Les données sensibles revisitées (1999), préparé par M. Spiros Simitis

Professeur à l'Université Johan Wolfgang Goethe de Francfort sur le Main, Directeur du Centre de recherche pour la protection des données (Allemagne)

Examen des réponses au questionnaire du Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE 108) (Strasbourg, 24-26 novembre 1999)

I. Prémisses

La recherche d'une définition satisfaisante et d'une délimitation convaincante des «données sensibles» ainsi que l'analyse des conséquences des classifications des données à caractère personnel en vue d'une protection efficace des personnes concernées n'ont rien d'original. Elles ont même donné matière à réflexion dès que l'on a commencé à parler de protection des données. Les premières tentatives, en Norvège, visant à élaborer des méthodes pour faire des distinctions entre les données à caractère personnel, selon leur degré de sensibilité, sont tout aussi significatives pour l'importance accordée à une série de données dont le traitement était considéré comme particulièrement risqué pour les personnes concernées que la demande clairement formulée du législateur français d'interdire purement et simplement l'utilisation de telles données.

Si, au départ, comme l'illustre l'histoire des lois allemandes sur la protection des données, on s'intéressait essentiellement à la question de savoir si la «sensibilité» était réellement un critère valable pour déterminer les conditions du traitement, tant le contexte que les objectifs du débat ont été redéfinis par l'adoption de la Convention du Conseil de l'Europe sur la protection des données. Cette convention (article 6) sanctionne expressément la recherche d'un régime réglementaire particulier de données sensibles, position qui n'a cessé d'être réaffirmée par les recommandations du Conseil. Il est facile de voir les conséquences qui en découlent. L'existence de «données sensibles» par nature n'est plus contestée. La convention les a reconnues officiellement comme un élément central de tous les nouveaux règlements relatifs à l'utilisation des données à caractère personnel. Par conséquent, la seule question pertinente était dès lors de savoir comment satisfaire au mieux les attentes assurément restrictives imposées à l'utilisation des données sensibles énumérées par la convention.

Du coup, la référence aux données sensibles s'est ritualisée. Pas une seule loi adoptée après la convention ne néglige ou même n'omet d'inclure une disposition dont le libellé s'inspire de celui de la convention. Aussi évidentes que puissent être les différences entre, par exemple, les lois britannique, néerlandaise ou espagnole sur la protection des données, il est difficile de ne pas voir le consensus au sujet des données sensibles, qui bénéficient partout d'un statut spécial. Ainsi, lorsque la Directive de la CE sur la protection des données a été adoptée, en octobre 1995, la majorité des Etats membres, du fait notamment de l'influence du Conseil de l'Europe, avaient déjà soumis les données sensibles à des règles particulières. Il n'était donc pas surprenant que la directive s'ajoute à la liste alors déjà longue des règlements prescrivant un traitement particulier des données sensibles.

Mais la directive a opté pour une approche plus radicale. Au lieu de s'en tenir au libellé souple de la convention, elle interdisait le traitement des données sensibles mentionnées au paragraphe 1er de l'article 8. Si l'on veut apprécier correctement l'étendue de l'interdiction, il

faut tenir compte des différences structurelles entre la convention, d'une part, et la directive de l'autre. La convention n'est, au bout du compte, qu'une proposition. Les Etats se voient donner la possibilité de limiter les risques résultant du traitement de données à caractère personnel en appliquant un modèle réglementaire approuvé au niveau international. Toutefois, la convention ne préjuge pas de la décision. En d'autres termes, ils sont parfaitement libres de promulguer un règlement correspondant aux principes de la convention, d'élaborer des règles répondant mieux à leurs attentes, ou même de s'abstenir de toute restriction. Il n'en va pas de même dans le cas de la directive, dont les clauses ne sont pas des propositions, mais des prescriptions et dans la mesure où des alternatives sont tolérées, elles doivent s'intégrer au cadre réglementaire qu'elle définit. Lorsqu'un règlement commun est à la fois l'incitation et l'objectif, la conformité l'emporte nécessairement.

Par conséquent, des différences telles que des perceptions manifestement contradictoires des données sensibles ne peuvent être maintenues. Des pays qui, comme l'Autriche et l'Allemagne, avaient toujours refusé toute catégorisation abstraite des données à caractère personnel et préconisaient à la place une appréciation selon le contexte, doivent donc abandonner leur approche traditionnelle et reconnaissent expressément pour la première fois l'existence des données sensibles. C'est ainsi que la nouvelle loi autrichienne sur la protection des données énumère, conformément à la directive, les données sensibles (section 4, paragraphe 2) et précise, de nouveau en accord avec les attentes de la directive, les conditions de leur utilisation (section 9). De même, le projet de transposition de la directive dans le droit allemand confirme la volonté de revoir l'attitude adoptée jusqu'à présent à l'égard des données sensibles et incorpore des dispositions relatives à leur traitement.

En définitive, la directive termine donc ce que la convention avait commencé. Les données sensibles sont considérées, au niveau national comme au niveau international, comme un élément constitutif de tout règlement concernant l'utilisation des données à caractère personnel. Toutefois, aussi paradoxal que cela puisse paraître, plus la liste des lois attachant une importance particulière aux données sensibles s'allongeait, plus augmentait le nombre des questions critiques soulevées à propos de l'étendue précise de la sensibilité et de la crédibilité d'une approche intentionnellement prohibitive. Ainsi, les clauses insérées systématiquement dans un nombre sans cesse croissant de règlements n'ont pas dissipé les interrogations et les doutes. Mais on est progressivement passé de remarques assez générales à une analyse détaillée des données sensibles.

De fait, tant que la demande d'un régime clairement restrictif reprenait les formulations contenues soit, comme dans le cas de données révélant l'origine raciale, les opinions politiques ou les convictions religieuses, dans les constitutions nationales, soit, comme dans le cas des données sur l'état de santé, qui faisaient traditionnellement l'objet de règlements particuliers, il ne semblait pas nécessaire d'envisager d'aller plus loin. Les lois sur la protection des données insistaient simplement sur des exigences bien connues tout en soulignant qu'elles entendaient exclure l'utilisation de telles données. Toutefois, lorsqu'il faut transformer cette intention en orientations concrètes pour les diverses opérations de traitement, les références abstraites à des données sensibles se révèlent rapidement tout aussi indéfendables qu'une politique strictement prohibitive. Autrement dit, tous les règlements existants sont, malgré leurs différences, marqués par deux dilemmes fondamentaux qu'illustre également presque chaque réponse au questionnaire:

a. l'affirmation persistante que les données sensibles peuvent et doivent être définies de manière exhaustive se heurtent aux tentatives constantes de contourner ou de revoir la liste apparemment définitive;

b. l'intention catégoriquement déclarée de limiter radicalement le traitement des données sensibles est contredit par une liste pratiquement sans fin d'exceptions.

II. Règlements et expériences

1. La relativité des listes

Pour la plupart des lois sur la protection des données, l'énumération des données sensibles est exhaustive. C'est ainsi que les lois autrichienne, britannique, espagnole, estonienne, finlandaise, française, grecque, hongroise, italienne, suisse ou tchèque n'hésitent pas à qualifier explicitement d'exhaustive la liste qu'elles contiennent. Seul un très petit nombre de lois, par exemple celles du Danemark et de l'Islande, considèrent que leurs listes sont simplement indicatives. Mais ce qui apparaît à première vue comme une attitude incontestablement exceptionnelle exprime en réalité une conviction partagée par tous les législateurs. La grande majorité des lois actuelles peuvent certainement donner à penser que l'adjectif « sensible » est réservé à une catégorie exclusive de données soigneusement choisies par le législateur. En réalité, aucune d'entre elles ne se contente de dire que sa liste est exhaustive. Au contraire, toutes prévoient des moyens de rouvrir la liste en apparence définitivement close.

a. La clause législative

Le plus facile est probablement de déclarer, comme le fait par exemple la loi estonienne, que la liste peut être complétée par la loi. Ce qui ressemble à un truisme superflu a en fait une fonction stratégique. Le législateur peut à tout moment exercer son privilège pour déterminer le contenu de la loi, mais les individus peuvent être sûrs qu'il n'y a qu'un moyen de modifier la composition de la liste et par conséquent l'accès aux données les concernant, à savoir l'adoption d'une loi. La modification est donc liée à un processus rigoureusement formalisé qui garantit un maximum de transparence et de stabilité et les protège donc contre des changements trop rapides et trop nombreux. Mais l'intervention du législateur a également un autre aspect important. Elle est la preuve qu'il n'y a pas de liste définitive de données sensibles. L'idée encore répandue selon laquelle la liste ne contient pas plus que quelques données fixées une fois pour toute est une pure fiction. Le mieux que l'on puisse espérer est qu'au moins certaines de ces données soient incluses dans la plupart des énumérations. L'intervention du législateur illustre et concrétise la variabilité de la liste.

Que cette intervention n'est qu'un moyen théorique de mettre en question et revoir la composition de la liste, les réponses au questionnaire le démontrent. Ainsi, la Finlande a modifié l'énumération initiale afin d'inclure l'appartenance à un syndicat, addition envisagée également par les Pays-Bas et la Norvège. Ces deux pays entendent en outre réviser l'énumération actuelle, le premier en supprimant les données d'ordre psychologique, le second en redéfinissant la référence aux affaires familiales. Le Portugal, enfin, a renoncé, tout comme l'Estonie, à une protection spéciale des données liée aux biens et à la situation financière des personnes concernées, mais a inclus dans sa liste les données génétiques. Chacun de ces cas montre que l'énumération des données sensibles est partout considérée comme une indication éphémère. Les législateurs, tout comme l'avait annoncé le T-PD, lors de sa 4ème réunion, en

mai 1990, concernant l'application de l'article 6, partent du principe qu'il y aura réexamen de la liste, en fonction, à la fois de l'expérience de l'utilisation des données individuelles et de nouvelles exigences.

L'inclusion de l'appartenance à un syndicat est un exemple typique d'alignement sur des règles élaborées par les tribunaux dans des affaires de discrimination ainsi qu'à l'occasion de questionnaires utilisés par les employeurs. Pour ce qui est des données relatives à la situation financière, l'abandon de leur statut spécial est en particulier le résultat de l'impact croissant des lois d'ouverture, dont le principal objectif est d'accroître la transparence des activités financières. La nécessité de limiter néanmoins l'accès aux informations en relation avec la situation financière et, par conséquent, sur la solvabilité des personnes concernées est on ne peut mieux illustrée par le rôle fondamental des lois sur la protection des données à propos du traitement des données sur les consommateurs. Mais pour nécessaires que soient des mesures restrictives, elles ne justifient évidemment pas, comme le montrent par exemple la loi danoise sur les registres privés ou la loi irlandaise sur la protection des données, d'être intégrées à une liste de données sensibles. Enfin, rien n'illustre mieux la nécessité de mettre à jour les listes que les données génétiques. On n'en parlait pratiquement pas lorsque les premières listes ont été établies. Mais aujourd'hui, il n'y a aucun doute qu'aucune autre catégorie de données ne donne d'informations aussi complètes sur les personnes concernées. Les risques du traitement de données à caractère personnel n'avaient donc jamais été aussi évidents auparavant. Qu'il s'agisse de la possibilité de trouver un emploi, des chances d'obtenir une assurance maladie ou des limites de la marchandisation croissante des individus, l'accessibilité des données génétiques détermine la réponse. Aucune liste de données sensibles ne peut donc négliger les données génétiques sans que l'on s'interroge sur son sérieux.

b. Le processus d'interprétation

On peut aussi assurément modifier les listes en interprétant les éléments qui y figurent déjà. Les réponses au questionnaire montrent que le processus d'interprétation a du reste influé sur l'étendue des listes. Si la plupart des données se retrouvent sur toutes les listes, il est clair que leur interprétation n'est pas identique. C'est ainsi que les lois estonienne, française et norvégienne reconnaissent que les restrictions applicables au traitement des données liées à la race ou à l'origine ethnique ne sont pas pertinentes pour la nationalité. En d'autres termes, elles considèrent toutes la nationalité comme une donnée manifestement «non sensible». Le droit autrichien adopte une position plus libérale, et voit dans la nationalité une donnée «moins sensible». La CNIL, en revanche, n'est manifestement pas disposée à «banaliser» réellement les données sur la nationalité. Elle demande en fait que l'on analyse de façon approfondie, en tout état de cause, la nécessité de les traiter. La loi néerlandaise va nettement plus loin. D'après l'exposé des motifs du décret sur les données sensibles et l'opinion de l'organe chargé de la protection des données, l'application correcte des règles régissant l'utilisation de données indiquant la race ou l'origine ethnique présuppose une interprétation large qui doit nécessairement couvrir aussi la nationalité.

Les données génétiques constituent un autre exemple tout aussi significatif. Dans leur cas, étant donné l'absence de référence explicite dans les listes de données sensibles, l'interprétation joue un rôle particulièrement important. Elle peut même aider à combler la lacune. Il ne faudrait toutefois pas sous-estimer les difficultés. Il y a certainement des cas où il est tout à fait possible de considérer les données génétiques comme des données sanitaires ou médicales. Mais il n'est pas justifié pour autant de conclure que les données génétiques peuvent être classées en toute circonstance dans l'une ou l'autre de ces deux catégories. La

plupart des lois ont donc évité une classification générale et insistent à la place sur les utilisations spécifiques des données génétiques. L'importance croissante de ces dernières rend toutefois difficile le maintien d'une approche aussi soigneusement différenciée qui laisse inévitablement de côté un nombre sans cesse croissant d'opérations de traitement. C'est pourquoi les premières hésitations ont été progressivement abandonnées. Les données génétiques, comme le montrent l'exemple des lois autrichienne, islandaise, norvégienne, portugaise et suisse, mais aussi la Recommandation R (99) 5 sur la protection des données médicales, sont simplement classées comme données sanitaires ou médicales. Et même là où le doute persistait, les interventions répétées du législateur, invariablement pour limiter l'utilisation des données génétiques, étaient, comme en France, considérées comme une preuve de la sensibilité particulière de ces dernières, justifiant pleinement qu'elles soient traitées comme toutes les autres données sensibles.

c. L'incidence du contexte

Les considérations comme celles qui sous-tendent la clause législative et le processus d'interprétation aboutissent tôt ou tard à un point de vue qu'illustrent les réponses britannique, danoise, française et suisse au questionnaire. La sensibilité n'est plus perçue comme un attribut donné a priori. Au contraire, toute donnée à caractère personnel peut, selon l'objectif ou les circonstances du traitement, être sensible. Par conséquent, il faut évaluer les données par rapport au contexte qui détermine leur utilisation. Les intérêts particuliers du contrôleur ainsi que des destinataires potentiels des données, les buts pour lesquels celles-ci sont recueillies, les conditions du traitement et ses conséquences possibles pour les personnes concernées sont des facteurs qui, au total, permettent de discerner à la fois l'étendue et les effets du traitement et ainsi de déterminer son degré de sensibilité. Une évaluation de la sensibilité demande donc plus qu'un simple coup d'œil sur les données. Il est fort possible, par exemple dans le cas de données génétiques ou de données sur les condamnations pénales, que les risques pour les personnes concernées soient plus ou moins évidents mais la sensibilité ne peut être réellement affirmée que si tous les éléments caractéristiques de l'opération particulière de traitement sont pris en compte.

L'importance du contexte est également illustrée par deux exemples assez atypiques qui sont tous deux mentionnés dans le questionnaire. Le premier est le cas des images et des sons. L'Autriche, le Danemark, la France, l'Islande, l'Italie, la Norvège, les Pays-Bas et la Suisse ont répondu exactement de la même façon. Tous ces pays ont souligné le lien entre les circonstances du traitement et toute tentative de classer les données. Et de fait, dans la plupart des lois nationales, il est clair maintenant qu'il importe peu que les données soient stockées dans un ordinateur, regroupées dans un fichier ou contenues sur une cassette vidéo tant qu'elles peuvent être attribuées à une personne identifiable. L'étape suivante, toutefois, dépend elle aussi du contexte. Ces éléments caractéristiques ouvrent ou au contraire ferment la voie à des règles qui resserrent les restrictions. Par exemple, des données sur des photos et des cassettes vidéo, comme le font observer les réponses néerlandaise, italienne et norvégienne, peuvent être sensibles toutes les fois qu'elles révèlent des informations sur la race ou sur le comportement sexuel de la personne concernée. Le législateur peut, comme le montre par exemple la réponse de la France, limiter la compétence de l'organe de supervision en cas de vidéo-surveillance des espaces publics. Il n'y a toutefois pas de règlement de ce genre pour l'évaluation des données. Au contraire, la surveillance des espaces publics, comme cela est illustré par les cassettes vidéo de la police couvrant des manifestations, est un exemple particulièrement pertinent de la sensibilité des données recueillies.

De même, l’utilisation d'identificateurs personnels, quelle qu’en soit la forme, est inévitablement liée au traitement de données à caractère personnel. En outre, la sensibilité d'au moins certains des identificateurs semble être hors de question. Les empreintes génétiques, les numéros de sécurité sociale et numéros d'identification personnelle sont les exemples les plus évidents. Mais là encore c'est malgré tout une approche fondée sur le contexte qui prédomine. Un usage clairement limité à des fins définies de façon exhaustive par la loi et l'exclusion délibérée de chiffres donnant des informations sur les personnes concernées sont parmi les mesures qui, comme l'illustrent les réponses des Pays-Bas, de la France, du Portugal et de la Suisse, permettent mais en même temps restreignent l'utilisation d'identificateurs personnels à quelques opérations de traitement spécifiées dans des conditions clairement prescrites.

C'est, enfin, la même approche résolument axée sur le contexte qui domine enfin lorsque des données à caractère personnel sont regroupées pour l'établissement d'un fichier soit général, soit, comme dans le cas des données de transmission, un fichier sur la mobilité. Comme le montrent des dispositions telles que l’article 15 de la Directive ou l’article 2 des lois françaises sur la protection des données, les profils sont particulièrement sensibles lorsqu'ils reposent sur un traitement automatisé de données à caractère personnel. La réflexion sur les profils ne remplace toutefois pas les considérations sur les données utilisées. Il faut au contraire évaluer ces dernières dans chaque cas en tenant compte de leur utilisation possible pour un profil particulier. C'est précisément pour cela que le traitement des données de transmission, par exemple, est soumis à des restrictions impératives délimitant leur employabilité. Pour résumer, les classifications absolues des données à caractère personnel sont, là comme ailleurs, remplacées par une évaluation de la situation. La sensibilité n'est plus un attribut accordé une fois pour toutes, mais une caractéristique déterminée par le contexte de l'usage prévu qui doit donc, en conséquence, être constamment réévalué.

2. Diversité des données

L'hypothèse selon laquelle certaines données sont sensibles par nature conforte l'idée qu’elles font partie d'un petit groupe de données reconnues au niveau national et international, interprétation qu’encouragent le libellé de la convention comme celui de la directive. Pourtant, les réponses au questionnaire donnent une image différente, qui confirme en fait une tendance visible depuis les premières années de la protection des données. S’il est vrai que la reconnaissance des données énumérées par la convention ainsi que par la directive transcendent de loin les frontières nationales, il est exact aussi que ces mêmes données ne sont en définitive rien de plus que le noyau dur des listes nationales. Les législateurs nationaux ont allongé la liste primaire de toute une série de données très différentes, mais qui ont tout de même quelque chose en commun. Le choix des données supplémentaires reflète les problèmes caractéristiques d'un pays ou d'une société particulière. En d'autres termes, alors que le noyau dur est fondé sur des énumérations étroitement liées aux conventions internationales sur les droits de l'homme, les additions renationalisent, du moins jusqu’à un certain point, l'intervention du législateur.

Un premier exemple, quelque peu surprenant, est celui des données concernant l'appartenance à un syndicat. La convention ne les avait pas incluses, la directive les cite expressément. La divergence n'a rien d'accidentel. A l'époque de la convention, les Etats scandinaves, en particulier, ne voyaient aucune raison de les mentionner. Pour eux, une telle référence est tout simplement inutile lorsque la négociation collective fonctionne de façon efficace et sans heurts. Mais pour ceux qui préconisaient l'inclusion de ces données, l'argument décisif était

que, selon leur expérience, les travailleurs syndiqués étaient encore en butte à des discriminations, qu'il fallait donc les protéger en empêchant une collecte des données révélant l'appartenance à un syndicat. Mais les points de vue divergent encore, comme l'illustrent les réponses de l'Autriche. Ils coïncident tout à fait avec la position défendue à la fin des années 70 et au début des années 80 en particulier en Norvège et en Suède.

Un deuxième exemple, tout aussi caractéristique, est celui des références aux données sur la sécurité sociale, par exemple dans les lois grecque et suisse. La formulation, en droit danois et islandais, est plus générale. Au lieu de mentionner la sécurité sociale, il est question de données liées aux «problèmes sociaux». Mais il s'agit d'informations liées au soutien fourni dans des situations économiquement, physiquement et psychologiquement critiques. Toutefois, même dans les pays où, comme en Allemagne, la loi a délibérément renoncé, jusqu'ici, à énumérer les données sensibles, le traitement des données de sécurité sociale est soumis à un régime nettement restrictif. Il y a peu d'autres obstacles aussi élevés que le «secret social». La justification est partout la même. Dans la mesure où les risques individuels sont socialisés, la transparence du comportement individuel augmente. L'octroi d'un soutien est conditionné par une quantité sans cesse croissante de données décrivant méticuleusement à la fois les problèmes et la situation générale des personnes concernées. Par conséquent, là où les systèmes de sécurité sociale sont institutionnalisés et constamment étendus, les données qu'ils traitent atteignent rapidement le plus haut degré de l'échelle de sensibilité.

Les transformations sociales sont également à l'origine du troisième exemple. Les drogues et la toxicomanie génèrent leur propre base de données. Celle-ci va d'une documentation détaillée de l'histoire personnelle des personnes concernées et d'informations sur les diverses formes d'aide fournie aux données policières et condamnations pénales. Pour nécessaire que puisse être le recueil de données, il accentue inévitablement la vulnérabilité des personnes concernées. Des lois comme les lois islandaise et norvégienne sur la protection des données ont, en conséquence, expressément inclus les données liées à une toxicomanie ou à l'alcoolisme dans leurs listes de sensibilité.

3. Degrés de protection

La logique de la sensibilité semble impliquer que toutes les données en cause devraient l'objet du même degré de restriction. C'est pourquoi la plupart des réponses au questionnaire rejettent catégoriquement l'idée que les degrés de protection puissent différer. Le refus pur et simple a parfois été souligné par une déclaration permettant de discerner l'argument décisif. Ainsi, la réponse de l'Italie attire l'attention sur la structure de la disposition pertinente de la loi sur la protection des données. Comme dans tous les règlements similaires, la loi juxtapose simplement les diverses données et choisit une formulation qui désavoue toutes les tentatives de traiter quelques données que ce soient différemment.

Mais c'est l'inverse qui se produit. Déjà trois des lois qui sont favorables, au moins «en principe», à des règles uniformes, tolèrent des distinctions. Les réponses de l'Autriche, de la France et de l'Italie attirent l'attention sur le degré élevé de sensibilité des données génétiques et de la nécessité de garantir en conséquence une plus grande protection. La réponse de la Hongrie va plus loin et préconise ouvertement une hiérarchie. En particulier, les données concernant l'origine raciale ou ethnique, les opinions politiques, l'affiliation à un parti ou les convictions religieuses sont considérées comme plus sensibles. La loi danoise intensifie également la protection des données liées aux «questions politiques» mais en partie seulement. Tant qu'elles n'ont pas été accessibles au grand public, il est interdit de les traiter.

La tendance à assouplir les restrictions pour certaines des données sensibles n'est pas moins courante. L’exemple classique est celui des condamnations pénales. Il est intéressant de noter que ni la convention ni la directive ne les incluent dans leur liste actuelle. Elles sont citées et, dans le cas de la directive, également traitées à part. Mais qu'elles soient directement placées sur la liste des données sensibles ou simplement mentionnées en liaison avec elles, aucune loi n'a jamais envisagé d’interdire absolument le traitement des condamnations pénales ou même d'assimiler les restrictions à leur utilisation à ce que l'on considère en général comme une norme appropriée pour les données sensibles. Au contraire, toutes les lois optent pour un système canalisant avec soin l'accès.

Les condamnations pénales confirment et soulignent ainsi la réponse des Pays-Bas au questionnaire. Il n'y a pas, en définitive, de catégorie spéciale de données sensibles, mais simplement un régime spécial pour chacune de ces catégories de données. Leur utilisation peut être considérée en général comme une source possible de risques particuliers pour les personnes concernées. Toutefois, la question de savoir si ces risques justifient une exclusion de leur traitement, et jusqu'à quel point, ne peut faire l'objet que d'une réponse séparée pour chaque catégorie de données et tenant compte des circonstances propres à leur utilisation spécifique. Ainsi, aussi bien la relativité des restrictions que la nécessité d'une approche situationnelle se trouvent une fois de plus confirmées.

III. Conclusions et recommandations

1. Souplesse croissante

La volonté d'élaborer et d'appliquer des règles intensifiant la protection des personnes concernées selon le degré de sensibilité des données traitées est évidente. Mais, d'une part, il n'existe pas de liste exhaustive généralement acceptée de données sensibles, et d'autre part leur utilisation ne peut être interdite inconditionnellement. Les sources des listes varient autant que leur contenu. Les accords internationaux et les constitutions nationales ne font que répondre à des demandes spécifiques de branches particulières des droits nationaux et à l'apparition de nouveaux problèmes sociaux et politiques à l'origine de leurs composantes.

En outre, la sensibilité n'est jamais qu'un dispositif d'alarme. Elle signale que les règles normalement applicables au traitement des données à caractère personnel ne garantissent peut-être pas une protection adéquate. Sa conséquence première est donc de stimuler un processus de réflexion dont l'objectif est de repérer une faiblesse des règlements existants et de définir les améliorations nécessaires. Aussi bien le point de départ que l'étendue de toutes les considérations sont déterminés par les contextes potentiels des traitements. Ils permettent de discerner les risques spécifiques et de concevoir les antidotes. Autrement dit, l'interdiction est une conséquence possible, mais en aucune manière obligatoire. Et même lorsqu'il apparaît justifié d'interdire l'utilisation de certaines données, l'interdiction demeure une réaction circonscrite au contexte qui légitime et en même temps limite l'exclusion du traitement.

Pour qu'un règlement soit à la fois crédible et transparent, il faut donc que deux conditions soient respectées. Premièrement, les règlements généraux doivent bannir les énoncés déclarant expressément ou implicitement que tout traitement de données sensibles est interdit. Tout ce qu'ils peuvent demander est une protection adéquate. Deuxièmement, les listes de données sensibles doivent être libellées d'une manière qui indique sans ambiguïté leur caractère de simple exemple. Leurs composantes peuvent donc toujours être complétées ou remplacées.

Ces deux impératifs, toutefois, révèlent et soulignent aussi les limites des règlements généraux. Si c'est véritablement le contexte qui doit être le critère principal sur lequel on s'appuie pour réaffirmer les éléments indispensables d'une protection adéquate, les conditions du traitement doivent être fixées dans un règlement sectoriel. C'est seulement lorsque le législateur peut se concentrer pleinement sur un contexte particulier qu'il est aussi en mesure d'atteindre un degré de précision correspondant de façon satisfaisante aux particularités des circonstances du traitement. Une approche situationnelle, comme l'on démontré toutes les expériences au niveau national et au niveau international, est aussi nécessairement une approche sectorielle.

2. Garantie d'une protection fiable

Les règles résolument fondées sur le contexte ne constituent toutefois que l'une des conditions d'un règlement à la fois satisfaisant et efficace des données sensibles. L'autre condition tout aussi décisive est la réduction des listes actuelles d'exception à quelques cas énumérés de façon exhaustive et définie avec précision. Pratiquement aucune des exceptions actuelles ne peut faire l'économie d'un examen approfondi. Déjà, l'exception apparemment incontestable qui vient en tête de chaque liste - le consentement de la personne concernée - n'est guère convaincante. Le consentement, contrairement à une opinion encore répandue, n'est pas un passe-partout ouvrant l'accès à n'importe quelles données auxquelles s'intéressent les responsables potentiels du traitement. Les relations employeurs/employés ne sont qu'un exemple parmi beaucoup d'autres montrant que le consentement ne garantit pas nécessairement une participation des personnes concernées leur permettant de décider librement si les données qui les concernent pourraient être traitées à des fins connues d'eux et approuvées par eux. Les possibilités d'agir et d'influer sur le traitement dépendent essentiellement des circonstances dans lesquelles il est demandé aux personnes concernées de donner leur accord et plus précisément de leur position particulière par rapport à celui qui traite les données. Les relations employeurs/employés soulignent l'aspect fallacieux de l'hypothèse selon laquelle le consentement inclut et garantit le pouvoir des personnes concernées de déterminer l'utilisation des données qui se rapportent à elles. C'est pourquoi aussi bien les lois nationales que des documents internationaux tels que le code de pratique de l'OIT sur la protection des données à caractère personnel des travailleurs excluent délibérément un consentement toutes les fois que l'employeur a l'intention d'utiliser, par exemple, les données sur les condamnations pénales ou les données génétiques. C'est la loi et non les parties qui, dans chaque cas, conditionnent l'accès.

Mais le point qui est probablement le plus critique, sur les listes d'exception, tient aux clauses qui légitiment un accès pour des motifs d'intérêt public ou pour lutter contre des activités criminelles et garantir la sécurité publique. Des termes comme «intérêt public» ou «sécurité publique» sont de facto une carte blanche permettant de contourner en fin de compte toutes les restrictions. C'est pourquoi les références à l'un comme à l'autre sont généralement suivies d'une phrase précisant que les conditions de l'accès doivent être régies par la loi. Toutefois, toutes les dispositions de ce type portent uniquement sur la forme, et non sur la substance des règles futures. L'intérêt public et la sécurité publique demeurent donc une source inépuisable d'interventions adaptant le traitement des données sensibles aux politiques de l'Etat. C'est ainsi que la crise des systèmes traditionnels de sécurité sociale n'a fait qu'intensifier les efforts visant à obtenir un nombre sans cesse croissant de données sanitaires, non seulement pour mettre en place une base de données solide pour la réduction devenue urgente et indispensable des coûts de plus en plus élevés, mais aussi pour des mesures destinées à inciter les personnes concernées à acheter moins de médicaments et à réduire substantiellement le nombre de

visites chez le médecin. L'impact de ces politiques sur les efforts déployés pour promulguer des règles applicables au traitement des données sensibles est facile à repérer dans la directive.

Au total, les dispositions ne contenant pas plus de quelques termes très généraux imposent aux personnes concernées le risque d'un accès à leurs données dont les conditions et les limites sont indiscernables. De plus, elles contredisent ouvertement l'intention du législateur de restreindre sérieusement le traitement dans le cas des données sensibles. La sensibilité se trouve ramenée à une fonction purement ornementale lorsque l'accès peut être élargi sans aucune difficulté. Les exceptions ne peuvent certainement être évitées. Mais pour justifiées qu'elles puissent paraître, elles sont intolérables tant que leur formulation n'est pas précise, leurs objectifs et leurs conséquences non clairement déterminés, les données demandées non limitées aux informations réellement nécessaires et l'utilisation limitée à des responsables de traitement définis de façon non ambiguë.

3. Effets extraterritoriaux

Les règlements soumettant les données sensibles à un régime particulièrement protecteur attirent spécialement l'attention sur les flux transfrontières. Plus on insiste sur la sensibilité, plus il apparaît logique de garantir l'utilisation de données sensibles indépendamment du lieu où elles sont traitées. Au moins tant que la sensibilité est considérée comme une émanation de valeurs fondamentales universellement reconnues, comme le respect des opinions politiques et des convictions religieuses, ou le rejet de la discrimination raciale et ethnique, des règles spéciales pour les flux transfrontières semblent être un complément obligatoire des dispositions régissant le traitement des données sensibles à l'intérieur des frontières nationales.

Toutefois, avant d'étendre le régime spécial, il faudrait examiner attentivement les effets des normes usuellement applicables. Le principe fondamental a déjà été élaboré par les premières lois sur la protection des données et sans cesse réaffirmé depuis lors par tous les règlements nationaux et souligné dans nombre des réponses au questionnaire. Il ne peut y avoir de transfert que si une protection équivalente est garantie dans le pays du destinataire. La recherche d'une telle protection s'applique à toutes les données à caractère personnel. En outre, elle n'implique pas l'existence de dispositions identiques. Tout ce qu'elle demande est un règlement fonctionnellement équivalent. C'est exactement dans ce sens que la directive (article 25) non seulement demande un niveau adéquat de protection, mais énumère aussi, compte tenu de l'expérience des autorités nationales de protection de données, certains des critères à prendre en compte afin d'évaluer correctement les règles dans le pays du destinataire.

En résumé, ni le déroulement ni le résultat de l'évaluation ne sont déterminés par des considérations abstraites, mais par des circonstances caractérisant l'opération de traitement spécifique. En d'autres termes, ce qui compte, c'est le cas individuel. Par conséquent, toutes les fois que le traitement concerne des données soumises à un traitement spécial, l'admissibilité d'un transfert dépend de l'existence d'une protection bénéficiant du même privilège dans le pays de destination. Cette approche est manifestement partagée par le T-PD lors de sa 8ème réunion en janvier 1993 sur l'interprétation de l'article 6 de la Convention et tout particulièrement sur les « garanties appropriées » requises par la Convention pour toute utilisation de telles données. L'approche cas par cas garantit donc une souplesse qui permet d'adapter les exigences afin d'assurer une protection correspondant aux risques du transfert

particulier. Par conséquent, des dispositions supplémentaires portant spécifiquement sur les flux transfrontières de données sensibles sont superflues.

Il peut toutefois être indiqué de compléter le chapitre III de la convention par des dispositions portant explicitement sur la transmission de données à caractère personnel à des pays qui ne sont pas parties à la convention. D'autant que les règlements actuels incitent manifestement à des erreurs d'interprétation, en particulier dans le cas de données sensibles. Une règle telle que celle qui figure au paragraphe 3 de l'article 12 n'est compréhensible que s'il existe des normes communes régissant le traitement de données à caractère personnel. Mais précisément, cette hypothèse, à quelques exceptions près, ne s'applique pas aux Etats qui ne sont ni parties à la convention ni membres de l'Union européenne.