pour conséquence une obligation pour le responsable de traitement de communiquer ses procédures internes mais uniquement des informations sur les modalités du traitement poursuivi. En lien avec le considérant 51 et dans un souci d'équilibre, il devrait être envisagé de prévoir l'insertion d'une référence à l'intérêt légitime du responsable de traitement afin qu'il puisse s'opposer à une communication sans limites concernant son fonctionnement interne.

[8] EBA Consultation Paper on draft Guidelines for assessing the suitability of members of the management body and key function holders of a credit institution, 18 avril 2012.
[9] http://www.justice.public.lu/fr/affaires-penales/casier-judiciaire/index.html

Article 12 : Procédures et mécanismes prévus pour l'exercice des droits de la personne concernée

Dans l'hypothèse où une personne concernée interrogerait un responsable de traitement quant au traitement des données la concernant, l'article 12 (2) impose à ce dernier de répondre dans un délai d'un mois. Ce délai ne peut être maintenu. Il ne tient pas compte de la complexité éventuelle de la demande nécessitant le cas échéant des recherches sur de multiples supports (par exemple pour retrouver un enregistrement téléphonique). Il serait préférable de retenir un « *délai raisonnable* » de réponse, sans mention chiffrée, avec le cas échéant des indications dans les Considérants sur ce qu'il convient d'entendre par « *raisonnable* ».

Une solution alternative consisterait à imposer la réponse dans un délai d'un mois tout en permettant au responsable de traitement, au cas où les informations demandées ne seraient pas encore disponibles d'indiquer au demandeur un délai endéans lequel les informations seront délivrées. Proposition d'amendement : « *Si les informations ne peuvent être disponibles endéans le délai d'un mois, le responsable de traitement indique le délai endéans lequel les informations pourront être délivrées* ».

Concernant la forme de la réponse devant être apportée, elle devrait, selon le projet de règlement, être donnée par écrit ou par voie électronique si la personne formule sa demande de cette manière. Cette obligation peut être difficilement réalisable pour le responsable de traitement en fonction de la nature, du volume ou de la quantité de données ou de traitements concernés. Il serait préférable de prévoir que le responsable de traitement réponde de la manière appropriée en fonction du type de demande qui lui est faite.

Par ailleurs, lorsque le responsable de traitement estime qu'une demande est manifestement excessive, il peut exiger le paiement de frais. Il lui incombe cependant de faire la preuve que la demande est excessive. Sur ce point, la Commission est habilitée à « *préciser davantage les critères et conditions applicables* » à ces demandes et aux frais pouvant être éventuellement demandés (article 12 (5)). Comme à de nombreuses reprises dans ce projet de règlement, ce pouvoir normatif de la Commission pourrait avoir pour conséquence de rendre inefficace cette clause si d'aventure elle fixait des critères ne permettant que difficilement au responsable de traitement de faire valoir qu'une demande est manifestement excessive. A tout le moins, il pourrait être envisageable qu'une demande effectuée une fois par an ne soit pas excessive et puisse être effectuée sans frais. Plutôt que de laisser à la Commission ce pouvoir normatif, il serait plus sûr et prévisible pour les entreprises si les critères permettant de considérer des demandes comme « excessives » étaient déterminés dans le règlement lui-même (par exemple, demandes répétées, demandes non motivées, absence d'intérêt légitime, …). Il serait en effet souhaitable de limiter ce type de demandes aux seules personnes justifiant d'un intérêt légitime afin d'éviter une avalanche de demandes surtout de personnes n'ayant aucun lien avec l'entreprise concernée.

Article 14 : Informations à fournir à la personne concernée

Le projet de règlement prévoit un nombre relativement important d'informations à fournir. La fourniture de la plupart de ces informations était déjà prévue dans les textes actuels. Cependant, un point h) a été introduit et prévoit la fourniture de « *toute autre information nécessaire pour assurer un traitement loyal des données à l'égard de la personne concernée, compte tenu des circonstances particulières dans lesquelles les données à caractère personnel sont collectées* ». Sur ce point, le paragraphe 7 permet à la Commission d'adopter des actes délégués. Cette faculté de la Commission crée une certaine insécurité juridique, des obligations supplémentaires pouvant être imposées au responsable de traitement sans que celles-ci n'aient pu faire l'objet de débat en amont.
Concernant le point c), la durée pendant laquelle les données seront conservées peut être variable, d'autant plus si un recours intervient qui a pour effet d'allonger les délais.
L'article 14.5 prévoit un certain nombre d'exceptions et notamment le cas de figure où « *les données ne sont pas collectées auprès de la personne concernée et l'enregistrement ou la communication des données sont expressément prévus par la législation* » (point c). Il serait préférable de remplacer les termes « *enregistrement* » et « *communication* » par le terme plus général de « *traitement* » afin de ne pas être trop restrictif. A titre d'exemple, la « *conservation* » pourrait tout autant être citée dans ce paragraphe 5.

2. Droits des personnes concernées

Article 15 : Droit d'accès de la personne concernée

Conformément à l'esprit du texte, toute référence à la notion d'intérêt légitime de la personne concernée demandant l'accès aux données la concernant a disparu. Il n'est dès lors plus requis de faire valoir une justification particulière pour accéder à ses données. Ce droit d'accès semble fondamental. Aucun cas d'exception n'est prévu. Pourtant, les informations à fournir sont similaires à celles figurant à l'article 14 et il serait raisonnable de prévoir que, si celles-ci ont déjà été fournies lors de la collecte au titre de cet article 14, le responsable du traitement pourrait être exempté de les fournir de nouveau. Ce droit d'accès devrait en tout état de cause s'exercer en tenant compte des remarques formulées ci-dessus notamment quant à la forme de la réponse apportée ou au délai de réponse (paragraphe 2).
Proposition d'amendement : Ajout d'un paragraphe 1bis : « *les dispositions du paragraphe 1 ne s'appliquent pas lorsque la personne concernée dispose déjà des informations visées à ce paragraphe* ».

Article 17 : Droit à l'oubli numérique et à l'effacement

Cet article prévoit qu'une personne puisse demander l'effacement des données à caractère personnel la concernant. Cela n'est cependant pas adapté à la réalité des systèmes informatiques existants. Il parait peu réaliste, voire impossible, de supprimer toutes traces informatiques des traitements effectués étant donné que les données sont souvent conservées sur de nombreux serveurs de sauvegarde, souvent situés dans des lieux différents pour des raisons de sécurité, voire dans un autre Etat dans le cas des groupes de société dont la gestion des ressources informatiques est confiée à

la maison mère. Par ailleurs, il semble peu probable de parvenir à supprimer des données particulières compte tenu du nombre et du flux de données traitées chaque jour par une société et conservées de manière globalisées sur des serveurs centraux. Pour des raisons évidentes de sécurité, les copies de sauvegarde ne sont jamais manipulées ; elles ne sont pas accessibles de manière journalière). C'est la raison pour laquelle l'effacement total des données, y compris dans les archives (sauvegardes), ne sera jamais possible. Afin de permettre une application viable de cette disposition, le droit à l'effacement ne devrait concerner que les bases de données actuelles.

Il est heureux de relever que des cas d'exception sont prévus notamment dans l'hypothèse où la conservation des données est prévue par un texte de loi. Ce cas d'exception pourrait être étendu et il pourrait être également fait référence aux textes règlementaires.

Article 18 : Droit à la portabilité des données

Ces articles font uniquement référence aux traitements effectués de manière «*automatisée dans un format structuré*» sans intervention humaine. Le considérant 55 donne l'exemple d'une application automatisée en citant « *un réseau social* ». Ces articles ne s'inscrivent que dans le strict cadre de ce type de traitements. Ils ne sont en tout état de cause pas adaptés à une autre situation au vu des termes et des notions utilisés relativement vagues. Cet article devrait en conséquence préciser de manière liminaire : « *Dans le cas de données stockées sur des plateformes internet de réseaux sociaux,…* ».

Article 19 : Droit d'opposition

La notion de « *raisons impérieuses et légitimes justifiant le traitement* » est incertaine et introduit une insécurité juridique. Il appartiendra sans doute aux tribunaux de définir au cas par cas si le responsable du traitement avait des *« raisons impérieuses et légitimes justifiant le traitement* ».

Article 20 : Mesures fondées sur le profilage

Les restrictions prévues à l'article 20 sur le profilage ne doivent pas aboutir à l'impossibilité pour les établissements bancaires d'évaluer la capacité d'un client à rembourser un crédit. Il résulte en effet des directives européennes l'obligation pour le banquier au « crédit responsable » qui lui impose de vérifier la capacité de remboursement du client demandeur de prêt.

Chapitre IV - Responsable du traitement et sous-traitant

Article 28 : Documentation

L'un des objectifs du règlement semblait être celui d'alléger les charges administratives pesant sur les entreprises. Au vu de l'ensemble des obligations de documentation figurant à l'article 28, cet objectif n'est pas atteint. En effet, cet article implique un coût

administratif excessif en raison des chicanes administratives impliquées par le maintien de cette documentation.
Alors que bon nombre de notifications (pour des traitement ordinaires n'impliquant pas de traitement de données sensibles) bénéficient de dérogations et d'allègements sous l'empire de la directive de 1995, le nouveau projet de règlement implique que tout traitement devra faire l'objet d'une documentation, ce qui alourdit les charges administratives, contrairement à l'objectif affirmé du projet de règlement. Des dérogations devraient être prévues afin d'alléger les procédures pour des traitements habituels et mineurs.

Articles 31 et 32 : Violations de données à caractère personnel

Voir ci-dessus commentaires sous la définition de « violation de données à caractère personnel » (article 4.9).

Le délai de 24 heures pour déclarer toute violation est excessif, surtout si la violation n'emporte pas de conséquences pour la ou les personnes concernées. Un délai de 72 serait plus raisonnable, d'autant plus que, si la violation a été réalisée, le délai de notification ne permet de toute façon pas de revenir en arrière. Au contraire, le délai de 72 heures permettrait en outre de préciser les mesures qui ont immédiatement été prises, à la différence du délai de 24 heures, trop court.

Plutôt que de reporter à un acte délégué le fait de définir les cas dans lesquels la violation est « *susceptible de porter atteinte à la protection des données à caractère personnel ou à la vie privée de la personne concernée* », le texte des articles 31 et 32 devrait être plus précis et en limiter le champ d'application aux seuls cas dans lesquels la violation est susceptible d'entraîner, par exemple, le vol ou l'usurpation d'identité, une atteinte à l'intégrité physique, une humiliation grave ou une réputation entachée. Une telle restriction du champ d'application des obligations résultant des articles 31 et 32 aurait pour avantage de se calquer sur le régime de responsabilité du code civil, selon lequel chacun répond du dommage qu'il a causé. En l'absence de dommage, aucune obligation ne saurait être due.

Article 33 : Analyse d'impact relative à la protection des données

Le projet de règlement prévoit que les responsables de traitement devront effectuer une analyse d'impact relative à la protection des données lorsque les traitements présentent des risques au regard des droits et libertés des personnes concernées. La réalisation de telles analyses d'impact risque d'être lourde et coûteuse d'un point de vue administratif, d'autant plus que le projet de règlement impose de demander l'avis des personnes concernées au sujet du traitement prévu. Rien n'indique comment cet avis devra être demandé auprès des personnes concernées et il paraît en pratique très lourd administrativement d'adresser (par exemple) un courrier à l'ensemble des clients d'une entreprise pour recueillir leur avis. Rien n'indique non plus ce qu'il adviendra de cet avis. S'il s'agit d'un simple avis consultatif, un tel avis ne présente aucune utilité, et ne crée que des lourdeurs administratives supplémentaires.

Articles 35 à 37 : Délégué à la protection des données

L'article 35 assure une protection élevée du délégué à la protection des données dans l'entreprise. En particulier « *le délégué ne peut être démis de ses fonctions que s'il ne remplit plus les conditions requises pour l'exercice de celles-ci* ». Une telle formulation semble exclusive des dispositions de droit du travail des Etats membres. En tout état de cause, le délégué doit pouvoir être licencié comme tout autre employé en cas de faute grave.

Compte tenu du fait qu'une fonction réunissant les conditions d'indépendance requises par l'article 37 existe déjà dans les établissements financiers (celle de compliance officer), il serait opportun que le compliance officer puisse réunir les fonctions de compliance et de délégué à la protection des données.

Chapitre VI et VII – Autorités de contrôle

L'article 51 établit les compétences des autorités de contrôle. L'article 51.2 prévoit une autorité « *chef de file* » suivant le régime du « *guichet unique* ». Cette autorité est déterminée par le principal établissement du responsable du traitement.

La combinaison des définitions de « *responsable de traitement* » et de « *sous-traitant* » avec les dispositions relatives à la répartition des compétences entre autorités aboutit à une situation peu claire dans laquelle il est incertain quelle autorité sera compétente : celle du pays d'établissement du responsable du traitement ou celle du pays d'établissement du sous-traitant. La rédaction du texte risque d'aboutir à des situations peu claires, incohérentes ou plusieurs autorités de différents pays se considèrent comme compétentes. En effet, pour ce qui concerne les groupes d'entreprise, la détermination du « *responsable du traitement* » peut être complexe, et il est rare que la maison-mère ait réellement une vue d'ensemble de tous les traitements effectués par les différentes entités du groupe. Le considérant 27 et l'article 4(13) se réfèrent au lieu où sont prises effectivement les décisions, ce qui suppose « *l'exercice effectif et réel d'activités de gestion déterminant les décisions principales quant aux finalités, aux conditions et aux modalités du traitement dans le cadre d'une installation stable* ». Ce peut être, suivant le cas, soit le siège de la maison-mère, soit celui des filiales, soit des deux conjointement. Toutefois, ceci n'est pas automatique, dépend du type de traitement concerné et risque d'aboutir à des situations incertaines dans lesquelles différentes autorités pourraient être compétente pour un même groupe, suivant le type de traitement effectué. Le problème est que les relations entre maison-mère et filiales ne fonctionnent pas forcément suivant le modèle responsable de traitement – sous-traitant suggéré par le projet de règlement.

Si le principe du guichet unique est appliqué de manière stricte et implique que seule l'autorité du pays d'établissement de la maison mère est compétente, le risque pour le Luxembourg est de voir les compétences de la CNPD lui échapper dans la mesure où nombre d'entreprises implantées au Luxembourg sont des filiales. Il en est particulièrement ainsi dans le secteur bancaire et financier.

C'est la raison pour laquelle l'ABBL estime que le principe du guichet unique devrait être reconsidéré. La situation sous l'empire de la directive de 1995 est actuellement beaucoup plus simple et plus claire dans la mesure où chaque entreprise établie sur le territoire d'un Etat membre relève de la compétence de l'autorité de cet Etat membre. De plus, ce modèle permet également à chaque citoyen d'être assuré d'une proximité de l'autorité compétente face à un éventuel problème.

Enfin, la compétence des autorités de contrôle pour imposer des sanctions sera délicate à définir, tout dépend de la responsabilité de la faute, en fonction de l'entité (maison-mère ou filiale) responsable du traitement.

Chapitre VIII – Recours, responsabilité, sanctions

Article 73 : Droit d'introduire une réclamation auprès d'une autorité de contrôle

L'article 73.2 introduit le droit pour tout organisme, organisation ou association d'introduire une réclamation si les droits dont jouit une personne concernée ont été violés. Etant donné qu'il s'agit de vie privée, les actions collectives devraient être réservées au cas les droits de plusieurs personnes ou d'un ensemble de personnes déterminées (groupe de personne ayant un intérêt commun ou étant dans la même situation) ont été violés.

Article 77 : Droit à réparation et responsabilité

L'article 77 permet à toute personne ayant subi un dommage du fait d'un traitement illicite d'obtenir réparation du préjudice subi. Toutefois, l'article 77.3 procède à un retournement de la charge de la preuve dans la mesure où c'est au responsable du traitement de s'exonérer de cette responsabilité en prouvant que le fait qui a provoqué le dommage ne lui est pas imputable. Le principe de la responsabilité civile délictuelle est que c'est à celui qui prétend de prouver. La victime doit ainsi prouver la faute, qu'elle a subi un dommage et que le lien de causalité entre la faute et le dommage. Inverser la charge de la preuve risque de laisser place à un contentieux énorme où toute personne peut accuser une autre d'être à l'origine d'un dommage qu'elle aurait subi.

Article 79 : Sanctions

Outre les sanctions pénales (déterminées par chaque Etat membre), le projet de règlement prévoit que les autorités de contrôle peuvent imposer des sanctions administratives. Celles-ci sont extrêmement (même exagérément) élevées. S'il est compréhensible qu'elles doivent être dissuasives, de telles sanctions ne devraient pas aboutir à la fermeture d'une entreprise. Or, le niveau des sanctions (jusqu'à 1% du chiffre d'affaires annuel mondial) est tel qu'elles peuvent aboutir à l'asphyxie d'une société. De plus, la rédaction de l'article 79 laisse à penser que les autorités de contrôle ne disposent d'aucune marge de manœuvre et doivent imposer telle sanction en cas de violation de telle disposition du règlement. La rédaction de l'article 79 devrait laisser place à plus de flexibilité et laisser aux autorités de contrôle une marge de

manœuvre leur laissant la possibilité de choisir parmi un éventail de sanctions, en fonction du type de violation commis.

Concernant le point 6 n), il conviendrait d'ajouter à la fin de cette disposition *« sans préjudice de l'article 84* », dans la mesure où l'article 84 introduit des possibilités d'exemptions pour les professionnels soumis à un secret professionnel.

Actes délégués

La faculté pour la Commission européenne d'adopter des actes délégués est trop nombreuse (45 cas dans le projet de règlement) et excessive dans de nombreux cas. Cette faculté introduit une incertitude juridique. L'article 26(5), par exemple, donne des pouvoirs exorbitants à la commission pour ce qui concerne les responsabilités, obligations et missions du sous-traitant, le traitement de données au sein d'un groupe d'entreprises, etc.

Dans bon nombre de cas, les actes délégués sont envisagés pour définir ou préciser des éléments essentiels, qui devraient rester du ressort du règlement et non d'un acte délégué.

Le délai qui s'écoulera entre l'adoption du règlement et l'adoption des actes délégués comporte le risque d'une application extrêmement difficile du règlement tant que les actes délégués n'ont pas été adoptés. Pour une meilleure cohérence, soit le règlement devrait être plus précis et englober certains aspects laissés aux actes délégués, soit le règlement devrait surseoir à son application tant que les actes délégués n'ont pas été adoptés. Une telle manière de procéder s'impose considérant la lourdeur des sanctions pénales en cas de non-respect des dispositions du règlement.

Lien avec la législation actuelle

La question se pose de savoir si les nouvelles obligations imposées par le projet de règlement se substitueront totalement aux obligations sous l'empire de la directive de 1995 et des législations nationales qui l'ont transposée. En particulier, les entreprises ont déployés des efforts importants afin de se conformer à leurs législations nationales. Pour tous les traitements qui ont déjà été autorisés sous l'empire des législations nationales, une présomption de conformité devrait être introduite afin d'éviter de soumettre les entreprises à des études d'impact pour ces traitements. En revanche, un nouveau traitement devra respecter les règles issues du projet de règlement. Une clause en ce sens devrait être intégrée au projet de règlement.

Contact : bourin@abbl.lu